шифрування трафіку (TLS, SRTP), VoIP фаєрволу (обхід NAT, приховування топології мережі, конфіденційність користувача, стан дзвінків та сесій) та листи контролю доступу ACL (“чорні” та “білі” списки, захист від DoS атак).

Перелік посилань:

1. Звіт Communications Fraud Control Association // Fraud Loss Survey // 2019 URL:https://cfca.org/slug/cfca-2019-fraud-loss-survey-pdf

Скрипка Олександр Володимирович
студент групи УБД-21, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. БАЗИ ДАНИХ З ОСОБИСТИМИ ДАНИМИ КОРИСТУВАЧІВ У ВІДКРИТОМУ ДОСТУПІ

За умов стрімкого зростання кіберризиків і кіберзагроз важливим є висвітлення основних проблем національної системи кіберзахисту. В умовах війни з Росією нам необхідно постійно мати повноцінну і точну інформацію про нашого ворога. Але також не потрібно забувати і про власну безпеку. Найбільш чутливими даними є інформація про громадян(їх особисті дані), критичну інфраструктуру, комерційні компанії, державні установи(документи державного значення, державні таємниці). В тезі розглянуто одну із найактуальніших проблем сьогодення в сфері інформаційної та кібербезпеки – витік персональних даних користувачів в масштабні бази даних, які знаходяться у відкритому доступі.
Ключові слова: безпека, база даних, інформація, персональні дані, користувачі, відкритий доступ, конфіденційність, загроза інформаційній безпеці.

Сьогодні життєдіяльність людини є неможливою без надання інформації про себе іншим членам суспільства, державним органам, громадським організаціям. Як зазначено у ст. 2 Закону України «Про інформацію» від 02.10.1992 р. [1, с. 650], кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свободи і законних інтересів. Широке розповсюдження і застосування інформаційних технологій, глобальних інформаційних систем, введення автоматизованих баз даних, суттєво спрощує реалізацію громадянами цього права. Але попри всі переваги є один суттєвий мінус: існує великий ризик несанкціонованого втручання в особисте життя людини і неправомірне використання особистих даних. Тому право на захист персональних даних є одним з фундаментальних прав людини. Конституцією України закріплено положення про те, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Попри закон, недобросовісні власники сайтів та програм користуються незнанням і неуважністю користувачів. Дуже часто при прийняті “Умов використання’’ програмою і/або послугами сайту мало хто звертає увагу на пункт “Передача персональних даних’’. Зазвичай, саме там вказано умови зберігання та обробки персональних даних, їх передача третім особам для

надання послуг. Через недбале виконання умов і ненадійний захист інформації зі сторони постачальника послуг, дані користувачів опиняються у відкритому доступі(зазвичай у вигляді баз даних). В більшості випадків компанія, яка надає послуги користувачам, може продати їх дані іншим компаніям заради вигоди. Або піддатися хакерській кібератаці, мета якої викрасти персональні дані користувачів для подальшого аналізу і використання в особистих цілях. Прикладом може бути витік персональних даних користувачів таких компаній як ПриватБанк, Нова пошта, Київстар, Moneyveo. Приклад наведено на рис. 1. Крім комерційних компаній, є приклади і державних установ таких як: ДАІ(Державна автомобільна інспекція), ДРФО(Державний реєстр фізичних осіб), ЦВК(Центральна виборча комісія), Центральний державний електронний архів. Приклади наведено на рис. 2 та рис. 3.

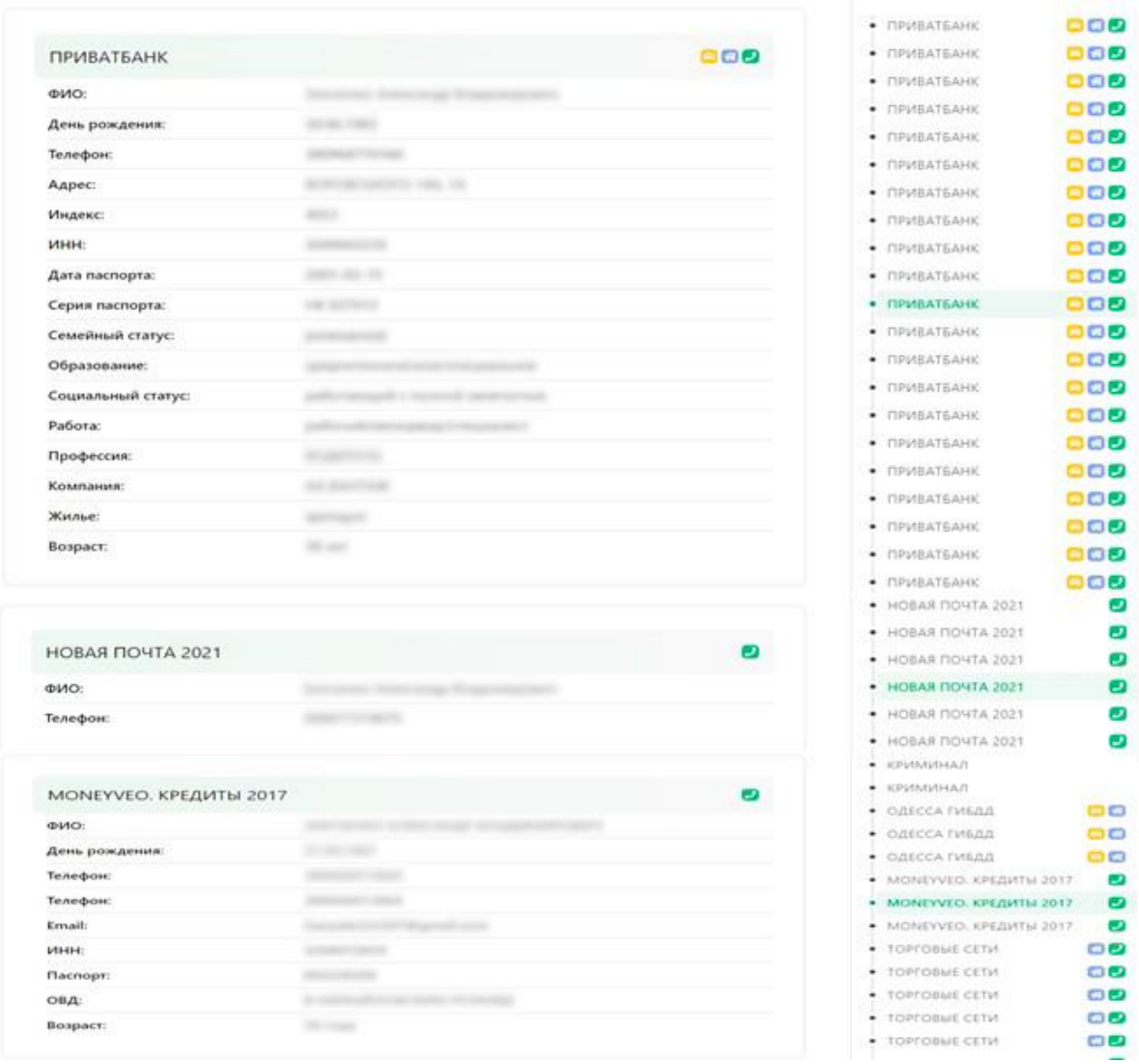


Рис. 1 – відомості про користувачів в базі даних “Комерційних компаній”

Рис. 2 – відомості про користувачів в базі даних ДРФО

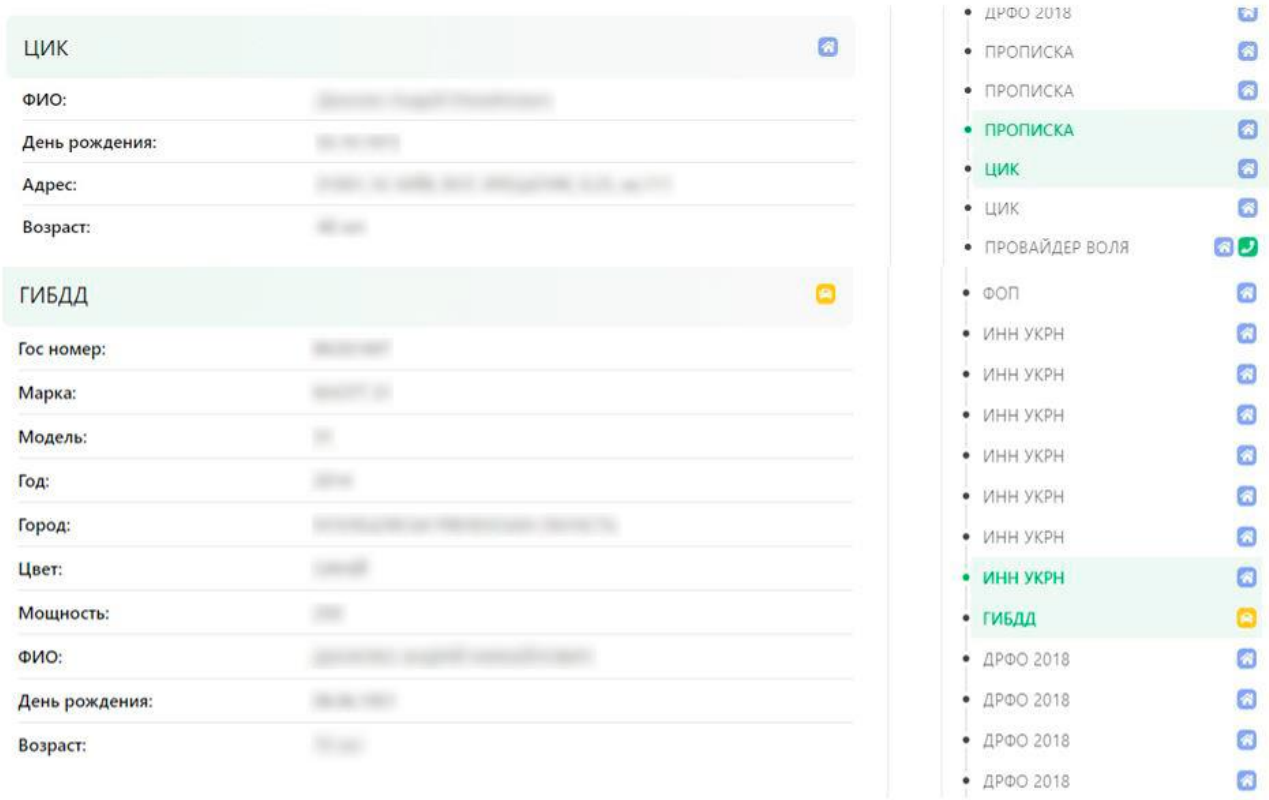


Рис. 3 – відомості про користувачів в базі даних ЦВК та ДАІ

Дані користувачів на рисунках приховано відповідно до статті 32 Конституції України[4, с. 141]. Майже всі відкриті бази даних України, Білорусі та Росії містяться в Telegram боті, який розроблений російською платформою “Глаз Бога”, що спеціалізується в наданні послуг з кібербезпеки та аналізу великої кількості даних. Цей бот є дуже потужним інструментом пошуку даних та відомостей, що дійсно загрожує безпеці нашої держави на інформаційному та кібер фронтах. Не варто забувати, що і користувачі, переважно, самі “віддають” свої дані зловмисникам. Найпоширенішим методом введення в оману користувачів є соціальна інженерія. Проблема полягає в тому, що велика кількість користувачів не має достатніх навичок цифрової грамотності в інформаційному та кіберпросторі. Проєкт Міністерства цифрової трансформації “Дія.Цифрова Освіта” набирає все більшої популярності серед інтернет

користувачів та являє собою онлайн-платформу, мета якої навчити користувачів цифровим навичкам за домогою освітніх серіалів та бліц-опитувань. Тому необхідно приділяти увагу як стану захищеності даних, так і цифровому розвитку громадян.

Перелік посилань:
1. Про інформацію: Закон України від 02.10.1992 р. // Відомості Верховної Ради України (ВВР). – 1992. – № 48. – ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Платформа “Глаз Бога”. URL: https://ru.wikipedia.org/wiki/Глаз_Бога
3. Зелена книга “Правові взаємовідносини в інтернеті”. URL: https://issuu.com/internews-ukraine/docs/_____7952f9f78639d6
4. Конституція України [Електронний ресурс] // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – с. 141. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

Вдовиченко Максим Сергійович, студент БСДМ-61
Державний університет телекомунікацій

ЗАХИСТ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

Фахівцям з кібербезпеки добре відоме таке поняття, як кінцева точка. Під цим терміном маються на увазі кінцеві пристрої в мережі: робочі станції, ноутбуки, планшети, смартфони, сервери. Кожне робоче місце співробітника організації та будь-яке периферійне устаткування, підключене до мережі - це кінцева точка, яка може стати об'єктом атаки. Відсутність належного захисту цього сегмента корпоративної мережевої інфраструктури може призвести до катастрофічних наслідків.

Безпека кінцевих точок — це практика захисту кінцевих точок або точок входу пристроїв кінцевих користувачів, таких як настільні ПК, ноутбуки та мобільні пристрої, від використання зловмисниками та кампаніями. Системи безпеки кінцевих точок захищають ці кінцеві точки в мережі або в хмарі від загроз кібербезпеці. Безпека кінцевих точок еволюціонувала від традиційного антивірусного програмного забезпечення до комплексного захисту від складних зловмисних програм і нових загроз нульового дня.

Компанії будь-якого розміру можуть стати жертвами атак. Згідно з даними звіту Verizon Data Breach Investigations Report, 43% кібератак націлені на компанії малого бізнесу. Часто вони не мають жодних засобів захисту, а зловмисники можуть використовувати їх, щоб проникнути в системи великих компаній.

Кіберзлочинці атакують кінцеві точки, оскільки вони дають їм змогу легко отримувати доступ до корпоративних даних і за своєю природою вразливі до загроз. Вони захищені не системою безпеки в мережі, а окремими заходами, які впроваджують користувачі. А люди, як відомо, здатні робити помилки. В умовах розподіленої роботи, коли офісні, віддалені й гібридні працівники використовують усе більше пристроїв у різних точках світу, захищати кінцеві точки стало ще складніше.

У сучасному середовищі загроз, які постійно еволюціонують, системи

забезпечення захисту кінцевих точок є вкрай необхідними. У світлі того, як все більше підприємств впроваджують такі практики, як BYOD (Bring Your Own Device – принеси свій власний пристрій), а також у зв'язку зі зростанням числа мобільних загроз, безпека кінцевих точок стає все більш актуальною. Сьогодні співробітники підключаються до мереж компанії, використовуючи свої ноутбуки або мобільні пристрої, і вдома, і в дорозі. Ці фактори самі по собі ускладнюють безпеку кінцевої точки підприємства, але вони ускладнюються політиками віддаленої роботи та BYOD, які роблять безпеку периметра дедалі недостатнішою та створюють уразливості. Ландшафт загроз також ускладнюється: хакери завжди винаходять нові способи отримати доступ, викрасти інформацію або змусити співробітників надати конфіденційну інформацію.

Безпека кінцевої точки — це практика захисту даних і робочих процесів, пов’язаних з окремими пристроями, які підключаються до мережі. EPP (Endpoint Protection Platforms - Платформи захисту кінцевих точок) перевіряють файли, коли вони надходять у мережу. Сучасні EPP використовують потужність хмари для зберігання постійно зростаючої бази даних інформації про загрози, звільняючи кінцеві точки від навантаження, пов’язаного зі збереженням усієї цієї інформації локально та обслуговуванням, необхідним для підтримки актуальності цих баз даних. Доступ до цих даних у хмарі також забезпечує більшу швидкість і масштабованість.

Коли EPP налаштовано, воно може швидко виявляти зловмисне програмне забезпечення та інші загрози. Деякі рішення також включають EDR (Endpoint Detection and Response - Виявлення та реагування на кінцеву точку). Можливості EDR дозволяють виявляти більш складні загрози, такі як поліморфні атаки, безфайлове шкідливе програмне забезпечення та атаки нульового дня. Використовуючи безперервний моніторинг, рішення EDR може запропонувати кращу видимість і різноманітність варіантів реагування.

Рішення EPP доступні в локальних або хмарних моделях. Хоча хмарні продукти є більш масштабованими та легше інтегруються у вашу поточну архітектуру, певні нормативні/відповідні правила можуть вимагати локальної безпеки.

Захищати кінцеві точки важливо, оскільки порушення безпеки даних призводить до матеріальних збитків та інших руйнівних наслідків для підприємств. Згідно зі звітом Ponemon Institute за 2021 рік, підготованим на замовлення IBM, середня вартість збитків від порушення безпеки даних складає 4,24 млн дол. США в усьому світі й 9,05 млн дол. США в Сполучених Штатах. Збитки від порушень безпеки даних, що пов’язані з віддаленою роботою, у середньому становлять ще 1,05 млн дол. США. Найбільше збитків від порушення безпеки даних (38%) пов’язані з утратою бізнесу, зокрема плинністю клієнтів, скороченням доходів через збої в роботі системи та витратами на налагодження нового бізнесу через шкоду репутації.

Перелік посилань:

1. Endpoint Detection and Response (EDR) https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr

2. What Is Endpoint Security? https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html#endpoint-security

Бригинець Анастасія Андріївна,
студентка групи БСД-31, ННІЗІ ДУТ, Київ, Україна

АНАЛІЗ ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАННЯ ПРОМИСЛОВИХ ІОТ МЕРЕЖ

Сучасний світ розвивається стрімкими темпами, щодня у повсякденне життя мільярдів людей приходять нові, надсучасні технології. Промислові підприємства, звісно, також прагнуть бути конкурентоспроможними, а тому намагаються оптимізувати процес виробництва із застосуванням практик IoT, що призвело до виникнення нової підтехнології промислового інтернету речей (IIoT). До 2020 року розмір ринку промислового інтернету речей сягнув 110 мільярдів доларів США. Нині промисловий Інтернет речей становить понад 17% від кількості проектів Інтернету речей у всьому світі. У цій роботі буде розглянуто детальніше усі особливості функціонування IIoT.

Ключові слова: IoT, IIoT, безпека процесів, інформація, автоматизація, розумне виробництво.

Промисловий Інтернет речей (IIoT) — це використання інтелектуальних датчиків і приводів для вдосконалення виробничих і промислових процесів. Також відомий як промисловий інтернет або Індустрія 4.0, IIoT використовує потужність розумних машин і аналітику в реальному часі, щоб скористатися перевагами даних, які виробляли прості машини в промислових умовах роками. Філософія, що лежить в основі IIoT, полягає в тому, що розумні машини здатні збирати і аналізувати дані в режимі реального часу не тільки краще, ніж люди, але і вони також краще передають важливу інформацію, яку можна використовувати для швидшого й точнішого прийняття бізнес-рішень.

Підключені датчики та процеси дозволяють компаніям швидше виявляти неефективність і проблеми та економити час і гроші, одночасно підтримуючи зусилля бізнес-аналітики. У виробництві, зокрема, IIoT має великий потенціал для контролю якості, стратегій тривалого розвитку, екологічних практик, відстеження ланцюга постачання та його загальної ефективності. У промисловому середовищі IIoT є ключовим для таких процесів, як прогнозне технічне обслуговування (PdM), розширене обслуговування на місцях, управління енергією та відстеження активів.

Отже, як саме працює IIoT? Фактично, це мережа інтелектуальних пристроїв, підключених до систем, які відстежують, збирають, обмінюються та аналізують дані. Кожна промислова екосистема IoT складається з:

• підключених пристроїв, які можуть моніторити, передавати та зберігати інформацію про себе;

• державної та/або приватної інфраструктури передачі даних;

• аналітики та програм, які генерують бізнес-інформацію з вихідних даних;

• зберігання даних, які генеруються пристроями IIoT;

• людських ресурсів.

Робототехніка й автоматизовані машини можуть працювати ефективніше й точніше, підвищуючи продуктивність і допомагаючи виробникам оптимізувати свої функції. Крім того, фізичні машини можна підключити до програмного забезпечення за допомогою датчиків, які постійно контролюють продуктивність. Це дає змогу виробникам краще розуміти робочі показники окремих одиниць обладнання, а також цілих масивів даних. Системи даних із підтримкою IIoT дають змогу виробникам підвищувати ефективність роботи за рахунок обходу мануальних завдань і функцій і впровадження автоматизованих, цифрових; прийняття рішень на основі даних щодо всіх виробничих функцій і моніторингу продуктивності з будь-якого місця – на виробництві чи за тисячі миль.

У звіті Cyber Security Trend найчастішою причиною порушень кібербезпеки (37% випадків) було названо саме людський фактор [1]. Промисловий Інтернет речей дає виробникам можливість оцифрувати майже кожну частину свого бізнесу. Зменшуючи частку виконання роботи людиною, знижується і найбільший ризик, що може призводити до витоків даних та порушення цілісності і функціоналу системи. Програми та механізми з підтримкою штучного інтелекту та машинного навчання можуть виконувати більшу частину необхідних обчислень самостійно, усуваючи можливість зробити просту помилку та поставити під загрозу критичні дані, що належать виробнику.

Ніщо так не впливає на виробництво, як простій машин. Aberdeen Research Group підрахувала, що середня вартість години простою на всіх типах виробництва становить 260 000 доларів США. Що може бути причиною таких серйозних проблем, з якими виробники не можуть працювати? Відповідь проста – відсутність належного та прогнозованого технічного обслуговування. Коли технічне обслуговування у промисловості є реактивним, а не проактивним, виробники зупиняють процеси, намагаючись визначити, у чому проблема, як її можна відремонтувати та скільки це буде коштувати. Завдяки профілактичному технічному обслуговуванню на основі рішень IIoT усі ці проблеми усуваються. Коли продуктивність і функції обладнання постійно контролюються, виробники можуть створити плани робіт. Тоді вони можуть запланувати технічне обслуговування до простою, що принесе їм прибуток, оскільки вони: матимуть запчастини, необхідні для роботи; заздалегідь знатимуть вартість проєкту та зможуть скласти для нього бюджет; переконаються, що обладнання працює з максимальною ефективністю.

Усі дані та сенсори, необхідні для повноцінно функціонуючого виробничого процесу IIoT, також допомагають підвищити безпеку на робочому місці. «Розумне виробництво» перетворюється на «розумну безпеку», коли всі датчики IIoT працюють разом, щоб стежити за безпекою на робочих місцях. Інтегровані системи безпеки захищають працівників у цеху, на лінії та під час розподілу. Якщо сталася аварія, усі на об’єкті можуть бути попереджені, операції можуть бути припинені, а керівництво компанії може втрутиться та переконається, що аварію та інцидент було вирішено. Цей інцидент також може

створити цінні дані, які можуть допомогти запобігти повторенню схожих подій у майбутньому. Деякі виробники використовують нову опцію – це використання мобільних технологій серед своїх співробітників. Мобільні технології були частиною IoT з самого початку, і тільки зараз вони використовуються в промислових операціях IoT. Так звані «wearables» допомагають керівництву стежити за такими речами, як постава співробітників і рівень навколишнього шуму, із подальшою можливістю покращення умов роботи та потенційним підвищенням продуктивності. Також існує можливість інформування співробітників, у разі коли вони не дотримуються належних процедур безпеки на робочому місці, щоб вони могли виправити свої дії та залишатися в безпеці на роботі.

Знання — це сила, і знання, які надаються виробникам через рішення IIoT, дають їм інструменти, необхідні для зниження витрат і отримання більшого доходу. Керована даними інформація про операції, виробництво, маркетинг, продажі тощо може спрямувати бізнес у прибутковий напрямок. Усі вищезазначені переваги інтернету речей – прогнозоване технічне обслуговування, менше помилок, покращений контроль якості та максимальна ефективність підвищать прибутки для виробника. Промисловий IoT також пропонує, мабуть, найцінніший інструмент для керівників виробничих компаній – статистику з будь-якого місця та в будь-який час. Дистанційний моніторинг виробничих операцій тепер можливий 365 днів на рік, 24/7, з будь-якої точки світу. Це 360-градусний огляд усього виробничого процесу та подальше обслуговування, яке надається клієнтам на шляху до покупки, є безцінним активом [2].

Перелік посилань:

1. Mendoza M. Industrial IoT – The Top 5 Benefits of Industry 4.0 [Електронний ресурс] / Michael Mendoza – Режим доступу до ресурсу: https://global.hitachi-solutions.com/blog/industrial-iot-benefits/.

2. Posey B. Industrial internet of things (IIoT) [Електронний ресурс] / Brien Posey – Режим доступу до ресурсу: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT.

Шулімова Дар'я Денисівна
студентка групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

ОСНОВНІ РИЗИКИ ДЛЯ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Смартфони все частіше використовуються для роботи. За їх допомогою користувачі передають бізнес-інформацію через незахищені канали зв'язку. Все більше співробітників переглядають декілька поштових скриньок (організації та власних) з одного слабозахищеного мобільного пристрою. У зв'язку з цим все більше кіберзлочинців переходять на онлайн-шахрайство, включаючи вимагання та шантаж. Отримавши навіть віддалений (а не прямий, за допомогою крадіжки) доступ до мобільного пристрою, зловмисник зможе дізнатися не тільки особисті, а й банківські або корпоративні доступи. Крім цього, існують інші загрози для мобільних пристроїв, здатні відкрити хакерам доступ до смартфону.

Як зловмисники змушують користувачів переходити по зараженому посиланню.

Для атак зловмисники використовують фішинг та методи соціальної інженерії, які змушують співробітників натискати на заражені посилання. Їх надсилають електронною поштою або у повідомленнях месенджерів.

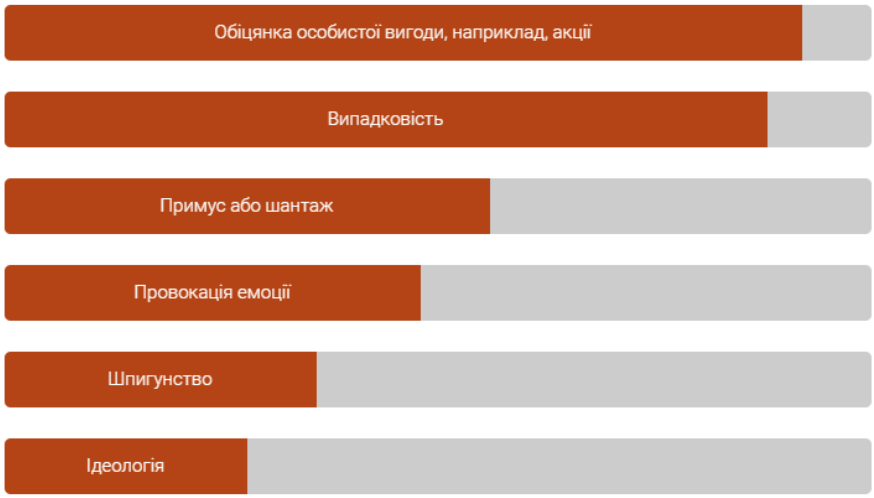


Рис.1 – Цілі, за якими зловмисники здійснюють атаки

Проблема 1. Соціальна інженерія

Згідно зі звітом FireEye, 91% кіберзлочинів розпочинають атаку з електронної пошти. Цей вид атаки розрахований на те, що жертва натисне на посилання і цим надасть зловмисникам доступ до свого пристрою. Користувачі смартфонів піддаються найбільшому ризику, адже багатьом клієнтам мобільної пошти будуть відображуватися імена відправників, які легко підробити — й обманом змусити людину думати, що лист прийшов від того, кого він знає.

Користувачі частіше реагують на фішингову атаку на мобільному пристрої, ніж на комп'ютері, адже маленький екран не дозволяє побачити деталі, які видають зловмисника. Уразливими є месенджери, соціальні мережі та ігри. Згідно зі звітом Wandera, 83% фішингових атак за останній рік прийшли у вигляді текстових повідомлень у Facebook Messenger та WhatsApp. Ті, хто вже натискав на фішингове посилання, з величезною ймовірністю, повторять свою дію у майбутньому.

До соціальної інженерії можна віднести також і «погану гігієну паролів», через що зловмисникові дуже легко отримати доступ до смартфона. Згідно з аналізом LastPass, половина фахівців використовують однакові паролі для організацій та приватних облікових записів. Як наслідок, вкрадені паролі стають причиною злому корпоративної мережі.

Проблема 2. Мобільне шахрайство з рекламою

Шахрайство з рекламою може мати декілька форм, однак найбільш поширеною є використання шкідливих програм для кліків по оголошеннях, які нібито робить реальний користувач, що використовує вебсайт або додаток.

Наприклад, користувач завантажив гру або неперевірений месенджер — небезпечні додатки у фоновому генерують шахрайські кліки на законних оголошеннях. Таким чином, шахраї обкрадають бізнес. Для користувачів це небезпечно тим, що працюючі у фоновому режимі програми сповільнюють роботу смартфона, розряджають акумулятор або навіть викликають перегрів.

Проблема 3. Використання незахищених Wi-Fi з'єднань

Мобільний пристрій знаходиться в тій же мережі, в якій працюють і комп'ютери компанії. Користувачі постійно підключаються до загальнодоступних мереж Wi-Fi, а вони не завжди безпечні. Зловмисники можуть заразити смартфон у найближчому кафе, куди співробітник компанії зайшов випити кави та під'єднався до "безкоштовного wi-fi", а потім за допомогою пристрою, отримав доступ до корпоративної мережі.

Проблема 4. Витік даних після кібератак

Витік даних — одна з найбільших і частих погроз для організацій. Абсолютно кожна компанія може зіткнутися з витоком даних. Співробітники можуть ненавмисно переглянути посилання, додаток або відвідати сайт і, тим самим, відкрити доступ для зловмисників у мережу. Основна причина витоків — це помилки користувачів, наприклад, неправильне ведення електронного листування, ненавмисна вставка конфіденційної або службової інформації тощо. Більшість кібератак спрямовані на отримання конфіденційної інформації або доступу до фінансів. Ретельний підбір мобільних пристроїв і дотримання політики безпеки дозволить зберегти корпоративні дані від витоків.

Проблема 5. Людський фактор

Втрачений мобільний пристрій може представляти серйозну загрозу безпеці. Більшість людей досі не користується пін-кодами або біометричним захистом, ще більше - не використовує шифрування. У разі пошкодження або при втраті пристрою, користувачі стають легкою здобиччю зловмисника.

У звіті Wandera вказано, що 43% користувачів мають принаймні один смартфон без будь-якого захисту екрану блокування. А паролі використовують 4-символьні або дуже прості.

Ще одна проблема полягає в несвоєчасному оновленні програмного забезпечення (ПЗ). Смартфони являють особливий ризик для корпоративної безпеки. Більшість виробників мобільних пристроїв неефективно підтримують продукт і рідко випускають оновлення системи, а також виправлення безпеки. Та й у разі наявності оновлень, не всі користувачі проводять апдейт пристрою.

Рекомендації для захисту мобільних пристроїв:

- Варто розглянути можливість використання для роботи лише корпоративних мобільних пристроїв — зі встановленим програмним забезпеченням для захисту від найбільш поширених загроз;
- Потрібно регулярно оновлювати ПЗ і операційну систему мобільного пристрою;
- Встановлати лише офіційні додатки з перевірених джерел;
- Регулярно варто перевіряти додатки й видаляти будь-які, що поводять себе аномально, наприклад, занадто багато використовують енергії;

- Перейти на апаратну аутентифікацію — це найбільш ефективний спосіб підвищення безпеки та зменшення ймовірності фішингу;
- Варто використовувати шифрування й інструменти запобігання втрати даних (DLP), які допоможуть запобігти розкриттю конфіденційної інформації.
- Робити резервне копіювання даних регулярно;
- Налаштовувати права конфіденційності та захисту на мобільному пристрої.

Перелік посилань:

1. Смартфони та корпоративна інформація: основні ризики та як їм запобігти [Електронний ресурс] – Режим доступу: https://softline.ua/ua/news/smartfony-ta-korporatyvna-informatsiia-osnovni-ryzyky-ta-iak-im-zapobihty.html
2. MOBILE SECURITY [Електронний ресурс] – Режим доступу: https://www.digitalsecurity.film/mobile

Гайдур Ксенія Володимирівна
студентка групи ТСД-41, ТСМ ДУТ, Київ, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА. АКТУАЛЬНІ РІШЕННЯ

Визначено принципи та цілі інформаційної безпеки. З визначених цілей показано різницю між інформаційною та кібербезпекою. Надано рекомендації щодо використання рішення Cloudflare для захисту програмного забезпечення.

Інформаційна безпека (InfoSec) - це галузь, що постійно розвивається і є необхідною в широкому спектрі сфер, від безпеки мережі та інфраструктури до тестування та аудиту. Охоплює собою інструменти та процеси, які організації використовують для захисту і збереження цілісності інформації. Адже наслідки інцидентів безпеки включають крадіжку особистої інформації, підробку і видалення даних. Такі атаки можуть порушити робочі процеси та завдати шкоди репутації компанії, а також мати відчутні збитки.

Існують три принципи (тріада) розроблені:

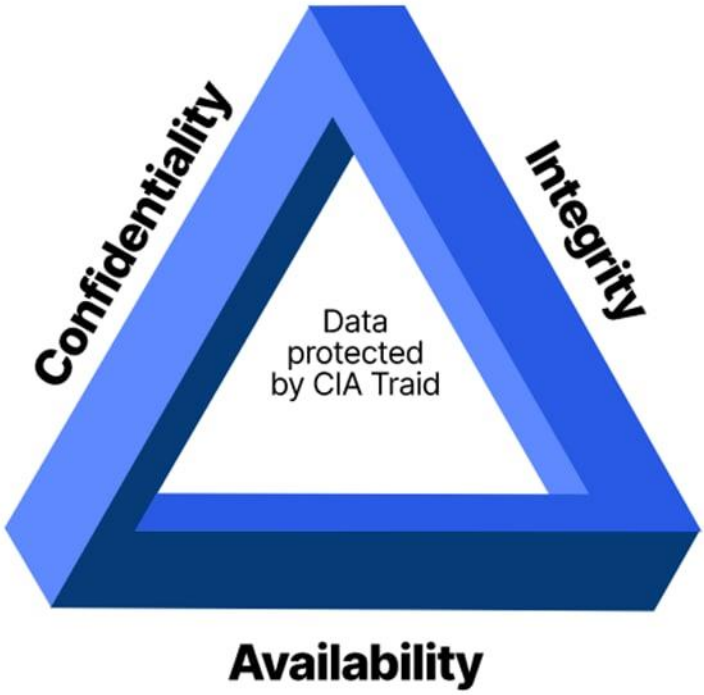


Рис. 1 - The CIA Triad defines three key principles of data security

Конфіденційність – запобігання несанкціонованому доступу, розголошенню інформації. Тобто встановлення певного контролю, наприклад: ідентифікація, аутентифікація, авторизація, шифрування.

Цілісність – даний принцип гарантує, що дані є точними й не змінюються з-за випадкових, шкідливих чи інших підозрілих обставин, які є несанкціонованими.

Доступність – відповідає за легкість з якою авторизовані користувачі отримують доступ до необхідної інформації при наявності відповідного рівня доступу та певного інструмента автентифікації.

Дані принципи безпеки тріади тісно пов’язані один з оним і разом працюють над тим, щоб інформація, яка зберігається у хмарі чи локально була надійно захищена.

Три базові цілі триади:

- Захист інформації
- Забезпечення точності інформації
- Утримання інформації доступною

Чим же тоді відрізняється інформаційна безпеки від кібербезпеки?

Різниця полягає в обсязі та меті. Дуже часто данні терміни використовуються як синоніми, але фактично кібербезпека являє собою підкатегорію інформаційної безпеки і має більш вузьке направлення. А точніше спрямована на вирішення технологічних проблем та захисту даних організацій від випадкового чи зловмисного доступу неавторизаваних сторін.

Актуальні рішення від розробників захисного програмного забезпечення:

Cloudflare – це глобальна хмарна платформа, призначена для того, щоб

зробити все, що ви підключаєтеся до Інтернету, безпечним, конфіденційним, швидким та надійним.

Дана платформа надає такі переваги:

- Захист корпоративної мережі, веб-сайтів, API, Інтернет-додатків і прискорення роботи веб-ресурсів.
- Усунення затримок за рахунок інтеграції з увімкненими сервісами продуктивності Cloudflare.
- Найшвидша глобальна хмарна мережа для веб-застосунків, призначена для оптимізації безпеки, продуктивності та надійності без роздмухування застарілих технологій.

До того ж Cloudflare допомагає перетворити економічну невизначеність на можливість. Надає можливість контролювати витрати, зменшує ризики ланцюга поставок та підвищує гнучкість бізесу.

Платформа Nexus від компанії Sonatype – це підтримка найбільшого у світі сховища компонентів з відкритим кодом (Central) і найпопулярніший в світі менеджер сховища (Nexus) розробленого на відкритому коді.

Nexus Repository - надає можливість керувати бібліотеками та зберігати артефакти в універсальному сховищі та ділитися ними між командами розробників.

Nexus Container - надає можливість визначати та усувати ризик OSS у контейнерах для захисту збірки та під час виконання.

Nexus Firewall - надає можливість автоматично зупиняти потрапляння дефектних компонентів з відкритим кодом у ваш SDLC.

- Запобігає проникненню критично зловмисних і потенційно скомпрометованих компонентів у робочі програми за допомогою автоматизації та постійного моніторингу.
- Скорочує проміжок часу від моменту виявлення вразливості до часу коли ви зможете впровадити виправлення безпеки.
- Надає можливість перевіряти відбитки пальців, а не імена файлів та маніфести пакетів.
- Надає повідомлення про реальний ризик, а не помилкові тривоги.

Перелік посилань:

1. Information Security: The Ultimate Guide [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/data-security/information-security-infosec.
2. The principles and fundamentals of information security. Posted on APRIL 16TH 2021 [Електронний ресурс] – Режим доступу: https://blog.box.com/principles-and-fundamentals-information-security.
3. Статистика. Математичні методи, моделі та інформаційні технології в економіці [Електронний ресурс] – Режим доступу: http://economics.kntu.kr.ua/pdf/3(36)/23.pdf.
4. Cloudflare [Електронний ресурс] – Режим доступу: https://www.cloudflare.com/.
5. Sonatype [Електронний ресурс] – Режим доступу: https://www.sonatype.com/.

Завадський Володимир В'ячеславович
Студент групи БСДМ-63, ННІЗІ ДУТ, Київ, Україна

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ФІЛЬТРАЦІЯ МЕРЕЖЕВОГО ВМІСТУ ТА ЗАПОБІГАННЯ ВИТОКАМ

Сучасні організації для ведення бізнесу значною мірою залежать від Інтернету, інтранетів та їх мережевих інфраструктур. Забезпечення безпеки та цілісності даних, які передаються між мережами, має важливе значення, особливо в світлі різноманітних регуляторних і законодавчих мандатів, яких вони повинні дотримуватися. У той же час проблеми з правозастосуванням, з якими вони стикаються, зростають, а потреба в ефективних засобах контролю безпеки більша, ніж будь-коли. Організації прагнуть запровадити технічні засоби контролю, щоб допомогти у забезпеченні дотримання своєї політики безпеки; однак за певних обставин деяким організаціям необхідно відстежувати вміст пакетів, що надходять і виходять з їхньої мережі, щоб гарантувати виявлення витоків конфіденційної інформації.

Ключові слова: кібербезпека, конфіденційність, фільтрація, політика безпеки, витоки, мережева інфраструктура.

Технології виявлення та запобігання на основі сигнатур або поведінки залежать від автоматизованого розпізнавання аномальних умов: у першому випадку через сигнатури, а в другому через перевищення встановленого порогу відхилення від відомих нормальних умов (або базового рівня).

Запобігання несанкціонованому розкриттю службових або конфіденційних даних (витоку інформації) за допомогою звичайних технологій (таких як виявлення або запобігання вторгненням) важко впоратися. Виявлення та запобігання вторгненням на основі сигнатур базується на сигнатурах атак (шаблони бітів у потоках пакетів); розширення, щоб включити слова або шаблони слів, які містяться у файлах додатків (базах даних, офісних документах продуктивності, портативних файлах документів або будь-якому з численних форматів файлів, які використовуються сьогодні), які б свідчили про витік інформації, є складною.

Традиційні технологічні рішення, такі як керування ідентифікацією та доступом, керування інформацією про безпеку, системи керування вмістом і керування цифровими правами — окремо чи в поєднанні — допомагають організаціям контролювати, хто має доступ до конфіденційних даних; однак, як тільки авторизований доступ надано, вони мало контролюють, як ці дані використовуються.

Політика безпеки обробки інформації повинна мати: сильну політику, яка чітко окреслює вимоги організації до обробки інформації та передбачає дисциплінарні заходи за порушення політики, є першим кроком у контролі витоків інформації через мережі. Але політика без засобів її реалізації залишається неефективною.

Обмеження протоколів або додатків, які можуть використовувати користувачі мережі для з'єднань із зовнішніми мережами, допомагає організаціям зменшити вектори, через які може витікати конфіденційна інформація. Однак встановлення занадто великої кількості обмежень заважатиме бізнесу, і організаціям потрібно знайти компроміс між безпекою та

зручністю використання.

HTTP/FTP. Будь-які типи документів можуть бути завантажені на веб-сайт, призначений для «прийняття» вкладень (електронна пошта через Інтернет, дошки оголошень тощо). Фільтрація універсального засобу пошуку ресурсів (URL), яка зазвичай є частиною захисного арсеналу компаній, може допомогти зменшити цей ризик. Безкоштовні веб-послуги електронної пошти зазвичай класифікуються в категорії «Веб-пошта» рішень для фільтрації URL-адрес; таким чином, доступ до цих служб можна обмежити шляхом впровадження відповідних засобів контролю безпеки над доступом до Інтернету (функціональність, яка доступна або в окремому рішенні, або як доповнення до існуючих серверів веб-кешування від кількох постачальників). Залишковий ризик походить від сайтів без категорії. Відмова в доступі до таких сайтів може додатково зменшити залишковий ризик, але може вважатися неприйнятним для бізнесу. Таким чином, що стосується контролю витоків, метод фільтрації URL є бінарним і не має деталізації.

HTTP/SFTP/SSH та інший зашифрований трафік. Сценарій подібний до попереднього. Керування є двійковим і не має деталізації. Після надання доступу подальший контроль над вмістом неможливий. [1, с. 290]

Однорангові програми. Ризик найкраще зменшити, запобігши використанню таких програм. Для максимальної ефективності можна використовувати комбінацію елементів керування на різних рівнях.

Технологія, розроблена для захисту дуже конфіденційних даних від витоків через мережі, є складною та дорогою з точки зору витрат на придбання та поточних операцій, а її ефективність залежить від того, який тип трафіку організація дозволяє проникати через свою периферію.

Шифрування — це палиця з двома кінцями: воно допомагає забезпечити конфіденційність інформації, що передається мережами, але також заважає організаціям зберігати видимість того, яка інформація залишає їхні мережі.

Щоб ефективно боротися з витоками інформації через мережі, організації повинні дотримуватися безперервного циклу планування інформаційної безпеки: оцінювати, проектувати, впроваджувати, навчати, контролювати та виправляти.

Обізнаність і розуміння співробітниками служби безпеки векторів, які можуть бути використані особами з лихими намірами, щоб викрасти конфіденційну або конфіденційну інформацію з мережі, є ключовим фактором для зменшення ризику.

Перелік посилань:

1. Tipton H. Information Security Managment Handbook / H. Tipton, M. Krause

Єрмак Максим Володимирович
Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ ORACLE IDENTITY AND ACCESS MANAGEMENT

Чи можна зараз представити інформаційну систему без користувачів? Хто будуть ці користувачі? Які буде мати права кожен із користувачів цієї системи? А хто має відповідати за розподіл прав для цих користувачів? Ці питання має бути укоріненні при створенні безпечної архітектури. На ці питання вже розробили відповіді за допомогою технології IAM.

Наразі вся архітектура інформаційної системи будується навколо користувача та інформації, яку він обробляє. Невід'ємною має бути також безпека всіх цих цифрових процесів обробки інформації. Тож проблема безпеки гостро стоїть перед організацією та розробниками. Вже з'явилось досить багато різних рішень по управлінню аккаунтами та доступом, рішення ідентифікації та аутентифікації, управлінню безпекою даних, управління базою даних. Але все ще замало компаній займаються цією проблемою комплексно. Адже, чим більше буде охочих вирішити цю проблему – тим ефективніше вона буде вирішена. За оцінкою аналітичних агенцій Forrester, KuppingerCole, Gartner котрі оцінюють рішення в категорії Identity and Access Management можна виділити таких вендорів, як IBM, SAP, Microsoft, Oracle, SailPoint, Dell та інші. Всі вони пропонують свої рішення та методології для розв'язання проблеми управління ідентифікацією та доступом користувачів інформаційної системи підприємства. При цьому вони всі різні, хоча й виконують приблизно одну функцію безпеки використовуючи, по-різному відображають дані, по-різному їх зчитують, по-різному інтерпретують результати та видають рекомендації.

Шлях цієї системи лежить від початку прийому співробітника на роботу до компанії. Новому співробітнику спочатку треба створити робочий аккаунт, зареєструвати його в системі, надати йому права та ролі, котрі він виконувати, якщо треба, додати до груп та надати доступ до різних сервісів компанії. Все це при ручному запиті може займати досить великий проміжок часу, не рахуючи те, що ресурсами можуть володіти абсолютно різні люди, погодження котрих необхідно для доступу в ці ресурси. При цьому, співробітник буде змінювати свою роль у компанії, йому знадобляться нові права та доступи а старі – навпаки, будуть непотрібні вже. Якщо мова йде про невелику компанію – новий співробітник за кілька днів зможе погодити всі необхідні йому доступи. Але, що робити, якщо компанія розрослася до 500 співробітників, або більше. Такий метод вже буде досить витратний щодо часу. Через це вкрай важливо такі дії замінити процесом автоматизації.

Головною задачею Identity and access management (IAM) наразі є централізоване управління ідентифікаційними даними, правами та доступами співробітників до інформації всередині компанії. Найчастіше використовуючись у великих компаніях для комунікації між відділами. впровадження IAM систем

у структуру організації займає від 6 місяців, залежно від рівня підготовки та кількості необхідних функцій системи. Такі системи дозволяють керувати політиками доступів, політиками паролів, ролями користувачів та створювати обширні звіти щодо цих політик.

Безпека цих систем запроваджується за допомогою багатофакторної аутентифікації та авторизації користувачів, використовуючи Single Sing-On (SSO), технологію переходу між ресурсами компанії без повторної аутентифікації, технології електронних підписів та відкритих ключів. Через роботу функцій безпеки система гарантує, що закріплені права за користувачем будуть «слідувати» за ним і на інших ресурсах компанії.

Таким чином, запровадивши систему IAM у інфраструктурі підприємства можливо досить суттєво пришвидшити процеси управління аккаунтами користувачів, без котрих неможливо функціонування організації. А також, що найголовніше, безпеку та непреривність цього процесу можна поліпшити за рахунок розмежування та обмеження доступу користувачів, за допомогою мінімальних привілеїв та двофакторної автентифікації.

Перелік посилань:
1. Что такое Identity and Access Management (IAM)? [Електронний ресурс] URL: https://www.oracle.com/cis/security/identity-management/what-is-iam (дата звернення 11.10.2022)
2. Сравнение систем управления доступом (IdM/IAM) [Електронний ресурс] URL: https://www.anti-malware.ru/comparisons/identity_management_systems_2015#part1 (дата звернення 11.10.2022)
3. **What is identity and access management? Guide to IAM** [Електронний ресурс] URL: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system (дата звернення 11.10.2022)

Андрущенко Катерина Юріївна
студентка групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

АВТОМАТИЗАЦІЯ ПРОЦЕСУ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

На сьогоднішній день ландшафт кіберзагроз змінюється настільки швидко, що командам безпеки складно організувати швидкий і ефективний процес реагування. Щодня аналітики приймають рішення, які можуть вплинути на всю організацію і безпека компанії надмірно залежить від персоналу, який часто використовує ручні процеси для обробки сповіщень безпеки і величезної кількості даних з різних систем захисту інформації.

Неправильно обраний процес реагування, відсутність доступу до необхідних систем, перенасиченість даними з різних рішень, виконання постійно повторюваних дій – все це ускладнює процес реагування і становить загрозу для організації.

Перш ніж станеться будь-який інцидент, важливо встановити належні заходи безпеки для зменшення ризиків інфікування вже відомими загрозами. Важливою частиною налаштування мережі є наявність всіх необхідних

інструментів моніторингу та введення журналів для збору та аналізу подій у мережі [1].

Організація процесу керування інцидентами ІБ без використання засобів автоматизації являє собою складне й трудомістке завдання. Необхідно збирати та консолідувати надвелику кількість даних у різних форматах, вести централізований архів. Для ручної обробки даних щодо подій та інцидентів ІБ потрібна велика кількість висококваліфікованих фахівців-аналітиків. Через великий обсяг рутинної роботи обробка подій найчастіше буває неповною, що не відбиває всього змісту поточної ситуації. Може статися, що інциденти ІБ, критичні для надійного й захищеного функціонування системи, виявляються поза полем зору аналітиків, і через це не приймаються відповідні превентивні заходи [2].

Спеціалізоване рішення для автоматизації реагування на інциденти – SOAR.

Рішення SOAR - Security Orchestration, Automation & Response, призначене для автоматизації і спрощення процес реагування на інциденти.

SOAR дозволяє чітко визначити процес реагування, якого слід притримуватись аналітику, поєднати дані з різних систем в одному інциденті, тобто збагатити інцидент даними з усіх пов’язаних рішень безпеки, забезпечити виконання необхідних дій в системах та автоматизувати повторювані дії.

Принцип роботи SOAR:

Системи захисту інформації при детектуванні загрози генерують спрацювання, який потрапляє в SOAR. На його підставі створюється інцидент, збагачується даними з інших засобів захисту - аналітик дотримуючись інструкції проводить розслідування, а вся послідовність дій в підсумку зберігається в консолі і може бути переглянута адміністратором.

Таким чином SOAR значно спрощує процес обробки інцидентів, дозволяє ефективно використовувати формалізовані плани реагування, зменшує час розслідування за рахунок автоматизації і надає необхідну візуалізацію дій при розслідуванні інцидентів.

Перелік посилань:

1. Від інциденту до вирішення: основні кроки протидії та відновлення у випадку кібератаки. URL: https://eset.ua/ua/blog/view/83/ot-intsidenta-k-resheniyu-osnovnyye-shagi-protivodeystviya-i-vosstanovleniya-v-sluchaye-kiberataki

2. Гладиш С. В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7536/11-Gladysh.pdf?sequence=1

Гінько Артем Олегович
студент групи БСДМ-63, ННІЗІ ДУТ, Київ, Україна

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ НА ОСНОВІ РІШЕННЯ VPN

Враховуючи поточний ландшафт, де віддалена або гібридна робота стала кращим середовищем, серйозне ставлення до захисту віддалених користувачів має вирішальне значення для підтримки захисту мережі та даних будь-якої організації.

Оскільки все більше людей працюють частково або повністю віддалено, перспективні та масштабовані практики та такі рішення, як впровадження рішення VPN ніколи не були настільки важливими.

Ключові слова: VPN, конфіденційна інформація, Інтернет, корпоративна мережа, контроль доступу

Віртуальна приватна мережа (VPN) — це служба, яка створює зашифроване з'єднання від однієї мережі до іншої. Це дозволяє співробітникам легко отримувати дистанційний доступ до приватної мережі організації, даних і додатків і спрямоване на те, щоб веб-трафік, що містить конфіденційну інформацію, не потрапляв у загальнодоступний Інтернет [1, с.1].

VPN працює, створюючи віртуальне з'єднання «точка-точка» та маскуючи трафік даних в Інтернеті, щоб захистити його від зовнішнього доступу.

Зазвичай існує два типи VPN для використання в бізнесі:

- VPN віддаленого доступу

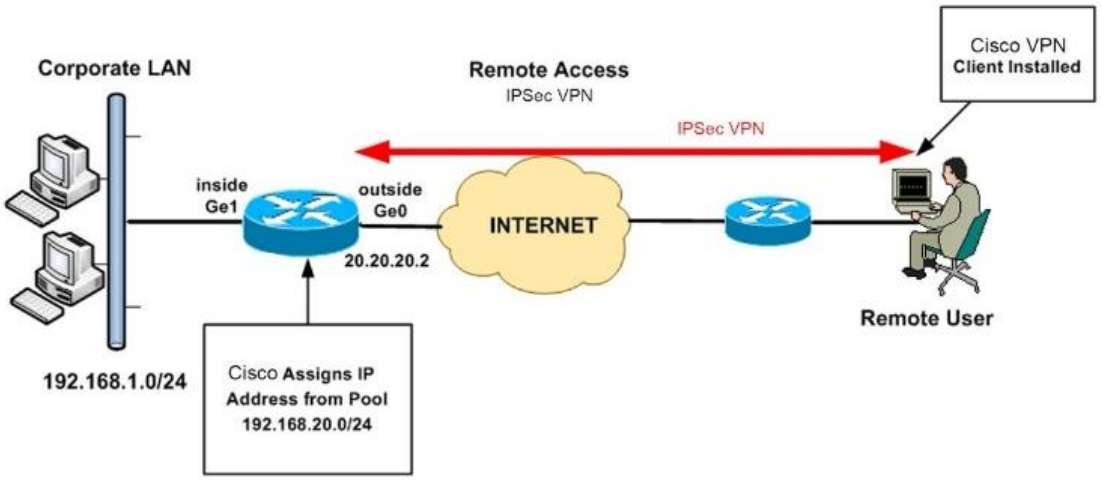


Рис. 1 – Схема роботи VPN віддаленого доступу

- Site-to-site VPN

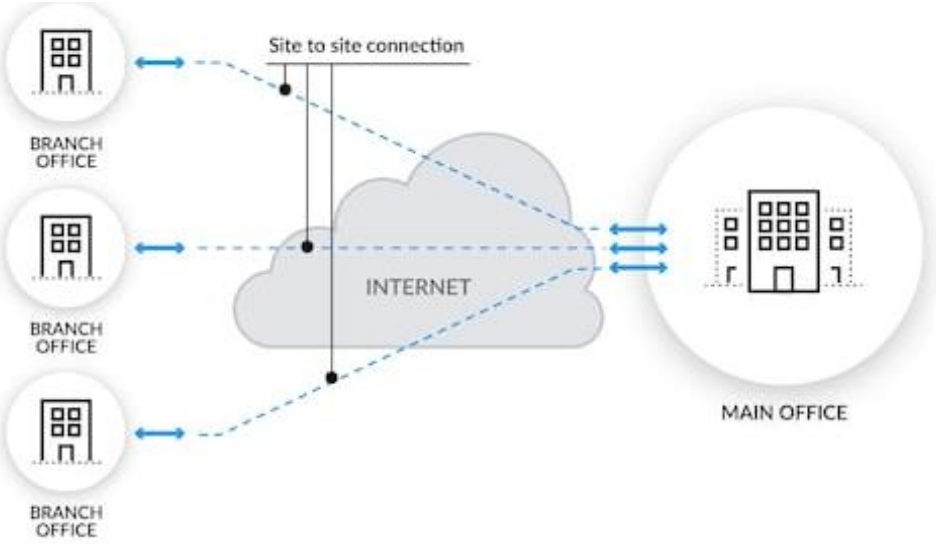


Рис. 2 – Схема роботи Site-to-site VPN

VPN віддаленого доступу створює щось на зразок зашифрованого тунелю між мережею та користувачем, щоб забезпечити безпечний доступ.

