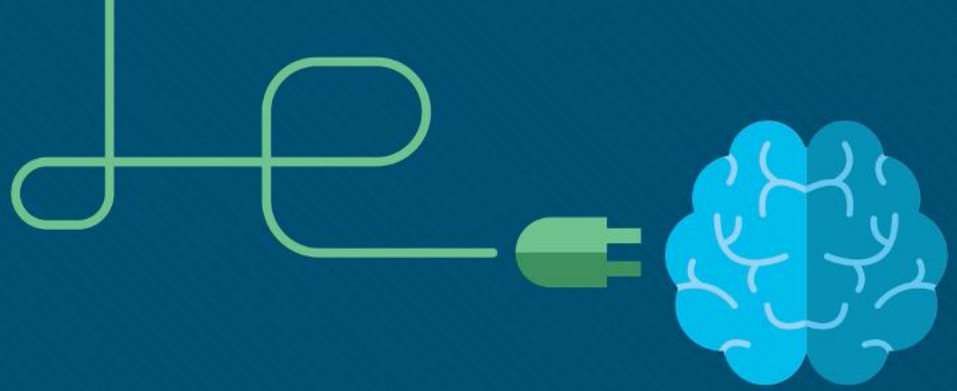


Розділ 4. Захист організації

Вступ до кібербезпеки (I2CS)

Мета розділу

Розділ 4. Захист організації

Мета розділу: Пояснити, як організації можуть захистити свою діяльність від цих атак.

Назва теми	Мета вивчення теми
Пристрої та технології кібербезпеки	Пояснити про різні брандмауери, засоби безпеки та програмне забезпечення, які використовуються фахівцями з кібербезпеки для захисту мережі, даних і обладнання організації.
Підхід до кібербезпеки на основі поведінки	Пояснити, як виявити кіберзагрозу за допомогою підходів безпеки, заснованих на поведінці.
Підхід Cisco до кібербезпеки	Пояснити підхід Cisco до кібербезпеки, включно з групою швидкого реагування CSIRT та що таке збірка сценаріїв з організації захисту.

4.1. Пристрої та технології кібербезпеки

Пристрої безпеки

- Пристроями безпеки можуть бути окремі пристрої, як-от маршрутизатор або програмні засоби, які запускаються на мережному пристрої. Вони діляться на шість загальних категорій.

  - **Маршрутизатори:** Хоча маршрутизатори в основному використовуються для з'єднання різних сегментів мережі разом, вони зазвичай також забезпечують основні можливості фільтрації трафіку. Ця інформація може допомогти вам визначити, які комп'ютери з певного сегмента мережі можуть взаємодіяти і з якими сегментами мережі.

  - **Міжмережні екрани** можуть глибше вивчати сам мережний трафік і виявляти шкідливу поведінку, яку потрібно заблокувати. Міжмережні екрани можуть мати складні політики безпеки, які застосовуються до трафіку, який проходить через них.

  - **Системи запобігання вторгнень (IPS)** використовують набір сигнатур трафіку, які відповідають шкідливому трафіку і атакам та блокують зв'язок при співпадінні.

Пристрої безпеки (Прод.)

- **Системи віртуальних приватних мереж VPN** дозволяють віддаленим співробітникам використовувати безпечний зашифрований тунель зі свого мобільного комп'ютера та безпечно підключатися до мережі організації. Системи VPN також можуть безпечно з'єднувати філії з мережею центрального офісу.

- **Антивірусне програмне забезпечення:** Ці системи використовують сигнатури або поведінковий аналіз програм для виявлення та блокування виконання шкідливого коду.

- **Інші пристрої безпеки** містять засоби захисту веб та електронної пошти, пристрої дешифрування, сервери керування доступом клієнтів та системи контролю безпеки.

Міжмережні екрани

- В комп'ютерних мережах міжмережний екран використовується для контролю або фільтрації повідомлень, яким дозволено входити/виходити до/з пристрою або мережі. Міжмережний екран може встановлюватися на одному комп'ютері з метою його захисту (міжмережний екран на базі вузла), або він може бути автономним пристроєм, який захищає комп'ютери та всі інші пристрої у мережі (мережний міжмережний екран).

- Оскільки комп’ютерні та мережні атаки стали більш складними, були розроблені нові типи міжмережних екранів для задоволення різних потреб.

