Sumy State University

Кафедра економічної кібернетики

Co-funded by the European Union

Інженерія кібербезпеки цифрової економіки

Спікер: Гриценко Костянтин, к.т.н., доцент кафедри економічної кібернетики СумДУ

E-maill: k.hrytsenko@biem.sumdu.edu.ua

https://ek.biem.sumdu.edu.ua/en/staff/hrytsenko-kostiantyn

Модуль Жан Моне «Розвиток цифрових компетентностей фахівців цифрової економіки та бізнес-лідерів: кращі європейські практики для України»

План

1 Кібербезпека персональних даних.

2 Кібербезпека даних організації.

3 Кібервійна.

4 Шкідливе програмне забезпечення.

5 Методи проникнення.

6 Вразливості кібербезпеки та експлойти.

7 Захист комп’ютера та комп’ютерної мережі.

8 Захист конфіденційності в Інтернет.

9 Пристрої та технології кібербезпеки.

10 Поведінковий підхід до кібербезпеки.

1 Кібербезпека персональних даних

Рівні кібербезпеки

Кібербезпека — це постійні зусилля, спрямовані на захист окремих осіб, організацій та урядів від цифрових атак шляхом захисту комп'ютерних систем, мереж і даних від несанкціонованого використання або пошкодження.

Персональний рівень: На персональному рівні вам потрібно захищати свою особу, свої дані та свої комп'ютерні пристрої.

Рівень організації: На рівні організації рівні кожен співробітник несе відповідальність за захист репутації, даних та клієнтів організації.

Урядовий рівень: Оскільки збирається та поширюється все більше цифрової інформації, її захист стає дуже важливим на урядовому рівні, де на карту поставлені національна безпека, економічна стабільність, а також безпека та добробут громадян.

Кібербезпека персональних даних

Персональні дані – це будь-яка інформація, яка може бути використана для вашої ідентифікації. Вона може існувати як офлайн, так і онлайн.

Офлайн-ідентичність

- Це реальна особистість, яку ви щодня представляєте вдома, в закладі освіти чи на роботі.
- Як результат, ваша родина та друзі знають деталі вашого особистого життя, включаючи ваше повне ім'я, вік та адресу.
- Важливо не забувати про важливість захисту вашої офлайн-ідентичності. Злодії можуть легко вкрасти ваші дані прямо у вас під носом, коли ви не дивитеся!

Онлайн-ідентичність

- Це не просто ім’я, це те, ким ви є і як ви презентуєте себе іншим онлайн.
- Вона включає ім’я користувача або псевдонім, який ви використовуєте для своїх онлайн-акаунтів, а також соціальну ідентичність, яку ви створюєте та відображаєте в онлайн-спільнотах і на веб-сайтах.
- Вам слід обмежити обсяг особистої інформації, яку ви розголошуєте через свою онлайн-ідентичність.

Персональні дані

Персональні дані описують будь-яку інформацію про вас (ім'я, ідентифікаційний код, дату та місце народження, дівоче прізвище вашої матері, фотографії або повідомлення, якими ви обмінювалися з іншими).
Кіберзлочинці можуть використовувати цю конфіденційну інформацію, щоб ідентифікувати вас та видати себе за іншу особу, порушуючи вашу конфіденційність та потенційно завдаючи серйозної шкоди вашій репутації.

Хакери можуть отримати доступ до ваших персональних даних через такі записи:

Медичні записи	Щоразу, коли ви відвідуєте лікаря, персональна інформація щодо вашого фізичного та психічного здоров'я та благополуччя додається до ваших електронних медичних карток. Оскільки більшість цих записів зберігаються в Інтернеті, вам потрібно знати, якою медичною інформацією ви ділитеся. Ці записи виходять за межі кабінету лікаря.
Освітні записи	Вони містять інформацію про вашу академічну кваліфікацію та досягнення. Вони також можуть включати вашу контактну інформацію, записи про відвідуваність занять, медичні записи та записи про вакцинацію, а також будь-які записи про спеціальну освіту, включаючи індивідуальні освітні програми.
Трудова та фінансова документація	Дані про зайнятість можуть бути цінними для хакерів, якщо вони зможуть зібрати інформацію про вашу попередню роботу або навіть оцінки вашої поточної ефективності. Ваші фінансові записи можуть містити інформацію про ваші доходи та витрати, виписки з кредитних карток та реквізити вашого банківського рахунку.

ПРИКЛАДИ КРАДІЖКИ ПЕРСОНАЛЬНИХ ДАНИХ

Витік даних Facebook у квітні 2021 року, коли в Інтернеті було знайдено дані понад 500 мільйонів користувачів Facebook.

Злом Optus (австралійського оператора мобільного зв'язку) у 2022 році. У результаті – витік особистих даних 10 млн клієнтів.

Злом Medibank (одного з найбільших австралійських приватних медичних страхувальників) у 2022 році. Загальна клієнтська база Medibank становить 4 млн клієнтів.

15 найбільших витоків даних 21 століття:

1. Yahoo, 2013, 3 мільярди облікових записів

2. Aadhaar, 2018, 1,1 мільярда ідентифікаційних даних

3. Alibaba, 2018, 1,1 мільярда даних користувачів

4. LinkedIn, 2021, 700 мільйонів користувачів

5. Sina Weibo, 2020, 538 мільйонів облікових записів.

Де знаходяться ваші персональні дані?

Уявіть, що вчора ви поділилися кількома фотографіями зі свого першого робочого дня з кількома близькими друзями. Але це ж має бути нормально, чи не так? Подивимося:

- Ви зробили кілька фотографій на роботі на свій мобільний телефон. Копії цих фотографій тепер доступні на вашому мобільному пристрої.

- Ви поділилися ними з близькими друзями, які живуть у різних куточках світу. Усі ваші друзі завантажили фотографії та тепер мають копії ваших фотографій на своїх пристроях.

- Один із ваших друзів був настільки гордий, що вирішив опублікувати та поділитися вашими фотографіями в Інтернеті. Фотографії більше не лише на вашому пристрої. Вони фактично опинилися на серверах, розташованих у різних частинах світу, і люди, яких ви навіть не знаєте, тепер мають доступ до ваших фотографій.

Де знаходяться ваші персональні дані?

Це лише один приклад, який нагадує нам, що щоразу, коли ми збираємо або передаємо особисті дані, нам слід думати про нашу безпеку.

В Україні діє Закон «Про захист персональних даних», що захищає вашу конфіденційність та персональні дані. Але чи знаєте ви, де знаходяться ваші персональні дані?

- Після призначення лікар оновить вашу медичну карту:
  - Для цілей виставлення рахунків ця інформація може бути передана страховій компанії.
  - У таких випадках ваша медична карта або її частина тепер доступна у страховій компанії.
- Картки лояльності крамниць можуть бути зручним способом заощадити гроші на покупках. Однак крамниця потім використовує цю картку для створення профілю вашої купівельної поведінки, який потім може використовувати для таргетованої реклами спеціальних пропозицій від маркетингових партнерів крамниці.

Розумні пристрої

- Подумайте, як часто ви використовуєте свої комп'ютерні пристрої для доступу до своїх персональних даних?

- Наприклад, якщо ви не обрали отримання паперових виписок, то ви, ймовірно, отримуєте доступ до цифрових копій виписок з банківського рахунку через вебсайт вашого банку.

- А під час сплати рахунку, дуже ймовірно, що ви перерахували необхідні кошти через мобільний банківський застосунок.

- Але окрім можливості доступу до вашої інформації, комп'ютерні пристрої тепер також можуть генерувати інформацію про вас.

- Носимі технології, такі як смарт-годинники та фітнес-трекери, збирають ваші дані для клінічних досліджень, моніторингу здоров'я пацієнтів, а також відстеження фізичної форми та самопочуття. Зі зростанням світового ринку фітнес-трекерів зростає й ризик для ваших персональних даних.

Крадіжка ідентичності

Кіберзлочинці не задовольняються крадіжкою ваших грошей заради короткострокової фінансової вигоди. Вони зацікавлені в довгостроковій вигоді від крадіжки персональних даних.

Крадіжка медичних даних

- Зростання вартості медичного обслуговування призвело до збільшення випадків крадіжки медичних даних, коли кіберзлочинці крадуть медичне страхування, щоб використовувати його для власних потреб.
- У таких випадках будь-які медичні процедури, проведені від вашого імені, будуть збережені у ваших медичних записах.

Банківські шахрайства

- Крадіжка персональних даних може допомогти кіберзлочинцям отримати доступ до банківських рахунків, кредитних карток, профілів у соціальних мережах та інших онлайн-акаунтів.
- Озброївшись цією інформацією, зловмисник може подати фальшиву податкову декларацію та отримати відшкодування. Вони навіть можуть взяти позики на ваше ім'я та зруйнувати ваш кредитний рейтинг.

Кому потрібні ваші персональні дані?

- Якщо ви не платите за це, ви не клієнт, ви — продукт, який продається.
- Не лише злочинці хочуть отримати ваші персональні дані. У таблиці наведено інші організації, які зацікавлені у вашій онлайн-ідентичності, та причини цього.

Ваш інтернет-провайдер	Ваш інтернет-провайдер відстежує вашу онлайн-активність, а в деяких країнах він може продавати ці дані рекламодавцям з метою отримання прибутку. За певних обставин інтернет-провайдери можуть бути юридично зобов'язані ділитися вашою інформацією з державними органами нагляду або органами влади.
Рекламодавці	Цільова реклама є частиною інтернет-досвіду. Рекламодавці відстежують вашу онлайн-активність, таку як ваші звички споживання та особисті вподобання, і надсилають вам цільову рекламу.
Пошукові системи та платформи соціальних мереж	Ці платформи збирають інформацію про вашу стать, геолокацію, номер телефону, а також політичні та релігійні ідеології на основі вашої історії пошуку та онлайн-ідентичності. Потім ця інформація продається рекламодавцям з метою отримання прибутку.
Вебсайти, які ви відвідуєте	Вебсайти використовують файли cookie для відстеження вашої активності, щоб забезпечити вам більш персоналізований досвід. Але це залишає цифровий слід, пов'язаний з вашою онлайн-ідентичністю, який часто може потрапити до рук рекламодавців!

КЕРУВАННЯ ОБЛІКОВИМИ ЗАПИСАМИ

Не використовуйте один і той самий пароль для різних сервісів та платформ.

Створення безпечного пароля є важливим, але незалежно від того, наскільки безпечним є ваш пароль, ви все одно можете бути вразливими через погане керування вашим обліковим записом.

Прикладом поганого керування обліковим записом може бути використання одного й того ж самого безпечного пароля та адреси електронної пошти для кількох облікових записів. Якщо один обліковий запис буде зламано, а ваше ім'я користувача та пароль будуть викрадені, хакери можуть використати цю інформацію для доступу до ваших інших онлайн-акаунтів.

Ви можете зручно увійти на такі веб-сайти, як наприклад Spotify, за допомогою відкритої авторизації через Facebook (**OAuth**), щоб вам не потрібно було створювати окремий обліковий запис для кожного сайту, який ви використовуєте. Однак ця зручність має свою ціну, оскільки щоразу, коли ви використовуєте свій логін Facebook для доступу до іншого сервісу, ви надаєте цьому іншому сервісу доступ до ваших особистих даних, що зберігаються Facebook.

Це також дозволяє зловмиснику потребувати доступу лише до вашого облікового запису Facebook, щоб почати отримувати доступ до всіх інших сайтів, до яких ви прив'язали цей логін Facebook. Використовуючи опцію входу за допомогою Facebook, ви по суті використовуєте Facebook як менеджер паролів, щоб запам'ятати ваше ім'я користувача та пароль для низки сайтів і сервісів.

МЕНЕДЖЕРИ ПАРОЛІВ

Менеджери паролів забезпечують рівень зручності, подібний до відкритої авторизації через Facebook (**OAuth**), але при цьому набагато безпечніші.

Менеджери паролів створюють зашифровану базу даних усіх ваших імен користувачів та паролів, до яких маєте доступ лише ви за допомогою головного пароля. Це означає, що вам потрібно запам’ятати лише один пароль, щоб мати доступ до всіх ваших облікових записів.

