ВАРІАНТИ ФОРМУВАННЯ ГРУП ДЛЯ УПРАВЛІННЯ РЕАГУВАННЯМ НА КІБЕРІНЦИДЕНТИ

Дьогтєва Ірина Оксентіївна,
асистент кафедри менеджменту та безпеки інформаційних систем,
Вінницький національний технічний університет, Україна

Цифрова трансформація бізнесу, активне використання нових технологій для підвищення ефективності та конкурентоспроможності, діджиталізація сервісів під час введення дистанційних режимів функціонування актуалізує питання діяльності компаній в рамках кібербезпеки та кіберстійкості.

Кіберстійкість вимагає від суб'єктів кібербезпеки ефективно та вчасно реагувати на кібератаки, забезпечувати в режимі реального часу готовність до реагування на поточні та потенційні кіберзагрози. За таких умов важливою є організація управління реагуванням на інциденти інформаційної безпеки в рамках роботи відповідних груп. На сьогодні прикладами таких груп можуть слугувати Security Operations Centres, Security Incident Response Teams та Information Security Incident Response Team, тощо.

«Група реагування на інциденти» відповідно до ISO/IEC 27035-1:2016 [1] це команда належно кваліфікованих та надійних членів організації, які займаються вирішенням інцидентів протягом їхнього життєвого циклу. Дана група здебільшого забезпечує функцію організаційного характеру і, по суті, охоплює процес інцидентів з інформаційною безпекою, пов'язаних з інформаційними технологіями загалом.

В рамках роботи груп реагування на інциденти варто також зауважити, що поняття «управління інцидентами інформаційної безпеки» можуть різнитись. Наприклад, міжнародні стандарти ISO/IEC 27000 визначають таке управління або в якості набору процесів для виявлення, звітності, оцінки, реагування, вирішення та вивчення інцидентів з інформаційної безпеки [2], або в якості застосування послідовного та ефективного підходу до обробки інцидентів інформаційної безпеки [1].

В стандарті ISO/IEC 27043:2015 [3], наприклад, також зазначені ще такі загальновживані терміни для групи реагування на інциденти: CERT (Команда екстреного реагування на комп'ютерні інциденти) та CSIRT (Група реагування на інциденти з комп'ютерної безпеки).

Термін CERT має американське походження (офіційно зареєстрований в США Координаційною групою CERT (CERT / CC)) та захищений авторським правом. В класичному розумінні дана група зосереджена на інцидентах інформаційно-комунікаційних технологій. В Україні, зокрема, з 2007 року розпочав свою діяльність спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) Держспецзв'язку, який з 2009 року має статус CERT та є повноправним членом групи FIRST (Форум команд реагування на інциденти інформаційної безпеки). CERT-UA (Урядова

команда реагування на комп’ютерні надзвичайні події України) виконує ряд завдань пов’язаних з кіберінцидентами [4].

Історично з метою розширення терміну CERT був введений термін CSIRT, наразі вони використовуються в якості синонімів, останній переважно в Європі. Визначення CSIRT пропонується в ISO/IEC 27035-3:2020, зокрема це команда експертів з безпеки для підтримки розгляду інцидентів інформаційної безпеки [5], тобто вважають, що дана група може бути представлена у вигляді сервісної організації, яка відповідає за отримання, перегляд та реагування на повідомлення про інциденти та діяльність із комп’ютерної безпеки.

Існує ще ряд різних абревіатур, що позначають подібні групи, наприклад: CIRT (Група Реагування на Комп'ютерні Інциденти), SERT (Група Оперативного Реагування на Інциденти Безпеки).