    - **Міжмережний екран NAT** фільтрує з'єднання на основі IP-адрес джерела та призначення.

    - **Міжмережний екран транспортного рівня** фільтрує на основі портів відправника та отримувача, стану з'єднання.

Міжмережні екрани (прод.)

- **Міжмережний екран прикладного рівня** – фільтрування на основі типу застосунку, програми або сервісу.
- **Міжмережний екран на основі контексту** – фільтрування на основі користувача, пристрою, ролі, типу застосунку та профілю загроз.
- **Проксі-сервер** фільтрує запити веб-контенту, наприклад URL-адреси, доменні імена та типи медіа.
- **Зворотній проксі-сервер** – розміщується перед веб-серверами і захищає, приховує, розвантажує та розподіляє доступ до веб-серверів.
- **Міжмережний екран (NAT)** - приховує або маскує приватні адреси вузлів у мережі.
- **Міжмережний екран на основі вузла** фільтрує порти та виклики системних служб на одному комп'ютері.

Сканування портів (Port Scanning)

- В мережах кожному застосунку, запущеному на пристрої, призначається ідентифікатор, який називається номером порта. Саме завдяки використанню цього номеру на обох кінцях сеансу зв'язку необхідні дані передаються до потрібного застосунку. Сканування портів – це процес зондування комп'ютера, сервера або іншого мережного пристрою для виявлення відкритих портів Він може бути використаний зловмисниками як інструмент розвідки для ідентифікації операційної системи та служб, що працюють на комп'ютері або вузлі, або може бути використаний мережним адміністратором для перевірки мережних політик безпеки.

- Завантажте та запустіть інструмент сканування портів, наприклад Zenmap. Введіть IP-адресу свого комп’ютера, виберіть профіль сканування за замовчуванням і натисніть «сканувати».

- Після сканування Nmap повідомлятиме про всі активні служби (наприклад, веб-сервіси, поштові служби тощо) та номери портів.

Сканування портів (прод.)

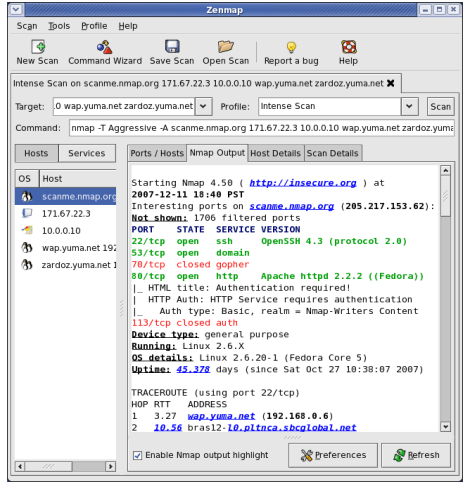
- Сканування також повідомить одну з таких відповідей:
  - «Open» або «Accepted» означає, що до порту або служби, запущеної на комп'ютері, можуть отримати доступ інші мережні пристрої.
  - «Closed», «Denied» або «Not Listening» означає, що порт або служба не запущені на комп'ютері, і тому не можуть бути використані.
  - «Filtered», «Dropped» або «Blocked» означає, що доступ до порту або служби заблоковано брандмауером, і тому його не можна використовувати.

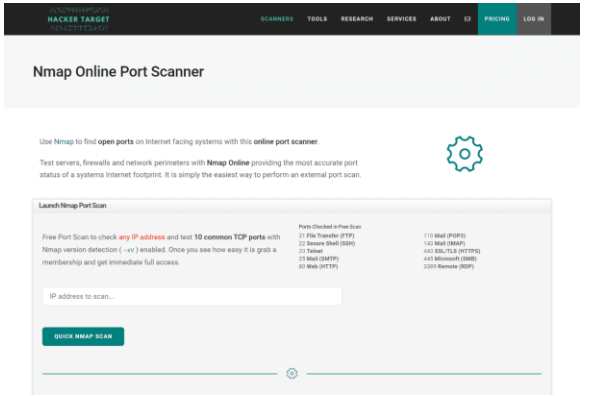
Сканування портів (прод.)

- Щоб виконати сканування портів з поза меж вашої мережі, вам потрібно буде запустити його з публічною IP-адресою міжмережного екрана або маршрутизатора.

- Введіть запит "яка моя IP-адреса?" в пошукову систему, наприклад Google, щоб дізнатися цю інформацію.

