Найкращі практики безпеки - чек лист нульового рівня

- Виконайте оцінку ризиків:
  Знання та розуміння цінності того, що ви захищаєте, допоможе виправдати витрати на безпеку.
- Розробіть політики безпеки:
  Створіть політику, яка чітко окреслює правила організації, посадові ролі, а також відповідальність і очікування для співробітників.
- Заходи фізичної безпеки:
  Заходи фізичної безпеки – обмежте доступ до комунікаційних шаф, серверних кімнат, а також до систем пожежогасіння.
- Заходи управління людськими ресурсами:
  Необхідно виконати перевірку даних всіх співробітників.
- Виконайте перевірку резервних копій:
  Запровадьте регулярне резервне копіювання та тестування відновлення даних з резервних копій.
- Встановлення виправлень та оновлень, пов'язаних з безпекою:
  Регулярно оновлюйте операційні системи та програми сервера, клієнта та мережного пристрою.
- Використовуйте засоби контролю доступу:
  Налаштуйте ролі і рівні привілеїв користувачів, а також надійну автентифікацію.
- Регулярно перевіряйте реагування на інциденти:
  Використовуйте команду з реагування на інциденти та перевіряйте сценарії реагування на надзвичайні ситуації.
- Впроваджуйте моніторинг мережі, аналітику та інструменти керування:
  Виберіть рішення для моніторингу безпеки, яке інтегрується з іншими технологіями.
- Встановіть пристрої захисту мережі:
  Використовуйте маршрутизатори, міжмережні екрани та інші пристрої безпеки нового покоління.
- Впроваджуйте комплексне рішення безпеки кінцевих вузлів:
  Використовуйте антизловмисне і антивірусне програмне забезпечення корпоративного рівня.
- Навчайте користувачів:
  Забезпечте навчання працівників процедурам безпеки.
  Однією із найбільш відомих і шанованих організацій з навчання кібербезпеки є Інститут SANS.
- Шифруйте данні:
  Шифруйте всі конфіденційні дані компанії, включно з електронною поштою.

- IPS може блокувати або відхиляти трафік на основі спрацювання правила або при збігу сигнатури.
- IDS сканує дані і перевіряє їх базі даних правил або сигнатур атак, шукаючи шкідливий трафік.
- DLP призначена для запобігання крадіжці конфіденційних даних або їх витоку з мережі.
- SIEM збирає з пристроїв безпеки в мережі та аналізує попередження безпеки, журнали та інші дані, отримані в реальному часі та в минулому.