*SNM. #4. Fails samples – вчимося на чужих помилках ****

- *Системний та мережевий моніторинг. Лекція #9. Найвідоміші приклади порушення кібербезпеки.*

- План лекції . Тема 9. Найвідоміші приклади порушення кібербезпеки
- Найвідоміші приклади порушення кібербезпеки

Вступ.

Сьогодні я хочу запросити вас у захоплюючу, але й тривожну подорож світом кібербезпеки.
Наша тема - найвизначніші провали в моніторингу та побудові систем безпеки.
Ми дослідимо історії, де недоліки в моніторингу та недосконаліть систем безпеки призвели до катастрофічних наслідків.

Чому це важливо?

Вивчення помилок інших - це безцінний урок для запобігання власним.

Розуміючи, де і чому система дала збій, ми можемо вдосконалювати свої методи моніторингу та будувати більш стійкі до атак системи безпеки.

Що ми будемо досліджувати:

Гучні випадки кібератак:
Як недоліки в моніторингу призвели до викрадення даних, фінансових втрат та пошкодження репутації.

- Поширені помилки в моніторингу та побудові систем безпеки:
- Недостатнє охоплення інфраструктури
- Недосконаліть процесів реагування на інциденти
- Ігнорування попереджувальних сигналів

Практичні поради:
Як удосконалити свій підхід до моніторингу
Як будувати більш стійкі до атак системи безпеки
Наш девіз:

"Вчимося на чужих помилках, щоб не повторювати їх у своїх системах!"

Найвідоміші приклади порушення кібербезпеки

Розглянемо приклади внутрішніх загроз , які заслуговують на особливу увагу. Вивчення цих реальних випадків може бути дуже корисним для зміцнення вашої позиції кібербезпеки проти внутрішніх загроз.

❖ **Атаки соціальної інженерії: Mailchimp і Cisco.** Зловмисники можуть легко видати себе за людину, якій ви довіряєте.
Згідно зі звітом Verizon про розслідування порушень даних за 2023 рік, атаки соціальної інженерії спричиняють 17% усіх порушень даних і 10% випадків кібербезпеки, що робить соціальну інженерію одним із трьох найпоширеніших векторів кібератак. Такі атаки націлені на співробітників організацій, щоб обманом змусити їх розкрити особисту інформацію. Якщо зловмисникам вдасться скомпрометувати паролі співробітників до корпоративних ресурсів, вони можуть отримати несанкціонований доступ до критично важливих даних і систем організації.

➢ **Mailchimp**

У січні 2023 року Mailchimp, відома платформа для електронного маркетингу та інформаційних бюлетенів, виявила неавторизованого користувача у своїй інфраструктурі . Вони заявили, що зловмисник отримав доступ до одного з інструментів, які Mailchimp використовує для адміністрування облікових записів користувачів і підтримки клієнтів. Раніше зловмисник націлився на співробітників Mailchimp і зумів отримати облікові дані їхніх облікових записів за допомогою методів соціальної інженерії. Після цього зловмисник використав скомпрометовані облікові дані для доступу до даних 133 облікових записів Mailchimp. Mailchimp стверджував, що жодної конфіденційної інформації не було вкрадено, але в результаті злому могли бути розкриті імена та електронні адреси клієнтів.

➢ **Cisco**

У травні 2022 року Cisco, багатонаціональна компанія цифрового зв'язку, дізналася про зловмисника в їхній мережі. Їхнє внутрішнє розслідування показало, що зловмисник провів серію складних голосових фішингових атак для доступу до облікового запису Google співробітника Cisco. Оскільки облікові дані співробітника були синхронізовані в браузері, зловмисник міг легко отримати доступ до внутрішніх систем Cisco. Отримавши початковий доступ, зловмисник намагався якомога довше залишатися в мережі Cisco і підвищити рівень доступу. Однак команда безпеки Cisco успішно видалила зловмисника з мережі. Пізніше банда програм-вимагачів Yanluowang опублікувала витік файлів на своєму веб-сайті. За словами Cisco, це порушення не вплинуло на їхні бізнес-операції.

Чого ми можемо навчитися з цих інцидентів безпеки IT?

Створення політики кібербезпеки з чіткими інструкціями є важливим, але цього може бути недостатньо. Ви також повинні регулярно проводити навчання, щоб переконатися, що ваші співробітники повністю розуміють ключові правила цієї політики та підвищити їх загальну обізнаність щодо кібербезпеки. Якщо ваші співробітники знають типи атак соціальної інженерії та знають, як захистити свої корпоративні облікові записи, у них менше шансів потрапити на пастки шахраїв. Привілейовані облікові записи потребують ще більш розширеного захисту, оскільки їхні користувачі зазвичай мають доступ до найважливіших систем і даних. Якщо хакери отримають доступ до таких облікових записів, наслідки для безпеки та репутації організації можуть бути руйнівними. Дуже важливо забезпечити своєчасне виявлення та запобігання зловмисній діяльності в привілейованих облікових записах. Розгляньте можливість розгортання рішень, які забезпечують багатофакторну автентифікацію (MFA), аналітику поведінки користувачів і об'єктів (UEBA) і безперервний моніторинг

SNM. #4. Fails samples – вчимося на чужих помилках ***

- *Системний та мережевий моніторинг. Лекція #9. Найвідоміші приклади порушення кібербезпеки.*

користувачів, зокрема інструменти моніторингу Microsoft Hyper-V , Citrix і VMware Horizon для віртуальних кінцевих точок.

❖ **Зловживання привілеями: Міжнародний комітет Червоного Хреста (МКЧХ) .** Іноді люди зловживають наданими їм привілеями. Організації зазвичай мають багато користувачів із підвищеними привілеями, наприклад адміністраторів, технічних спеціалістів і менеджерів. Деякі можуть отримати доступ лише до певних критичних ресурсів, таких як певні бази даних або програми. Інші можуть мати повний доступ до кожної системи в мережі та навіть мати можливість створювати нові привілейовані облікові записи, не привертаючи чиєїсь уваги. Якщо привілейовані користувачі мають зловмисні наміри або були скомпрометовані, це може призвести до витоку даних, фінансового шахрайства, саботажу та інших серйозних наслідків. На жаль, важко виявити, чи зловживає користувач із підвищеними правами доступу своїми привілеями, оскільки такі зловмисники часто вміло приховують свої дії.

➢ **Міжнародний Комітет Червоного Хреста (МКЧХ)**

У січні 2022 року МКЧХ зазнав кібератаки та масового витоку даних . За словами колишнього радника МКЧХ з питань кібервійни Лукаша Олейніка, це був, мабуть, найбільший і найделікатніший злом в історії гуманітарних організацій. Порушення призвело до компрометації даних про понад 515 000 уразливих людей, розлучених зі своїми родинами через конфлікт, міграцію та інші катастрофи. Спочатку припускали, що злом стався внаслідок нападу на одного з субпідрядників організації. Однак розслідування показало, що атака була спрямована саме на сервери МКЧХ. Зловмисники скомпрометували привілейовані облікові записи, використовували методи бокового переміщення для ескалації своїх привілеїв і діяли під виглядом адміністраторів, щоб отримати конфіденційні дані.

Чого ми можемо навчитися з цього випадку зловживання привілеями?

Існують різні способи для організацій, щоб успішно запобігти інцидентам, подібним до того, який пережив Червоний Хрест. Зокрема, ви можете захистити привілейовані облікові записи вашої організації, увімкнувши MFA та ручне схвалення запитів на доступ до найважливіших активів. Багато організацій також мають привілейовані облікові записи, якими користуються кілька людей, наприклад облікові записи адміністратора або облікові записи керування службами. У цьому випадку ви можете використовувати вторинну автентифікацію, щоб розрізняти дії окремих користувачів під такими обліковими записами. Крім того, детальний запис активності користувачів і ретельні аудити можуть спростити реагування на порушення даних і процеси розслідування інцидентів.

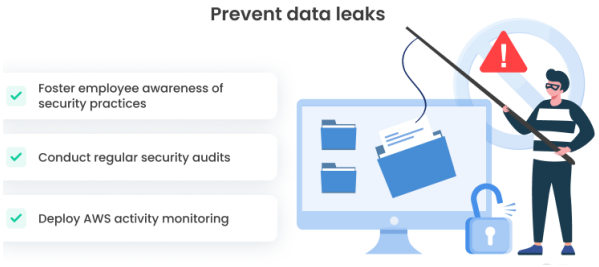
❖ **Витік даних: Pegasus Airlines.** Це дорого, щоб зробити речі приватними, і дешево, щоб зробити їх публічними. Організації докладають багато зусиль і ресурсів для захисту даних. Однак інколи помилка, недбала поведінка чи брак уваги можуть означати, що всі ці зусилля були марними. Ненавмисні дії співробітників, такі як використання незахищених пристроїв, використання неправильних конфігурацій безпеки або випадковий обмін даними, часто призводять до витоку даних. Якщо їх вчасно помітити, вони можуть не завдати шкоди. Однак якщо такі помилки виявляють зловмисники, вони мають більший шанс прокласти шлях до витоку даних. Останнє стосувалося Pegasus Airlines.

➢ **Авіакомпанія Pegasus Airlines**

У червні 2022 року авіакомпанія Pegasus Airlines виявила помилку в конфігурації однієї зі своїх баз даних. Виявилося, що співробітник авіакомпанії неправильно налаштував параметри безпеки та відкрив 6,5 терабайт цінних даних компанії. В результаті неправильної конфігурації блоку AWS 23 мільйони файлів з польотними картами, навігаційними матеріалами та особистою інформацією екіпажу були доступні для загального перегляду та редагування.

Що ми можемо дізнатися з цього витоку даних?

Щоб переконатися, що ваші співробітники не допускають подібних помилок, обов'язково проводите регулярні тренінги з кібербезпеки, а також створіть політику безпеки у своїй компанії. Переконайтеся, що співробітники, які працюють із конфігураціями бази даних, знають правильний спосіб налаштування баз даних і знають про найкращі практики, щоб уникнути розголошення даних. Регулярні перевірки безпеки можуть допомогти вашій організації вчасно виявити та усунути неправильні конфігурації або вразливі місця в базах даних і системах. Регулярно перевіряючи безпеку вашої інфраструктури, ви можете запобігти використанню зловмисниками прогалин у безпеці або помилок співробітників. Увімкнення моніторингу активності користувачів на AWS також може допомогти вам швидко виявляти підозрілі події та реагувати на них, зменшуючи ризик викрадення критичних даних із ваших хмарних середовищ.



❖ **Крадіжка інсайдерських даних: інвестування Cash App.** Інсайдери – це люди, яким ми схильні довіряти. На відміну від зовнішніх хакерів, інсайдери можуть отримати доступ до конфіденційних даних організації та викрасти їх майже без зусиль, якщо вони мають достатньо дозволів. Ці інсайдери можуть включати поточних або колишніх співробітників, сторонніх постачальників, партнерів і скомпрометованих користувачів. Відповідно до звіту Verizon про розслідування витоку даних за 2023 рік, інсайдери можуть викрасти дані з метою фінансової вигоди та шпигунства, з ідеологічних міркувань або через образу. Для організацій крадіжка інсайдерських даних може спричинити фінансові втрати, репутацію та втрату довіри клієнтів, а також юридичну відповідальність.

➢ **«Cash App».**

У грудні 2021 року Block, Inc. виявила інцидент із кібербезпекою, який стався в її дочірній компанії Cash App. Колишній співробітник завантажив внутрішні звіти з інформацією про понад 8 мільйонів колишніх і поточних клієнтів Cash App Investing. Не кажучи про те, чому та як довго колишній співробітник все ще мав доступ до конфіденційних внутрішніх даних, компанія стверджувала, що викрадені звіти не містять жодної особистої інформації, такої як імена користувачів, паролі чи номери соціального страхування.

Чого ми можемо навчитися з цього прикладу крадіжки інсайдерських даних?