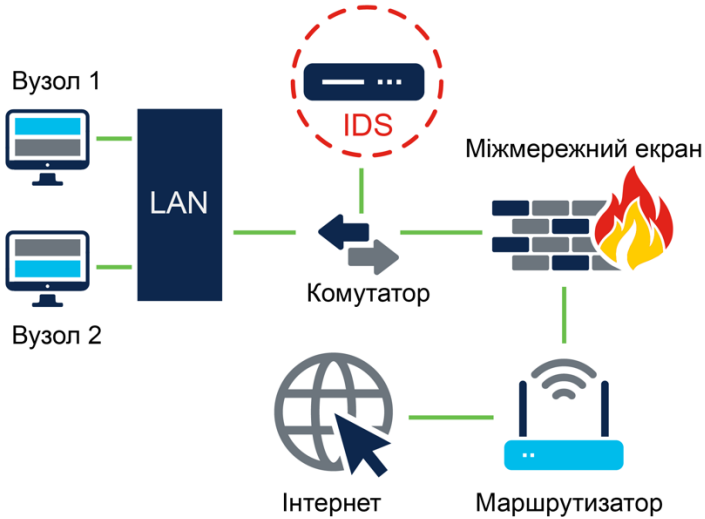
- Перейдіть до Nmap Online Port Scanner, введіть свою загальнодоступну IP-адресу у полі введення та натисніть «Quick Nmap Scan». Якщо відповіддю будуть відкриті порти 21, 22, 25, 80, 443 або 3389, то швидше за все, на вашому маршрутизаторі або міжмережному екрані ввімкнено переадресацію портів, і ви використовуєте сервери у вашій приватній мережі.





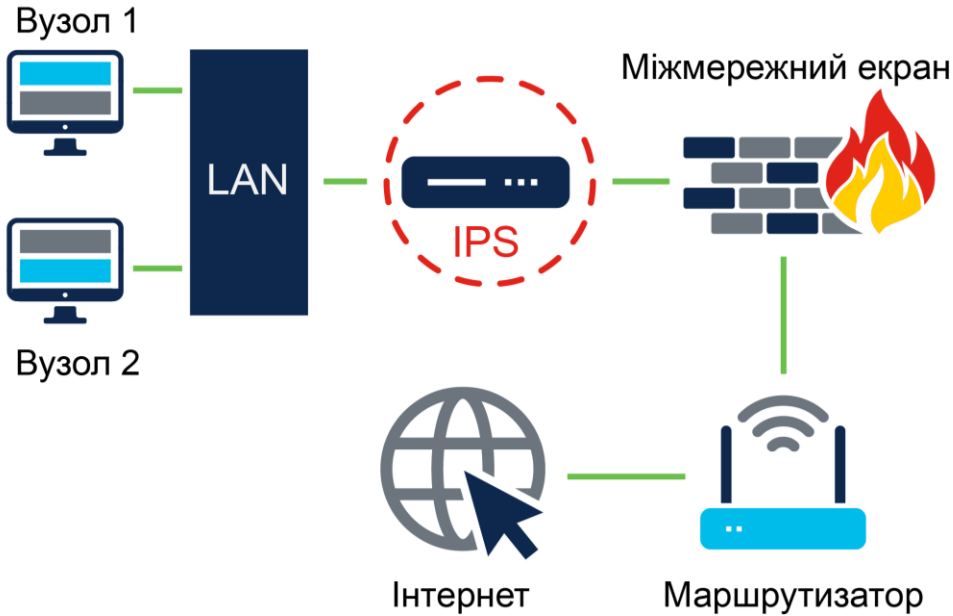
Системи виявлення та запобігання вторгнень

- Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) — це засоби безпеки, розгорнуті в мережі для виявлення та запобігання шкідливій діяльності.
- IDS може бути як виділеним мережним пристроєм, так і одним із кількох інструментів на сервері, міжмережному екрані чи навіть в операційній системі комп'ютера, наприклад Windows чи Linux, який сканує дані на основі бази даних правил чи сигнатур атак, шукаючи шкідливий трафік.
- При виявленні відповідності правилам або сигнатурам IDS реєструє виявлення атаки та створює попередження для мережного адміністратора. Він не вживає заходів, а отже, не запобігає атакам. Завдання IDS - виключно виявлення, реєстрація та створення попередження.
- Сканування, яке виконує IDS, уповільнює роботу мережі (відоме як затримка). Щоб запобігти затримці у мережі, IDS зазвичай розміщують офлайн (в автономному режимі), окремо від звичайного мережного трафіку. Дані копіюються або віддзеркалюються комутатором, а потім пересилаються до IDS для проведення аналізу в режимі офлайн.