VPN типу «**сайт-сайт»** надає користувачам доступ до з'єднання з двома або більше мережами, скажімо, між філіями та головним офісом. Однак це рішення не працює за межами офісної філії, тому його не можна використовувати для віддаленої роботи.

У кожному випадку VPN є частиною філософії безпеки на основі периметра, згідно з якою, як випливає з назви, інструменти та пристрої встановлюються навколо кордону мережі, щоб забезпечити її безпеку. Філософія безпеки, заснована на периметрі, зосереджує зусилля на захисті кордонів, але робить мало, коли кіберзлочинець порушує їх.

VPN працює шляхом встановлення зашифрованих з'єднань між пристроями. (VPN часто використовують протоколи шифрування IPsec або SSL/TLS) [2, с.3]. Усі пристрої, які підключаються до VPN, встановлюють ключі шифрування, і ці ключі використовуються для кодування та декодування всієї інформації, що надсилається між ними. Цей процес може додати невелику затримку до мережевих з'єднань, що сповільнить мережевий трафік.

Ефект цього шифрування полягає в тому, що з'єднання VPN залишаються приватними, навіть якщо вони простягаються через загальнодоступну інфраструктуру Інтернету

Оскільки VPN працюють таким чином, багато компаній використовують їх для контроля доступу — іншими словами, щоб контролювати, які користувачі мають доступ до ресурсів. Компанія встановлює кілька різних VPN, і кожна VPN підключається до різних внутрішніх ресурсів. Призначаючи користувачів цим VPN, різні користувачі можуть мати різні рівні доступу до даних.

VPN далеко не абсолютно безпечні. Вони не призначені для заміни засобів безпеки, таких як антивірусне програмне забезпечення, і *мають* належати до ширшої системи безпеки.

В одному дослідженні IT-фахівців, які працюють в організаціях, які використовували VPN для доступу до мережі та/або заходів безпеки, майже **40% респондентів вважали, що їхню мережу вже було зламано** .

Однак це стрімке зростання кількості співробітників, які працюють вдома, у поєднанні зі збільшенням використання хмарних додатків означало, що IT-відділи мали важке завдання збалансувати продуктивність і безпеку.

У результаті кіберзлочинці націлюються на ці вразливості, зламуючи імена користувачів і паролі для доступу до служб VPN і використовуючи вразливості в самій службі VPN [2, с.2]. Організації часто не усвідомлюють, що їм загрожує небезпека, і пропускають критичні виправлення, які допомагають підтримувати безпеку, лише посилюючи ризик.

В іншому дослідженні, проведеному в 2021 році, 94% опитаних організацій повідомили, що вони знають, що їхні VPN вразливі до кібератак і експлойтів, а 72% були стурбовані тим, що їх VPN може поставити під загрозу здатність підтримувати безпеку свого середовища.

Перелік посилань:

1. What is a VPN?, Journal of Internet URL: https://www.cloudflare.com/learning/access-management/what-is-a-vpn/
2. Rama Bansode, Anup Girdhar, Common Vulnerabilities Exposed in VPN – A Survey, Journal of Physics: Conference Series URL: https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/012045

Кукшин Дарія Вікторівна
Студентка групи БСДМ-61, ННІЗІ ДУТ,Київ,Україна

DLP-СИСТЕМИ ТА ЇХ РОЛЬ У БОРОТЬБІ З ІНСАЙДЕРАМИ

За останні 20 років світ зробив технічний переворот. Зараз ми вже не уявляємо наше життя без електронних пристроїв. Інтернет змінив світ до невпізнанності. Кожна людина має телефон, а в кожному домі є пристрої підключені до Інтернету. Але з розвитком технологій та масовим їх використанням ростуть і різні інформаційні загрози. Тепер ми коли думаємо про безпеку, то захищаємо не тільки своє майно замками, а і захищаємося в онлайні. Ми живемо в епоху, коли кожен має задуматися, що таке інформаційна безпека та як її досягти і особливо це стосується бізнесу, адже інформація зберігається на електронних носіях і потрібно її захищати від стороннього впливу.

Розробляючи модель загроз і порушника для організації, досвідчений фахівець з кібербезпеки не повинен забувати про загрози, які можуть бути створені інсайдерами (внутрішніми порушниками), а також повинен задуматися про застосування DLP-систем для запобігання витоку даних (DLP - Data Leak/Leakage/Loss Prevention).

Внутрішні порушники (інсайдери) – це співробітники та керівники організації, а також особи, які мають з нею активні договірні відносини: партнери, постачальники, аутсорсери, підрядники, замовники та інші

контрагенти. Інсайдери відрізняються хорошими знаннями про роботу компанії, які вже мають або легко можуть отримати санкціонований і найчастіше розширений доступ до IT-активів. Акціонери, керівники вищої ланки, навіть лінійні менеджери, користуючись своїм посадовим становищем та обґрунтовуючи термінову службову необхідність, можуть намагатися отримувати високопривілейований доступ в обхід стандартних процедур інформаційної безпеки, а також можуть активно протидіяти заходам захисту (наприклад, DLP-системам) або процедурі розслідування в у разі виявлених порушень.

Отже, інсайдерами можна вважати як осіб, які навмисне здійснюють несанкціонований доступ до інформації, що захищається з різними деструктивними цілями, так і тих, чиї акаунти та робочі станції були скомпрометовані зловмисниками. Шкідливе ПЗ, потрапивши в інфраструктуру цільової атакованої організації, буде спочатку працювати від імені викраденого облікового запису, з подальшими спробами отримати доступ до високопривілейованих акаунтів і відключенням усіх захисних систем. Саме на цьому етапі кібератаки, коли несанкціоновані дії виконуються з-під облікових записів звичайних, низькопривілейованих користувачів, ми і можемо здійснити реагування та запобігти негативним наслідкам злому за допомогою систем класу DLP. Цей клас рішень здійснює контроль за роботою співробітників з інформацією, що захищається, за потоками конфіденційних даних в інфраструктурі компанії та способами їх обробки.

Контрольовані канали потенційного витоку інформації у різних виробників DLP-систем можуть відрізнятися, але, як правило, основними способами розкрадання даних є:

- копіювання файлів на знімні накопичувачі (флешки, CD/DVD-диски) та мобільні пристрої (смартфони, планшети);
- передача електронною поштою;
- передача через веб-сервіси (месенджери, соцмережі, хмарні сховища);
- передача через послуги синхронізації даних (наприклад, OneDrive, Dropbox);
- передача через AirDrop та Bluetooth-з'єднання;
- передача через буфер обміну (можливість скопіювати дані через віддалене RDP-підключення);
- роздрукування, фотографування та сканування документів.

За принципом роботи системи DLP можна умовно поділити на агентні та безагентні, з можливістю оперативного блокування несанкціонованих дій «на льоту», що дозволяють лише здійснювати пост-моніторинг виконаних дій. Також DLP-рішення відрізняються за функціональними можливостями виявлення конфіденційної інформації в потоках даних, за кількістю файлових форматів і мережевих протоколів, що підтримуються, за наявності функціоналу пошуку та класифікації конфіденційної інформації на мережевих сховищах і на локальних дисках, а також за наявності додаткових модулів.

Агентні системи запобігання витоку даних мають на увазі установку DLP-агента на всі контрольовані пристрої (ПК, ноутбуки, сервери, мобільні пристрої. Такий DLP-агент працює аналогічно антивірусу: встановлюється в операційну систему на низькому рівні, здійснює перехоплення системних викликів, контролює роботу дискової підсистеми та мережеву активність для виявлення інформації, що захищається. Мінусами агентного DLP-рішення можна назвати можливість відключення/зупинення DLP-агента високопривілейованим користувачем (локальним адміністратором), залежність агента від оточення (може некоректно працювати на атакованій зловмисниками системі), ресурсомісткість (підвищене споживання обчислювальних ресурсів пристрою, на якому його встановлено).

Безагентні системи функціонують лише на рівні контролю мережевого трафіку, і навіть встановлюються на точки обробки потоків інформації (корпоративні проксі-сервери, поштові сервери, файлові сервери, сервери бізнес-додатків). При роботі DLP-систем на рівні контролю мережевого трафіку їх підключення здійснюється через SPAN-порт маршрутизатора (схема «дзеркалювання», mirroring), або через TAP-підключення (установка пристрою з DLP-компонентом «в розрив» мережного з'єднання). У разі використання TAP-підключення можна виконувати інспекцію SSL/TLS-трафіку, частка якого у сучасному інтернеті близька до 90%. Встановлення DLP-компонент на важливі інфраструктурні об'єкти (поштові, файлові, бізнес- та проксі-сервери) передбачає контроль обробки інформації незалежно від кінцевих точок користувача - інакше кажучи, співробітник може працювати з корпоративною електронною поштою з особистого iPhone, на якому немає DLP- агента, проте його дії з інформацією, що захищається, будуть відстежуватися.

Функціональні характеристики способів виявлення конфіденційної (захищається) інформації в потоках даних грають вирішальну роль при виборі DLP-системи, оскільки можливості семантичного аналізу вмісту визначають кінцеву ефективність системи запобігання витоків даних.

Семантичне ядро DLP-системи може використовувати:

- Регулярні вирази: застосовується для структурованих даних, таких як паспортні дані, дані банківських карток та номерів страхування.
- Порівняння за ключовими словами: застосовується для пошуку конкретних «таємних» слів у вмісті файлів (назва нового продукту, хімічні формули, найменування компаній-постачальників).
- Пошук по повному збігу файлів: застосовується контролю обробки відомих заздалегідь і незмінних файлів (наприклад, підписані електронним підписом договору, зашифровані файлові контейнери).

Зазначимо також, що впровадження DLP-системи - це комплексний процес, який включає оцінку поточного стану процесів ІБ в компанії, аналіз інформації, що представляє цінність і обробляється в цифровому вигляді, проведення класифікації ІТ-активів, що містять конфіденційні дані, опитування відповідальних та власників бізнес-процесів. Для юридичного та документарного обґрунтування роботи DLP-системи слід запровадити в компанії

режим комерційної таємниці, підготувати список відомостей, що становлять комерційну таємницю компанії, потім ознайомити з документами співробітників компанії під розпис, особливо підкресливши у них факт застосування у компанії DLP-системи. Крім того, як організаційні заходи боротьби з внутрішніми загрозами можна застосовувати проведення перевірок претендентів при прийомі на роботу, психофізіологічні дослідження із застосуванням поліграфа, навчання та регулярне підвищення поінформованості працівників у галузі інформаційної безпеки та вимог організації з роботи з інформацією, а також безперервне забезпечення та контроль кадрової та психологічної безпеки членів колективу - виявлення негативних тенденцій, робота з негласними інформаторами, взаємодія з формальними та неформальними лідерами колективів

Отже, підсумувавши усе вище сказане, можемо зазначити, що DLP-системи можуть бути успішно застосовані для боротьби як з внутрішніми порушниками, так і із зовнішніми загрозами: наприклад, шпигунське ПЗ, що потрапило в систему, буде вести себе як типовий інсайдер: сканувати корпоративну мережу, шукати цінну інформацію в мережі і локально , намагатись передати знайдені дані назовні. Такий кіберінцидент може призвести до істотних збитків для компанії.

Перелік посилань:

1. What is DLP? Data Loss Prevention for Critical Business Information Стаття.- [Електронний ресурс]. – Режим доступу: https://www.exabeam.com/dlp/data-loss-prevention-policies-best-practices-and-evaluating-dlp-software/
2. Data Loss Prevention (DLP) Стаття.- [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/
3. What is Data Loss Prevention (DLP) Стаття.- [Електронний ресурс]. – Режим доступу: https://www.egress.com/resources/cybersecurity-information/email-dlp-and-data-loss-prevention/what-is-dlp

Крук Дмитро Миколайович
студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

ЗБЕРЕЖЕННЯ ТА БЕЗПЕКА ЦИФРОВИХ АКТИВІВ У BLOCKCHAIN

На сьогоднішній день технологія Blockchain стає все більш популярною, а цифрові активи на її основі починають використовувати як засіб платежу та збереження цінностей. Користувачі повинні взяти до уваги довгий список факторів і прийняти стандартні заходи безпеки, щоб гарантувати, що вони не піддаються непередбачуваним загрозам, пов’язаним зі збереженням своїх активів. У цій роботі будуть розглянуті заходи безпеки, які потрібно враховувати, і як їх застосовувати.

Ключові слова: Blockchain, цифрові активи, цифрові гаманці, кібербезпека.

Blockchain являє собою захищені від несанкціонованого доступу та захищені від несанкціонованого доступу цифрові реєстри, реалізовані розподіленим способом і, як правило, без центрального органу (тобто банку, компанії чи уряду). На базовому рівні вони дозволяють користувачам спільноти записувати транзакції в загальному реєстрі всередині цієї спільноти, тому що при нормальній роботі Blockchain-мережі жодна транзакція не може бути змінена

після публікації. У 2008 році ідея Blockchain була об'єднана з кількома іншими технологіями та обчислювальними концепціями для створення сучасних криптовалютних грошей, захищених за допомогою криптографічних механізмів, замість центрального сховища чи органу. Перший такий валютою на основі Blockchain був Bitcoin [1].

На сьогоднішній день кількість цифрових активів, створених на основі Blockchain значно збільшилась. Оскільки такі типи активів є формою збереження вартості та можуть бути способом розрахунків, вони потребують правильного зберігання та захисту. Для зручного та надійного користування цифровими активами були створені цифрові гаманці.

Гарячий гаманець — це хмарна інфраструктура зберігання цифрових активів, підключена до Інтернету. Ця структура гаманця завжди доступна для користувачів і дозволяє проводити миттєві транзакції, оскільки ключі зберігаються в хмарі. До них відносяться гаманці для персональних комп'ютерів, мобільні та веб-гаманці.

На відміну від гарячих гаманців, холодні гаманці дозволяють користувачам зберігати свої особисті ключі в автономному середовищі. Завдяки офлайновій природі вони забезпечують кращий захист від хакерів та інших загроз в Інтернеті. Типи гаманців, які в основному називають холодними, це паперові та апаратні гаманці. Останні є вдосконаленими USB-накопичувачами, призначеними для зберігання закритих ключів в автономному режимі.

Незважаючи на те, що холодні гаманці здаються більш захищеними, вони все одно не можуть зберегти активи на 100%.

Існують додаткові кроки та рекомендації щодо захисту цифрових активів з використанням крипто-гаманців [2], а саме:

- Шифрування гаманця;
- Створення резервної копії гаманця;
- Використання надійних паролів для підтвердження транзакцій;
- Використання двофакторної автентифікації;
- Використання мультипідпису;
- Оновлення програмного забезпечення;
- Перевірка та відправлення на підтверджені адреси;

Для найкращого захисту рекомендується використовувати рішення «холодного» збереження цифрових активів у комплексі кроками, описаними вище. Необхідно зберігати гаманець у надійному місці та ніколи не надавати доступ до пристроїв стороннім особам.

Перелік посилань:

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. URL:https://bitcoin.org/bitcoin.pdf

2. Crypto Security Guide 2022: Everything You Need to Do to Secure Crypto Investments. 2022. URL: https://cryptolinks.com/news/crypto-security-guide-2021

Кострoміна Марія Олександрівна *УБДМ-61*
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації

ОЦІНКА СТІЙКОСТІ КІБЕРБЕЗПЕКИ ТА ЧОМУ ЦЕ ВАЖЛИВО

Розглянуто поняття кіберстійкості. Досліджена різниця між поняттями «кубербезпека» та «та куіберстійкість». Розглянута методика зміцнення імунітету підприємства за рахунок кіберстійкості. Надані рекомендації з щодо покращення кіберстійкості підприємств у нових реаліях у тому числі за рахунок автоматизації процесів із забезпечення кібербезпеки.

Стійкість до кіберзагроз – це здатність організації передбачати кіберзагрози, готуватися до них, реагувати на них, відновлюватися та адаптуватися до них.

В ідеалі кіберстійка організація може протистояти як відомим, так і невідомим кризам, загрозам, супротивникам та іншим викликам, пояснює Дейв Адкінс, викладач і директор з кібербезпеки в Університеті штату Нью-Йорк в Олбані [1].

«Кіберстійкість є обов'язковою умовою для сучасних організацій, оскільки реальність така, що жоден бізнес не є надто малим, надто незрозумілим або надто невідомим, щоб піддатися кібератаці», – попереджає Джеррод Пайкер, аналітик конкурентної розвідки з кібербезпеки фірми Deep Instinct.

На макрорівні кіберстійкість означає, що організація може підтримувати критично важливі бізнес-операції навіть під час кіберінциденту, обмежуючи потенційний вплив на свою здатність отримувати прибуток, пояснює Девід Чаддок, директор із кібербезпеки фірми цифрових послуг West Monroe.

Проте кіберстійкість — це набагато більше, ніж просто здатність реагувати на подію кібербезпеки та відновлюватися після неї. «Справді стійкі організації також здатні ефективно сприймати, впроваджувати та приймати нові ініціативи та заходи безпеки — як технічні, так і процедурні — у великих масштабах і швидше», — зазначає Чеддок [2].

Планування кіберстійкості

Створення плану кіберстійкості потребує підтримки та участі всіх частин організації, включаючи фінанси, IT та операційну службу. «Важливо, щоб департаменти працювали разом, щоб класифікувати інформацію та ризики, а також визначати, де розмістити засоби контролю та де покладено відповідальність», — каже Пайкер. «Після узгодження плану необхідно скласти бюджет для фінансування фактичної реалізації плану».

Важливо залучити всю організацію. «Це не просто технічна проблема, яка знаходиться під контролем IT-директора або CISO», — каже Адкінс. «Ваші співробітники та постачальники можуть відігравати вирішальну роль у виявленні потенційних атак, щоб обмежити їхній вплив» [3].

Крім того, зважаючи на те, що тенденція до віддаленої роботи

продовжується, кіберобізнаність і навчання співробітників важливі як ніколи. «Це означає офіційну політику, навчання, симуляцію навчань і постійний аналіз ризиків», — каже Адкінс.

Адкінс радить організаціям використовувати настільні вправи, щоб перевірити практику і час інцидентів. «Набагато легше виправити недолік у вашому плануванні та процесах, коли ви не перебуваєте в центрі кризи», — каже він. «У розпал інциденту допускаються помилки, результатом яких часто стають неправильні рішення, що впливає на швидке повернення до нормальної роботи».

П'ять кроків до досягнення кіберстійкості

На завершення Чеддок пропонує виконати п’ять кроків, щоб досягти стану повної кіберстійкості [4].

1. Чітка стратегія – визначте та озвучте спільну мету та підвищте обізнаність про ризик (загрози, наслідки, толерантність до ризику), щоб усі були узгоджені на шляху вперед.

2. Управління. Для розвитку культури «довіряй, але перевіряй» необхідна система стримувань і противаг. Також важливо мати чітко визначені KPI/KPE, які можна виконати та виміряти, щоб забезпечити більш обґрунтоване прийняття рішень.

3. Тісна співпраця. Існує багато зацікавлених сторін, окрім IT та безпеки, які повинні мати місце за столом кібербезпеки. Безпека – це не лише проблема IT; спілкування має першочергове значення.

4. Цілісний підхід – необхідна однакова зосередженість на всіх областях NIST CSF, а не лише на можливостях захисту. Також необхідні інвестиції у функції реагування та відновлення.

5. Практика. Почніть із документування планів реагування на інциденти, а потім відпрацюйте стратегію внутрішнього реагування або вправ із ізоляції критичної системи принаймні раз на рік. Це експоненціально збільшить час реагування служби безпеки.

Перелік посилань:

1. John P., Mello Jr., The pandemic and your remote workforce: 9 ways to stay secure URL: https://techbeacon.com/security/pandemic-your-remote-workforce-9-ways-stay-secure

2. Stan Wisseman, How to boost your enterprise's immunity with cyber resilience URL: https://techbeacon.com/security/how-boost-your-enterprises-immunity-cyber-resilience

3. Ron Ross, Withdrawn NIST Technical Series Publication, 2019 URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

4. John Edwards, Cyber Resiliency: What It Is and How To Build It, 2022 URL: https://www.informationweek.com/strategic-cio/cyber-resiliency-what-it-is-and-how-to-build-it

КІБЕРБЕЗПЕКА КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Григоренко Дмитро Юрійович
Студент групи БСДМ-63,ННІЗІ ДУТ, Київ, Україна

На сьогодні існують багато організацій, які потрібно захищати. Так як з кожним днем

створюють все більше нових методів отримання конфіденційної інформації. Інформаційна безпека стосується політики, процедур і технічних заходів, які використовуються для запобігання несанкціонованому доступу, зміні, крадіжці або фізичному пошкодженню інформаційних систем. Контроль складається з усіх методів, політики та організаційних процедур, які забезпечують безпеку активів організації, точність і достовірність його облікових записів, і оперативне дотримання стандартів управління. Для менеджерів з інформаційної безпеки обговорювалися різні питання щодо вразливостей інформаційної системи, як-от зловмисне програмне забезпечення, мережеве зберігання даних, безпечне використання Інтернету та програм, уразливості програм, аналіз впливу на безпеку та показники.

Ключові слова: інформаційна система, кібербезпека, корпоративні системи.

Системи загального призначення та спеціалізовані системи перетворюють необроблені дані в корисну інформацію для прийняття рішень

Інформаційна система — це набір взаємопов’язаних компонентів, які працюють разом для збору, обробки, зберігання та поширення інформації для підтримки прийняття рішень. Вони також підтримують координацію, нагляд, аналіз та візуалізацію організації.

Крім того, IT-технологія описує будь-яку технологію, яка керує або забезпечує зберігання, обробку та передачу даних в організації. Усе, що стосується комп’ютерів — програмне забезпечення, мережі, інтранети, веб-сайти, сервери, бази даних і телекомунікації — підпадає під IT-парадигму.

Більшість сучасних компаній значною мірою залежать від цих систем для управління своїми операціями та прийняття рішень, від електронної пошти до баз даних і адміністрування веб-сайтів.

Інформація починається як необроблені дані, що представляють події, що відбуваються в організаціях або у фізичному середовищі; вона ще не була організована таким чином, щоб люди могли її зрозуміти та використовувати. Це вихідний матеріал для обробки та стосується фактів, подій і транзакцій. Таким чином, мета ІС полягає в тому, щоб перетворити вихідні ресурси в корисну інформацію, яку можна використовувати для прийняття рішень в організації.

Наприклад, лікарні мають великі бази даних пацієнтів, щоб мати змогу ефективно відстежувати історію хвороби. Університети мають системи для управління персоналом, студентами та оплатою, а також розширюють мережі для адміністрації кампусу. Навіть невеликий бізнес з доставки їжі додому потребує системи управління та відстеження замовлень.

Хоча інформаційні системи можуть відрізнятися за способом їх використання в організації, усі вони мають такі компоненти [1, с.1280]:

Апаратне забезпечення. Для виконання системи використовують локальне обладнання, наприклад комп’ютер або хмарні служби;

Програмне забезпечення. Це програми, які використовуються для адміністрування, обробки та аналізу;

Бази даних. Системи працюють з ресурсами, організованими в таблицях і файлах;

Мережа. Різні ресурси повинні бути підключені один до одного, особливо якщо багато різних людей в організації використовують одну систему;

Процедури. Вони описують, як конкретні дані та ресурси обробляються та аналізуються для отримання відповідей, для яких розроблена система («бізнес-логіка»).

Цілісність основного бізнесу компанії та захист клієнтів є критично важливими, а цінність і важливість інформаційної безпеки в організаціях роблять це пріоритетом. Усім організаціям потрібен захист від кібератак і загроз безпеці, і інвестування в цей захист є важливим. Порушення даних займає багато часу, коштує дорого та шкідливо для бізнесу. Завдяки потужній інформаційній безпеці компанія знижує ризик внутрішніх і зовнішніх атак на системи інформаційних технологій. Вони також захищають конфіденційні дані, захищають системи від кібератак, забезпечують безперервність роботи та забезпечують спокій усіх зацікавлених сторін, зберігаючи конфіденційну інформацію від загроз безпеці [2].

Перелік посилань:

1. Salem Al-Mamary, Yaser Hasan & Shamsuddin, Alina & Aziati, A. ResearchGate. (2014). *The Role of Different Types of Information Systems In Business Organizations* URL: https://www.researchgate.net/publication/264556488_The_Role_of_Different_Types_of_Information_Systems_In_Business_Organizations_A_Review accessed September 2019.
2. **The Importance of Information Security in Your Organization: Top Threats and Tactics. 2021. URL: https://www.auditboard.com/blog/importance-of-information-security-in-organization/**

Івахненко Маріанна Володимирівна
студентка групи БСДМ-53, ННІЗІ ДУТ, Київ, Україна
email: miva736@gmail.com

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. МЕТОДОЛОГІЇ АНАЛІЗУ БЕЗПЕКИ IIoT МЕРЕЖ

Протягом багатьох років безпека не розглядалася як важливий аспект архітектури програмного забезпечення. Довгі роки досліджень показали, що аналіз безпеки повинен бути частиною життєвого циклу розробки програмного забезпечення (SDLC). З цієї причини аналіз безпеки архітектури відіграє важливу роль для усунення загроз безпеці, які містяться в архітектурі. Метою аналізу загроз є виявлення, визначення пріоритетів і пом'якшення потенційних загроз безпеці. Аналіз загроз системи особливо важливий, оскільки доведено, що причиною багатьох вразливостей є потоки архітектурного проектування. Виправлення цих вразливостей на ранніх етапах зменшить витрати в процесі та зменшить вектор атаки.

Ключові слова: захист, безпека, аналіз безпеки, аналіз загроз.

Найбільш часто використовуваними методологіями є випадки неправильного використання, дерева атак, проблемні рамки та кілька підходів, орієнтованих на програмне забезпечення. Загалом можна згрупувати всі методи, орієнтовані на ризик, атаки та програмне забезпечення [1, с. 48].

1. Випадки неправильного використання (MUC): Ця методологія є розгалуженням розробки на основі варіантів використання та вимог. Випадки зловживання використовуються для захоплення потоків загроз, альтернативних

потоків, сценаріїв пом’якшення, тригерів, профілів зловмисників тощо. Компоненти, які використовуються в методології, поділяються на 3 типи: випадки зловживань, карти MUC і сценарії MUC.

• Дерева атак: у цьому підході кореневий вузол розгалужується на можливі вектори атак. Таким чином, єдиний шлях атаки почнеться з гілки та закінчиться в кореневому вузлі. Цей підхід зазвичай використовується в поєднанні з іншими. Перша частина аналізу полягає в картографуванні атак за допомогою дерев атак, а в другій частині комбінований підхід дозволяє визначити сценарії зловживання.

• Фрейми проблем: цей підхід використовується для опису проблем у програмному забезпеченні. Зазвичай це виконується на рівні абстракції класів і звертається до інтерфейсів і вимог.

• Цільово-орієнтоване розроблення вимог (GORE): це цільовий підхід, і він знаходиться на рівні абстракції систем, які спілкуються одна з одною для досягнення цілей.

2. Аналіз загроз, орієнтований на ризик: ця методологія зосереджена на активах і цінності для компанії. Основною метою цієї методології є пошук відповідного пом’якшення, щоб мінімізувати ризик. Основна увага приділяється оцінці фінансових втрат у разі можливої атаки. У результаті для цієї методології будуть визначені вимоги безпеки, а активи з найвищими активами матимуть найвищий пріоритет.

Однією з найбільш часто використовуваних методологій є STRIDE. Його можна визначити на різних рівнях абстракції. З цієї причини вона вважається однією з найбільш гнучких моделей для моделювання загроз. STRIDE — це модель аналізу загроз, створена корпорацією Майкрософт у 1999 році. З того часу багато що змінилося, а методології розвивалися разом із ускладненням систем [2]. STRIDE може забезпечити повне покриття для аналізу загроз. Моделювання загроз може бути реалізовано на рівні компонентів або на рівні функціональності системи. Ця методологія забезпечує чітке розуміння вразливостей системи та можливого впливу вразливості кожного компонента на всю систему. STRIDE означає аналіз загроз безпеці в 6 категоріях: спуфінг, фальсифікація, відмова, розкриття інформації, відмова в обслуговуванні (DOS), підвищення привілеїв [1].

Спуфінг: спуфінг — це тип атаки, коли зловмисник заволодіває компонентом/користувачем і виконує дії від їх імені, фальсифікуючи власну особу. Прикладом такого типу атак може бути незаконне отримання доступу до аутентифікаційної інформації користувача та її використання для виконання різноманітних дій у системі.

Іншим прикладом, більш пов’язаним із промисловим середовищем, є зловмисник, який витягує криптографічний ключ із пристрою, використовуючи вразливості апаратного чи програмного забезпечення пристрою та періодично звертаючись до системи та виконуючи дії під ідентичністю оригінального власника ключа.

Втручання: втручання може являти собою будь-яку форму саботажу, але в

основному це означає навмисну модифікацію компонента/мережі, щоб зробити його шкідливим для системи. Втручання включає неавторизовані зміни в даних, якими обмінюються компоненти або зберігаються в одному з них. Втручання на рівні пристрою може здійснюватися шляхом повної або часткової заміни програмного забезпечення пристрою. Ця дія потенційно відкриває компонент для описаної вище атаки спуфінгу.

Відмова: відмова — це термін у сфері безпеки, що описує нездатність компонента, який виконує дію, змінити право власності на дію. Хорошим прикладом цього є підписані транзакції в системі, що підтверджують автентичність власника транзакції. Загроза відмови — це здатність одного з компонентів виконувати незаконну операцію в системі, яка не має можливості відстежувати заборонені операції.

Розкриття інформації: розкриття інформації — це термін, що описує сценарій, коли компонент може надати інформацію неавторизованим третім особам. Наприклад, якщо компонент працює з інфікованим програмним забезпеченням, зловмисник може потрапити в компонент і отримати витік інформації або проникнути в канал зв’язку між компонентами.

Відмова в обслуговуванні (DOS): атаки типу «відмова в обслуговуванні» в основному мають на меті зробити службу/компонент тимчасово недоступними або відмовити в обслуговуванні дійсним користувачам системи. DOS-атаки можуть завдати серйозної шкоди загальній системі, якщо компоненти взаємозалежні. Відмова в обслуговуванні, як правило, досягається шляхом затоплення, що означає надсилання ненормальної кількості запитів до цільової служби за короткий проміжок часу. У індустріальному світі ця атака також може бути виконана на фізичному рівні.

Підвищення привілеїв: у цій атаці непривілейований компонент/користувач отримує привілейований доступ і може виконувати неавторизовані дії в системі. Цю атаку можна здійснити, використовуючи слабкі місця потоку проектування або конфігурації системи. Більш складний сценарій для здійснення атаки полягає в проникненні в усі системи захисту та перетворенні в довірену частину системи. Це може спричинити ризик невизначеної атаки.

Перелік посилань:
1. Sukiasyan A. Secure Data Exchange in IIoT / Anna Sukiasyan., 2019. – 100 с.
2. Shostack A. Experiences threat modeling at Microsoft / Shostack A., 2019.

Цигикал Богдан Олександровичч
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Що ми розуміємо під технічної системи захисту інформації? Основні технічні засоби – це технічні засоби, призначені для обробки, зберігання та передавання закритої інформації.

Існують і допоміжні технічні засоби та системи, призначені для обробки відкритої інформації. Але вони можуть утворювати технічні канали витоку закритої інформації. Отже, приступаючи до захисту інформації на певному об'єкті, необхідно, в першу чергу, визначити, які види інформації підлягають захисту, а, подруге, які приміщення у будівлі (або всю будівлю) необхідно захищати.

Ключові слова: технічні засоби, технічний захист інформації.

Об'єкт технічного захисту інформації – це будова, приміщення, окремий основний технічний засіб або їх група, об'єднана загальним призначенням, які підлягають захисту від технічних розвідок.

Якщо треба захищати велику кількість приміщень (велику група, яка, наприклад, складається з підгруп), об'єкт захисту може складатися зі всієї будівлі. Якщо необхідно захистити декілька видів інформації, що циркулює у приміщеннях об'єкту, то використовується комплексний захист інформації.

Також необхідно знати ступень таємності інформації, що підлягає захисту. Крім того обов'язково необхідно знати загрози для інформації, які можуть виходити від потенційного супротивника. Загроза для інформації – це виток, можливість блокування або порушення цілісності інформації, яка може здійснюватися під час використання технічних засобів, недосконалих з точки зору захисту інформації, або інші канали витоку інформації.

При цьому слід пам'ятати, що для кожного виду інформації та кожного виду загроз існують цілком конкретні засоби захисту та способи їх застосування, отже треба користуватися тими системами та засобами захисту, що найбільш повно відповідають потенційним загрозам для кожного з видів інформації, яку слід захищати на конкретному об'єкті.

При цьому необхідно виявити всі потенційні канали витоку інформації та забезпечити їх блокування з рівнем технічного захисту, відповідним ступеню таємності інформації та рівню потенційних загроз. Рівень технічного захисту інформації – це сукупність вимог, в тому числі і тих, що нормуються, які визначаються режимом доступу до інформації та загрозами для її безпеки. Взагалі у технічному захисті інформації розрізняють два основні методи: пасивний та активний методи захисту інформації [9].

Активний захист побудовано на постановці перешкоди зняттю інформації шляхом випромінювання завад у канал витоку, рівень яких перевищує рівень небезпечних сигналів, які можна зняти з каналів витоку. До активного захисту також відносяться методи протидії, що засновані на постійному контролі середовища розповсюдження небезпечних сигналів необхідними для цього

приладами та комплексами, які дозволяють виявляти спроби зняття інформації та активного пошуку і знешкодження засобів зняття інформації.

Пасивний захист побудовано на зниженні спроможності певного технічного джерела витоку або середи розповсюдження небезпечних сигналів до передачі інформації шляхом технічних змін його властивостей, наприклад, шляхом екранування електромагнітного випромінювання.

Перелік посилань:

1. Алексенцев А. И. Понятие и назначение комплексной системы защиты информации // Вопросы защиты информации. - 1996. - № 2. - с. 2 - 3.

2. Остапов С. Е. О-76 Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

3. Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест /За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.

Томин Оксана Василівна
студентка групи КСМ-61, КНУБА, Київ, Україна

ОСНОВНІ ВРАЗЛИВОСТІ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ. СПОСОБИ ЗАХИСТУ СИСТЕМИ

Відеоспостереження є основою сучасної системи безпеки, забезпечує прямий моніторинг місця, допомагає запобігти вторгненню, виявити підозрілу активність, виявити надзвичайні ситуації та провести розслідування. Аналіз відео може допомогти виявити зловмисників, зокрема спроби підключитися до локальної мережі для викрадення конфіденційної інформації. Відеоспостереження містить багато інформації і тому стало джерелом величезної небезпеки. Системи відеоспостереження забезпечують можливість побудови розподілених систем з можливістю віддаленого доступу та можливістю інтеграції з іншими системами. Однак для них характерні проблеми, пов’язані з безпекою мережі, тобто вразливість даних і пристроїв. У кожного пристрою є свої слабкі місця, і камери відеоспостереження не є винятком.

Ключові слова: відеоспостереження, камера, захист, загроза, злам.

Встановлюючи камеру безпеки або цифровий відеореєстратор необхідно враховувати той факт, що вони піддаються високому ризику злому програмного забезпечення. Тому важливо знати, як працюють атаки камер безпеки для захисту систем відеоспостереження, які існують ризики несанкціонованого доступу до ресурсів корпоративної мережі передачі даних, що пов’язано з недоліками в налаштуваннях безпеки бездротової мережі.

На етапі аналізу вразливості системи необхідно враховувати, що система відеоспостереження може використовуватися для вирішення технічних завдань і організації бізнес-процесів підприємств. Тому можливою ціллю зловмисника може бути інша система, а обладнання системи відеоспостереження може бути використано як проміжний етап атаки. Крім того, системи відеоспостереження часто інтегруються з іншими підсистемами безпеки та системами автоматизації. Питання інформаційної безпеки систем відеоспостереження стає завданням захисту всіх систем, з якими вони інтегруються або обмінюються даними.

Для того, щоб використовувати найбільш ефективні засоби безпеки, необхідно визначити типи загроз і проаналізувати способи атаки на системи

відеоспостереження. Існує три основних види загроз для систем відеоспостереження:

- злам для отримання доступу до даних;
- злам для перехоплення керування або відключення системи;
- злам із метою несанкціонованого використання обчислювальних потужностей системи.

Ефективна безпека відеокамер надзвичайно важлива через велику кількість таких найпоширеніших атак як MitM, DoS, встановлення зловмисного програмного забезпечення, підвищення привілеїв і ACE (виконання довільного коду). Раніше функції камери були лише незначним аспектом можливостей виробників. Сьогодні це змінилося, оскільки кіберзлочинці створюють більш складні хаки. Це призвело до того, що виробники камер, інтегратори та користувачі зосередили увагу на кібербезпеці камер.

Відповідний захист мережевих камер відеоспостереження забезпечується на трьох рівнях: технологія, обробка і підтримка кінцевих користувачів.

Сама камера має бути створена за принципом «безпечної конструкції» та включати такі функції, як Trusted Platform Module (TPM), параметри безпечного завантаження та підписане та зашифроване вбудоване програмне забезпечення. Пристрої з інтегрованим модулем TPM забезпечують розширені криптографічні параметри, придатні для захисту сертифікатів і відповідних їм ключів від несанкціонованого доступу. Закриті ключі зберігаються в модулі довіреної платформи та ніколи не залишають його; усі криптографічні операції, які вимагають використання закритого ключа, натомість надсилаються до TPM для обробки. Це гарантує, що секретна частина сертифіката ніколи не залишає безпечне середовище в TPM і залишається захищеною навіть у разі порушення безпеки. Безпечне завантаження гарантує, що камера завантажуватиметься лише з авторизованою мікропрограмою. Це також гарантує, що на вашому пристрої немає зловмисного програмного забезпечення після відновлення заводських налаштувань.

Всупереч поширеній думці, більшість порушень безпеки мережі є результатом людської помилки, поганого обслуговування або неправильно встановлених параметрів. Найкраще захистити мережу підприємства шляхом впровадження стандартних, простих процесів і процедур, в першу чергу це стосується кожного бізнесу.

Творець технічної частини повинен надати підтримку іншим професіоналам, наприклад програмістам і системним адміністраторам – це підтримка кінцевих користувачів. Це буде спрямовано на навчання користувачів багатьом способам захисту своїх пристроїв від вразливостей. Підтримка також вбачає навчання їх керувати паролями та сертифікатами для програмного забезпечення відеоспостереження, вбудованого в пристрої. Вона вимагає, щоб виробники моніторили та негайно і відкрито повідомляти про типові загрози безпеці та вразливості.

Розглянемо основні рекомендації щодо способів забезпечення безпеки систем відеоспостереження. Використовуючи їх, можна побудувати комплексну

ефективну програму профілактики та реагування.

Перш за все, потрібно регулярно перевіряти вразливість кожного компонента системи відеоспостереження. Ця перевірка повинна включати тестування всіх протоколів, апаратного забезпечення та мікропрограми. Тому кожен компонент системи відеоспостереження буде проходити ретельну перевірку на здатність протистояти кібератакам. Тестування протоколу – перевірка безпеки мережевих комунікацій, надійності шифрування та можливості несанкціонованого перехоплення даних. Аналіз прошивки пристрою повинен включати встановлення доступних оновлень.

Також, необхідно обмежити кількість користувачів і мінімізувати фізичний доступ до систем відеоспостереження. Чим більше людей впливають на роботу системних компонентів або даних, тим більша ймовірність, що система й надалі буде вразливою до кібератак.

Теж не використовуйте пароль за замовчуванням. Підібрати пароль для системи (якщо він був встановлений виробником) нескладно. Пароль за замовчуванням пристрою необхідно змінювати. Таким чином, велика можливість уникнути найпоширеніших помилок жертв злому, але ця процедура не вирішує проблему захисту загалом. Камери відеоспостереження мають внутрішню операційну систему, а також інші програми, які можуть мати вразливості та дають можливість використовувати їх для отримання доступу до системи.

Розглянемо і кілька заходів фізичного захисту систем відеоспостереження.

- використання телекомунікаційних шаф, що замикаються;
- зберігання серверного та важливого комутаційне обладнання в окремих закритих кімнатах;
- прокладання кабелю у важкодоступних місцях;
- використання для прокладання та монтажу кабелів, труб, закритих лотків і коробів, монтажних коробів;
- установка в спеціальних вандалостійких варіантів виконання обладнання в особливо легковразливих зонах або легкодоступних місцях.

Отже, оскільки вторгнення, злами та атаки стають новою реальністю в кіберпросторі, то розвиток систем відеоспостереження та інших систем вимагає постійної співпраці між інтеграторами та виробниками для створення та впровадження методів, необхідних для забезпечення кібербезпеки, та надавати необхідну підтримку, щоб допомогти кінцевим користувачам протистояти цим загрозам.

Перелік посилань:

1. Дудатьев А.В., Баришев Ю.В., Войтович О.П. Метод оцінювання безпеки інформаційних ресурсів підприємства на основі аналізу вразливостей. Вісник Хмельницького національного університету. № 4. 2008. С. 78–83.
2. Полевщиков А.А. Кібербезпека мережевого відеоспостереження: теорія та практика. Алгоритм безпеки.. 2017. № 5. С. 30–32

Ахтьоров Владислав Юрійович,
студент групи БСДМ-61, ННЗІ ДУТ, Київ, Україна.

ТЕСТУВАННЯ БЕЗПЕКИ ДЛЯ ВЕБ

Поміж різних засобів забезпечення захисту нформація для веб, тестування безпеки надає найбільш чітку інформацію про вразлиовтсі в системі, та ціну реалізації загроз на систему. Для запобігання багатьом загрозам тестування безпеки виступає ключовим елементом, який впроваджується з самих ранніх етапів існування проекту і проводовжує використовуватись на протязі всього життєвого циклу.

Ключові слова : SDLC, STLC, тестування на проникнення, тестування безпеки, веб.

Для забезпечення достатнього рівня захищенності веб-сайтів, веб-ресурсів та веб-додатків необхідне впровадження практик безпеки з самих ранніх етапів їх ствоерння до останніх стадій їх підтримки. Одним з методів забезпечення безпеки вистпає тестування безпеки.

Тестування безпеки – це процес тестування, аналізу та звітування рівня безпеки. Цей процесс є широким та різноплановим, а підбір технік тестування проводиться з врахуванням індивідуальних особливостей проекту.

Тестування і його типи пов’язані з життєвим циклом веб-сайту або веб-додатку. Життєвий цикл проекту (SDLC- Software Development Life Cycle) включає в себе планування, дизайн, впровадження та підтримку. Всі етапи життєвого циклу мають свої унікальні характеритсики та спроможні створити нові загрози для безпеки. Таким чином на стадії планування може бути описана система неспромжна забезпечити достатній рівень захисту інформації, при дизайні описані компоенти системи та їх взаємодія може бути представлена з уразливостями, при впровадженні виникають основні вразиловості, так як на цьому етапі створюється вихідний код проекту. На етапі підтрмки проекту можуть бути виявлені нові вразливості, які не були помічені на минулих етапах.

Для знаходження вразливостей та недоліків веб-сайту або веб-додатку на всіх етап проекту проводиться тестування на тестування безпеки. Таким чином виникає життєвий цикл тестування (STLC – Software testing Life Cycle). Тестування може проводитися з етапу планування до етапу підтримки проекту. Під час планування аналізується сам опис проекту та потенційні вразливості в ньому. Під час етапу підтримки активно проводится тестування вже створених компоненів, нових компонентів та проводится рергесивне тестування системи після впровадження нових компонентів та функцій. Тестування на будь-якому із етапів надає інформацію про рівень безпеки системи та дозволяє отримати чітку картину про систему в цілому [1].

До осовних типів тестування безпеки можна віднести :

- Ручні перевірки;
- Моделювання загроз;
- Перегляд вихідного коду;
- Тестування на проникнення;

Ручні перевірки робляться експертами та перевіряють впроваджені політики, процеси, а також дизайн та архітектуру веб-сайту або веб-додатку. Подібний тип тестування можна проводити з самих ранніх етапів життєвого циклу проекту.

Моделювання загроз – це перевірка системи та аналіз ризиків на основі потенційної реалізації певної загрози. Для проведення такого тестування необхідно формувати чіткий опис загроз, які будуть актуальними для даної системи.

Перегляд вихідного коду може проводитися лише зі стадії впровадження та є доволі затротною формою тестування, проте він надає чіткі дані про вразливості в системі на рівні коду, адже будь яка загроза яка є в системі може бути знайдена на рівні вихідного коду.

Тестування на проникнення - це імітована кібератака на комп'ютерну систему з метою перевірки на наявність уразливостей, які можна використовувати. У контексті безпеки веб-додатків тестування на проникнення зазвичай використовується для посилення брандмауера веб-додатків (WAF) [3]. Подібне тестування можна проводити лише після етапу впровадження, але воно надає найбільш практичні данні про вразлиості системи.

Таким чином можна зробити висновок, що тестування безпеки може надати різнопланову інформацію про вразиловості та недоліки системи, а завдяки тому що воно може проводитись з самих ранніх етапів життєвого циклу, забезпечення безпеки проходить ще до моменту коли загрози можуть бути реалізовані.

Перелік посилань :
1. Penetration Testing.[Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/application-security/penetration-testing/.
2. What Is the Software Development Life Cycle?. [Електронний ресурс] – Режим доступу:L: https://phoenixnap.com/blog/software-development-life-cycle.
3. Saad E., Mitchell R. Web Security Testing Guide v4.2. - 2021 рік - с. 18-19.

Ахтьоров Владислав Юрійович,
студент групи БСДМ-61, ННІ ДУТ, Київ, Україна.

ДИНАМІКА ЗАГРОЗ ДЛЯ ВЕБ-САЙТІВ НА ОСНОВІ OWASP TOP 10

Відслідкування змін в динаці загроз є ключивим елементом в побудові ефективної системи захисту, адже для чіткого та швидкого реагування на кібератаку необхідно мати систему яка спроможна забезпечити відповідний набір засобів для подібного реагування, сформований з врахування актуальних загроз.

Ключові слова : веб-безпека, OWASP TOP 10 , кіберзагрози, ін'єкції.

Відслідкування самих критичних та поширених загроз для веб-ресурсів є одним з ключовим елементів побудови системи захисту. В сучасному світі технологій динамічні та швидкі зміни в загрозах не дозволяюь орієнтуватися на

старі сатистичні дані та звітності, а отже не дозволяють залишати підхід до забезпечення захисту незмінним.

Динамічні зміни в актуальних загрозах за останні роки можна відслідкувати на основі порівняння останньої версії OWASP TOP 10 та її попередника.

Згідно з OWASP TOP 10 2021 самими критичними загрозами для веб-сайтів виступають : 1). Порушення контрою доступу ; 2). Збої в криптографічних алгоритмах ; 3). Інєкції; 4). Небезпечний дизайн ; 5). Помилки в конфігурації безпеки ; 6). Вразриливі та застарілі компоненти ; 7). Помилки в ідентифікаія та аутентифікації ; 8). Проблеми з інтеграцією 9). Проблеми з логуванням та моніторингом ; 10). Підробка запитів зі сторони сервера.

Сучасні системи захисту мають бути створені саме з врахуванням цих загроз. Для порівняння, OWASP TOP 10 2020 представляє SQL та інші типи ієкцій веб-сайтів, як найкритичнщу загрозу, в порівнні з її 3 місцем в останній версії списку. Подібні зміни можна відслідкувати в багатьох пунках списку. Таким чином порушення контрою доступу виступало лише 5 в списку загроз, а проблеми з логуванням та моніторингом — 10 [1].

Також варто помітити, що змінюється не лише порядок загроз. Багато вказаних в OWASP TOP 10 2021 загроз є новими для списку, в порівнянні з минулим роком. Підробка запитів зі сторони сервера. проблеми з інтеграцією , збої в криптографічних алгоритмах, небезпечний дизайн, помилки в ідентифікаія та аутентифікації є новими актуаьними вразливостяи які не мало такої критичності в минилому.

Загрози, які втратили свою актуальність включають в себе міжсайтовий скриптинг, витік конфіденційної інформації, XML загрози, небезпечна десеріалізція та використання компонентів з відомими вразливостями. Можна помітити, що витік конфіденційної інформації, як загроза в останньому списку був позначений лише як симпотм для збоїв в криптографічних алгоритмах, а використання компонентів в відомими вразливостями було віднесено до більш широкої категорії вразриливих та застарілих компонентів[2].

Окрім самих загроз змінюється ще й динаміка кібератака. В останні роки все більше зростає актуальність викоритсання ransomware, особливо для корпаративних мереж. Також помітна тенденція зростання DdoS-атак[3].

Таким чином можна прийти до висновку, що змінюється не лише актуальність та критичність певних загроз, але й статсистика кібератак, які ці загрози реалізують. Для побудови ефективної системи захисту необхідно враховувати динаміку зміни актуальності певних загроз та формувати відповідні міри опираючись на нові загрози.

Перелік посилань :
1. OWASP Top 10 - 2021. OWASP, 2021. [Електронний ресурс] – Режим доступу: https://owasp.org/Top10/#welcome-to-the-owasp-top-10-2021.
2. OWASP Top 10 Security Risks & Vulnerabilities. [Електронний ресурс] – Режим доступу: https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/.
3. Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022. [Електронний ресурс] – Режим доступу: https://purplesec.us/resources/cyber-security-statistics/#Recent

Каленський Юрій Миколайович
Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ЗАХИСТ РЕСУРСІВ В ХМАРІ ЗА ДОПОМОГОЮ AWS GUARDDUTY

Публікація актуалізує важливість захисту ресурсів в хмарі. Більшість підприємств та організацій використовують хмару для зберігання інформації або обчислення великих масив даних. Часто ця інформація є чутливою або секретною, несанкціонований доступ до якої може призвести до різного виду втрат (репутаційні, інтелектуальні, фінансові тощо). Тому захист хмарного середовища є важливою частиною процесу забезпечення інформаційної безпеки.
Ключові слова: AWS, хмара, хмарні обчислення, GuardDuty .

Amazon GuardDuty – це автоматизований сервіс виявлення загроз, який постійно відстежує підозрілу активність і несанкціоновані дії для захисту облікових записів AWS, робочих навантажень та даних, що зберігаються в Amazon S3 (Simple Storage Service) (Рис. 1) [1]. GuardDuty поєднує в собі машинне навчання, виявлення аномалій, мережевий моніторинг і виявлення шкідливих файлів, використовуючи як розроблені AWS, так і іншими провідними вендорами, джерела. GuardDuty здатний аналізувати десятки мільярдів подій серед багатьох джерелах даних AWS, таких як журнали подій AWS CloudTrail, журнали потоків Amazon Virtual Private Cloud (VPC), журнали аудиту служби Amazon Elastic Kubernetes (Amazon EKS) і журнали запитів DNS.

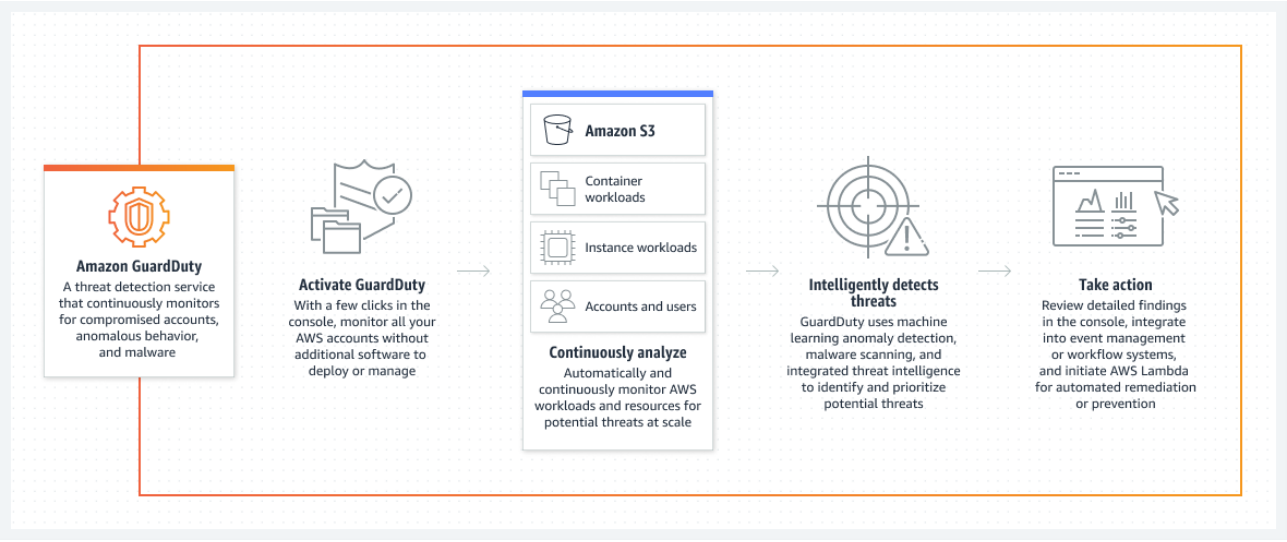


Рис. 1 – Як працює AWS GuardDuty

Варто зазначити, що даний сервіс необхідно використовувати з іншими сервісами AWS для максимального рівня захисту хмарної інфраструктури та даних. Наприклад, з AWS Lambda, CloudWatch, VPC та іншими.