SNM. #4. Fails samples – вчимося на чужих помилках ***

- *Системний та мережевий моніторинг. Лекція #9. Найвідоміші приклади порушення кібербезпеки.*

Першим кроком до захисту конфіденційних даних вашої організації є обмеження доступу користувачів до них. Розгляньте можливість впровадження принципу найменших привілеїв, щоб встановити надійне керування доступом і захистити ваші критично важливі системи та цінні дані від можливого компрометування. Моніторинг активності користувачів і перевірки можуть допомогти вашій команді з кібербезпеки виявити підозрілу поведінку співробітників, наприклад доступ до даних або послуг, не пов'язаних з посадою, відвідування загальнодоступних хмарних служб зберігання або надсилання електронних листів із вкладеннями в приватні облікові записи. Після розірвання контракту працівника забезпечте належний процес звільнення. Це має включати деактивацію облікових записів, доступ до VPN і доступ до віддаленого робочого столу, зміну паролів і видалення облікових записів співробітників із груп електронної пошти та списків розсилки.

❖ **Крадіжка інтелектуальної власності: Yahoo, Pfizer, Proofpoint.** Комерційна таємниця є основною мішенню для багатьох кіберзлочинців. Інтелектуальна власність є одним із найцінніших типів даних, якими може володіти організація. Яскраві ідеї, інноваційні технології та складні формули дають бізнесу конкурентну перевагу. Не дивно, що зловмисники часто атакують комерційні таємниці жертв. Yahoo У лютому 2022 року старший науковий співробітник

➢ **Yahoo**

Цянь Санг викрав інтелектуальну власність компанії через 45 хвилин після отримання пропозиції про роботу від конкурента Yahoo, The Trade Desk. Через два тижні після інциденту під час криміналістичного аналізу Yahoo виявила, що горезвісний співробітник завантажив 570 000 файлів зі свого корпоративного ноутбука на два персональних зовнішніх накопичувачі. Викрадені файли містили вихідний код AdLearn – двигуна Yahoo для купівлі реклами в реальному часі – а також інші файли зі сховищ Yahoo Github.

➢ **Pfizer**

У жовтні 2021 року співробітник, який пропрацював 15 років, викрав 12 000 конфіденційних документів із даними про вакцину проти COVID-19, відносини між Pfizer і BioNTech та експериментальні моноклональні методи лікування раку. Компанія Pfizer подала до суду на свого колишнього співробітника за завантаження файлів, що містять комерційну таємницю, на приватні облікові записи Google Drive і особисті пристрої. Цілком можливо, що злочинець мав намір передати викрадену інформацію Xencor, одному з конкурентів Pfizer, який раніше запропонував колишньому співробітнику Pfizer роботу.

➢ **Proofpoint**

У січні 2021 року екс-директор відділу національних партнерських продажів Proofpoint викрав комерційні секрети компанії та поділився ними з конкурентами. Документи містили стратегію та тактику конкуренції з Abnormal Security – компанією, куди пішов працівник. Представники Proofpoint стверджують, що зловмисник забрав USB-накопичувач із конфіденційними документами, незважаючи на підписання угод про неконкуренцію та невимагання на початку роботи.

Чого ми можемо навчитися з цих випадків крадіжки інтелектуальної власності?

Перш за все, вам потрібно визначити, яка інформація є вашою найцінніщою інтелектуальною власністю, де вона розташована та хто справді потребує до неї доступу. Коли мова заходить про спеціалістів з технологій, ви не можете не надати їм доступ до відповідних ресурсів. Однак ви повинні надати їм лише ті права доступу, які необхідні для виконання їх роботи. Розгляньте можливість використання вдосконалених рішень для керування доступом, щоб запобігти несанкціонованому доступу до вашої інтелектуальної власності. Щоб посилити захист інтелектуальної власності вашої організації, ви можете скористатися надійними інструментами моніторингу активності користувачів і аналізу поведінки користувачів і об'єктів (UEBA) . Такі рішення можуть допомогти вам виявити підозрілу активність у вашій мережі, забезпечити оперативне реагування на інциденти безпеки та зібрати детальні докази для подальших розслідувань. Розгляньте можливість розгортання засобів захисту від копіювання або керування USB-пристроєм , які унеможливлять копіювання конфіденційних даних або використання несанкціонованого пристрою USB для співробітників.

❖ **Атаки сторонніх постачальників:** Субпідрядники часто мають ті самі права доступу, що й внутрішні користувачі.

Наявність складного ланцюжка постачання з численними субпідрядниками, постачальниками та сторонніми службами є нормою для сучасних організацій. Однак надання стороннім особам доступу до вашої мережі пов'язане з ризиками кібербезпеки. Однією з причин є те, що ваші треті сторони не завжди можуть дотримуватися всіх необхідних процедур безпеки. Таким чином, немає гарантії, що хакери не дістануться до активів вашої організації, використовуючи вразливі місця ваших постачальників.

➢ **T-Mobile**

У січні 2023 року телекомунікаційний провайдер T-Mobile виявив шкідливу активність у своїх системах. Виявилося, що зловмисник зловжив одним із API, який був частиною ланцюжка поставок T-Mobile. У період з 25 листопада 2022 року по 5 січня 2023 року зловмиснику вдалося викрасти особисті дані з 37 мільйонів облікових записів клієнтів. Представники T-Mobile заявили, що викрадена інформація не містила ідентифікаційних номерів, податкових ідентифікаційних номерів, паролів і PIN-кодів, даних платіжних карток або будь-яких інших фінансових даних. Однак цей інцидент все одно скомпрометував платіжні адреси клієнтів, електронні адреси, номери телефонів, дати народження та номери рахунків T-Mobile.

➢ **Volkswagen**

У травні 2021 року Volkswagen Group виявила, що зловмисники отримали доступ до незахищеного файлу конфіденційних даних, зламавши постачальника, з яким дилери Volkswagen співпрацювали для цифрових продажів і маркетингу. Порушення вплинуло на понад 3 мільйони поточних і потенційних клієнтів Audi – дочірньої компанії Volkswagen Group. Хоча більшість зламаних даних містили лише контактні дані клієнтів та інформацію про придбані або запитувані транспортні засоби, конфіденційні дані близько 90 000 клієнтів також були розкриті. У свою чергу Volkswagen пообіцяв постраждалим безкоштовні послуги із захисту кредитів.

Чого ми можемо навчитися з цих прикладів порушень кібербезпеки?