Системи виявлення та запобігання вторгнень (прод.)

- IPS може блокувати або відхиляти трафік на основі спрацювання правила або при збігу сигнатури. Однією з найбільш відомих систем IPS/IDS є Snort. Комерційна версія Snort - це Cisco's Sourcefire. Sourcefire може у реальному часі виконувати аналіз трафіку і портів, ведення журналів, пошук і зіставлення контенту, а також виявлення спроб зондування, атак і сканування портів. Це рішення також інтегрується з іншими сторонніми інструментами для створення звітності, аналізу файлів журналів та продуктивності.



Виявлення в реальному часі

- Багато організацій сьогодні не здатні виявити атаки впродовж кількох днів чи навіть місяців після їх появи.

- Виявлення атак у реальному часі потребує активного зондування на наявність атак за допомогою міжмережного екрану та мережних пристроїв IDS/IPS. Також для виявлення шкідливих програм слід використовувати клієнт/серверне програмне забезпечення нового покоління з під'єднання до глобальних онлайн-центрів аналізу загроз. Сьогодні активні пристрої сканування та програмне забезпечення повинні виявляти аномалії мережі, використовуючи аналіз з урахуванням контексту та на основі поведінки.

- DDoS - це одна з найбільших загроз, яка потребує виявлення та реагування у реальному часі. Для багатьох організацій регулярні атаки DDoS порушують роботу інтернет-серверів і негативно впливають на доступність мережі. Від атак DDoS надзвичайно важко захиститись, оскільки пакети-нападники, що виглядають як дозволений трафік, надходять від сотень або тисяч підставних вузлів-зомбі.

Захист від шкідливого програмного забезпечення

- Одним із способів захисту від атак нульового дня та вдосконалених стійких загроз (APT) є використання розширеного рішення для виявлення шкідливих програм на корпоративному рівні, як-от Cisco **Advanced Malware Protection (AMP) Threat Grid**

- AMP - це клієнт/серверне програмне забезпечення, яке розгортається як окремий сервер на кінцевих точках або на інших мережних пристроях безпеки. Воно аналізує мільйони файлів і зіставляє їх із сотнями мільйонів інших проаналізованих зразків шкідливих програм на предмет поведінки, яка виявляє APT. Цей підхід забезпечує глобальну оцінку шкідливих атак, серій зловмисних операцій і їх поширення.

    - **Команді Операційного центру безпеки:** Threat Grid дозволяє команді Операційного центру безпеки (SOC) Cisco збирати більш точні дані, які можна використати.
    - **Група реагування на інциденти:** має доступ до інформації з розслідування кіберінцендентів, на основі якої вона може швидше аналізувати та розуміти підозрілу поведінку.

Захист від шкідливого ПЗ (прод.)

- **Команда розвідки загроз:** Використовуючи цей аналіз, команда розвідки загроз (Threat Intelligence) може активно покращувати інфраструктуру безпеки організації.
- **Інженерна команда з інфраструктури системи безпеки:** Загалом, інженерна команда з інфраструктури системи безпеки може швидше аналізувати інформацію про загрози та реагувати на них, в більшості автоматизовано.

Найкращі практики безпеки

- Багато державних та експертних організацій опублікували рекомендації щодо передових практик безпеки. Деякі найбільш корисні рекомендації містяться в репозиторіях організацій, наприклад, в Ресурсному центрі комп'ютерної безпеки Національного інституту стандартів та технологій США (NIST).

  - **Виконайте оцінку ризиків:** Знання та розуміння цінності того, що ви захищаєте, допоможе виправдати витрати на безпеку.

  - **Створіть політику безпеки:** Чітко окреслює правила організації, посадові ролі, обов'язки та очікування працівників.

  - **Заходи фізичної безпеки:** Обмежте доступ до комунікаційних шаф, серверних кімнат, а також до систем пожежогасіння.

Найкращі практики безпеки (прод.)