Для прикладу роботи AWS GuardDuty та його взаємодії з іншими сервісами AWS візьмемо загрозу викрадених облікових даних [2]:

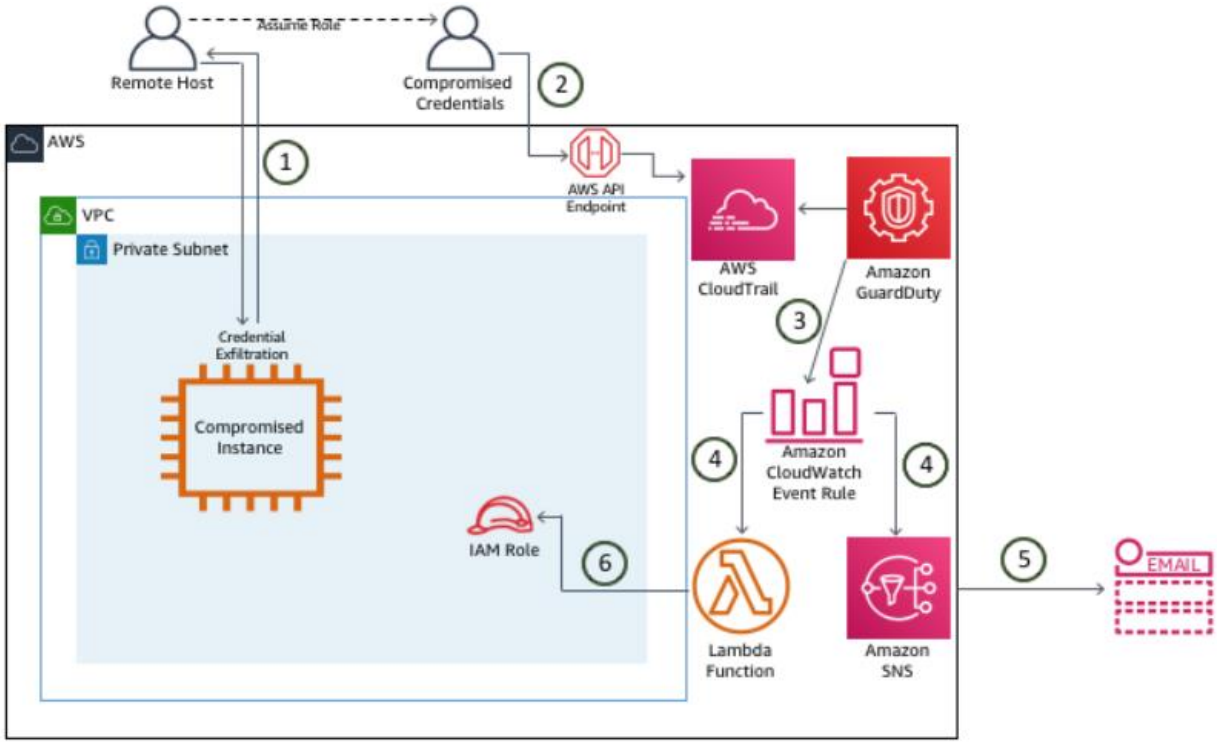


Рис. 2 – Сценарій виявлення і боротьби з загрозою викрадених облікових даних

Спроба зловмисника використати скомпрометовані облікові дані та алгоритм дії AWS GuardDuty з інших сервісів безпеки:

1. Зловмисник компрометує інстанс (віртуальну машину) EC2 і викрадає облікові дані через службу метаданих.
2. Зловмисник налаштовує користувача CLI для здійснення викликів API.
3. GuardDuty генерує результат (інформацію про подію №2) і надсилає його на консоль GuardDuty і CloudWatch Events.
4. Правило події CloudWatch створює повідомлення через AWS SNS і запускає функцію Lambda.
5. SNS надсилає електронний лист із інформацією про результат роботи GuardDuty.
6. Функція Lambda додає політику IAM до зламаного користувача, скасовуючи всі активні сеанси, і протягом однієї хвилини після виявлення GuardDuty електронною поштою надсилається повідомлення про виправлення.

Після цього скомпрометовані дані вважаються вилученими, а адміністратори безпеки сповіщені про спробу отримання несанкціонованого доступу.

Таким чином, GuardDuty, у поєднанні з іншими сервісами, є надійним інструментом захисту ресурсів (інформаційних, обчислювальних тощо) в хмарі AWS.

Перелік посилань:

1. Amazon GuardDuty [Електронний ресурс]. Режим доступу: https://aws.amazon.com/guardduty/
2. Threat Detection with AWS GuardDuty [Електронний ресурс]. Режим доступу: https://scalesec.com/blog/threat-detection-with-aws-guardduty/#iam-role-credential-exfiltration

Бурлін Михайло Олександрович
студент групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

НАСКІЛЬКИ ЕФЕКТИВНИМ Є АНТІ-СПАМ РІШЕННЯ СЬОГОДНІ

*Експерти стверджують, що **50% повідомлень електронної пошти,** надісланих у всьому світі, були зазначені як спам.*

Рішення для боротьби зі спамом дуже допоможуть у бізнесі, якщо ви отримуєте спам у величезних обсягах. Спам є серйозною загрозою безпеці, оскільки він прямо чи опосередковано впливає на кожного користувача Інтернету, і немає реального вирішення проблеми спаму порівняно з антивірусними програмами. *Спам, надісланий невідомими відправниками, можна ефективно відфільтрувати за допомогою проактивного рішення для захисту від спаму* , що економить час.

Сьогодні існує безліч методів фільтрації спаму , і всі вони мають лише одну мету, а саме «ВИДАЛИТИ або ЗУПИНИТИ» небажані листи. Нижче наведено кілька способів.

Фільтрація спаму за вмістом

Це найпоширеніший спосіб блокування спаму. Найпоширеніші спам-слова: додатковий дохід, грошовий приз і ти переможець. Такі яскраві слова чи електронні листи потрібно фільтрувати.

Внесення певних IP-адрес у чорний список

Спамери здебільшого використовують IP-адресу для злому . У такому випадку організаціям потрібно внести в чорний список певні IP- адреси. Таким чином вони можуть *запобігти спаму з цих IP-адрес* .

Чорний список у реальному часі

Цей чорний список у режимі реального часу схожий на чорний список, за винятком того, що його ведуть сторонні підприємства. Щоразу, коли надходить лист, фільтр щоразу підключає його до сторонньої системи, щоб порівняти адресу відправника з попередньо встановленим списком. Такий аутсорсинг ефективний в організаціях, де IT-персонал не має достатньо часу, щоб вручну витрачати на ведення чорних списків.

Евристичні фільтри

Евристичні фільтри – це форма фільтрів на основі вмісту, які зосереджуються на підозрілих словах, які зазвичай зустрічаються в спам-повідомленнях . Підозрілі слова, які часто надходять, як-от «Rolex», «Віагра» тощо, позначаються високими балами, тоді як терміни, які зустрічаються в звичайних електронних листах, отримують нижчі бали. За визначенням адміністратора програми захисту від спаму , фільтр блокує повідомлення, що

містять слова з високими балами.

Байєсовські фільтри

Байєсовські фільтри вважаються передовою та новою формою методів фільтрації вмісту. Ці фільтри використовують на практиці математичну ймовірність класифікації різних повторюваних слів у двох окремих списках, тобто сміття та законні. *Для безперервного збереження цього списку після аналізу вмісту електронних листів, отриманих користувачами, байєсовським фільтрам потрібен проміжок часу* . Таким чином, їх ефективність помітна, поки ви їх використовуєте. У першому випадку вам, можливо, доведеться видалити непотрібні файли самостійно.

Метод захисту від спаму DNS

Система DNS-пошуку шукає ім'я домену відправника, яке він використовує для ідентифікації . Система намагається перевірити адресу електронної пошти за допомогою дійсного запису MX . Якщо відповідності немає, то повідомлення вважатиметься небажаним і автоматично видалятиметься системою. Цей пошук точно виявить доменне ім’я, пов’язане з сервером, і виявився корисним для виявлення спаму.

OOP Spam Filter API

Якщо ви також шукаєте спам-фільтр електронної пошти , зверніть увагу на наведену нижче версію API фільтра спаму. Це може допомогти вам впоратися з вашими потребами. Цей спам-фільтр створений для фільтрації будь-якого обміну вмістом, будь то блог, форум чи соціальні мережі. Використання різних інструментів поєднується таким чином, що допомагає ефективно виявляти кількість спам-слів у вмісті та не залишає жодних недоліків. Він підтримує такі функції:

Алгоритм машинного навчання

Добре навчений і вбудований алгоритм машинного навчання визначає, чи є вміст спамом чи ні.

Підрахунок спаму

Він використовує розширений евристичний метод фільтрації спаму . Оцінка в діапазоні від 0 до 6 присвоюється кожному вмісту, і один із них має більшу ймовірність вважатися спамом.

Виявлення спаму

Вміст, що містить велику кількість слів, виявляється зі списку поширених підозрілих спам-слів . Цей список може бути попередньо встановлений або постійно підтримуватися фільтром залежно від математичної ймовірності отриманих повідомлень.

Чорний список Список IP-адрес

Екран здатний підтримувати постійний список IP-адрес спамерів, які оновлюються на їхніх серверах і класифікуються як чорний список IP-адрес і викидають спам-повідомлення.

Алгоритм виявлення викидів мови

Ця конкретна техніка фільтра дозволяє аналізувати мову, отриману у вмісті, і гарантує, що вона добре інтегрується з вашими очікуваннями. Він розгорнутий

на Rapid API, де ви можете легко знайти детальну інформацію про додаток.

Перелік посилань:
1. DuoCircle // Spam filter: why is spam filter necessary // липень 31 2021. URL: https://www.duocircle.com/spam-filtering/spam-filter-why-is-spam-filter-necessary#:~:text=The%20spam%20filter%20is%20mandatory,reduce%20the%20amount%20of%20spam
2. WebTel // Spam solutions // жовтень 11, 2022. URL: https://webtel.in/Blog/what-are-email-spam-filters-and-why-are-they-necessary
3 MailChannels // what is spam filtering // URL: https://www.mailchannels.com/what-is-spam-filtering/

Порохницький Олександр Андрійович
Студент групи УБДМ-51, ННІЗІ ДУТ, Київ, Україна

ВПЛИВ НА ІНФОРМАЦІЙНУ СТАБІЛЬНІСТЬ КОЛЕКТИВУ

Колектив компанії – це жива екосистема організації що схильна до певного роду захворювань та пертурбацій, в залежності від внутрішніх так і зовнішніх чинників. Фейки один з чинників який може з легкістю вплинути на колектив та створити певні проблеми для керівництва в майбутньому. Кожний працівник організації це актив, про який керівництво слід піклуватися та захищати, в разі виникнення певного роду нештатних ситуація.

Ключові слова: інформаційна безпека, колектив, фейки, дезінформація, актив.

1. Фейки, дезінформація та інші загрози.

Фейки – це в більшості випадків ненавмисне спотворення інформації людьми. Тобто, не правильне сприйняття якогось джерела або інформації з подальшою спробою перетворенням її у факт. Таке перетворення може створити хибне уявлення про людину, ситуацію або інший факт.

Дезінформація – це цілеспрямоване спотворення інформації яке використовується для власних цілей. Її застосування свідчить про навмисне введення в оману людину або ж організацію, за для власного збагачення або дискредитації об’єкту дезінформації.

Представленні поняття дадуть загальне розуміння що може стати зовнішнім подразником колективу, яке інколи має досить впливове значення на працездатність.

Розглядаючи внутрішні подразники, можливі конфлікти в колективі з різних причин. До них можна віднести: сімейні проблеми, випадки під час робочого процесу та зменшення активності організації(як результат зовнішнього впливу).

2. Колектив та його інформаційна стабільність.

Стабільність колективу це запорука росту організації. В цьому контексті не мається на увазі стагнація, стабільність інформаційного стану компанії має на увазі що колектив не розвалиться від першої ж інформаційної атаки із зовні або зсередини.

Кожна людина це особистість, до якої потрібний власний підхід. Завдання

керівника встановити робочий контакт, який допоможе при досягання поставлених цілей. Встановлення цього контакту допоможе вирішити купу проблем пов'язаних з інформаційної стабільністю.

Керівник відділу - це лідер який повинен розуміти усю ситуацію та компенсувати втрати та допомагати своїм підлеглим у вирішенні питань які можуть вплинути на колектив. Також в його компетенції є надання усіх ресурсів, розробка плану та перевірки виконаних завдань.

3. Захист та протидія впливу.

В першу чергу слід визначити курс інформаційної стабільності, виставити правила поширення інформації та певний інформаційний етикет. Ці дії будуть спрямовані на стабілізацію колективу та майбутньому уникненні конфліктів при умові дотримання правил.

В другу чергу при виникненні певних ситуацій, причиною яких можу бути зовнішній чинник або ж внутрішній. Керівнику слід провести загальну бесіду або особисту з членами колективу та спростувати або підтвердити ту інформацію через яку сталась проблема.

Захист інформаційної стабільності в колективі лягає на плечі керівника та HR їх вплив на цю стабільність повинний бути найбільший.

4. Заходи для покращення інформаційного стану.

Заходи з покращення цього стану можуть бути різними але їх основною частиною повинні бути об'єднання колективу. Уникнення розповсюдження фейків та дезінформації або ж їх своєчасне спростування для зменшення негативного впливу. В разі виникнення екстрених ситуацій пов'язаних з ситуацією в країні або локальних місцях, надання офіційних інструкцій працівникам та відповідно їх дотримання самим керівником.

Перелік посилань:

1. Почепцов Г.Г. (ДЕЗ)ИНФОРМАЦИЯ : книга. Київ 2019 – 248с ISBN 978-966-437-563-1
2. Kristin Ryba Leading Through Change: How to Create Stability in the Workplace URL: https://www.quantumworkplace.com/future-of-work/how-to-create-stability-in-the-workplace

Самко Владислав Васильович
студент групи УДБМ-61, ННІЗІ ДУТ, Київ, Україна

ЗАХИСТ ІНФОРМАЦІЇ У ХМАРІ. ЗАХИСТ ІНФОРМАЦІЇ У ПРОЦЕСІ ОБРОБКИ З ВИКОРИСТАННЯМ КОНФІДЕНЦІЙНОГО КОМП'ЮТИНГУ

У сучасному світі та IT-середовищі з кожним днем набирає популярності використання хмарних сервісів. Все більше організацій переводять свої потужності та сервіси у хмару. Безумовно використання хмарних сервісів несе велику кількість переваг, таких як: економія на апаратних ресурсах; зниження

витрат та відповідальності за адміністрування систем, підвищення доступності, тощо. Але з перенесенням систем у хмару виникають і нові завдання по контролю та захисту таких систем. Однією з таких проблем є захист інформації при її зберіганні, передачі та обробці у хмарі.

Досить популярною на даний момент технологією яка використовується для вирішення такої задачі є BYOK(Bring your own key) – це популярна послуга у провайдерів хмарних послуг яка дозволяє користувачам самостійно генерувати криптографічні ключі та управляти ними[1]. При використанні такої технології ключі зберігаються на стороні клієнта, часто використовуючи KMS(Key management service) та HSM(Hardware security module). Користувач може сам визначати які сервіси матимуть можливість використання тих чи інших ключів. Поєднуючи цю технологію з методами захисту інформації при передачі вдається забезпечити безпеку інформації на двох етапах її життєвого циклу. А що ж відбувається на етапі обробки інформації в хмарі.

Захист інформації з використанням конфіденційного комп'ютингу

При проведенні криптографічних операцій у хмарі, сервісам які їх виконують повинні бути доступні криптографічні ключі[1]. Наприклад, при шифруванні хмарним сервісом певної інформації для її подальшої передачі ключ яким здійснюється це шифрування використовується оперативною пам'яттю машини та знаходиться там у відкритому вигляді.

Таким чином під час його використання в хмарних системах до нього можуть отримати доступ сторонні сервіси, адміністратори провайдера хмарних послуг, шкідливе ПЗ якщо машина інфікована, гіпервізор, тощо. Тож необхідно визначити спосіб захисту та ізоляції даних та криптографічних ключів в обробці від таких загроз. Для такого захисту створено технологію конфіденційного комп'ютингу (CC – confidential computing). Така технологія існує досить довго, але лише у 2019 році група виробників ПЗ, процесорів та хмарних провайдерів — Alibaba, AMD, Baidu, Fortanix, Google, IBM/Red Hat, Intel, Microsoft, Oracle, Swisscom, Tencent and VMware — створили Confidential Computing Consortium (CCC) – організацію яка визначає стандарти CC та контролює розвиток open-source CC[2].

Технологія CC використовує набір методів поєднуючи їх для ізоляції та захисту даних в захищеному сегменті системи. Інформація, що оброблюється в такому сегменті доступна лише певному переліку авторизованих сервісів і невидима для будь-чого іншого, включаючи хмарного провайдера. Одним з основних методів реалізації CC є використання технології TEE(Trusted Execution Environment) – виділення сегменту процесору який використовує вбудовані ключі шифрування та атестаційні механізми для захисту даних. Атестаційний механізм несе відповідальність за перевірку сервісів, що намагаються отримати доступ до захищеного сегменту перевіряючи не лише їх право на доступ, але і їх цілісність. У разі порушення цілісності у доступі буде відмовлено. Також TEE володіє і власним сертифікатом який дозволяє підтвердити автентичність

інформації при отриманні її авторизованими сервісами. Також можна використовувати і інші методи захисту інформації при обробці. Наприклад: гомоморфне шифрування, яке дозволяє проводити операції над зашифрованими даними та отримувати їх результат у зашифрованому вигляді, не розшифровуючи дані для обробки; MPC(Multi-party computation) – метод обробки даних при якому на вхід подаються таємні дані від декількох учасників так, щоб в результаті обробки жоден з учасників не міг прочитати таємні данні інших; тощо.

У кожного з методів є свої переваги та недоліки, але можливість TEE ефективно працювати з великими об'ємами даних робить його досить ефетивним та популярним рішенням.

Таким чином використання CC дозволяє забезпечити захист ключів шифрування та конфіденційних даних під час їх обробки у хмарі, а поєднання його з іншими методами захисту інформації такими як: KMS; HSM; тощо, дозволяє захистити інформацію на всіх етапах її життєвого циклу.

Перелік посилань:

1. Moritz Eckert. Bring your own key (BYOK) was a lie! URL: https://blog.edgeless.systems/bring-your-own-key-was-a-lie-92587d7c73ec
2. Nataraj Nagaratnam. Confidentail computing. IBM Cloud Learn Hub. URL: https://www.ibm.com/cloud/learn/confidential-computing

Грабовий Вадим Андрійович
студент кафедри Інформаційна та кібернетична безпека, ННІЗІ ДУТ,
Київ, Україна
email: vadimofua@gmail.com

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

На сьогоднішній день, в умовах гібридної війни, забезпечення кібербезпеки критичної інформаційної інфраструктури є як ніколи важливою. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, та інші. Розглянуто чинне законодавство та проаналізовано підзаконні нормативно-правові акти України у галузі кібербезпеки критичної інформаційної інфраструктури.

Ключові слова: кібербезпека, критична інформаційна інфраструктура, Закон України, право.

З появою кіберпростору з'явилось як багато нових можливостей для комунікацій, бізнесу так і багато ризиків та загроз кібербезпеки. Для мінімізації цих ризиків необхідно вжити заходів для забезпечення кращої кібербезпеки у світі в цілому, адже просто відмовитись від цифровізації означатиме зупинку модернізації державі [1, с. 100].

Під час правового регулювання інформаційної інфраструктури в Україні йде правове забезпечення безпеки усіх учасників інформаційних відносин. Інформаційні відносини, які виникають при використанні цифрових технологій, вимагають: визначення державного підходу до правового регулювання поданих

відносин; розробки методології забезпечення інформаційної безпеки інформаційної інфраструктури та її користувачів [2, с. 2012].

Сам об'єкт критичної інформаційної інфраструктури визначається як комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [3].

Відповідно до Стратегії розвитку інформаційного суспільства в Україні, інформаційна інфраструктура — сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування [4].

За результатами дослідження встановлено, що у Законі Україні «Про основні засади забезпечення кібербезпеки України» є певні недоліки, зокрема даний закон не визначає підстави віднесення організацій до суб'єктів критичної інформаційної інфраструктури, і як результат, всі інформаційні об'єкти, які належать цим організаціям, виходячи із Порядку формування переліку об'єктів критичної інформаційної інфраструктури, також не визначені. Така невизначеність уповільнює ідентифікацію критичних інформаційних систем і знижує рівень ефективності забезпечення безпеки [3, с. 2013].

Проаналізувавши нормативно-правові документи в галузі забезпечення безпеки критичної інформаційної інфраструктури, передачі на обміну інформації у даній систем дозволяє розглянути наступну структуру органів виконавчої влади України [3, с. 2013-2015]:

- відповідно до ч. 1 ст. 5 Закону України «Про основні засади кібербезпеки України» Президент України здійснює координацію діяльності у сфері кібербезпеки, включаючи забезпечення безпеки критичної інформаційної інфраструктури, як складової національної безпеки і оборони України;
- указом Президента України від 07.06.2016 р. № 242/2016 утворено Національний координаційний центр кібербезпеки та призначено керівником Центру секретаря Ради національної безпеки і оборони України;
- Кабінет Міністрів України здійснює державний контроль у сфері безпеки критичної інформаційної інфраструктури, визначає порядок підготовки і використання ресурсів єдиної мережі електрозв'язку для забезпечення функціонування значущих об'єктів критичної інформаційної інфраструктури та механізм визначення категорій даних об'єктів;
- Постановою Кабінету Міністрів України від 19.06.2019 р. № 518 визначено Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури.
- Державна служба спеціального зв'язку та захисту інформації України забезпечує функціонування інформаційних систем, інформаційно-телекомунікаційних мереж і автоматизованих систем управління, що знаходяться на території України, в дипломатичних представництвах і консульських установах України.

- До завдань Національного координаційного центру з комп'ютерних інцидентів віднесені забезпечення координації діяльності суб'єктів критичної інформаційної інфраструктури України з питань виявлення, попередження і ліквідації наслідків комп'ютерних атак і реагування на комп'ютерні інциденти.
- Відповідно до Закону України "Про основні засади кібербезпеки України" Міністерство цифрової трансформації України за погодженням з Державною службою спеціального зв'язку та захисту інформації України та Службою безпеки України визначає порядок, технічні умови установки і експлуатації засобів, призначених для пошуку ознак комп'ютерних атак в мережах електрозв'язку, які використовуються для організації і захисту взаємодії об'єктів критичної інформаційної інфраструктури.
- Поряд з тим, Кабінет Міністрів України також затвердив Порядок ведення Державного реєстру об'єктів критичної інформаційної інфраструктури України. Цей Реєстр формується і ведеться Державною службою спеціального зв'язку та захисту інформації України з метою обліку, зберігання і надання інформації в електронному та паперовому вигляді про об'єкти критичної інформаційної інфраструктури, що належать на законних підставах суб'єктам критичної інформаційної інфраструктури. Інформація (відомості та/або дані), яка надається суб'єктами критичної інформаційної інфраструктури, відповідно до Порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування, у Державну службу спеціального зв'язку та захисту інформації України повинна бути актуальною, повною і достовірною.

Перелік посилань:

1) Бакалінська О. Правове забезпечення кібербезпеки в Україні [Електронний ресурс] / О. Бакалінська, О. Бакалинський. – 2019. – Режим доступу до ресурсу: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf.
2) Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України [Електронний ресурс] / [М. Ковалів, Р. Скриньковський, Ю. Назар та ін.]. – 2021. – Режим доступу до ресурсу: https://cutt.ly/EB0D85U.
3) ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://ips.ligazakon.net/document/t172163?an=1.
4) Про схвалення Стратегії розвитку інформаційного суспільства в Україні [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.kmu.gov.ua/npas/246420577.

Запорожченко Михайло Михайлович
студент групи АКБ-125, ННІЗІ ДУТ, Київ, Україна

БАЗОВІ СТРАТЕГІЇ ПОПЕРЕДЖЕННЯ ЗАГРОЗ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Анотація. Соціальна інженерія була і залишається актуальною загрозою для компаній незалежно від сфери їх діяльності. Оскільки реалізація соціоінженерних атак може навіть не вимагати глибоких технічних навичок, захист від них є вкрай важливим. Далі розглянуто базові стратегії, за допомогою яких можна зменшити ймовірність реалізації подібних атак.

Ключові слова: соціальна інженерія, кібербезпека, фішинг, аудит.

Згідно WEF Global Cybersecurity Outlook 2022 [1] соціальна інженерія посідає друге місце серед найбільш турбуючих організації кіберзагроз, одразу після програм-вимагачів. Згідно IBM Security X-Force Threat Intelligence Index 2022 Full Report [2] найбільш розповсюдженими методами отримання зловмисниками первинного доступу до мереж жертв є дві загрози: фішинг (41%) та експлуатація вразливостей (34%), за якими слідують вкрадені облікові дані, брут-форс атаки, RDP, знімні носії та розпилення паролів. Значна кількість компаній може стати жертвою цільової фішингової атаки, про що свідчить середня частота відкликів співробітників на атаки у 17.8% для звичайних атак та 53.2% для вішингу (голосового фішингу).

На сьогоднішній день у зловмисників існує велика кількість можливостей для того, щоб дізнатися інформацію про організацію, яка була обрана ними в якості об'єкта атаки. Через недбалість або необізнаність персоналу, відповідального за інформаційну безпеку, в мережі у відкритому доступі може міститися більше корисної для зловмисників інформації, ніж організація може уявити. Це дозволяє зловмисникам підвищити свої шанси на успішну кібератаку за рахунок більш детальної розвідки і, відповідно, ретельнішої підготовки, наприклад, на основі зібраної інформації підготувати більш деталізовану цільову фішингову атаку.

Типовими атаками для соціальної інженерії є фішинг (вішинг, смішинг), претекстінг, приманка, спуфінг, послуга за послугу (Quid Pro Quo), тейлгейтінг тощо. Оскільки атаки з використанням методів соціальної інженерії спрямовані на людей, то до найуразливіших факторів організації проти загроз з використанням цих методів доцільно буде віднести в першу чергу саме необізнаність персоналу (або топ-менеджменту компанії у разі вейлінгу – полювання на «китів»), неналежне його тренування з питань безпеки, прогалини в політиках інформаційної безпеки, неналежну мотивацію тощо [3].

В більшості випадків соціоінженерні атаки спрямовані на конкретного співробітника компанії, тому їх нелегко одразу виявити, проте можна їх попередити, як мінімум шляхом доведення до всього персоналу, навіть якщо він безпосередньо не пов'язаний із забезпеченням безпеки, інформації про актуальні загрози та розповсюджені тактики соціальної інженерії, які використовуються зловмисниками. Окрім цього доцільно буде впровадити та дотримуватися парольної політики, фізичної безпеки і періодично проводити аудити і моніторинг.

Підвищення обізнаності персоналу. Проведення роботи з персоналом щодо підвищення його обізнаності з питань виявлення та протидії загрозам соціальної інженерії помітно підвищить рівень захисту компанії вцілому, оскільки зменшить кількість найбільш вразливих ланок в її системі захисту – співробітників. Необхідно визначити перелік цілей захисту від соціальної інженерії та осіб, які будуть відповідальні за доведення цих цілей до персоналу. Цей процес можна підкріпити описом реальних випадків інцидентів, які сталися внаслідок соціоінженерних атак, таким чином, кожний буде розуміти, до чого

такі атаки можуть призвести і навіщо від них захищатися.

Періодично необхідно проводити семінари з персоналом, на яких демонструвати практичні приклади реалізації соціоінженерних атак, описувати основні їх характеристики та надавати рекомендації щодо протидії ним.

Загрози соціальної інженерії повинні бути оцінені належним чином. На оцінку може впливати кількість відкритої інформації про компанію, кількість співробітників, підрозділів, сфера діяльності тощо, а також наслідки, до яких призведе потенційний інцидент.

Також компанія повинна впровадити алгоритм дій персоналу у разі підозри або виявлення соціоінженерної атаки, включити його у політику інформаційної безпеки та довести до всіх співробітників [4].

Фізична безпека. Одним з перших заходів, яких необхідно вжити для протидії соціальній інженерії, є забезпечення фізичного захисту. Ці заходи повинні практично унеможливити потрапляння неавторизованого персоналу в будівлю та приміщення об’єкта захисту та можуть включати в себе пропуски з фотокарткою працівника, які він показує при вході та виході; журнали відвідувачів, підрядників з підписами їх та відповідального співробітника, тимчасові перепустки тощо.

Парольна політика. Зазвичай першою (а в деяких випадках – єдиною) перешкодою для зловмисників при вторгненні в системи компанії або обліковий запис її співробітника є пароль. Використання паролів є доволі розповсюдженим, оскільки така форма автентифікації дешевша та простіша для впровадження, ніж біометричні сканери, ключ-карти тощо, хоча і забезпечує нижчий рівень безпеки.

Парольна політика повинна бути частиною політики інформаційної безпеки компанії і визначати вимоги до стійкості, періодичності зміни, зберігання паролів, щоб їх не можна було легко підібрати брут-форсом, за словником, маскою, вивідати у співробітника тощо. Адміністратори безпеки повинні контролювати дотримання персоналом вимог парольної політики та періодично нагадувати про постійно існуючу загрозу компрометації паролю внаслідок соціоінженерної атаки.

Аудит і моніторинг. Ці процеси значно впливають на безпеку систем та мереж організації. Активний моніторинг допомагає своєчасно виявляти інциденти, що виникають, та інші події, і відповідно, швидше їх локалізовувати та знешкоджувати, обмежуючи при цьому потенційний збиток, якого вони можуть завдати.

Аудит дозволяє виявити наявні вразливості та можливості для вдосконалення. Сьогодні компанії-аудитори пропонують таку послугу, як аудит методами соціальної інженерії. Такий вид аудиту дозволяє виявити, наскільки компанія вразлива до соціоінженерних атак, яка частка співробітників була скомпрометована, а також прогалини в захисті IT-інфраструктури компанії та рекомендації щодо їх усунення.

Такі аудити можуть охоплювати весь персонал компанії, лише тих співробітників, які володіють найважливішими даними, а також тих співробітників, які вже піддавалися атакам. Найбільш популярними сценаріями

при проведенні такого виду аудиту є фішингова розсилка на поштові скриньки, розсилки на поштові скриньки зі шкідливим вкладенням, розсилка вірусних посилань в месенджерах та соціальних мережах, підключення USB-носіїв зі шкідливим файлом та розповсюдження емуляторів USB-HID (BadUSB).

Перевагою аудитів методами соціальної інженерії є те, що аудитори на основі аналізу інформації про персонал та компанію, про її засоби захисту (антивіруси, спам-фільтри тощо) та конфігурації засобів комунікації шукають реальні способи взаємодії зловмисника з співробітником також розроблюють і на практиці перевіряють можливі в умовах діяльності конкретної компанії сценарії атаки.

Висновки. Соціальна інженерія залишається доволі актуальною загрозою інформаційної безпеки. Наразі не існує єдиного контрзаходу, який зміг би гарантовано запобігти реалізації соціоінженерних атак, однак комплексний підхід, який буде охоплювати як організаційні, так і технічні заходи, допоможе мінімізувати такі ризики. Однак першочерговою задачею залишається проведення роботи з персоналом, який працює в компанії і відповідає за захист інформації, якою вона володіє.

Перелік посилань:

1. World Economic Forum Global Cybersecurity Outlook 2022. URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

2. IBM Security X-Force Threat Intelligence Index 2022 Full Report. URL: https://www.ibm.com/downloads/cas/ADLMYLAZ

3. Social Engineering Attacks: Management and Prevention. URL: https://www.webroot.com/us/en/resources/tips-articles/social-engineering-attacksmanagement-and-prevention

4. What is Social Engineering? URL: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

Мальгіна Катерина В`ячеславівна
студентка групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

IT-ризики політики BYOD

З дистанційними працівниками завжди існує підвищений ризик використання персоналом персональних пристроїв замість корпоративних, особливо тому, що концепція наявності двох телефонів, двох ноутбуків або двох настільних комп'ютерів може здатися громіздкою. Тому деякі організації запроваджують політику Bring Your Own Device (BYOD), яка має низку переваг для бізнесу.

Основними перевагами політики BYOD є :

· Ознайомлення – люди знайомі зі своїми пристроями та звикли до пристороя.

· Продуктивність – менше часу витрачається на вивчення нового апаратного чи програмного забезпечення.

· Фінансова економія – організації можуть заощадити гроші на купівлі

обладнання.
Але якщо прийняти політику BYOD, слід враховувати деякі ризики безпеки.
· Втрата даних – передача даних з особистих пристроїв на робочі може призвести до навмисної або випадкової втрати даних. Крім того, деякі особисті пристрої (наприклад, ноутбуки або планшети) можуть використовуватися іншими членами сім'ї, що також може призвести до випадкової втрати даних.
· Ризики GDPR (General Data Protection Regulation) – коли особисті пристрої потенційно використовуються іншими членами родини, можуть виникнути проблеми з відповідністю GDPR, якщо на пристрої зберігаються конфіденційні дані.
· Застаріле програмне забезпечення – окремі люди навряд чи дотримуватимуться того самого протоколу оновлення програмного забезпечення на своїх персональних пристроях, що й IT-відділ компанії. Таким чином, вони можуть мати застаріле програмне забезпечення та операційні системи, залишаючи пристрій відкритим для кібератак.
· Слабка безпека – безпека персональних пристроїв може бути не такою надійною, як політика безпеки компанії, яка включатиме брандмауери, програмне забезпечення для захисту від шкідливих програм, багатофакторну автентифікацію та регулярні оновлення.
· Відокремлення співробітників – якщо працівник залишає бізнес, важче переконатися, що дані компанії видалено з пристрою.

Створення політики BYOD
Щоб вирішити ці проблеми безпеки, важливо створити політику BYOD, якої повинні дотримуватися всі співробітники, які використовують власні пристрої.
Перше, про що користувачі повинні знати, це те, що якщо вони використовують власні пристрої для комерційних цілей, вони повинні відчувати себе комфортно з організацією, яка здійснює керування пристроями на їхніх машинах, як якщо б вони належали компанії. Це включатиме:
· Прийнятне використання – визначення того, які завдання дозволено виконувати з особистих пристроїв, як-от запити на щорічну відпустку, звіти про витрати, електронні листи чи дзвінки клієнтам, до яких ресурсів компанії вони можуть отримати доступ зі своїх пристроїв, а також скільки особистого використання їм дозволено під час роботи день.
· Заборони – визначення того, що персоналу заборонено робити за допомогою особистих пристроїв, наприклад передавати дані клієнтів або банківські реквізити, які дані їм заборонено зберігати, а також які програми заборонено. Також можна заблокувати пристрій, щоб запобігти копіюванню з бізнес-програм в особисті.
· Мінімальні стандарти – визначення мінімальних прийнятих стандартів щодо версій ОС і конкретного використовуваного програмного забезпечення.
· Багатофакторна автентифікація – забезпечення багатофакторної автентифікації персональних пристроїв, які використовуються в бізнес-цілях, для доступу до бізнес-даних.

· Доступ – визначення того, який доступ організація повинна мати до персональних пристроїв. Чим менше доступу має ІТ-відділ, тим менш безпечним є пристрій. Крім того, важливо чітко визначити, які особисті пристрої можуть підключатися до мережі компанії, а які ні.
· Відшкодування – узгодження того, чи буде компанія відшкодовувати будь-які витрати на придбання пристрою, а також скільки (якщо такі є) витрат на дані буде покрито.
· Забезпечення – забезпечення виконання політики BYOD, яка покладається на співпрацю співробітника, може бути складним. Якщо вони не дотримуються цієї політики, пристрої загрожують безпеці, і вони потенційно можуть нести відповідальність у разі порушення даних.

Перелік посилань:

1. Tech target // Part of: What to know before deploying BYOD in the enterprise// січень 02 2022.
URL: https://www.techtarget.com/searchmobilecomputing/tip/3-BYOD-security-risks-and-how-to-prevent-them
2. ManageEngine Academy // Your BYOD plan - savior or security threat?// жовтень 11, 2022.
URL: https://www.manageengine.com/academy/byod-device-management.html
3. National Cyber Security Centre // Device Security Guidance // травень 10, 2022
URL: https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device#:~:text=BYOD%20is%20the%20concept%20of,the%20property%20of%20the%20user.

Гарнатко Леонід Олегович
студент групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Анотація. Поняття «інформаційна безпека» з’явилось завдяки розвитку засобів інформаційних комунікацій серед суспільства. У сучасному світі стрімкий розвиток інформаційних технологій не є новиною. Збільшується кількість інформаційних систем, програмних забезпечень , які допомагають персоналу підприємства управляти інформаційними потоками. Відповідно до цього збільшується кількість цінної інформації. Тому питання про її захист стоїть досить гостро.

Метою роботи є розгляд проблемних питань по управлінню інформаційною безпекою підприємства для забезпечення нормального функціонування і динамічного розвитку організації..

Основний матеріал. Необхідно зазначити, що у науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека».

Поняття «інформаційна безпека» слід розглядати як стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення

Інформаційна безпека підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів з досягнення стану захищеності інформаційного середовища організації. Така

діяльність повинна забезпечувати нормальне функціонування і динамічний розвиток підприємства. [1].

Мета інформаційної безпеки полягає в тому, щоб зберегти цілісність, повноту та точність інформації, зменшити ризик несанкціонованих змін у інформаційних системах.

Захист інформації на підприємстві є важливим завданням, що може впливати на фінансову та виробничу його діяльність і як наслідок на ринок, в якому існує. Для того, щоб забезпечити підприємству розвиток та конкурентоспроможність, необхідно створити ефективну систему управління інформаційною безпекою.

У інформаційну безпеку підприємства входить сукупність напрямів, методів, засобів і заходів, що знижують незахищеність інформації і не дають можливість зловмисникам доступу до інформації, її розповсюдженню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою – комплексність. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи[2].

Якщо конфіденційність, цілісність, доступність, достовірність тощо знаходяться в критичному стані, то це може призвести до досить негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами, безпековими, фінансовими й іншими критичними системами;

розголошення відомостей, що становлять комерційну й інші види таємниць; порушення достовірності персональних даних фізичних осіб .

Наслідком вище сказаного може стати: проблеми у виробництві зберіганні та збуті продукції; відмова в обслуговуванні, на недоступність бази даних критичної інфраструктури, фінансові втрати, та витрати на усунення наслідків порушення; невиконання договірних зобов'язань, та можливих подальших судових процесів тощо.

Для розв’язання проблем інформаційної безпеки підприємства необхідно створити підрозділ інформаційної безпеки, який входить до складу служби внутрішньої безпеки підприємства. Даний підрозділ повинен підкорятися вищому керівництву. Загалом до таких підрозділів входять такі фахівці як системні адміністратори та адміністратори безпеки. [3]

Завдання у сфері захисту інформації. До основних завдань підрозділу інформаційної безпеки належить захист інформації в інформаційно-телекомунікаційних системах.

У цілому до основних завдань підрозділу належать:

- керування доступом користувачів до інформаційних ресурсів систем з метою захисту від неправомірного випадкового або навмисного втручання у роботу і несанкціонованого (із перевищенням наданих повноважень) доступу до програмних і апаратних ресурсів як персоналу, так і сторонніх осіб;
- захист даних, що передаються каналами зв’язку;
- захист інформації з обмеженим доступом від витоку;

- захист інформації від спеціальних впливів;
- реєстрація, збереження і надання даних про події, що відбувалися у системі і стосувалися інформаційної безпеки (ІБ);
- контроль роботи користувачів системи адміністраторами та обов'язкове повідомлення адміністратора безпеки про будь-які спроби несанкціонованого доступу до ресурсів системи;
- контроль і підтримка цілісності критичних ресурсів системи захисту і середовища виконання прикладних програм;
- забезпечення функціонування програмно-технічних комплексів з метою захисту інформації від впровадження у роботу потенційно небезпечних програм і засобів подолання системи захисту;
- керування та моніторинг засобів захисту інформації.

Вищезазначені завдання у сфері захисту інформації та інформаційної безпеки покладені в основу Концепції технічного захисту інформації в Україні, яка є складовою забезпечення національної безпеки України. [4]

Висновки

Збереження інформації – це те питання, яке заслуговує уваги, адже хто володіє інформацією, той володіє світом. Тому важливо слідкувати за потоками отриманої інформації, за її цілісністю, правдивістю та актуальністю. У наш час існує безліч інформаційних технологій, які дозволять зробити цей процес швидшим та зручнішим, проте необхідно пам'ятати, що останнє рішення завжди залишається за людиною, за керуючою особою. Проте накопичення інформації – це не єдине, на що потрібно звернути увагу. Існує також така проблема як захист інформації на підприємстві та управління інформаційною безпекою підприємства. Для цього необхідно оцінити ризики та можливі причини втрати цінної для підприємства інформації. Після того, як ризики будуть оцінені, необхідно виконати ряд дій по нормативам управління інформаційною безпекою підприємства. Для цього існують певні заходи. Якщо дотримуватись правил управління інформаційними ресурсами, то можна уникнути ситуацій втрати інформації. Фахівці з управління інформаційною безпекою здатні вирішувати завдання теоретичного та практичного характеру, що безпосередньо пов'язані з усіма аспектами захисту інформації. Отже грамотна інформаційна безпека – це складова, яка дозволить підприємству залишатися на високому рівні і бути конкурентоспроможним та успішним.

Перелік посилань:

1. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.
2. Шевченко С.Ю. Формування системи управління інформаційної безпеки підприємства / С.Ю. Шевченко // Економіка підприємства: теорія та практика: зб. мат. IV міжнар. наук.- практ. конф. 12 жовт. 2012р., - К.: КНЕУ, 2012.
3. Чунарьова А.В. Система управління інформаційною безпекою на базі міжнародних стандартів серії ISO / А.В. Чунарьова, А.В. Чунарьов // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: науково-технічний збірник. – К.: НТУУ "КПІ" , 2012. – № 2(24). – С.50-53.
4. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.

Алексеєнко Олександра Анатоліївна
студентка групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

ЯК ПОБУДУВАТИ НАДІЙНУ АРХІТЕКТУРУ БЕЗПЕКИ ХМАРНИХ СИСТЕМ

Найбільш недооцінена, але вкрай важлива частина інтеграції технологій хмарних систем – створення архітектури безпеки хмарних обчислювань. Її ціль полягає у виявленні та усуненні слабких місць системи, які можуть виникати в результаті організації безпеки залежно від продукту ніж від системи. Належним чином розроблена хмарна архітектура безпеки керується загрозами, з якими стикається підприємство, тоді як засоби керування хмарною безпекою є тактичними заходами, які вживаються для зменшення ризиків інформаційної безпеки.

Незалежно від того, чи переносите ви наявні програми в хмару чи створюєте їх у Amazon Web Services (AWS), Microsoft Azure (Azure) або Google Cloud Platform (GCP), є аспекти безпеки, які надаються спільно з постачальником хмари. Розробка хмарної інфраструктури вимагає від архітектора безпеки хмари свідомо думати про такі речі, як поверхня атаки, яку представляють веб-інтерфейси, критичність інформаційних активів і різні вектори атак, які можуть бути використані зловмисником.

Можна виділити 7 наступних елементів, які вирізняють ефективну архітектуру безпеки хмарних обчислень і які слід враховувати при її створенні:

Створення безпеки на кожному рівні

Існує низка окремих технологій безпеки, які необхідно вибрати, розгорнути, налаштувати, підтримувати та контролювати для безпечної хмарної інфраструктури. Найкращий спосіб підійти до цього завдання — зрозуміти обсяг зусиль та подумати про це з точки зору рівнів — рівня оркестровки, рівня гіпервізора, рівня додатків, рівня гостьової системи, рівня мережі та фізичного рівня. Захист будь-якої хмарної інфраструктури потребує кількох технологій і процесів, які будуть продиктовані моделями розгортання, конфіденційністю даних, що зберігаються, і нормативними вимогами. Лише застосовуючи стратегію поглибленого захисту та застосовуючи такі методи, як автоматичне оновлення операційної системи, безпечне кодування та моніторинг активності, ви можете зменшити вплив зовнішніх загроз.

Забезпечення доступності та відновлюваності

Одним із ключових компонентів архітектури хмарної безпеки, який повинен мати кожне розгортання, є план аварійного відновлення. Його необхідно мати на випадок збою вашої хмарної інфраструктури або чогось ще більш руйнівного, наприклад, атаки програм-вимагачів. Архітектура має включає в себе підтримку будь-яких резервних копій, які знадобляться для відновлення повної робочої потужності. Іншим аспектом хмарної архітектури безпеки, який не можна ігнорувати, є стійкість. Дехто може вважати, що відмовостійкість зосереджена навколо розробки архітектури, але насправді рівень інфраструктури, мережа та дані також повинні розглядатися як частина рівняння.

Централізоване керування компонентами

Це інтеграція централізованого метода та засоба контролю величезної

кількості пов’язаних із безпекою даних із повного набору інструментів, розгорнутих у хмарній інфраструктурі. Це допоможе забезпечити комплексне уявлення про стан безпеки хмари, що особливо важливо в багатохмарних сценаріях, де брокери хмарних послуг часто використовуються для централізації та інтеграції всього керування хмарою в одному місці. Для менш складних хмарних середовищ можна використовувати єдиний продукт або платформу, які можна інтегрувати в усі середовища постачальників для забезпечення контролю політики безпеки та керування доступом незалежно від базової хмарної інфраструктури.

Масштабованість та адаптивність

Перш ніж будувати свою хмарну архітектуру безпеки, важливо зрозуміти порогові значення, які необхідно встановити, щоб можна було проектувати в правильному горизонтальному чи вертикальному розширенні. Горизонтальне масштабування стосується надання додаткових серверів для задоволення потреб бізнесу, часто розподіляючи навантаження між серверами, щоб обмежити кількість запитів, які окремий сервер отримує одночасно. Вертикальне масштабування — це, по суті, зміна розміру сервера без зміни коду. Можна збільшити потужність існуючого обладнання або програмного забезпечення, просто додавши ресурси.

Система нотифікації – сповіщень

Навіть гарно спланована система може розвалитись через невірно налаштовану систему сповіщень. Те, як усі компоненти хмари взаємодіють з кожним користувачем, має вирішальне значення для розуміння того, що відбувається у вашому хмарному середовищі. Хмарні та інфраструктурні події, створені за допомогою розгорнутих інструментів безпеки, а також журнали з переліком подій програм і користувачів, відіграватимуть важливу роль у процесі виявлення, якщо в майбутньому виникне подія безпеки або операційна проблема.

Підбір правильного сховища для розгортання хмарної системи

У хмарі доступно багато різних типів сховищ, і важливо розуміти кожен тип і вибрати ті, які найкраще підходять для вашого розгортання. Кожен варіант зберігання, ймовірно, матиме власні унікальні параметри безпеки. Вибраний тип має брати до уваги класифікацію даних вашої організації та політику безпеки даних, перш ніж зупинитися на певному дизайні безпеки зберігання.

Централізація, стандартизація та автоматизація (CSA)

Централізація, стандартизація та автоматизація (CSA) є одним із останніх елементів, на які слід звернути увагу при розробці та архітектурі хмарної безпеки. Термін «централізація» в цьому контексті означає, що коли ви обираєте інструменти та хмарні служби, ви хочете, щоб вони могли інтегруватися в єдину інформаційну панель, щоб забезпечити видимість для тих, хто керує хмарними ресурсами. У багатьох хмарних розгортаннях з часом починають накопичуватися численні інструменти керування, інформаційні панелі та інтерфейси. Одним із потенційних рішень цієї проблеми є використання продуктів одних і тих же постачальників у якомога більшій кількості хмарних середовищ.

Якщо автоматизація є основною ідеєю DevOps, буде логічним сказати, що

DevSecOps також керується цією концепцією. Запуск хмарних інструментів безпеки вручну не є стійким рішенням. Необхідність автоматизації засобів контролю безпеки (разом із оркестровкою) може значною мірою зменшити тягар захисту цих середовищ.

Перелік посилань:
1. Cyber Risk // Without a Solid Cloud Security Architecture, Overall Strategy Weakens // липень 12б 2021. URL: https://www.kroll.com/en/insights/publications/cyber/cloud-computing-security-architecture-strategy
2. Wealth management // Confused about the Cloud? // жовтень 11, 2022. URL: https://www.ic3.gov/media/2019/190910.aspx
3. Cesar Bravo. Mastering Defensive Security: Effective techniques to secure your Windows, Linux, IoT, and cloud infrastructure / by Cesar Bravo [Електронний ресурс] – Режим доступу: https://ru.b-ok.xyz/book/18663733/00a8df

Макеєв Микола Броніславович,
Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна.

ФАЄРВОЛИ ЯК ОСНОВНИЙ ЕЛЕМЕНТ ЗАХИСТУ

Кібернетичні загрози є невід’ємною частиною інформаційних технологій. Для протидії цим загрозам використовують великий перелік різних засобів та методів, але основним є брандмауер. Брандмауер є першим пристроєм фільтрації трафіку на вході до локальної мережі та границях двох мереж. Брандмауер є невід’ємним та необхідним програмно-апаратним рішенням для забезпеченням необхідного рівня безпеки у мережі.

Ключові слова: Брандмауер, кіберзагрози, моніторинг

Мережева інфраструктура організації являє собою набір всіх програмних та апаратних ресурсів мережі організації. Для безпечення її безпеки необхідно формування комплексної захисту, яка спроможна ефективно забезпечувати захист від різномамітних загроз. Одним з ключових елементів цієї системи є брандмауер.

Брандмауер — це пристрій безпеки мережі, який відстежує та фільтрує вхідний і вихідний мережевий трафік на основі попередньо встановлених політик безпеки організації.Брандмауер виконує наступні функції[1]:

-Обмеження доступу до інформації всередені мережі;

-Попередження витоків інформації;

-Впровадження політики безпеки інформації організації;

-Аудит, через записи журналу моніторингу.

Брандмауери можна класифікувати за різними категоріями, проте самими найпоширенішими факторами розподілення виспають їх архітектура та функціонал.

За архітектурою вони поділяються на програмні та апаратні. Апаратний брандмауер це спеціалний фізичний пристрій який знаходиться між шлюзом та хостами в мережі. Програмний брандмаер це просто програма встановлена на хості, яка фільтрує вхідний та вихідний трафік виключно для цього хосту.

За функціоналом брандмауери поділяють на[1]:

- Фільтруючий пакети брандмауер;

- Сесіонний браундмауер;
- Брандмауер прикладного рівня;
- SMLI браундмаер;
- Брандмаер наступного покоління;
- Загрозо-орієнтований бранндмауер наступного покоління;
- NAT браундмаер:
- Хмарний браундмаер;
- UTM браундмаер.

Вибір брандмауера для організації базується на данних по кіберзагрозам, моделі загроз та моделі порушника[2]. Різний функціонал та архітектура брандамуера дозволяє реалізовувати різні політики безпеки та забезпечувати захист від відповідних загроз. Багато реалізацій брандмауера включають функції різних типів брандмауерів, тому вибір типу рідко є ключовою проблемою Наприклад, брендмауери наступного покоління можуть включати нові функції, а також деякі з них від брандмауерів фільтрації пакетів, сесіонних браундмауерів або SMLI браундмаерів. Вибір ідеального брандмауера починається з розуміння архітектури та функцій приватної мережі, що захищається, але також вимагає розуміння різних типів брандмауерів і політик брандмауера, які є найбільш ефективними для організації.

Можна зробити висновок, що брандмауер є невід'ємним та необхідним рішенням для сучасної мережевої інфраструктури. Незважаючи на еволюцію загроз, дане програмно-апаратне рішення еволюціонує разом з ними та на даний час все ще є актуальним.

Перелік посилань:

1. Kanneth I. Network Firewalls [Електронний ресурс] / Ingham Kanneth – Режим доступу до ресурсу: https://www.researchgate.net/publication/228394375_Network_Firewalls.
2. Choosing the Right Firewall For Your Organization: A Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.cbtnuggets.com/blog/certifications/security/choosing-the-right-firewall-for-your-organization-a-guide.

Макеєв Микола Броніславович,
студент групи БСДМ-61, ННЗІ ДУТ, Київ, Україна.

ОСНОВНІ ЕЛЕМЕНТИ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЯК ОСНОВА СУЧАСНОЇ БЕЗПЕКИ

Знання основних елементів захисту мережевої інфраструктури є необхідним знанням для правильної побудови надійної та безпечної мережі. Комплекс з цих елементів, є необхідною складовою для роботи в умовах сучасних кібернетичних загроз. При розробці плану мережі потрібно орієнтуватись на базові елементи захисту цієї мережі, основні загрози нашого сьогодення та виходити з їх можливостей.

Ключові слова: мережева інфраструктура, брандмауер, VPN, IDS, IPS.

При розробці мережевої інфраструктури ключовими факторами є безпека та надійність. Щоб їх забезпечити, необхідно прийняти міри безпеки. Для цього використовують такі засоби[1]:

1) Брандмауер — це пристрій безпеки мережі, який відстежує вхідний і вихідний мережевий трафік і вирішує, чи дозволяти чи блокувати певний трафік на основі визначеного набору правил безпеки. Брандмауер може бути апаратним, програмним, програмним забезпеченням як послугою (SaaS), публічна хмара, або приватна хмара.

В основному використовуються апаратні, або програмно-апаратні засоби. В їх основі лежить програмний фаєрвол, який розгорнутий на спеціалізованій апаратній частині, або неспеціалізованій апаратній частині. Він встановлюється на границях різних мереж.

До основних типів брандмауерів входять:

- брандмауер фільтрації пакетів
- брандмауер проксі
- брандмауер наступного покоління (NGFW)
- брандмауер перевірки стану

2) Віртуальна приватна мережа (VPN)[2]: Використовуючи вдосконалені методи шифрування з'єднань між кінцевими точками, VPN може створювати безпечні канали передачі даних через Інтернет.

VPN класифікується за наступними категоріями:

- Віддалений доступ. Конфігурація хост-мережа аналогічна підключенню комп'ютера до локальної мережі;
- Site-to-site. Конфігурація "site-to-site" з'єднує дві мережі.

Ця технологія широко використовується при облаштуванні мережі, як засіб для надійного облаштування каналів зв'язку на підприємствах між віддаленими мережами.

3) Системи виявлення[2]: системи виявлення(IDS) та запобігання вторгненням(IPS) відстежують, записують, захищають і повідомляють про будь-які потенційно руйнівні дії в мережі. Ці системи виявлення вторгнень можуть спостерігати за мережею, документувати інформацію про діяльність, запроваджувати протоколи реагування та подавати вичерпні звіти з деталями своїх спостережень. Існує багато способів класифікації різновидів безпеки мережевої інфраструктури.

Даний елемент захисту мережевої інфраструктури є необхідність в умовах сучасних загроз та постійних атак на інфраструктуру.

Таким чином, коректно спланована та налаштована мережа є запорукою сучасної кібербезпеки.

Перелік посилань:

1. Doyle L. Explore 9 essential elements of network security [Електронний ресурс] / L. Doyle, C. Kology. – 2021. – Режим доступу до ресурсу: https://www.netcov.com/what-is-network-infrastructure-security/.
2. Undestanding network infrastructure security [Електронний ресурс] – Режим доступу до ресурсу: https://www.netcov.com/what-is-network-infrastructure-security/.

Бойко Владислав Олександрович
студен групи БІКС-61, КНУБА, Київ, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА ВЕБ-ДОДАТКІВ

Сьогодні наше повсякденне життя все більше залежить від використання веб-додатків, від складних продуктових систем та як рішення певних бізнес-процесів до простих програм для створення нотаток тощо. Атаки на веб-додатки можуть призвести до знищення інформації, її модифікації та загрози цілісності й конфіденційності, тому забезпечення безпеки веб-додатків є гарячою темою у сфері інформаційної безпеки.

Ключові слова: веб-додаток, ін'єкції, вразливості, скриптинг, захист.

З кожним роком відбувається розвиток нових веб-технологій, а разом і з ними зростає кількість загроз, що становлять небезпеку для ресурсів, що побудовані на даних технологіях. Якщо не зважати на переваги веб-додатків, то можна виявити, що вони викликають низку проблем із безпекою, що виникають внаслідок нехтування безпекою додатку на етапі розробки, або його безвідповідального адміністрування.

Спеціалізованих засобів захисту веб-додатків досить мало, здебільшого це завдання покладають (або сподіваються що воно буде вирішене) на розробників та адміністраторів програм, яким слід визначити функції, критично важливі для безпеки, і протестувати ці функції для перевірки правильності роботи.