Деяким із цих інцидентів можна було б запобігти за допомогою відповідних сторонніх практик управління кіберризиками. Вибираючи стороннього постачальника, зверніть увагу на його політику кібербезпеки та закони та норми, яких вони дотримуються. Якщо потенційному субпідряднику чи постачальнику послуг бракує практик кібербезпеки, які є критично важливими для вашої організації, подумайте про додавання

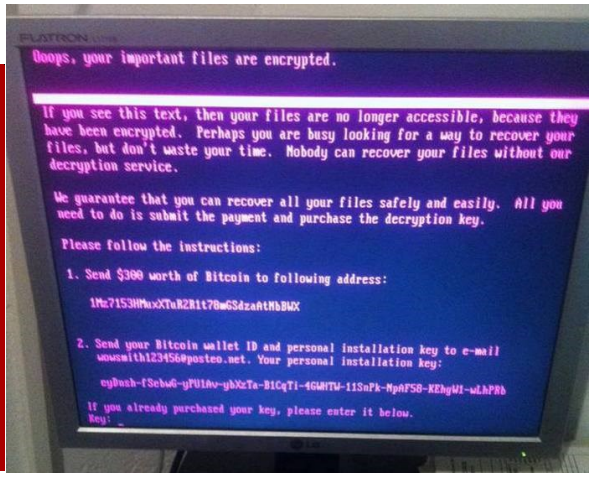
SNM. #4. Fails samples – вчимося на чужих помилках ***

- *Системний та мережевий моніторинг. Лекція #9. Найвідоміші приклади порушення кібербезпеки.*

відповідної вимоги до вашої угоди про рівень обслуговування. Обмежте доступ субпідрядника до ваших важливих даних і систем настільки, наскільки це необхідно для їх роботи. Щоб посилити захист своїх найважливіших активів, застосуйте додаткові заходи кібербезпеки, як-от MFA, підтвердження входу вручну та своєчасне керування привілейованим доступом . Регулярні перевірки безпеки API можуть допомогти виявити вразливі місця та недоліки в реалізації API. Таким чином ви можете мінімізувати ризики, пов'язані з інтеграцією зі сторонніми службами. Крім того, подумайте про розгортання рішень моніторингу, щоб побачити, хто що робить з вашими критично важливими даними. Ведення записів про діяльність сторонніх користувачів дає змогу швидко й ретельно перевіряти кібербезпеку та розслідувати інциденти.

А тепер повернемося додому і згадаємо дві найголосніші за останні роки вірусні хвилі, які прокотилися Україною.

❖ **Petya. Кібератака 2017 року**



Petya — це сімейство шкідливих програм для шифрування , які вперше були виявлені в 2016 році. Зловмисне програмне забезпечення спрямоване на системи на базі Microsoft Windows, заражаючи головний завантажувальний запис для виконання корисного навантаження, яке шифрує таблицю файлової системи жорсткого диска та запобігає завантаженню Windows. Згодом він вимагає від користувача здійснити платіж у біткойнах , щоб відновити доступ до системи.

Варіанти Petya вперше були помічені в березні 2016 року, і вони поширювалися через заражені вкладення електронної пошти.

З власного досвіду, пригадую як дві чарівних жіночки - бухгалтер та юрист з організації, де я на той час працював бігали, заламуючи руки після отримання та відкриття листів від нібіто партнерів. Після цього чомусь їхні ноути запускали chkdsk або scandisk і все ☹. Як не дивно, великої шкоди ці випадки організації не нанесли, бо всі юридичні договори велися у Office 365, а сервер бухгалтерія (на той час це була російська 1С) знаходився на віртуальному сервері у кластері Hyper-V.
Саме дивне, що випадок інфікування двох ноутбуків приніс нашій організації більше користі ніж шкоди:

- ✓ Персонал побачив, що буває, якщо відкривати листи з невідомих джерел, і Фальковський не повинен був проводити довгі виховні бесіди.
- ✓ Керівництво виділило кошти на придбання файервол-кластеру з двох пристроїв McAfee NGF 1035-C2

Всі епопеї літа 2017 року організація пройшла вже без мене, бо я змінив місце роботи, але і Petya також її минув ☺.

27 червня 2017 року почалася масштабна глобальна кібератака (українські компанії одними з перших заявили про атаку) із застосуванням нового варіанту Petya. Того дня «Лабораторія Касперського» повідомила про зараження у Франції, Німеччині, Італії, Польщі, Великій Британії та Сполучених Штатах, але більшість заражень була спрямована на Росію та Україну, де спочатку було атаковано понад 80 компаній, у тому числі Національний банк. України. 28 червня 2017 року ESET підрахувала, що 80% усіх заражень припадало на Україну, а Німеччина була другою найбільш постраждалою з приблизно 9%. Прес-секретар президента Росії Путіна Пєсков заявив, що напад не завдав серйозної шкоди Росії. Експерти вважали це політично вмотивованим нападом на Україну, оскільки він стався напередодні українського свята Дня Конституції.

Засновник компанії Oktava Cyber Protection Олександр Кардаков наголошує, що вірус Petya на три дні зупинив третину економіки України, завдавши збитків на понад 400 мільйонів доларів.

Новий варіант поширювався через експлойт EternalBlue, який на початку 2017 року використовувався програмою - вимагачем WannaCry. Дослідники з питань безпеки, Google і кілька урядів звинуватили в атаках NotPetya російський уряд, зокрема хакерську групу Sandworm у складі ГРУ російської військової розвідки.
Касперський назвав цей варіант «NotPetya», оскільки він має значні відмінності в роботі порівняно з попередніми варіантами. Інженер McAfee Крістіан Бік заявив, що цей варіант був розроблений для швидкого поширення, і що він був націлений на «повні енергетичні компанії, електромережі , автобусні станції, АЗС, аеропорти та банки».

Вважалося, що механізм оновлення програмного забезпечення MEDoc — української програми підготовки до сплати податків, яка, за словами аналітика F-Secure Мікко Гіппьонена була «майже державним стандартом» серед компаній, які ведуть бізнес у країні, — був зламаний для поширення шкідливе програмне забезпечення. Аналіз ESET виявив, що бекдур був присутній у системі оновлення принаймні за шість тижнів до атаки, описуючи це як «ретельно сплановану та добре виконану операцію». Розробники MEDoc заперечували, що несуть повну відповідальність за кібератаку, заявляючи, що вони також були жертвами.