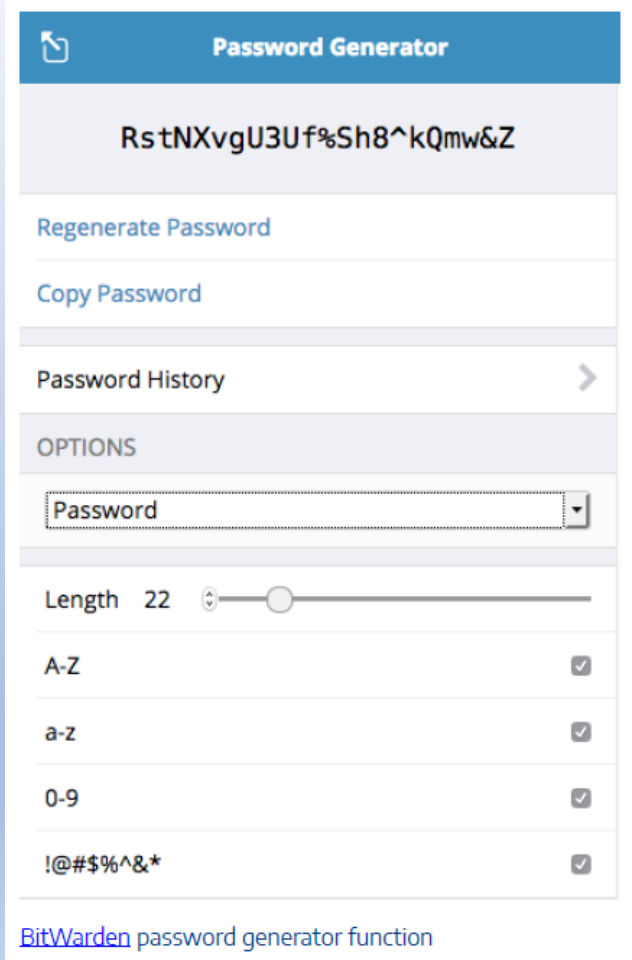
Більшість менеджерів паролів мають можливість генерувати безпечні паролі, які можна використовувати для нових або існуючих входів до облікових записів. Оскільки вам потрібно запам’ятати лише один головний пароль, то ви можете генерувати та зберігати складні паролі для своїх потреб. Таким чином, ви не покладаєтеся на свою пам’ять та прості паролі, щоб запам’ятати багато різних даних для входу до облікового запису.

Щоб спростити вхід на веб-сайт, більшість менеджерів паролів мають розширення для браузера, які або автоматично вставляють інформацію в обов'язкові поля для входу, або дозволяють копіювати та вставляти дані. Не всі веб-сайти та програми дозволяють автоматичне заповнення або вставку даних в поля для входу.

МЕНЕДЖЕРИ ПАРОЛІВ

1Password
Bitwarden
Password Safe
iCloud Keychain
Keepass

Існує велика кількість менеджерів паролів. Багато з них мають блоги на своїх вебсайтах, де обговорюється, як вони працюють і що роблять для захисту ваших даних.



BitWarden password generator function

МЕНЕДЖЕРИ ПАРОЛІВ

Під час прийняття рішення слід враховувати такі питання:

1. Мій пароль зберігається лише на моєму комп'ютері чи він має резервну копію в хмарі?

З огляду на зростаючу популярність використання менеджерів паролів, вони є головною мішенню для витоку даних через величезну кількість інформації про облікові записи, яку вони можуть зберігати. Вам доведеться вибирати між максимальною безпекою та зручністю використання. Якщо менеджер паролів зберігає паролі в хмарі, то він часто має застосунок для мобільного телефону та розширення для веб-браузера, що дозволяє синхронізувати паролі на різних пристроях. Це означає, що ваша інформація надсилається через Інтернет, щоб ваші інші пристрої мали доступ до неї, що робить це менш безпечним, ніж якби вона взагалі не надсилалася через Інтернет.

МЕНЕДЖЕРИ ПАРОЛІВ

2. Якщо резервні копії зберігаються в хмарі, то чи шифрується інформація до чи після резервного копіювання?

Якщо інформація зашифрована після резервного копіювання в хмарі, то вона потенційно була надіслана через Інтернет у вигляді звичайного тексту, і зловмисникам набагато легше отримати до неї доступ.

3. Чи були в минулому зафіксовані випадки порушення роботи менеджера паролів, і як на це відреагував сервіс?

У 2022 році LastPass зазнав порушення безпеки. LastPass публічно розповів про порушення, як воно сталося та що було викрадено. Такий тип комунікації важливий, оскільки дозволяє користувачам змінювати свої паролі, імена користувачів тощо, щоб уникнути проблем у майбутньому.

ДВОФАКТОРНА ТА БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ

В останні роки двофакторна автентифікація (2FA) та багатофакторна автентифікація (MFA) стали більш поширеними способами входу в онлайн-акаунти, допомагаючи захистити користувачів від витоків даних.

Після того, як користувач ввів свої звичайні дані для входу (ім'я користувача та пароль), йому пропонується підтвердити свою особу іншим способом, тобто ввести код, надісланий текстовим повідомленням (SMS) або електронною поштою, підтвердити спробу входу через застосунок на мобільному телефоні або ввести код, згенерований пристроєм автентифікації.

2FA вимагає двох методів автентифікації, а MFA вимагає двох або більше методів.

Two methods of authentication

2 Кібербезпека даних організації

Типи даних організації

Традиційні дані зазвичай генеруються та підтримуються всіма організаціями, великими та малими.

Вони включають:

- **Транзакційні дані -** деталі, що стосуються купівлі-продажу, виробничої діяльності та основних організаційних операцій, як-от будь-яка інформація, що використовується для прийняття рішень щодо працевлаштування.

- **Інтелектуальна власність** - патенти, торговельні марки та плани нових продуктів, дозволяє організації отримувати економічну перевагу над конкурентами. Ця інформація часто вважається комерційною таємницею, і її втрата може мати катастрофічні наслідки для майбутнього компанії.

- **Фінансові дані** - звіти про прибутки та збитки, баланси та звіти про рух грошових коштів, надають уявлення про стан компанії.

Інтернет речей (IoT) і Великі дані (Big Data)

- **Інтернет речей (IoT)** — це велика мережа фізичних об'єктів, таких як датчики, програмне забезпечення та інше обладнання.
- Усі ці «речі» підключені до Інтернету та мають можливість збирати та обмінюватися даними.
- Можливості зберігання даних розширюються завдяки хмарним технологіям та віртуалізації.
- Поява Інтернету речей призвела до експоненціального зростання обсягів даних, створивши нову сферу інтересів у технологіях та бізнесі під назвою **«Big Data»**.

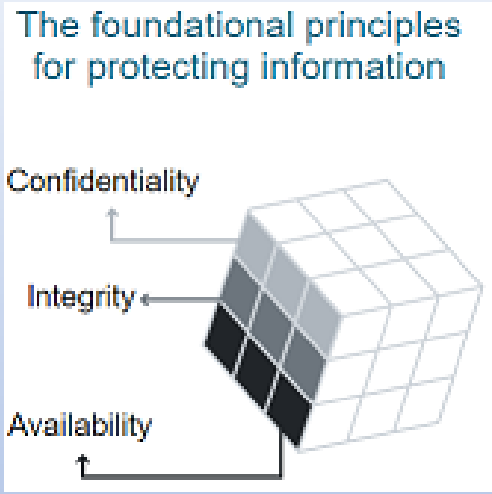
Куб кібербезпеки

Ця модель кібербезпеки має три виміри:

1. **Основоположні принципи захисту інформаційних систем**
   - **Конфіденційність** – це набір правил, що запобігають розголошенню конфіденційної інформації неавторизованим особам, ресурсам і процесам. Методи її забезпечення включають шифрування даних, перевірку особи та двофакторну автентифікацію.

   - **Цілісність** гарантує, що системна інформація або процеси захищені від навмисної або випадкової модифікації. Один зі способів забезпечити це – використовувати **хеш-функцію** або **контрольну суму**.

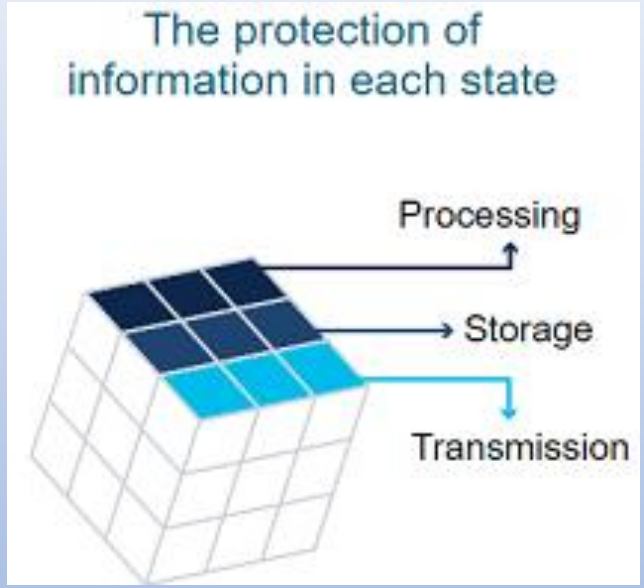
   - **Доступність** означає, що авторизовані користувачі мають доступ до систем і даних, коли і де це потрібно, а ті, хто не відповідає встановленим умовам, не мають доступу. Цього можна досягти шляхом обслуговування обладнання, ремонту апаратного забезпечення, підтримки операційних систем і програмного забезпечення в актуальному стані, а також створення резервних копій.



Куб кібербезпеки

2. Захист інформації в кожному з її можливих станів

- **Оброблення** стосується даних, які використовуються для виконання операції, такої як оновлення запису бази даних (**дані в процесі оброблення**).
- **Сховище** стосується даних, що зберігаються в пам'яті або на постійному пристрої зберігання даних, такому як жорсткий диск, твердотільний накопичувач або USB-накопичувач (**дані в стані спокою**).
- **Передача** стосується даних, що передаються між інформаційними системами (**дані в русі**).



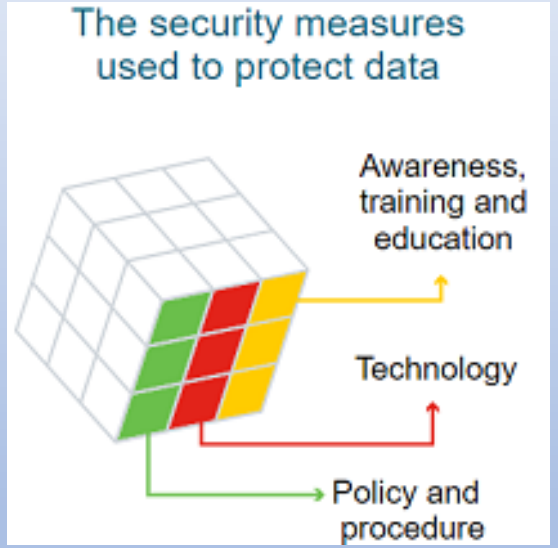
Куб кібербезпеки

3. Заходи безпеки, що використовуються для захисту даних

- **Підвищення обізнаності, навчання та освіта** – це заходи, що вживаються організацією для забезпечення обізнаності користувачів про потенційні загрози кібербезпеці та дії, які вони можуть вжити для захисту комп'ютерних систем.

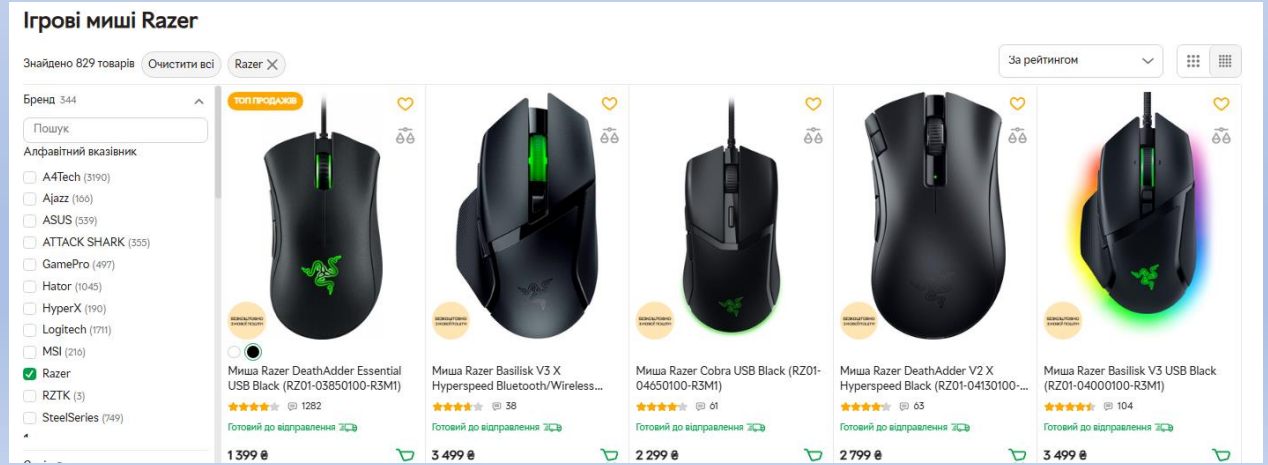
- **Технологія** стосується програмних та апаратних рішень, призначених для захисту комп'ютерних систем, таких як брандмауери, які постійно моніторять вашу мережу в пошуках можливих кіберінцидентів.