При розробці веб-додатку, який буде позиціювати себе захищеним, важливо оцінити та змоделювати життєздатність загроз. Моделювання загроз - це процес, який використовується для підвищення безпеки додатків шляхом вказівки загрози та вразливості, намічаючи заходи щодо пом'якшення або усунення наслідків загрози в системі [1].

До актуальних та головних проблем, що становлять небезпеку для веб-додатку та інформації, що циркулює в ньому, можна віднести такі як:

- Ін'єкція шкідливого коду. Використовується для впровадження шкідливого коду в базу-даних, операційну систему тощо; для отримання конфіденційної інформації, доступу до ресурсів та інфраструктури додатку [2]. Види ін'єкцій: SQL, кодова, Xpath, CRLF тощо.
- Міжсайтовий скриптинг (XSS). Дана атака являє собою маніпулювання вразливим веб-ресурсом для встановлення шкідливого коду JavaScript. Може бути як пасивним (для активації необхідні маніпуляції або дії користувача, що зберігається в БД, пулі повідомлень тощо), або активним (зберігається на сервері, спрацьовує як тільки жертва відкрила сторінку).
- Використання компонентів з вразливостями. Являє собою загрозу у вигляді «Троянського коня»: використання вразливих бібліотек, фреймворків або плагінів, що призводять до Ddos-атаки, втрати інформації або її витік.
- Невірна конфігурація безпеки. Загроза являє собою помилки конфігурації, використання облікових записів по замовчуванням,

незахищенні файли або каталоги, застаріле та не актуальне ПЗ. Результатом даної загрози може бути обхід системи індетифікації, отримання конфіденційної інформаці, або доступ до керування застосунком.

Виявлення проблем з безпекою та вразливі місця необхідно виявляти, перш ніж зловмисники зможуть їх знайти та використати. Регулярний процес виявлення вразливостей протягом життєвого циклу розробки є гарантом безпеки.

Враховуючи всі загрози, що становлять небезпеку для повноцінного функціонування веб-додадку, можна виділити основні методи та засоби для досягнення безпеки, сюди відноситься:

- Запобігання ін'єкціям. Досягається за допомогою розробки комплексних методик забезпечення безпеки БД. Основним із методів комплексного захисту є параметризація запитів до БД.
- Перевірка даних. Всі дані, які отримані з веб-форм, як на стороні клієнта, так і на стороні сервера необхідно контролювати. Досягається це, при перевірці простих помилок на зразок незаповненого поля введення, на сервері за допомогою механізму перевірки даних.
- Запобігання міжсайтовому скриптингу. Даний тип захисту схожий до методу захисту від SQL ін’єкції, при динамічній генерації коду сторінку, необхідно використовувати спеціальні функції для зміни та набуття атрибутів, а також шаблонізатори.
- Перевірка та шифрування паролів. Для повного захисту даних необхідно шифрувати дані паролей за допомогою спец. алгоритмів, а також валідувати дані, що приходять з полів вводу користувача.
- Контроль процесу завантаження файлів. В даному методі захист, необхідно розробити механізм валідації файлів таких як: перейменування, зміна розширення, зміна дозволів, створення спец. Файлу який відкриває доступ тільки до вказаних типів файлів тощо.

Враховуючи вище викладене, можна сказати, що сучасні веб-додатки є перспективними технологіями, але не зважаючи на це, завжди існує вірогідність того, що додаток може втратити свою безпеку, цілісність, конфіденційність інформації, яка знаходиться в ньому. Завчасно приділена увага до безпеки, може допомогти уникнути в подальшому проблем із застосунком.

Перелік посилань:

1. Що таке моделювання загроз? Визначення з технопедії – theastrologypage [Електроний ресурс]. – режим доступу: http://surl.li/dkhqn
2. Cross Site Scripting (XSS) – OWASP [Електроний ресурс]. – режим доступу: https://owasp.org/www-community/attacks/xss/

Бовкун Валерія Борисівна
студентка групи БСДМ-63, ННІЗІ ДУТ, Київ, Україна

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ ЗА ДОПОМОГОЮ РІШЕНЬ CISCO

Цифровізація продовжує змінювати світ. Те, як живемо, працюємо, граємо та навчаємося, змінилося. Кожна організація, яка хоче надавати послуги, яких потребують клієнти та співробітники, повинна захистити свою мережу. Безпека мережі також допомагає захистити конфіденційну інформацію від атак. Зрештою, це захищає не тільки бізнес активи, а й репутацію.

Ключові слова: мережева безпека, конфіденційні дані, корпоративна мережа, контроль доступу, зловмисне програмне забезпечення, Cisco, VPN, IPS, мережева аналітика

Безпека мережі – це захист основної мережевої інфраструктури від несанкціонованого доступу, неправомірного використання або крадіжки. Це передбачає створення безпечної інфраструктури для безпечної роботи пристроїв, програм, користувачів і програм.

Безпека мережі поєднує кілька рівнів захисту на межі та в мережі. Кожен рівень безпеки мережі реалізує політики та засоби контролю. Авторизовані користувачі отримують доступ до мережевих ресурсів, але зловмисники блокуються від здійснення експлойтів і загроз.

Види мережевої безпеки [1]:

1. Брендмауер — це пристрій безпеки мережі, який відстежує вхідний і вихідний мережевий трафік і вирішує, дозволяти чи блокувати певний трафік на основі визначеного набору правил безпеки. Cisco пропонує як брандмауери, орієнтовані на загрози, так і пристрої уніфікованого керування загрозами (UTM).

2. Система запобігання вторгненням (IPS) сканує мережевий трафік, щоб активно блокувати атаки. Пристрої Secure IPS роблять це шляхом кореляції величезних обсягів глобальної інформації про загрози, щоб не тільки блокувати зловмисну діяльність, але й відстежувати розвиток підозрілих файлів і зловмисного програмного забезпечення в мережі, щоб запобігти поширенню спалахів і повторного зараження.

3. Workload security. Безпека робочого навантаження захищає робочі навантаження, що переміщуються між різними хмарними та гібридними середовищами. Ці розподілені робочі навантаження мають більші поверхні атаки, які необхідно захистити, не впливаючи на гнучкість бізнесу.

4. NetWORK security. Безпека мережі — це бачення Cisco щодо спрощення мережі, робочого навантаження та багатохмарної безпеки шляхом надання уніфікованих засобів контролю безпеки в динамічних середовищах [2].

5. SecureX — це хмарна вбудована платформа, яка поєднує портфоліо Cisco Secure і корпоративну інфраструктуру. Це дозволяє радикально скоротити час очікування та завдань, які виконує людина.

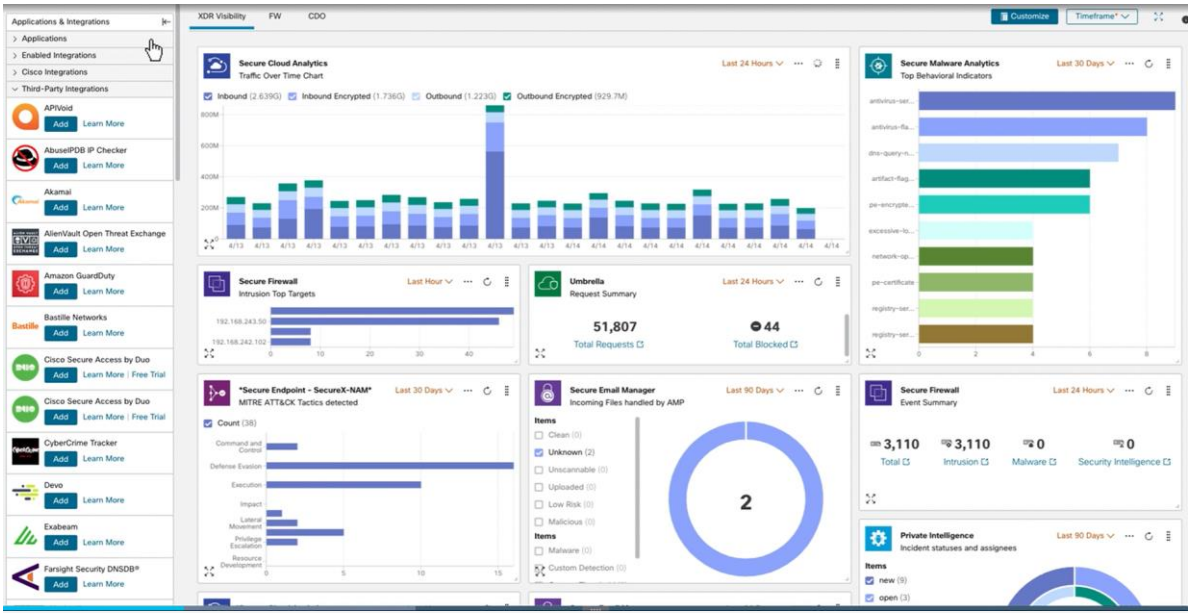


Рис. 1 - Аналітика SecureX

6. Network segmentation. Програмно визначена сегментація розміщує мережевий трафік у різні класифікації та полегшує застосування політик безпеки. В ідеалі класифікації базуються на ідентифікації кінцевої точки, а не просто на IP-адресах. Ви можете призначати права доступу на основі ролі, розташування тощо, щоб потрібний рівень доступу надавався потрібним людям, а підозрілі пристрої локалізувалися та виправлялися.

7. VPN. Віртуальна приватна мережа шифрує з'єднання від кінцевої точки до мережі, часто через Інтернет. Як правило, VPN із віддаленим доступом використовує IPsec або рівень захищених сокетів для автентифікації зв'язку між пристроєм і мережею.

8. Access control. Не кожен користувач повинен мати доступ до мережі. Щоб уникнути потенційних зловмисників, потрібно розпізнавати кожного користувача та кожен пристрій. Тоді буде змога застосувати політики безпеки. Можливо заблокувати несумісні кінцеві пристрої або надати їм лише обмежений доступ. Цей процес є контролем доступу до мережі (NAC).

9. Anti-virus and anti-malware software. Зловмисне програмне забезпечення включає віруси, хробаки, трояни, програми-вимагачі та шпигунські програми. Іноді зловмисне програмне забезпечення заражає мережу, але залишається бездіяльним протягом кількох днів або навіть тижнів. Найкращі програми захисту від зловмисного програмного забезпечення не лише сканують на наявність зловмисного програмного забезпечення під час входу, але й безперервно відстежують файли, щоб знайти аномалії, видалити зловмисне програмне забезпечення та усунути пошкодження. Будь-яке програмне забезпечення, яке використовується для ведення свого бізнесу, потребує захисту, незалежно від того, створюють його IT-спеціалісти чи купуєте. На жаль, будь-яка програма може містити діри або вразливості, які зловмисники можуть використати для проникнення у корпоративну мережу. Безпека програм охоплює апаратне забезпечення, програмне забезпечення та процеси, які

використовуються, щоб закрити ці діри.

10. Behavioral analytics. Щоб виявити ненормальну поведінку мережі, необхідно знати, як виглядає нормальна поведінка. Інструменти поведінкової аналітики автоматично розпізнають дії, які відхиляються від норми. Тоді команда безпеки зможе краще визначати ознаки компрометації, які становлять потенційну проблему, і швидко усувати загрози.

11. Хмарна безпека – це широкий набір технологій, політик і програм, які застосовуються для захисту онлайн-IP, служб, програм та інших важливих даних. Це допомагає вам краще керувати безпекою, захищаючи користувачів від загроз будь-де, де вони мають доступ до Інтернету, і захищаючи корпоративні дані та програми в хмарі [3].

12. Організації повинні переконатися, що їхні співробітники не надсилають конфіденційну інформацію за межі мережі. Технології запобігання втраті даних або DLP можуть перешкодити людям завантажувати, пересилати чи навіть друкувати критичну інформацію небезпечним способом.

13. Шлюзи електронної пошти є вектором загроз номер один для порушення безпеки. Зловмисники використовують особисту інформацію та тактику соціальної інженерії, щоб створювати складні фішингові кампанії, щоб обманювати одержувачів і надсилати їх на сайти, що розміщують шкідливі програми. Програма безпеки електронної пошти блокує вхідні атаки та контролює вихідні повідомлення, щоб запобігти втраті конфіденційних даних.

14. Security information and event management. Рішення веб-безпеки контролюватиме використання Інтернету вашим персоналом, блокуватиме веб-загрози та заборонятиме доступ до шкідливих веб-сайтів. Це захистить корпоративний веб-шлюз на сайті або в хмарі. «Веб-безпека» також стосується кроків, які вживаються для захисту корпоративного веб-сайту.

16. Бездротові мережі не такі безпечні, як дротові. Без суворих заходів безпеки встановлення бездротової локальної мережі може бути схоже на розміщення портів Ethernet скрізь, включаючи паркування. Щоб запобігти поширенню експлойтів, потрібні продукти, спеціально розроблені для захисту бездротової мережі.

Перелік посилань:

1. Cisco Secure Products and Solutions URL: https://www.cisco.com/site/us/en/products/security/index.html

2. How Cisco Firewall Threat Defense 7.0 delivers NetWORK URL: https://www.cisco.com/c/en/us/products/security/firewalls/network.html

3. What Is Cloud Security? URL: https://www.cisco.com/c/en/us/products/security/cloud-security/what-is-cloud-application-security/index.html

Нечаєв Юрій Андрійович
студент групи БІКС-2М, ФАІТ, КНУБА, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. БАЗОВІ АСПЕКТИ ЗАХИСТУ СЕРВЕРУ

З кожним роком зловмисники винаходять все більш витончені способи атак, саме тому безпека сервера має вирішальне значення для захисту будь-якої системи, яка в тому чи інакшому вигляді працює із інформацією з обмеженим доступом. Безпека сервера охоплює процеси та інструменти, які використовуються для захисту цінних даних і активів, що зберігаються на серверах організації, а також для захисту ресурсів сервера. Через конфіденційну інформацію, яку вони зберігають, сервери часто стають мішенню для кіберзлочинців, які прагнуть використати слабкі місця в системі безпеки серверів для фінансової вигоди.
Ключові слова: безпека мережі, контроль загроз, інформаційна безпека, захист серверу.

Одним із найважливіших аспектів захищеності серверу є комплексний підхід до безпеки мережі — це комбінація апаратних і програмних засобів, які працюють на рівнях 3 і 4 — мережевому та транспортному рівнях стеку OSI, основною функцією яких є керування доступом до корпоративної мережі та вбудованих у мережу ресурсів. Безпека мережі є необхідною складовою інформаційної безпеки серверу, оскільки відповідає за контроль над авторизацією користувачів, виявляє та запобігає несанкціонованому доступу в мережу, з метою завдати шкоди або скомпрометувати дані на серверах.

Елементи повної багаторівневої архітектури безпеки, яка реалізує безпеку мережі в організації, поділяються на дві загальні категорії: контроль доступу та контроль загроз [1]:

1. Управління доступом. Безпека мережі починається з контролю доступу. Якщо зловмисники отримують доступ до мережі, вони можуть стежити за трафіком і досліджувати внутрішню інфраструктуру. Після відображення інфраструктури вони можуть розпочати DDoS-атаку або вставити зловмисне корисне навантаження у вхідний трафік. Таким чином, управління доступом обмежує переміщення зловмисників по мережі.

2. Контроль загроз. Навіть за наявності управління доступом можуть виникнути загрози. Наприклад, зловмисник може скомпрометувати облікові дані співробітника, щоб отримати доступ. Таким чином, необхідний контроль загроз, який перевіряє трафік, який уже дозволений. Контроль загроз запобігає заподіянню шкоди зловмисникам у мережі. Технології контролю загроз починаються з брандмауера та балансувальника навантаження. Ці пристрої захищають мережу від атак типу DoS/DDoS. Далі IDS/IPS протидіє відомим атакам, що проходять через мережу.

Багаторівневий підхід до мережевої безпеки реалізує засоби контролю в багатьох точках мережі. Щоб забезпечити комплексний контроль доступу та контроль загроз, необхідно використати наступні ключові інструменти інформаційної безпеки:

- Брандмауер: брандмауер встановлює бар’єр між надійними та ненадійними областями мережі. Таким чином, брандмауер здійснює контроль

доступу та макросегментацію на основі IP-підмереж. Також, брандмауер може виконувати більш детальну сегментацію мережі, відому як мікросегментація.

- Балансувальник навантаження: балансувальник навантаження розподіляє навантаження на основі вхідних показників. Впроваджуючи спеціальні методи пом'якшення, балансувальник навантаження може вийти за рамки традиційного балансування навантаження, щоб забезпечити можливість поглинати певні атаки, наприклад об'ємну DDoS-атаку.

- IDS/IPS: класичний IDS/IPS розгортається за брандмауером і забезпечує аналіз протоколу та зіставлення сигнатур у різних частинах пакета даних. Аналіз протоколу — це перевірка його відповідності публічно до оголошеної специфікації протоколу. Зіставлення сигнатур запобігає відомим атакам, таким як впровадження SQL(SQL-injection).

- Пісочниця: пісочниця може емулювати середовище кінцевої системи та визначати, чи намагається об'єкт шкідливого програмного забезпечення, наприклад, виконати сканування портів.

Отже, захист серверу, напряму залежить від захищеності безпеки мережі. В свою чергу, безпека мережі – це широкий термін, який охоплює безліч технологій, пристроїв і процесів. У найпростішому вигляді це набір правил і конфігурацій, призначених для захисту цілісності, конфіденційності та доступності комп'ютерних мереж і даних за допомогою як програмних, так і апаратних технологій. Кожній організації, незалежно від розміру, галузі чи інфраструктури, потрібен певний рівень мережевих рішень безпеки, щоб захистити її від постійно зростаючого ландшафту кіберзагроз у всьому світі.

Перелік посилань:

1. NETWORK SECURITY AND NUMBER THEORY BASICS [Електронний ресурс] – Режим доступу: https://sist.sathyabama.ac.in/sist_coursematerial/uploads/SCS1316.pdf (дата звернення 30.09.2022).

Скибун Олександр Жоржович,
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

КІБЕРБЕЗПЕКА КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ В СУЧАСНИХ УМОВАХ РОЗВИТКУ ЦИФРОВОГО СУСПІЛЬТСВА

В рамках цього дослідження розглянуто вплив на рівень кібербезпеки через стрімке збільшення кількості корпоративних та державних інформаційних систем, локальних обчислювальних мереж, інформаційно-комунікаційна систем, яке пов'язане із цифровізацією та віртуалізацією діяльності на рівні усіх сфер суспільства, коли поряд із традиційною економікою розвивається цифрова та широко використовуються можливості електронних комунікацій, послуг на базі електронних комунікацій, Інтернет речей, штучний інтелект тощо. Це пов'язане з можливістю доступу широких верств населення до електронних комунікацій, глобальної мережі передачі даних, сучасного комунікаційного кінцевого обладнання. В свою чергу вказане сприяє поширенню таких нових явищ як кіберінцидент, кіберзлочин, кібератака, кібершахрайство, кіберрозвідка, кібертероризм.

Ключові слова: цифрове суспільство, кібербезпека, кіберзахист, корпоративна інформаційна система, локальні обчислювальні мережі, інформаційно-комунікаційна система.

Сучасний етап розвитку суспільства характеризується подальшим збільшенням цифрової складової в усіх сферах суспільства та суспільних відносинах, коли починає формуватися: *е-бізнес, е-економіка, телемедицина, е-освіта, е-послуги, е-розваги* тощо. На сьогодні все більше комунікацій, інформаційних та комунікативних процесів відбувається у цифровому та віртуальному просторах. Так, сучасні тренди ведення бізнесу та загальносвітові тенденції вимагають від компаній нарощувати рівень цифровізації та віртуалізації виробничих процесів та діяльності, а саме: мати свій сайт, корпоративну пошту, сторінки у соціальних мережах та присутність компанії у пошукових системах, впроваджувати нові методи роботи: робота поза межами офісних приміщень (віддалені робочі місця), електронний документообіг (запровадження системи електронного документообігу та цифрового підпису), переведення традиційних нарад, зустрічей, консультацій, переговорів у віртуальний простір на спеціалізовані платформи (наприклад Zoom, Google Meet, Microsoft Teams). На сьогодні досить активно цифровізація та віртуалізація впроваджується у таких сферах як: медична, освітня, банківська, сфера державних послуг (державних, приватних) для населення та бізнесу тощо.

Так, у рамках медичної реформи створено та впроваджується у використання медична інформаційна система eHealth в якій «щодня через сайт helsi.me понад 210 000 пацієнтів записуються на прийом до лікаря», при цьому сама «система підключена до eHealth та надає функціонал для участі в реформі», якою «користуються понад 1 100 закладів охорони здоров'я, 21 000 лікарів по всій Україні» [1]. Тобто, подальший розвиток вказаного проєкту з побудови медичної інформаційної системи буде включати у себе значні масиви інформації, що є досить чутливою для пацієнтів, а саме: персональні дані, історії хвороб, результати аналізів та тестів, а також багато інформації щодо медичних працівників, медичних закладів, закупівель медичного обладнання, послуг, ліків тощо. Додатково розширюється перелік послуг у цій системі, наприклад, запроваджено використання електронного лікарняного та видача ліків за електронними рецептами.

Впродовж останніх заклади освіти масово почали переходити на нові види, технології та інструменти надання освітніх послуг для можливості продовження навчання у дистанційному онлайн форматі, а тому виникла потреба у побудові корпоративних мереж, інформаційно-комунікаційних систем, локальних обчислювальних мереж, створенні та наповненні сайтів, ведення комунікацій у соціальних мережах, запровадженні цифрових форм дистанційної онлайн освіти з використанням можливостей Zoom, Google Meet, Microsoft Teams, а також спеціалізованих сервісів CLASSDOJO, GOOGLE CLASSROOM, DING TALK. Крім того проходження зовнішнього незалежного оцінювання також потребує створення електронного кабінету через який відбуваються усі комунікації.

У сучасних умовах досить динамічно розвивається цифрова та віртуальна складові банківської сфери, коли до масового переведення отримання заробітної плати, пенсій, стипендії та інших виплат на карточку додається мобільний банкінг, віртуальні банківські карти, що сприяє розвитку Інтернет торгівлі на

рівні великих компаній (ROZETKA) та на рівні приватних оголошень (OLX). Також до цих проектів долучаються компанії, які здійснюють доставку товарів (Нова Пошта, Укрпошта разом із компаніями, які здійснюють термінову доставку до «дверей» замовника (Glovo). Крім того, сьогодні є можливість розрахуватися карточкою або додатком з мобільного телефону у переважній більшості магазинів, а також зняти готівку на касі.

Постійно зростає кількість користувачів соціальних мереж та соціальних медіа, де зосереджуються величезні масиви персональних даних та приватної інформації (Twitter, Facebook, Instagram), а також у месенджерах (Telegram, WhatsApp, Viber).

Також необхідно звернути увагу на доволі вдалий проєкт цифровізації та інформатизації, який було започатковано в Україні – це «ДІЯ», де надаються адміністративні послуги за такими напрямами: «єробота; пенсії, пільги та допомога; сім'я; ліцензії та дозволи; безпека та правопорядок; транспорт; земля, будівництво, нерухомість; довідки та витяги; навколишнє середовище; здоров'я; документи та громадянство; підприємництво» (https://diia.gov.ua/). Крім цього, багато державних послуг надається через Центри надання адміністративних послуг (https://www.cnaprv.gov.ua/).

При всьому позитивізмі щодо результатів широкого впровадження у повсякденне життя великої кількості нових послуг та можливостей, які відкриваються для населення/споживачів у рамках формування цифрового суспільства та цифрової держави виникає і негативна сторона, а саме: перехід злочинів та шахраїв у цифровий простір, які також пристосовуються до нових цифрових та віртуальних реалій. На сьогодні вже стало буденними такі явища як: кіберінцидент, кіберзлочин, кібератака, кібершахраї, кіберрозвідка, кібертероризм тощо. В таких умовах зростають вимоги до рівнів комп'ютерної, ІТ, цифрової грамотності як населення, так і спеціалістів, які працюють із базами даних у корпоративних інформаційних систем, локальних обчислювальних мережах та інформаційно-комунікаційних системах компаній і корпорацій приватного та державного секторів. При цьому досить гостро постає питання щодо кіберзпеки та кібергігієни, адже, як показує практика, людський фактор дуже часто стає причиною масштабних кіберінцидентів, які впливають на сталість та стійкість функціонування корпоративних мереж (електронних інформаційних ресурсів), адже при цьому «мова йде не тільки про запобігання витоку корпоративної інформації, зниження обсягів паразитного трафіку і відбитті атак на ресурси компанії, але і про оптимізацію роботи системи в цілому» [2]. Ось чому головним завданням, яке постає, є створення умов для набуття громадянами та спеціалістами високого рівня компетентностей з питань кібергігієни та кіберзахисту, оскільки подальший розвиток суспільства, техніки та технологій буде тільки збільшувати рівень цифрового та віртуального просторів.

Оскільки «об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації», а тому головним завданням, яке ставиться перед відповідними підрозділами та

спеціалістами із кіберзахисту є «забезпечення безпеки (захищеності) електронних інформаційних ресурсів» [3]. Так, положеннями Закону України «Про основні засади забезпечення кібербезпеки України» «кібербезпека» визначається як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі», а «кіберзахист» як «сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [3].

З огляду на вищевказане питання кібербезпеки та кіберзахисту набувають домінуючого становища в сучасній системі факторів, що визначають стійкість та сталість функціонування корпоративних інформаційних систем (корпоративні мережі, інформаційно-комунікаційні системи, локальні обчислювальні мережі тощо) як на рівні приватного бізнесу, так і на державному рівні.

Перелік посилань.

1. Мобільний додаток медичного сервісу Helsi https://www.ukrinform.ua/rubric-society/3147788-medicnij-servis-helsi-zapustiv-mobilnij-dodatok.html
2. Мехед Д., Ткач Ю., Базилевич В., Гур'єв В., Усов Я. Аналіз вразливостей корпоративних інформаційних систем. ЗАХИСТ ІНФОРМАЦІЇ, Том 20 № 1 (2018). https://jrnl.nau.edu.ua/index.php/ZI/article/view/12453,
3. Про основні засади забезпечення кібербезпеки України : закон України від 5 жовтня 2017 року № 2163-VIII / Голос України від 09.11.2017 – № 208.

Журавель Вячеслав Олександрович,
студент групи БСДМ-61, ННЗІ ДУТ, Київ, Україна

ПОРІВНЯННЯ РІЗНОВИДІВ МІЖМЕРЕЖЕВИХ ЕКРАНІВ ДЛЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ТА КІНЦЕВИХ ПРИСТРОЇВ

Міжмережевий екран — це один з різновидів захисту та організації мережі та зв'язку між пристроями. Правильно налаштований міжмережевий екран — це перший та важливий крок до безпеки обладнання та запобіганню зовнішніх та деяких можливих внутрішніх атак.

Ключові слова: Брандмауер, міжмережевий екран, netfilter

При побудові корпоративної мережі одним з важливих кроків буде правильне налаштування міжмережевого екрану — физичних пристроїв чи програмного забезпечення, що виконує роль розмежування доступу пристроїв до спілкування між собою через мережу (допуск, відмова, форвардинг), та в деяких вападках шифрування мережевого трафіку, згідно до певних заданих налаштувань.

Вони можуть використовуватись як для захисту окремих кінцевих пристроїв (host-based firewall), так і для захисту усієї мережі та певних її частин (network firewall).

Фаєрволи існують на трьох мережевих рівнях, мають два типи фільтрації, та можуть використовуватись для різних масштабів мережі, як було описано вище.

Порівняння міжмережевих екранів за мережевими рівнями:

- Мережевий рівень — на даному рівні захист забезпечується екрануючим маршрутизатором. В цьому випадку фільтрація пакетів буде відбуватися на мережевому та транспортному рівнях.

- Прикладний рівень (проксі-сервер) — популярний в сучасному світі мереж тип фаєрволу що забезпечує фільтрацію трафіку на прикладному рівні, дозволяючи більш гнучко налаштовувати та контролювати пропуск трафіку.

- Рівень з'єднання — схожий на прикладний рівень метод захисту, але навідміну від нього потребує спеціального налаштування під кожну мережеву службу та сервіс (HTTP, FTP, тощо).

За масштабами захисту вони поділяються на фаєрволли захисту кінцевих пристроїв та мережі:

Використання міжмережевого екрану захисту для мережі частіше за все виконує роль шлюзу мережі. Забеспечення подібного захисту виконується за допомогою ASIC-accelerated та PC-based пристроїв.

ASIC-accelerated фаєрволи фільтрують трафік на апаратному рівні, через що такі пристрої іноді можуть коштувати багато, як для невеликої компанії, але дане рішення є більш ефективним зі сторони швидкодії та обслуговування великих об'ємів трафіку.

Для компаній менших розмірів більше може підійти використання PC-based фаєрволів, що можуть бути як appliances, так і базуватися на дистрибутивах для звичайних комп'ютерів.

Appliances пристрої у якості переваг можуть відмічати те що потребують значно менших зусиль для налаштування, аппаратне забезпечення буде повністю підтримуватися программним забезпеченням фаєрволу, а також зазвичай мають більшу кількість мережевих портів.

PC-based пристрої натомість можуть бути значно дешевшими рішеннями, що використовують у більшості аналогічне програмне забепечення та можуть бути встановленні як в пристрої настільного формфактору, так і на серверне обладнання для встановлення в серверні шкафи. В даному випадку при налаштуванні буде відомо повні характеристики пристрою та буде більша гнучкість при налаштуванні.

Фаєрволи для end-point пристроїв можуть мати такі ж фаєрволи як і у PC-based пристроїв (у більшості випадків при використанні netfilter у якості PC-based фаєрволу), так і інші, що більш направлені на захист саме кінцевих пристроїв. Прикладом таких фаєрволів може бути брандмауер Windows чи вбудовані в антивірус фаєрволи такі як ZoneAlarm Next Gen.

За типами фільтрації їх поділяють на stateless та stateful:

- stateless фільтрація — фільтрація на основі статичних правил;

- stateful фільтрація — фільтрація на основі аналізу з'єднань та контекстної фільтрації. Даний тип фільтрації складніший в налаштуванні, але більш

ефективний, ніж stateless.

Перелік посилань:
Firewalls — немного теории для начинающих или что надо знать перед покупкой - Режим доступу до ресурсу: https://habr.com/post/130090/
Мережевий екран - https://uk.wikipedia.org/wiki/Мережевий_екран

Бугай Олексій Олегович
студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

ПРОБЛЕМАТИКА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРОМИСЛОВИХ МЕРЕЖ IOT

Інтернет **речей (IoT)** швидко змінює технологічний ландшафт. Підприємства в усьому світі використовують IoT для отримання таких переваг, як безперебійна співпраця, доступ до вичерпних даних і здатність приймати більш сильні бізнес-рішення на основі розуміння, отриманого з значних даних.

Через експоненційне зростання кількості пристроїв Інтернету речей, збільшення кількості конфіденційних даних, які ці пристрої обробляють, і їх здатність працювати з мінімальним втручанням людини, двері залишаються широко відкритими для високих ризиків кібербезпеки. IT-фахівці вважають, що близько 60% пристроїв IoT є вразливими до атак середнього або високого рівня.

Ключові слова: IoT, конфіденційні дані, корпоративна мережа, контроль доступу, зловмисне програмне забезпечення, ботнет

Екосистема IoT складається з численних взаємопов'язаних пристроїв, побудованих з унікальними датчиками, які збирають, обмінюються, обробляють, діють і зберігають дані. Це створює зростаючий ризик для користувачів Інтернету речей, оскільки хакери можуть використати вразливість одного пристрою в екосистемі та потенційно отримати «чорний» доступ до всієї мережі вашого бізнесу та сіяти хаос.

5 ризиків, пов'язаних з Інтернетом речей:

1. Відсутність належного контролю безпеки в більшості пристроїв Інтернету речей. Незважаючи на те, що в програмному забезпеченні пристроїв Інтернету речей регулярно з'являється кілька недоліків, більшість пристроїв Інтернету речей не мають можливості виправляти останні оновлення безпеки. Як наслідок, пристрої нескінченно піддаються зростаючим ризикам безпеки.

У багатьох системах операційної технології відсутні вузлові точки фільтрації, такі як брандмауери або ACL маршрутизатора, що робить стандартну тактику відновлення мережі неефективною, коли йдеться про запобігання поширенню зловмисного програмного забезпечення. Насправді це може спровокувати критичні збої або збої в інфраструктурі. Більшість пристроїв IoT навіть не мають базових систем шифрування для захисту даних під час передачі та зберігання. Фактично, понад 95% усього трафіку пристроїв IoT є незашифрованим [1]

2. Загроза для захисту конфіденційних даних Датчики на пристроях IoT збирають (можливо зберігають і обмінюються)

величезні обсяги конфіденційних даних без вашого відома чи явної згоди. Наприклад, пристрій IoT здатний збирати дані.

3. Вразливі паролі за замовчуванням кіберзлочинцям легко використовувати жорстко закодовані та вбудовані облікові дані для входу в бізнес-мережу. Коли цілий рядок пристроїв IoT має однакові облікові дані (наприклад, ім'я користувача: admin і пароль: admin), це слугує відкритим запрошенням для хакерів.

4. Неможливість навчити кожного користувача безпеці Інтернету речей. Регулярне навчання з питань безпеки довело свою ефективність у значному зниженні ймовірності та впливу кібератак. Однак підприємства не можуть використовувати цей інструмент для навчання користувачів функціональності Інтернету речей і пов'язаним із цим ризикам через відсутність широких універсальних знань і обізнаності щодо Інтернету речей на рівні користувача.

5. Вроджена вразливість до кібератак. Кіберзлочинець може використати незахищений пристрій IoT. Приблизно 72% організацій зазнали збільшення кількості інцидентів із безпекою кінцевих точок та Інтернету речей минулого року, а 56% організацій очікують компромісу через атаку, спричинену кінцевою точкою чи Інтернетом речей, протягом наступних 12 місяців.

Ось список найпоширеніших шляхів, якими може скористатися хакер [2]:

- Атаки ботнетів: під час атаки хакери використовують ботнети, сукупність підключених до Інтернету пристроїв, заражених шкідливим програмним забезпеченням, для здійснення таких дій, як витік облікових даних, несанкціонований доступ, крадіжка даних і DDoS-атаки.
- Відмова в обслуговуванні/розподілена відмова в обслуговуванні (DoS і DDoS): під час атак DoS або DDoS хакери можуть наповнювати системи бізнесу кількома запитами даних, спричиняючи їх уповільнення, збій або навіть завершення роботи.
- Зловмисне програмне забезпечення: атаки зловмисного програмного забезпечення на екосистему IoT вашого бізнесу можуть виявитися фатальними. Всю мережу пристроїв IoT можна зламати та перетворити на ботнети, які діють за командами хакерів.
- Пасивне прослуховування телефонних розмов/атаки типу «людина посередині» (MITM): такі атаки включають несанкціоновану організацію, яка проникає в мережу вашої компанії та поводиться як інсайдер, що ставить безцінні дані компанії під серйозну небезпеку.
- Ін'єкція мови структурованих запитів (ін'єкція SQL): метод, який може знищити базу даних, ін'єкція SQL передбачає введення шкідливого коду в оператори SQL.
- Wardriving атаки: щоб здійснити wardriving атаку, хакер використовує технологію для ідентифікації незахищених бездротових мереж (у цьому випадку мережеві пристрої IoT підключені).

- Експлойти нульового дня: уразливість нульового дня — це невиявлена вразливість у програмному або апаратному забезпеченні, яка може спричинити серйозні проблеми, якщо нею скористається хакер.

Вищезазначені ризики не повинні повністю перешкоджати використовувати технологію Інтернету речей у своєму бізнесі. Можливо отримати цінні переваги цієї технології за допомогою належної інформації та впровадження найкращих практик і стратегій безпеки, які допоможуть подолати та уникнути ризиків, пов'язаних із Інтернетом речей. Деякі кроки в правильному напрямку включають ретельну оцінку ризиків (стосовно IoT), автоматизоване та регулярне керування виправленнями, керування політикою безпеки як для внутрішніх систем, так і для сторонніх систем тощо.

Перелік посилань:

1. Syed Rizvi PhD, Ryan Pipetti, Nicholas McIntyre, Jonathan Todd, Iyonna WilliamsThreat model for securing internet of things (IoT) network at device-level URL: https://www.sciencedirect.com/science/article/abs/pii/S2542660520300731
2. Jessica Lulka, Top 5 IoT security threats and risks to prioritize URL: https://www.techtarget.com/iotagenda/tip/5 IoT-security-threats-to-prioritize

Бородань Владислав Володимирович
студент групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

ОСОБЛИВОСТІ ВИКОРИСТАННЯ CISCO SAFE ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ ВІД КІБЕРАТАК

Сьогодні такі атаки, як фішинг, програми-вимагачі та мережеві загрози, стали звичним явищем для функціонування корпоративних мереж. Жодна компанія на сучасному ринку, а також жоден продукт, який виходить на ринок, не може бути 100% застрахованим від ризиків та вразливостей. Потрібен архітектурний підхід, який буде спроможним охопити весь спектр складових компонентів — від кінцевих користувачів до мережевих пристроїв та програм. Будь-які дані в організації передаються з офісів, віддалених вузлів до центрів обробки даних у хмару. Коли зловмисники порушують мережу, наявність захисту від інформаційних загроз, яка допоможе адекватно реагувати, мінімізувати вплив атаки, або зовсім знешкодити, є головною для організацій та установ.

Технології, які використовують організації, частіше за все представлені десятками продуктів, які не сумісні між собою, та призводять до все більшого кола проблем. В свою чергу, це збільшує площу атаки та, як результат, ускладнює захист. Зловмисники використовують цю вразливість для розробки та впровадження все нових, складних загроз. Тому галузь інформаційної безпеки потребує ресурсів та реалізацій, які були б здатні спростити цю актуальну проблему.

Рішення має бути комплексним, надійним і стосуватися не лише IT продуктів, які використовуватиме компанія, а й зосередитися на загрозах для актуальних вимог бізнесу [1, с.212]. Рішення Cisco SAFE відповідає цій потребі.

Модель включає: сучасні методи безпеки, архітектурні рішення та лабораторно перевірені проекти, які стосуються критичних питань безпеки. Вони

були розгорнуті, протестовані, і задокументовані [2, с.11].

Cisco SAFE містить:

- деталізовані випадки, що ілюструють мережу, яку можуть атакувати зловмисники;
- можливості безпеки, зіставлені з поширеними загрозами;
- еталонні архітектурні рішення, які логічно можуть бути впровадженні в безпеку організації чи установи;
- проекти з використанням еталонних архітектурних рішень для загальних сценаріїв розгортання та рішень Cisco SAFE.

Модель безпеки Cisco SAFE здатна бути переналаштованою під вимоги компанії, які є найбільш актуальними. Використовуючи увесь наявний інструментарій Cisco SAFE, компанії можуть аналізувати загрози та ризики, та обирати саме те рішення, яке здатне захистити бізнес в режимі реального часу[3, с.22].

Перелік посилань:

1. Chris Carthern, William Wilson, Richard Bedwell, Noel Rivera. Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA / Apress. 2015. 856 p.
2. Firepower Management Center Configuration Guide. [Електронний ресурс] - Режим доступу: http://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/ fpmc-config-guide-v601.html
3. Cisco Firepower Threat Defense Quick Start Guide for the ASA. [Електронний ресурс] - Режим доступу: http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ ftd-55xx-X-qsg.html

Цуранов Микита Олександрович
студент групи БСДМ-62, ННІЗІ ДУТ, Київ Україна

ЗАХИСТ КІНЦЕВИХ ПРИСТРОЇВ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ

Корпоративна мережа це в першу чергу простої які до неї підключаются – кінцеві пристрої. Кінцевими пристроями є комп'ютери співробітників, мобільні девайси, принтери, сканери і тд. Усі ці пристрої приносят користь компанії виконуючи свою роботу. Також кінцеві пристрої так чи інакше мають доступ до певної інформації та певних ресурсів компанії що може стати проблемою якщо до кінцевого пристрою зловмисник отримає доступ.

Ключові слова: захист корпоративної мережі, захист кінцевих пристроїв, кінцеві пристрої корпоративної мережі

Кінцеві пристрої є дуже привабливою цілю для хакерів та кіберзлочинців. Ком'ютери працівників мають доступ до чутливої інформації компанії, що є кінцевою метою зловмисників. До кінцевого пристрою легше отримати доступ. Першою причиною є те, що компанії не приділяють увагу захисту кінцевих пристроїв. Друге це те, що користувачі кінцевих пристроїв здебільшою мірою не дуже обізнані з небезпек інтернет мереж. Тому зловмисникам легше отримати доступ до чутливої інформації через кінцевий пристрій ніж спробувати зламати захищені ресурси підприємства.

Захист кінцевих пристроїв корпоративної мережі це набір певних

інструментів та практик. Інструменти захисту кінцевих пристроїв можуть бути:

- Сканер вразливостей кінцевих пристроїв;
- Сканер встановлених програм користувачів;
- Пісочниця для перевірки підозрілих файлів;
- Постійний зв’язок з кінцевим пристроєм;
- Захист від програм-вимогачів;
- Веб-фільтрація та DNS-фільтрація;
- AntiVirus/IPS.

Кращими практиками щодо захисту кінцевих пристроїв є:

- Недовіра усім кінцевим пристроям мережі. Тобто вважати, що кожен пристрії є загрозою корпоративній мережі;
- Використання захищенних протоколів підключення для усіх пристроїв;
- Чітке розділення прав доступу;

Сканер вразливостей дозволяє мати актульний статус кожного кінцевого пристрою. Це допоможе зрозуміти загальний стан інфраструктури та вразливостей які можуть використати зловмисники. Також важливим є змога усувати ці вразливості якнайшвидше.

Сканер встановлених програм дозволяє команді безпеки дозволяти чи забороняти ті чи інші програми які також можуть бути використані зловмисником. Стороні програми можуть бути використані для проникнення у систему або для ескалації привилегій.

Пісочниця – інструмент для безпечного запуску виконуємих файлів та перевірки їх поведінки. Це дозволяє отримати швидкий вердикт щодо файлу – безпечний або зловмисний.

Постійний зв’язок з кінцевим пристроєм – це інструмент для швидкого реагування на подію зараження кінцевого пристрою. Постійний зв’язок дозволяю одразу додати пристрій в карантин, щоб обмежити доступ до критично важливих ресурсів мережі.

Захист від програм вимогачів - цей інструмент дозволяє постійно сканувати систему та підозрілі файли на програми які можуть зашифровати файлову систему кінцевого пристрою та обмежити його використання(кінцевого пристрою).

Веб-фільтрація та DNS-фільтрація – такі інструменти дають змогу фільтрувати до яких категорій сайтів буде мати користувач, по-друге це захист від веб-експлойтів там веб-загроз. DNS-фільтрація також дозволяє обмежувати доступ до певних категорій DNS, але найважливішим є моніторинг доступу до командних серверів зловмисників.

AntiVirus/IPS – класичні засоби захисту для запобігання вторгенню та скинуванню на відомі сигнатури вірусів.

Далі йдуть практики захисту кінцевих пристроїв, або певні організаційні або технічні методологіх забезпечення безпеки. **Недовіра усім кінцевим пристроям мережі** – це принцип який вбачає розуміння, що загроза йде з

середини мережі. Тому захист вибудовується таким чином, що захист мережі є не тільки проти зовніх чиників, а й захист від самих кінцевих пристроїв.

Використання захищенних протоколів підключення для усіх пристроїв – це шифрування кожного з'єднання як у самій мережі так і підключення які здійснюються відаленими користувачами до внутрішних ресурсів. Це зменшує ризик отримання конфіденційних даних зловмисником.

Чітке розділення прав доступу – дозволяє розмежувати групи користувачів та їх вплив на системи та ресурси компанії у разі зламі кінцевого пристрою.

Отже, захист кінцевого пристрою це не тільки інструмени запобіганню вторгненню, а також організаційні заходи та певні принципи побудови захисту. Лише комплексний підхід до забезпечення безпеки дозволить максимально мінімізувати разики так посили захист.

Перелік посилань:

1.DataSheet FortiClient 7.0
URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/forticlient.pdf

2. Enterprise Endpoint Security Demands a Defense-in-depth Strategy
URL: https://delinea.com/blog/endpoint-security-demands-a-defense-in-depth-strategy

3. What is endpoint security?
URL: https://nordlayer.com/blog/what-is-endpoint-security/

4. What is Endpoint Security & Why is it Important?
URL: https://www.beyondtrust.com/resources/glossary/endpoint-security

Кравчук Валерія Валеріївна
студентка групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

ЗАПОБІГАННЯ ФІШИНГОВИМ АТАКАМ. ЯК РОЗПІЗНАТИ ТА ЗАПОБІГТИ ФІШИНГОВИМ АТАКАМ У 2022 РОЦІ

Фішинг — один із найпоширеніших методів атаки, з якими, ймовірно, стикається кожна компанія. Він є надзвичайно прибутковим методом атаки для кіберзлочинців, оскільки щороку їх жертвами стають тисячі людей. На щастя, завдяки їхній звичайній природі шахрайства з фішингом можна уникнути, якщо знаєти, як правильно його ідентифікувати та запобігати їм.

United States Computer Emergency Readiness Team (US-CERT) (US-CERT) визначає фішинг як форму соціальної інженерії, яка використовує електронну пошту або шкідливі веб-сайти для отримання особистої інформації від особи чи компанії, видаючи себе за надійну організацію чи юридичну особу. Фішингові атаки часто використовують електронну пошту як засіб, надсилаючи повідомлення користувачам, які нібито надійшли від установи чи компанії, з якою особа веде бізнес, наприклад банківської чи фінансової установи, або веб-

служби, через яку особа має обліковий запис.

Мета фішингу — змусити одержувача виконати бажану дію зловмисника, наприклад надати облікові дані для входу чи іншу конфіденційну інформацію. Наприклад, фішинговий електронний лист, який начебто надійшов від банку, може попереджати одержувача про те, що дані його облікового запису зламано, спрямовуючи особу на веб-сайт, де її ім'я користувача та/або пароль можна скинути. Цей веб-сайт також є шахрайським, розробленим, щоб виглядати законним, але існує виключно для збору реєстраційної інформації від жертв фішингу.

Ці шахрайські веб-сайти також можуть містити зловмисний код, який виконується на локальній машині користувача, коли користувач натискає посилання з фішингового електронного листа, щоб відкрити веб-сайт.

USA.gov перераховує деякі широко поширені фішингові шахрайства, про які повідомляють агентства та корпорації, показуючи, що фішингові електронні листи можуть приймати різні форми, наприклад:

- Електронні листи від ваших знайомих, які стверджують, що опинилися в чужій країні, з проханням переказати гроші, щоб вони могли поїхати додому.
- Електронні листи, які нібито надійшли від авторитетних інформаційних організацій, які використовують популярні новини. Ці електронні листи зазвичай просять одержувачів натиснути посилання, щоб прочитати повну історію, що, у свою чергу, веде користувача на шкідливий веб-сайт.
- Електронні листи, які нібито надійшли від організацій, що містять посилання на подані скарги або прохання до одержувачів перевірити страхове покриття банківських вкладів.
- Електронні листи з погрозами завдати шкоди одержувачам, якщо не будуть виплачені суми в тисячі доларів.
- Електронні листи, які нібито є підтвердженням скарг, поданих одержувачем. Не зареєструвавши жодних скарг, одержувачі схильні натискати ці посилання, щоб дізнатися, на що посилається. Посилання та вкладення, звичайно, містять шкідливий код.

Це, звичайно, не вичерпний список. Фішингові електронні листи можуть мати будь-яку форму, що ускладнює для одержувачів фільтрацію спаму та фішингових листів від легітимних повідомлень.

Поширені типи фішингових атак на компанії.

- Видача себе за компанію

Однією з найпоширеніших форм фішингу є те, що зловмисники видають себе за ваш бренд. Зазвичай це робиться за допомогою електронної адреси, пов'язаної з доменом, дуже схожим на цільову компанію (наприклад, «first.name@amazon-support»).

- Фішинг

Цей тип схеми передбачає використання підробленої назви компанії (видання себе за іншу особу), а також ключових даних про ціль. Як і в продажах, представник знаходить ім'я, посаду та іншу персоналізацію та включає це в електронний лист із рекламою. Зловмисники знаходять ті самі моменти та використовують їх, щоб залучити більше жертв у свою пастку. Це особливо небезпечний прийом.

- Захоплення облікового запису електронної пошти

Усі члени вашої виконавчої та управлінської команди вразливі. Якщо фішинговий шахрай отримає облікові дані електронної пошти високопоставленого керівництва, цілком імовірно, що він націлиться на будь-кого, хто зможе, використовуючи цю саму електронну адресу. Потенційними цілями можуть бути: колеги, члени команди та навіть клієнти (якщо вони вже отримали цю інформацію за допомогою злому).

- Фішингові електронні листи

Подібно до афери із захопленням облікового запису електронної пошти, ця фішингова атака здійснюється електронною поштою. Різниця полягає в тому, що фішинговий шахрай використовує електронну адресу, яка нагадує законну електронну адресу, особу чи компанію. Електронний лист міститиме прохання натиснути посилання, змінити пароль, надіслати платіж, відповісти з конфіденційною інформацією або відкрити вкладений файл.

- Телефонний фішинг або голосовий фішинг

Використовуючи технологію Voice over Internet Protocol (VoIP), шахраї знову видають себе за компанії. Ця техніка також використовує інші типи фішингу, включаючи використання особистих даних про цілі та видавання себе за окремих осіб компанії (наприклад, генерального директора), щоб отримати кращий погляд на шахрайство в цілому.

Як захиститись від такого роду атак та попередити це?

Нижче наведені рекомендації від різних фахівців з безпеки крупних компаній, яким чином можна попередити фішингові атаки та як захистити співробітників та клієнтів від крадіжки даних.

Єдина помилка компаній, яка робить їх уразливими для фішингових атак, це відсутність належних інструментів і неспроможність навчити працівників їхній ролі в інформаційній безпеці.

Співробітники володіють повноваженнями та загальними знаннями, які мають вирішальне значення для успіху порушення безпеки компанії. Метою фішингу є збір конфіденційної інформації з метою використання цієї інформації для отримання доступу до захищених іншим чином даних, мереж тощо. Успіх зловмисника залежить від встановлення довіри з його жертвами. Ми живемо в епоху цифрових технологій, і збирати інформацію стало набагато простіше,

Зловмисники використовують різні методи фішингу:

– Вбудовування посилання в електронний лист, яке перенаправляє вашого співробітника на незахищений веб-сайт, який запитує конфіденційну інформацію.

– Встановлення трояна через зловмисне вкладення електронної пошти або оголошення, що дозволить зловмиснику використовувати лазівки та отримувати конфіденційну інформацію.

– Підробка адреси відправника в електронному листі, щоб виглядати як авторитетне джерело та запитувати конфіденційну інформацію.

– Спроба отримати інформацію про компанію по телефону, видаючи себе за відомого постачальника компанії або IT-відділ

Ось кілька кроків, які компанія може вжити, щоб захистити себе від фішингу.

– Навчити своїх співробітників і проводите навчальні заняття з імітаційними сценаріями фішингу.

– Встановити фільтр СПАМу, який виявляє віруси, порожні відправники тощо.

– Підтримувати всі системи в актуальному стані за допомогою останніх виправлень безпеки та оновлень.

– Встановити антивірусне рішення, запланувати оновлення сигнатур і відстежувати статус антивіруса на всьому обладнанні.

– Розробити політику безпеки, не обмежується терміном дії пароля та складністю.

– Розгорнути веб-фільтр для блокування шкідливих веб-сайтів.

– Шифрувати всю конфіденційну інформацію компанії.

– Вимагати шифрування для працівників, які працюють віддалено.

Існує кілька кроків, які компанія може вжити для захисту від фішингу. Вони повинні стежити за поточними стратегіями фішингу та підтвердити, що їх політика безпеки та рішення можуть усунути загрози в міру їх розвитку. Не менш важливо переконатися, що їхні співробітники розуміють типи атак, з якими вони можуть зіткнутися, ризики та способи їх усунення. Проінформовані співробітники та належним чином захищені системи є ключовими для захисту компанії від атак.

Новий вектор загрози, представлений тенденцією BYOD, полягає в тому, що програми на мобільних пристроях співробітників можуть отримувати доступ до їхніх адресних книг і експортувати їх на сайти в Інтернеті, відкриваючи контакти зловмисникам, які використовують їх для цілеспрямованого фішингу. Одним з важливих кроків для компаній є запобігання потенційним зловмисникам доступу до корпоративного каталогу, який містить імена, адреси електронної пошти та іншу особисту інформацію про співробітників. Рекомендується інсталювати програмне забезпечення мобільної безпеки на пристроях користувачів, яке сканує програми та запобігає доступу користувачів до корпоративних мереж, якщо вони мають програми, що порушують конфіденційність.

Іншим кроком є захист мобільних користувачів від відвідування фішингових сайтів, навіть якщо вони знаходяться в мережі Wi-Fi, яку компанія

не контролює. Ці засоби захисту необхідно виконувати на рівні мережі, оскільки фільтрування електронної пошти недостатньо. Атаки можуть здійснюватися через корпоративну електронну пошту, через особисту електронну пошту користувача, яка може бути підключена до його мобільного пристрою, або через SMS-повідомлення користувачу. Користувачі мобільних пристроїв мають бути підключені через віртуальні приватні мережі (VPN) до служб, які забезпечують безпечну систему доменних імен (DNS) і чорні списки для запобігання доступу до фішингових сайтів.

Крім того, виявляється, що самі користувачі часто є найкращим каналом для виявлення, звітування та захисту від фішингових атак. Важливою практикою, яку мають застосовувати підприємства, є створення систем, де користувачі зможуть швидко й легко повідомити про фішинг-атаку, скерувати її до IT-спеціалістів, відфільтрувати та розмістити в системі, щоб IT-спеціалісти могли швидко й легко додати їх до чорних списків, захистити як внутрішніх співробітників, так і тих, хто працює віддалено або на мобільних пристроях.

Перелік посилань:

1. 10 Ways to Prevent Phishing Attacks// вересень 14, 2022. URL: https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/
2. Digital Guardian's Blog// Phishing Attack Prevention// березень 14, 2022. URL: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams
3. Digital Guardian's Blog// What is a Phishing Attack? Defining and Identifying Different Types of Phishing Attacks// вересень 11, 2018. URL: https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks

Дрось Данило Анатолійович, *студент*
Державний університет телекомунікацій, ННІЗІ,
м.Київ

ЗАПОБІГАННЯ І ПРОТИДІЯ МЕТОДАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ – ЩО ЦЕ І НАВІЩО ПОТРІБНО?

Ключові слова: соціальна інженерія, фішинг, кібербезпека, соціотехніка вішинг, фармінг.

Що ми знаємо про кібербезпеку? Кібербезпека – це набір процесів, практичних порад і технологічних рішень, які допомагають захистити критично важливі системи та мережі від кібератак. Оскільки об’єм даних збільшується й усе більше користувачів працюють і спілкуються звідусіль, кіберзлочинці розробляють складні методи, щоб отримувати доступ до ресурсів, викрадати дані, саботувати роботу компаній або вимагати гроші. Щороку кількість атак збільшується, а зловмисники розробляють нові методи для уникнення виявлення. Ефективна програма з кібербезпеки включає фахівців, процеси та технологічні рішення, які разом зменшують ризик перерв у роботі компаній, фінансових втрат і підриву репутації внаслідок атак.

