УДК 621.391

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Правило В. В., Хижняк С. П.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: v.v.pravylo@ukr.net, khizhnyak56843@gmail.com

PROBLEMS OF CYBERSECURITY OF THE INTERNET OF SPEECHES

In this paper, we look at several cybersecurity issues, as well as the importance of preserving information from cyber-attacks.

Як і будь-яка інша технологія, що розвивається, Інтернет речей (IoT) також має безліч переваг та ризиків.[1] Прихильники технологій та виробники пристроїв IoT просувають Інтернет речей як засіб зробити наше щоденне життя кращим та простішим завдяки мільярдам «розумних» пристроїв IoT (наприклад, смарт-телевізори, розумні холодильники, розумні кондиціонери, розумні духовки, розумні камери, розумні кросівки, розумні дверні дзвінки, розумні системи поліцейського спостереження та дорожнього руху, інтелектуальне відстеження здоров'я та ефективності, тощо).

Є деякі проблеми, пов'язані з використанням пристроїв Інтернету речей. Загрози кібербезпеки можуть привести до пошкодження або крадіжки даних з мінімальними зусиллями з боку злочинців. Пристрої Інтернету речей нові і люди можуть скористатися недоліками кібербезпеки зі злим умислом.

Ми живемо в епоху Інтернету речей, і, хоча цифрове з'єднання - це дуже добре, воно створює безліч дрібних точок, де кіберзлочинці можуть проникнути в дані [2]. Безпека Інтернету речей спрямована на вирішення цих проблем і забезпечення безпечного використання Інтернету речей.

Багато з нас покладаються на Інтернет речей в деяких досить важливих справах в суспільстві, навіть якщо ми цього не усвідомлюємо. Комунальні підприємства, такі як енергетика і водопостачання, часто покладаються на пристрої Інтернету речей для управління ними. Датчики Інтернету речей для бізнесу допомагають забезпечити дотримання нормативних вимог і прискорити процес оплати. Коли безпека Інтернету речей знаходиться під загрозою на цьому рівні, стає ще простіше зрозуміти, чому так важливо зберігати дані в безпеці.

Якщо ви щось чуєте про технології, ви повинні знати про Штучний інтелект (ШІ) та автоматизацію. Вони вже допомагають експертам у багатьох галузях сортувати величезні обсяги даних та приймати важливі рішення. Зрештою, автоматизація та ШІ можуть бути використані в інтересах

адміністраторів Інтернету речей і співробітників служби безпеки мережі. Подібні інструменти дозволять цим сторонам виявляти потенційно проблемний трафік і шаблони даних. ШІ може навіть використовуватися для забезпечення дотримання правил, пов'язаних з даними. Але є проблема: коли люди використовують автономні системи, щоб робити вибір, який впливає на безліч реальних людей, стає дійсно очевидним, що одне незручне нелюдське рішення може завдати великої шкоди.

Отже, якщо хтось хоче найближчим часом створити додаток на основі Інтернету речей, він повинен розглянути такі проблеми безпеки, як ці. Для вирішення проблем безпеки, які створюють штучний інтелект і автоматизація необхідний: захист Інтернету речей від атак та захист призначених для користувача даних від крадіжок.

Безпека інтернету речей залишиться головним пріоритетом. Згідно з прогнозами GSMA, до 2025 року кількість підключень до IoT подвоїться і досягне майже 25 млрд в усьому світі, а в міру збільшення популярності IoT зростає ризик кібератак. Кібербезпека IoT викликає занепокоєння у 95% респондентів опитування, проведеного аналітиками IoT Analytics, причому майже 40% «дуже стурбовані» можливими вразливостями інтернету речей. 88% вказали, що підтримують впровадження правил забезпечення безпеки IoT і прийняття галузевих стандартів для управління передовими методами кібербезпеки. Передбачається, що ринок безпеки IoT виросте до $ 36,6 млрд до 2025 року [3].

Пристрої Інтернету речей стають все більш популярними і коли ми довіряємо технологічним компаніям виробляти ці пристрої, ми повинні піти на певний ризик. Технологічні компанії не завжди проявляють належну обачність, коли справа доходить до роботи з пристроями Інтернету речей і зниження ризиків безпеки.

[4] Багато пристроїв Інтернету речей не оновлюються. Коли наші ранні комп'ютерні системи зіткнулися з тією ж проблемою, її (в деякій мірі) було виправлено за допомогою автоматичних оновлень програмного забезпечення. Але якщо справа доходить до пристроїв Інтернету речей, довговічність не завжди є пріоритетом для виробників. Немає простого способу оновлювати пристрої IoT на ходу. Виробники просто створюють щось, щоб привернути увагу своєї аудиторії, а потім працюють над наступним гаджетом, що відповідає цим вимогам. IoT-пристрої потребують належного тестування, перш ніж вони будуть випущені для широкої публіки. Поточні недостатні зусилля для цього не захищають споживачів або обладнання.

Також повинні бути чіткі стандарти безпеки, щоб забезпечувати нашу безпеку кожен день − в школі, на роботі, в Інтернеті, в транспортних засобах та стоячи перед холодильником. Стандарти безпеки, які регулюють пристрої IoT,

неясні. У кращому випадку вони неоднозначні. Більшість пристроїв Інтернету речей складається з безлічі компонентів, вироблених в усьому світі. Це тому, що частини, з яких складаються ці пристрої, дуже спеціалізовані − їх можуть робити тільки деякі сутності. Це створює проблему: коли всі частини створюються окремо, всі вони покладаються на свої власні набори стандартів безпеки. Різні стандарти безпеки роблять пристрої Інтернету речей уразливими. Коли справа доходить до захисту конфіденційності користувачів, це велика проблема.

В налаштуваннях IoT ризикованими є не тільки самі атаки, але і прогнозування і запобігання цих атак, які представляють собою найбільшу проблему. Кібератаки Інтернету речей надзвичайно непередбачувані, більшість хакерів використовують нові сучасні методи, щоб зламати систему безпеки і якомога довше уникнути виявлення. Пристрої Інтернету речей повинні мати можливість миттєво обробляти дані, що ускладнює реалізацію процесів безпеки. Ці процеси безпеки сповільнюють здатність пристрою IoT виконувати функції.

Моніторинг за допомогою ШІ може допомогти в прогнозуванні та запобігання атак в майбутньому. Експертам необхідно виявляти уразливості і усувати їх у міру їх появи.

Сучасні хмарні сервіси вже використовують аналіз загроз для прогнозування проблем безпеки. Ми поступово наближаємося до деяких рішень безпеки для Інтернету речей, але для цього потрібен час.

Ще одним складним питанням, яке потрібно вирішити, є той факт, що певні невеликі атаки IoT насправді можуть уникнути виявлення. Це робить їх особливо небезпечними. Мікропроникнення IoT легко проскакують через багато елементарних мереж безпеки, які ми використовуємо для захисту пристроїв IoT. Кіберзлочинці можуть повільно збирати інформацію, замість того, щоб одночасно передавати у власність величезну кількість записів.

Немає сумнівів що нам потрібно приділяти більше уваги кібербезпеці Інтернету речей, щоб зробити пристрої Інтернету речей більш безпечними у використанні і зберігати інформацію від атак, бо інформація у наш час безцінна.

Література

1. https://www.rapyder.com/blogs/top-10-iot-security-solutions-for-common-iot-security-issues/
2. https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/
3. https://cutt.ly/Yxfi7xW
4. https://option3ventures.com/iot-security-challenges/