4 липня 2017 року український відділ боротьби з кіберзлочинністю конфіскував сервери компанії після виявлення «нової активності», яка, на його думку, призведе до «неконтрольованого поширення» шкідливого програмного забезпечення. Українська міліція порадила користувачам MEDoc припинити використання програмного забезпечення, оскільки припускала, що бекдур все ще присутній. Аналіз конфіскованих серверів показав, що оновлення програмного забезпечення не застосовувалося з 2013 року, були докази російської присутності, а обліковий запис співробітника на серверах було зламано. Керівник підрозділів попередив, що MEDoc може бути притягнуто до кримінальної відповідальності за здійснення атаки

SNM. #4. Fails samples – вчимося на чужих помилках ***

- *Системний та мережевий моніторинг. Лекція #9. Найвідоміші приклади порушення кібербезпеки.*

через недбалість щодо забезпечення безпеки їхніх серверів. Засновник компанії Oktava Cyber Protection Олександр Кардаков наголошував, що вірус Petya зупинив третину економіки України протягом трьох днів, що призвело до збитків на суму понад 400 млн дол.

У звіті, опублікованому Wired , за оцінкою Білого дому загальні збитки, завдані NotPetya, перевищують 10 мільярдів доларів. Цю оцінку повторив колишній радник з внутрішньої безпеки Том Боссерт , який на момент атаки був найвищим посадовцем уряду США, який займався кібербезпекою.

Під час атаки, розпочатої 27 червня 2017 року, система радіаційного контролю на Чорнобильській АЕС вийшла з ладу. Також постраждали кілька українських міністерств, банків і систем метро. Кажуть, що це була найбільш руйнівна кібератака в історії.

Серед постраждалих в інших країнах були

- ✓ британська рекламна компанія WPP,
- ✓ американська фармацевтична компанія Merck & Co. (міжнародна компанія, яка веде бізнес як MSD),
- ✓ російська нафтова компанія «Роснефть» (її видобуток нафти не постраждав),
- ✓ багатонаціональна компанія юридична фірма DLA Piper ,
- ✓ французька будівельна компанія Saint-Gobain та її роздрібні та дочірні торгові точки в Естонії,
- ✓ британська компанія споживчих товарів Reckitt Benckiser ,
- ✓ німецька компанія особистої гігієни Beiersdorf ,
- ✓ німецька логістична компанія DHL ,
- ✓ Продовольча компанія США Mondelez International
- ✓ оператор американської лікарні Heritage Valley Health System
- ✓ Шоколадна фабрика Cadbury в Гобарті , Тасманія, є першою компанією в Австралії, яка постраждала від Petya.
- ✓ Повідомлялося, що 28 червня 2017 року постраждав найбільший контейнерний порт Індії JNPT. Всі операції порту було зупинено.
- ✓ Прінстонська громадська лікарня в сільській місцевості Західної Вірджинії повинна була замінити всю свою комп'ютерну мережу для відновлення.
- ✓ Перерва в бізнесі Maersk, найбільшого в світі оператора контейнеровозів і суден постачання, оцінювалася в розмірі від 200 до 300 мільйонів доларів США втрачених доходів.
- ✓ Відповідно до річного звіту компанії за 2019 рік, вплив на FedEx у 2018 році оцінюється в 400 мільйонів доларів.

Єнс Столтенберг , генеральний секретар НАТО, наполягав на посиленні кіберзахисту альянсу, заявивши, що кібератака може спровокувати дію принципу 5 статті колективної оборони.

Страховик перевізників Mondelez International, Zurich American Insurance Company , відмовився виплачувати претензію щодо усунення збитків від зараження Notpetya на тій підставі, що Notpetya є «воєнним актом», який не покривається полісом. У 2018 році Mondelez подала до суду на Zurich American на 100 мільйонів доларів. Позов було врегульовано у 2022 році, а умови врегулювання залишаються конфіденційними.

Пом'якшення впливу

Було виявлено, що можна зупинити процес шифрування, якщо заражений комп'ютер негайно вимкнути, коли з'явиться фіктивний екран chkdsk, і аналітики безпеки запропонували створити файли лише для читання perfc з іменами та/або perfc.dat в установці Windows каталог може запобігти виконанню корисного навантаження поточного навантаження. Адреса електронної пошти, зазначена на екрані викупу, була призупинена її постачальником, Posteo, через порушення її умов використання. Як наслідок, заражені користувачі фактично не могли надіслати необхідне підтвердження платежу зловмиснику. Крім того, якщо файлова система комп'ютера базувалася на FAT, послідовність шифрування MFT пропускалася, і відображалося лише повідомлення програми-вимагача, що дозволяло тривіально відновити дані.

Microsoft уже випустила виправлення для підтримуваних версій Windows у березні 2017 року для усунення вразливості EternalBlue. Після цього з'явилися виправлення для непідтримуваних версій Windows (таких як Windows XP) у травні 2017 року, безпосередньо після WannaCry. Wired вважає, що «виходячи з масштабів шкоди, завданої Petya на даний момент, схоже, що багато компаній відклали виправлення, незважаючи на явну та потенційно руйнівну загрозу поширення подібного програмного забезпечення-вимагача». Деякі підприємства можуть вважати, що інсталяція оновлень на певних системах надто руйнівна через можливий простій або проблеми з сумісністю, що може бути проблематичним у деяких середовищах.

Чого ми можемо навчитися з прикладу кібератаки 2017 року Petya?