Одна із проблем з якою можна стикнутися у забезпеченні кібербезпеки це соціальна інженерія. Зараз докладніше це розберемо. Соціальна інженерія – це мистецтво маніпулювання людьми через виконання дій, або розголошення конфіденційної інформації іншим способом, ніж як через засоби технічного руйнування баз даних. Термін "соціальна інженерія" використовується для опису цілої низки низькотехнологічних підходів, розроблених шахраями для того, щоб змусити потенційну жертву повідомити особисті дані або взяти участь у діях, які можуть зробити її комп'ютер вразливим до атак. Це може відбуватися як через Інтернет, так і під час особистого контакту. Найбільш популярною схемою впливу на особу, яка використовується в соціальній інженерії є схема Шейнова, яка полягає у таких кроках: формування цілі впливу на об'єкт (1), пошук інформації про об'єкт (2), виявлення найбільш зручних цілей впливу (3), створення найбільш сприятливих умов для впливу на об'єкт (4), примус до потрібної дії (5), результат (6).

Соціальна інженерія базується на досить простих психологічних особливостях людини, таки як: принцип зворотності («ти мені – я тобі»), принцип соціальної перевірки (ви оцінюєте свою поведінку в контексті поведінки більшості), повага до авторитетів (ви будете більше довіряти лікарю та поліцейському, аніж пересічній людині). Всі ці принципи застосовуються і при здійсненні «офлайнового» шахрайства, однак мають свою специфіку під час вчинення у мережі Інтернет.

Для аналізу ефективності боротьби із соціальною інженерією як одним із проявів кіберзлочинності необхідно ознайомитися із основними способами її застосування на практиці. Так, до них можна віднести наступні:

Фішинг. Цей вид шахрайства побудований на надсиланні листа, ніби від банку чи іншою установи, в якому міститься посилання у якому необхідно ввести пароль чи іншу конфіденційну інформацію, яка необхідна шахраю. При цьому приводи для надсилання такої інформації можуть бути різними, наприклад, відновлення бази даних після її випадкової втрати.

Вішинг. Назва цього виду інтернет-шахрайства пішла від попереднього та полягає у імітування дзвінків на мобільний телефон, ніби як від банківської установи (із попередньо записаним голосом) та отриманні запиту про комунікацію із банком для підтвердження тієї чи іншої інформації. При цьому жертва отримує вимогу сказати свій пароль або іншу конфіденційну інформацію, яка необхідна для доступу до банківських рахунків.

Фармінг. Процедура полягає у перенаправленні жертви на неправдиву IP-адресу. Шахрай встановлює на комп'ютерах шкідливу програму, яка після запуску на комп'ютері забезпечує перенаправлення жертви замість шуканих нею сайтів на підроблені сайти.

Соціотехніка

Використовуючи соціотехніку, зловмисники втираються в довіру до користувачів і обманом змушують їх передавати відомості облікового запису або завантажувати шкідливе програмне забезпечення. Під час таких атак зловмисники маскуються під відомий бренд, співробітників або друзів жертви

та використовують психологічні прийоми, як-от відчуття нагальності, щоб маніпулювати людиною.

Чому кібербезпека важлива?

Сучасний світ як ніколи оснащений великою кількістю засобів зв'язку. Світову економіку формують люди, які спілкуються, перебуваючи в різних часових поясах, і отримують доступ до важливої інформації звідусіль. Кібербезпека стимулює продуктивність і впровадження інновацій, що дає користувачам змогу впевнено працювати та спілкуватись онлайн. Правильні рішення й процеси дають змогу компаніям і державним установам користуватися технологіями для покращення спілкування та надання послуг, не ризикуючи постраждати від атак.

Оскільки все більше організацій упроваджують моделі гібридної роботи, що дають робітникам змогу працювати як в офісі, так і віддалено, варто розгортати нову модель безпеки, яка захищатиме користувачів, пристрої, програми та дані, хоч де вони зберігатимуться. Принцип інфраструктури з моделлю нульової довіри полягає в тому, що більше не можна довіряти запиту на доступ, навіть якщо він надходить із внутрішньої мережі. Щоб знизити ризик, припустіть, що вас зламали, і перевіряйте всі запити на доступ. Надавайте користувачам доступ до потрібних їм ресурсів лише з мінімальними правами.

За кібербезпеку відповідають не лише фахівці з безпеки. Сьогодні робочі й особисті пристрої використовуються по черзі, а багато кібератак починаються з надсилання фішингового електронного листа працівникам. Навіть великі забезпечені ресурсами компанії стають жертвами соціотехнічних кампаній. Боротьба з кіберзлочинністю й убезпечення мережі вимагає спільних зусиль усіх працівників. Треба проводити регулярне навчання своєї команди, щоб вона могла захищати особисті пристрої та розпізнавати й зупиняти атаки. Відстежувати ефективність своїх програм, використовуючи симуляції фішингу.

У якості висновку слід зазначити, що основним недоліком у сфері запобігання негативним проявам соціальної інженерії є відсутність системної роботи щодо її виявлення та подолання, наявність лише декларативних положень у стратегіях (іншими вони і не можуть бути, що зрозуміло) та відсутність прийнятих законодавчих та підзаконних актів на їх конкретизацію та розвиток, низький рівень проінформованості населення щодо можливих загроз соціальної інженерії (варто відзначити позитивну роботу деяких банків у цій сфері), а також високу латентність злочинів у цій сфері, що унеможливлює виявлення та притягнення до відповідальності усіх винних осіб.

Перелік посилань:

1. Стаття https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/
2. Що таке кібербезпека? https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity
3. Конфіденційність та безпека https://support.skype.com/uk/faq/FA10921/shcho-take-sotsial-na-inzheneriya

Пацьора Елла Сергіївна
студентка групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

УПРАВЛІННЯ ДОСТУПОМ ДО МЕРЕЖІ В ЕРУ IOT

Широке впровадження продуктів IoT в офісах і політика роботи з дому надають нові бізнес-можливості. Але водночас вони створюють нові виклики. По-перше, практично не існує стандартизації конфігурації пристроїв для IoT. У будь-якій організації потенційно активно використовуються сотні типів пристроїв і операційних систем, багатьом із яких бракує безпеки корпоративного рівня. Крім того, з урахуванням нових політик роботи вдома, що вимагають від більшої кількості співробітників використання віртуальних приватних мереж (VPN) для безпечного підключення до офісу, труднощі з розумінням та забезпеченням належного доступу до цих пристроїв є саме тим, чому кінцеві точки залишаються головною метою кібератак.
Ключові слова: IoT, управління доступом до мережі, комп'ютерна система, кінцеві точки.

IoT розгортається для вирішення більшості сучасних проблем у багатьох областях, таких як логістика, транспорт, моніторинг забруднення, охорона здоров'я, домашня автоматизація, розумне місто, розумний офіс, управління інфраструктурою, сільське господарство, енергетика, управління корисними копалинами та ефективним використанням води [1, с. 117]. З появою бездротових сенсорних мереж, вбудованих систем, датчиків, приводів, хмарних сервісів, IoT став дуже популярним. Це започаткувало еру, коли розумні об'єкти спілкуються з іншими розумними об'єктами. Розумні пристрої збирають масу конфіденційних даних, у тому числі ідентифікаційну інформацію, вони здатні відчувати навколишнє середовище, передавати й обробляти отримані дані, а потім давати відповідь навколишньому середовищу, тому їх потрібно захищати різними законами, стандартами та правилами кібербезпеки.

Оскільки IoT і мобільні пристрої продовжують поширюватися, площа атак на підприємства стає все ширшою. Виявлено нові прогалини та вразливі місця в периметрі мережі. І в той же час експлойт нульового дня та постійні загрози стають більш витонченими у своїх стратегіях атак на кінцеві точки. Архітекторам безпеки потрібні покращені засоби управління доступом, щоб захистити пристрої та ширшу мережу від загроз і відповідати дедалі суворішим стандартам відповідності.

Управління доступу до мережі (NAC) визначається як програмне забезпечення, яке дозволяє IT-менеджерам створювати, застосовувати, керувати та оновлювати політики безпечного доступу по всьому периметру організації, приділяючи особливу увагу системам віддаленого доступу, таким як мобільні пристрої, веб-програми, кінцеві точки, які працюють за межами мережі.

На відміну від апаратного забезпечення для управління доступу до мережі, яке знаходиться в пристрої фізичної безпеки, програмне забезпечення до мережі розгортається або локально, або через загальнодоступні хмарні ресурси для економічності, масштабованості та легкого керування. Декілька факторів

зробили програмне забезпечення для управління доступу до мережі обов'язковим компонентом у захисту інформації.

Зазвичай у комп'ютерній системі управління доступу визначає, чи дозволено суб'єкту, таких як процесу, пристрою чи користувачу, виконувати операції, а саме читати, записувати чи оновлювати, на об'єкті, таких як база даних, файл або служба, на основі певних політик. Іншими словами, він керує тим, хто або що, може переглядати чи використовувати ресурси. Управління доступом, як правило, зберігає такі властивості [2, с. 17]:

- Конфіденційність: інформацію можуть переглядати авторизовані користувачі, і інформація повинна бути конфіденційною.
- Цілісність: авторизовані користувачі можуть лише переписувати інформацію, і інформація має бути захищена від підробки та зміни іншими.
- Доступність: інформація має бути доступною за запитом для використання, що стосується можливості користувача отримати доступ до ресурсу.

Основні функції програмного забезпечення для управління доступом до мережі [3]:

- Сумісність: програмне забезпечення має співіснувати та підключатися до існуючої цифрової екосистеми, включаючи апаратне забезпечення, додатки для підвищення продуктивності, програми безпеки та інфраструктуру безпеки.
- Плагін керування ідентифікацією та доступом: він має бути готовий до інтеграції з бажаним каталогом ідентифікаційних даних, отримувати правильні облікові дані, щоб дозволити або заборонити доступ.
- Гостьовий доступ: він повинен підтримувати доступ користувачів за межами безпосередньої корпоративної мережі, бажано дозволяючи обмежений доступ за часом і ретельно відстежуючи використання мережі.
- Додаткові послуги: програмне забезпечення також повинне запропонувати додаткові можливості безпеки (крім управління доступом) для подальшого зміцнення мережі за допомогою захисту від зловмисного програмного забезпечення, віртуальної приватної мережі та автоматизації.
- Управління: він повинен мати централізовану інформаційну панель для визначення політики, надання доступу та керування затвердженнями, що охоплює весь локальний пристрій, віддалену кінцеву точку та крайовий ландшафт.

Перелік посилань:

1. Sandeep Saxena, Ashok Kumar Pradhan. Internet of Things. Security and Privacy in Cyberspace. 2022. 117 pages.
2. Shantanu Pal. Internet of Things and Access Control. Sensing, Monitoring and Controlling Access in IoT-Enabled Healthcare Systems. 2021. 17 pages.
3. Top 10 Network Access Control Software Solutions in 2021 [Електронний ресурс] – Режим доступу: https://www.spiceworks.com/it-security/network-security/articles/top-10-network-access-control-software-solutions/

Тищенко Віталій Сергійович
Студент групи АІКБ-11, ННІЗІ ДУТ, Київ, Україна

АНАЛІЗ ІСНУЮЧИХ ТЕХНІК ПОШИРЕННЯ І РОЗПІЗНАВАННЯ ФЕЙКОВИХ НОВИН ТА ДЕЗІНФОРМАЦІЇ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Із розвитком технологій у сфері масової комунікації Україна і світ постають перед новими викликами. Одним із найскладніших і найпідступніших сьогодні є дезінформація.У Кодексі практики ЄС щодо протидії дезінформації вказано, що дезінформація має на меті економічні вигоди для поширювача. Тож ключовою ознакою дезінформації, яка відрізняє це явище від звичайної недостовірної інформації, є умисел на її створення. Тобто дезінформація — це неправдива, оманлива, маніпулятивна інформація, створена навмисне заради економічних, політичних або інших вигод.

Ключові слова: дезінформація, фейкові новини, масова комунікація.

Фейки та дезінформація поширюються в основному через інтернет, наприклад новинних ресурсів, ЗМІ, які належать впливовим особам, чати в месенджерах, та соціальних мережах, SMS-повідомленнях. Також варто виділити мотиви їх поширення, тобто з якою метою вони поширюються, це може бути як і фінансова вигода, репутаційна або випадковість. Основною проблемою постає швидкість їх створення та реагування на них. Нейронна мережа, яка навчена розрізняти неправдиву інформацію використовуючи різні сервіси для перевірки тексту або повідомлення або фото, дає можливість ідентифікувати походження інформації або змісту повідомлення з неправдивою інформацією, маркуючи її певним чином.

До головних особливостей дизінформації належать[1]:

- надзвичайно великий об'єм;
- неконсистентність;
- велика кількість каналів поширення;
- викривлення реальних фактів, а інколи їх повна фальсифікація.

Найпопулярнішими і найбільшими місцями в мережі є: Facebook, Instagram, Youtube, Viber та Telegram, TikTok.

В Facebook існують три основні загрози: алгоритми, боти та опитування/тести. В Viber та Telegram основну загрозу поширення дезінформації становлять анонімні новинні канали та групи, групові чати (будинку, роботи, та інше), а також деякі «інсайдери» зі «100% достовірною інформацією» про ту чи іншу подію або особу. Загроза в мережі TikTok дещо схожа з месенджерами, однак відрізняються тим, що поширення фейків дуже швидке поширення відео. В YouTube поширення відбувається через популярних блогерів, відомих особистостей, та «клікбейтні» назви. Поширення в Instagram відбувається знову ж таки через авторитет деяких відомих та публічних осіб, які поширюють фейки через особисту вигоду, або як приклад, працюють на державні органи ворожої країни посилаючи певні наративи для залякування, ввід в оману, та інше.

Велика кількість каналів поширення забезпечує можливості донесення пропаганди до користувачів з різних країн, з джерел, які ніяк не асоціюються з країною її походження. До того ж, інформація, отримана з різних джерел виглядає більш правдивою для користувача. Неконсистентність пропаганди йде всупереч класичним уявленням про ведення інформаційної війни [2], де кожне повідомлення має бути узгоджене з іншими і з загальною ідеологією.

Проте, неузгодженість окремих каналів або й окремих повідомлень пропаганди має свою перевагу: отримання інформації начебто з різних точок зору підвищує довіру до джерела інформації. Викривлення або фальсифікація реальних фактів – є одним з головних чинників, які зумовлюють ефективність такої пропаганди та складність їй протидіяти. Аналізуючи літературні джерела щодо проблематики виявлення фейкових новин на основі машинного навчання [3], можна класифікувати підходи до виявлення фейкових новин на дві великі групи: з попереднім навчанням та з самонавчанням.

Алгоритми першої групи потребують навчання та перевірки на двох окремих множинах вхідних даних, які дозволяють точно підібрати вагові коефіцієнти і забезпечують високу ефективність кінцевої системи.

Алгоритми з самонавчанням не потребують окремого етапу навчання для забезпечення результату. Вони застосовуються тоді, коли ручна класифікація вхідних даних для навчання є дуже трудомістким завданням, а також коли потрібно, щоб система могла сама підлаштовуватися при зміні умов реального середовища застосування.

На основі особливостей даних, які враховуються алгоритмами, їх можна поділити на:

- content-based: враховують текстову інформацію (тобто текст самої новини, поста в соцмережі чи твіту, описи профілів у соціальній мережі);
- social-based: враховують соціальну складову (особливості поширення поста в соцмережі та реакції користувачів на нього);
- combined: використовують обидва підходи.

FAKEDETECTOR – фреймворк з попереднім навчанням що здійснює визначення рівня довіри до самого інформаційного контенту, його автора та його теми.

Перший метод ґрунтується на твердженні, що неправдиві новини можна виявляти за кількістю та особливостями реакцій користувачів на неї. У якості алгоритму, який враховує соціальні особливості поширення фейку автори пропонують використати підхід “harmonic boolean label crowdsourcing (HC) on social signals”, або HCCB-3.

Прикладом підходу, який би об’єднував в собі використання як текстової так і соціальної складової в одному алгоритмі, є алгоритм – unsupervised framework, або UFD. Він ґрунтується на врахуванні реакції користувачів на певну новину. Вважається, що коментуючи пост, користувач таким чином висловлює свою думку про нього (правдива, на його думку, ця інформація, чи ні), а отже, ці дані можна використовувати в якості фактора при розпізнаванні фейку.

У залежності від конкретної групи, до якої належить користувач, при

аналізі інформаційного контенту його реакція враховується з певним коефіцієнтом. У якості основного алгоритму автори використовують Collapsed Gibbs Sampling, update правило якого вираховується на основі кількості реакцій користувачів з довіреної та недовіреної груп. Це дозволяє алгоритму підлаштовуватися під змінні умови застосування, проте накладає певні обмеження на наявність реакцій на дописи.

Отже, в сучасній ситуації важливо проаналізовати особливості поширення фейків та дизінформації, сучасні підходи до розпізнавання фейкових новин у соціальних мережах, найбільш перспективний підхід для ефективного виявлення неправдивої інформації, розповсюджуваної в соціальних мережах у рамках ведення інформаційної пропаганди, який полягає в комбінованому використанні двох алгоритмів, які враховують різні сторони інформаційного контенту та особливостей його поширення в соціальних мережах. Проте, роботу алгоритму в умовах інформаційної пропаганди та захисту від неправдивої інформації можна покращити, якщо сформувати базу даних з оцінками довіри до авторів дописів і враховувати її при прийнятті рішень щодо нових дописів.

Перелік посилань:

1. Paul, Christopher and Miriam Matthews, The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of September 29, 2020 [Електронний ресурс]. Режим доступу: https://www.rand.org/pubs/perspectives/PE196.html.
2. M. L. Della Vedova, E. Tacchini, S. Moret, G. Ballarin, M. DiPierro and L. de Alfaro, "Automatic Online Fake News Detection Combining Content and Social Signals," 22nd Conference of Open Innovations Association (FRUCT), Jyvaskyla, 2018. - pp. 272-279.
3. J. Zhang, B. Dong and P. S. Yu, "Fakedetector: Effective Fake News Detection with Deep Diffusive Neural Network," 2020 IEEE 36th International Conference on Data Engineering (ICDE), Dallas, TX, USA, 2020, pp. 1826-1829.

Козирєв Олексій Олексійович,
студент групи КСМ-51, ФАІТ КНУБА, Київ, Україна

ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Технічний захист інформації - це діяльність, спрямована на забезпечення безпеки незашифрованої інформації (даних) шляхом використання технічних засобів, програмних та апаратних засобів відповідно до чинного законодавства. Метою такого захисту є захист технічних даних, ноу-хау, патентної інформації, внутрішньо розроблених або придбаних методів та ліцензій. Методи та засоби технічного захисту також захищають інформацію організації про фінансові операції, кредити, контрагентів, персональні дані працівників, керівництва, клієнтів та постачальників.

Ключові слова: захист інформації, криптографія, технічний захист, шифрування.

Створення ефективної системи захисту конфіденційної інформації потребує свідомих і постійних зусиль. Процес складається з декількох етапів:

1. Ретельний аналіз доступних джерел інформації.

2. Вибір концепції інформаційної безпеки, що відповідає конкретним обставинам і характеристикам використовуваних даних.
3. Здійснення заходів захисту.
4. Розробка специфічних для компанії заходів щодо захисту даних.

Всі заходи повинні відповідати чинному законодавству, інакше можуть виникнути юридичні суперечки. У зв'язку з цим персонал служби інформаційної безпеки повинен постійно переглядати нормативні акти, вимоги та закони, щоб запобігти порушенням та не допустити втягнення компанії в судові спори. Нормативна база повинна стати основою для створення всієї системи інформаційної безпеки компанії.

Важливим кроком є вивчення ризиків та виявлення джерел небезпеки. Від цього залежить ефективність системи захисту інформації. Якщо всі потенційні загрози правильно ідентифіковані, ризик витоку даних зводиться до мінімуму. Необхідно здійснити наступні кроки :

- Скласти список всіх пристроїв, що містять конфіденційну інформацію. Також слід враховувати всі існуючі та альтернативні канали зв'язку, дротові та бездротові.
- Визначити найбільш критичні зони, обмежити доступ та створити систему контролю за пересуванням співробітників та сторонніх осіб.
- За результатами аналізу розрахувати розмір збитків та наслідки несанкціонованого доступу та шахрайського використання інформації.Скласти перелік документів та інформаційних форм, які підлягають першочерговому захисту. Визначити рівень доступу та створити список довірених користувачів.
- Створити відділ інформаційної безпеки - самостійний підрозділ, до складу якого входитимуть фахівці з безпеки, системні адміністратори та програмісти.

Основними завданнями відділу інформаційної безпеки є:

- Загальний технічний захист інформації;
- Запобігати несанкціонованому доступу та використанню конфіденційної інформації.
- Забезпечення цілісності інформаційних масивів, навіть в умовах надзвичайних ситуацій (пожежа, стихійні лиха).

Технічні методи захисту інформації повинні бути адаптовані до конкретної ситуації на підприємстві. Найбільш ефективними заходами є :

- Криптографічний захист інформації (шифрування) ;
- Використання електронних підписів для підтвердження того, що автори є довіреними користувачами.
- Резервне копіювання баз даних та операційних систем.
- Налаштування системи паролів для ідентифікації та аутентифікації співробітників.

- Моніторинг подій в інформаційній системі. Відстежування спроб входу і виходу, маніпуляцій з документами.
- Використання смарт-карт, електронних ключів у системі доступу та обмеження пересування персоналу.
- Встановлення та використання мережевих екранів (брандмауерів) в комп'ютерах.

На додаток до цих заходів має бути введена процедура моніторингу та тестування працівників з високими правами доступу. Бажано мати IT-менеджера та працівника служби безпеки в приміщенні, де обробляються конфіденційні дані.

Перелік посилань:

1. Технології захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: lekzii.pdf (wunu.edu.ua)

2. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України No125 від 8.11.2005. (Серія видань «Тимчасове положення»).

Цибенко Роман Станіславович
студент групи КСМ-51, ФАІТ КНУБА, Київ, Україна

ЗАХИСТ ЛОКАЛЬНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

Корпоративна мережа — це комунікаційна система, якою володіє та керує одна організація відповідно до правил цієї організації. Корпоративна мережа відрізняється від мережі, наприклад, Інтернет-провайдера тим, що правила призначення IP-адрес, роботи з Інтернет-ресурсами тощо єдині для всієї корпоративної мережі, а провайдер контролює лише базовий сегмент мережі, що дозволяє своїм клієнтам самостійно керувати своїми сегментами мережі, які можуть бути частиною адресного простору провайдера, а також бути прихованим механізмом трансляції мережевих адрес для однієї чи кількох адрес провайдера.

Ключові слова: система, безпека, мережа, інформація, дані, захист.

Безпека корпоративної мережі.

При розробці корпоративних мережевих систем безпеки оцінюється динаміка поля загроз та їх можливі пошкодження, а також необхідність ступеня інтенсивності використання механізмів захисту в структурі мережі для нейтралізації атак. До того ж після тестування корпоративної мережі проводиться низка превентивних заходів щодо прогнозування вірусних атак, дослідження шкідливого коду та його знищення.

Чому необхідно забезпечити безпеку?

Цілі дуже залежать від індивідуальної ситуації. Але можна виділити три основних, характерних для всіх випадків.

1. Запобігання будь-яким спробам змінити інформацію, зберігаючи її незмінною.

2. Гарантійність та конфіденційність усіх даних.
3. Доступність всіх дій та збереження здатності до виконання операцій.

Незмінність гарантує, що у разі вторгнення зловмисника в операційну систему ПК файли не будуть знищені. Також неможливо змінити вміст і замінити вихідні файли.

Конфіденційна інформація включає наступну інформацію:

• відомості, що становлять комерційну таємницю;
• персональні дані авторизованих користувачів;
• список користувачів і паролів;
• документація, яка використовується всередині компанії;
• бухгалтерська звітність;
• збережена робоча переписка;
• кадри фото та відеозйомок, спостережень;
• інша важлива інформація.

Такі файли представляють особливий інтерес для злочинців і конкурентів, оскільки їх можна використовувати не тільки для розкрадання фінансових коштів, але й для розкриття даних в особистих цілях.

Існує ще одна проблема щодо вжиття заходів безпеки: забезпечення доступності. Сервери, принтери, робочі станції, важливі файли та інші ресурси мають бути доступними для всіх користувачів цілодобово та без вихідних.

Методи захисту.
Усі заходи щодо забезпечення безпеки мають бути заздалегідь розроблені, сформульовані у вигляді плану. Одним з найважливіших моментів є недопущення форс-мажорних ситуацій.

Для забезпечення захисту створюються фізичні перешкоди для проникнення зловмисників на комп'ютер. Встановлюється контроль над усіма ресурсами системи. Криптографічне перетворення інформації з метою маскування здійснюється при її передачі на великі відстані. Завершальним етапом є створення правил безпеки, що змушує всіх співробітників організації їх виконувати.

Програмні засоби.
Здебільшого забезпечення безпеки локальних мереж залежить від програмних засобів. До них належать:

1. Міжмережеві екрани. Це проміжні елементи комп'ютерної мережі, які служать для фільтрації вхідного і вихідного трафіку. Зменшується ризик

несанкціонованого доступу до інформації.
2. Проксі-сервери. Впровадити обмеження маршрутизації між глобальною та локальною частинами мережі.
3. VPN. Вони дозволяють передавати інформацію через зашифровані канали.
4. Різні набори протоколів, необхідні для створення безпечного з'єднання та встановлення контролю над елементами локальної мережі.

Всі ці програми інтегровані в операційну систему і є спеціалізованими, шифрують дані, які розділяють інформаційні потоки.

Перелік посилань:

1. Захист інформації в локальних мережах [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Захист_інформації_в_ локальних_мережах
2. Черемушкин Д. В., Осовецький Л. Г.// Дослідження шкідливого коду. - Вісник ІТМО
3. Методи захисту локальної мережі. URL: https://xserver.a-real.ru/blog/useful/metody-zashchity-lokalnoy-seti
4. Корпоративна мережа [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Корпоративна_мережа

Ющенко Матвій Олександрович *УБДМ-61*
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації

ВИЗНАЧЕННЯ ДОЦІЛЬНОГО СПОСОБУ МОНІТОРИНГУ ЗОВНІШНІХ І ВНУТРІШНІХ ПРОЦЕСІВ В ІНТЕРЕСАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)

Розглянуто способи моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації). Наведено задачі моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства. Основним способом моніторингу визначено клас рішень SIEM. Розглянуто цілі використання SIEM, основних представників даного класу рішень, їх переваги та недоліки.

На сучасному етапі інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої організації.

Створення розвиненого і захищеного середовища є неодмінною умовою розвитку підприємства, в основі якого мають бути найновіші автоматизовані технічні засоби. Це пов'язано з постійно зростаючою кількістю загроз, кібератак та інших негативних факторів, що впливають на інфраструктуру підприємств.

Сьогодні ця проблема є актуальною, так як незахищеність інформації може дуже дорого обійтися для будь-якої компанії. Дуже важливо вчасно отримувати дані про загрози, уразливості, порушення та інциденти в корпоративній інформаційній системі. Це дозволить своєчасно відреагувати і усунути їх.

Тому компаніям необхідно впроваджувати автоматизовані засоби, які допоможуть проводити моніторинг зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства. Одним з кращим типів рішень на даний момент є клас рішень SIEM.

Незважаючи на свою відносну зрілість, ринок SIEM все ще зростає двозначними темпами. Основною тенденцією є все більш широке використання поведінкової аналітики та автоматизації для фільтрації менш нагальних попереджень, щоб групи безпеки могли зосередитись на найбільших загрозах. Аналітики розглядають хмару як зростаючий засіб надання послуг SIEM, як для малих, так і для великих організацій, які шукають простіших способів відстежувати складне середовище.

Програмне забезпечення Security Information and Event Management (SIEM) надає спеціалістам інформаційної безпеки підприємства можливість відстежувати всі події, які відбуваються в їхньому IT-середовищі [1].

Технологія існує вже більше десяти років. Вона поєднує в собі управління подіями безпеки (SEM) – аналіз даних журналу та подій у режимі реального часу, щоб забезпечити моніторинг загроз, кореляцію подій, реагування на інциденти, та управлінням інформаційною безпекою (SIM), яка збирає, аналізує та звітує про дані журналу.

SIEM збирає та агрегує дані журналу, згенеровані на всій технологічній інфраструктурі організації, від хостових систем і додатків до мережевих та захисних пристроїв, таких як брандмауери та антивірусні фільтри.

Після цього програмне забезпечення визначає та класифікує інциденти та події, а також аналізує їх. SIEM забезпечує дві основні цілі, які мають бути досягнуті [1]:

1) надавати звіти про інциденти та події, пов'язані з безпекою, такі як успішні та невдалі входи в систему, активність зловмисного програмного забезпечення та інші можливі зловмисні дії; та

2) надсилати сповіщення, якщо аналіз показує, що будь-яка діяльність виконується проти заздалегідь визначених наборів правил і, таким чином, вказує на потенційну проблему безпеки.

SIEM в основному використовується великими організаціями та державними компаніями, де дотримання правил залишається найважливішим фактором використання цієї технології.

На ринку SIEM є декілька домінуючих постачальників на основі продажів у всьому світі, зокрема IBM, Splunk та HPE. Є щонайменше ще кілька основних гравців, а саме: Alert Logic, Intel, LogRhythm, ManageEngine, Micro Focus, Solar Winds і Trustwave [2].

Прикладом SIEM є IBM QRadar. У більшості фірм IBM QRadar SIEM оцінюється високо, але складність впровадження може обмежити привабливість середніх та великих підприємств, які потребують основних можливостей SIEM, та тих, хто шукає єдину платформу, яка охоплює широкий спектр моніторингу безпеки та експлуатаційних технологій.

LogRhythm – ще один постачальник SIEM з високими рейтингами та популярністю. Цю систему легше розгортати, ніж деякі інші найпопулярніші продукти SIEM, але вона не може розширюватися, щоб підтримувати дуже великі обсяги подій. SIEM від LogRythm найкраще підходить для малих та середніх організацій, які вже мають певну функцію розвідки та аналітики загроз.

Програмне забезпечення SIEM від McAfee, можливо, відстає від IBM, Splunk та LogRhythm у загальній конкуренції SIEM, але його простота розгортання, а також інтеграція з іншими інструментами McAfee роблять його сильним конкурентом у багатьох списках SIEM.

Перелік посилань:

1. What is SIEM software? How it works. URL: https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html

2. Top SIEM Products. URL: https://www.esecurityplanet.com/products/top-siem-products.html

Стешенко Олександр Михайлович
студент групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ПЕРЕВАГИ SOCaaS ПРИ ВИБОРІ ПІДПРИЄМСТВОМ МОДЕЛІ ОПЕРАЦІЙНОГО ЦЕНТРУ БЕЗПЕКИ

SOC є невід'ємною частиною мінімізації витрат на потенційний витік даних, оскільки вони не лише допомагають організаціям швидко реагувати на вторгнення, а й постійно покращують процеси виявлення та запобігання. Всеосяжна стратегія центру операцій із забезпечення безпеки обертається навколо управління загрозами, що включає збір даних і аналіз цих даних на предмет підозрілої активності, щоб зробити всю організацію більш безпечною. При правильній реалізації центр управління безпекою може надати організації численні переваги.

Ключові слова: SOC, моделі SOC, SOCaaS.

Центр управління безпекою (SOC) - це командний центр для групи фахівців в галузі інформаційних технологій (IT), які мають досвід в галузі інформаційної безпеки (Infosec), які відстежують, аналізують та захищають організацію від кібератак[1].

У SOC інтернет-трафік, мережі, робочі станції, сервери, кінцеві пристрої, бази даних, програми та інші системи постійно перевіряються на наявність ознак порушення безпеки. Співробітники SOC можуть працювати з іншими командами або відділами, але, як правило, вони працюють автономно зі співробітниками, які мають високі навички в галузі IT та кібербезпеки, або передані на аутсорсинг стороннім постачальникам послуг. Більшість SOC працюють цілодобово, а співробітники працюють позмінно, щоб постійно реєструвати активність та усувати загрози.

Перед створенням SOC організація повинна визначити свою стратегію кібербезпеки відповідно до поточних бізнес-цілей та проблем. Керівники департаменту посилаються на оцінку ризиків, яка фокусується на тому, що потрібно для підтримки місії компанії, і згодом надають інформацію про цілі, які необхідно виконати, а також про інфраструктуру та інструменти, необхідні для досягнення цих цілей, а також про необхідні навички персоналу.

Існує кілька узгоджених рекомендацій щодо запуску SOC. Перш ніж SOC зможе стати успішним, важливо вибрати модель SOC, найбільш ефективну для цієї організації, укомплектувати команду найкращими фахівцями з безпеки та

впровадити належні інструменти та технології.

Більшість великих організацій мають власні SOC, у той час як компанії, які не мають персоналу або ресурсів для самостійного обслуговування, можуть вирішити передати деякі або всі обов'язки SOC назовні.

Центр управління безпекою як послуга (SOCaaS), який деякі відкидають як «маркетинговий термін», набирає обертів і стає окремим ринком, оскільки він вирішує деякі ключові проблеми, що стоять перед більшістю організацій, а також вирішує інші завдання безпеки та фінансів[2].

По суті, термін SOCaaS відноситься до типу керованої служби безпеки (MSS). Як і MSS, SOCaaS включає весь моніторинг і управління системами виявлення вторгнень, брандмауерами, антивірусними і антиспамовими системами, віртуальними приватними мережами (VPN), захистом кінцевих точок (EPP) і виявленням і реагуванням кінцевих точок (EDR). Крім того, SOCaaS включає служби, які зазвичай входять до складу рішень керованого виявлення та реагування (MDR) і можуть розглядатися як еволюція як MSS, так і MDR.

Прагнення цифрової трансформації та хмарних сервісів для підвищення ефективності, підвищення гнучкості та скорочення витрат швидко та значно розширило поверхню атаки для більшості організацій. Кібер-зловмисники користуються цими тенденціями, оскільки співробітники стають все більш мобільними та віддаленими, отримуючи доступ до додатків, систем, служб та даних як локально, так і у хмарі з-за меж корпоративної мережі. Швидке збільшення кількості людей, які працюють вдома, прискорило цю тенденцію та посилило ризик.

Прагнучи захистити конфіденційні дані відповідно до зростаючого числа правил захисту даних у всьому світі, а також захистити інтелектуальну власність та іншу конфіденційну комерційну інформацію, більшість організацій вклали значні кошти в інструменти моніторингу безпеки на підприємстві та у хмарі.

Однак для багатьох організацій це спричинило щоденну лавину попереджень системи безпеки. Більшості цих організацій, особливо малим та середнім підприємствам, важко чи неможливо розслідувати та аналізувати кожне попередження.

Ще одним ключовим фактором стала нестача навичок кібербезпеки, що стосується організації всіх розмірів. SOCaaS дозволяє використовувати переваги центру управління безпекою (SOC) або додаткових ресурсів SOC без необхідності шукати та утримувати людей із необхідними навичками. SOCaaS також забезпечує можливість швидкого нарощування ємності та з набагато меншими витратами, ніж підтримка додаткових потужностей власними силами.

Перед обличчям все більш складного та швидко мінливого середовища бізнесу, IT та кіберзагроз зростає попит на SOCaaS, оскільки більшість організацій бачать цінність запропонованих переваг, які включають:

- безперервний та всебічний централізований моніторинг та аналіз корпоративних систем на предмет підозрілої активності за фіксованою та передбачуваною щомісячною або річною вартістю;

- поліпшення часу та методів реагування на інциденти;
- швидше виявлення подій безпеки, таких як компрометація та стримування загроз;
- дозвіл всіх попереджень для максимальної віддачі від існуючих систем;
- зниження витрат та впливу інцидентів безпеки на бізнес.

У той час як мікро- і малі підприємства, як правило, потребують SOCaaS для виконання всіх функцій SOC, великі підприємства, як правило, використовують групи аналітиків SOCaaS для доповнення внутрішніх команд, у той час як організації середнього розміру зазвичай знаходяться десь посередині між цими крайнощами. В результаті більшість постачальників SOCaaS зазвичай спеціалізуються на одному або двох із цих підсегментів, і дуже мало хто обслуговує однаково всі сегменти ринку. Очікується, що тенденція до спеціалізації обслуговування потреб певного підсегменту ринку збережеться. Постачальники SOCaaS, орієнтовані на малий та середній бізнес, будуть вдосконалювати пропозиції, щоб надавати інформацію та рекомендації, що дозволяють організаціям спільно управляти своєю безпекою, наприклад, із зовнішніми командами SOC, тоді як постачальники, орієнтовані на середні, великі та дуже великі підприємства, будуть розширювати свої можливості щодо ризиків, периферійної безпеки, а також безпеки IoT.

Хоча SOCaaS перетворився на дискретний ринок, і жодна організація не може сказати, що їй не потрібні централізовані, скоординовані погляди на її стан безпеки та здатність реагувати на погрози та інциденти, не всі служби надають всі можливості всім організаціям.

Тому важливо, щоб кожна організація:

- визнавала важливість та переваги об'єднання всіх загроз безпеці, інструментів та систем у єдину точку управління для обробки та дозволу всіх попереджень, моніторингу та реагування на всі індикатори компрометації (IoC), а також для оцінки ефективності існуючих засобів контролю;
- розвивала повне розуміння своїх поточних та майбутніх вимог до моніторингу кібербезпеки та реагування з боку постачальників послуг керованої безпеки (MSSP);
- визнавала, що деякі пропозиції SOCaaS найкраще підходять для організацій певного розміру та галузі, а деякі пропонують спеціалізовану підтримку для регульованих галузей;
- визначала, які постачальники послуг найкраще задовольняють ці потреби, незалежно від того, чи називається послуга SOCaaS чи ні.

Пропозиції SOCaaS, визначені вище, вирішують важливі завдання, що стоять перед більшістю організацій в епоху цифрових технологій та після пандемії. Вони приносять користь організаціям усіх розмірів і типів і тому заслуговують на розгляд у рамках будь-якої стратегії кібербезпеки.

Перелік посилань:

1. DEFINITION security operations center (SOC) [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC?_gl=1*1e1zmol*_ga*MTgyMjgyOTQ1OC4xNjIyNTgwMzY3*_ga_RRBYR9

2. Why your business needs SOC as a service [Електронний ресурс] – Режим доступу до ресурсу: https://www.computerweekly.com/opinion/Why-your-business-needs-SOC-as-a-service

Лабяк Дар'я Сергіївна
Студентка групи УБДМ-51, ННІЗІ ДУТ, Київ, Україна

ВНУТРІШНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Статистика з кожним роком змінюється щодо загроз інформаційної безпеки, але, на жаль, не в кращу сторону. Відсутність захисту даних, побічні ефекти глобальної пандемії та зростання складності експлойтів призвели до величезного зростання кількості взломів та хакерських атак. Крім того, COVID-19 та повномасштабне вторгнення Росії збільшило кількість віддаленої робочої сили, створивши ідеальний шлях для кібератак. Підприємства задля безпеки своїх співробітників, з ким це можливо, перевели співробітників на віддалену роботу. Тому питання захисту ще більше набуває популярності, а особливо питання захисту від внутрішніх загроз.

Ключові слова: внутрішні загрози, підприємство, інформаційна безпека, навмисні та ненавмисні загрози.

Для початку розберемось, що таке внутрішня загроза. Внутрішньою загрозою прийнято вважати те, що джерело самої загрози знаходиться в середині підприємства. Крім того, внутрішня загроза — це потенційна можливість для інсайдера завдати шкоди організації шляхом використання свого привілейованого рівня знань та/або доступу [1].

Людина приходить працювати в організацію А з метою викрадення конфіденційної інформації та в подальшому її продати іншим зацікавленим сторонам, організації Б, яка бажає нашкодити підприємству А, що є їхніми конкурентами . Людину приймають на роботу на підприємство А без перевірок судимості, перегляду того, на кого працювала раніше, а також, не підписує договір про нерозголошення конфіденційної інформації. Тобто, через нехтуваннями такими правилами на перевірку особи, можлива загроза, що людина розкриє конфіденційну інформацію організації А і за це не буде нести ніякої відповідальності. Це є прикладом навмисної внутрішньої загрози.

Також, слід пам'ятати, що існує ненавмисна внутрішня загроза. Ненавмисні загрози — це дії, здійснені без злого наміру, які, тим не менш, становлять серйозну загрозу інформаційній безпеці. Основною категорією ненавмисних загроз є помилка людини.

По-перше, чим вищий рівень працівника, тим більшу загрозу він становить для інформаційної безпеки. Це правда, тому що працівники вищого рівня зазвичай мають більший доступ до корпоративних даних і користуються більшими привілеями щодо організаційних інформаційних систем.

По-друге, особливо серйозні загрози інформаційній безпеці створюють працівники двох сфер організації: людські ресурси та інформаційні системи. Працівники відділу кадрів зазвичай мають доступ до конфіденційної особистої

інформації про всіх співробітників. Подібним чином працівники ІБ не тільки мають доступ до конфіденційних організаційних даних, але й часто контролюють засоби створення, зберігання, передачі та зміни цих даних.

Та найчастіше ігноруються в системах інформаційної безпеки охоронці та прибиральники, якщо ми говоримо про організації, що все ж таки мають офіс на сьогоднішній час. Компанії часто передають послуги охорони та прибирання на аутсорсинг. Як і підрядники, ці особи працюють на компанію, хоча технічно вони не є працівниками. Більше того, вони зазвичай присутні, коли більшість, якщо не всі, інші працівники пішли з офісу. Вони зазвичай мають ключі від кожного кабінету або приміщення, і ніхто не сумнівається в їхній присутності навіть у найбільш чутливих частинах будівлі. Задля захисту від цієї загрози, необхідним є встановлення камер та щоб певний час зберігались записи з цих камер[2].

Навмисні чи ні, внутрішні загрози мають значний вплив на репутацію, надійність, безпеку та довіру до підприємства. Таким чином, такі інциденти заслуговують на увагу менеджменту у всіх галузях, щоб зменшити вплив інцидентів, та організації були готові ефективно реагувати на нові загрози. Одним із викликів, з якими сьогодні стикаються підприємства, є захист своїх активів у віртуальному середовищі, які є вразливими до атак як зсередини, так і ззовні [3].

Важливим запобіжним заходом внутрішніх загроз є розвиток співробітників в темі інформаційної безпеки. Кожна організація по-різному до цього ставиться, адже не існує універсальних правил та засобів. Однак для всіх організацій вкрай важливо розглянути принципи забезпечення цілісного підходу, що ґрунтується на оцінці ризиків, для запобігання внутрішнім загрозам:

- Навчати співробітників, як правильно поводитися в інформаційному просторі не лише на роботі, але й в приватному житті. Проводити тренінги та надсилати періодично брошури з правилами кібергігієни.
- Використовувати новітні технології щодо запобігання, виявлення та звітування потенційних інцидентів.
- Впровадити бізнес процеси щоб реагувати та аналізувати тенденції з метою покращення загальних програм.
- Розробити політики та процедури, підтримувати їх в актуальному стані та забезпечити виконання усіх правил усіма співробітниками та підрядниками.

Перелік посилань:

Insider Threats: The Danger Inside Organizations [Електронний ресурс] – Режим доступу: https://www.globalsign.com/en-sg/blog/insider-threats-danger-inside-organizations
Computer Security & Threat Prevention for Individuals & Organizations [Електронний ресурс] – Режим доступу: https://study.com/academy/lesson/computer-security-threat-prevention-for-individuals-organizations.html
Unintentional Threats to Information Systems [Електронний ресурс] – Режим доступу: https://www.ques10.com/p/48135/unintentional-threats-to-information-systems-1/

Маницький Володимир Євгенійович
студент групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

КЕРУВАННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ НА БАЗІ РІШЕННЯ GLUU

Централізована авторизація користувачів, керування їх доступами використовується майже у всіх компаніях. Це пов'язано як з безпекою так і зі зручністю. Як простий приклад: працівник звільнився або був звільнений, в нього був свій акаунт для VPN, пошти, RDP і внутрішніх сервісів. Після звільнення ці доступи необхідно видалити, щоб колишній співробітник не мав змоги продовжувати користуватись внутрішніми ресурсами компанії. Щоб адміністратор не заходив на кожен сервер і вручну не видаляв користувача, витрачаючи свій час і ризикуючи пропустити щось через звичайний людський фактор, існують рішення для керування ідентифікацією та доступом, звідки і ведеться керування користувачами.

Існують різні рішення для керування користувачами, і хоча найвідомішим, мабуть є Azure Active Directory, але уваги також заслуговує Open-source продукт для Linux-серверів – GLUU. Він підтримує найпоширеніші протоколи: LDAP, RADIUS, SAML, тощо. Простий в установці і налаштуванні. Але не дивлячись на простоту, має певні нюанси в інтеграції з іншими продуктами, з якими може зіткнутись адміністратор. Має досить зручний GUI(graphical user interface) для створення користувачів, груп, моніторингу подій та невдалих спроб входу.

Далі більш детально про переваги і певні недоліки GLUU:

Free Open Source Software

The Gluu server це FOSS (Free Open Source Software) для IAM(Identity and Access Management). Тобто продукт повністю безкоштовний і кожен хто має потребу у використанні рішення для керування користувачами може встановити його на сервер. Для цього достатньо додати репозиторій на сервері, та встановити Gluu за допомогою пакетного менеджера (apt у випадку Ubuntu Server). Після цього запустити сервіс і запустити скрипт який проведе фінальну інсталяцію, вам потрібно просто вводити дані для генерації сертифікатів, вказати domain name, тощо. І все – Gluu Server готовий до використання. Після цього треба зайти на IP-адресу або domain name під адмін-користувачем, що був створений під час інсталяції.

Open Web Standards

Сервер Gluu можна розгорнути для підтримки таких відкритих стандартів для автентифікації, авторизації, федеративної ідентифікації та керування ідентифікацією:

- OAuth 2.0
- OpenID Connect
- User Managed Access 2.0 (UMA)
- SAML 2.0
- System for Cross-domain Identity Management (SCIM)
- FIDO Universal 2nd Factor (U2F)
- FIDO 2.0 / WebAuthn
- Lightweight Directory Access Protocol (LDAP)

- Remote Authentication Dial-In User Service (RADIUS)

Тобто всі найпоширеніші відкриті протоколи. Як приклад можна взяти LDAP. LDAP — відносно простий протокол, що використовує TCP/IP і дозволяє проводити операції аутентифікації (bind), пошуку (search) та порівняння (compare), а також операції додавання, зміни або видалення записів. Зазвичай LDAP-сервер приймає вхідні з'єднання на порт 389 по протоколах TCP або UDP. Для LDAP-сеансів, інкапсульованих в SSL, зазвичай використовується порт 636. Gluu має власний LDAP сервер і надає змогу додавати туди користувачів або групи за допомогою GUI. А далі вже за звичайною схемою Ви підключаєте свої сервіси через LDAP до серверу Gluu і вони беруть користувачів з його бази.

Identity Management

Ідентифікацією та даними об’єктів, такими як профілі користувачів, дані конфігурації, маркери та облікові дані, можна керувати через інтерфейс адміністратора «oxTrust» або за допомогою браузера LDAP. oxTrust – має досить широкий функціонал з керування користувачами. Можна додавати спеціальні поля з додатковими даними. Але у випадку якщо треба більш детально переглянути, змінити, додати інформацію – можна використати браузер LDAP. Він має менш зручне керування але тоді ви можете побачити опис об’єкту так, як бачить його сторонній сервіс при підключенні і при потребі, змінити. Сервер Gluu також підтримує протокол SCIM, який можна використовувати для надсилання даних на сервер Gluu із зовнішніх джерел ідентифікаційних даних, таких як системи керування ідентифікацією та хмарні програми.

Підтримка сервісу

Не дивлячись на те, що продукт безкоштовний, він має досить активну підтримку, але є нюанси. Gluu пропонує безкоштовну та VIP-підтримку. Будь-хто може переглядати або зареєструватися та публікувати запитання на порталі підтримки Gluu. Заявки, відкриті спільнотою, є публічними, і ми докладаємо всіх зусиль, щоб на них відповісти вчасно. Приватна підтримка, гарантований час відповіді та консультаційна підтримка доступні за контрактом на платну підтримку.

Можливість налаштування HA-кластеру

Gluu server надає можливість налаштування відмовостійкого кластеру. Це робиться для того, щоб при виході з ладу одного сервера, інший одразу міг підхопити його функції. Тобто встановлюється два або більше серверів з налаштованим Gluu server, при цьому на них вмикається реплікація, щоб дані співпадали. Це досить поширена практика, щоб зменшити час недоступності сервсів, адже без ha-кластеру доступ буде втрачено, поки будуть тривати роботи по відновленню, а у випадку з кластером відбудеться автоматичне переключення на працюючий сервер. Кроки для налаштування досить детально описані у офіційній документації Gluu.

Можливі складнощі в роботі із сервісом

Gluu має трохи іншу структуру всередині LDAP-серверу ніж найпоширеніший Active Directory. А саме інші назви деяких полів об’єкту. Тому при інтеграції із іншими продуктами за допомогою LDAP можуть винкнути

складнощі із користувачами і групами. В цьому випадку необхідне налаштування не лише зі сторони Gluu, а і зі сторони сервісу, який буде підключатись. Тобто вказати, які поля - за що відповідають. Також за замовчуванням LDAP «слухає» на localhost, що може потребувати додаткової конфігурації.

Перелік посилань:
1. Clustering for HA
URL: https://gluu.org/docs/gluu-server/4.0/installation-guide/cluster/
2. Gluu Server 4.0 Documentation
URL: https://gluu.org/docs/gluu-server/4.0/
3. LDAP: з чого почати?
URL: http://docs.linux.org.ua/Адміністрування/using_ldap/

Басюк Ілля Богданович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ЗАХИСТ ЦИВІЛЬНОЇ АВІАЦІЇ ВІД КІБЕРЗАГРОЗ

Розглядаючи комп'ютерно-інтегровані авіаційні системами, що забезпечують зв'язок між об'єктами діяльності цивільної авіації в межах каналів «земля-повітря» та «повітря-повітря» , дедалі гостріше постає питання безпечної експлуатації таких авіаційних систем з точки зору негативного впливу постійно зростаючих з кожним роком. Зважаючи на постійно зростаючу статистику кібератак на роботу цивільної авіації в світовому масштабі, після глибокого аналізу та опрацювання зазначеної проблематики, забезпечення кібернетичної безпеки та організації захисту каналів «земля-повітря» та «повітря-повітря» парку перебуваючих в експлуатації повітряних суден авіакомпаній України. Авторами планується ряд науково технічних рішень щодо розробки та впровадження ефективних методів та засобів щодо забезпечення вимог, забезпечення кібернетичної безпеки та організації захисту каналів.

Ключові слова: комп'ютерно-інтегрована авіаційна система, кіберзагроза, кібернетична безпека, авіаційна галузь, повітряне судно, методи автентифікації, інфраструктура відкритих ключів.

Основні попереджуючі знаки забезпечення кібернетичної безпеки цивільної авіації україни та світу [1, с. 24]:

Перелік посилань:
1. СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ЦИВІЛЬНОЇ АВІАЦІЇ УКРАЇНИ ТА СВІТУ.
URL:**https://www.researchgate.net/publication/344385843_SUCASNIJ_STAN_ZABEZPECENNA_KIBERNETICNOI_BEZPEKI_CIVILNOI_AVIACII_UKRAINI_TA_SVITU**

Харитонов Олександр Володимирович
Студент группы УИКБ51, ННІЗІ ДУТ, Київ, Україна

АВТОМАТИЗАЦІЯ УПРАВЛІННЯ ІНЦИДЕНТАМИ

В тезі коротко описано, що таке управління інцидентами та які інструменти використовуються для автоматизації процесів управління інцидентами, описані програмні продукти для автоматизації діяльності фахівців з кібербезпеки, такі як: SIEM та SOAR. Для більш гарного уявлення було розкрито ці два поняття, та для чого, що використовується. Також були приведені переваги автоматизації як для персоналу, так і для клієнтів.

Управління інцидентами у кібербезпеці - це набір мір і заходів спрямованих на боротьбу з кіберзагрозами і зменшенню наслідків атак. Управління інцидентами включає: Моніторинг подій кібербезпеки, реагування на інциденти, розслідування та запобігання

Для автоматизації управління інцидентами використовують SIEM-системи, SOAR та EDR-рішення [1]

SIEM (**Security information and event management**) - це клас програмного забезпечення спрямованих на зборі та аналізі подій кібербезпеки. За допомогою SIEM систем спеціалісти з інформаційної та кібернетичної безпеки можуть виявляти кібератаки та порушення політик безпеки, що є найважливішим для вчасного та ранніх стадіях мінімізувати шкоду. Також SIEM системи допомагають оцінити захищеність інформаційних систем та актуальні для підприємства риски. [2]

SOAR (System Orchestration and Response) - клас програмних продуктів, призначених для оркестровки систем безпеки, тобто їх координації та управління ними. Зокрема, рішення класу SOAR дають змогу збирати дані про події інформаційної безпеки з різних джерел, обробляти їх і автоматизувати типові сценарії реагування на них.

Рішення для управління подіями та інформацією про безпеку (SIEM) багато в чому схожі на SOAR-рішення, внаслідок чого одне поняття іноді підміняють іншим. Однак між ними є суттєва різниця: тоді як SIEM-рішення націлені на збір інформації та ручне управління інцидентами, SOAR-системи розраховані на автоматизацію й оркестровку роботи декількох різних систем інформаційної безпеки, зокрема, на етапі реагування. У результаті SIEM-рішення чудово доповнюють SOAR як джерело інформації про події. [3]

Автоматизоване керування інцидентами - це практика автоматизованого реагування на інциденти, щоб переконатися, що ключові події ідентифікуються та розглядаються найбільш ефективним і надійним способом. Час має важливе значення, коли справа доходить до управління інцидентами. Отже швидкість є головною перевагою автоматизованого керування інцидентами. Роботи, що потребують багато часу, можна виконувати значно швидше завдяки автоматизації. [4]

Переваги автоматизованого управління інцидентами

Швидкість обробки подій: при обробці подій вручну фахівці, швидше за все, введуть дані більше ніж один раз і, швидше за все, припустяться помилок (наприклад, не зможуть змінити статус проблеми в системі). Фахівцям не доведеться перемикатися між програмами чи виконувати операції вручну, якщо вони використовують автоматизоване рішення для керування проблемами.

Як альтернатива, вони можуть перенаправити цей час на оперативне вирішення інших проблем, що значно підвищить задоволеність клієнтів і персоналу.

Забезпечення прозорості дій: більшість співробітників хочуть отримувати інформацію про кожну проблему, яку вони представляють. Автоматизоване

керування інцидентами дозволить вам забезпечити їм необхідну прозорість. як?

У кожній точці терміну дії квитка, від моменту його призначення фахівцю до моменту його вирішення, працівник може отримати сповіщення через чат після надсилання квитка. [4]

Співробітнику не доведеться просити фахівців про оновлення статусу, і він завжди буде проінформований без необхідності відвідувати конкретну програму.