- **Заходи щодо безпеки людських ресурсів:** Перевірку репутації мають пройти всі працівники.
- **Виконання і перевірка резервних копій:** Регулярно виконуйте резервне копіювання та перевіряйте можливість відновлення даних з них.
- **Підтримка виправлень і оновлень системи безпеки**: Регулярно оновлюйте операційні системи і програмне забезпечення серверів, клієнтів і мережних пристроїв.
- **Використання засобів контролю доступу**: Налаштуйте ролі і рівні привілеїв користувачів, а також надійну аутентифікацію.
- **Регулярна перевірка реагування на інциденти**: Сформуйте команду реагування на інциденти і перевірте сценарії аварійного реагування.

Найкращі практики безпеки (прод.)

- **Впровадження інструменту моніторингу, аналізу та керування мережею**: Виберіть рішення для моніторингу безпеки, яке інтегрується з іншими технологіями.
- **Впровадження мережних пристроїв безпеки:** Використовуйте нове покоління маршрутизаторів, міжмережних екранів та інших пристроїв безпеки.
- **Впровадження комплексного рішення безпеки кінцевих вузлів:** Використовуйте на рівні підприємства антивірусні програми від всіх видів шкідливого ПЗ.
- **Навчання користувачів:** Забезпечте навчання працівників процедурам безпеки. Однією із найбільш відомих і шанованих організацій з навчання кібербезпеки є Інститут SANS. Натисніть тут , щоб дізнатися більше про SANS та типи навчання та сертифікації, які вони пропонують.
- **Шифрування даних:** Шифруйте всі конфіденційні дані компанії, включно з електронною поштою.

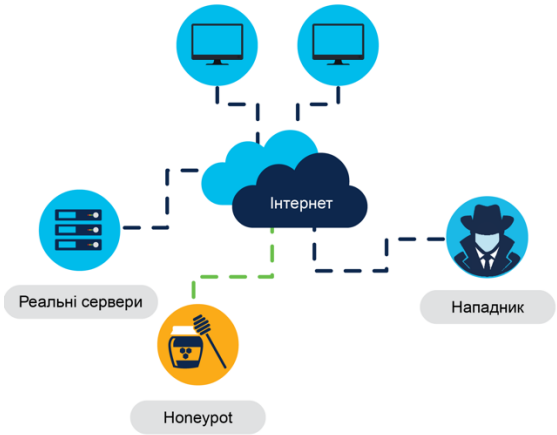
4.2 Підхід до кібербезпеки на основі поведінки

Безпека на основі аналізу поведінки

- Безпека на основі поведінки — це форма виявлення загроз, яка передбачає захоплення та аналіз потоку трафіку між користувачем у локальній мережі та локальним або віддаленим пунктом призначення. Будь-які зміни в звичайних моделях поведінки розцінюються як аномалії і можуть свідчити про атаку.

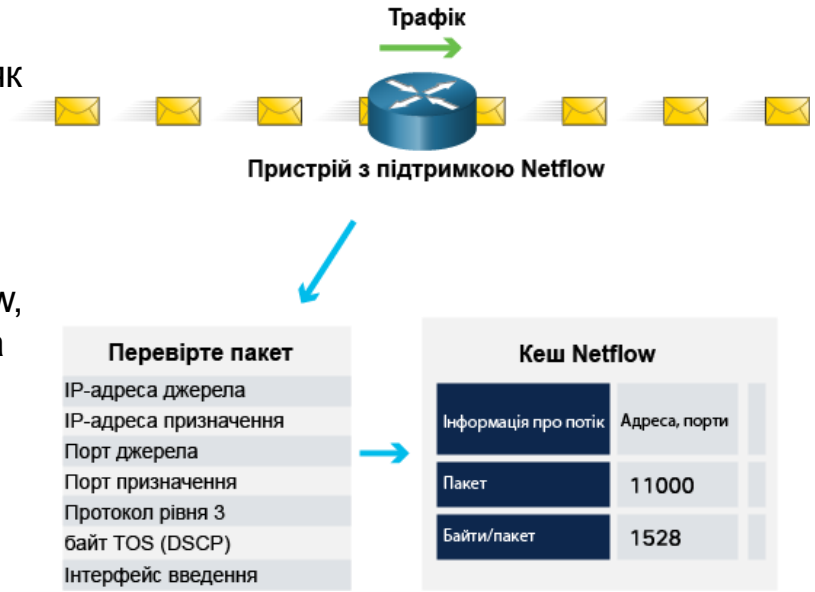
  - **Пастки Honeypot:** Це інструмент виявлення на основі поведінки, який заманює зловмисника, звертаючись до його передбачуваної моделі шкідливої поведінки. Після того, як зловмисник опинився всередині honeypot, адміністратор мережі може захопити, зареєструвати та проаналізувати його поведінку, щоб можна було створити кращий захист.