- ✓ Petya продемонстрував, як кібератаки можуть завдати шкоди на мільярди доларів та порушити роботу критично важливих систем. Це підкреслює важливість кібербезпеки для організацій усіх розмірів.
- ✓ Вірусом використовувалася комбінація методів атаки, включаючи шкідливі програми-вимагачі та соціальну інженерію. Це підкреслює необхідність багаторівневого захисту для захисту від різних типів кібератак.
- ✓ Вірус поширювався через вразливість у програмному забезпеченні бухгалтерського обліку M.E.Doc. Це підкреслює важливість своєчасного виявлення та виправлення вразливостей у системах.
- ✓ Petya зашифрував дані на заражених комп'ютерах, що призвело до значних втрат даних. Це підкреслює важливість регулярного резервного копіювання даних та наявності планів відновлення після аварій.
- ✓ Приклад продемонстрував, як кібератаки можуть мати каскадний вплив, що призводить до порушень в інших системах та секторах. Це підкреслює важливість підготовки до кібератак та підвищення обізнаності про кібербезпеку серед співробітників.
- ✓ Petya продемонстрував, що кібератаки не мають меж і можуть зачепити країни в усьому світі. Це підкреслює важливість міжнародного співробітництва для боротьби з кіберзлочинністю та обміну інформацією про кіберзагрози.
- ✓ Випадок з Petya показав, що організаціям необхідно бути стійкими до кіберзлочинів та мати плани відновлення після кібератак. Це включає в себе можливість швидко ідентифікувати, реагувати та відновлюватися після кіберінцидентів.
- ✓ Уряди відіграють важливу роль у забезпеченні кібербезпеки своїх країн. Це включає в себе розробку та впровадження політики кібербезпеки, сприяння співпраці між державним і приватним секторами та підвищення обізнаності про кібербезпеку серед громадян.

SNM. #4. Fails samples – вчимося на чужих помилках ***

- *Системний та мережевий моніторинг. Лекція #9. Найвідоміші приклади порушення кібербезпеки.*

✓ Інвестування в кібербезпеку є вигідним. Організації, які інвестують у кібербезпеку, краще підготовлені до кібератак і з меншою ймовірністю зазнають значних збитків.

✓ Кіберзагрози постійно розвиваються, тому організаціям та урядам необхідно постійно вдосконалювати свої кіберзахисні заходи. Це включає в себе відстеження нових кіберзагроз, оновлення систем безпеки та навчання співробітників.

❖ **Кібератака на «Київстар» (2023)**

Невдовзі до повномасштабного російського вторгнення критична інфраструктура України зазнала масштабних кібератак в січні та лютому 2022 року. Тоді низка експертів називали ці атаки провісниками швидкої російської військової агресії проти України. Однак у перші тижні російського вторгнення Україні вдалося зберегти стабільну роботу банків, операторів зв'язку та систем енергетики, що здивувало багатьох спостерігачів. Наприкінці 2022 року через російські ракетні удари по українській енергосистемі в українському суспільстві виникли побоювання щодо роботи критичної інфраструктури, проте питання кібербезпеки відійшли на другий план. При цьому в Україні відзначався високий рівень диджиталізації різних сфер життя.

Після початку російського вторгнення та на тлі проблем з електроенергією українські мобільні оператори запровадили систему внутрішньонаціонального мобільного роумінгу, щоб у разі недоступності послуг одного оператора абонент міг скористатися послугами іншого.

Восени 2023 року президент компанії «Київстар» Олександр Комаров розповідав про підготовку компанії до нових можливих обстрілів та блекаутів. Однак незабаром його компанія зазнала найбільшої хакерської атаки. Вже після атаки Комаров у грудні 2023 року говорив, що з початку російського вторгнення «Київстар» відбив понад 500 атак хакерів.

У 2023 році «Київстар» налічував 23 мільйони абонентів мобільного зв'язку, що становило більше половини населення країни, тоді як у другого найбільшого оператора зв'язку Vodafone Україна налічувалося близько 15 млн абонентів. Також «Київстар» мав понад один мільйон абонентів фіксованого інтернету.

Протягом 2023 року в українському суспільстві ходили чутки про швидку націоналізацію компанії «Київстар». Зокрема це пов'язувалося з потенційним арештом частки російського олігарха Михайла Фрідмана в компанії «Київстар», який потрапив під санкції України.

До осені 2023 року компанія «Київстар» на 100 % належала холдингу Veon. У свою чергу 48 % акцій компанії Veon належить компанії LetterOne, 38 % володів Михайло Фрідман. Однак у компанії «Київстар» заявляли, що її материнська компанія має «тисячі власників», і жоден з них не має вирішального впливу на роботу і Veon, і «Київстару». Також ЗМІ зазначали, що у листопаді 2023 року до складу Ради директорів компанії увійшов американський політик Майк Помпео, що розцінювалося як спроба компанії відмежуватися від своїх зв'язків із російськими власниками

Атака
12 грудня 2023 року о 5:26 ранку фахівці «Київстар» виявили нетипову поведінку в їхній комп'ютерній мережі.

О 6:30 співробітники «Київстар» зрозуміли, що компанія зазнає потужної хакерської атаки. При цьому метою атаки була core network — ядро мережі, що відповідає за обробку та маршрутизацію трафіку між користувачами та сервісами.

О 8:04 «Київстар» публічно повідомив про технічний збій у своїй роботі та попередив про можливі обмеження послуг для своїх абонентів. У цей же час у внутрішніх чатах співробітників компанії поширилися повідомлення про атаку на core network та бази даних компанії. У цей же час деякі анонімні телеграм-канали почали поширювати фейкову інформацію про обшуки в офісах «Київстар».

Протягом кількох наступних годин став очевидним масштаб проблеми. По всій Україні абоненти компанії «Київстар» залишилися без мобільного зв'язку та домашнього інтернет. Абонентам перестали приходити сповіщення про повітряну тривогу. Припинив роботу і офіційний сайт компанії, та її мобільний додаток. Виникли проблеми у роботі всіх систем, пов'язаних із цим оператором. Так, у низці міст довелося вручну відключати вуличне освітлення. Перестала працювати частина банкоматів та платіжних терміналів українських банків. Про значні проблеми повідомили в Ощадбанку, Приватбанку та Райффайзен Банку. Інші банки зазнали менше труднощів. Однак monobank заявив, що зазнав масованої DDoS-атаки протягом 12 грудня, проте банк «зберіг ситуацію під контролем». З проблемами зіткнулися і інтернет-магазини, і Нова пошта, і різні сервіси на кшталт Tabletki.ua, Uklon або Glovo. Також в уряді України повідомили про збої у роботі деяких охоронних систем та гарячих ліній.

Ближче до полудня «Київстар» офіційно визнав, що зазнав великої хакерської атаки. У ЗМІ з'явилися повідомлення, що відновлення мережі може тривати щонайменше тиждень.

