Урок № 9.

Тема уроку: Інструктаж з БЖД. Виявлення атак. Захист периметра комп’ютерних мереж. Керування механізмами захисту.

На цьому уроці ти дізнаєшся про захист комп’ютерних мереж, про міжнародні стандарти інформаційної безпеки.

Правила поведінки за комп'ютером:

Пам’ятай:

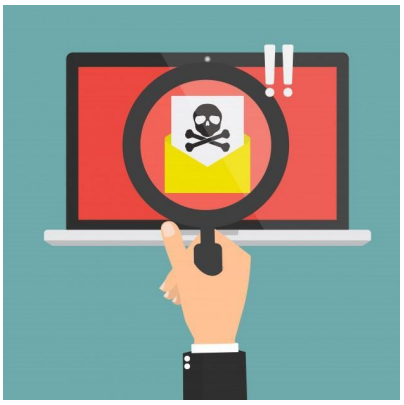
- Робоче місце за комп'ютером потрібно тримати у порядку.
- Не клади зайвих речей на стіл біля комп'ютера.
- Прибирай пил з комп'ютера спеціальною ганчіркою, коли він вимкнений.

Виконуй:

- Слідкуй за осанкою (спина повинна бути прямою).
- Очі мають бути на відстані 50 – 60 см від екрану монітору.
- Кожні 30 хвилин роби перерву в своїй роботі.

Виявлення атак. Захист периметра комп’ютерних мереж.

Процес виявлення атак є процесом оцінки підозрілих дій, які відбуваються в корпоративній мережі. Інакше кажучи, виявлення атак (intrusion detection) - це процес ідентифікації й реагування на підозрілу діяльність, спрямовану на обчислювальні або мережні ресурси.



Основні підходи до виявлення атак практично не змінилися за останню чверть століття і, незважаючи на гучні заяви розробників, можна з упевненістю стверджувати, що виявлення атак базується або на методах *сигнатурного аналізу*, або на методах *виявлення аномалій*. Можливо також спільне використання зазначених вище методів.

Існує кілька способів класифікації систем виявлення атак, кожен з яких заснований на різних характеристиках:

- *Спосіб контролю за системою* (поділяються на network-based, host-based і application based).
- *Спосіб аналізу.* (частина системи визначення проникнення, яка аналізує події, отримані з джерела інформації та приймає рішення, чи відбувається проникнення). Способами аналізу є виявлення зловживань (misuse detection) та виявлення аномалій (anomaly detection).

Затримка в часі між отриманням інформації з джерела та її аналізом і прийняттям рішення. Залежно від затримки в часі, системи виявлення атак діляться на interval-based (або пакетний режим) і real-time.

Аналіз активності.

Статичні і динамічні IDS.

- Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПО, помилки в конфігураціях і т. д. Статичні IDS перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення.
- Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережеві пакети, що передаються за певний проміжок часу. Динамічні IDS реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

Мережеві IDS.

- Мережеві IDS (англ. Network-based IDS, NIDS) розташовуються в стратегічному

місці або в таких місцях мережі, де можливий контроль трафіку всіх пристроїв у мережі. Вони здійснюють контроль усього трафіку даних всієї підмережі та порівнюють трафік, який передається в підмережі з бібліотекою відомих атак. Як тільки розпізнана атака або визначено відхилення у поведінці, відразу надсилається попередження адміністратору.

Хостові IDS.

- IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються

хостовими або системними IDS.

Експертні системи.

- Експертна система складається з набору правил, які охоплюють знання людини-експерта. Використання експертних систем являє собою розповсюджений метод виявлення атак, при якому інформація про атаки формулюється у вигляді правил. Ці правила можуть бути записані, наприклад, у вигляді послідовності дій або сигнатури. При виконанні кожного з цих правил приймається рішення про наявність несанкціонованої діяльності. Важливим достоїнством такого підходу є практично повна відсутність фіктивних тривог.

Сигнатурний аналіз заснований на припущенні, що сценарій атаки відомий і спроба її реалізації може бути виявлена в журналах реєстрації подій або шляхом аналізу мережевого трафіку.

Стандарти кібербезпеки.

Стандарти кібербезпеки – це методи, що зазвичай викладені в опублікованих матеріалах, які намагаються захистити кібернетичне середовище користувача чи організації.

Це середовище включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію в режимі зберігання або транзиту, програми, служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж.

Основна мета — знизити ризики, включаючи попередження або пом’якшення кібератак. Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології.