УДК 004.056.5

КІБЕРБЕЗПЕКА В УМОВАХ ІНТЕРНЕТУ РЕЧЕЙ

Куник В. І., студ. гр КБ-181
Науковий керівник: **Базилевич В. М.,** к.е.н., доцент
Національний університет «Чернігівська політехніка»

Актуальність обраної теми обумовлена відсутністю глибокої науково практичного опрацювання питань забезпечення кібербезпеки в умовах застосування Інтернет речей. Розробками в сфері досліджень і стандартизації інтернету речей займаються багато країн на рівні національних ініціатив, наприклад ANSI (США), BSI (Великобританія), ETSI (Європа),а також на рівні інтернаціональному: ITU, ISO, IEC. Інтернет речей (Internet of things, IoT) має великий вплив на наше життя – 25 мільярдів пристроїв – від управління інфраструктурою та фабриками до машин легеневого серця та безлічі інших медичних пристроїв, а також пристрої в наших автомобілях та будинках. Але це не безпечно. Одна з оцінок розвитку Інтернету речей надає економічний ефект в межах 3,9 трлн до 11,1 трильйона доларів на рік до 2025 році. Фактичний вплив буде залежати від прийняття рішень підприємствами та споживачами. Безпека стане ключовим елементом цього прийняття – і вартості бізнесу. Захист рішень на базі IoT від тих, хто планує завдати шкоди, буде мати вирішальне значення для зростання IoT, а також для особистої та ділової безпек

Атакуючі користувачі, ймовірно, шукатимуть можливості поставити під загрозу критичну інфраструктуру кожної країни, а також пов’язану набагато ширшими зв’язками екосистему споживчих та промислових пристроїв, відомих як Інтернет речей. Інтернет речей з'єднує мільярди нових пристроїв з Інтернетом, але це також розширює потенціал атаки кібер-дійових осіб проти мереж та інформації. Дослідники з безпеки продовжують розкривати вразливі місця у споживацьких продуктах, включаючи автомобілі та медичні прилади. Якщо атакуюча сторона отримає можливість створювати значні фізичні ефекти в обраній країні через кібер-засоби, вони отримають нові можливості для примусу та стримування. Наприклад, кібератака на українську енергетичну мережу в 2015 році призвела до відключення живлення протягом декількох годин.

Широке включення "розумних" пристроїв у повсякденні об'єкти – це зміна того, як люди та машини взаємодіють між собою та навколишнім світом, часто підвищуючи ефективність, зручність та якість життя. Їх розгортання також приводило до появи нових вразливих місць як в інфраструктурі, яку вони підтримують, на яку вони покладаються, так і на процеси, якими вони керують.

Проектування систем IoT для забезпечення безпеки – це спосіб життя з завданнями на всіх етапах життєвого циклу. Більшість із цих завдань значною мірою пов'язані з дизайном та розробкою програмного коду. Отже, основні вимоги що потрібно розглянути, це: 1) запити; 2) загрози, які ви хочете захистити. Ті, хто пов'язаний з безпекою, повинні збалансувати захист від витрат та час на його забезпечення. Але занадто багато компромісів або забагато винятків призведуть до вразливості системи безпеки платформи IoT. Пристрій запуску повинен бути одним із кінців ланцюжка довіри переходячи від пристрою до серверних додатків. Справжнє безпечне завантаження вимагає апаратного забезпечення.

1. Комунікаційні технології. Шифрування сьогодні є прийнятною частиною будь-якого рішення для безпечного IoT. Але шифрування є складним і має наслідки від апаратного забезпечення до ключового управління. Проте час і витрати на розробку та експлуатацію безпечних комунікацій, достатніх для вирішення запланованих загроз, можна легко занизити.

2. Послуги, мови та інструменти. Слабкі сторони програмного забезпечення у системі та коді є однією з трьох чудових дверей, що призводять до використання вразливостей в роботі IoT. Неадекватні аналізи загроз або вимоги, а також слабкі або невиконані процедури часто призводить до слабкості програмного забезпечення. Отримання та ретельне використання

служб, пов'язаних із безпекою, мовами, стандартами дизайном та кодуванням, а також інструментами, які їх підтримують, можуть здаватися дорогими, доки вартість не призведе до серйозного порушення, якого можна було б запобігти.