- **Політика кібербезпеки** стосується адміністративних заходів, які забезпечують основу для того, як організація впроваджує кібербезпеку, зокрема плани реагування на кіберінциденти та рекомендації щодо найкращих практик кібербезпеки.



Приклади витоку даних

- У серпні 2020 року елітний бренд ігрових аксесуарів Razer зіткнувся з витоком даних, в результаті якого було викрито особисту інформацію приблизно 100 000 клієнтів.
- Консультант з кібербезпеки виявив, що хмарний кластер (група пов'язаних серверів, які забезпечують зберігання даних, бази даних, мережеві з’єднання та програмне забезпечення через Інтернет) був неправильно налаштований та відкрив сегмент інфраструктури Razer для загальнодоступного Інтернету, що призвело до витоку даних.
- Razer знадобилося понад три тижні, щоб захистити хмарний кластер від публічного доступу, протягом яких кіберзлочинці мали доступ до інформації про клієнтів, яка могла бути використана для соціальної інженерії та шахрайських атак.
- Організаціям необхідно застосовувати проактивний підхід до хмарної кібербезпеки, щоб забезпечити захист конфіденційних даних.



Порушення безпеки даних

- Порушення безпеки даних стають поширеними, а наслідки — серйозними.
- Інтернет речей об’єднує дедалі більше пристроїв, створюючи більше можливостей для кібератак.
- Приклади порушення безпеки даних включають:
  - **Ботнет Persirai**
    - У 2017 році ботнет Інтернету речей (IoT) Persirai атакував понад 1000 різних моделей IP-камер, отримавши доступ до відкритих портів для введення команди, яка змушувала камери підключатися до сайту, що встановлював на них шкідливе програмне забезпечення.
    - Після завантаження та запуску шкідливого програмного забезпечення воно видалялося і, таким чином, могло працювати в оперативній пам'яті, щоб уникнути виявлення.
    - Понад 122 000 цих камер від кількох різних виробників були викрадені та використані для здійснення DDoS-атак без відома їхніх власників.
    - DDoS-атака має місце, коли кілька пристроїв, заражених шкідливим програмним забезпеченням, перевантажують ресурси цільової системи.
  - У травні 2025 року Національний центр кібербезпеки Великої Британії (NCSC) звинуватив росію у зламі 10 тисяч камер на кордонах України, біля військових об’єктів і вокзалів для стеження за допомогою Україні. Зловмисники також використали легальні муніципальні сервіси, зокрема камери дорожнього спостереження. Злам давав змогу отримати скриншот зображення з камер. Причинами, які сприяли успіху цієї кібератаки були: слабкий захист комп’ютерних мереж, невчасне оновлення програм, відсутність сегментації мереж, невикористання двофакторної автентифікації, слабкі паролі, ненавчаність персоналу основам кібербезпеки. Під час цієї кібератаки були використані вразливості, виявлені у 2020 та 2021 роках: CVE-2020-12641, CVE-2020-35730, CVE-2021-44026.

Порушення безпеки даних

- **Агентство з юридичної допомоги Великої Британії:**
  - 23 квітня 2025 року агентство з юридичної допомоги Великої Британії було атаковано хакерами, внаслідок чого було викрадено значну кількість персональних даних, включно із кримінальними записами людей, які з 2010 року подавали заяви на отримання юридичної допомоги.
  - Зловмисники отримали доступ до інформації, що стосується заявників, що змусило агентство призупинити роботу своїх онлайн-сервісів.
  - Хакери змогли отримати доступ до персональних даних заявників, зокрема адрес, дат народження, національних ідентифікаційних номерів, а також фінансової інформації – суми внесків, боргів і платежів.
  - Зловмисники можуть використовувати цю інформацію, щоб видавати себе за клієнта.
  - У таких випадках клієнту буде дуже важко довести протилежне, враховуючи, що хакер має доступ до персональної інформації клієнта.

Порушення безпеки даних

Наведені приклади показують, що потенційні наслідки порушення безпеки можуть бути дуже серйозними.

Репутаційна шкода	Порушення кібербезпеки може мати негативний довгостроковий вплив на репутацію організації, яка будувалася роками. Клієнтів, особливо тих, хто постраждав від порушення, необхідно буде повідомити, і вони можуть вимагати компенсації та/або звернутися до надійного та більш безпечного конкурента. Працівники також можуть вирішити звільнитися через скандал. Залежно від серйозності порушення, відновлення репутації організації може зайняти багато часу.
Вандалізм	Хакери можуть пошкодити вебсайт організації, опублікувавши неправдиву інформацію. Вони можуть навіть внести кілька незначних змін до номера контактного телефону або адреси вашої організації, що може бути складно виявити. У будь-якому випадку, онлайн-вандалізм може негативно вплинути на репутацію та довіру до вашої організації.
Крадіжка	Витік даних часто пов’язаний з кіберінцидентом, коли було викрадено конфіденційні персональні дані. Кіберзлочинці можуть оприлюднити цю інформацію або використати її для крадіжки грошей та/або ідентичності людини.
Втрата доходу	Фінансові наслідки порушення кібербезпеки можуть бути руйнівними. Наприклад, хакери можуть зламати вебсайт організації, перешкоджаючи їй вести бізнес онлайн. Втрата інформації про клієнтів може перешкодити зростанню організації. Це може потребувати подальших інвестицій в інфраструктуру кібербезпеки організації. Також що організації можуть зіткнутися з великими штрафами або стягненнями, якщо вони не захищають онлайн-дані.
Пошкоджена інтелектуальна власність	Порушення кібербезпеки може мати руйнівний вплив на конкурентоспроможність організації, особливо якщо хакери зможуть отримати доступ до конфіденційних документів, комерційної таємниці та інтелектуальної власності.

Внутрішні та зовнішні загрози

- Кібератаки можуть виникати як всередині організації, так і ззовні.
- **Внутрішні загрози**
  - Працівники, контрактні співробітники або довірені партнери можуть випадково або навмисно вчиняти такі дії:
    - неналежне поводження з конфіденційними даними
    - сприяння зовнішнім атакам шляхом підключення заражених USB-носіїв до комп'ютерних систем організації
    - запуск шкідливого програмного забезпечення в комп’ютерній мережі організації шляхом натискання на шкідливі електронні листи або відвідування шкідливих вебсайтів
    - загрожування роботі внутрішніх серверів або пристроїв мережевої інфраструктури
- **Зовнішні загрози**
  - Аматори або досвідчені зловмисники поза організацією можуть:
    - використовувати вразливості в комп’ютерній мережі
    - отримувати несанкціонований доступ до комп’ютерних систем
    - використовувати соціальну інженерію для отримання несанкціонованого доступу до даних організації

3 Кібервійна

Мета кібервійни

- Головною метою кібервійни є отримання переваги над супротивниками, незалежно від того, чи є це держави, чи конкуренти. Кібервійна передбачає такі дії:

- **Збирання інформації про технології та/або оборонні таємниці**

  - Країна чи міжнародна організація може вести кібервійну, щоб викрасти оборонні секрети та зібрати інформацію про технології, які допоможуть скоротити розрив у промисловості та військовому потенціалі.

  - Крім того, скомпрометовані конфіденційні дані можуть дати зловмисникам важелі впливу для шантажу персоналу іноземного уряду.

  - Частка кібершпигунства середі цілей кібервійни складає 70-80%, а 20-30% - це спроби зупинки критичної інфраструктури, а також вплив на масову свідомість населення країни супротивника, наприклад, через злам медіа та інформаційні кампанії у соцмережах.

Мета кібервійни

- **Впливати на інфраструктуру іншої країни**
  - Окрім промислового та військового шпигунства, одна країна може постійно вторгатися в інфраструктуру іншої країни, спричиняючи збої та хаос.
  - Кібератака може вимкнути електромережу великого міста. Подумайте про наслідки, якщо це станеться: дороги будуть перевантажені, обмін товарами та послугами буде зупинено, пацієнти не зможуть отримати необхідну допомогу у разі надзвичайної ситуації, доступ до Інтернету буде перервано. Відключивши електромережу, кібератака може мати величезний вплив на повсякденне життя пересічних громадян.
  - Приклад – кібератака на державні реєстри України, що відбулась 19 грудня 2024 року. Реєстри відновили 20 січня 2025 року.

4 Шкідливе програмне забезпечення

Типи шкідливого програмного забезпечення

- Кіберзлочинці використовують багато різних типів шкідливого програмного забезпечення в своїй діяльності.
- **Шкідливе програмне забезпечення** – це будь-який код, який може красти дані, обходити засоби контролю доступу або завдавати шкоди комп'ютерній системі чи компрометувати її. Знання типів шкідливого програмного забезпечення та способів його поширення є ключем до його стримування та видалення.

Шпигунське програмне забезпечення:

- Шпигунське програмне забезпечення відстежує вашу онлайн-активність і може реєструвати кожне ваше натискання клавіші на клавіатурі, а також захоплювати ваші дані, включаючи конфіденційну персональну інформацію, таку як банківські реквізити.
- Його метою є шпигування за вами. Шпигунське програмне забезпечення робить це, змінюючи налаштування безпеки на ваших пристроях.
- Воно часто поєднується з легальним програмним забезпеченням або троянськими кіньми.

Типи шкідливого програмного забезпечення

Рекламне програмне забезпечення:

- Часто рекламне програмне забезпечення встановлюється разом із деякими версіями легального програмного забезпечення, і його призначення полягає в автоматичному показі реклами користувачеві, найчастіше у веб-браузері, бо важко ігнорувати постійні спливаючі рекламні вікна на екрані.
- Рекламне програмне забезпечення часто постачається разом зі шпигунськими програмами.

Бекдор:

- Це шкідливе програмне забезпечення, яке обходить звичайні процедури автентифікації та отримує несанкціонований доступ до комп'ютерної системи. В результаті хакери можуть отримати доступ до ресурсів комп'ютерної системи та виконувати на ній віддалені системні команди.
- Бекдор працює у фоновому режимі та його важко виявити.

Типи шкідливого програмного забезпечення

Програми-шантажисти:

- Це шкідливе програмне забезпечення розроблено таким чином, щоб утримувати комп'ютерну систему або дані, що містяться в ній, доки не відбудеться платіж.
- Програми-шантажисти зазвичай шифрують вашу інформацію, щоб ви не мали до неї доступу. Деякі версії програм-шантажистів можуть використовувати певні вразливості системи для її блокування.
- Програми-шантажисти часто поширюються через фішингові електронні листи, які заохочують вас завантажувати шкідливі вкладення, або через вразливість програмного забезпечення.

Залякуюче програмне забезпечення:

- Цей тип шкідливого програмного забезпечення використовує тактику «залякування», щоб обманом змусити вас виконати певну дію.
- Ці програми в основному складаються з вікон у стилі операційної системи, які попереджають вас про те, що ваша система перебуває під загрозою та потребує запуску певної програми, щоб повернутися до нормальної роботи. Якщо ви погодитеся запустити цю програму, то ваша система заразиться шкідливим програмним забезпеченням.

Типи шкідливого програмного забезпечення

Руткіт:

- Мета цього шкідливого програмного забезпечення полягає в модифікації операційної системи для створення бекдору, який зловмисники можуть використовувати для віддаленого доступу до вашого комп'ютера. Більшість руткітів використовують вразливості програмного забезпечення для доступу до ресурсів, які не повинні бути доступні (підвищення привілеїв), та зміни системних файлів.

- Руткіти також можуть змінювати засоби системної криміналістики та інструменти моніторингу, що робить їх дуже важкими для виявлення. Якщо руткіт заразив комп'ютер, видаліть його та перевстановіть усе необхідне програмне забезпечення.

