ЗАХИСТ ІНФОРМАЦІЇ У СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Деркач Я.О., Агеєв Д.В.
Харківський національний університет радіоелектроніки, Україна

Відповідно до сучасних досліджень [1, 2] на IoT припадає понад 30% усіх підключених до мережі пристроїв середнього підприємства. 57% цих пристроїв уразливі до атак середнього або високого рівня.

Крім того, база даних Gartner Machina IoT Forecast прогнозує, що до 2030 року на підприємствах буде понад 18 мільярдів підключених пристроїв.

Крім того, 98% усього трафіку Інтернету речей є незашифрованим.

Незашифровані дані, що надходять із некерованих пристроїв IoT, потенційно можуть призвести до витоку даних або успішної атаки програм-вимагачів.

Метою доповіді є аналіз методів захисту інформації у системах інтернету речей.

Проведений аналіз показав, що поширеними атаками на IoT є [2-4]:

- DDoS-атака. Аномально висока активність може призвести до значних затримок у роботі системи або взагалі її зупинки. Вдало скоригована та налаштована DDoS-атака може викликати системну помилку компонента безпеки, приховуючи реальні шкідливі дії;
- експлойт програмного забезпечення. багато кіберзлочинців використовують відомі вразливості в програмній частині пристрою для проведення атаки;
- MITM-атака. Хакери можуть перехопити мережевий трафік (вставши посеред каналу передачі між пристроєм відправником та пристроєм одержувачем) та отримати облікові дані або конфіденційну інформацію, яку пристрої IoT передають через корпоративні мережі;
- фізичне втручання. Простого підключення кіберзлочинцем USB флешки зі шкідливим кодом, до зовнішнього пристрою IoT достатньо, щоб поширити шкідливе програмне забезпечення через мережу і шпигувати по комунікаціях, що проходять в ній;
- брутфорс атаки. В компаніях зазвичай не приділяється достатньо уваги парольній безпеці пристроїв IoT, що робить їх вразливими до потенційних атак грубою силою.
- перехоплення прошивки. Якщо оновлення мікропрограми пристрою не було підписано криптографічно або прошивка передається по незахищеному каналу зв'язку – це дозволяє зловмисникам перехопити її та завантажувати шкідливе ПЗ на пристрої під виглядом апдейтів.

Для захисту від цих атак необхідно використовувати низку заходів [2-4].

1. Управління поверхнею атаки, інвентаризація та моніторинг усіх пристроїв. Адміністратори безпеки повинні знати точну кількість використовуваних пристроїв, а також ідентифікатори виробників, серійні номери, версії обладнання та прошивки. Моніторинг, аналіз та звітність у

режимі реального часу є вкрай важливими для організацій, щоб мати можливість керувати ризиками Інтернету речей.

2. Сегментація мережі. Сегментація запобігає отриманню зловмисником доступу до всієї мережі організації, обмежуючи поверхню атаки та мінімізуючи збитки.

3. Встановлення надійних паролів для IoT. Пароль має бути стійким для підбору, унікальним для кожного захищеного пристрою та відповідати політикам керування паролями організації.

4. Захист пристроїв IoT фізично. Фізичний захист пристроїв має дуже велике значення, оскільки IoT пристрої, доступні ззовні, можуть зазнати фізичного втручання зловмисників з метою отримання несанкціонованого доступу або завантаження в систему шкідливого ПЗ.

5. Своєчасні оновлення прошивок. Регулярне оновлення ПЗ значно покращує загальну безпеку IoT.

Виявлення атак і захист мережі IoT стали дуже складним завданням для механізмів безпеки, таких як системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS). Це призводить до великої затримки у виявленні атак і до збільшення кількості помилкових спрацьовувань, що генеруються поточними системами моніторингу. Для вирішення цього завдання необхідно для захисту в системах інтернету речей застосувати методи машинного навчання.

Перетворення захисту IoT пристроїв в автоматизовані політики, які захищають IoT в інфраструктурі, може зробити систему інтернету речей організації менш ризикованою.

Поєднання цих політик з повним спектром хмарних і локальних служб безпеки, щоб блокувати всі відомі та невідомі загрози, спрямовані на IoT. пристрій – це кінцева мета захисту інформації.

Впровадження ефективних стратегій кібербезпеки, регулярне оновлення програмного забезпечення та освіта користувачів допоможуть мінімізувати ризики безпеки у системах інтернету речей.

Список літератури

1. Anand Oswal. Securing IoT without Added Burden. URL: https://www.paloaltonetworks.com/cybersecurity-perspectives/expanding-iot-visibility.

2. IoT security survey reveals alarming challenges and costs. URL: https://www.iot-now.com/2023/10/18/137178-iot-security-survey-reveals-alarming-challenges-and-costs/.

3. Ge, Mengmeng, et al. "Deep learning-based intrusion detection for IoT networks." *2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC)*. IEEE, 2019.

4. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

5. Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409.