Хакерам вдалося не лише вивести з ладу головний пункт управління мережею «Київстар», а й «знести» конфігурацію на транзитних базових станціях.

Абонентам «Київстар» виявився недоступний національний роумінг, хоча рекомендація абонентам «Київстар» скористатися такою можливістю з'явилася на державному сервісі «Дія». За словами Мінцифри України, роумінг не працював через те, що «мережа Київстару не може передати інформацію про своїх абонентів мережам інших операторів». Однак у Держспецзв'язку України заявили, що для запобігання перевантаженню інших операторів зв'язку на запит СБУ було тимчасово заблоковано національний роумінг для абонентів «Київстар».

Інші українські оператори зв'язку, Vodafone та lifecell, продовжували працювати, хоча й повідомили про збільшення навантаження на їхню інфраструктуру через наплив абонентів. Так, у lifecell повідомили, що попит на eSIM збільшився удесятеро.

Відновлення
12 грудня 2023 року до 20:00 «Київстар» почав відновлювати доступ абонентів до послуг фіксованого зв'язку.

13 грудня 2023 року «Київстар» почав поступово відновлювати мобільний зв'язок. З 18.00 почалося включення голосових дзвінків з мобільного зв'язку в окремих регіонах України, SMS та мобільний інтернет залишалися недоступними. Водночас МВС України попередило про активізацію шахраїв, які використовували фішингові посилання з фальшивими повідомленнями нібито від «Київстар» про терміни відновлення зв'язку та компенсацій абонентам.

14 грудня 2023 року «Київстар» увімкнув голосовий зв'язок та відновив роботу домашнього інтернету на 93 %.

SNM. #4. Fails samples – вчимося на чужих помилках ***

- *Системний та мережевий моніторинг. Лекція #9. Найвідоміші приклади порушення кібербезпеки.*

15 грудня 2023 року «Київстар» увімкнув мобільний інтернет по всій підконтрольній Україні території, включаючи стандарт 4G.

21 грудня 2023 в «Київстар» заявили, що повністю відновили всі базові сервіси, які постраждали через хакерську атаку. Раніше у компанії запевнили, що, попри збій в роботі, який стався після хакерської атаки 12-го грудня, абонентська інформація та персональні дані перебувають у безпеці. Після відновлення від хакерської атаки в компанії вирішили скасувати планову плату за тариф для всіх своїх користувачів.

Наслідки
Президент компанії «Київстар» Олександр Комаров заявив, що компанія зазнала дуже потужної хакерської атаки на віртуальну інфраструктуру. За його словами, IT-інфраструктура компанії була «частково зруйнована». При цьому компанія «Київстар» заявила, що персональні дані абонентів не скомпрометовані: «Це війна. Вона відбувається не тільки на полі бою, а й у віртуальному просторі, в кіберпросторі. На жаль, ми уражені внаслідок цієї війни. Це було проникнення в інфраструктуру та її руйнування». За його словами, «це найбільша хакерська атака на телеком-інфраструктуру у світі. Вдалих атак такого масштабу не було. І, будьмо відверті, не так багато країн, на які напала Росія». При цьому він зазначав, що терміни відновлення роботи сервісів неясні.

До ліквідації наслідків атаки були залучені компанії Microsoft, Cisco, Ericsson.

За словами офіційних осіб ЗСУ, збій у роботі «Київстар» не вплинув на дії українських військовослужбовців на лінії фронту. У ГУР МО України заявили, що основною метою атаки був удар по цивільному населенню України, а не військовим.

Заступник глави Нацбанку України Олексій Шабан заявив, що українські банки мають створити резервні канали зв'язку для своєї інфраструктури через збої частини POS-терміналів після хакерської атаки на «Київстар». Він також зазначив, що Нацбанк «протягом 2022—2023 років постійно фіксував кібератаки різного рівня складності на об'єкти інформаційної інфраструктури банків та небанківських фінустанов» та закликав фінансові установи до посилення їхньої кібербезпеки.

Розслідування
У розслідуванні того, що сталося, брали участь співробітники СБУ та Держспецзв'язку України.
СБУ відкрила кримінальну справу за фактом атаки на «Київстар» за вісьмома статтями Кримінального кодексу України.

12 грудня 2023 року СБУ висунула версію, що за тим, що сталося, стоять спецслужби Росії.

12 грудня 2023 року російське хакерське угруповування Killnet заявило, що стоїть за атакою на «Київстар». Однак жодних доказів угруповання не надало.

13 грудня 2023 року гендиректор «Київстар» Олександр Комаров заявив, що хакери зламали комп'ютерний захист компанії за допомогою скомпрометованого облікового запису одного із співробітників «Київстар». Він зазначив, що у будь-якій організації можуть бути люди, які «наводять російські ракети або віддають свої паролі, тому що добре працюють соціальні інженери».

13 грудня 2023 року відповідальність за атаку взяло на себе російське хакерське угруповання «Солнцепёк». На своєму телеграм-каналі вони заявили, що знищили «10 тисяч комп'ютерів, понад 4 тисячі серверів, всі системи хмарного зберігання даних і резервного копіювання». Вони заявили, що атакували «Київстар», оскільки компанія «забезпечує зв'язок Збройних Сил України, а також державні органи та силові структури України». Вони також пригрозили іншим українським компаніям, які допомагають українській армії. Того ж дня СБУ заявила: «Відповідальність за атаку вже взяло на себе одне з російських псевдохакерських угруповань. Вона є хакерським підрозділом головного управління Генштабу Збройних Сил Росії», уточнивши що мають на увазі саме «Солнцепёк».

У телеграм-каналі «Солнцепёк» опублікували чотири скріншоти, які повинні були підтвердити їхню причетність до атаки на «Київстар». Колишній заступник глави українського Держспецзв'язку Віктор Жора зазначав: «Якщо опубліковані скріншоти справжні, то ворог був присутній у мережі досить довго, добре вивчив топологію та інфраструктуру сервісів». Американський фахівець з кібербезпеки Алекс Холден зазначав, що скріншоти були зроблені ще в листопаді 2023 року. Холден говорив, що згідно з ними хакери отримали доступ до системи Active Directory, яка дозволяє «адміністраторам керувати доступом користувачів до різних ресурсів, встановлювати правила безпеки, надавати дозволи на використання різних програм та служб, інтегрувати нові комп'ютери в мережу». Віктор Жора зазначав, що згідно з цими знімками хакери отримали доступ до ключових вузлів інфраструктури «Київстар» — контролера домену та сервісів віртуалізації. За словами Жори, такий доступ неможливо отримати швидко і діяльність хакерів вимагала максимальної скритності дій. Холден зазначав, що на скріншотах не було даних, які б говорили про отримання хакерами доступ до персональних даних абонентів «Київстар».

