Рекомендації щодо посилення кіберзахисту роутерів TP-Link
(актуальні для пристроїв інших виробників)

1. Перевірити модель пристрою (зазначено на самому пристрої або можна перевірити в його веб-інтерфейсі на сторінці About).
2. Перевірити наявність підтримки:
   a. відкрити сторінку моделі на сайті TP-Link (https://www.tp-link.com/);
   b. переконатись, що оновлення доступне для цієї моделі.
3. Пристрій вважається небезпечним, якщо не має оновлень через End of Support. Рекомендується замінити його на новий. При цьому, необхідно вимкнути віддалений доступ до нього та залишити можливість внесення змін лише з внутрішньої мережі.
4. Оновити прошивку:
   a. онлайн оновлення (якщо підтримується):
      i. зайти в веб-інтерфейс та відкрити сторінку Firmware Upgrade / System Update;
      ii. натиснути Check for Updates / Online Upgrade;
      iii. якщо доступно, натиснути Upgrade дочекатись завершення і перезавантаження;
   b. локальне оновлення через файл:
      i. завантажити оновлення для вашої моделі з офіційного сайту TP-Link;
      ii. розпакувати архів та отримати .bin файл;
      iii. зайти в веб-інтерфейс та відкрити Advanced > System Tools > Firmware Upgrade (може відрізнятись залежно від версії пристрою) натиснути Browse > вибрати файл > Upgrade.
5. Не вимикати пристрій під час процесу оновлення (забезпечити гарантоване живлення).
6. Вимкнути віддалений доступ:
   a. у веб-інтерфейсі відкрити Remote Management / Remote Access;
   b. встановити Remote Management IP Address значення 0.0.0.0 або іншу підконтрольну тільки вам IP-адресу;
   c. переконатись, що веб-інтерфейс недоступний з мережі Інтернет.
7. Змінити пароль доступу до пристрою:
   a. відкрити розділ Administration / Password;
   b. змінити стандартний пароль на складний (рекомендується мінімум 15 символів, використовуючи великі і малі літери, спеціальні символи та цифри);
8. Здійснювати періодичну перевірку:
   a. регулярно (рекомендується - раз на місяць) перевіряти наявність оновлень;
   b. контролювати статус підтримки пристрою;
   c. перевіряти налаштування пристрою щодо наявності несанкціонованих модифікацій у конфігурації.
9. Перевірити користувачів роутера, видалити невідомі акаунти.