Атака 1: Атака на Colonial Pipeline (травень 2021 року)

Опис атаки:
Colonial Pipeline — одна з найбільших трубопровідних систем для палива в США. Атака була проведена за допомогою **шкідливого ПЗ (Ransomware) під назвою DarkSide**. Зловмисники отримали **доступ до мережі компанії** через скомпрометований **пароль від облікового запису VPN**, який **не був захищений двофакторною автентифікацією**. Це призвело до шифрування даних та зупинки роботи трубопроводу. Для відновлення систем компанія змушена була сплатити хакерам викуп у розмірі приблизно 4.4 мільйони доларів у біткойнах.

Аналіз тріади CIA:

Confidentiality (Конфіденційність): Порушено. Хоча основною метою було вимагання грошей, а не викрадення даних, зловмисники все ж викрали 100 ГБ корпоративних даних перед шифруванням, погрожуючи оприлюднити їх у разі несплати викупу. Це означає, що конфіденційна інформація була розголошена.

Integrity (Цілісність): Порушено. Дані на серверах компанії були зашифровані та пошкоджені, що робило їх непридатними для використання. Цілісність інформації була порушена.

Availability (Доступність): Порушено. Це найбільш очевидний наслідок атаки. Компанія була змушена зупинити всі операції з транспортування палива, щоб запобігти поширенню атаки. Це призвело до масових перебоїв з постачанням палива на східному узбережжі США.

Заходи безпеки:
1. Багатофакторна автентифікація (MFA) для всіх віддалених доступів.
   Обґрунтування: Найімовірніше, запобігла б цю атаку, навіть якщо пароль був би викрадений. Посилює Confidentiality та Integrity, ускладнюючи несанкціонований доступ.
2. Регулярне навчання співробітників кібербезпеці та фішингу.
   Обґрунтування: Співробітники мають розуміти важливість використання складних унікальних паролів і не переходити за підозрілими посиланнями. Посилює Confidentiality.
3. Чітка стратегія резервного копіювання та відновлення (Backup & Disaster Recovery Plan).
   Обґрунтування: Наявність ізольованих (відключених від мережі) резервних копій даних дозволила б відновити системи без сплати викупу. Це ключовий захід для забезпечення Availability та Integrity.
4. Сегментація мережі.
   Обґрунтування: Поділ корпоративної мережі на сегменти (наприклад, відокремлення IT-мережі від операційних технологій OT) міг би запобігти поширенню шкідливого ПЗ на критичні системи управління трубопроводом. Посилює Availability та Integrity.

Висновок:
Навіть одна слабка ланка (скомпрометований пароль) може призвести до катастрофічних наслідків для критичної інфраструктури. Атака на Colonial Pipeline показала важливість:
Обов'язкового впровадження MFA.
Наявності плану відновлення після інцидентів, що не залежить від вимог зловмисників.
Пріоритетного захисту систем, від яких залежить фізична безпека та економіка.

Атака 2: Масове викрадення даних через уразливість в Log4j (грудень 2021 року).

Опис атаки:
Log4Shell — критична вразливість нульового дня (CVE-2021-44228) у популярній бібліотеці для логування Log4j, яка використовується в мільйонах програмних продуктів по всьому світу. Вразливість дозволяла зловмисникам **виконувати довільний код на віддаленому сервері без автентифікації**. Це призвело до масового сканування інтернету, викрадення даних, **встановлення майнерів криптовалют та бекдорів у корпоративних мережах**.

Аналіз тріади CIA:

Confidentiality (Конфіденційність): Порушено. Це основний наслідок. Зловмисники отримували доступ до серверів і викрадали конфіденційні дані, включаючи особисту інформацію (PII), ключі API, конфігураційні файли з паролями.

Integrity (Цілісність): Порушено. Атакувальники модифікували системи, встановлюючи шкідливе ПО, бекдори та скрипти для майнингу. Це змінило стан систем та даних, порушивши їх цілісність.

Availability (Доступність): Можливо порушено. Хоча основним наслідком не була масова DDoS-атака, встановлення майнерів могло спричинити значне навантаження на сервери, що призводило до їх уповільнення або недоступності для законних користувачів.

Заходи безпеки:

1. Регулярне оновлення та управління вразливостями (Patch Management).
   Обґрунтування: Швидке встановлення оновлень (патчів) для Log4j від розробників програмного забезпечення було ключовим засобом запобігання експлуатації вразливості. Це основа захисту Confidentiality, Integrity та Availability.
2. Застосування Web Application Firewall (WAF).
   Обґрунтування: WAF може блокувати зловмисні запити, що експлуатують вразливість Log4Shell, на межі мережі, надаючи час на встановлення патчів. Посилює Confidentiality та Integrity.
3. Постійний моніторинг мережевої активності та SIEM/SOC системи.
   Обґрунтування: Виявлення незвичайних зовнішніх з'єднань або спроб виконати підозрілі команди на серверах могло б сигналізувати про компрометацію на ранній стадії. Посилює Confidentiality та Integrity.
4. Створення картки активів (Asset Inventory).
   Обґрунтування: Організації повинні точно знати, яке програмне забезпечення та версії використовуються в їхній інфраструктурі, щоб швидко визначити, чи уразливі вони до таких загроз. Це фундамент для ефективного Patch Management.

Висновок:
Інцидент з Log4j наочно продемонстрував ризики, пов'язані з **використанням відкритого ПЗ** та складних ланцюжків поставок (software supply chain).
Ключові висновки:
Швидкість реакції критично важлива: Час між оголошенням вразливості та початком масової експлуатації становив години, а не дні.
Необхідність прозорості: Компанії мають мати повне уявлення про всі програмні компоненти, які вони використовують.
Захист — це безперервний процес: Недостатньо встановити захист один раз. Потрібні процеси для моніторингу загроз, управління вразливостями та негайного реагування на інциденти.