  - **Cisco Cyber Threat Defense Solution Architecture:** Це архітектура безпеки, яка використовує виявлення на основі аналізу поведінки та індикаторів атаки для забезпечення більшої прозорості, контексту і контролю. Мета полягає в тому, щоб знати, хто здійснює атаку, який тип атаки вони здійснюють і де, коли і як відбувається атака. Для досягнення зазначеної мети ця архітектура безпеки використовує багато технологій захисту.



NetFlow

- Технологія NetFlow використовується для збору інформації про дані, що проходять через мережу, зокрема про те, які є пристрої в мережі, а також коли і як користувачі та пристрої мають доступ до мережі.
- NetFlow - важлива технологія для виявлення кібератак, яка базується на аналізі поведінки. Комутатори, маршрутизатори і міжмережні екрани, оснащені NetFlow, можуть повідомляти інформацію щодо входу, виходу та транзиту даних у мережі.
- Ця інформація надсилається збирачам NetFlow, які збирають, зберігають та аналізують дані NetFlow, які можна використовувати для встановлення базової поведінки для більш ніж 90 атрибутів, таких як IP-адреса джерела та призначення.



Тестування на проникнення

- Тестування на проникнення, широко відоме як «pen testing», є актом оцінки комп'ютерної системи, мережі або організації на наявність вразливостей безпеки. Тестування на проникнення спрямоване на злом систем, на людей, процеси і код, щоб виявити вразливості, які можна було б експлуатувати. Ця інформація потім використовується для покращення захисту системи, щоб забезпечити кращу здатність протистояти кібератакам у майбутньому.

    - **Крок 1. Планування:** Тестувальник на проникнення збирає якомога більше інформації про цільову систему або мережу, її потенційні вразливості та експлойти для використання проти неї. Це передбачає проведення пасивної або активної розвідки (отримання відбитка, footprinting) та дослідження вразливості.

Тестування на проникнення (прод.)

- **Крок 2: Сканування:** Тестувальник на проникнення проводить активну розвідку, щоб дослідити цільову систему або мережу та виявляти потенційні слабкі місця, які, якщо їх експлуатувати, можуть дати зловмиснику доступ.

- Активне спостереження може мітити:

  - сканування портів для виявлення потенційних точок доступу до цільової системи
  - сканування вразливостей для виявлення потенційних уразливостей конкретної цілі, які можна експлуатувати
  - встановлення активного з'єднання з ціллю (перерахування) для ідентифікації облікового запису користувача, облікового запису системи та облікового запису адміністратора.

Тестування на проникнення (прод.)

- **Крок 3: Отримання доступу:** Тестувальник на проникнення намагатиметься отримати доступ до цільової системи та перевіряти мережний трафік, використовуючи різні методи для експлуатації системи, зокрема:

  - запуск експлойту з корисним навантаженням в систему
  - злам фізичних бар'єрів до активів
  - соціальна інженерія
  - використання вразливостей веб-сайту
  - використання вразливостей програмного та апаратного забезпечення або неправильних конфігурацій
  - злам безпеки засобів контролю доступу
  - злам слабко зашифрованого Wi-Fi.

Тестування на проникнення (прод.)

- **Крок 4: Підтримання доступу:** Тестувальник на проникнення підтримуватиме доступ до цілі, щоб з'ясувати, які дані та системи є вразливими для експлуатації. Важливо, щоб дії залишалися непоміченими, зазвичай використовуючи бекдори, троянські коні, руткіти та інші приховані канали, щоб приховати свою присутність.

- Коли ця інфраструктура буде створена, тестувальник на проникнення приступить до збору даних, які вважаються цінними.

- **Крок 5:** Тестувальник на проникнення надасть зворотний зв'язок за допомогою звіту, який рекомендує оновлення продуктів, політик та навчання для підвищення безпеки організації.