Ключовими можливостями є наступні фактори:

Алгоритми кластеризації та зіставлення шаблонів можна використовувати для зменшення шуму, наприклад помилкових тривог.

Розпізнавайте закономірності до того, як вони вплинуть на ймовірність збоїв.

Зверніть увагу на багатофакторні аномалії, які виходять за межі статичних порогів або числових викидів, щоб завчасно ідентифікувати аномальні обставини та поведінку та пов’язати їх із наслідками для бізнесу.

Визначте причинно-наслідковий зв’язок, визначте ймовірне джерело подій за допомогою топології та машинного навчання та прив’яжіть ці проблеми до шляху клієнта за допомогою дерев рішень, випадкових лісів і аналізу графів.

Сприяти автоматизації рутинних завдань із низьким або помірним ризиком. Без необхідності створювати з’єднання з іншими системами механізм робочого процесу дозволяє вирішувати питання, які є терміновими та знаходяться під вашим контролем.

Визначте пріоритет проблем і запропонуйте можливі рішення, безпосередньо або через інтеграцію на основі попереднього досвіду. Щоб уникнути повторення проблем, слідкуйте за тим, до кого зверталися протягом усієї послідовності подій для виправлення у сховищі.

Чат-боти та віртуальні помічники підтримки (VSA) можна використовувати для підвищення ефективності роботи користувачів і автоматизації повторюваних завдань, одночасно демократизуючи доступ до інформації. [4]

Перелік посилань

1. Управління інцидентами (Incident Management). URL: https://encyclopedia.kaspersky.ru/glossary/incident-management/
2. SIEM (Security information and event management).URL: https://encyclopedia.kaspersky.ru/glossary/siem/
3. SOAR (Security Orchestration, Automation and Response). URL: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/
4. Автоматизоване управління інцидентами // Вересень 15, 2022. URL: https://hashdork.com/uk/automated-incident-management/

Матюх В.Ю.
студент групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Для нейтралізації існуючих загроз і забезпечення інформаційної безпеки підприємства створюють систему менеджменту у сфері інформаційної безпеки, в рамках якої (системи) проводять роботу за кількома напрямками:

- формування та практична реалізація комплексної багаторівневої політики інформаційної безпеки підприємства та системи внутрішніх вимог, норм і правил;
- організація департаменту (служби, відділу) інформаційної безпеки;
- розробка системи заходів і дій на випадок виникнення непередбачених ситуацій («Управління інцидентами»);
- проведення аудитів (комплексних перевірок) стану інформаційної безпеки на підприємстві.

Кожен з цих напрямків організаційної роботи має свої особливості і має реалізовуватися з використанням специфічних методів менеджменту та у відповідності зі своїми правилами. Політики і правила інформаційної безпеки є організаційними документами, регулюючими діяльність всієї організації або окремих підрозділів (категорій співробітників) в роботі з інформаційними системами та інформаційними потоками. Департамент інформаційної безпеки є вузько спеціалізованим підрозділом, який вирішує специфічні питання захисту інформації.

Інформаційний менеджмент представляє персонал інформаційних підрозділів як один з пріоритетних ресурсів, який реалізує інформаційну стратегію організації.

Управління інформаційним персоналом організації – комплекс управлінських заходів, які забезпечують відповідність кількісних і якісних характеристик персоналу та спрямованості і мотивації його професійної діяльності цілям і завданням організації. Система управління інформаційними ресурсами організаційно базується на розробці положення про відділ управління інформаційними ресурсами та захисту інформації. Зміст діяльності і призначення відділу визначається, виходячи з таких підсистем загальної системи діяльностей:

- документно-інформаційні ресурси
- управління інформаційною діяльністю
- комунікації.

З метою підвищення ефективності діяльності організацій пропонується введення посади CIO (Chief Information Officer) –професійного менеджера, який має системний стратегічний погляд на бізнес, поєднує компетенції менеджера і фахівця з захисту інформації, інформаційних потоків і структур, бере на себе відповідальність за формування інфраструктури для створення єдиної захищеної

інформаційної системи підприємства, відповідає за організацію всіх інформаційних потоків всередині організації, за її представлення у зовнішньому середовищі, відповідає за забезпечення інформацією всіх функціональних спеціалістів компанії і керівників; має знання і навички формування і використання інформаційних ресурсів в управлінні підприємствами і бізнес-процесами.

Менеджмент інформаційної безпеки - це циклічний процес, що включає:

- усвідомлення ступеня необхідності захисту інформації;
- збір та аналіз даних про стан інформаційної безпеки в організації;
- оцінку інформаційних ризиків;
- планування заходів щодо обробки ризиків;
- реалізацію та впровадження відповідних механізмів контролю;
- розподіл ролей та відповідальності;
- навчання та мотивацію персоналу;
- оперативну роботу щодо здійснення захисних заходів;
- моніторинг функціонування механізмів контролю,
- оцінку їх ефективності та відповідні коригувальні впливи.

Система заходів з реагування на інциденти забезпечує готовність всієї організації (включаючи Департамент інформаційної безпеки) до осмислених цілеспрямованих дій у разі будь-яких подій, пов'язаних з інформаційною безпекою. Проведення внутрішніх аудитів інформаційної безпеки (періодичних або пов'язаних з певними подіями) має забезпечити контроль за поточним станом системи заходів щодо захисту інформації та, зокрема, незалежну перевірку відповідності реального стану справ встановленим правилам і вимогам.

Рисунок 10.2 – Структура організаційної діяльності у сфері інформаційної безпеки на підприємстві

При цьому кожен з напрямків діяльності має постійно вдосконалюватися, а конкретні завдання повинні постійно уточнюватися відповідно до зміни в організаційній структурі, виробничих процесах або зовнішньому середовищі.

Перелік посилань:

1.Матвієнко О. Інформаційний менеджмент: аналіз предметної галузі//Вісник Книжкової палати. - 2004. - № 8. - С. 13-17.

2. Матвієнко О.В., Цивін М.Н. Основи менеджменту інформаційних систем: навчальний посібник. Київ: Центр навчальної літератури, 2005. 176с.

3. Ярочкин В.І. Безпека інформаційних систем. - М.: вид. "Вісь-89", 2006.

Кизим Валентин Володимирович,
Студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна
м.Київ

ЦИФРОВА ГРАМОТНІСТЬ ТА ЇЇ ВПЛИВ НА КІБЕРБЕЗПЕКУ

Цифрові технології вже досить давно стали нормою в повсякденному житті в Україні. Проте лише відносно недавно вони почали інтегруватись з іншими основними аспектами нормального життя, такими як взаємодія з державою, документообіг, медицина, тощо. І це створило нові складнощі в забезпечені інформаційної безпеки та збережені конфіденційності даних. Не в останню чергу це пов'язано з досі відносно низьким рівнем цифрової грамотності звичайного населення, в особливості, старшого покоління, що народилось та виховувалось в епоху до появи масового розповсюдження та використання інтернету.
Ключові слова: цифрова грамотність, людський фактор, інформаційна безпека, електронний документообіг.

Україна – поки ще одна з небагатьох країн світу, яка активно запроваджує та інтегрує практику так званої «діджиталізації» в майже усі сфери управління та сервіси держави. Згідно повідомлень Міністерства цифрової трансформації України станом на 23 травня лише застосунком для мобільних пристроїв «Дія» користувалось вже більше 17 млн. осіб [1]. Додаток дає змогу зберігати та застосовувати рівнозначно з оригіналами 15 цифрових документів та отримувати 9 видів послуг. На самому ж порталі доступно вже 72 послуги. І цей концепт особливо показав свою ефективність під час повномасштабного вторгнення Російських Окупаційних Військ після 24 лютого, коли електронні документи часто було єдиним, що вдалось зберегти після обстрілів та у випадку раптової евакуації з зони бойових дій.

Проте діджиталізація, також, породила і нові проблеми та головний біль для фахівців з забезпечення інформаційної безпеки. Не дивлячись на широке розповсюдження технологій Інтернет в наш час, досить значна частина населення все ще не володіла ними в достатній мірі, що призводило до необачного їх використання та навіть інцидентів порушення безпеки з провини самих користувачів. Виникали й проблеми з забезпеченням безпеки даних і в установах, що вели свою діяльність з використанням цифрових сервісів. Все це було викликано все ще досить низьким рівнем цифрової грамотності як користувачів, так і значної кількості не пов'язаного з ІТ-технологіями персоналу. В інформаційній безпеці людський фактор відіграє дуже значну роль, часто являючись чи не найслабшою ланкою в системах захисту. Тому критично важливо, щоб достатнім рівнем знань про інформаційну безпеку були забезпечені не тільки відповідальні фахівці, а й пересічний персонал та користувачі [2, с. 438].

Розв'язати цю проблему взялось окремо як Міністерство цифрової трансформації України, так і приватні ініціативи від провідних ІТ-компанії та фахівців в сфері захисту інформаційних технологій. Зокрема Мінцифри створило та всіляко заохочує населення вивчати їх курси медіаграмотності, в той час як приватні компанії розміщують свої курси за допомогою навчальних платформ, таких як Prometheus та схожих. Це приносить результати. Так, згідно з

дослідженням Мінцифри, з 2019 по 2021 рік кількість користувачів з рівнем цифрових навичок «Базовий» та «Вище базового» виросла з 47 до 52,2 відсотків, в той час як кількість користувачів з відсутнім рівнем навичок впала з 15,1 до 11,2 відсотків [3].

Рис.1 – Статистика опитування рівня володіння цифровими навичками серед респондентів.

Це показує зацікавленість населення в підвищенні своїх компетенцій та покращенню навичок володіння цифровими технологіями. А, отже, й позитивно впливає на процес забезпечення інформаційної безпеки в цілому.

Збройна агресія зі сходу також досить суттєво вплинула на розвиток медіаграмотності населення за допомогою наглядної демонстрації наслідків недостатнього розвитку навичок медіа та цифрової грамотності.

Висновок: забезпечення достатнього рівня цифрової грамотності пересічних користувачів є не менш важливою задачею для забезпечення достатнього рівня кібербезпеки в державі та на підприємствах. Робота в цьому напрямку активно ведеться та вже приносить позитивні результати. Нинішні активні бойові дії також активно підштовхують цей процес. Очікується, що в майбутньому рівень цифрової грамотності пересічного населення продовжить зростати та розвиватись.

Перелік посилань:

1. Кількість користувачів додатку "Дія" перевищила 17 мільйонів, – Мінцифри [Електронний ресурс] // БізнесЦензор. – 2022. – Режим доступу до ресурсу: https://biz.censor.net/news/3343506/kilkist_korystuvachiv_dodatku_diya_perevyschyla_17_milyioniv_mintsyfry.

2. «СВІТ ТЕЛЕКОМУНІКАЦІЇ ТА ІНФОРМАТИЗАЦІЇ» Збірник матеріалів XI Міжнародної науково-технічної конференції студентства та молоді – Київ: Державний університет телекомунікацій, 2021. – 652 с. – (Державний університет телекомунікацій).

3. "ЦИФРОВА ГРАМОТНІСТЬ НАСЕЛЕННЯ УКРАЇНИ" звіт за результатами загальнонаціонального опитування [Електронний ресурс] // Міністерство цифрової трансформації України. – 2021. – Режим доступу до

ресурсу: https://osvita.diia.gov.ua/uploads/0/2625-doslidzenna_2021_ukr.pdf.

Кисельов Олексій Володимирович
студент групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

ПРОТОКОЛ WEBSOCKET ЯК МЕХАНІЗМ ЗАХИСТУ КАНАЛІВ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

Історично склалося так, що створення веб-додатків, які потребують двостороннього зв'язку між клієнтом і сервером (наприклад, обмін миттєвими повідомленнями та ігрові додатки) вимагало зловживання HTTP для опитування сервер для отримання оновлень при одночасній відправці висхідних повідомлень у вигляді окремих HTTP-виклики [RFC6202].

Це призводить до різноманітних проблем:

- Сервер змушений використовувати ряд різних базових TCP
- Дротовий протокол має високі накладні витрати, оскільки кожне повідомлення між клієнтом і сервером має HTTP-заголовок.
- Скрипт на стороні клієнта змушений підтримувати відображення від вихідних з'єднань до вхідних з'єднань для відстеження відповідей.

Більш простим рішенням було б використання одного TCP-з'єднання для трафіку в обох напрямках. Це те, що забезпечує протокол WebSocket. У поєднанні з WebSocket API [WSAPI] він забезпечує альтернативу HTTP-опитуванню для двостороннього зв'язку з веб-сторінки до віддаленого сервера.

WebSocket - протокол зв'язку поверх TCP-з'єднання, призначений для обміну повідомленнями між браузером і веб-сервером в режимі реального часу. Протокол повністю асинхронний та симетричний. Він застосовується для організації чатів, онлайн-табло і створює постійне з'єднання між клієнтом та сервером, яке обидві сторони можуть використовувати для надсилання даних.

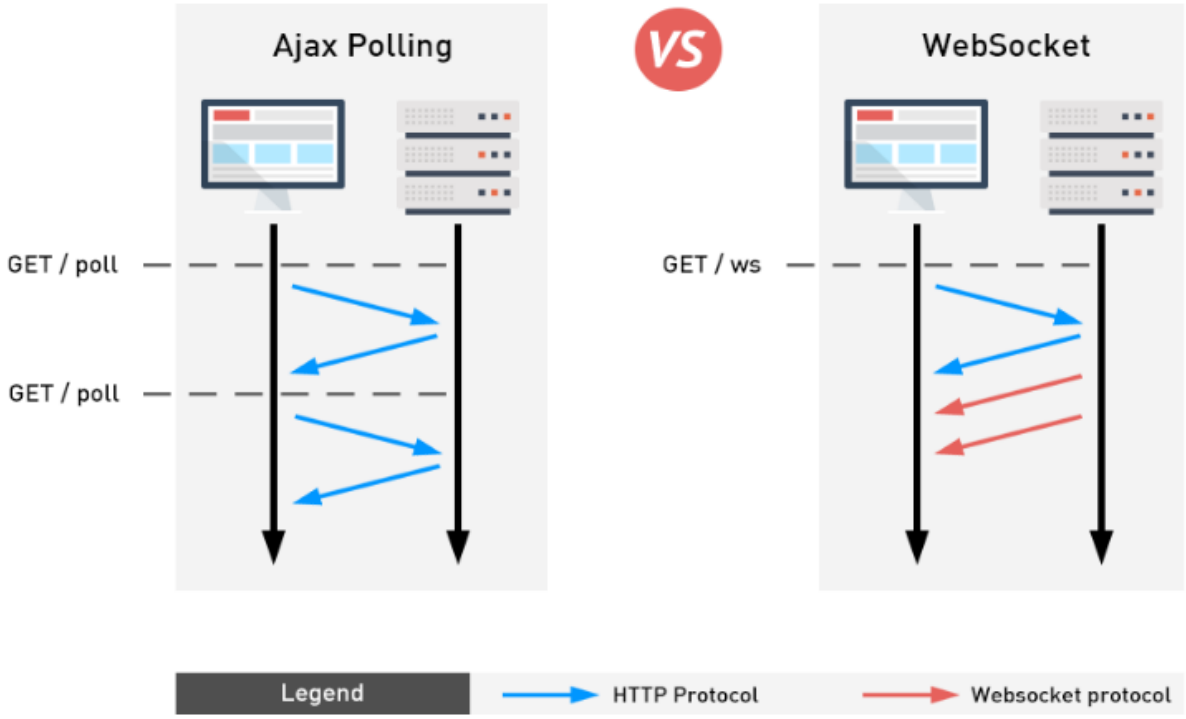
WebSockets дозволяють як серверу, так і клієнту передавати повідомлення в будь-який час без будь-якого відношення до попереднього запиту. Однією з помітних переваг використання WebSockets вирішує кілька проблем з HTTP:

- Двонаправлений протокол - будь-який клієнт/сервер може надіслати повідомлення іншій стороні (у HTTP запит завжди ініціюється клієнтом, а відповідь обробляється сервером, що робить HTTP однонаправленим протоколом)
- Повнодуплексний зв’язок - клієнт і сервер можуть одночасно спілкуватись один з одним
- Єдине TCP-з’єднання - на початку клієнт і сервер спілкуються через TCP-з’єднання, потім протягом усього життєвого циклу - через з’єднання WebSocket.

Встановлення з’єднання на базі WebSocket

Протокол "WebSocket" - це серйозне розширення HTTP, яке дає змогу веб-додаткам підтримувати багатокористувацьку взаємодію в режимі реального часу, що є хорошою перевагою в порівнянні з протоколом HTTP не тільки в плані

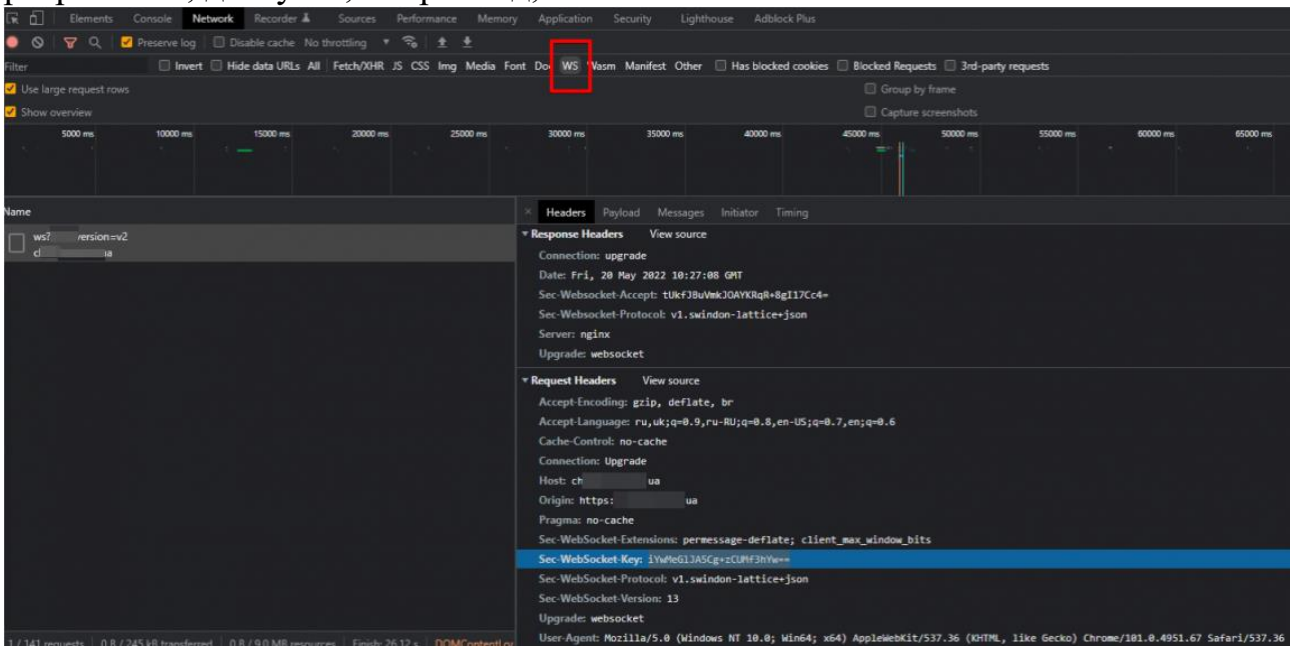
функціональності, а й з боку забезпечення належного рівня безпеки переданих даних.



Взаємодія між клієнтом і сервером починається з рукостискання. Для рукостискання клієнт і сервер використовують протокол HTTP, але з деякими відмінностями у форматі повідомлень, що передаються. Не дотримуються всіх вимог до HTTP-повідомлень.

Після того як рукостискання виконано, початкове з'єднання **HTTP** замінюється з'єднанням **WebSocket**, яке використовує те ж з'єднання **TCP/IP**. На цьому етапі будь-яка із сторін може розпочати відправлення даних.

Для моніторингу трафіку **WebSocket** зручно використовувати інструменти розробника, доступні, наприклад, в Chrome.



Дані протоколу **WebSocket** передаються як послідовність кадрів. Фрейм має заголовок, у якому міститься така інформація:
- чи фрагментоване повідомлення;
- тип даних — all code;
- чи піддавалися повідомлення маскування - прапор маски;
- розмір даних;
- ключ маски (32 біти);
- інші керуючі дані (ping, pong...).

Усі повідомлення, надіслані клієнтом, мають шифруватися. Шифрування проводиться звичайним **XOR** із ключем маски. Клієнт повинен змінювати ключ для кожного переданого кадру. Сервер не повинен шифрувати повідомлення. Шифрування повідомлень, що передаються, некриптостійке, щоб забезпечити конфіденційність, для **WebSocket** слід використовувати протокол **TLS** і схему **WSS**.

Безпека протоколу WebSocket

Проблеми безпеки, пов'язані з WebSocket API, мають фундаментальну основу, яка полягає в можливості встановити з'єднання між сторонами, не запитуючи дозволу в користувача; крім того, запит надсилається без сповіщення самого користувача. Атакуючому ж у такій ситуації достатньо виконати JavaScript код на стороні жертви, щоб змусити його встановити з'єднання з довільним сервером за протоколом WebSocket. З'єднання може бути використано атакуючим для обміну даними з жертвою. Таким чином, відбувається порушення вимоги безпеки "Безпечне управління сесіями" і "Контроль доступу", а також стає можливим порушення вимоги безпеки "Безпечне кешування". Оскільки не всі проксі-сервери коректно розуміють протокол WebSocket, зловмисник може змусити проксі кешувати нав'язані йому дані. Надалі ця вразливість застосовується для порушення інших вимог безпеки, шляхом нав'язування JavaScript коду клієнту жертви.

Фундаментальна проблема породжує кілька загроз. Для цих загроз наводяться сценарії атаки, що показують те, як зловмисник може ними скористатися.

Cross-Site WebSocket Hijacking

Протокол WebSocket використовує Origin-based модель безпеки під час роботи з браузерами. Інші механізми безпеки, наприклад SOP (Same-origin policy), WebSocket не застосовуються. RFC 6455 вказує, що при установці з'єднання сервер може перевіряти Origin, а може і ні. Поле заголовка **Origin** у рукостисканні клієнта означає походження скрипта, який встановлює з'єднання. Вразливість **CSWSH** пов'язана зі слабкою або невиконаною перевіркою заголовка **Origin** у рукостисканні клієнта. Це різновид вразливості підробки міжсайтових запитів (**CSRF**) лише для **WebSocket**. Якщо програма **WebSocket** використовує файли **cookie** для керування сеансами користувача, зловмисник може підробити запит на рукостискання за допомогою атаки **CSRF** і контролювати повідомлення, що надсилаються та одержуються через з'єднання **WebSocket**. Сторінка зловмисника може надсилати довільні повідомлення на

сервер через з'єднання та зчитувати вміст повідомлень, отриманих назад із сервера. Це означає, що, на відміну від звичайного **CSRF**, зловмисник отримує двосторонню взаємодію зі скомпрометованим додатком.
Захиститися від **CSWSH** можна двома способами:
- перевіряти заголовок **Origin** запиту на рукостискання **WebSocket** на сервері;
- використовувати індивідуальні випадкові токени (наприклад, **CSRF**-токени) у запиті на рукостискання та перевіряти їх на сервері.

Перелік посилань:

1. The WebSocket Protocol. RFC6455. URL: https://www.rfc-editor.org/rfc/rfc6455
2. Research and Defense of Cross-Site WebSocket Hijacking Vulnerability. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/9182458
3. WebSocket: Lightweight Client-Server Communications / Andrew Lombardi, 2015. - 144 с.
4. Cross-Site-WebSocket-Hijacking: https://svyat.tech/Cross-Site-WebSocket-Hijacking/
5. https://eir.zntu.edu.ua/bitstream/123456789/4877/1/MR_Lohvynenko.pdf

Врадін Клим Сергійович
Студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ПРОГРАМИ-ВИМАГАЧІ

Великі компанії щомісяця зазнають мільйонів кібератак. Оскільки кіберзлочинність стає все більш поширеною - цього року очікується, що її втрати становитимуть 6 трильйонів доларів, що робить її більш прибутковою, ніж уся світова торгівля нелегальними наркотиками. Ефективна кібербезпека вимагає постійних зусиль, які охоплюють не тільки безпеку додатків, тестування на проникнення та управління інцидентами, але й поведінку співробітників, ризики третіх осіб та багато інших потенційних уразливостей.

Ransomware - програма-вимагач, яка шифрує файли на комп'ютері жертви, вимагаючи за розшифрування грошей. По суті — мережевий черв'як, що самостійно розповсюджується в інтернеті та в локальних мережах через уразливість у ПЗ, особливо в Microsoft Windows.

Одна з найпопулярніших і найскладніших загроз, LockBit (група RaaS), зберігає свої позиції лідера серед загроз ransomware. Кожен з його варіантів, а саме LockBit 1.0, LockBit 2.0 та LockBit 3.0, завдав серйозних збитків та наслідків під час своїх шкідливих кампаній, і продовжує це робити.

Згідно зі звітом Digital Shadows, у II кварталі 2022 року LockBit була найактивнішим угрупуванням у світі кіберзлочинності, встановивши рекорд за найбільшою кількістю жертв (231) за квартал.

LockBit RaaS згодом перетворився на поширену загрозу. Експерти вважають, що ця група загроз продовжуватиме націлюватися на підприємства по всьому світу, вдосконалюючи свої можливості. Тому пропонується використовувати проактивні підходи до безпеки, такі як обмін інформацією про загрози в режимі реального часу для попереднього виявлення та отримання

інформації про такі загрози з перших рук [1].

Bitdefender, антивірусний бренд, якому довіряють понад 500 мільйонів користувачів у 150 країнах світу, є одним із провідних світових постачальників споживчих продуктів кібербезпеки та піонером у галузі антивірусного захисту. Цей бренд отримав безліч антивірусних нагород від провідних лабораторій онлайн-тестування, включаючи AV-Comparatives, AV-Test, PCMag та Anti-Malware Testing Standard Organization.

Топ 10 [2]:

1) Bitdefender;
2) Norton;
3) Total AV;
4) Panda;
5) ESET Internet Security;
6) McAfee;
7) Kaspersky;
8) Intego;
9) Avira;
10) Avast.

Перелік посилань:

1. Щоденні новини кібербезпеки CYWARE Social [Електронний ресурс]: https://cyware.com/news/lockbit-ransomware-the-most-active-global-threat-3474dd13
2. Топ 10 ПЗ для боротьби з ransomware 2022 року [Електронний ресурс]: https://www.antivirusguide.com/best-ransomware-protection/?lp=true&utm_source=google&utm_medium=cpc&sgv_medium=search&utm_campaign=6478205166&utm_content=77388860066&utm_term=%2Bransomware%20%2Bprotection&cid=380751417359&pl=&feeditemid=&targetid=kwd-53624185010&mt=b&network=g&device=c&adpos=&p1=&p2=&geoid=9061013&gclid=CjwKCAjwzNOaBhAcEiwAD7Tb6AgW05BEK-XRtuXVQBXWkMAhVDXtH3Kh8IqG6K2uRFQhZzA8kxA8dhoCpHwQAvD_BwE

Герніченко Гліб Дмитрович

Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ. АКТУАЛЬНІСТЬ ТА ПРОБЛЕМИ

Кібербезпека являє собою дуже комплексний та клопіткий комплекс заходів, що складається з численних аспектів. Безліч фахівців фактично щоденно працюють над створенням нових методів та заходів боротьби з кіберзагрозами, створюючи ефективні засоби захисту від шкідливого програмного забезпечення, розроблюючи актуальні політики безпеки та клопітно вивчаючи методи роботи кіберзлочинців. Проте, дуже часто можна побачити, що вся ця клопітка праця може анулюватись через банальні проґавини у дуже простих та на перший погляд очевидних речах. Однією з таких речей є грамотне управління ідентифікацією та доступом.

Ключові слова: інформаційна безпека, кібербезпека, IAM, інформаційна система, доступ користувачів, ідентифікація користувачів.

Управління ідентифікацією та доступом користувачів(IAM) – комплекс

заходів, що спрямовані на отримання санкціонованого доступу до ресурсів особою, що має право на отримання такого доступу, в правильний час та з суто позитивною метою[1]. Існує велика кількість засобів, які дозволяють розгорнути в інформаційні системі корпорації систему IAM, проте як би фахівці не намагались розроблювати надійні засоби контролю доступу та ідентифікації завжди присутній ризик нехтування політикою безпеки, помилки при розгортанні системи, або вдалих дій збоку злочинців.

В 2017 році компанія Deloitte, що консультувала великі державні та фінансові установи США та ще ряд мультинаціональних компаній сама стикнулася з хакерською атакою фактично через відсутність багатофакторної авторизації у власній інформаційній системі. Зловмисники просто зламали пароль облікового запису адміністратора, який мав доступ до усієї мережі корпорації. Також через відсутність багатофакторної авторизації в 2014 році постраждала компанія Home Depot, що є однією з найбільших корпорацій з питань нерухомості у США. Хакери вторглись у систему через зламаний акаунт вендора та просто втрутили у систему шкідливе програмне забезпечення, що викачувало дані та передавало їх зловмисникам. [2]

З наведених вище прикладів можна зрозуміти, що IAM хоча й на перший погляд є доволі очевидною технологією, що має бути втілена в інформаційну систему компанії однією з перших, але дуже часто через людський фактор є ігнорованою навіть у великих корпораціях. З цього можна зробити висновок, що проблема є актуальною та має постійно нагадуватись, задля того щоб керівництво компаній слідкувало за постійною актуалізацією та оновленням систем IAM.

Перелік посилань:

1. Gartner Glossary: Information Technology Glossary Identity and Access Management (IAM) . [Електронний ресурс] – Режим доступу: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

2. Manage engine. 3 Mange identity failures of the last decade [Електронний ресурс] – Режим доступу: https://download.manageengine.com/active-directory-360/data-breaches-due-to-poor-iam-strategy.pdf

Дигас Максим Віталійович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

За рахунок масової комп’ютеризації та інформатизації товарів і послуг суб’єкти підприємницької діяльності мають доступ до різноманітної інформації, і тим самим у них полегшуються процеси виробництва, управління і збуту продукції. Однак, останнім часом почастішали випадки електронного шахрайства та кіберзлочинності, що негативно відобразилося на бізнесі.

Гостра проблема інформаційної безпеки комерційних організацій набула важливого значення в сучасних умовах масового застосування комп’ютерних інформаційних систем. Відповідно, надійним засобом захисту підприємства від інформаційних загроз є створення дієвої та ефективної системи захисту

Ключові слова: електронне шахрайство, підприємницька діяльність, кіберзлочинність, захист підприємства, проблема інформаційної безпеки.

Перелік посилань:
1. Марков А.С. Менеджмент інформаційної безпеки: основні концепції. Питання кібербезпеки. 2014 №1 С.67-73

Якубович Ігор Віталійович
Студент групи БСДМ-41, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОЛБЕМИ КІБЕРБЕЗПЕКИ. ВИТІК ІНФОРМАЦІЇ.

Витік інформації в загальному плані можна розглядати як неправомірний вихід конфіденційних відомостей за межі організації або кола осіб, котрим ці відомості були довірені. По своїй сутності завжди припускає протиправне (таємне або явне, усвідомлене або випадкове) оволодіння конфіденційною інформацією, незалежно від того, яким шляхом це досягається.

Витік даних - це коли конфіденційні дані випадково стають доступними фізично, в Інтернеті чи будь-якій іншій формі, включаючи втрачені жорсткі диски або ноутбуки. Це означає, що кіберзлочинець може отримати несанкціонований доступ до конфіденційних даних без будь-яких зусиль.

Значна частина особистих даних інтернет-користувачів може бути використана кіберзлочинцями у шкідливих цілях або продана на чорних ринках.

Потрібно скоротити витік особистих даних інтернет-користувачів, таких як: інформації в соцмережах, електронних листах і месенджерах, інформації про онлайн-платежі, історії місцеперебувань, щоб вони не потрапили до рук зловмисників. Перераховані види інформації – це лише частина даних, які складають цифровий слід кожної людини. Повнота цього цифрового портрета залежить від конкретних звичок поширення особистої інформації та ставлення до конфіденційності інтернет-користувача. Значна частина ваших даних може бути використана кіберзлочинцями у шкідливих цілях або продана на чорних ринках. Навіть якщо ви вважаєте, що ваші дані нікого не цікавлять, в інтернеті жертвою кіберзлочинців може стати кожен. Однак, хороша новина полягає в тому, що існує досить багато способів зменшення свого цифрового сліду. Наявність ризиків зовсім не означає, що варто перестати використовувати інтернет-сервіси, але необхідно дотримуватися балансу між приватністю й зручністю.

Перший крок у зменшенні цифрового сліду - це перевірка основних налаштувань конфіденційності в соцмережах: хто саме може переглядати ваші публікації й особисті дані та скільки інформації вони можуть бачити. Далі необхідно очистити список друзів: почніть із видалення з друзів усіх незнайомців, яких ви навіть не пам'ятаєте, а потім переходьте до знайомих, яких ви не дуже добре знаєте, а також до людей, із якими перестали спілкуватися. Якщо ви думаєте, "яка різниця, хто бачить мої публікації?", насправді це має велике значення. З ваших соціальних мереж можна отримати багато інформації, яку потім можна використовувати у шкідливих цілях". Наприклад, відомо багато випадків, коли шахраї збирали інформацію про звички знаменитостей, відстежуючи їхні акаунти в Instagram, щоб пограбувати їхні будинки.

Більшість людей мають десятки, а може й сотні різних акаунтів в інтернеті - різні веб-сайти для покупок, фітнес-додатки, кулінарні сайти, ігри та багато

інших. Кожен із цих сайтів і додатків зберігає різні типи конфіденційної інформації, яка може зацікавити зловмисників, зокрема ім'я, дату народження й номер телефону.

Щоб полегшити процес реєстрації, сьогодні доступна технологія єдиного входу через облікові записи Google, Facebook або Apple. І оскільки майже ніхто не має повного списку всіх сайтів, магазинів і додатків, у яких реєструвався протягом багатьох років, опція єдиного входу може стати в нагоді. Незалежно від того, який саме обліковий запис ви використовували, усі вони дають можливість з'ясувати, які сторонні програми мають до нього доступ.

Як додають фахівці з кібербезпеки, ще один спосіб зменшити свій цифровий слід - це скасування підписок на електронні розсилки новин, які ви отримуєте. Багато підписок підключаються автоматично при створенні облікових записів у різних сервісах і інтернет-магазинах, які потім відправляють вам електронні листи з новинами й різними пропозиціями знижок на товари та послуги. Більшість людей не читають дрібний шрифт при реєстрації, а просто автоматично все підтверджують, щоб швидше її закінчити. Тому в кінцевому підсумку такі користувачі мають сотні непрочитаних рекламних листів. Після очищення пошти від непотрібних підписок, розумним кроком буде створення окремої адреси електронної пошти, яка буде використовуватися для покупок.

Процес мінімізації цифрового сліду не обмежується згаданими вище кроками. Ще одним важливим інструментом для зменшення цифрового сліду є віртуальна приватна мережа (VPN), яка працює як зашифрований тунель для вашого інтернет-трафіку і захищає Вас від відстеження. Ви також можете використовувати перевірку конфіденційності Google і інші інструменти, щоб побачити, які дані сервіс зберігає і припинити це за потреби. Крім цього, якщо вам цікаво дізнатися, яку інформацію про вас має Twitter або Facebook, ви можете завантажити копію всіх даних, яку вони зберігають.

Як повідомляв УНІАН, в Україні щодня фіксується близько 300 тис. нових кіберзагроз для інформаційної безпеки. При цьому, знайти хакерів-зловмисників украй складно, компаніям залишається лише проводити щохвилинні моніторинги на предмет виявлення кіберзагроз із метою їхнього подальшого блокування.

Перелік посилань:

https://www.unian.ua/science/kiberbezpeka-fahivci-dali-poradi-yak-skorotiti-vitik-osobistih-danih-v-interneti-novini-11390800.html

https://www.upguard.com/blog/data-leak#:~:text=A%20data%20leak%20is%20when,the%20sensitive%20data%20without%20effort

Капелюшна Тетяна Вікторівна
к.е.н., доцент, доцент кафедри управління інформаційною та кібернетичною безпекою
Стежко М.В. *студент групи УБД-41*
ДУТ, Київ, Україна

ІНФОРМАЦІЙНА СКЛАДОВА В УПРАВЛІННІ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

Безпека інформації та інформаційного поля у функціонування підприємств відіграє важливу роль, оскільки від захисту їх цілісності, достовірності залежать управлінські рішення, а отже й результати діяльності, тобто економічна безпека діяльності підприємства.

З кібернетичної точки зору, інформація - це все, що надходить у систему для управління. Інформація має відповідати характеристикам: надійність (реальна, достовірна, без помилок); своєчасність та актуальність (затримка в часі отриманої інформації уповільнює управлінський процес); повнота (смислове наповнення), тому має підлягати захисту, щоб відповідати заявленим характеристикам та мати цінність. Захищена інформація убезпечує підприємство від фінансових втрат через неналежне використання інформації або її зберігання.

Інформаційна складова в управлінні економічною безпекою підприємства нині відіграє важливу роль, оскільки в епоху цифровізації збільшуються масиви обробки даних, тому питанню її захисту потрібно приділяти належну увагу.

Ключові слова: інформація, інформаційна складова, економічна безпека підприємства, роль інформації у економічній безпеці підприємства.

На сьогодні інформація виокремлюється як фактор виробництва (доповнюються до факторів: земля, праця, капітал та підприємницькі здібності), оскільки інформація, яка отримана вчасно дозволяє реагувати на загрози та невизначеності, або ж на екзогенні виклики. Інформація з економічної точки зору дозволяє реагувати на зміни, що відбуваються на ринку, переорієнтовувати виробництво у відповідності до останніх тенденцій та вимог ринку.

Із зростанням ролі та значення інформації актуальним стає вислів: «Хто володіє інформацією, той володіє світом» (Нотан Ротшильд, уживаний також У. Черчіллем), який звучить, як гасло сьогоднішньої епохи цифрових технологій. Діджиталізація та інформатизація суспільства характеризується зростанням кількості інформації, збільшенням масштабів її опрацювання.

Щодня підприємства і організації оперують величезною кількістю інформації, і ця кількість постійно зростає, тому актуалізується питання збереження та конфіденційності інформації.

Нині хмарні сховища, які використовуються компаніями для збереження даних не гарантують їх надійність та доступність, оскільки файли користувачів перебувають на сервері і можуть бути звідти видалені без попереджень і згоди власників цих даних.

Доцільно притримуватися принципу децентралізації, коли зашифровані файли діляться на частини і зберігаються на жорстких дисках користувачів і в дата-центрах по всьому світу (переглянути, змінити інформацію не може навіть

власник дата-центру), тобто можна убезпечити дані компанії від неправомірного доступу до неї, викривлення достовірності інформації, порушення її цілісності.

Держава теж дбає про безпеку інформації (для вдосконалення та оптимізації електронної взаємодії органів влади та системи державних електронних реєстрів), так з кінця 2019 року уряд запустив «експеримент верифікації даних у реєстрах» з метою: зіставлення реєстрів; перевірки повноти та достовірності даних користувачів у наявних реєстрах; запровадження унікального електронного номеру для профайлу з персональними даними людини, який стане єдиним ідентифікатором; виправлення помилок та оптимізації реєстрів; впровадження електронного сервісу, який дозволить у подальшому заповнювати реєстри без помилок. [1, с. 23].

З точки зору управління підприємствами, інформація слугує підґрунтям для прийняття управлінських рішень та організації їх реалізації.

З кібернетичної точки зору, інформація - це все, що надходить у систему для управління нею, отже, має вона має відповідати характеристикам: надійність (реальна, достовірна, без помилок); своєчасність та актуальність (затримка в часі отриманої інформації уповільнює управлінський процес); повнота (смислове наповнення). Інформація має підлягати захисту для того, щоб відповідати цим характеристикам та мати цінність.

При оцінці економічної безпеки діяльності підприємства чільне місце належить інформаційній, як одній із базових складових безпеки.

Варто приділити увагу питанню захисту інформації та інформаційних потоків підприємства, проводити моніторинг можливих варіантів захисту в середовищі її поширення, особливо в режимі віддаленого доступу, проводити оцінку її захисту на кожному етапі роботи із нею з метою безпечного функціонування підприємств та управління його економічною безпекою.

Перелік посилань:

1. Цифрові трансформації в Україні. Рекомендації та першочергові кроки для розвитку цифрового потенціалу України відповідно до європейських тенденцій. Поліський фонд міжнародних та регіональних досліджень, 2020 – 76 с. [Електронний ресурс] – Режим доступу:http://eap-csf.org.ua/wp-content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf

Давиденко Ілля Миколайович
студент групи КСМ-51,
ФАІТ КНУБА, Київ, Україна

БЕЗПЕКА ТА ЗАХИСТ ДАННИХ У МОБІЛЬНИХ ДОДАТКАХ

Безпека данних мобільних додатків - це практика захисту даних у мобільних додатках, вашої цифрової особи від хакерських атак у всіх можливих формах. Це включає втручання, зворотне проектування, шкідливе програмне забезпечення, реєстратори ключів, атаки зловмисних додатків, крадіжки пристрою, несанкціонованого доступу або втрати мобільних пристроїв та інші форми маніпуляції або втручання.

Ключові слова: безпека даних, шкідливе програмне забеспечення, атаки зловмисних

додатків

Комплексна стратегія безпеки мобільних програм включає наступні технологічні рішення, такі як захист мобільних програм, а також передові методи використання та корпоративні процеси. Мобільну безпеку також називають бездротовою безпекою. У сучасну епоху кількість користувачів мобільних пристроїв значно зросла, тому дуже важливо запобігати ризикам, пов’язаним із мобільними пристроями. Як правило, смартфони викрадають, щоб отримати доступ до секретних даних у вашому мобільному телефоні. Завантажувати додатки, яка не є безпечними дуже небезпечно.

Мобільні додатки, пов'язані з бізнес-брендами, часто стають метою шахраїв, які використовують своїх клієнтів, дітей своїх клієнтів, або атакують сам бізнес. Якщо зловмисники націлені на пристрій користувача, наслідки можуть включати наступне:

- Крадіжка особистих даних
- Підміна номера рахунку
- Вкрадені облікові дані для входу
- Вкрадені та перепродані дані кредитної картки
- Несанкціонований доступ до бізнес-мереж

Переваги безпеки мобільних додатків

Мобільні додатки генерують дуже велику кількість даних про нас та наше життя. Тому забезпечення безпеки додатків для створення та використання цієї інформації має важливе значення. В іншому випадку небезпечні програми - простий шлях для зловмисного акту крадіжки та продажу вашої особистої інформації.

Є мобільні рішення, які можуть домогти зберегти інформацію:

- Підтвердження особистості

Підтвердження особи допомагає запобігти крадіжці зловмисником особистих даних користувачів та реєстрації облікових записів під їх ім'ям. Надійний процес перевірки особистості підтверджує, що користувач є тим, ким він є, та допомагає запобігти шахрайству зловмисником.

- Надійна автентифікація

Захоплення облікового запису – досить популярна проблема, бо паролі швидко застарівають. Надійні методи автентифікації гарантують, що лише законні користувачі отримують доступ до своїх облікових записів, а зловмисники не зможуть увійти до системи з поганими намірами.

- Біометрія

Біометрія - це ще один безпечний та зручний спосіб входу в мобільні програми, використовуючи дані, отримані від вашого власного тіла. Нема надійного способу визначити, хто вводить пароль. Розробник програми може лише визначити, чи введений пароль відповідає ключу пароля в серверній частині системи. Біометрія у свою чергу включає додатковий індикатор довіри, оскільки він підтверджує особу людини, яка пропонує біометричний зразок для перевірки. Тому що відбиток пальця, розпізнавання обличчя або сканування райдужної оболонки ока відображаються у реальному часі та підключаються до користувача у реальному часі.

Рекомендації щодо безпеки мобільних додатків:

- Проведіть навчання цифрової безпеки

  Навчіть свою команду розпізнавати проблеми безпеки та уникати ризикованої поведінки, виявляти фішинг та інші стратегії кібербезпеки. Потім попрактикуйте свої навички за допомогою неоголошених тестових фішингових листів, текстів та інших повідомлень.
- Випереджальний моніторинг несанкціонованих додатків

  Регулярно шукайте як на законних, так і на незаконних платформах додатків будь-які додатки, на яких вказано назву, логотип вашої організації або обмін повідомленнями. Зв'яжіться з платформою, щоб якнайшвидше видалити будь-які шахрайські програми.
- Забезпечте передові методи безпеки

  Кожен додаток слід розробляти з урахуванням вимог безпеки. Переконайтеся, що ваші розробники знайомі з кращими практиками та фреймворками безпеки мобільних додатків, такими як OWASP Mobile Top 10.

Перелік посилань:

1. https://www.ipl.org/essay/Essay-On-Mobile-Security-FCAV7KQ3RU
2. https://an-essay.com/mobile-phone-security
3. https://ivypanda.com/essays/mobile-security

Хуторний Владислав Ігорович
Студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ФІШИНГОВІ АТАКИ

В умовах сучасних реалій кібербезпека – одне з першочергових завдань, які потребують вирішення в Україні. За останні кілька років робилися неодноразові спроби дестабілізувати банківську систему країни та зламати бази даних державних органів. Зловмисники зацікавлені отримати доступ не лише до персональних відомостей українців, а й до їхніх банківських рахунків. Найпоширенішою причиною зливу особистої інформації стають погано захищені канали фінансових операцій через інтернет. Українські громадяни ризикують купуючи товари в неперевірених інтернет-магазинах або відвідуючи нелегальні онлайн-казино.

Фішинг (від англ. Phishing — видобування) — це вид інтернет-шахрайства, який полягає в крадіжці конфіденційних даних користувачів. Простіше кажучи, зловмисники «розводять» користувачів на те, щоб вони самі розкрили свої особисті дані, наприклад, номери телефонів, номери та секретні коди банківських карт, логіни та паролі електронної пошти та облікових записів в соціальних мережах. Для цього користувачам пропонують якусь послугу або можливість, яка приваблює їх до таких дій. Наприклад, користувачам соціальної мережі Instagram пропонують дізнатися, хто заходив на їх особисту сторінку (хоча насправді такої можливості сама соціальна мережа не надає), а клієнтам інтернет-магазинів пропонують товар з божевільною знижкою.

Інтерес зловмисників може викликати будь-яка інша конфіденційна інформація. Шахраї «вивуджують» дані користувачів під різними пристойними приводами: перевірка авторизації на сайті, необхідність «відписатися» від спаму в електронній пошті, оплата покупки за низькою ціною або з великою знижкою, необхідність встановити новий додаток.

Специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Для цього зловмисники оперують такими інструментами, як фішингові сайти, e-mail розсилка, фішингові landing page, спливаючі вікна, таргетована реклама. Користувач отримує пропозицію зареєструватися для отримання будь-якої вигоди або підтвердити свої персональні дані нібито для банківських або комерційних установ, клієнтом яких він є. Як правило, шахраї маскуються під відомі компанії, додатки соціальних мереж, сервіси електронної пошти. Електронна адреса відправника дійсно схожа на адресу знайомої користувачеві компанії. Наприклад, щоб замаскуватися під інтернет-магазин Aliexpress, шахраї шлють листи з адрес, що містять слово Alliexpress або Aliexxpress. Працює та сама схема, яка змушує людей купувати дешеві китайські кросівки таких «всесвітньо відомих брендів», як Pumma або Abibas. Зловмисники користуються низьким рівнем обізнаності користувачів, зокрема, незнанням елементарних правил мережевої безпеки. Перш за все, організаторів фішинг-атак цікавлять персональні дані, які дають доступ до грошей, тому жертвами фішингу можуть ставати не тільки окремі люди, а й банки, електронні платіжні системи, аукціони.

Приклади схем інтернет-фішингу:

1. Розсилка підроблених електронних листів, з проханням підтвердити логін і пароль. Зловмисники можуть заспамити повідомленнями мільйони адрес електронної пошти протягом декількох годин. Для цього бази попередньо купуються. Однак за такі дії передбачена кримінальна відповідальність, а сервери, з яких розсилається спам, обчислюють і банять, тому цей спосіб повільно відходить у минуле.
2. Шахраї створюють електронні листи з підробленим рядком «Mail From:», використовуючи недоліки в поштовому протоколі SMTP. Коли відвідувач відповідає на фішингові повідомлення, лист з відповіддю автоматично пересилається шахраям електронною поштою.
3. Фішингові схеми популярні при проведенні інтернет-аукціонів. При цьому товари виставляються на продаж через легальний інтернет-аукціон, однак кошти перераховуються через підроблений вебвузол.
4. Створення фішингових інтернет-магазинів. Товари продаються за викидними цінами або з великими знижками. Це приваблює відвідувачів і вони надають дані своїх банківських карт, не підозрюючи, що стають жертвою шахрайства [1].

Як розпізнати фішинг [2]:

1. Прохання підтвердити ваші особисті дані.
2. Адреса відправника не виглядає справжньою
3. Велика кількість граматичних помилок в тексті листа

4. Наявність підозрілих файлів, прикріплених до листа
5. Текст листа спрямований викликати паніку, поспіх
6. Увесь текст посилання міститься у зображенні
7. Неперсоналізоване привітання у листі

Перелік посилань:

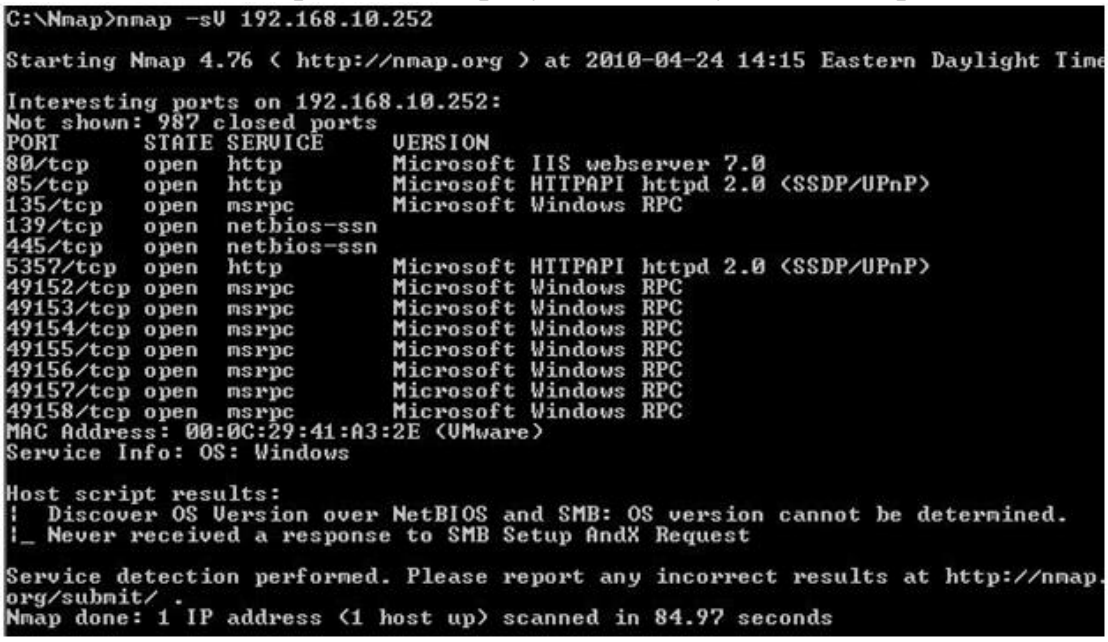
1. Що таке фішинг і фішингова атака [Електронний ресурс]: https://hostiq.ua/blog/ukr/internet-phishing/
2. Топ-7 способів розпізнати фішин [Електронний ресурс]: https://prozakupki.prom.ua/top-7-sposobiv-rozpiznati-fishingoviy-elektronniy-list/

Мурзін Ігор Васильович
студент групи БСДм-51, ННІЗІ ДУТ, Київ, Україна

СКАНУВАННЯ ЗА ДОПОМОГОЮ HONEYPOT

Уявіть себе на місці кіберзлочинця: ви займаєтеся тим, що кожного разу перевіряєте IP-адреси щодо наявності вразливостей і відкритих портів, чи не так? Отже, ви напевно запускаєте nmap і починаєте сканувати потенційну жертву. А тепер увага: якщо ви бачите результат, подібний до такого, це має вас насторожити:

Рис- 1. Підозрювальний результат сканування nmap



Як можна побачити, занадто багато відкритих портів відображаються в результаті сканування nmap. Сучасний сервер, можливо, оснащений фаєрволом, ніколи б не дав таких результатів сканування, так що можна вважати, що ви маєте справу з пасткою, підготовленою для кіберзлочинців. Іншим знаком, що наштовхує на думку про те, що ви маєте справу з пасткою, є вкрай застаріла

операційна система, що також фігурує в результатах сканування. Утиліта Netcat показує аналогічний результат: [1]

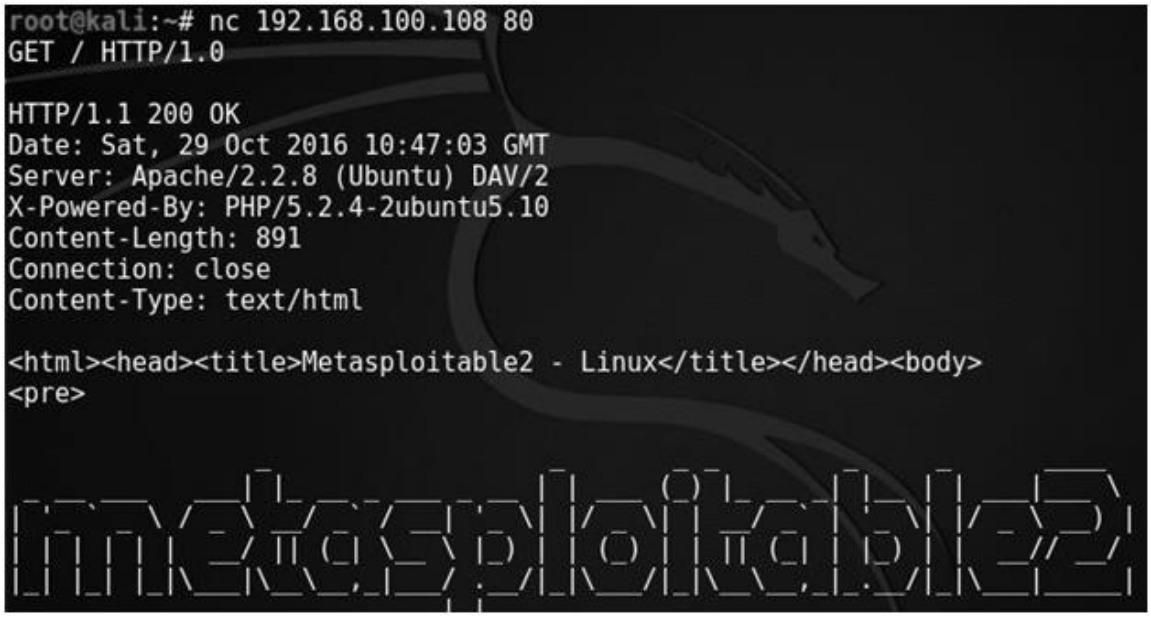


Рис.2 –Результат сканування утилітою Netcat

Тут можна спостерігати стару версію Apache. Deep web honeypots Можна зустріти кілька видів приманок, що серфять у глибокій павутині (deep web), але ми розглянемо два основних типи: honeypot, зроблений федеральними агентами, і honeypot, зроблений фішерами (кіберзлочинцями, що займаються фішингом).