У компанії «Київстар» заперечували заяви угруповання «Солнцепёк» про знищення тисяч комп'ютерів, а продемонстровані хакерами скріншоти в компанії назвали «довільно зібраними технологічними даними».

Чого ми можемо навчитися з прикладу кібератаки «Київстар» у 2023 році?
Атака на "Київстар" продемонструвала, що кіберзлочинці можуть завдати шкоди навіть найстійкішим організаціям. Це підкреслює необхідність постійного вдосконалення кіберзахисних заходів та тестування їх на стійкість до нових та витончених методів атак.

- ✓ Через атаку "Київстар" було втрачено доступ до деяких даних та систем. Це підкреслює важливість наявності надійних планів резервного копіювання та відновлення, які дозволяють організаціям швидко відновитися після кіберінцидентів.
- ✓ "Київстар" тісно співпрацював з державними органами під час та після атаки. Це підкреслює важливість співпраці між державним і приватним секторами для боротьби з кіберзлочинністю та обміну інформацією про кіберзагрози.
- ✓ "Київстар" публічно оголосив про кібератаки. Це підкреслює важливість прозорості та відкритості у питаннях кібербезпеки, що дозволяє іншим організаціям вчитися на чужих помилках та вживати заходів для захисту від подібних атак.
- ✓ Ця атака підвищила обізнаність про кіберзагрози серед населення України. Це підкреслює важливість освіти та навчання з питань кібербезпеки для всіх користувачів, щоб вони могли краще захищати себе від онлайн-ризиків.
- ✓ Кібербезпека – це не просто технічна проблема, а й питання управління, культури та людського фактора. Це підкреслює необхідність комплексного підходу до кібербезпеки, який поєднує в собі технічні заходи, політики та процедури, а також навчання та підвищення обізнаності співробітників.

SNM. #4. Fails samples – вчимося на чужих помилках ***

- *Системний та мережевий моніторинг. Лекція #9. Найвідоміші приклади порушення кібербезпеки.*

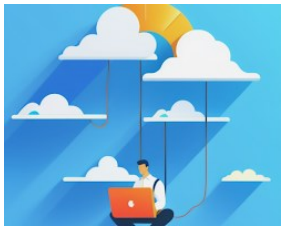
І два висновки, які повністю повторюють те, що суспільство винесло зі згаданої раніше атаки Petya

- ✓ Інвестування в кібербезпеку є вигідним. Організації, які інвестують у кібербезпеку, краще підготовлені до кібератак і з меншою ймовірністю зазнають значних збитків.
- ✓ Атака на "Київстар" продемонструвала, що кіберстійкість – це не просто відновлення після кіберінцидентів, а й здатність адаптуватися до нових кіберзагроз і продовжувати свою діяльність в умовах постійного кіберризику.

❖ **Факти помилок в налаштуванні моніторингу мереж та інфраструктури, що призвели до масштабних аварій за останні два роки:**

✓ **2023:**

17 січня: Аварія в Google Cloud призвела до збоїв у роботі багатьох онлайн-сервісів, включаючи YouTube, Gmail, Spotify та Pinterest. Причиною стала помилка в налаштуванні одного з балансувальників навантаження, що призвело до перевантаження та відключення деяких серверів.



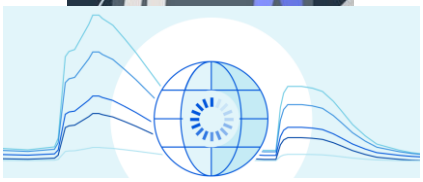
21 лютого: Аварія в Microsoft Azure призвела до збоїв у роботі багатьох веб-сайтів та онлайн-сервісів, включаючи Office 365, Teams та Xbox Live. Причиною стала помилка в налаштуванні системи кешування DNS, що призвело до неможливості для користувачів отримати доступ до деяких ресурсів.

8 березня: Аварія в Amazon Web Services (AWS) призвела до збоїв у роботі багатьох онлайн-сервісів, включаючи Reddit, Twitch та Snapchat. Причиною стала помилка в налаштуванні одного з мережевих маршрутизаторів, що призвело до втрати зв'язку між деякими серверами.

✓ **2022:**

4 грудня: Аварія в Facebook призвела до збоїв у роботі Facebook, Instagram та WhatsApp. Причиною стала помилка в налаштуванні системи доменних імен (DNS), що призвело до неможливості для користувачів отримати доступ до цих сервісів.

9 жовтня: Аварія в Cloudflare призвела до збоїв у роботі багатьох веб-сайтів та онлайн-сервісів, включаючи Wikipedia, Reddit та Discord. Причиною стала помилка в налаштуванні одного з балансувальників навантаження, що призвело до перевантаження та відключення деяких серверів.



22 лютого: Аварія в OVHcloud призвела до збоїв у роботі багатьох веб-сайтів та онлайн-сервісів, розміщених в Європі. Причиною стала пожежа в одному з дата-центрів, що призвело до втрати живлення та доступу до даних.

Важливо зазначити, що це лише деякі з найвідоміших прикладів аварій, пов'язаних з помилками в налаштуванні моніторингу мереж та інфраструктури. Насправді, подібні інциденти трапляються значно частіше, але не завжди отримують широке висвітлення в ЗМІ.

Це підкреслює важливість ретельного налаштування та тестування систем моніторингу, а також постійного навчання та підвищення кваліфікації персоналу, відповідального за кібербезпеку.

Налаштування моніторингу, навчання персоналу та збереження конфіденційності є важливими аспектами в управлінні будь-якою системою.

Оптимальний підхід передбачає розробку докладного плану та процедур для кожного з цих аспектів. Важливо постійно вдосконалювати ці процеси, враховуючи зміни в інфраструктурі та потреби організації.