Типи шкідливого програмного забезпечення

Віруси:

- Вірус – це комп’ютерна програма, яка під час виконання розмножується та приєднується до інших виконуваних файлів, таких як документ, шляхом вставки свого коду.
- Більшість вірусів потребують взаємодії з кінцевим користувачем для початку активації та можуть запускатися у певний час чи дату.
- Віруси можуть бути відносно нешкідливими, наприклад відображати кумедне зображення. Або ж вони можуть бути руйнівними, наприклад, змінювати або видаляти дані. Кібератака з використанням вірусу Petya відбулася в Україні наприкінці червня 2017 року. Вірус Petya блокував комп'ютерні системи компаній, вимагаючи за розблокування 300 доларів у біткойнах. Він зупинив третину економіки України на три дні, що стало наслідком для збитків у понад 400 мільйонів доларів.
- Віруси також можуть бути запрограмовані на мутацію, щоб уникнути виявлення.
- Більшість вірусів поширюється через USB-накопичувачі, оптичні диски, мережеві ресурси або електронну пошту.

Троянський кінь:

- Це шкідливе програмне забезпечення виконує шкідливі операції, маскуючи свої справжні наміри. Воно виглядає легітимним, але дуже небезпечним.
- Трояни використовують ваші привілеї користувача, і ви можете знайти їх у файлах зображень, аудіофайлах чи іграх.
- На відміну від вірусів, трояни не самовідтворюються, а діють як приманки, щоб пронести шкідливе програмне забезпечення повз нічого не підозрюючих користувачів.

Типи шкідливого програмного забезпечення

Черв’яки:

- Цей тип шкідливого програмного забезпечення реплікується, щоб поширюватися з одного комп'ютера на інший. На відміну від вірусу, для якого потрібна програма-носій, черв'яки можуть працювати автономно. Окрім початкового зараження носія, вони не потребують участі користувача та можуть дуже швидко поширюватися мережею.

- Черв'яки використовують системні вразливості, мають спосіб поширення та містять шкідливий код (корисне навантаження), щоб завдати шкоди комп'ютерним системам або мережам.

- Черв'яки відповідальні за одні з найруйнівніших атак в Інтернеті. У 2001 році черв'як Code Red заразив понад 300 000 серверів лише за 19 годин.

Симптоми шкідливого програмного забезпечення

Незалежно від типу шкідливого програмного забезпечення, яке заразило комп'ютерну систему, ви можете звернути увагу на деякі поширені симптоми. До них належать:

- збільшення використання центрального процесора, що уповільнює роботу вашого пристрою;
- часте зависання або збої комп'ютера;
- зниження швидкості перегляду вебсторінок;
- незрозумілі проблеми з мережевими підключеннями;
- змінені або видалені файли;
- наявність невідомих файлів, програм або значків на Робочому столі;
- запущені невідомі процеси;
- вимкнення або переналаштування програм;
- надсилання електронних листів без вашого відома чи згоди.

5 Методи проникнення

Соціальна інженерія

Людська помилка є однією з основних причин порушень безпеки.

- **Соціальна інженерія** – це маніпулювання людьми для виконання певних дій або розголошення конфіденційної інформації. Соціальні інженери часто покладаються на готовність людей допомогти, але також використовують їхні слабкості. Наприклад, зловмисник телефонує уповноваженому співробітнику з терміновою проблемою, яка вимагає негайного доступу до комп'ютерної мережі, та апелює до марнославства чи жадібності співробітника, або ж посилається на його авторитет, використовуючи методи хаосу, щоб отримати цей доступ.

Претекстування

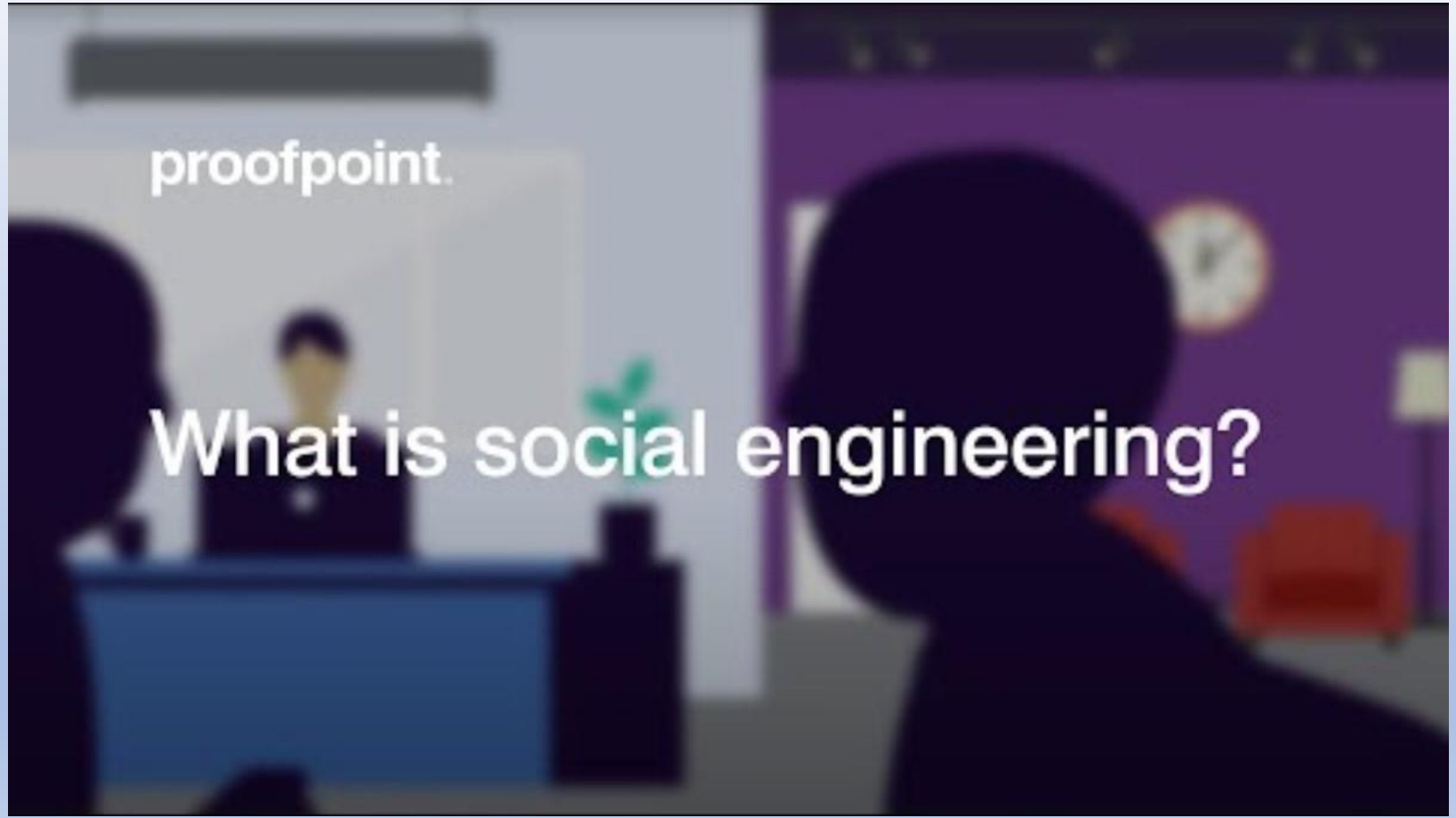
- Це коли зловмисник телефонує особі та бреше їй, щоб отримати доступ до конфіденційних даних. Наприклад, вдаючи, що йому потрібні персональні або фінансові дані людини для підтвердження її особи.

Соціальна інженерія

- **Заїзд на роботу** – коли зловмисник переслідує уповноважену особу в безпечному фізичному місці.

- **Щось за щось (quid pro quo)** - коли зловмисник вимагає персональну інформацію від когось в обмін на щось, наприклад, подарунок.

Соціальна інженерія



Як уникнути фішингової атаки?

- **Не відкривати електронні листи від незнайомих людей та компаній.**
- **Налаштувати блокувальник спаму у своєму поштовому клієнті.**
- **Наводити курсор миші на посилання, щоб перевірити справжню URL-адресу.** Перевіряти повідомлення на наявність орфографічних або граматичних помилок, скептично ставлячись до привабливих пропозицій — чи це надто добре, щоб бути правдою?
- **Не розголошувати жодної персональної інформації електронною поштою** — надійний банк не запитуватиме особисту інформацію електронною поштою.

Як уникнути соціальної інженерії?

- **Уникайте «єдиної точки відмови».** Не використовуйте одну й ту саму адресу електронної пошти для кожного сайту чи сервісу, який ви використовуєте в Інтернет. Чим більше взаємопов'язані та залежні ваші облікові записи, тим більшої шкоди може завдати вам порушення безпеки. Наприклад, не використовуйте свою адресу Gmail для відновлення пароля кожного сервісу.
- **Використовуйте різні логіни для кожного сервісу.** Ніколи не використовуйте один і той самий пароль більше одного разу. І переконайтеся, що ваші паролі надійні.
- **Використовуйте двофакторну автентифікацію.** Після введення правильного імені користувача та пароля вам буде запропоновано підтвердити свою особу іншим способом.
- **Проявіть креативність із питаннями безпеки.** Додаткові питання безпеки, на які веб-сайти просять вас відповісти, мають бути ще однією лінією захисту, але часто ці питання легко вгадати або виявити. Ви можете змінити розташування літер у своїй відповіді або скористатися власною спеціальною системою кодування, щоб переконатися, що лише ви знаєте ці відповіді на питання безпеки, наприклад, **pordwass**.

Як уникнути соціальної інженерії?

- **Часто перевіряйте свої облікові записи та персональні дані,** щоб бути в курсі як крадіжки персональних даних, так і шахрайства з кредитними картками, перевіряйте баланс своїх рахунків. Ви можете скористатися **Google Alerts**, щоб перевірити, чи не були ваші дані опубліковані десь в Інтернеті.
- **Уникайте фішингових листів.** Фішингові електронні листи стає все важче виявити, а стати їхніми жертвами стає легше.

Denial-of-Service (DoS)

Denial-of-Service (DoS) атака призводить до переривання мережевого обслуговування користувачів, пристроїв та програм.

Надмірна кількість трафіку - коли мережа, хост або програма отримує величезний обсяг даних зі швидкістю, який не може вчасно обробити. Це призводить до повільної передачі або відповіді, або ж до збою пристрою чи служби.

Шкідливо відформатовані пакети

- **Пакет** – це набір даних, що передається між програмою-джерелом та програмою-отримувачем через комп'ютерну мережу. Під час надсилання шкідливо відформатованого пакета програма-одержувач не може його обробити.
- Припустимо, що зловмисник пересилає пакети, які містять помилки, або неправильно відформатовані пакети, які програма-отримувач не може ідентифікувати. Це призведе до дуже повільної роботи або збою програми-отримувача.

Розподілена DoS-атака

Розподілена DoS-атака (DDoS) схожа на звичайну DoS-атаку, але походить з кількох скоординованих джерел. Наприклад:

- Хакер створює мережу (ботнет) заражених комп’ютерів, які називаються зомбі, контрольованими сервером управління.
- Зомбі-комп'ютери постійно сканують та заражають нові комп’ютери, створюючи все більше й більше зомбі.
- Хакер наказує серверу управління змусити зомбі здійснити DDoS-атаку.

Ботнет

- **Бот-комп'ютер** зазвичай заражається через відвідування небезпечного вебсайту або відкриття зараженого вкладення електронної пошти чи медіафайлу.

- **Ботнет** – це група ботів, підключених через Інтернет, якими може керувати зловмисник. Він може містити десятки тисяч або навіть сотні тисяч ботів, якими зазвичай керує сервер управління. Заражені боти намагаються зв'язатися з сервером управління в Інтернеті.

- Активація цих ботів призводить до розповсюдження шкідливого програмного забезпечення, запуску DDoS-атак, розповсюдження спам-листів або виконання атаки методом перебору паролів.

- Кіберзлочинці часто здають ботнети в оренду третім сторонам для зловмисних цілей.

Атака на шляху

- Зловмисники, що атакують на шляху, перехоплюють трафік між двома пристроями, наприклад, веб-браузером і веб-сервером, щоб зібрати інформацію з одного з них або видати себе за нього.

- Цей тип атаки називається атакою «зловмисник посередині» або «зловмисник у мобільному пристрої».

Зловмисник посередині

- Атака «зловмисник посередині» відбувається, коли кіберзлочинець отримує контроль над пристроєм без відома користувача.

- Маючи такий рівень доступу, зловмисник може захопити інформацію користувача, перш ніж той надішле її за призначенням.

- Використання такого типу атаки часто призводить до крадіжки фінансової інформації.

Атака на шляху

Зловмисник у мобільному пристрої

- «Зловмисник у мобільному пристрої», різновид атаки «людина посередині», — це тип атаки, що використовується для отримання контролю над мобільним пристроєм користувача.

- Під час зараження мобільного пристрою шкідлива програма витягує конфіденційну інформацію користувача та надсилає її зловмиснику.

- **ZeuS** — це один із прикладів пакета шкідливого програмного забезпечення з можливостями «зловмисника у мобільному пристрої». Він дозволяє зловмиснику непомітно перехоплювати SMS-повідомлення з двофакторною аутентифікацією, що надсилаються користувачам ZeuS.

SEO (Search Engine Optimization) - отруєння

- **Пошукова оптимізація або SEO (Search Engine Optimization)** полягає в покращенні веб-сайту організації для підвищення його видимості в результатах пошуку.

- Пошукові системи працюють, представляючи користувачам список веб-сторінок, сформованих на основі пошукових запитів користувачів. Веб-сторінки у цьому списку ранжуються відповідно до релевантності їхнього контенту.

- Хоча багато легальних компаній спеціалізуються на пошуковій оптимізації веб-сайтів для їх кращого позиціонування, зловмисники використовують популярні пошукові терміни та SEO, щоб просувати шкідливі веб-сайти на вищі місця при видачі пошуковою системою результатів пошуку. Цей метод називається SEO-отруєнням.

- Найпоширенішою метою SEO-отруєння є збільшення трафіку до шкідливих сайтів, які можуть містити шкідливе програмне забезпечення або намагатися здійснити соціальну інженерію.

Атаки на паролі

Введення імені користувача та пароля є однією з найпопулярніших форм автентифікації на веб-сайті. Тому розкриття вашого пароля — це простий спосіб для кіберзлочинців отримати доступ до вашої найціннішої інформації.

Розпилення пароля:

- Хакер намагається отримати доступ до системи шляхом «розпилення» кількох поширених паролів на багато облікових записів. Наприклад, хакер використовує «Password123» для великої кількості імен користувачів. Потім використовує інший поширений пароль, наприклад «qwerty».
- Така техніка дозволяє хакеру залишатися непоміченим та уникати частих блокувань облікових записів.

Атаки зі словником:

- Більшість програмного забезпечення для злому паролів використовують так звану атаку за словником, щоб спочатку перевірити популярні слова або фрази, такі як abc123, trustno1, drowssap, password123 тощо. Хакер систематично намагається використовувати кожне слово зі словника або список часто вживаних слів як пароль, щоб зламати обліковий запис, захищений паролем.

Атаки на паролі

Атака методом перебору

- Найпростіший і найпоширеніший спосіб отримання доступу до вебсайту, захищеного паролем, полягає в тому, що хакер використовує всі можливі комбінації літер, цифр і символів у паролі, доки не отримає правильний пароль. Ви можете сповільнити процес перебору пароля, збільшивши довжину та складність вашого пароля. Але «abcdefghijklmnopqrstuvwxyz» може бути довгим, але не складним.

Веселкова атака

- Паролі в комп'ютерній системі зберігаються не у вигляді звичайного тексту, а у вигляді хешованих значень (числових значень, що однозначно ідентифікують дані).
- Веселкова таблиця функціонує як розширений словник попередньо обчислених хешів та паролів.
- На відміну від атаки методом перебору, яка має обчислювати кожен хеш, веселкова атака порівнює хеш пароля з тими, що зберігаються у веселковій таблиці. Коли хакер знаходить збіг, він ідентифікує пароль, який використовувався для створення хешу.

Перехоплення мережевого трафіку

- Перехоплюючи мережевий трафік, можна легко зчитувати незашифровані паролі.

Просунуті постійні загрози

- Зловмисники також досягають проникнення за допомогою **просунутих постійних загроз APT (advanced persistent threats)** — багатофазної, довгострокової, прихованої та просунутої операції проти конкретної цілі.

- Окремому зловмиснику часто бракує навичок, ресурсів або наполегливості для виконання APT.

- Через складність та рівень кваліфікації, необхідних для здійснення такої атаки, APT зазвичай добре фінансується та спрямована на організації або країни з політичних або бізнес-причин.

- Основна мета APT — розгорнути спеціалізоване шкідливе програмне забезпечення на одній або кількох цільових комп'ютерних системах та залишатися там непоміченим.

6 Вразливості кібербезпеки та експлойти

Вразливості апаратного забезпечення

Вразливості апаратного забезпечення найчастіше є результатом недоліків конструкції обладнання.

- Наприклад, тип пам'яті, який називається оперативною пам'яттю (RAM), складається з конденсаторів (компонентів, які можуть утримувати електричний заряд), встановлених дуже близько один до одного. Однак, через їх близькість, зміни, внесені до одного з цих конденсаторів, можуть вплинути на сусідні конденсатори.

- Цей недолік конструкції створює експлойт під назвою **Rowhammer**. Шляхом багаторазового доступу (молоткового зчитування) рядка пам’яті, експлойт Rowhammer запускає електричні перешкоди, які зрештою пошкоджують дані, що зберігаються в оперативній пам'яті.

Meltdown та Spectre

- Meltdown та Spectre – дві вразливості апаратного забезпечення, які впливають майже на всі центральні процесори (ЦП), в настільних комп'ютерах, ноутбуках, серверах, смартфонах, інтелектуальних пристроях та хмарних сервісах.

- Зловмисники, які використовують ці вразливості, можуть зчитувати всю пам'ять із заданої системи (**Meltdown**) та дані, що обробляються іншими програмами (**Spectre**).
-
- Через численні спроби запуску атак експлуатація вразливостей Meltdown та Spectre може поставити під загрозу великі обсяги даних пам'яті навіть у комп'ютерній системі з мінімальною ймовірністю збою чи іншої помилки.

Вразливості програмного забезпечення

- Помилки в операційній системі або коді програми зазвичай призводять до вразливостей програмного забезпечення. Наприклад, у 2015 році вразливість **SYNful Knock** у маршрутизаторах Cisco дозволила зловмисникам отримати контроль над маршрутизаторами корпоративного рівня, з яких вони могли контролювати весь мережевий зв'язок та заражати інші мережеві пристрої.

- Коли на маршрутизатори встановлюється змінена версія операційної системи, вразливість проникає в маршрутизатор. Щоб уникнути цього, слід завжди перевіряти цілісність завантаженого образу операційної системи та обмежувати фізичний доступ до такого обладнання лише уповноваженим персоналом.

Вразливості програмного забезпечення

Більшість вразливостей безпеки програмного забезпечення поділяються на кілька основних категорій.

Переповнення буфера:

- **Буфер** – це область пам’яті, виділена певній програмі. Під час запису даних за межі буфера виникає вразливість. Змінюючи дані за межами буфера, програма може отримати доступ до пам’яті, виділеної іншим процесам. Це може призвести до збою комп’ютерної системи, компрометації даних або підвищення привілеїв.

Вразливості програмного забезпечення

Неперевірені вхідні дані:

- Програми часто потребують введення даних, але ці вхідні дані можуть містити шкідливий контент, який змушує програму діяти певним чином. Наприклад, розглянемо програму, яка отримує зображення для оброблення. Зловмисник може створити файл зображення з недійсними розмірами. Зловмисно створені розміри зображення можуть змусити програму виділити буфер неправильного розміру.

Умова змагання:

- Ця вразливість описує ситуацію, коли результат події залежить від упорядкованості дій. Вона стає джерелом ризику, коли необхідні події не відбуваються у правильному порядку або у належний час.

Вразливості програмного забезпечення

Недоліки в практиках кібербезпеки:

- Автентифікація, авторизація та шифрування захищають комп'ютерні системи та конфіденційні дані.
- Розробникам слід використовувати методи кібербезпеки та бібліотеки, які вже були створені, протестовані та перевірені, і не слід намагатися створювати власні алгоритми кібербезпеки. Це, ймовірно, лише призведе до появи нових вразливостей.

Проблеми з контролем доступу:

- **Контроль доступу** – це процес контролю за тим, хто що робить. Він охоплює різні аспекти - від управління фізичним доступом до обладнання до визначення того, хто має доступ до певного ресурсу, наприклад, файлу, і що він може з ним робити, наприклад, читати або змінювати файл.
- Неправильне використання засобів контролю доступу створює багато вразливостей безпеки.
- Майже всі засоби контролю доступу та методи безпеки можна подолати, якщо зловмисник має фізичний доступ до цільового обладнання. Наприклад, незалежно від налаштувань дозволів для файлу, хакер може обійти операційну систему та зчитати дані безпосередньо з диска.

Оновлення програмного забезпечення

- Мета оновлень програмного забезпечення — залишатися в курсі подій та уникати використання вразливостей. Microsoft, Apple та інші виробники операційних систем щодня випускають патчі та оновлення. Організації оновлюють такі програми, як веб-браузери, мобільні застосунки та веб-сервери.

- Незважаючи на те, що організації докладають багато зусиль для пошуку та виправлення вразливостей програмного забезпечення, вони регулярно виявляють нові вразливості. Ось чому деякі організації використовують сторонніх дослідників кібербезпеки, які спеціалізуються на пошуку вразливостей у програмному забезпеченні, або інвестують у свої команди з тестування на проникнення, які займаються пошуком, знаходженням та виправленням вразливостей програмного забезпечення, перш ніж вони можуть бути використані зловмисниками. Приклад цієї практики - проект **Zero** від Google, створений у 2014 році. Після виявлення кількох вразливостей у програмному забезпеченні, яке використовується кінцевими користувачами, Google сформував постійну команду, яка займається пошуком вразливостей програмного забезпечення.

Криптоджекінг

- **Криптоджекінг** – це загроза, коли на комп'ютері користувача, мобільному пристрої або сервері, використовуються ресурси для «майнінгу» криптовалют без згоди чи відома користувача. Найбільш вираженим ефектом криптоджекінга є зниження продуктивності процесора (зазвичай це проявляється через збільшення шуму вентилятора).

- **Мережевий криптоджекінг** (також відомий як, попутний крипто-майнінг) - найбільш поширена форма крипто-майнінгових шкідливих програм. Як правило, ця шкідлива дія виконується за допомогою скриптів, запущених на веб-сайті, що примушує веб-браузер жертви автоматично майнити криптовалюту під час відвідування цього веб-сайту. Такі мережеві майнери таємно реалізуються на самих різних веб-сайтах, незалежно від їх популярності.

- Мережевий криптоджекінг був вперше виявлений у вересні 2017 року, коли крипто-майнер CoinHive був офіційно представлений на публіку. CoinHive включає в себе крипто-майнер JavaScript, який, як стверджується, був створений з благородною метою: дозволити власникам веб-сайтів монетизувати їх вільно доступний контент, не використовуючи рекламу.

7 Захист комп’ютера та комп’ютерної мережі

Захист комп'ютера

Увімкніть брандмауер	Вам слід використовувати принаймні один тип брандмауера (програмний брандмауер або апаратний брандмауер на маршрутизаторі) для захисту вашого комп'ютера від несанкціонованого доступу. Брандмауер слід увімкнути та постійно оновлювати, щоб запобігти доступу хакерів до ваших персональних даних або даних організації.
Встановіть антивірус та антишпигунське програмне забезпечення	Шкідливе програмне забезпечення, таке як віруси та шпигунські програми, призначене для отримання несанкціонованого доступу до вашого комп'ютера та даних. Після встановлення віруси можуть знищити ваші дані та уповільнити роботу комп'ютера. Вони можуть розсилати спам-листи, використовуючи ваш обліковий запис. Шпигунське програмне забезпечення може відстежувати вашу онлайн-активність, збирати вашу персональну інформацію або створювати небажані спливаючі вікна у веб-браузері, коли ви перебуваєте в Інтернеті. Щоб запобігти цьому, завантажуйте програмне забезпечення лише з перевірених веб-сайтів. Було б корисно завжди використовувати антивірусне програмне забезпечення для забезпечення додаткового рівня захисту. Це програмне забезпечення, яке часто включає антишпигунське програмне забезпечення, призначене для сканування вашого комп'ютера та вхідної електронної пошти на наявність вірусів та їх видалення.
Налаштуйте операційну систему та браузер	Хакери завжди намагаються скористатися вразливостями вашої операційної системи або веб-браузера. Тому, щоб захистити свій комп'ютер і дані, вам слід налаштувати середній або високий рівень безпеки на вашому комп'ютері та веб-браузері. Вам також слід регулярно оновлювати операційну систему вашого комп'ютера, включаючи веб-браузер, а також завантажувати та встановлювати останні оновлення програмного забезпечення та оновлення безпеки від постачальників програмного забезпечення.
Налаштуйте захист паролем	Усі ваші комп'ютери мають бути захищені паролем, щоб запобігти несанкціонованому доступу. Будь-яка інформація, що зберігається, особливо конфіденційні дані, має бути зашифрована. Зберігайте на своєму мобільному пристрої лише необхідну інформацію на випадок її крадіжки або втрати. Пам'ятайте, що якщо будь-який із ваших пристроїв буде скомпрометовано, то злочинці зможуть отримати доступ до всіх даних через вашого постачальника послуг хмарного сховища, такого як iCloud або Google Диск.