Як інструмент для забезпечення комплексного підходу в питанні моніторингу і реагування на інциденти у вигляді єдиної платформи для збору, зберігання і обробки інформації про стан безпеки IT-інфраструктури, вразливості та інциденти інформаційної безпеки визначають Операційний центр безпеки (Security Operations Centres - SOC). Природно, що функція реагування на інциденти (повністю або частково) поряд з іншими завданнями входить до компетенції SOC. Даний центр безпеки відомий під різними назвами, включаючи «операційний центр» і «центр зв’язку». Його структура має централізований характер на відміну від попередніх варіантів та опікується питаннями безпеки на організаційному та технічному рівнях.

Загалом SOC в рамках управління інцидентами покликаний покривати такі аспекти як людські ресурси (структура, якість персоналу, залучення фахівців, тощо), процеси (сортування, аналіз інцидентів, звітність про інциденти, реагування на інциденти, робота з питань усунення наслідків інцидентів, виявлення вразливостей, робота щодо усунення вразливостей) і технології (готовність мережевої інфраструктури, кореляція, аналіз, моніторинг безпеки, управління безпекою, журнал безпеки, оцінювання, відстеження вразливостей) [6]. SOC збирають дані, пов’язані з інформаційними системами, які вони захищають, і обробляють їх для виявлення підозрілих дій.

Операції SOC варіюються від реагування на інциденти комп'ютерної безпеки до пристроїв безпеки. Хоча класично, це команда, яка складається здебільшого з аналітиків з безпеки, в завдання яких входить виявлення та аналіз інцидентів кібербезпеки, оперативне реагування, запобігання їх виникненню і підготовка звітності. В межах звітності, зазвичай очікується, що SOC навчатиме користувачів, як вони повинні повідомляти про інциденти безпеки, і інформувати про доступні для користувачів канали для повідомлення про події, які ідентифікуються як інцидент безпеки [6].

Типовий центр операцій безпеки (SOC) контролюється експертами з безпеки для виявлення аномальної діяльності та аналізу даних безпеки з мереж, серверів та баз даних певної компанії з метою забезпечення захисту від потенціальних атак. Автор [7] зосереджує увагу на забезпеченні захисту в режимі реального часу операційним центром, який виступає в ролі централізованого погляду на

загальну інфраструктуру організації підприємства та окремі інформаційні системи.

SOC малих організацій відрізняються від команд інформаційної безпеки у великих організаціях. Вони укомплектовані аналітиками, старшими аналітиками, менеджерами та лідером, який контролює всі функції. Члени команди фокусуються на ідентифікації загроз, виявленні вразливостей і аномалій, які можуть викликати безпековий інтерес. Відповідний процес зазвичай не координується з іншими видами груп інформаційної безпеки [8].

Отже, за умов актуальності захисту від атак у кіберпросторі, враховуючи збільшення кількості та номенклатури таких атак, розширення географії комплексних кібератак, коли зловмисники застосовують набір методів, технологій, інструментів та програмних засобів в рамках реалізації однієї атаки, зростає кількість як самих груп реагування на інциденти, так і варіабельність їх задач та комплектацій.

Список літератури

1. ISO/IEC 27035-1:2016, Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en (accessed 14.01.2022).

2. ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (accessed 14.01.2022).

3. ISO/IEC 27043:2015, Information technology — Security techniques — Incident investigation principles and processes. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27043:ed-1:v1:en (accessed 14.01.2022).

4. CERT-UA - Урядова команда реагування на комп'ютерні надзвичайні події України: веб-сайт. URL: https://cert.gov.ua (дата звернення: 05.01.2022).

5. ISO/IEC 27035-3:2020, Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-3:ed-1:v1:en (accessed 14.01.2022).

6. Joseph Muniz, Gary McIntyre, Nadhem AlFardan Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press, 2015. 448 p.

7. Darren Death Information Security Handbook: Develop a threat model and incident response strategy to build a strong information security framework. Packt Publishing Ltd, 2017. 330 p.

8. Eric C. Thompson Designing a HIPAA-Compliant Security Operations Center: A Guide to Detecting and Responding to Healthcare Breaches and Events. Apress, 2020. 231 p.