Зменшення наслідків

- Хоча сьогодні більшість організацій усвідомлюють загальні загрози безпеці та докладають значних зусиль для їх запобігання, жоден набір практик безпеки не є надійним. Тому організації повинні бути готові стримати збиток, якщо станеться порушення безпеки. І вони повинні діяти швидко!
    - **Розкажіть про проблему:** Спілкування створює прозорість, що дуже важливо в таких ситуаціях.
        - Всі внутрішні співробітники повинні бути поінформовані і чітко озвучений план дій.
        - З зовнішніми клієнтами необхідно зв'язатися безпосередньо, а також потрібно зробити офіційне повідомлення.
    - **Будьте щирими та відповідальними:** Відповідайте на порушення чесно і щиро, беручи відповідальність за вину організації.

Зменшення наслідків (прод.)

- **Надайте подробиці:** Поясніть, чому ситуація відбулася і що конкретно було скомпрометовано. Загалом очікується, що організації оплачуватимуть будь-які витрати клієнтів, пов'язані з подіями крадіжки особистих даних, що сталися в результаті порушення безпеки.

- **Знайдіть причину:** Вживайте заходів, щоб зрозуміти, що спричинило та сприяло порушенню. Це може передбачати найм експертів-криміналістів для дослідження та з'ясування деталей.

- **Застосовуйте отриманий досвід:** Переконайтеся, що всі уроки, отримані під час розслідувань кіберінцедентів, враховані, щоб запобігти подібним порушенням у майбутньому.

- **Перевірте і ще раз перевірте:** Зловмисники часто намагаються залишити чорні ходи для полегшення майбутніх втручань. Щоб запобігти цьому, ви повинні переконатися, що всі системи чисті, немає ніяких «чорних ходів» для видалення, і більше нічого не скомпрометувати.

- **Навчайте:** Підвищуйте обізнаність, тренуйте та навчайте співробітників, партнерів і клієнтів, як запобігти майбутнім порушенням.

Що таке управління ризиками?

- **Управління ризиками:** Це формальний процес постійного виявлення та оцінки ризиків з метою зменшення впливу загроз і вразливостей. Ви не можете повністю усунути ризик, але ви можете визначити прийнятні рівні, зваживши вплив загрози з витратами на впровадження засобів контролю для її пом'якшення. Вартість засобів захисту завжди повинна дорівнювати, щонайбільше, вартості активу, який ви захищаєте.

  - **Окресліть ризик:** Визначте загрози, які підвищують ризик. Загрози можуть містити процеси, продукти, атаки, потенційний збій або порушення роботи послуг, негативне сприйняття репутації організації, потенційну юридичну відповідальність або втрату інтелектуальної власності.

  - **Оцініть ризик:** Визначте серйозність кожної загрози. Наприклад, деякі загрози можуть призвести до зупинки всієї організації, тоді як інші загрози можуть бути лише незначними незручностями. Ризик можна визначити за пріоритетом, оцінюючи фінансовий вплив (кількісний аналіз) або масштабований вплив на діяльність організації (якісний аналіз).

Що таке управління ризиками? (прод.)

- **Реагуйте на ризик:** Розробіть план дій для зменшення загального ризику організації, в якому детально вказано, де ризик можна усунути, пом'якшити, перенести чи прийняти.
- **Слідкуйте за ризиком:** Постійно переглядайте будь-який ризик, який зменшується шляхом усунення, пом'якшення чи перенесення. Пам'ятайте, що ви не можете усунути всі ризики, тому ви повинні уважно стежити за будь-якими загрозами.

4.3 Підхід Cisco до кібербезпеки

Cisco's CSIRT

- Багато великих організацій мають групу реагування на інциденти з комп'ютерною безпекою (CSIRT), щоб отримувати, переглядати та реагувати на повідомлення про інциденти комп'ютерної безпеки. Cisco CSIRT робить ще один крок і забезпечує профілактичну оцінку загроз, план пом'якшення, аналіз тенденцій інцидентів та огляд архітектури безпеки, щоб запобігти інцидентам безпеки.

- CSIRT Cisco використовує проактивний підхід, співпрацюючи з Форумом груп реагування на інциденти з кібербезпеки (FIRST), Національним обміном інформацією з безпеки (NSIE), Обміном інформації про оборонну безпеку (DSIE) та Центром аналізу та дослідження операцій DNS (DNS-OARC), щоб бути в курсі нових розробок. Це гарантує, що ми будемо в курсі нових подій.

- Існують державні та публічні організації CSIRT, такі як відділ CERT Інституту програмного забезпечення в університеті Карнегі-Меллона, які допомагають організаціям та державним CSIRT розвивати, застосовувати та вдосконалювати свої можливості з керування інцидентами.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

computer emergency response team CERT-EU for the EU institutions, bodies and agencies

FIRST
Improving Security Together

APCERT
Asia Pacific Computer Emergency Response Team

Software Engineering Institute
Carnegie Mellon University

Збірка сценаріїв з організації захисту

Найкращий спосіб підготуватися до порушення безпеки - це запобігти йому. Організації повинні керуватися наступним:

- як визначити ризик кібербезпеки для систем, активів, даних і можливостей
- впровадження запобіжних заходів та навчання персоналу
- гнучкий план реагування, який мінімізує вплив і збиток у разі порушення безпеки
- заходи та процеси безпеки, які необхідно запровадити після порушення безпеки.

Вся ця інформація має бути додана до посібника з безпеки.

Посібник з безпеки (прод.)

Посібник з безпеки — це набір повторюваних запитів або звітів, які описують стандартизований процес виявлення інцидентів та реагування на них. В ідеалі посібник з безпеки повинен:

- висвітлювати, як ідентифікувати та автоматизувати відповідь на поширені загрози, такі як виявлення комп'ютерів, заражених шкідливим програмним забезпеченням, підозріла мережна активність або невдалі спроби аутентифікації
- описувати та визначати вхідний та вихідний трафік
- надавати зведену інформацію, разом з тенденціями, статистикою та метриками.
- забезпечувати зручний та швидкий доступу до статистики та метрик
- корелювати події з усіх відповідних джерел даних.

Інструменти для запобігання та виявлення інцидентів

Ось деякі з інструментів, що використовуються для запобігання та виявлення інцидентів:

- **Система керування інформаційною безпекою та подіями безпеки (SIEM)** збирає та аналізує сповіщення безпеки, журнали та інші дані в реальному часі та дані отримані в минулому від пристроїв безпеки в мережі, щоб полегшити раннє виявлення кібератак.

- **Система запобігання втраті даних (DLP)** призначена для запобігання крадіжці конфіденційних даних або їх витоку з мережі. Вона відстежує та захищає дані в трьох різних станах: дані, що використовуються (дані, до яких отримує доступ користувач), дані в русі (дані, що переміщуються по мережі) і дані в стані спокою (дані, що зберігаються в комп'ютерній мережі або пристрої).

Cisco ISE та TrustSec

Cisco Identity Services Engine (ISE) і TrustSec забезпечують доступ користувачів до мережних ресурсів, створюючи політики контролю доступу на основі ролей.

4.4 Контрольна робота

Що ми вивчили у цьому розділі?

- Пристроями безпеки можуть бути окремі пристрої, як-от маршрутизатор або програмні засоби, які запускаються на мережному пристрої.
- В комп'ютерних мережах міжмережний екран використовується для контролю або фільтрації повідомлень, яким дозволено входити/виходити до/з пристрою або мережі.
- Сканування портів - це процес зондування комп'ютера, сервера або іншого мережного пристрою для виявлення відкритих портів.
- Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) — це засоби безпеки, розгорнуті в мережі для виявлення та запобігання шкідливій діяльності.
- Виявлення атак у реальному часі потребує активного зондування на наявність атак за допомогою міжмережного екрану та мережних пристроїв IDS/IPS.
- Безпека на основі поведінки — це форма виявлення загроз, яка передбачає захоплення та аналіз потоку трафіку між користувачем у локальній мережі та локальним або віддаленим пунктом призначення.
- NetFlow - важлива технологія для виявлення кібератак, яка базується на аналізі поведінки.

Що ми вивчили у цьому розділі? (прод.)

- Тестування на проникнення спрямоване на злом систем, на людей, процеси і код, щоб виявити вразливості, які можна було б експлуатувати.
- **Управління ризиками:** Це формальний процес постійного виявлення та оцінки ризиків з метою зменшення впливу загроз і вразливостей.
- Посібник з безпеки — це набір повторюваних запитів або звітів, які описують стандартизований процес виявлення інцидентів та реагування на них.