Безпека домашньої бездротової мережі

- Бездротові мережі дозволяють пристроям з підтримкою Wi-Fi підключатися до комп’ютерної мережі за допомогою SSID.
- Бездротовий маршрутизатор можна налаштувати так, щоб він не транслював SSID, але для бездротової мережі має бути налаштований належний захист.
- Хакери знають попередньо встановлений SSID та пароль за замовчуванням, тому, щоб запобігти проникненню зловмисників у вашу домашню бездротову мережу, вам слід змінити ці дані.
- Ви можете зашифрувати бездротовий трафік, увімкнувши бездротовий захист та функцію шифрування WPA2 на вашому бездротовому маршрутизаторі.
- Навіть з увімкненим шифруванням WPA2 бездротова мережа все ще може бути вразливою.
- **Виявлення вразливості в протоколі WPA2 у 2017 році**
- Атаки перевстановлення ключів (KRACK) зловмисниками, які порушують шифрування між бездротовим маршрутизатором та бездротовим пристроєм, надаючи їм доступ до мережевих даних, можуть використовувати цю вразливість.
- Ця вразливість впливає на всі сучасні, захищені мережі Wi-Fi, і щоб пом'якшити цю ситуацію, вам слід:
  - Оновлювати всі пристрої з підтримкою бездротового зв'язку, як тільки стануть доступні оновлення безпеки
  - Використовувати дротове з'єднання для будь-яких пристроїв із дротовою мережевою картою
  - Використовувати надійний VPN-сервіс під час доступу до бездротової мережі.

Ризики загальнодоступних бездротових мереж

- Коли ви не вдома, то можете отримати доступ до своєї онлайн-інформації та переглядати веб-сторінки через загальнодоступні бездротові мережі або точки доступу Wi-Fi.

- Однак, це пов’язано з певними ризиками, тому краще не отримувати доступ до персональної інформації та не надсилати її через загальнодоступний Wi-Fi.

- Було б корисно постійно перевіряти, чи ваш пристрій не налаштовано на обмін файлами та медіафайлами та чи вимагає він автентифікації користувача з шифруванням.

- Вам також слід використовувати зашифрований VPN-сервіс, щоб запобігти перехопленню вашої інформації іншими (що називається «підслуховуванням») через загальнодоступну бездротову мережу.

- VPN-сервіс надає вам безпечний доступ до Інтернету, шифруючи з’єднання між вашим пристроєм та VPN-сервером.

- Навіть якщо хакери перехоплюють передачу даних у зашифрованому VPN-тунелі, вони не можуть її розшифрувати.

Резервне копіювання даних

- Наявність резервної копії може запобігти втраті даних.
- Для правильного резервного копіювання даних вам знадобиться додаткове місце для зберігання, і ви повинні регулярно копіювати дані туди.

Деякі з додаткових місць зберігання даних:

Домашня мережа	Локальне зберігання ваших даних означає, що ви маєте повний контроль над ними.
Додаткове місцезнаходження	Ви можете скопіювати всі свої дані на зовнішній жорсткий диск або створити резервні копії важливих папок на флеш-накопичувачах або DVD-дисках. У цьому випадку ви є власником даних і несете відповідальність за вартість та обслуговування обладнання для зберігання даних.
Хмара	Ви можете підписатися на хмарний сервіс сховища даних, такий як AWS. Вартість цього сервісу залежатиме від необхідного вам обсягу місця для зберігання, тому вам, можливо, доведеться більш вибірково підходити до резервного копіювання даних. Ви матимете доступ до резервних копій даних, поки маєте доступ до свого облікового запису. Однією з переваг використання хмарного сервісу сховища даних є те, що ваші дані будуть у безпеці у разі збою пристрою зберігання даних або у разі виникнення екстремальної ситуації, такої як пожежа чи крадіжка.

8 Захист конфіденційності в Інтернет

Двофакторна автентифікація

- Популярні онлайн-сервіси, такі як Google, Facebook, Twitter, LinkedIn, Apple та Microsoft, використовують **двофакторну автентифікацію**, щоб додати додатковий рівень безпеки для входу в обліковий запис.

- Окрім вашого імені користувача та пароля, двофакторна автентифікація вимагає другого токена для підтвердження вашої особи. Це може бути:
  - фізичний об’єкт, такий як кредитна картка, мобільний телефон або брелок
  - біометричне сканування, таке як відбиток пальця або розпізнавання обличчя та голосу
  - код підтвердження, надісланий через SMS або електронну пошту.

Відкрита авторизація

- Відкрита авторизація (OAuth) – це протокол відкритого стандарту, який дозволяє вам використовувати свої облікові дані для доступу до сторонніх програм, не розкриваючи свій пароль.

- Що це означає на практиці? Наприклад, вам потрібно потрапити на портал електронного навчання але ви не пам’ятаєте свої дані для входу. Портал дозволяє вам входити, використовуючи облікові дані з веб-сайту соціальної мережі, такої як Facebook, або через інший обліковий запис, наприклад, Google. Тож ви легко входите на портал електронного навчання, використовуючи свої існуючі облікові записи соціальних мереж.

Конфіденційність електронної пошти та веб-браузера

- Ці проблеми можна мінімізувати, увімкнувши режим приватного перегляду у вашому веб-браузері.
- Багато з найпопулярніших веб-браузерів мають свою назву для режиму приватного перегляду:
  - **Microsoft Internet Explorer:** Приватно
  - **Google Chrome:** Інкогніто
  - **Mozilla Firefox:** Приватна вкладка або приватне вікно
  - **Safari:** Приватний перегляд

- Як працює приватний режим?
  - Коли ввімкнено приватний режим, файли cookie — файли, що зберігаються на вашому пристрої для позначення відвідуваних вами веб-сайтів — вимкнено.
  - Видаляйте всі тимчасові файли Інтернету та видаляйте історію переглядів, коли закриваєте вікно або програму.
  - Це може допомогти запобігти збору іншими інформації про вашу онлайн-активність та спонуканню вас до покупки за допомогою цільової реклами.

Конфіденційність електронної пошти та веб-браузера

- Ці проблеми можна мінімізувати, увімкнувши режим приватного перегляду у вашому веб-браузері.
- Багато з найпопулярніших веб-браузерів мають свою назву для режиму приватного перегляду:
  - **Microsoft Internet Explorer:** Приватно
  - **Google Chrome:** Інкогніто
  - **Mozilla Firefox:** Приватна вкладка або приватне вікно
  - **Safari:** Приватний перегляд

- Як працює приватний режим?
  - Коли ввімкнено приватний режим, файли cookie — файли, що зберігаються на вашому пристрої для позначення відвідуваних вами веб-сайтів — вимкнено.
  - Видаляйте всі тимчасові файли Інтернету та видаляйте історію переглядів, коли закриваєте вікно або програму.
  - Це може допомогти запобігти збору іншими інформації про вашу онлайн-активність та спонуканню вас до покупки за допомогою цільової реклами.

Кібербезпека персональних даних

Персональну інформацію, як правило, не слід поширювати в незашифрованих сервісах або на веб-сайтах. Ви можете розглянути можливість використання **віртуальної приватної мережі (VPN)**, яка створює безпечне з'єднання «точка-точка».

Розгляньте можливість встановлення розширення для браузера, щоб зупинити відстеження в Інтернеті:
DuckDuckGo Privacy Essentials
Privacy Badger
HTTPS Everywhere

Також корисно регулярно видаляти файли **cookie**, які ви могли зібрати під час перегляду, щоб веб-сайти не запам'ятовували вашу попередню поведінку.

Переконайтеся, що ви регулярно оновлюєте свій браузер до останньої версії.

9 Пристрої та технології кібербезпеки

Пристрої кібербезпеки

- Пристрої безпеки можуть бути автономними пристроями, такими як маршрутизатор, або програмними інструментами, що працюють на мережевому пристрої. Вони поділяються на шість загальних категорій.

  - **Маршрутизатори:** Хоча основним призначенням маршрутизатора є з'єднання різних сегментів мережі, він зазвичай забезпечує базові можливості фільтрації трафіку. Ця інформація може допомогти вам визначити, які комп'ютери з певного сегмента мережі можуть взаємодіяти з якими сегментами мережі.

  - **Брандмауери** можуть глибше аналізувати мережевий трафік, щоб блокувати шкідливу поведінку. Брандмауери можуть мати складні політики безпеки, що застосовуються до трафіку, що проходить через них.

  - **Системи запобігання вторгненням (IPS)** використовують набір сигнатур трафіку, які зіставляють та блокують шкідливий трафік і кібератаки.

Пристрої кібербезпеки

- **Віртуальні приватні мережі:** VPN дозволяють віддаленим співробітникам використовувати захищений зашифрований тунель зі свого комп'ютера та безпечно підключатися до мережі організації. VPN також можуть безпечно з'єднувати філії з мережею центрального офісу.

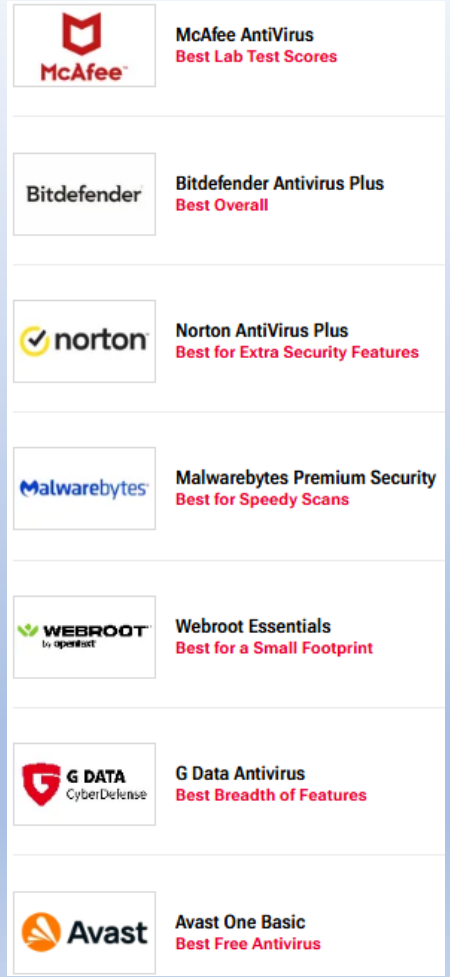
- **Антивірус або захист від шкідливих програм:** ці системи використовують сигнатури або поведінковий аналіз програм для виявлення та блокування виконання шкідливого коду.

- **Інші пристрої безпеки**: Інші пристрої безпеки включають пристрої безпеки для веб-сайтів та електронної пошти, пристрої дешифрування, сервери контролю доступу клієнтів та системи управління безпекою.

Найкращі VPN у 2025 році

NordVPN Best Premium Features	**TunnelBear VPN** Best for First-Time VPN Users
Proton VPN Best Overall	**IPVanish VPN** Best for Multi-Device Households
Surfshark VPN Best for Protecting Many Devices	**PureVPN** Best for Streaming Enthusiasts
Private Internet Access VPN Best for Customizable Interface	**CyberGhost VPN** Best for Frequent Travelers
ExpressVPN Best for Global Location Spoofers	**Mullvad VPN** Best for Bargain Hunters

Найкраще антивірусне забезпечення для Windows у 2025



Брандмауери

- У комп'ютерних мережах брандмауер контролює або фільтрує дозволений трафік. Ви можете встановити брандмауер на одному комп'ютері для захисту цього одного комп'ютера (**брандмауер на базі хоста**) або це може бути окремий мережевий пристрій, який охоплює всю комп’ютерну мережу та всі хости в цій мережі (**мережевий брандмауер**).

- Оскільки комп'ютерні та мережеві атаки стають все більш витонченими, то розвиваються нові типи брандмауерів, які служать різним цілям:

  - **Брандмауер мережевого рівня**: фільтрує трафік на основі IP-адрес джерела та призначення.

  - **Брандмауер транспортного рівня:** фільтрує трафік на основі портів джерела та призначення, а також станів з'єднання.

