МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛТАВСЬКА ДЕРЖАВНА АГРАРНА АКАДЕМІЯ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЕКОНОМІКИ, УПРАВЛІННЯ,
ПРАВА ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ
щорічної студентської наукової конференції

17 листопада 2020 року

Полтава 2020

Тези наводяться без змін та редагування. Відповідальність за зміст і редакцію матеріалів несуть автори та наукові керівники.

Для здобувачів вищої освіти закладів вищої освіти

Матеріали щорічної студентської наукової конференції Полтавської державної аграрної академії, 17 листопада 2020 р. – Полтава: ПП «АСТРАЯ», 2020. – 113 с.

озброєння та військової техніки: зб. матеріалів VIII міжнародної науково-практичної конференції, Київ. 2020. – DOI: 10.13140/RG.2.2.22122.13760.

Рень В. І., здобувач вищої освіти СВО Бакалавр
Спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Слюсарь І. І.

АНАЛІЗ КАТЕГОРІЙ ВРАЗЛИВОСТЕЙ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

На даний час, Інтернет речей (Internet of Things, IoT) стрімко розвивається [1]. Однак, механізми кібербезпеки IoT-пристроїв ще далека від досконалості. Наприклад, згідно [2], експерти з безпеки з IBM X-Force виявили, що на ботнет Mozi тепер припадає 90 % трафіку з пристроїв IoT. Як відомо, Mozi вийшов з від вихідних кодів сумнозвісних сімейств шкідливих програм, таких як Mirai, IoT Reaper і Gafgyt. Ботнет здатний до DDoS-атак, крадіжки даних, виконання команд або корисного навантаження.

Все це свідчить про необхідність ретельного вибору пристроїв IoT при створенні проектів системи Smart Home. При цьому потрібно звернути увагу на низку категорій основних вразливостей потенціальних елементів даної системи [3]: слабкі, передбачувані і жорстко закодовані паролі; небезпечні мережні підключення; небезпечні інтерфейси екосистем; відсутність безпечного механізму оновлень; використання небезпечних або застарілих компонентів; недостатній захист приватності; небезпечна передача і зберігання даних; відсутність можливості налаштування пристрою; небезпечні настройки за замовчуванням; відсутність фізичного захисту.

З іншого боку, масштабне впровадження IoT супроводжується появою нової номенклатури пристроїв IoT. Для вирішення питання щодо їх кібербезпеки доцільно використовувати наступну схему [4].

На першому етапі проводиться аудит за кількома напрямами: аналіз архітектури пристрою; дослідження можливості модифікації вбудованого програмного забезпечення та/або зміни конфігурації і віддаленого управління; виявлення найбільш критичних проблем безпеки і перевірка можливих шляхів їх реалізації.

На другому етапі визначається об’єкт дослідження: програмне забезпечення, необхідне для роботи пристрою (firmware); апаратна частина пристрою; системи захисту, що реалізовані в пристрої.

На третьому етапі формується результат перевірки: схема поверхні атаки (attack surface) для пристрою; список раніше невідомих вразливостей (0-day) в прошивці пристрою; список всіх відомих вразливостей (1-day) в сторонньому коді, що використовується в по пристрою; рекомендації щодо підвищення рівня безпеки досліджуваного пристрою.

При цьому, в якості узагальнених рекомендацій щодо реалізації системи Smart Home необхідно звернути увагу на наступні положення [5].

1. Захист роутеру Wi-Fi. Більшість користувачів після установки роутера залишають налаштування за замовчуванням, що є досить поширеною помилкою. Це може становити велику загрозу безпеці підключених пристроїв. Тому, слід негайно змінити паролі (WPA2 або WPA3 на новіших моделях) для підключення до роутера і для доступу до його конфігурації.

2. Шифрування веб-трафіку. Найпростіший метод – створити віртуальну приватну мережу (VPN), яка буде працювати як зашифрований тунель для веб-трафіку. Це дозволить не тільки захистити персональні дані від сторонніх осіб, але і в разі необхідності – отримати доступ до них з будь-якої точки світу.

3. Безпека смартфона. Мобільні пристрої володіють функціоналом комп'ютерів і використовуються не тільки для дзвінків, але і для фотозйомки, зберігання файлів, отримання і відправки електронної пошти. Оскільки більшість цих завдань передбачає доступ до особистих даних і підключення до інтернету, смартфон повинен бути надійно захищений. Хоча для більшості смартфонів доступні рішення з безпеки, які допомагають запобігти проникненню загроз на пристрій, для додаткового захисту слід зашифрувати всі конфіденційні дані на смартфоні. Таким чином, в разі отримання доступу до пристрою, кіберзлочинці не зможуть прочитати особисті дані користувача.

3. Захист смарт-телевізору. Щоб захистити смарт-телевізор, спочатку слід правильно налаштувати його. Перш за все необхідно визначити параметри конфіденційності для даних, які може збирати провайдер, а потім настроїти батьківський контроль для захисту дітей від небажаного контенту. Крім того, важливо перевірити наявність оновлень програмно-апаратних засобів, і, звичайно, завантажити рішення з безпеки для захисту смарт-телевізора.

4. Оновлення програмного забезпечення пристрою (це базове правило кібербезпеки). Будь-які виправлення безпеки та оновлення слід застосовувати відразу після їх виходу, інакше користувач ризикує стати жертвою атак кіберзлочинців.

Список використаних джерел:

1. Слюсарь Игорь, Слюсар Вадим. Особенности интеграции объектов дополненной реальности и Smart House. *XVIII International Scientific and Practical Conference «Modern science, practice, society»*: Abstracts, Boston, USA, 25-26 May 2020. Boston, 2020. Pp. 434-437. – DOI: 10.46299/isg.2020.xviii.

2. URL: https://internetua.com/ibm-obnarujila-botnet-kotoryi-ispolzuet-90-trafika-s-ustroistv-interneta-vesxei (дата звернення: 29.10.2020).

3. URL: https://m.habr.com/ru/company/dsec/blog/509276/ (дата звернення: 29.10.2020).

4. URL: https://dsec.ru/security-audit/research/issledovanie-iot-i-setevyh-ustrojstv/ (дата звернення: 29.10.2020).

5. URL: https://www.unian.net/science/kiberbezopasnost-sovety-kak-usilit-zashchitu-interneta-veshchey-novosti-11172053.html (дата звернення: 29.10.2020).