Федеральні агенти запускають приманки, які симулюють ринки збуту наркотиків та дитячої порнографії, злочинці підключаються до них та їх легко спіймати.

Зловмисники, які займаються фішингом, можуть створити сайт, який маскується під легітимний, він надасть фальшиву форму для входу, за допомогою якої можна вкрасти ваші облікові дані чи іншу особисту інформацію.

Незважаючи на те, що приманки типу honeypot часто грамотно налаштовані і їх важко виявити, все ж таки є способи розпізнати, що ви маєте справу саме з ними. Насамперед завжди перевіряйте URL-адресу. Часто зловмисні URL-адреси відрізняються від легітимних тільки буквою, не лінуйтеся витратити час на ретельну перевірку URL-адреси.

Крім цього, якщо довірений веб-сайт починає запитувати у вас облікові дані або інформацію про гроші, чого раніше за ним не було помічено, це теж має вас дуже серйозно насторожити. Для простого користувача існують золоті правила, які дають змогу уникнути пасток: ніколи не кликати підозрілі посилання, що прийшли з неперевірених джерел, перевіряти наявність підозрілого сайту на DBL (список заблокованих доменів), де перераховані сотні шкідливих сайтів.

[2]

Приховуємо свою особу від honeypot Все це вже обговорювалося мільйон разів, але для перешкоди ідентифікації ви повинні дотримуватися таких правил:

- Завжди використовуйте VPN.
- Завжди використовуйте Tor.
- Придумайте фальшиву особу.
- Ніколи не надайте особисту інформацію, яка може допомогти пов'язати вашу фальшиву особу з вашою реальною.
- Не завантажуйте програмне забезпечення, зображення, PDF-файли або інші файли, якщо вони не отримані з вкрай надійного джерела.
- Якщо ви дійсно серйозно ставитеся до конфіденційності, використовуйте Whonix.

Honeypots у внутрішніх мережах

Припустимо, ви перебуваєте у внутрішній мережі і підозрюєте, що хтось запустив у ній honeypot. Як це можна виявити? На жаль, якщо ви хочете уникнути виявлення, ви не можете запустити сканування вразливостей або nmap, ви можете лише відстежувати підозрілу активність. Але можна зв'язати будь-яку IP-адресу з відповідним хостом за допомогою сканування ARP, а потім запустити Wireshark для сніфінгу запитів NetBios. Дуже малоймовірно, що запит NetBios надходить із honeypot. Таким чином, будь-який хост без імені NetBios потенційно може бути honeypot[3].

Висновки Ми коротко поговорили про те, як виявити працюючий honeypot, про їх особливості роботи в мережі та про те, як убезпечити себе від деяких приманок хакерів. Для повного розуміння теми все ж таки рекомендується встановити хоча б один honeypot, вивчити його налаштування і відзначити особливості.

Перелік посилань:

1. The Honeynet Project, ICnow Your Enemy: Learning about security threats // Addison-Wesley, 2004
2. Детальний посібник з Honeypot [Електронний ресурс] – Режим доступу https://habr.com/ru/company/alexhost/blog/528796/
3. Nawrocki M., Wahlisch M., Schmidt T. C., Keil C., Schonfelder J. A Survey on Honeypot Software and Data Analysis, CoRR, vol. abs/1608.06249, 2016. [1]

Бойко Анна Олександрівна
студентка групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ WEB-РЕСУРСІВ

Зростаюча популярність і складність архітектури веб-додатків може стати основним джерелом бізнес-ризиків, якщо власник ресурсу не подбає про якісної системи протидії хакерським атакам. За статистикою більше 80% випадків компрометації сайтів припадає на уразливості веб-додатків, що може виражатися як у блокуванні ресурсу, так і в доступі зловмисників до конфіденційної бази даних і фінансових транзакцій. Якісний захист веб-ресурсів – один з головних пунктів при формуванні результативної системи безпеки організації.

Число компаній, які застосовують веб-технології для підвищення продуктивності роботи і залучення нових клієнтів, зростає з кожним роком. Безсумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберзагроз. Так, компанія Symantec в своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зломі веб-сайтів зазвичай використовують вразливості веб-додатків, що працюють на сервері, або експлуатують деякі вразливості операційної системи, на якій працюють ці додатки. Наприклад, за допомогою атак типу XSS хакер може перенаправити запити користувачів на шкідливі веб-сторінки, а за допомогою SQL-ін'єкцій – витягувати з баз даних сайту різну конфіденційну інформацію.

У відповідь на масові зломи систем безпеки був створений консорціум OWASP – Open Web Application Security Project, це відкритий проект забезпечення безпеки веб-додатків. Однак і зловмисники, і фахівці в області кібербезпеки продовжують знаходити вразливості в веб-додатках, які можуть привести до серйозних втрат з боку бізнесу. Основною причиною більшості взломів в веб-додатках є написаний розробниками програмний код. Розробники можуть допускати помилки при написанні коду або не усвідомлювати всю важливість використання прийомів безпечного програмування – все це призводить до появи вразливостей в додатках [1].

Види атак і основні уразливості веб-додатків

Різноманітна архітектура, висока ступінь поширення та інтеграція web-додатків в мережеву інфраструктуру робить їх головною мішенню для хакерів. У своїй основі методи зловмисників залишилися практично незмінними і спрямовані на наступні уразливості:

- SQL ін'єкції;
- Міжстайтовая підробка запитів;
- Відсутність функції контролю доступу;
- Міжсайтовий скриптинг;
- Чутлива експозиція даних;
- Автоматизований перебір паролів (brute-force атаки);
- Міжсайтовая підробка запитів;
- Віддалений і локальний інклуд;
- Неперевірений перехід і редирект.

Якщо на стадії розробки програми не були виявлені аномалії в роботі, то навіть низькокваліфікований хакер без використання спеціалізованих засобів може скомпрометувати систему безпеки мережі. Часто одного браузера достатньо для здійснення зловмисних цілей і злому web-додатки.

Окремо варто сказати про так звані уразливість нульового дня. Вони специфічні для кожного окремого додатка і про їх існування стає відомо ще до моменту розробки захисних механізмів. Завдяки уразливість нульового дня зловмисники можуть протягом кількох місяців експлуатувати пролом у захисті

програми, так як на виявлення, локалізацію та усунення проблеми службам інтернет безпеки доводиться витрачати забагато часу.

Із завданням результативного протидії 0day-погроз не зможе впоратися стандартний метод сигнатурного аналізу даних. Класичні системи захисту не в змозі виявити заздалегідь не сконфігуровані патерни і сигнатури, тому рекомендується віддати перевагу машинного навчання і проактивним технологій (аналіз поведінки, емуляція коду, евристичний аналіз), які працюють на запобігання зараження шкідливим ПЗ [2].

Тест на проникнення

Важливий організаційний момент при побудові системи захисту веб-додатків – тест на проникнення. Саме він стане оптимальним способом перевірки захищеності інформаційної системи за допомогою імітації спрямованих атак. Тест на проникнення дає можливість оцінити захищеність інформаційної системи від несанкціонованого впливу, використовуючи різні моделі вторгнень. Тест на проникнення для веб-додатків фокусує свою увагу виключно на оцінці рівня захисту веб-додатків. Процес складається з активного аналізу додатків і пошуку в них вразливостей, технічних помилок або інших проблем. Інформацію про всі слабкі місця відображається в підсумковому звіті [1].

Міжмережевий екран для веб-додатків

Як можна здогадатися з назви, пристрої WAF (Web Application Firewall) розроблені для усунення вразливостей тільки в рамках веб-додатків. В цьому їх слабкість, але в тому числі і перевага, так як WAF рішення (віртуальні або апаратні) справляються з завданням усунення несправностей у веб-застосунках на порядок краще IPS і NGFW.

WAF функціонує як проксі-сервер і, аналізуючи протоколи HTTP/HTTPS, пропускає тільки безпечні запити від користувачів. Виявлення аномалій в роботі додатків проводиться як за допомогою класичного сигнатурного аналізу з постійно оновлюваною бібліотекою шкідливих сигнатур, так і, що важливо, з допомогою машинного навчання. Інтелектуальна система виявлення атак працює в автоматизованому режимі і завдяки тонкій настройці під кожне окреме застосування може без участі програмістів випустити пакет виправлень для системи і захистити сайт навіть від атак нульового дня.

Установка Web Application Firewall – це ефективне рішення для протидії атакам хакерів на веб-додатки. Але не варто забувати, що при значній кількості переваг пристрою WAF являють собою робочий інструмент, результативність якого багато в чому залежить від якісного адміністрування і розробника [2].

Перелік посилань:

1. Кращі рішення для захисту сайтів та web-додатків [Електронний ресурс] – режим доступу: http://softkb.com.ua/krashhi-rishennya-dlya-zahystu-sajtiv-ta-web-dodatkiv/

2. Захист веб-додатків: чому це важливо? [Електронний ресурс] – режим доступу: https://itbiz.ua/statti-ta-obzori/zaxist-veb-dodatkiv-chomu-ce-vazhlivo/

Кухар Олександр Павлович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

ВРАЗЛИВОСТІ ЛАНЦЮГА ПОСТАВОК ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вразливості ланцюгів поставок програмного забезпечення – це справжній виклик для галузі кібернетичної безпеки. Вони показують важливість захисту як кожного об'єкта окремо, так і окремих їх груп та всіх об'єктів в цілому. Успішна атака на одну ланку ланцюга може скомпрометувати весь ланцюг аж до кінцевого споживача.

Ланцюги поставок все частіше стають початковим вектором атаки. Про це свідчить звіт компанії Verizon «2022 Data Breach Investigations Report», в якому компанія зазначає, що 62% з досліджених ними проникнень сталися в результаті компрометації ланцюга поставок [1, с. 7].

Повторне використання кодової бази – це стандартна практика при розробці програмного забезпечення. Розробники спираються на компоненти свого інструментарію, такі як стандартна бібліотека транслятора певної мови програмування, сам транслятор, інструменти збірки та дистрибуції програмного забезпечення, використовують сторонні бібліотеки, користуються сервісами керування версіями, репозиторіями, створюють вузли розповсюдження оновлень і тому подібне. Інструменти, якими користуються розробники, стандартні та сторонні бібліотеки можуть бути створені як цим розробником, так і сторонніми розробниками – постачальниками відповідних інструментів та послуг. Сторонні розробники, своєю чергою, можуть мати власних постачальників інструментів для реалізації своєї діяльності, а останні – своїх постачальників. Сукупність таких постачальників і називають ланцюгом поставок.

Успішні атаки на ланки ланцюга поставок можуть призвести до компрометації великої кількості організацій, яким ці ланки надають послуги, і які, своєю чергою, можуть виступати ланками в інших ланцюгах поставок. Таким чином компрометація однієї ланки ланцюга, ставить під загрозу весь поточний ланцю аж до кінцевого споживача. Компрометацію ланок ланцюга можна порівняти з латеральним рухом зловмисника мережею після подолання засобів захисту мережевого периметру.

Виділяють такі типи атак на ланцюги поставок [2]:

- Скомпрометовані інструменти побудови програмного забезпечення чи інфраструктура оновлення;
- Вкрадені сертифікати підписування коду або підписані від імені компанії шкідливі додатки;
- Скомпрометований спеціальний код, доставлений в апаратне забезпечення чи компоненти прошивки;
- Попередньо встановлене на пристроях (камерах, USB, телефонах та інших) шкідливе програмне забезпечення.

Можливі вразливості, внесені зловмисником чи такі, що виникли природним чином, в використовуваних компонентах, отриманих від сторонніх постачальників, ставлять перед розробником непрості питання:

- Якщо в результаті тестування програмного продукту було виявлено вразливість, пов'язану з використанням стороннього компонента, то що стало причиною її виникнення: наявність стороннього компонента, чи неправильне його використання розробником?
- Якщо вразливість в продукті виникла через наявність стороннього компонента, це означає що вразливим є цей компонент, а тому потрібно зрозуміти хто повинен виправити вразливість: розробник продукту (якщо він має змогу це зробити), постачальник стороннього компонента, чи обидві сторони?
- Якщо розробник продукту може виправити вразливість своїми силами, чи зобов'язаний він повідомити постачальника стороннього компонента про виявлену вразливість?
- Якщо розробник продукту виправив вразливість у своєму продукті, а також сповістив постачальника стороннього компонента про виявлену в такому компоненті вразливість, і постачальник випустив оновлення компонента з виправленням вразливості, то чи потрібно розробнику продукту використовувати оновлений компонент?

Відповіді на зазначені вище питання матимуть вплив не лише на робочий процес розробників програмних продуктів, але й на складність реалізації процесу патч-менеджменту в організаціях.

Наразі всі проблеми в області вразливостей та атак на ланцюги поставок не вирішені. Компанія Microsoft для захисту від атак на ланцюги поставок рекомендує наступне:

- Підтримуйте безпечну інфраструктуру збірки та оновлення
- Створіть засоби оновлення програмного забезпечення в межах життєвого циклу програмного забезпечення
- Розробіть порядок реагування на інциденти атак на ланцюги поставок

В цілому, вразливості ланцюгів поставок програмного забезпечення ставлять складні питання перед спеціалістами з кібернетичної безпеки та показують наскільки важливою є безпека не лише окремої компанії, а й всіх компаній разом.

Перелік посилань:

1. Звіт компанії Verizon // 2022 Data Breach Investigations Report // URL: https://www.verizon.com/business/resources/T1db/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
2. Supply chain attacks. Posted on October 20, 2022 [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware

Павлюк Артем Вікторович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ЛОГІЧНА БОМБА

Логічна бомба це програма, яка запускається за певних часових або інформаційних умов для здійснення зловмисних дій. Такі програми часто зустрічаються в різних вірусах по типу хробаків, троянів та тому подібних. До логічних бомб як правило відносить код, який призводить до не повідомлених заздалегідь наслідків для користувачів. Такі програми є загрозою для конфіденційності даних та збереження їх цілісності.

Ключові слова: логічна бомба, кібербезпека, конфіденційні дані, цілісність даних.

Однією з проблем збереження даних компанії є логічні бомби. Зловмисник може непомітно занести вірус з логічною бомбою на сервери компанії. Це все може робитись для масового саботажу багатьох компаній в один момент. Також це може бути направлено на момент заключення певного контракту компанією, щоб вона зазнала значних втрат, як матеріальних так і репутаційних. Занесення вірусу може бути не лише зовні а і з середини компанії, якщо працівник має достатній доступ він зможе занести вірус на сервер замаскувавши його під оновлення системи або ж допоміжних програм, зазвичай приводом до застосування такої програми є озлобленість працівника на компанію або якщо працівник працює на компанію конкурента[1]. Завдяки такому, після проведення атаки зловмисника буде важче виявити, бо якщо активація була проведене через кілька років після занесення програми на сервер, то знайти цю інформацію буде дуже складно.

На що ж здібні логічні бомби, та чому їх потрібно остерігатись ?

Логічні бомби можуть активувати різні вірусні програми в самий непідходящий момент. Наприклад при DDOS атаці може бути активований вірус який менш помітно витягне конфіденційну інформацію та зможе передати інформацію зловмиснику.

Також однією з проблем може бути те що код логічної бомби може бути доданий до якоїсь нормальної програми, тому зловмисник може зробити все так що жертва сама завантажить програне забезпечення з вбудованим вірусом. Такі атаки більш націлені на звичайних користувачів для створення наприклад ботнет мережі, або ж на когось одного для атаки на конфіденційні дані персонального комп’ютера жертви.

Однією з таких проведених атак є атака проти Південної Кореї, внаслідок дії логічної бомби було стерто інформацію на жорстких дисках і головних завантажувальних записах, одночасно принаймні в 3 банках та 2 медійних компаніях[2]. Також атака цього типу була проведена на «АВТОВАЗ», він став першим підприємством в СРСР, на якому в листопаді 1982 року з допомогою логічної бомби в комп'ютерній програмі (автор — програміст УВП), внаслідок чого був зупинений конвеєр.

Перелік посилань:

1. Розуміння про логічну бомбу [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Логічна_бомба#cite_note-7

2. Атака проти Південної Кореї 20 березня 2013 [Електронний ресурс] – Режим доступу: https://web.archive.org/web/20140104132246/http://www.wired.com/threatlevel/2013/03/logic-bomb-south-korea-attack/

Бондар Іван Володимирович
Студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ЗАХИЩЕНІСТЬ ХМАРНИХ ТЕХНОЛОГІЙ

В сучасному світі хмарні технології все частіше починають використовуватися для різних цілей та потреб, до того ж їх використовують як звичайні поодинокі користувачі так і цілі організації та державні структури, школи, університети та інші. За допомогою цих ресурсів люди мають можливість використання обчислювальних ресурсів і пам'яті спільного пулу віддалених серверів, усуваючи проблеми масштабованості, хмарні обчислення забезпечують практично необмежену потужність, що в свою чергу може зацікавити зловмисників, які виявлять намір перехопити конфіденційні данні, підмінити їх, використати проти власника або багато чого іншого.

Хмарні ресурси надають людям доступ до апаратних та програмних активів, які більшість користувачів малого і навіть середнього бізнесу не змогли б собі дозволити. Для виконання хмарних обчислень використовують центри обробки даних (ЦОД), що являють собою сукупність серверів, які розміщені в одній мережі. Метою створення ЦОД є підвищення ефективності та захищеності. Для забезпечення достатнього рівня захисту центрів обробки даних використовується мережевий та фізичний фільтри та системи моніторингу активності в мережі. Крім того, важливо забезпечити відмовостійкість і надійне електроживлення ЦОДу. На даний момент ринок насичений різними рішеннями щодо захисту серверів і ЦОД від різноманітних загроз а також атак. Проте, кількість цих завдань значно збільшилась внаслідок поступової заміни апаратних систем, що вважались класичними, на віртуальні платформи. У зв’язку з цим, до вже відомих типів загроз додалися складності, пов’язані з контролем хмарного середовища, трафіку між гостьовими машинами та розмежуванням прав доступу. З’явились більш суворі вимоги зовнішніх регуляторів, а також розширилися внутрішні питання щодо політики захисту ЦОД. Станом на сьогодні, до роботи ЦОД висуваються суворі вимоги щодо закриття технічних питань та питань, пов’язаних з їх безпекою. Наразі практично всі компанії, що використовують дані системи, на серйозному рівні зайнялися питаннями посилення безпеки в них, хоча ще декілька років назад інтерес був лише теоретичний. Особливо гостро питання безпеки постають для бізнес-систем та додатків. Головною причиною масштабного перенесення більшості систем на хмарні сервіси стала віртуалізація. Звісно ж, разом з цим, постає ряд завдань щодо забезпечення безпеки в новому середовищі. Це вимагає особливого підходу. Більшість загроз вже достатньо вивчені та для них розроблені заходи протидії. Однак, слід провести адаптацію цих заходів для використання в хмарному середовищі. Одною з перших проблем з безпеки, яка виникає – це контроль та управління

хмарними сервісами. Адже відслідкувати всі ресурси сервісів, віртуальних машин, процесів – досить важка справа. Даний тип загроз є високорівневим, так як він пов'язаний з керуванням безпосередньо хмарним середовищем, як єдиною інформаційною системою, отже для нього необхідно налагоджувати індивідуальну систему захисту. Для цього використовують модель управління ризиками для хмарних інфраструктур. За основу забезпечення фізичної безпеки взятий суворий контроль фізичного доступу до всіх елементів даної інфраструктури. Основою мережевого захисту є міжмережевий екран та захист від вторгнень. Під використанням міжмережевого екрану розуміють роботу з фільтрації, метою якої є розмежування внутрішніх мереж ЦОД на підмережі з різним рівнем довіри. До наявних атак на хмарне середовище відносять наступні:
- традиційні атаки на програмне забезпечення;
- функціональні атаки на елементи хмарної інфраструктури;
- атаки, що спрямовані на клієнта хмарного середовища;
- атаки на контролер середовища (гіпервізор);
- атаки на системи керування.

Ефективна архітектура безпеки хмарного середовища має визначати та боротись з цими атаками. Вирішенням проблем безпеки стають такі рішення:
- шифрування даних, що зберігаються;
- захист даних при передачі;
- аутентифікація користувачів;
- ізоляція користувачів один від одного.

Таким чином, хмарні технології – це дуже перспективний напрямок, що постійно розвивається та позитивно впливає на майбутнє вдосконалення інформаційних технологій. А отже і питання безпеки в цьому середовищі буде залишатись завжди актуальним. Основними способами захисту інформації в хмарних технологіях є: шифрування, поділ даних і аутентифікація. Тільки при належному ставленні до захисту даних в хмарних середовищах можна стверджувати, що дані захищені.

Перелік посилань:

1. Бердник А. Угрозы облачных вычислений и методы их защиты [Електронний ресурс] / Алексей Бердник. – 2013. – Режим доступу до ресурсу: https://habr.com/ru/post/183168/.

2. Маньшин Г. Г. Парадигма безопасности облачных вычислений [Електронний ресурс] / Г. Г. Маньшин, В. А. Артамонов, Е. В. Артамонова // МАИТ. – 2020. – Режим доступу до ресурсу: http://itzashita.ru/oblachnyie-vyichisleniya/paradigma-bezopasnostioblachnyih-vyichisleniy.html.

3. Що таке хмарні технології і як вони можуть допомогти вашому підприємству [Електронний ресурс]: https://business.diia.gov.ua/cases/tehnologii/so-take-hmarni-tehnologii-i-ak-voni-mozut-dopomogti-vasomu-pidpriemstvu.

Ветлицька Олена Сергіївна
аспірантка кафедри Інформаційної та кібернетичної безпеки
ННІЗІ ДУТ,
Київ,
Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. СУЧАСНІ МЕТОДИ ВИЯВЛЕННЯ АВТОМАТИЗОВАНИХ АККАУНТІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

Проведено дослідження актуальних загроз від ботів, наведено ознаки ботів, за якими їх можна виявити та описано найбільш актуальні методи виявлення ботів у різних джерелах. Боти зазвичай імітують поведінку користувача або замінюють його. Боти є автоматизованими, тому вони працюють набагато швидше, ніж користувачі. Вони виконують корисні функції, наприклад обслуговування клієнтів або індексація пошукових систем. Однак роботи можуть бути шкідливими програмами, які використовуються для отримання повного контролю над комп'ютером.

Ключові слова: соціальні мережі, автоматизовані акаунти (боти).

В сучасному світі соціальні мережі мають великий вплив. За останніми оцінками 58.4% населення користуються соціальними мережами, а середнє використання соціальних мереж становить 2 години 27 хвилин на добу [1]. При цьому соціальні мережі використовуються не тільки для спілкування та отримання освітнього та розважального контенту, але й для отримання новин.

«Бот» (скорочено від «робот») – це програма, яка виконує автоматичні заздалегідь налаштовані завдання, що повторюються. Боти є автоматизованими, тому вони працюють набагато швидше, ніж користувачі.

Зі зростанням кількості користувачів зростає і кількість автоматизованих акаунтів (ботів) у соціальних мережах. Основними цілями створення автоматизованих акаунтів зазвичай є:

1. Автоматизований збір даних для використання на сторонніх ресурсах.
2. Використання облікових записів для впливу на громадську думку.
3. Використання облікових записів для шахрайства.

Присутність автоматизованих облікових записів у соціальних мережах загрожує і компаніям, які володіють соціальним мережам, та їх користувачам.

Компанії зазнають як іміджевих втрат - здешевлення рекламних контрактів та зниження потоку інвестицій, так і технічні – автоматизовані акаунти витрачають потужності, призначені для легітимних користувачів.

Користувачі, у свою чергу, зазнають як точкового шахрайства, так і перебувають під впливом масштабних інформаційних кампаній, покликаних впливати на громадську думку. Згідно з дослідженням [2], 45% публікацій про пандемію коронавірусу COVID-19 були створені акаунтами, які більше схожі на роботів, ніж на реальних користувачів.

Для виявлення та боротьби з автоматизованими акаунтами дослідники використовують різні підходи, методи та алгоритми.

Перелік посилань:

1. Global social media statistics research summary 2022. // URL: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social- media-research/. (27.05.2022)

2. Uyheng J., Carley K. Bots and online hate during the COVID-19 pandemic: Case studies in the United States and the Philippines // Journal of Computational Social Science – 2020. – № 3. P. 445-468. DOI: https://doi.org/10.1007/s42001-020-00087-4

Мужанова Т.М., *к.держ.упр, доцент, доцент кафедри управління інформаційною та кібернетичною безпекою ДУТ, м.Київ*
Легомінова С.В., *д.е.н., професор, завідувач кафедри управління інформаційною та кібернетичною безпекою ДУТ, м.Київ*

ОСНОВНІ ВІДМІННОСТІ МІЖ ВЕРСІЯМИ СТАНДАРТУ ISO/IEC 27002 2022 ТА 2013 РОКІВ

Розглянуто відмінності між міжнародним стандартом ISO/IEC 27002:2013 та його оновленою версію від 2022 року. Встановлено, що в ISO/IEC 27002:2022 внесені такі зміни: оновлено назву та словник у контексті кібербезпеки та захисту даних, удосконалено структуру й запропоновано інший підхід до класифікації заходів безпеки, додані нові види заходів з урахуванням розвитку технологій інформаційної та кібербезпеки.

Ключові слова: ISO/IEC 27002:2022, ISO/IEC 27002:2013, відмінності між ISO/IEC 27002:2022 та ISO/IEC 27002:2013.

Міжнародний стандарт ISO/IEC 27002 пропонує кращі практичні поради щодо менеджменту інформаційної безпеки для організацій усіх типів і розмірів, встановлює керівні рекомендації та загальні принципи для ініціювання, впровадження, підтримки та вдосконалення системи менеджменту інформаційної безпеки на основі вимог стандарту ISO 27001.

На початку цього року Міжнародна організація зі стандартизації спільно з Міжнародною електротехнічною комісією презентували оновлену версію стандарту - ISO/IEC 27002:2022 [1], яка має низку суттєвих відмінностей від попереднього варіанту - ISO/IEC 27002:2013 [2].

По-перше, була змінена назва стандарту. Попередня версія стандарту мала заголовок «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою». Стандарт випуску 2022 року називається «Інформаційна безпека, кібербезпека та захист приватності. Заходи інофрмаційної безпеки (англ. Information security, cybersecurity and privacy protection - Information security controls), що свідчить про зосередження основної уваги на проблеми забезпечення кібербезпеки та захисту даних.

З огляду на це у перелік термінів стандарту внесено поняття, пов'язані з персональними даними (PII – Personally Identifiable Information) та деякими

аспектами кібербезпеки, зокрема безпекою кінцевих точок.
По-друге, внесено зміни до структури документа, представлено заходи управління безпекою (controls) на основі простої класифікації та пов'язаних критеріїв (attributes).
Діючий стандарт значно довший за попередню версію (164 та 80 сторінок відповідно), а самі заходи з управління безпекою змінено й оновлено. Деякі заходи було об'єднано або видалено, а деякі додано. Так, ISO 27002:2013 представляв 114 заходів безпеки, об'єднаних у 14 категорій, серед яких, наприклад, політики інформаційної безпеки, управління активами, контроль доступу, мережева безпека тощо. Натомість у версії стандарту 2022 року перераховано 93 заходи безпеки, які згруповані в 4 блоки: робота з людьми (8 заходів); організаційний (37 заходів); технологічний (34 заходи); фізичний (14 заходів).
Зміни у загальній структурі стандарту показані на рис.1.

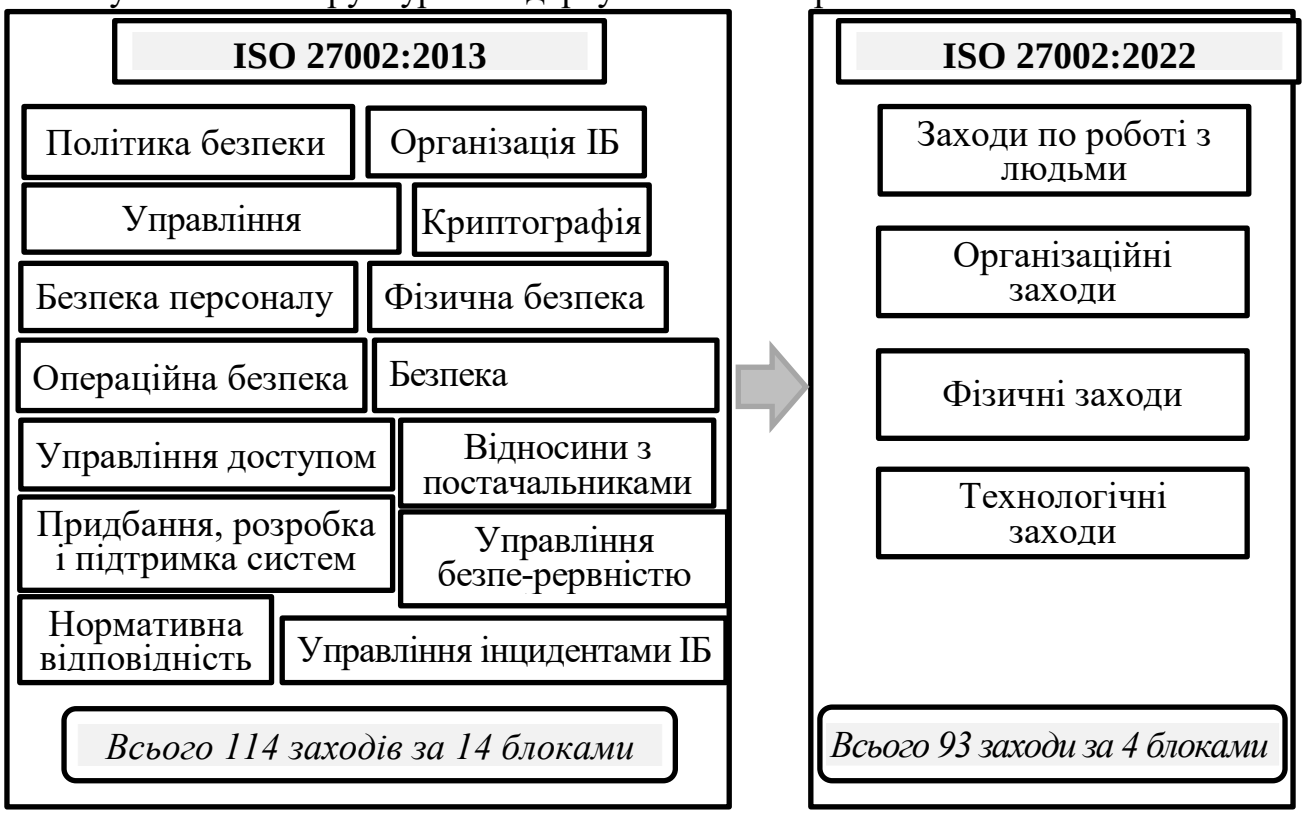


Рис.1 - Зміни у стандарті ISO 27002:2022 у порівнянні з версією 2013 року

По-третє, до рекомендованих заходів управління безпекою в оновленому стандарті додані цілком нові заходи, серед яких розвідка загроз; інформаційна безпека використання хмарних сервісів; готовність ІКТ до безперервності бізнесу; моніторинг фізичної безпеки; управління конфігурацією; видалення інформації; маскування даних; запобігання витоку даних; моніторингова діяльність; веб-фільтрація; безпечне кодування.
Крім цього, в оновленій версії стандарту введено класифікацію заходів управління безпекою за декількома критеріями:

- тип заходів (запобігання, виявлення, коригування);
- властивості інформаційної безпеки (конфіденційність, цілісність, доступність);

- концепції кібербезпеки (визначення, захист, виявлення, реагування, відновлення);
- операційні можливості (управління активами, безпека додатків, управління загрозами і вразливостями, відповідність нормативним вимогам тощо);
- сфери (domains) безпеки: управління вищого рівня та екосистема (Governance and Ecosystem); захист (Protection); оборона (Defence); стійкість (Resilience).

Таким чином, у результаті порівняння двох версій міжнародного стандарту ISO/IEC 27002 від 2013 та 2022 року вставновлено, що в останній акцентовано увагу на проблемах кібербезпеки та захисту даних і відповідних чином оновлено назву та словник, удосконалено структуру й запропоновано інший підхід до класифікації заходів безпеки, додані нові види заходів з урахуванням розвитку технологій інформаційної та кібербезпеки.

Перелік посилань:
1. ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. 80 p.
2. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls. 164 p.

Киричук Анна Олександрівна
Студентка групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

ЦЕНТР ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ (SOC). НАПРЯМКИ І ТЕХНОЛОГІЇ ЗАХИСТУ

Взломи і масові витоки чутливих даних (наприклад, облікові записи користувачів, номери банківських карт та ін.) є трендом останніх років у всьому світі. При цьому, за статистикою Cisco, на виявлення злому мережі в організації може йти до півроку. Таким же трендом останнім часом є і поняття SOC (Security Operations Center), на який покладають завдання по боротьбі з цільовими кібератаками. Центр управління безпекою (SOC) - це централізована функція всередині організації, що використовує людей, процеси і технології для постійного моніторингу та поліпшення стану безпеки організації за допомогою запобігання, виявлення, аналізу та реагування на інциденти кібербезпеки.

SOC діє як концентратор або центральний командний пункт, збираючи дані телеметрії з усієї IT-інфраструктури організації, включно з її мережами, пристроями, пристроями та сховищами інформації, хоч би де ці активи були розташовані. Поширення просунутих загроз вимагає збору контексту з різних джерел. Тобто, SOC - це точка кореляції для кожної події, зареєстрованої в організації, що відстежується. Для кожної з цих подій SOC повинен вирішити, як вони будуть управлятися і діяти.

Функція оперативної групи з питань безпеки і, часто, оперативного центру безпеки (SOC), полягає в цілодобовому моніторингу, виявленні, розслідуванні та реагуванні на кіберзагрози. Оперативні групи з питань безпеки відповідають за моніторинг та захист багатьох активів, таких як інтелектуальна власність, персональні дані, бізнес-системи та цілісність бренду. Як виконавчий компонент загальної системи кібербезпеки організації, оперативні групи з питань безпеки

виступають центральним пунктом співпраці в скоординованих зусиллях з моніторингу, оцінки та захисту від кібератак.

SOC, як правило, будується на основі зіркоподібної архітектури, де промені цієї моделі можуть включати різноманітні системи, такі як рішення для оцінки вразливостей, системи управління, ризиків і відповідності (GRC), сканери додатків і баз даних, системи запобігання вторгненням (IPS), аналітика поведінки користувачів і організацій (UEBA), виявлення і усунення наслідків кібератак (EDR), а також платформи розвідки загроз (TIP).

SOC виконує такі основні функції:

1. Проведення інвентаризації наявних ресурсів.
2. Підготовка та профілактичне обслуговування.
3. Безперервний проактивний моніторинг.
4. Ранжування та управління оповіщеннями.
5. Реагування на загрози.
6. Відновлення та усунення наслідків.
7. Ведення журналів.
8. Розслідування першопричини.
9. Доопрацювання та покращення безпеки.
10. Управління комплаєнсом.

Ефективна видимість та управління загрозами спирається на багато джерел даних, але може бути важко відсортувати корисну та своєчасну інформацію. Найбільш цінними даними виявилися дані про події, отримані за допомогою контрзаходів та IT-активів, індикатори компрометації (IoC), отримані внутрішньо (за допомогою аналізу шкідливого програмного забезпечення) та ззовні (за допомогою каналів розвідки загроз), а також системні дані, доступні з датчиків (наприклад, хост, мережа, база даних і т.д.).

Такі джерела даних – це не просто вхідні дані для управління загрозами. Вони додають контекст і роблять інформацію цінною і дієвою для більш точної, достовірної і швидкої оцінки в ході ітеративних і інтерактивних зусиль з управління загрозами. Цей потік інтегрує IT-операції та команди і інструменти безпеки в реагування на інциденти, коли відбувається критична подія.

Всі ці оцінки допоможуть визначити пріоритети, де необхідно збільшити інвестиції або зменшити тертя, щоб забезпечити відповідність впровадження управління загрозами поставленим цілям. Консультанти і тести на проникнення можуть допомогти оцінити стратегію і організаційну зрілість, а також перевірити реакцію системи безпеки на атаки, щоб отримати поточну оцінку здатності організації виявляти і стримувати зловмисні події.

Статистика з минулих звітів Micro Focus SIOC показує, що тільки 25% проектів створення SOC домоглися виконання поставлених цілей. При цьому, найпоширеніші помилки це:

- Недоліки підтримки.
- Більша увага на технічні рішення.
- Порушення принципу "від простого до складного".

- Відсутність фокусу.
- Відсутність процесного підходу.

Для досягнення найкращих результатів SOC повинен бути в курсі останніх розвідувальних даних про загрози та використовувати цю інформацію для вдосконалення внутрішніх механізмів виявлення та захисту. Як зазначає InfoSec Institute, SOC споживає дані зсередини організації та співвідносить їх з інформацією з ряду зовнішніх джерел, які надають уявлення про загрози та вразливості.

Перелік посилань:

1. ISO 18788 Security Operations Management System Training
2. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response.
3. ISO/IEC 27035:2011

Долинський Олександр Ігорович
Студент групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

КІБЕРБЕЗПЕКА КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Кібербезпека була основною опорою для структури інформаційної безпеки для підтримки конфіденційності, узгодженості та цілісності даних клієнтів, особливо коли йдеться мова про корпоративні інформаційні системи. Дані системи потребують високого рівня безпеки, адже це має вплив на кінцевих користувачів що використовують даний інформаційний портал. Безпечна та успішна платформа електронної комерції потребує надійної інфраструктури. Також, існує проблема відсутності довіри в багатьох сферах корпоративної діяльності, на що, безумовно вплинуло те, що клієнти нерідко можуть зустрічатися з порушенням їх інформаційної безпеки.

Безпека є однією з найважливіших змінних, які впливають на клієнтів, що залучені до співпраці з корпоративною інформаційною системою. Оскільки велика частина клієнтів, які користуються користуються будь-якими корпоративними інформаційними платформами (інтернет-магазини, компанії, що надають інформаційні послуги тощо) здебільшого набувають кращих знань щодо запобіжних заходів для збереження їх власної безпеки під час користування віддаленими інформаційними системи, проте, залишається частина, що знаходиться в групі ризику та все ще має початковий рівень проінформованості.

Освіта клієнтів та працівників корпоративних інформаційних систем завжди буде основним елементом архітектури безпеки будь-якої корпоративної інформаційної системи.

Стійкий до кібернетичних загроз бізнес поєднує в собі можливості кібербезпеки, безперервності бізнесу та стійкості підприємства. Застосування плавних стратегій безпеки для швидкого реагування на загрози може

мінімізувати шкоду та продовжувати працювати під час атаки. Для досягнення подібного стану слід впроваджувати інноваційні технологічні і не технологічні бізнес-моделі безпеки, це зміцнює довіру клієнтів і дозволяє фактично опрацьовувати потенційні загрози бізнесу в інформаційному середовищі.

Для досягнення вище описаних результатів є декілька порад:

1. Стимулюйте цінність завдяки новим інвестиціям. Лідери в питанні інформаційної безпеки додатково масштабують, додатково навчають і співпрацюють, щоб збільшити користь від інноваційних технологій. Більший масштаб – гнучкість масштабування, яка є дуже важливою для охоплення найбільш ефективних програм безпеки.
2. Тренуйтеся більше. Представлення нових інструментів означає, що коучинг має вирішальне значення, щоб спонукати до найефективніших з них. Швидкість, з якою організації усвідомлюють порушення безпеки, швидше для тих, хто надає вищий рівень навчання.
3. Співпрацюйте більше – організації, які найкраще співпрацюють у два рази краще захищаються від атак, ніж інші. Слід подумати про швидке масштабування та розгортання співпраці з іншими компаніями на ринку, в тому числі конкурентами, щоб зрозуміти, наскільки можуть бути ефективними інвестиції в нові технології безпеки, що полягають у підвищенні рівня виявлення загроз та ризиків, та їх подальшого опрацювання.

Ключові слова: кібербезпека, інформаційна безпека, безпечна інформаційна діяльність підприємства, попередження кібернетичних загроз

Перелік посилань:

1. Cybersecurity in a Digital Era. URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20in%20a%20digital%20era/Cybersecurity%20in%20a%20Digital%20Era.pdf

2. CYBERSECURITY BASICS. Cybersecurity for small business. URL: https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf

Катков Юрій Ігорович, *дтн, доцент кафедри Комп'ютерних наук*
Цибульник Сергій Сергійович
*студент групи КМДМ-51, ННІІТ**,** Київ, Україна*

ПЛАТФОРМА ПРОВЕДЕННЯ ПЕРЕВІРКИ ЗАХИЩЕНОСТІ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ МЕТОДАМИ RED TEAMING

У статті розглядається проблема застосування методології Red Teaming та тестування на проникнення. У світі кібербезпеки завжди є необхідність пошуку нових способів боротьби з загрозами, що розвиваються. Тому пошук передових рішень є актуальним та своєчасним. Це є основою боротьби з кіберзлочинцями. Робиться аналіз методів застосування. Показані переваги та недоліки цих методів, та де вони найкраще підходять для досягнення конкретних цілей. Надаються пропозиції щодо їх впровадження.

У світі кібербезпеки завжди є необхідність пошуку нових способів боротьби з загрозами, що розвиваються [1 ст.15]. Тому пошук передових рішень є основою боротьби з кіберзлочинцями. Звідси створення платформ кібербезпеки для проведення перевірки захищеності інтелектуальних систем, що забезпечує всебічну видимість, виявляє поверхню атаки, що постійно змінюється, дозволяючи фахівцям з безпеки розуміти і визначати пріоритети вразливостей, виявляти загрози і швидко реагувати на них, а також застосовувати правильні заходи безпеки в потрібний час для зниження ризиків – є актуальнім та своєчасним завданням. У цьому контексті застосування методології Red Teaming та методів тестування на проникнення залишається одним із перспективних напрямків. Але треба розуміти як їх ефективне застосовувати.

Сучасна методології Red Teaming включає набір методів, що забезпечують підвищення безпеки цільової системи. Перевагою методології Red Teaming є можливість описання процесів захисту чи сценаріїв атак, які перевіряють поточну безпеку системи організації, намагаючись зламати її як справжній хакер. Завдяки цим сценаріям атак можна візуалізувати стратегію безпеки системи та її реакцію на атакуючого. Це забезпечує ширше уявлення про стан безпеки організації, а саме включають: процеси тестування на проникнення, соціальну інженерію, фізичне вторгнення, експлуатацію прикладного рівня та експлуатацію мережевих служб. Методологія Red Teaming допомагає класифікувати всі пов'язані активи відповідно до рівня їх ризику. Це допомагає виявити всі проблеми безпеки та лазівки, що присутні в системі. Це також допомагає максимізувати віддачу від інвестицій, зроблених для забезпечення безпеки організації.

Процедури тестування на основі методів Red Teaming мають багато варіантів, кожен з яких підходить для різних умов або галузей. Це дозволяє оцінювати систему захисту організації, піддаючись кільком кібератакам. Допомагає організації дізнатися, наскільки безпечні її політики. Для реалізації такого підходу компанії або звертаються до власної IT-команди, щоб взяти на себе роль хакерів, або звертаються до зовнішньої групи експертів для отримання

об'єктивної та детальної інформації. Таким чином, методи Red Teaming допомагають оцінить, наскільки добре працює система безпеки організації під час атаки.

З іншого боку є методи тестування на проникнення (пентест). Тестування на проникнення – це метод оцінки безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника. Процес тестування на проникнення включає активний аналіз системи на наявність потенційних уразливостей, які можуть спровокувати некоректну роботу цільової системи, або повна відмова в обслуговуванні. Аналіз ведеться з позиції потенційного атакуючого. Він може включати активне використання вразливостей системи. Результатом роботи є звіт, що містить у собі всі знайдені вразливості системи безпеки, а також може містити рекомендації щодо їх усунення. Мета випробувань на проникнення – оцінити можливість його здійснення та спрогнозувати економічні втрати внаслідок успішного здійснення атаки. Випробування проникнення є частиною аудиту безпеки. Фахівець, який проводить випробування на проникнення, називається пентестером. Таким чином, результатом проведення випробування на проникнення, як правило, є звіт, що містить виявлені в ході аналізу вразливості та опціональні рекомендації щодо їх усунення.

В основі випробувань на проникнення можуть бути використані різні методики. Основними їх відмінностями є наявність інформації про систему, що досліджується. Вона може бути закритою (напівприкритою), відкритою або цільовою. При перевірці закритих систем (систем типу «чорний ящик») атакуючий не має початкових відомостей про пристрій цілі, що атакується. Початкове завдання такого виду перевірки — збирання необхідної інформації про розташування цільової системи, її інфраструктуру. При перевірці відкритих систем (доступна повна інформація про цільову систему) або (є лише часткова інформація) атакуючий може мати деякі початкові відомості про пристрій мети, що атакується. До цільових систем належать комп'ютерні системи з доступом до Інтернету. Випробування проникнення має проводитися до запуску цільової системи масового використання. Це дає певний рівень гарантії, що будь-який атакуючий не зможе завдати шкоди, прямої або непрямої роботи досліджуваної системи.

Звідси бачимо, що методи Red Teaming та тестування на проникнення мають свої переваги та недоліки та найкраще підходять для досягнення конкретних цілей. Наприклад, методологія Red Teaming прагне якнайшвидше проникнути всередину і отримати доступ до конфіденційної інформації. Для цього застосовуються методи, що імітують дії хакера та намагається уникнути виявлення. З іншого боку, тестування на проникнення має тенденцію виявляти якомога більше можливих ризиків або вразливостей та прогалин у конфігурації безпеки у певний час для системи. Тобто використовує виявлені проблеми та оцінює ризик, пов'язаний із уразливістю.

Відповідно до досліджень [2, 3, 4] процес тестування на проникнення зазвичай займає до 1-2 тижнів, тоді як отримання результатів за допомогою методології Red Teaming може тривати до 3-4 тижнів. При цьому Red Teaming не

шукає численних уразливостей у вашій системі. Натомість кожна атака приймає спосіб мислення хакера, який має обмежений час, щоб знайти і використовувати відразу доступні вразливості, які допоможуть їм досягти своїх цілей.

Таким чином, методологія Red Teaming – це практика енергійного тестування політик, планів, систем та припущень безпеки за допомогою змагального підходу. Моделювання атак хакерів робить методологію Red Teaming більш надійною, оскільки вона виявляє вразливості системи і реалізує її можливу експлуатацію як хакера. Комбінуючи такі процеси там, де це необхідно, методологія Red Teaming зламує цифрову безпеку компанії, щоб з'ясувати її найгірші сторони. У той же час тестування на проникнення є вибором для організації, безпека якої знаходиться на початковому етапі. Однак, якщо компанія шукає більш кращих політик безпеки та заходи щодо посилення безпеки, то тут треба застосовувати інші методи Red Teaming.

Ключові слова: кібербезпека, ***методологія Red Teaming, тестування на проникнення****.*

Перелік посилань:

1. Даник, Юрій Григорович. Національна безпека: запобігання критичним ситуаціям: монографія / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін ; Національна академія оборони України, Житомир. військ. ін-т радіоелектроніки ім. С. П. Корольова. - Житомир : Рута, 2006. – 386с.
2. Катков Ю. І. Аналіз причин критичних ситуацій в інформаційно-інтелектуальних системах//Зв'язок. – 2018. – №3(133) – С. 12-19. http://con.dut.edu.ua/index.php/communication/article/view/1999
3. What is Red Teaming? Benefits & Methodology. Updated on: March 9, 2022 // [Електронний ресурс] – Режим доступу URL: https://www.getastra.com/blog/security-audit/red-team-methodology/#:~:text=Red%20Team%20Methodology%20gives%20a,system%20against%20a%20real%20cyberattack
4. 5 Things Every Red Team Needs to Optimize Operations //[Електронний ресурс] – Режим доступу URL: https://www.netspi.com/resources/tip-sheets/5-things-every-red-team-needs-to-optimize-operations/

Побойний О.С
Державний Університет Телекомунікацій
Навчально-науковий інститут Захисту інформації

ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ВНУТРІШНІХ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Створення ефективної системи управління інформаційною безпекою є неможливим без чіткого визначення загроз інформації, що охороняється. Під загрозами інформації прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного володіння інформацією.

За джерелом походження загрози інформаційній безпеці можуть поділятися на внутрішні та зовнішні. Проаналізувавши можливості утворення внутрішніх та зовнішніх загроз, можна перерахувати їх в порядку зменшення імовірності реалізації:

- внутрішні загроз;
- зовнішні загрози;
- загрози, які створюють випадкові особи.

До внутрішніх загроз відносять дії (навмисні чи не навмисні) співробітників, що протидіють інтересам підприємства, наслідком яких може бути втрата інформаційних ресурсів, підрив іміджу компанії, виникнення проблем у відносинах з реальними чи потенційними партнерами.

Значна частина внутрішніх загроз реалізується за участі персоналу, то ж можна сказати, що головним джерелом загроз є працівники конкретної організації.

Таким чином внутрішні загрози можуть утворюватися внаслідок:

- непрофесійних дій працівників;
- низького стану виховної та профілактичної роботи в організації;
- недосконалої системи заробітної плати та стимулювання праці персоналу;
- порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації;
- психологічних та комунікаційних особливостей працівників;

Для нейтралізації внутрішніх загроз потрібно прийняти наступні заходи:

- організаційні заходи з захисту інформації;
- контрольно-правові заходи (контроль за виконанням персоналом вимог відповідних нормативних документів);
- інженерно-технічні заходи;
- робота з кадрами (підбір та навчання персоналу, підвищення їхньої кваліфікації);
- психологічні заходи (встановлення відео спостереження).

Отже, внутрішні загрози безпеки існують завжди і не залежать від ролі, місця, значення організації чи наявності зовнішніх загроз.

Тому потрібно серйозно звертати увагу на проблеми захисту інформації від внутрішніх загроз, адже для цього існують всі необхідні засоби як технічні так і організаційні.

Перелік посилань:

1. Ткачук Т., Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту, Право України № 3, 2011. – 366с.
2. Скиба В., Курбатов В. Керівництво по захисту від внутрішніх загроз інформаційної безпеки М.: видавництво Пітер, 2008. – 320с.
3. Скляренко А. Загрози конфіденційності інформації, пов’язані з персоналом, бізнес та безпека №1, 2010. – 92с.

Баленко О.А., *студентка групи УБДМ-61*
Державний університет телекомунікацій
м. Київ, Україна

СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В сучасному інформаційному середовищі вагомий внесок в структуризацію управління бізнес-процесами і процесами захисту підприємств становить створення та впровадження в дію так званих систем менеджменту інформаційної безпеки (СМІБ). СМІБ – це одна з основних частин загальної системи менеджменту, яка заснована на підході бізнес-ризиків при створенні, впровадженні, функціонуванні, моніторингу, аналізі, підтримці і поліпшенні інформаційної безпеки. Розробка і впровадження цієї системи здійснюється згідно встановленому стандартами порядку.

Метою інформаційного менеджменту є забезпечення ефективного розвитку комерційного підприємства за допомогою оперативного і гнучкого регулювання різних видів інформаційної діяльності (пошук, збір, аналіз, обробка, передача, зберігання та використання різної інформації) [1].

Організація повинна вводити, виконувати, використовувати, контролювати, переглядати, підтримувати і удосконалювати документовані положення СМІБ у рамках усієї бізнес-діяльності організації, а також ризиків, з якими вона стикається.

Для вирішення основних питань і завдань СМІБ було затверджено стандарт ISO 27001, який включає такі загальні процеси:

Планування – створення СМІБ;

Виконання – впровадження і використання СМІБ;

Перевірка – моніторинг і перевірка СМІБ;

Покращення – підтримка і вдосконалення СМІБ [2].

Першочерговим завданням СМІБ є забезпечення інформаційної безпеки і безпеки інформаційних технологій. З огляду на це було створено ще один стандарт для підтримки СМІБ - Стандарт BSI-100-2 «Методика впровадження системи менеджменту інформаційної безпеки IT». В цьому стандарті більше уваги приділяється не питанням управління і організації, а питанням стосовно інформаційних технологій, тобто більш технічним аспектам захисту, виявлення загроз і вразливостей, забезпечення безпечного мережевого обладнання і т.д.

Отже, зацікавлення підприємств у впровадженні СМІБ з часом лише зростає, оскільки необхідність у забезпеченні безпечного функціонування інформаційних систем підприємств буде завжди. Кожен директор зацікавлений в ефективному функціонуванні свого підприємства, тому і доцільність використання систем менеджменту з інформаційної безпеки є своєчасною для підприємств [2,3].

Перелік посилань:

1. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємства. 2016. С. 80-85.

2. Дорофеев А.В., Марков А. С. Менеджмент информационной безопасности: основные концепции. Вопросы кибербезопасности. 2014. С. 67-70.

3. Електронний ресурс. URL: https://refdb.ru/look/2806257.html

Якименка Юрія Михайловича
доцента кафедри УІКБ, ННІЗІ ДУТ, Київ, Україна

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ МЕНЕДЖМЕНТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Головною проблемою з кібербезпеки на сьогодні залишається створення ефективної системи менеджмента (управління) у області інформаційної безпеки (ІБ) – СМІБ (СУІБ). Це питання важливе не тільки для «молодих» компаній, що розбудовують свій бізнес із використанням сучасних інформаційних технологій управління, але й для організацій, що давно працюють на ринку, які приходять до необхідності модернізувати існуючу систему ІБ. Необхідність підвищення ефективності системи ІБ пов'язана в першу чергу із проблемами захисту інформації в сучасних умовах зростання негативніх впливів на інформаційні ресурси, процеси і засоби будь-якої організації (комерційної або державної). Пропонується розгляд послідовності створення системи ІБ, в тому числі і СУІБ організації в кілька етапів.
Ключові слова: інформаційна безпека, системи менеджмента, управління, СМІБ, СУІБ, ISO/IEC.

Відповідальність за формування й реалізацію ІБ у різних областях інформаційної діяльності організації встановлюється звичайно на рівні керівництва підприємства й містить у собі наступне коло питань [1]:

- формування єдиної концепції й програми робіт в області ІБ;
- розробка багаторівневої політики ІБ і системи структурної й персональної відповідальності за її реалізацію;
- забезпечення виконання положень політики й програми реалізації ІБ;
  планування й виділення необхідних ресурсів для системної реалізації ІБ;
- формування структурних підрозділів і служб ІБ;
- контроль і аудит поточного стану системи ІБ.

Організація процесів управління ІБ є основою функціонування загальної системи безпеки підприємства (компанії) і концентрується на створенні системи управління інформаційною безпекою (СУІБ), базою якої є вимоги по забезпеченню інформаційної безпеки у міжнародних стандартах - ISO/IEC: 27001-27005, 27007, 27031, 27035 і національних стандартів України - ДСТУ ISO/IEC: 27001, 27002, 27005, 27007, 27031, 27035 ч.1- 3.