Брандмауери

- **Брандмауер прикладного рівня:** фільтрує трафік на основі застосунку, програми чи служби.
- **Брандмауер контекстно-залежного рівня:** фільтрує трафік на основі користувача, пристрою, ролі, типу застосунку та профілю загрози.
- **Проксі-сервер:** фільтрує запити веб-контенту, такі як URL-адреси, доменні імена та типи медіа.
- **Реверсний проксі-сервер:** розміщені перед веб-серверами, реверсні проксі-сервери захищають, приховують, розвантажують та розподіляють доступ до веб-серверів.
- **Брандмауер трансляції мережевих адрес (NAT):** цей брандмауер приховує або маскує приватні адреси мережевих хостів.
- **Брандмауер на основі хоста:** фільтрує порти та виклики системних служб на операційній системі одного комп'ютера.

Сканування портів

- У комп’ютерній мережі кожній програмі, що працює на мережевому пристрої, призначається ідентифікатор, який називається номером порту. Цей номер порту використовується на обох кінцях передачі для передачі правильних даних до правильної програми. Сканування портів здійснює комп’ютер, сервер або інший мережевий хост, перевіряючи наявність відкритих портів. Сканування портів можна використовувати зловмисно як інструмент розвідки для ідентифікації операційної системи та служб, що працюють на хості, або ж його може безпечно використовувати мережевий адміністратор для перевірки політик безпеки мережі.

- Під час сканування портів буде відображено всі запущені служби, такі як веб-служби або служби електронної пошти, а також їхні номери портів.

Сканування портів

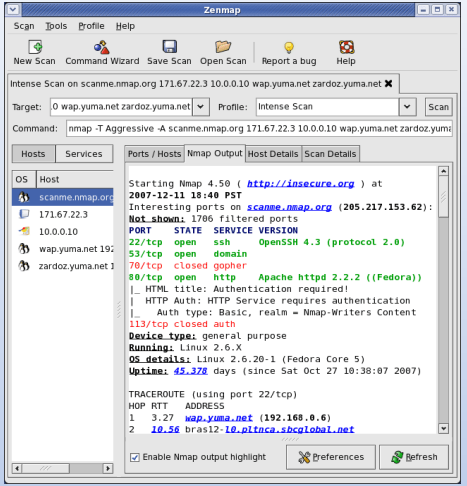
- Під час сканування також буде відображено одну з наступних відповідей:
  - «Відкрито» або «Прийнято» означає, що інші мережеві пристрої можуть отримати доступ до порту або служби, що працює на комп’ютері.
  - «Закрито», «Заборонено» або «Не прослуховується» означає, що порт або служба не працює на комп’ютері і, отже, не може бути використана.
  - «Відфільтровано», «Відхилено» або «Заблоковано» означає, що брандмауер блокує доступ до порту або служби і не може її використати.

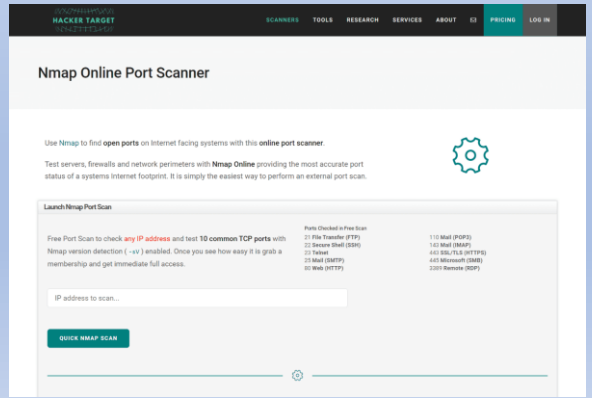
Сканування портів

- Щоб виконати сканування портів з-за меж вашої мережі, потрібно перевірити публічну IP-адресу вашого брандмауера або маршрутизатора.

- Введіть запит «яка моя IP-адреса?» у пошукову систему, таку як Google, щоб дізнатися цю інформацію.

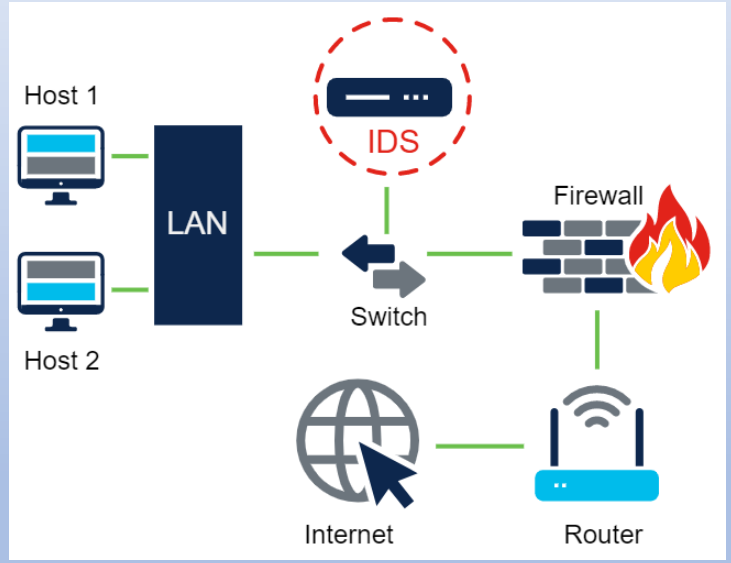
- Перейдіть до онлайн-сканера портів Nmap, введіть свою публічну IP-адресу в поле введення та натисніть “Швидке сканування Nmap”. Якщо відповідь “відкритj” для портів 21, 22, 25, 80, 443 або 3389, то, найімовірніше, на вашому маршрутизаторі або брандмауері ввімкнено переадресацію портів, і ви використовуєте сервери у своїй приватній мережі.





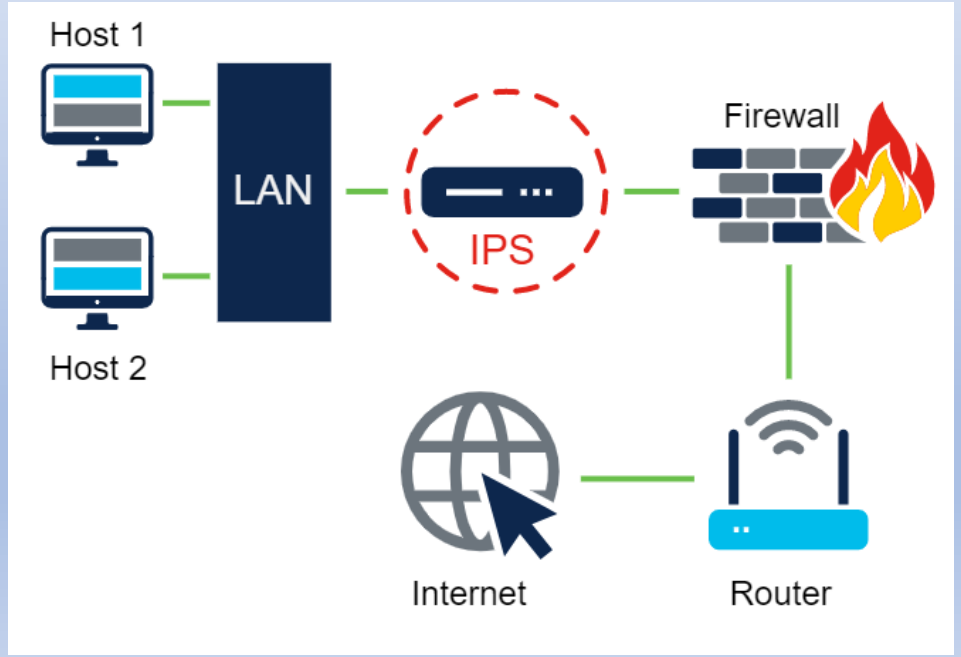
Системи виявлення та запобігання вторгненням

- **Системи виявлення вторгнень (IDS)** та **системи запобігання вторгненням (IPS)** – це заходи безпеки, розгорнуті в мережі для виявлення та запобігання шкідливій діяльності.
- **IDS може бути спеціалізованим мережевим пристроєм або одним із кількох інструментів на сервері, брандмауері або навіть операційній системі хоста, такій як Windows або Linux,** який сканує дані за базою даних правил або сигнатур атак, шукаючи шкідливий трафік.
- **Якщо буде виявлено збіг, то IDS зареєструє виявлення та створить сповіщення для мережевого адміністратора.** IDS не вживатиме жодних дій, а отже, не запобігатиме атакам. Завдання IDS полягає у виявленні, реєстрації та звітуванні.
- **Сканування, яке виконує IDS, уповільнює мережу (це називається затримкою).** Розміщення IDS в автономному режимі, окремо від звичайного мережевого трафіку, запобігає затримці мережі. Дані копіюються або дзеркалюються комутатором, а потім пересилаються до IDS для виявлення в автономному режимі.



Системи виявлення та запобігання вторгненням

- **Система запобігання вторгненням (IPS)** може блокувати або забороняти трафік на основі позитивного збігу правил або сигнатур. Однією з найвідоміших систем IPS/IDS є **Snort**. Він може виконувати аналіз трафіку та портів у режимі реального часу, ведення журналу, пошук та зіставлення контенту, виявляти зонди та атаки, а також виконувати сканування портів. Він також інтегрується зі сторонніми інструментами звітності, продуктивності та аналізу журналів.



Виявлення в режимі реального часу

- Багато організацій сьогодні можуть виявити атаки лише через кілька днів або навіть місяців після їх виникнення.

- Виявлення атак у режимі реального часу вимагає активного сканування на наявність атак за допомогою брандмауерів та мережевих пристроїв IDS/IPS. Корисно також використовувати клієнтські та серверні засоби виявлення шкідливого програмного забезпечення з підключенням до глобальних онлайн-центрів загроз. Сьогодні пристрої та програмне забезпечення активного сканування повинні виявляти мережеві аномалії за допомогою контекстного аналізу та аналізу поведінки.

- **DDoS** – одна з найпотужніших атак, що вимагає виявлення та реагування в режимі реального часу. DDoS-атаки регулярно паралізують інтернет-сервери та доступність мережі для багатьох організацій. Від цих атак надзвичайно важко захиститися, оскільки атаки походять від тисяч «зомбі-хостів» і виглядають як легітимний трафік.

Захист від шкідливого програмного забезпечення

- Один із способів захисту від атак нульового дня та просунутих постійних загроз (APT) — це використання рішень для виявлення шкідливого програмного забезпечення корпоративного рівня.

- Спеціалізоване клієнт-серверне програмне забезпечення можна розгортати на кінцевих точках хостів, як окремий сервер або на інших пристроях мережевої безпеки. Воно аналізує мільйони файлів і зіставляє їх із сотнями мільйонів інших інтерпретованих артефактів шкідливого програмного забезпечення на предмет поведінки, яка виявляє APT. Такий підхід забезпечує глобальне уявлення про атаки та розповсюдження шкідливого програмного забезпечення.

    - **Команда реагування на інциденти** має доступ до корисної з точки зору експертизи інформації, за допомогою якої вона може швидше аналізувати та розуміти підозрілу поведінку.

    - **Команда розвідки загроз**, використовуючи цей аналіз, може проактивно покращувати інфраструктуру безпеки організації.

    - **Команда інженерів інфраструктури безпеки** може швидше споживати інформацію про загрози та реагувати на неї, часто автоматизовано.

Найкращі практики кібербезпеки

- Професійні організації створили рекомендації щодо кібербезпеки:
  - **Проведіть оцінку ризиків:** знання та розуміння цінності того, що ви захищаєте, допоможе виправдати витрати на безпеку.
  - **Створіть політику безпеки:** чітко окресліть правила організації, посадові ролі, обов'язки та очікування від співробітників.
  - **Заходи фізичної безпеки:** обмеження доступу до мережевих шаф та місць розташування серверів, а також пожежогасіння.

Найкращі практики кібербезпеки

- **Заходи безпеки персоналу:** Перевірка біографічних даних має бути обов'язковою для всіх співробітників.
- **Створюйте та тестуйте резервні копії:** Регулярно створюйте резервні копії інформації та тестуйте відновлення даних з резервних копій.
- **Створюйте патчі та оновлення безпеки:** Регулярно оновлюйте операційні системи та програми серверів, клієнтів та мережевих пристроїв.
- **Застосовуйте засоби контролю доступу:** Налаштуйте ролі користувачів та рівні привілеїв, а також надійну автентифікацію користувачів.
- **Регулярно тестуйте реагування на інциденти:** Залучіть команду реагування на інциденти та протестуйте сценарії реагування на надзвичайні ситуації.