3. Сертифікація. Сертифікація безпеки може вимагатись для певного напрямку діяльності. Навіть якщо це не потрібно зараз, усвідомлюючи вимоги щодо сертифікації та включення корисних елементів у практику розробки, вже зараз потрібно створювати безпечні продукти та потенційно підготувати їх до вимог сертифікації в майбутньому.

4. Промислова кооперація. Боротьба з хакерами – це асиметрична війна. Співпраця щодо виявлення дефектів, відстеження та спільного використання розробників, навіть конкурентів, стала прийнятною практикою. Так NIST Cybersecurity Framework призвела до розробки основ для організації зусиль щодо впровадження та адаптації практик безпеки в організації.

Незалежно від того, написано цілком однією організацією або в тому числі сторонніми операційними системи, проміжне програмне забезпечення, бібліотеки або програми, які використовує продукт, навіть "малі" пристрої можуть мати великі коди.

Кардіостимулятор, що керує серцем людини, може мати 80 000 рядків коду; підключений термостат може використовувати Linux з повним стеком Інтернету плюс його додаток; сучасний автомобіль містить понад 100 мільйонів рядків коду.

Активне використання кіберпростору впливає на людську особистість. Застосування методів соціальної інженерії (Науки про управління поведінкою людини без технічних засобів, на основі психології) і інших способів масового розкрадання електронних грошей та інформації підвищує важливість забезпечення кібербезпеки, тому успішна «співпраця» між компаніями розробки IoT-технологій може відбуватися тільки в умовах забезпечення належного рівня кібербезпеки.

Майбутнє в умовах Інтернету речей повинно бути обов'язково усвідомлено і досліджено з різних точок зору: соціальної, психологічної, політологічної, військової та економічної. Безліч нестандартних (а найчастіше - конфліктних) ситуацій у світі, підключеному до єдиної Інтернет-системі, заснованому на принципах співпраці і існуючому за рахунок поновлюваних джерел енергії, вимагає підвищеної уваги.

Розвиток кібербезпеки передбачає, що фінансові інститути і підприємства, що займаються онлайн–торгівлею , почнуть широко застосовувати біометричну ідентифікацію. Поява портативних сканерів ДНК обіцяє чергову технологічну революцію в області ідентифікації клієнтів. це підвищить можливості захисту конфіденційної інформації і грошових коштів, а клієнт отримає можливість самостійно вибирати той спосіб захисту, який він вважає за краще.

Регулюючі органи повинні створити працездатну систему забезпечення кібербезпеки в кредитно-фінансовій сфері, в тому числі спеціальні наглядові підрозділи.

Продовженням політики регулятора в області забезпечення кібербезпеки повинні стати рекомендації для організацій кредитно фінансової сфери, виконання яких дозволить мінімізувати можливі наслідків кібератак.

Список використаних джерел

1. Jang-Jaccard J., Nepa S. A Survey of Emerging Threats in Cybersecurity // Journal of Computer and System Sciences. 2014. Vol. 80. Iss. 5. P. 973–993.
2. Elmaghraby A.S., Losavio M.M. Cyber Security Challenges in Smart Cities: Safety, Security and Privacy // Journal of Advanced Research. 2014. Vol. 5. Iss. 4. P. 491–497.
3. Electronic Voting in Switzerland [Електронний ресурс] – Режим доступу: http://web.archive.org/web/20070212194901/www.swissworld.org/dvd_rom/eng/direct_democracy_2004/content/votes/e_voting.html
4. Брусницын Н.А. Информационная война и безопасность. М.: Вита-Пресс, 2001. 280 с.
5. Information is Beautiful. New car source: Newcomb, D. 2013. “The Next Big OS War Is in Your Dashboard.” Wired. December 3. [Електронний ресурс] – Режим доступу: http://www.wired.com/2012/12/automotive-os-war/
6. Конявский В.А., Лопаткин С.В. Компьютерная преступность. Т. 1. М.: РФК-Имидж Лаб, 2006. 560 с.