Вимоги цих стандартів надають кращі практичні ради по менеджменту (управлінню) інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування СУІБ. Інформаційна безпека визначається стандартом ДСТУ ISO/IEC 27001 як «збереження конфіденційності (упевненості в тому, що інформація доступна тільки тим, хто вповноважено мати такий доступ), цілісності (гарантії точності й повноти інформації, а також методів її обробки) і доступності (гарантії того, що вповноважені користувачі мають доступ до інформації й пов'язаним з нею ресурсам)».

Сьогодні багато організацій вже вирішують завдання створення системи інформаційної безпеки, яка відповідала б «кращим практикам» і стандартам в області ІБ і сучасним вимогам захисту інформації. Тому зростає значимість в навчанні основних вимог стандартів в сфері ІБ і придбанні уміння їх реалізовувати на практиці, шо дозволить отримати:

- навички, які необхідні для розуміння принципів впровадження СУІБ відповідно

до вимог ISO 27001;
- розуміння взаємозв'язків СУІБ, включаючи управління ризиками і інцидентами ІБ, а також контроль і дотримання вимог різних зацікавлених сторін організації;
- повне уявлення про концепції, підходи, стандарти, методи і способи, що дозволяють ефективно управляти СУІБ;
- практику впровадження СУІБ відповідно до ISO 27001;
- розширення можливостей для аналізу і прийняття рішень в контексті управління інформаційною безпекою.
Це також підтверджується сучасними вимогами ринку праці, які визначені в знанні і вмінні використовувати стандарти в напрямках:
- моніторинг інцидентів ІБ;
- проведення оцінки ризиків ІБ;
- проведення розслідувань інцидентів ІБ;
- знання і розуміння вимог стандартів з управління ІБ (ISO 27001, ISO 27002) ;
- практичні навички впровадження системи менеджменту ІБ (СМІБ - СУІБ) і в складанні документів по ІБ.
Ще необхідно враховувати, що підвищення ефективності системи ІБ організацій пов'язана із загостренням проблем й впливом безлічі факторів захисту інформації [2]:
- підвищення відповідальності щодо забезпечення конфіденційності даних своїх клієнтів, субпідрядників, партнерів;
- слабість організаційної складової системи ІБ (відсутність класифікації даних по типах і з позицій їх конфіденційності, критичності для бізнесу).
- складності в обґрунтуванні адекватності заходів щодо захисту інформації й можливості використання правових методів розслідування інцидентів.
- актуальність забезпечення безперервності функціонування інформаційних систем (критичне питання для ведення бізнесу).
- підвищення ролі систем захисту, що запобігають вплив атак на інформаційні системи (ІС).
Тому при побудові (модернізації) системи ІБ доцільно керуватися концептуальною схемою її побудови, що включає обов'язковий етап діагностичного обстеження поточного стану й оцінку вразливостей і загроз, на основі яких проводиться проектування й впровадження ефективної СУІБ.
У міру розширення сфери використання ІС і їх ускладнення, проблема забезпечення ІБ загострюється. Безпеку вже неможливо забезпечити одним тільки набором технічних засобів і підтримувати тільки силами підрозділу безпеки. Це можна ефективно вирішити завдяки створенню і впровадженню СУІБ.
Першочерговими завданнями СУІБ є систематизація процесів забезпечення ІБ, розташування пріоритетів організації в області ІБ, досягнення адекватності системи ІБ існуючим ризикам, досягнення її «прозорості». Останнє особливо важливо, оскільки дозволяє чітко визначити, як взаємозалежні процеси й підсистеми ІБ, хто за них відповідає, які фінансові й людські ресурси необхідні для їхнього забезпечення й ін.

Більш детально послідовність створення системи ІБ, в тому числі і СУІБ, організації пропонується розглядати в кілька етапів [3]:
- підготовчий;
- аналітичний;
- дослідницький;
- іспитовий (аналіз отриманих результатів, документування);
- впровадження й технічна підтримка.

Розглянутий підхід до створення системи ІБ здатний допомогти керівникам промислових підприємств при проведенні організаційних робіт із проектування системи ІБ.

Не слід забувати, що успішне й ефективне управління системою ІБ можливо при використанні наукових методів при розробці концепції безпеки підприємства. Систему безпеки необхідно розглядати не тільки як інструмент, що забезпечує захист діяльності, але і як найважливіший ресурс і гарант успішного розвитку будь-якої організації.

Перелік посилань:

1. Лекция 4. Построение системы информационной безопасности. – URL: http://intuit.valrkl.ru/course-1312/index.html#ID.7.image.7.9.
2. Балановская А.В.Концептуальный подход к построению системы информационной безопасности промышленного предприятия // Вестник Самарского государственного университета. 2015. № 5 (127). С. 14–20 .- URL: https://cyberleninka.ru/article/n/kontseptualnyy-podhod-k-postroeniyu-sistemy-informatsionnoy-bezopasnosti-promyshlennogo-predpriyatiya.
3. Домарев В.В. Безопасность информационных технологий. Системный подход. К.: Диасофт, 2004. 992 с. – URL: https://m.books.ru/books/bezopasnost-informatsionnykh-tekhnologii-sistemnyi-podkhod-229927/.

Щавінський Юрій Віталійович
доцент кафедри УІКБ, ННІЗІ, Київ, Україна,
Аркуша Даніїл Олегович
студент групи УБДМ-61, ННІЗІ, Київ, Україна
Лисенко Артем Вячеславович
студент групи УБДМ-61, ННІЗІ, Київ, Україна

ВИКОРИСТАННЯ СЕНТИМЕНТНОГО АНАЛІЗУ ТЕКСТУ В КІБЕРБЕЗПЕЦІ

Динамічний розвиток інформаційних технологій є важливим чинником національної безпеки, однією з основ успішної внутрішньої та зовнішньої політики, необхідною умовою соціального й технологічного поступу держави. Поширення інформаційних технологій призвело до утворення інформаційного середовища, де відсутні державні кордони та обмеження на інформаційні впливи.

Глобальні системи масової комунікації сприяли утворенню кіберпростору, як віртуального середовища, що надає можливості як для реалізації суспільних

відносин на більш високому рівні так і для здійснення кібератак на інформаційні ресурси за допомогою засобів електронних комунікацій [1].

Застосування новітніх інформаційних технологій в процесах управління на всіх рівнях, крім безперечних переваг, посилює небезпеку несанкціонованого втручання в корпоративні інформаційні ресурси.

Кіберпростір разом з іншими фізичними просторами сьогодні визнається одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі [2].

Наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам держави у кіберпросторі, кіберзлочини і кібертероризм змушують світову спільноту, кожну державу розробляти організаційні, правові, наукові-технічні заходи, спрямовані на підвищення рівня кіберзахисту національних електронних інформаційних ресурсів. Реалії сьогодення свідчать про посилення загроз державі і суспільству в кіберпросторі та нагальну потребу в удосконаленні існуючих і пошуку нових способів захисту інформації в інформаційних системах з метою мінімізації загроз.

Одним із дієвих превентивних способів захисту інформації в інформаційних системах усіх рівнів є сентиментний аналіз текстів органами комплексної системи захисту. Він призначений для виявлення в текстах емоційно забарвленої лексики і емоційної оцінки авторів (думок) по відношенню до об'єктів (подій, процесів або їх властивостей чи атрибутів), мова про які йде в тексті. Емоційна складова, виражена на рівні лексеми або комунікативного фрагмента, називається лексичною тональністю (або лексичним сентиментом). Тональність всього тексту в цілому можна визначити як функцію (в найпростішому випадку суму) лексичних тональностей складових його одиниць (речень) і правил їх поєднання [3, с. 5].

Основним завданням в аналізі тональності є класифікація полярності даного тексту, тобто визначення, чи є виражена думка в документі або пропозиції позитивною, негативною або нейтральною по відношенню до потрібної теми. Полярність тексту визначають як за бінарною шкалою так і за багатобальною.

Сентиментний аналіз передбачає розрізнення суб'єктивного (на відміну від фактичного) матеріалу і виявлення різних форм інформаційної поведінки: почуттів, думок, настроїв і емоцій. Методи аналізу текстів є корисними для аналізу настрою на рівні суб'єкта, а також для розрізнення власника думки.

Сентиментний аналіз може проводитись у ручному режимі або автоматизованому. Ручний режим аналізу тональності проводиться експертами. Автоматизований аналіз тональності передбачає використання комп’ютерних програм із застосуванням алгоритмів машинного навчання, інструментів статистики і обробки природної мови, що дозволяє обробляти великі масиви тексту, включаючи вебсторінки, онлайн-новини, тексти дискусійних груп в мережі Інтернет, онлайн-огляди, вебблоги та соціальні медіа

[4, с. 384].

Сентиментний аналіз є основою інтелектуального аналізу текстів і його розвинені держави використовують для цілей національної безпеки та розвідки. Крім того, програмне забезпечення інтелектуального аналізу тексту можна використовувати для створення великих досьє інформації про конкретних людей та події, як спосіб визначення характеристик повідомлень, які можуть бути небажаним матеріалом (актом розпалювання ворожнечі, закликами до повалення конституційного ладу, підготовкою терористичних актів тощо).

Таким чином, застосування сентиментного аналізу, як одного із превентивних способів кіберзахисту дозволяє своєчасно виявити кіберзагрози, відстежувати та моніторити терористичну діяльність в кіберпросторі.

Перелік посилань:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. [Електронний ресурс] – Режим доступу: URL: https://zakon.rada.gov.ua/go/2163-19
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від від 26.08.2021р. № 447. [Електронний ресурс] – Режим доступу: URL: https://zakon.rada.gov.ua/go/n0055525-21
3. Liu B. Sentiment analysis and opinion mining //Synthesis lectures on human language technologies. – 2012. – Т. 5. – №. 1. – С. 1-167.
4. Chang, Wui Lee; Tay, Kai Meng; Lim, Chee Peng . A New Evolving Tree-Based Model with Local Re-learning for Document Clustering and Visualization. Neural Processing Letters. 2017. – 46 (2): 379–409. doi:10.1007/s11063-017-9597-3.

Хавер Анюта Вячеславівна
аспірантка групи АІКБ-11, Кафедри ІКБ ДУТ, Київ, Україна

МЕТОД ЗАХИСТУ ОБ'ЄКТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ ВІД СПЕЦІАЛЬНОГО ТРОЯНСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Оборона і захист своїх територій для України актуальні наразі як ніколи. Зокрема, такою територією є і кіберпростір. Найбільшими цілями для противника в кіберпросторі України є державні інформаційні системи та ресурси. До їх складу можна віднести інформаційні системи об'єктів критичної інфраструктури. Актуальність захисту таких систем є надзвичайно високою так як від їх функціонування залежить стан безпеки критичної інфраструктури. Розглянутий в дослідженні комплексний метод передбачає збереження кіберстійкості інформаційної системи об'єкта критичної інфраструктури при застосуванні спеціального троянського програмного забезпечення.

Ключові слова: кібербезпека, об'єкт критичної інформаційної інфраструктури, спеціальне троянське програмне забезпечення.

В умовах воєнного часу кіберпростір є ще одним середовищем для ведення воєнних дій. Ворог намагається завдавати ударів по інформаційній інфраструктурі України через кіберпростір, шляхом здійснення кібератак, завдаючи шкоди державним і приватним інформаційним ресурсам. Відтак особливої уваги до

забезпечення кібербезпеки та кіберстійкості потребують інформаційні систем об'єктів критичної інформаційної інфраструктури (ОКІІ). Під ОКІІ розуміємо комунікаційну або технологічну систему об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [1].

Система загальнодержавного нормативно-правового врегулювання кібербезпеки чітко визначає вектор захисту об'єктів критичної інфраструктури і спрямовує його на всебічне покращення та вдосконалення стосовно ОКІІ, зокрема це детально описано в "Плані реалізації стратегії кібербезпеки України (додаток до рішення Ради національної безпеки і оборони України від 30.12.2021 "Про План реалізації стратегії кібербезпеки України") [2].

За даними *CERT-UA* (*Computer emergency response team of Ukraine*) на державні організації України здійснюються регулярні кібератаки, переважна більшість яких працює за принципом ураження цільової системи ОКІІ спеціальним троянським програмним забезпеченням (СТПЗ) [3]. СТПЗ — це шкідливе програмне забезпечення, яке працює за принципом троянського коня, а саме маскується під легітимну програму чи процес в цільовій системі, використовуючи при цьому руткіти або інші додаткові засоби для ускладнення його виявлення та має приховані функції з метою нанесення шкоди цільовій системі або її інформаційним ресурсам.

СТПЗ може проникнути на цільову систему як самостійно так і у складі іншого програмного засобу. При цьому цілеспрямоване ураження ОКІІ СТПЗ зазвичай має на меті:

- виведення з ладу інформаційно-комунікаційної системи (ІКС) ОКІ;
- порушення конфіденційності, цілісності чи доступності інформації, яка циркулює в ІКС ОКІ;
- створення на базі ІКС ОКІ ботнет-мережі;
- кібершпигунство;
- кібертероризм.

Початковою точкою ураження СТПЗ в 98% випадків є інформаційна система підприємства, що підключена до глобальної мережі Інтернет. Ефективність застосовування ворогом методів соціальної інженерії на етапі доставки СТПЗ на цільову систему залишається високою та на жаль виправданою. Саме тому власникам інформаційно-комунікаційних систем критично важливо проводити інформування та навчання працівників засобам кібергігієни та кібербезпеки. Найчастіше зловмисниками для маскування інсталяції на цільову систему СТПЗ використовуються листи на електронну пошту, або приєднання "корисного навантаження" до файлів не ліцензійного офісного чи користувацького програмного забезпечення.

Структурно СТПЗ складається з двох основних функціональних елементів: серверної та клієнтської частини. Серверна програма заражає цільову систему, а клієнтська призначена для контролю, віддаленого управління та виконання інших дій над ураженою цільовою системою. Така взаємодія можлива завдяки використанню бекдора. Таким чином зловмисник має змогу отримати привілегії

суперкористувача та необмежений доступ до даних скомпрометованої системи. СТПЗ з функцією віддаленого доступу відноситься до класу *RAT* (*Remote access trojan*).

Задля захисту ОКІІ від СТПЗ необхідно вживати заходи, які можна умовно поділити на превентивний етап та заходи щодо реагування на інцидент кібербезпеки по факту його виявлення. Саме на симбіозі цих двох етапів базується запропонований метод захисту держави від СТПЗ. Варто відмітити, що в загальному замкнутий цикл захисту ОКІІ від СТПЗ буде заснований на наступному алгоритмі: підготовка; виявлення та аналіз; стримування, видалення і відновлення; постінцидентна робота [4, с.44].

Провівши якісну, комплексну оцінку та здійснивши підбір найбільш ефективних організаційних, правових, інженерно-технічних та програмних засобів (систем IPS, IDS, SIEM-систем, антивірусних програмних засобів, засобів адміністрування кінцевих точок та їх ефективності у виявленні СТПЗ) можна запропонувати оптимальні підходи до захисту від СТПЗ, забезпечити кіберстійкість ОКІІ від даного виду кіберзагроз.

Перелік посилань:

1.Закон України “Про критичну інфраструктуру” – [Електрон. Ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text;

2.Рішення Ради національної безпеки і оборони від 30 грудня 2021 року “Про план реалізації Стратегії кібербезпеки України” – [Електрон. ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text;

3. “Щодо невідкладних заходів кіберзахисту” – [Електрон. Ресурс] – Режим доступу: https://cert.gov.ua/article/1751036;

4. “Applied Incident Response” Steve Anson – John Wiley & Sons, Inc., 2020. - 464 p.

Пацьора Елла Сергіївна
студентка групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

ВАЖЛИВІ ЕЛЕМЕНТИ ЩОДО РІШЕННЯ БЕЗПЕКИ IOT

Пристрої IoT розгортаються в мережах із феноменальною швидкістю, до 1 мільйона пристроїв щодня. Незважаючи на те, що ці пристрої створюють нові та захоплюючі способи підвищення ефективності, гнучкості та продуктивності, вони також створюють новий ризик для мережі. Кількість атак на пристрої IoT збільшується, а масштаби та наслідки успішної атаки можуть бути руйнівними. Технологія IoT повністю працює в Інтернеті, а отже, вона більш уразлива до атак зловмисного програмного забезпечення. Уся конфіденційна інформація зберігається в онлайн-хмарі і хакери можуть легко отримати доступ до цієї інформації. Необхідно знати, які шкідливі програми атакують пристрої, щоб за допомогою алгоритму виявлення можна було легко знайти зловмисне програмне забезпечення на пристрої.

Ключові слова: IoT, інформаційні ризики, інформаційна мережа, кінцеві точки.

IoT розширює ландшафт загроз і поверхню атак. Крім простої небезпеки використання кінцевих точок мережі без контролю над заходами безпеки, IoT представляє чотири основні ризики, про які фахівці з безпеки повинні пам’ятати, розробляючи підхід до безпеки та визначаючи вимоги до рішення, яке є достатньо комплексним, щоб протистояти загрозам [1].

Уразливості. Пристрої IoT часто не розробляються та не розгортаються з урахуванням безпеки. Деякі навіть вважаються «безголовими», без можливості

запускати протоколи безпеки або оновлюватися. Компанії ніколи не уявляли, що принтер або термостат будуть задіяні в ботнет-атаці.

Незахищений зв'язок. Пристрої, які використовують загальнодоступні мережі, часто обмінюються даними без шифрування та надсилають дані через незахищені мережі. Трафік не контролюється, не керується та не захищений. Громадський Wi-Fi і нові підходи, які використовують Bluetooth, викликають особливе занепокоєння.

Витоки даних. Пристрої IoT являють собою неконтрольовану та некеровану точку входу та виходу в мережу. Таким чином, політики, встановлені для запобігання витоку даних, можуть не позначати дані, що проходять через ці пристрої. Пристрої мають бути включені до ширшої мережі, щоб політика була застосована.

Зараження шкідливими програмним забезпеченнями. Незахищені пристрої можуть постачатися зі шкідливим програмним забезпеченням або поширювати його. Потрапляючи в мережу, шкідливе програмне забезпечення поширюється з пристрою на пристрій.

Для керування ризиками, фахівці з безпеки повинні певною мірою контролювати інфраструктуру IoT або, принаймні, її зв'язок із мережею. Щоб мінімізувати ці загрози, необхідно звернути увагу на три стратегічні сфери: навчання, сегментація та захист [2].

Навчання

Важливо, щоб мережа знала щодо пристроїв, які спілкуються в мережі, і була достатньо розумною, щоб знати, як класифікувати та навчитися найкраще їх захищати. Без можливості дізнаватися про пристрої інтелектуальний захист від загроз неможливий. Оцінюючи додаток, потрібно звернути увагу на функціональність у двох ключових областях:

1. Ідентифікація та виявлення пристроїв. Додаток повинний мати можливість автоматично виявляти, профілювати та класифікувати те, що є в мережі, а також створювати повний перелік пристроїв.
2. Прогнозні дії. Наступне завдання полягає в тому, щоб вивчити поведінку та передбачити реакцію на напад до того, як він станеться. Наприклад, класифікуючи пристрій за трьома категоріями — керовані пристрої (пристрої, якими ви керуєте), дозволені пристрої (ті, які ви приймаєте, але не контролюєте), і несанкціоновані пристрої (підозрілі пристрої, які не відповідають політиці) — структура може вивчити нормальну базову діяльність для кожної категорії. Це також допомагає призначити оцінку ризику пристрою для сегментації та цілей політики.

Сегментація

Сегментація мережі та пристроїв полягає у призначенні політик і управлінні ризиками. Визначаючи вимоги до додатку, фахівці з безпеки повинні мати можливість керувати політиками, отримувати розуміння та бачити тенденції на основі профілів ризиків і типу інфраструктури. Є три ключових вимоги до сегментації.

1. Виявлення ризику. Першим порядком у сегментації є класифікація. Для ідентифікації категорій і оцінки ризику необхідно використовувати користувачів, дані, пристрої, розташування та безліч інших критеріїв.

2. Керування політиками та пристроями. У міру розширення мережі нові пристрої потрібно не тільки виявляти, але й налаштовувати на основі існуючих політик щодо пристроїв. Додаток має забезпечувати деталізацію, щоб бачити всю активність пристрою та відповідним чином установлювати політики.

3. Здійснення контролю. Як тільки зловмисник отримує доступ, зловмисник може тижнями блукати мережею, перш ніж діяти. Сегментація мережі, наприклад, ізоляція пристроїв IoT та інших пристроїв, серверів і портів, з якими вони спілкуються, дозволяє організації розділити ресурси на основі ризику.

Захист

Місія безпеки IoT полягає в тому, щоб спочатку захистити пристрій, а потім захистити мережу. Коли пристрій IoT захищено та стає частиною мережі, його необхідно захищати узгоджено з усіма іншими елементами мережі. Тому додаток повинен запроваджувати політику з автоматизацією в двох головних вимогах.

1. Гнучкість і ефективність політики. Щоб відповідати викликам IoT, необхідно застосовувати правила, що регулюють поведінку пристрою, який тип трафіку може генерувати пристрій, де він може бути в мережі та навіть чи може він бути в мережі взагалі. BYOD, додатки для соціальних мереж і хмарні додатки – це приклади, коли необхідно встановити та застосовувати різні політики.

2. Розвідка загроз. Після того, як контроль встановлено, додаток має мати можливість послідовно застосовувати політики та передавати інформацію про відповідність через мережу на всі пристрої, щоб створити інтелектуальну структуру, здатну вивчати загрози та реагувати на них.

Для комплексного рішення пристрої IoT повинні підпорядковуватися тим самим багаторівневим моніторингам, інспектуванням і політикам примусового виконання, що й решта пристроїв у розподіленій мережі. Лише тоді всі частини мережі зможуть спілкуватися одна з одною, щоб обмінюватися інформацією про політику та розвідкою про загрози та захищати дані додатків.

IoT спричинить кардинальні зміни в тому, як компанії використовують дані для прийняття рішень, і в тому, як ми керуємо своїм особистим життям [3]. Визначаючи вимоги до рішення безпеки IoT, фірми повинні розглянути підхід, заснований на інтелектуальній структурі безпеки всієї мережі, яка може навчатися та обмінюватися інформацією.

Перелік посилань:

4. Fortinet Threat Landscape Report Reveals IoT Devices in the Home Are the Latest Target for Cryptojacking [Електронний ресурс] – Режим доступу: https://investor.fortinet.com/news-releases/news-release-details/fortinet-threat-landscape-report-reveals-iot-devices-home-are

5. How to eliminate enterprise shadow IT [Електронний ресурс] – Режим доступу: https://www.cio.com/article/234745/how-to-eliminate-enterprise-shadow-it.html

6. Connected Devices Will Generate 79 Zettabytes of data by 2025 [Електронний ресурс] – Режим доступу: https://iotbusinessnews.com/2020/08/10/08984-connected-devices-will-generate-79-zettabytes-of-data-by-2025/

Воробей Віктор Вікторович
студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ФУНКЦІОНУВАННЯ БОТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ SPLUNK

Реалії сьогодення демонструють нам досить багате різноманіття тактик та технік, що використовують кіберзлочинці під час скоєння кіберзлочинів, пов'язаних з дестабілізацією та дискредитацією органів управління держав, органів виконавчої влади, викраденням персональних даних, вчинення деструктивних дій щодо засобів масової інформації, фінансовими махінаціями.
Ключові слова: інформаційна система організації, інформаційні ресурси, бот.

Серед всього різноманіття тактик та технік матриці MITRE хотілося б виокремити саме TA0011 (Command and Control), або згідно таксономії Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України - 05.Втручання.Бот. Саме інфікування робочої машини кінцевого користувача досить часто слугує зловмисникам відправною точкою за котрою слідує компрометація чутливої інформації організації та/або деструктивні дії стосовно неї.

Персональна машина користувача, сервер та будь який компонент інформаційно-комунікаційної системи, котрий слугує для обробки інформаційних ресурсів, заражений шкідливим програмним забезпеченням типу RCE (Remote Code Execution), що дає зловмисникам змогу виконувати команди операційної системи на інфікованій машині, називається – бот.

Досить часто зловмисники об'єднують декілька ботів задля спільного виконання задачі – здійснення розподіленої атаки на відмову в обслуговуванні (DDoS).

Задля захисту від подібної активності корпоративної інформаційної системи застосовують цілий ряд організаційно-технічних заходів, основним компонентом яких є створення Security Operations Center (далі - SOC). Це команда фахівців, котра відповідальна за кіберзахист компанії та в разі виявлення якихось безпекових порушень та/або вчинення зловмисних дій відповідальна за реагування на дані події та їх нівелювання (часто це передача необхідної інформації для розслідування команді реагування, або надання вказівок системним адміністраторам, або самостійно – залежно від процедурної політики організації).

Розглянута технологія, котра надає SOC можливість виявляти функціонування ботів в інформаційній системі організації базується на методиці використання SIEM Splunk. Дана система надає наступні засоби для забезпечення захисту інформаційної системи організації:

- Керування журналами: збирати, нормалізувати та агрегувати дані журналів для ефективного доступу до даних і керування ними;
- Моніторинг у режимі реального часу: спостерігати за діяльністю у мережевому середовищі в той момент, коли вона відбувається;
- Розслідування інциденту: шукати та детально переглядайте журнали для подальшого розслідування потенційного інциденту.

Але основною перевагою використання Splunk є агрегація та моніторинг комплексу організаційно-технічних заходів забезпечення стану захищеності інформаційної системи організації.

Нижче наведений список, що зазначає основні методи виявлення ботів за допомогою SIEM Splunk в корпоративній мережі за допомогою аналізу мережевого трафіку:

- Кількість потоків;
- Сума переданих байтів;
- Середня сума байтів що передаються;
- Середній час зв'язку з кожною унікальною IP-адресою;
- Кількість унікальних IP-адрес призначення;
- Кількість унікальних портів призначення;
- Найбільш часто використовуваний протокол;
- Відхилення від політики безпеки;
- Виявлення аномалій;
- Виявлення маячків добре відомого шкідливого програмного забезпечення;

Отже, проблема наявності ботів є досить актуальною і методи боротьби з ними мають бути комплексними. Перевага використання наведеної технології надає можливість агрегувати комплекс заходів захисту, моніторити їх функціональність та функцыонування інформаційної системи вцілому, запобігати та здійснювати реагування на кіберінциденти.

Перелік посилань:

1. ATT&CK Matrix for Enterprise [Електронний ресурс] – Режим доступу: https://attack.mitre.org/
2. Державна служба спеціального зв’язку та захисту інформації України: перелік категорій кіберінцидентів [Електронний ресурс] – Режим доступу: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv
3. Detecting TrickBot with Splunk [Електронний ресурс] – Режим доступу: https://www.splunk.com/en_us/blog/security/detecting-trickbots.html

Ганусяк Степан Ігорович
студент групи АІКБ-11,
ННІЗІ ДУТ, Київ, Україна

АНАЛІЗ АНОМАЛЬНОГО ТРАФІКУ BOTNET В ПРИСТРОЯХ IOT МЕТОДОМ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. Ботнет — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дозволяє зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Зазвичай використовуються для протиправної діяльності — розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні, отримання персональної інформації про користувачів, крадіжка номерів кредитних карток та паролів доступу. Кожен комп'ютер в мережі діє як «бот» і управляється шахраєм для передачі шкідливих програм або шкідливого контенту для запуску атаки. Ботнет деколи називають «армією зомбі», так як комп'ютери контролюються кимось іншим, крім їх власника.
Ключові слова: ботнет, програмне обезпечення бот, комп'ютери, програма, захист, доступ.

Ботнет відноситься до пристроїв, якими хакер керує віддалено. Ботнет — це об’єднаний термін взаємодії робота з мережею, де є два важливих учасники — ботмайстер і підлеглий бот. Підлеглий бот діє як підлеглий ботмайстра і виконує те, що просить ботмайстер. Завдання ботнету полягає в тому, щоб починати атаки, надаючи вказівки від ботмайстрів клієнтам-ботам, щоб функціонувати як раби ботмайстра. У наш час ботнет-атака відбувається настільки тихо, що програмне забезпечення для захисту від зловмисних програм взагалі не в змозі її виявити. Атака ботнету, що відбувається в однорангових мережах, стала проблемою, оскільки виявити командний центр не так просто. Але загалом важко визначити командно-контрольні атаки ботнету, можна спостерігати закономірності в даних, щоб отримати повну картину мережевого обміну даними, і можливе виявлення Botmaster.

Під час DDoS - атаки зловмисник, який є ботмайстром, має високоякісні обчислювальні системи та сервери для запуску командних і контрольних програм зловмисного програмного забезпечення, яке дає вказівки машинам на наступному рівні або рівні, які називаються обробниками. Ці обробники атакують клієнтів, роблячи їх рабами-ботами. Шкідлива діяльність ботнету виявляється різними методами. Як відомо з наведеної вище інформації, програмному забезпеченню виявлення зловмисного програмного забезпечення надзвичайно важко виявити ці атаки. Типовий підхід може полягати в аналізі даних мережевого трафіку, отриманих шляхом моделювання та ботнету на віртуальних машинах, і отриманні відповідних даних зв’язку та мережевого обміну протоколами TCP і UDP.

Алгоритми керованого навчання (наприклад, дерева рішень, машини підтримки векторів (SVM)) можуть ефективно класифікувати звичайний трафік від трафіку ботнету. Коли алгоритми неконтрольованого навчання, як-от алгоритм K-середніх, інтегруються з алгоритмами класифікації, результати покращуються. Нейронні мережі також є кращим способом підійти до великого

обсягу даних мережевого трафіку. Це дає нам більше шансів виявити інші шаблони в даних, на відміну від алгоритму машинного навчання. Загальні набори даних, які використовуються для такого типу аналізу: набір даних CTU-13, набір даних KDD Cup Nineteen, набір даних UNSW-NB15 і набір даних Bot-IoT. Існує багато інших наборів даних, розроблених або використаних залежно від мети дослідника. Вибір набору даних є особливо важливим критерієм для створення високоточної стабільної моделі для створення кращої системи виявлення ботнетів.

Процес вибору функції є важливим аспектом кожної моделі машинного навчання. У разі атак ботнету командування та керування (C&C) зміна даних IP-адреси, різних часів і методів обміну даними TCP може бути вирішальною функцією для захоплення Botmaster. Таким чином обробляється більшість наборів даних і об’єкти вибираються за потреби. Основним етапом виявлення ботнету є вибір відповідних методів, за допомогою яких можна підвищити точність моделі та запобігти неправильній класифікації даних.

Процес виконується централізованою організацією під назвою C&C, яку також називають ботмайстром. Ботмайстер — це особа, яка координує ініціювання, керування або призупинення атак на всі інфіковані машини (ботів). Таким чином, мета механізму C&C полягає в тому, щоб збільшити кількість зомбі-машин і координувати ці машини для багатьох руйнівних операцій. Відмінність ботнету від інших типів мережевих атак полягає в наявності C&C в мережі. Крім того, боти отримують інструкції від C&C і виконують їх. Інструкції/команди варіюються від ініціювання атаки хробака чи спаму через Інтернет до порушення законного запиту користувача.

Ботнет може робити все, що тільки можна уявити, використовуючи багато комп’ютерів, підключених до мережі. Розподілені ресурси живлення є ключовими моментами потужності ботнетів.

Завдяки розвитку технологій кожен персональний комп’ютер має велику обчислювальну потужність (CPU, GPU) і пропускну здатність. Таким чином, кожен персональний комп'ютер, який об'єднано в ботнет, робить ботнет більш потужним.

Роботи, які вимагають занадто великої обчислювальної потужності, можна легко виконати в розподілених мережах. У цьому типі мережі робота поділяється на підробки та призначається окремим машинам. Основна мета атак ботнетів полягає в об’єднанні цих кількох джерел і створенні неймовірно потужного джерела. Комбінованими джерелами можуть бути пропускна здатність або потужність обробки. Створивши ботнет, який містить достатньо ботів, зловмисники можуть використовувати його в багатьох шкідливих цілях.

Деякі приклади:

- розподілені атаки на відмову в обслуговуванні (DDoS);
- розсилка спаму;
- відстеження трафіку та клавіатурні журнали;
- зараження нових хостів - крадіжки особистих даних;
- атака на мережі чатів IRC4;

- хостинг нелегального програмного забезпечення;
- зловживання Google AdSense і додатки для реклами;
- натисніть шахрайство (Click Fraud);
- маніпулювання онлайн-опитуваннями;
- віддалене використання комп'ютерів;
- атака на банківські комп’ютери (банкомати чи будь-які інші, оскільки вони також підключені до мережі);
- ігри маніпуляції;
- експлуатація приватних документів.

Враховуючи сучасний рівень інформаційних технологій і відповідний розвиток технологій захисту інформації, питання даної теми є актуальними для вивчення та подальшого вдосконалення знань в напрямку безпеки інформації.

Перелік посилань:

1 Huaizhi Li// Botnet Forensic Analysis Using Machine Learning
2 Sathya D, Adithi P, Cemon Sharon Barboza, Bhoomika S, Chaitra B Katoti // A Report on Botnet Detection Techniques for Intrusion Detection Systems
3 Chigozie-Okwum C .C. Ajah Ifeyinwa Angela (PhD).// Botnet Identification Using Machine Learning. Techniques: A Survey

Єльський Костянтин Вячеславович
студент кафедри Інформаційна та кібернетична безпека, ННІЗІ ДУТ, Київ, Україна
email: koortttt@gmail.com

ПРОБЛЕМИ НЕЗАХИЩЕНИХ СИСТЕМ УПРАВЛІННЯ ВЕБ-ДОДАТКАМИ

На сьогодні ми не можемо представити життя без інтернету. Усі веб-додатки що були створенні, створюються та будуть створені, вимагають у розробників достатньо багато досвіду та навичок для створення добре працюючого продукту. Але для того, щоб підтримувати актуальність контенту, керувати заповненням сайту, виконувати дії щодо користувачів та тощо, потрібно мати доступ до панелі адміністрування. Панелі адміністрування повинні бути захищені настільки добре, наскільки це можливо.

Ключові слова: система управління, панель адміністрування, веб-додаток, організація розробки, безпека

Веб-додатки використовують різні організації, незалежно від їх сфери діяльності. Державні установи надають громадянам різні сервіси, ЗМІ розміщують актуальні новини на своїх майданчиках, ІТ та телекомунікаційні компанії рекламують та продають послуги та продукти. Різні організації використовують веб-додатки для забезпечення внутрішніх бізнес-процесів. Особливість розвитку сучасних інформаційних технологій така, що питання безпеки часто вирішуються за залишковим принципом.

Адміністративна панель сайту – це прихований від відвідувачів розділ, який необхідний для управління ресурсом. В адмін-панелі адміністратори працюють як зі структурою сайту, так і з контентом. Адміністративна панель, дозволяє створювати, змінювати і видаляти сторінки і розділи, текст, за

можливості відображати інформацію про користувачів, медіаконтент, тощо – в рамках, передбачених використовуваною системою управління контентом (CMS).

Супутніми ризиками несанкціонованого потрапляння у адміністративну панель веб-додатку є:

- Зникнення важливого контенту (фото, відео, медіа матеріали та інше);
- При наявності інформації про користувачів або, наприклад клієнтів, зловмисник отримає змогу завантажити, змінити або підмінити данні;
- Розсилка фішингових повідомлень «від компанії» користувачам або клієнтам, з метою крадіжки інформації, коштів або ресурсів;
- Завантаження шкідливого програмного забезпечення;
- Репутаційний збиток.

Більшість атак на веб-додатки:

- SQL-ін'єкції;
- Міжсайтовий скриптинг (XSS);
- Відсутність функції контролю рівня доступу;
- Неправильне налаштування безпеки;
- Автентифікація та керування сеансами;
- Виконання команд дистанційно.

Основною проблемою несанкціонованого проникнення у закриту частину веб-порталів, є небажання власника ресурсу використовувати та слідкувати технологіям захисту. У результаті це може призвести до невідворотних наслідків. Уникнення помилок, які ймовірно припустяться іншими, є одним із способів випередити хакерів. Також, завдяки технологіям захисту ніколи не буде повністю захищених веб-порталів від злому.

Тенденції ESET останніх 5-7 років говорить нам про те, що веб-ресурси все більше починають слідкувати за станом захищеності і також, працівники які працюють з ІТС починають дотримуватись та розуміти принципи ІТ-гігієни.

Дослідження рекомендує, щоб мати захищену систему управління веб-додатком потрібно, при розробці та під час технічного супровіду, використовувати найкращі практики та технології захисту які рекомендують експерти:

- виконувати оцінку загроз;
- слідкувати за оновленням технологій модулів та планігів, завдяки яким веб-додаток залишається захищеним;
- створювати привілеї та рівні доступу для адміністраторів веб-порталу;
- налаштовувати, актуалізувати та перевіряти доступи.

Крім цих заходів необхідно ввести процедуру перевірки і тестування співробітників з найвищими рівнями доступу. Власник веб-додатку може піддатися серйозному ризику через неналежне виконання рекомендацій. Слід зазначити, що загальний рівень захищеності веб-додатків залишається низьким. У більшій кількості додатків є недоліки різного ступеня небезпеки. Зловмисники можуть експлуатувати критично небезпечні вразливості та мають можливість виконання команд на сервері і повний контроль над системою. Успішні атаки можуть проводитися по відношенню до компаній з різних сфер економіки, від інтернет-магазинів до державних підприємств. Частка додатків, у яких кінцеві користувачі підпадають під загрозу є достатньо великою.

Перелік посилань:

1. Django web application security, MDN Web Docs – Режим доступу до ресурсу: https://developer.mozilla.org/en-US/docs/Learn/Server-side/Django/web_application_security.
2. The Best Practices For Web Application Security For SMB's 2022 – Режим доступу до ресурсу: https://www.bloggersideas.com/best-practices-for-web-application-security-for-smbs/
3. Тенденції поширення Інтернет-загроз році – Режим доступу до ресурсу: https://eset.ua/ua/news/view/789/tendentsii-rasprostraneniya-internet-ugroz-kak-izmenilas-dinamika-vo-vremya-pandemii
4. Тенденції розвитку загроз у 2021 році – Режим доступу до ресурсу: https://eset.ua/ua/news/view/854/tendentsii-razvitiya-ugroz-v-2021-godu-kak-ostavatsya-v-bezopasnosti-v-usloviyakh-neopredelennosti

Андрущенко Катерина Юріївна
студентка групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

АВТОМАТИЗАЦІЯ ПРОЦЕСУ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

На сьогоднішній день ландшафт кіберзагроз змінюється настільки швидко, що командам безпеки складно організувати швидкий і ефективний процес реагування. Щодня аналітики приймають рішення, які можуть вплинути на всю організацію і безпека компанії надмірно залежить від персоналу, який часто використовує ручні процеси для обробки сповіщень безпеки і величезної кількості даних з різних систем захисту інформації.

Неправильно обраний процес реагування, відсутність доступу до необхідних систем, перенасиченість даними з різних рішень, виконання постійно повторюваних дій – все це ускладнює процес реагування і становить загрозу для організації.

Перш ніж станеться будь-який інцидент, важливо встановити належні заходи безпеки для зменшення ризиків інфікування вже відомими загрозами. Важливою частиною налаштування мережі є наявність всіх необхідних інструментів моніторингу та введення журналів для збору та аналізу подій у мережі [1].

Організація процесу керування інцидентами ІБ без використання засобів автоматизації являє собою складне й трудомістке завдання. Необхідно збирати

та консолідувати надвелику кількість даних у різних форматах, вести централізований архів. Для ручної обробки даних щодо подій та інцидентів ІБ потрібна велика кількість висококваліфікованих фахівців-аналітиків. Через великий обсяг рутинної роботи обробка подій найчастіше буває неповною, що не відбиває всього змісту поточної ситуації. Може статися, що інциденти ІБ, критичні для надійного й захищеного функціонування системи, виявляються поза полем зору аналітиків, і через це не приймаються відповідні превентивні заходи [2].

Спеціалізоване рішення для автоматизації реагування на інциденти – SOAR.

Рішення SOAR - Security Orchestration, Automation & Response, призначене для автоматизації і спрощення процес реагування на інциденти.

SOAR дозволяє чітко визначити процес реагування, якого слід притримуватись аналітику, поєднати дані з різних систем в одному інциденті, тобто збагатити інцидент даними з усіх пов'язаних рішень безпеки, забезпечити виконання необхідних дій в системах та автоматизувати повторювані дії.

Принцип роботи SOAR:

Системи захисту інформації при детектуванні загрози генерують спрацювання, який потрапляє в SOAR. На його підставі створюється інцидент, збагачується даними з інших засобів захисту - аналітик дотримуючись інструкції проводить розслідування, а вся послідовність дій в підсумку зберігається в консолі і може бути переглянута адміністратором.

Таким чином SOAR значно спрощує процес обробки інцидентів, дозволяє ефективно використовувати формалізовані плани реагування, зменшує час розслідування за рахунок автоматизації і надає необхідну візуалізацію дій при розслідуванні інцидентів.

Перелік посилань:

1. Від інциденту до вирішення: основні кроки протидії та відновлення у випадку кібератаки. URL: https://eset.ua/ua/blog/view/83/ot-intsidenta-k-resheniyu-osnovnyye-shagi-protivodeystviya-i-vosstanovleniya-v-sluchaye-kiberataki

2. Гладиш С. В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7536/11-Gladysh.pdf?sequence=1

Береза Віталій Васильович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ДОСТУП ДО МЕРЕЖІ ОРГАНІЗАЦІЇ НА ОСНОВІ ПРИНЦИПІВ НУЛЬОВОЇ ДОВІРИ

Мережевий доступ з нульовою довірою (ZTNA) – це рішення інформаційної безпеки, яке забезпечує віддалений доступ до ресурсів, послуг та даних організації на основі чітко визначених політик контролю доступу. Даний підхід відрізняється від

стандартних методів тим, що надається доступ лише до певних служб, а не до всієї мережі. Для ефективного впровадження архітектури з нульовою довірою потрібно дотримуватись наступних правил:

1. Постійний моніторинг. Це означає, що користувачі можуть переміщатись по цифровим каналам підприємства, але ніколи не повинні залишатися без нагляду.
2. Принцип найменших привілей. Цей принцип означає надання доступу до найменшої кількості IT-ресурсів, необхідних користувачам для виконання своїх задач.
3. Двохфакторна автентифікація. Означає, що для отримання доступу користувачеві недостатньо ввести свій пароль, в якості другого фактору можуть бути використані: OTP, SMS-код або E-MAIL-код. Це дозволяє знизити ризики у разі компрометації параметрів облікового запису користувача
4. Постійна аналітика. Те, що автентифікація пройшла успішно і пристрою надано доступ не означає, що йому можна довіряти. Для отримання доступу EDR-клієнт встановлений на кінцевому пристрої повинен підтвердити те, що пристрій не було скомпрометовано і він відповідає корпоративним стандартам безпеки.
5. Мікросегментація. Означає розділення периметрів безпеки на зони, що обмежить доступ до сегментів мережі. Якщо одна зона буде скомпрометована, вся інша мережа залишиться у безпеці.

Сьогодні багато вендорів пропонують свої рішення для організації ZTNA. Для прикладу в рішенні Sophos ZTNA використовуються наступні елементи:

Sophos Central – хмарна консоль управління, забезпечує простоту розгортання, керування політиками контролю доступу, моніторинг і надання аналітичних даних.

Sophos ZTNA Client – разом з Intercept X (антивірусом Sophos) забезпечує віддалений доступ до необхідних ресурсів та моніторинг пристрою на відповідність корпоративним стандартам.

Sophos ZTNA Gateway – мережевий шлюз, який забезпечує доступ до мережі в якій знаходяться корпоративні ресурси.

Перелік посилань:

1. Інтернет ресурс «Sophos» - https://www.sophos.com/en-us/whitepaper/demystifying-zero-trust
2. Інтернет ресурс «Paloalto» - https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna
3. Інтернет ресурс «VMware» - https://cutt.ly/bNokbFA
4. Інтернет ресурс «Fortinet» - https://www.fortinet.com/solutions/enterprise-midsize-business/network-access/application-access

Соколянський Костянтин Анатолійович
студент групи БСДМ-53, ННІЗІ ДУТ, Київ, Україна

КІБЕРІНЦИДЕНТИ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ, МЕТОДИ РЕАГУВАННЯ, МІНІМІЗАЦІЯ ЗАПОДІЯНОЇ ШКОДИ

У 2022 році усі компанії, що використовують комп’ютерні системи у роботі, дедалі частіше стикаються з кіберінцидентами. В основному зловмисники для розповсюдження своєї діяльності використовують фішингові листи та дропери,

які в свою чергу шифрують, модифікують або іншим чином видозмінюють або викрадають інформацію, що порушує цілісність, доступність та конфіденційність інформації, яка становить цінність для підприємств. Саме тому у цій статті буде представлено план реагування на кіберінциденти у підприємствах з метою мінімізації потенційних ризиків при повільному або неякісному реагуванні на кіберінциденти.

Ключові слова: фішинг, дропер, кібербезпека, кіберінцидент, скомпрометований обліковий запис, програмне забезпечення, IOC, SIEM.

При виникненні ситуації, коли ПК у корпоративному середовищі було заражено, в першу чергу не потрібно піддаватися паніці та оперативно розподілити обов'язки між командою реагування. Рекомендується це зробити заздалегідь, оскільки, наприклад, при ситуації із шифрувальником кожна хвилина вирішує, наскільки критичними будуть збитки для компанії, що виявилася жертвою вірусної активності. Перше, на що потрібно звернути увагу, коли кіберінцидент виявлено – це обліковий запис жертви, яка спричинила кіберінцидент. Скоріш за все, людина не зможе пояснити, що саме сталося на його робочій станції або, в принципі, команда реагування не завжди може мати доступ до таких даних, тому рекомендується заблокувати потенційно скомпрометований обліковий запис на час розслідування. Якщо обліковий запис є привілейованим, рекомендується змінити пароль відразу, оскільки шкоди може бути заподіяно набагато більше за час проведення розслідування. Після цього об'єкт, на якому відбувся кіберінцидент слід заблокувати або ізолювати, оскільки поки не зрозуміло, який саме тип вірусу спричинив інцидент. Далі основна мета – це виявлення активності облікового запису на хостовій системі, де безпосередньо був спричинений інцидент, це можна зробити завдяки SIEM-системі при пошуку логів за обліковим записом. Також аналітики зацікавлені у тому, щоб знайти додаткові облікові записи, які могли бути задіяні на хостовій системі у тому проміжку часу, у якому безпосередньо був відкритий зловмисний об'єкт: на час розслідування ці облікові записи, за знайденою за ними підозрілою активністю, можуть бути заблоковані. Паралельно з аналізом активності користувачів, аби не гаяти час, можна проводити пошук по логах антивірусного програмного забезпечення, яке встановлено на робочих станцій у ролі агентів. Саме за допомогою антивірусу можна зрозуміти яке саме ПЗ спричинило зловмисну активність та, за можливості, вивантажити хеш зловмисного файлу для потенційного аналізу на індикатори компрометації (IOC). Також буде доречним дізнатися чи виконуються активні зловмисні дії протягом розслідування: операції з файлами, бічне пересування, мережеві комунікації, тощо. Якщо даний пункт проігнорувати, то компанія ризикує опинитися під загрозою інфікування «мережевим хробаком», який непомітно зможе пересуватися іншими робочими станціями наявними у підмережі, при умові, якщо робоча станція не була в свою чергу ізольована на мережевому рівні. Важливо також з'ясувати атрибути зміни файлів або інших показників, які дозволяють задати часову точку відліку для аналізу логів та виявити зразок зловмисного ПЗ. Після цих дій можна

перейти до аналізу угрупування, типу зловмисного ПЗ, що уразило робочу станцію та ідентифікувати потенційні TTP (тактики, техніки та процедури). Після виконання першочергових дій може прийматися рішення про блокування або видалення зловмисного ПЗ та переходу до пошукових зловмисних дій, які пов'язані з кіберінцидентом, і наявності нестандартного ПЗ на ураженому об'єкті/уражених об'єктах та використання його як можливої точки входу. Паралельно із пошуком зловмисних дій вірусної програми, може бути виконана процедура Threat Hunting з метою пошуку можливої реакції зловмисника на дії групи реагування по блокуванню зловмисного впливу і проведення аналізу зразка зловмисного програмного коду для розуміння послідовності зараження та наслідків, які були спричинені вірусним ПЗ. При аналізі зразка обов'язково слід вказати знайдені через SIEM-систему IOC для подальшого їх блокування на мережевому обладнанні, антивірусному ПЗ, поштових клієнтах, тощо. Після виконання наведених вище кроків робиться постановка задачі на відновлення постраждалих систем (резервні копії або форматування дисків та інсталяція операційної системи і ПЗ з чистих джерел), відновлення файлів користувача (за наявності резервних копій) та підготовка фінального звіту за кіберінцидентом.
Фінальним кроком є аналіз ефективності дій групи реагування, за необхідності – внесення правок у регламент проведення заходів з усунення наслідків викликаних зловмисним ПЗ, та проведення профілактичної бесіди з користувачем, який став жертвою кіберзлочину.

INFORMATION SECURITY MANAGEMENT. MEASURING ISMS PROCESSES

Baturkina Anastasiia
Student of UBDM-61, State University of Telecommunication
Kyiv, Ukraine

During the last couple of years, interest in becoming ISO 27001 certified or the use of the ISO 27001 as a best practice framework has rapidly grown. Today, a lot of companies, government institutions and municipalities require either ISO 27001 certification or must adhere to the best practices in the standard. It's also increasingly incorporated into tender requirements or used during procurements. The cyclic and iterative process we have come to know as PDCA or Plan-Do-Check-Act is still at the core of ISO 27001:2013 and even though it doesn't explicitly mention Plan-Do-Check-Act, it is applicable as a process framework. The following diagram illustrates how we see the link between PDCA and the ISO 27001:2013.

Measurement requirements are explicitly mentioned in section 9. Performance evaluation, but the ISO standard has, purposefully, not described concrete measurement points. Deciding exactly what to measure and the critical success factors or measurements goals should be defined by your organization and should be part of the alignment of the ISMS with business strategies and goals.

A metric can be defined as a system of measurements, for example the temperature scale Celsius provides the metric scale on which measurements can be performed. Other examples include scales such as percentages, numbers, fail/success or maturity scales such as the CMMI or Cobit maturity scale. It can even be as simple as a graduated level of satisfaction scale or colour scales. Measuring the effectiveness of ISMS processes is measuring how well they perform against a set of predefined goals or targets such as deviations from targets in numbers or percentages or level of satisfaction. The time factor is then added to ensure comparability and to detect changes over time.

This thesis will focus on five core processes that must be measured in order to maintain an effective ISMS:

- IT and business alignment
- Information security risk management process

What are the benefits of measuring? It provides input for better alignment with business strategy and is the basis for reporting to relevant internal and external stakeholders. The effectiveness of processes and IT controls are documented and success criteria are met. Trends that could lead to major non-conformities over time can be detected in time and dealt with (avoided or consequences reduced). Helps justify costs associated with the ISMS and implemented IT controls. Enables management oversight of our ISMS. Provides input as to where to improve or redesign the ISMS processes or redesign IT controls if they are over-performing, not working as intended or not addressing identified risks.

Measurement process and basic requirements In order to build a metric, we need to define the process including scope, ownership, targets and how the results are documented and used.

- All implemented ISMS processes and relevant IT controls should be measured in some way, whether they are grouped or measured individually.
- All measurements should have a defined purpose and output that is measurable and comparable over time. These provide indicators to the effectiveness of your ISMS processes and implemented controls.

Key requirements:

- What is being measured?
- Purpose of measurement
- How is it being measured and what is the frequency?
- Who is responsible for the actual measuring?
- Documenting that the measurement has been performed and output reported
- Evaluating the implemented measurement control. Changes to business, strategies, changed risk-landscape, etc, could have an impact measuring baseline

Suggested measurement points. The below mentioned measurement points are useful examples. Targets, Findings and Action plans vary in particular from company to company, but we have provided some examples to give an idea.

IT and business alignment. How do we ensure that the information security strategy and implemented information security processes are adequately supporting and taking into account the needs and requirements of business strategies and goals?

We can ask ourselves the following questions:

- Are the information security strategy and IT services bringing value to the business?
- Is management committed to ensuring continuous input to information security strategies and IT services?

Table 1. Measurements for IT and business alignment

Measurement	**Targets / Findings / Action plans**
% of business strategic goals and requirements supported by information security strategic goals and decisions. Method/sources: Review business strategic decisions and ensure that they have been risk-assessed in relation to IT and information security issues. Likewise all major information security strategic decisions should be reviewed and approved by upper management to ensure alignment with business services and strategies.	*Target* All business decisions need to be supported by IT decisions and specifically information security issues. If not relevant, this needs to be documented and approved as part of the project phase. *Finding* Our latest outsourcing and IT procurement decisions have not been aligned with our IT strategy and specifically not with information security requirements.

	Action plans Ensure that IT requirements are mandatory on the agenda and all relevant information security requirements and potential issues are identified and addressed.
Level of business (stakeholders) satisfaction with offered information security services and internal support. Does information security bring value to the stakeholders? Method/sources: Data collected through interviews or survey forms sent to relevant stakeholder of each business unit, business process or similar	*Target* Our baseline is above average e.g. high level of satisfaction with offered information security services (scale going from low over medium, high, to excellent). *Finding* Compared to last year we have increased the level of satisfaction from medium to high. *Action plans* No action plans

Information security risk assessment.

Questions we should ask could be:

- Are the IT risk processes addressing all relevant business risks?
- Does the business feel that their risk-input is being covered?
- Is the risk management process being carried out in a structured manner?

We also need to be able to ascertain how effective we are at treating identified risks, and how our risk posture changes over time. This includes identifying changes to risk patterns.

Table 2. Measurements for Information Security Risk Assessment

Measurement	**Targets / Findings / Action plans**
% of business processes and their-services covered by the risk management process. Method/sources: Interviews and correlation with management.	*Target* Depending on current maturity level of an organisation it could be all or only some of the business processes/IT-services. Extending coverage could be part of a maturity process. Target this year has been 50%. *Findings* Four critical business processes have not been subjected to a BIA (40%). *Action plans* We need to find out if it's a resource problem or poor risk planning.
Number of approved risk treatment plans actually being implemented compared to last risk assessment.	*Target*

Method/sources: Correlate with previous risk assessment reports.	We need to ensure that proposed and approved risk treatment plans are carried through and not forgotten or "saved for later". *Findings* Only 60% of the approved action plans have been implemented this year. This is a drop on 20% compared to last year. *Action plans* We need to analyse what went wrong. Is it a financial issue, lack of ownership or other factors?

List of links:

1) Gaffri Johnson Senior Security Advisor at Neupart, Measuring ISO 27001 ISMS processes, - 6-8 p.
2) How to measure ISO 27001 ISMS efficiency with KPIs, URL: https://www.neupart.com/good-enough-it-risk-management/27001-isms-kpi-metrics#:~:text=To%20make%20it%20short%2C%20ISMS,improvements%20and%20efficiency%20to%20management.