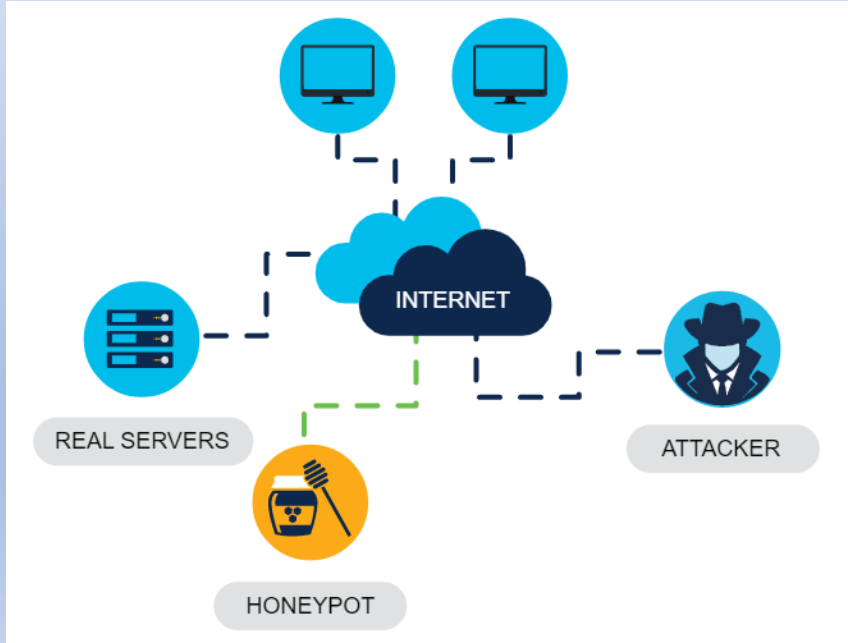
Найкращі практики кібербезпеки

- **Впроваджуйте інструменти моніторингу, аналітики та управління мережею:** виберіть рішення для моніторингу кібербезпеки, яке інтегрується з іншими технологіями.
- **Впроваджуйте пристрої мережевої кібербезпеки:** використовуйте маршрутизатори, брандмауери та інші засоби кібербезпеки.
- **Впроваджуйте комплексне рішення для захисту кінцевих точок:** використовуйте антивірусне та антивірусне програмне забезпечення корпоративного рівня.
- **Навчайте користувачів** процедурам кібербезпеки.
- **Шифруйте всі конфіденційні дані організації**, включаючи електронну пошту.

10 Поведінковий підхід до кібербезпеки

Кібербезпека на основі поведінки

- **Кібербезпека на основі поведінки** — це форма виявлення загроз, яка фіксує та аналізує трафік між користувачем у локальній мережі та локальним або віддаленим місцем призначення. Будь-які зміни у звичайних моделях поведінки розглядаються як аномалії та можуть свідчити про кібератаку.
  - **Приманка** — це інструмент виявлення на основі поведінки, який заманює зловмисників, використовуючи їхню модель передбачуваної шкідливої поведінки. Щойно зловмисник потрапляє всередину приманки, мережевий адміністратор може фіксувати, реєструвати та аналізувати його поведінку, щоб створити кращий захист.

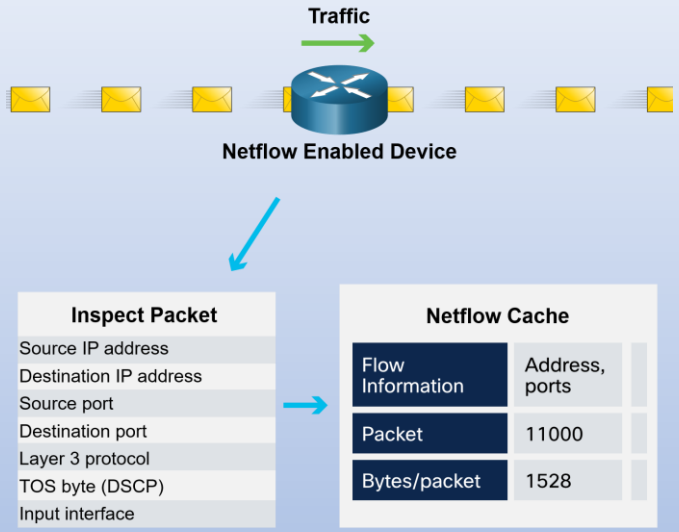


NetFlow

- Технологія NetFlow використовується для збору інформації про дані, що передаються мережею, зокрема про те, які пристрої знаходяться в мережі, а також коли і як користувачі та пристрої отримують доступ до мережі.

- NetFlow є важливим компонентом у виявленні та аналізі на основі поведінки. Комутатори, маршрутизатори та брандмауери, оснащені NetFlow, можуть повідомляти інформацію про дані, що входять, виходять та передаються мережею.

- Ця інформація надсилається колекторам NetFlow, які збирають, зберігають та аналізують дані NetFlow для встановлення базової поведінки за понад 90 атрибутами, такими як IP-адреса джерела та призначення.



Тестування на проникнення

- Тестування на проникнення оцінює комп'ютерну систему, мережу або організацію на наявність вразливостей кібербезпеки. Воно має на меті виявити системи, людей, процеси та код, які можуть використовувати вразливості кібербезпеки. Ця інформація покращує захист комп’ютерної системи, щоб забезпечити їй кращу стійкість до кібератак у майбутньому.

    - **Крок 1. Планування:** Тестер збирає якомога більше інформації про цільову комп’ютерну систему або мережу, її потенційні вразливості та експлойти для використання проти неї. Цей крок включає проведення пасивного або активного спостереження (футпринтингу) та дослідження вразливостей.

Тестування на проникнення

- **Крок 2: Сканування:** Тестер проводить активну розвідку, щоб дослідити цільову комп’ютерну систему або мережу та виявити потенційні слабкі місця, які, якщо їх використати, можуть надати зловмиснику доступ.

- Активне спостереження може включати:

  - сканування портів для виявлення потенційних точок доступу до цільової системи

  - сканування вразливостей для виявлення потенційно вразливих місць певної цілі

  - встановлюється активне з'єднання з цільовою системою для ідентифікації облікових записів користувача, системи та адміністратора.

Тестування на проникнення

- **Крок 3: Отримання доступу:** Тестер пробує отримати доступ до цільової комп’ютерної системи та перехопити мережевий трафік, використовуючи різні методи проникнення в систему, зокрема:
    - запуск експлойту з корисним навантаженням на систему
    - порушення фізичних бар’єрів для доступу до активів
    - соціальна інженерія
    - використання вразливостей веб-сайтів
    - використання вразливостей програмного та апаратного забезпечення або неправильних конфігурацій
    - порушення безпеки контролю доступу
    - злом слабкого зашифрованого Wi-Fi.

Тестування на проникнення

- **Крок 4: Збереження доступу:** Тестер підтримуватиме доступ до цілі, щоб з'ясувати, які дані та системи вразливі до злому. Тестер повинен залишатися непоміченим, зазвичай використовуючи бекдори, троянських коней, руткіти та інші приховані канали, щоб приховати свою присутність.

- Коли ця інфраструктура буде налагоджена, тестер збере дані, які він вважає цінними.

- **Крок 5: Аналіз та звітність**: Тестер надасть відгук у вигляді звіту з рекомендаціями щодо оновлень продуктів, політик та навчання для покращення кібербезпеки організації.

Пом’якшення впливу

- Хоча більшість організацій сьогодні знають про поширені загрози кібербезпеці та докладають значних зусиль для їх запобігання, жодні методи забезпечення кібербезпеки не є бездоганними. Тому організації повинні бути готові зменшувати збитки у разі порушення кібербезпеки.

  - **Повідомте про проблему:** комунікація створює прозорість, що є критично важливим у цій ситуації.
    - Інформування всіх співробітників та чіткий заклик до дії повинні відбуватися внутрішньо.
    - Інформування всіх клієнтів через пряме спілкування та офіційні оголошення повинні відбуватися зовні.

  - **Будьте щирими та відповідальними:** реагуйте на порушення чесно та щиро, беручи на себе відповідальність там, де винна організація

Пом’якшення впливу

- **Надайте деталі:** Будьте відвертими та поясніть, чому сталося порушення кібербезпеки та яка інформація була скомпрометована. Організації зазвичай покривають будь-які витрати клієнтів, пов’язані з послугами з крадіжки персональних даних, необхідними в результаті порушення кібербезпеки.

- **Знайдіть причину:** Вживіть заходів для розуміння того, що спричинило та сприяло виникненню порушення. Це може включати залучення експертів з криміналістики для дослідження та з'ясування деталей.

- **Застосуйте отримані уроки:** Переконайтеся, що будь-які уроки, отримані в результаті криміналістичних розслідувань, застосовуються для запобігання подібним порушенням.

- **Перевіряйте та ще раз перевіряйте:** Зловмисники часто намагаються залишити бекдор, щоб сприяти майбутнім порушенням. Щоб запобігти цьому, ви повинні переконатися, що всі комп’ютерні системи чисті, немає бекдорів для видалення та нічого іншого не скомпрометовано.

- **Навчайте:** Підвищуйте обізнаність, навчайте та просвіщайте співробітників, партнерів та клієнтів щодо запобігання майбутнім порушенням.

Управління ризиками

- **Управління ризиками:** формальний процес постійного виявлення та оцінки ризиків для зменшення впливу загроз і вразливостей. Ви не можете повністю усунути ризик, але можете визначити прийнятні рівні ризику, зваживши вплив загрози з вартістю впровадження заходів контролю для її пом'якшення. Вартість послуг завжди повинна бути щонайбільше рівною вартості активу, який ви захищаєте.

- **Окресліть ризик:** Визначте загрози, що збільшують ризик. Загрози можуть включати процеси, продукти, атаки, потенційний збій або переривання послуг, негативне сприйняття репутації організації, потенційну юридичну відповідальність або втрату інтелектуальної власності.

- **Оцінить ризик:** Визначте ступінь серйозності кожної загрози. Наприклад, деякі загрози можуть призвести до зупинки всієї організації, тоді як інші можуть бути лише незначними незручностями. Ви можете визначити пріоритет ризику, оцінивши фінансовий вплив (кількісний аналіз) або масштабований вплив на діяльність організації (якісне дослідження).

Управління ризиками

- **Реагуйте на ризик:** Розробіть план дій для зменшення загального ризику організації, детально визначивши, де ризик можна усунути, пом’якшити, передати або прийняти.

- **Моніторинг ризику:** Постійно переглядайте будь-який ризик, зменшений шляхом дій щодо усунення, пом’якшення або передачі. Пам’ятайте, що ви не можете усунути всі ризики, тому ви повинні ретельно стежити за будь-якими загрозами.

Посібник з кібербезпеки

Один із найкращих способів підготуватися до порушення кібербезпеки – це запобігти йому. Організації повинні керуватися таким:

- **визначити ризик кібербезпеки для систем, активів і даних**
- **впровадження запобіжних заходів та навчання персоналу**
- **гнучкий план реагування, який мінімізує вплив та збитки у разі порушення кібербезпеки**
- **планування заходів кібебезпеки, які мають відбуватися після порушення кібербезпеки**

Вся ця інформація має бути зібрана в посібник з кібербезпеки.

Посібник з кібербезпеки

Посібник з кібербезпеки – це набір повторюваних звітів, що окреслюють стандартизований процес виявлення кіберінцидентів та реагування на них. В ідеалі, посібник з кібербезпеки повинен:

- **Висвітлити, як виявляти та автоматизувати реагування на поширені загрози,** такі як виявлення комп'ютерів, заражених шкідливим програмним забезпеченням, підозріла мережева активність або нерегулярні спроби автентифікації.
- **Описати та чітко визначити вхідний та вихідний трафік.**
- **Надати зведену інформацію,** включаючи тенденції, статистику та розрахунки.
- **Надати зручний та швидкий доступ до ключової статистики та показників.**
- **Співвіднести події між усіма відповідними джерелами даних.**

Інструменти для виявлення та запобігання кіберінцидентам

Існує низка інструментів, що використовуються для виявлення та запобігання кіберінцидентам.

- **Система управління інформацією та подіями безпеки (SIEM)** збирає та аналізує сповіщення кібербезпеки, журнали та інші дані в режимі реального часу, історичні дані з пристроїв кібербезпеки в мережі, щоб полегшити раннє виявлення кібератак.

- **Система запобігання втраті даних (DLP)** розроблена для запобігання крадіжці або витоку конфіденційних даних з мережі. Вона контролює та захищає дані у трьох різних станах: дані, що використовуються (доступ користувача до даних), дані в русі (дані, що передаються мережею) та дані в стані спокою (дані, що зберігаються в комп'ютерній мережі або на пристрої).

Дякую за увагу !!!