ВАЖЛИВІСТЬ ПОБУДУВАННЯ ЦЕНТРУ УПРАВЛІННЯ БЕЗПЕКОЮ
ВАЖНОСТЬ ПОСТРОЕНИЯ ЦЕНТРА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОТИ
IMPORTANCE OF BUILDING OF SECURITY OPERATIONS CENTER

Науковий керівник - доцент кафедри радіотехнічних пристроїв
Старцев В.І., Старцев В.И., Starcev V.I.,
Студентка – Митрофановська А.В, Митрофановская А.В., Mytrofanovska A.V.,

Анотація: розглянуто важливість створення центру управління безпекою, що таке центр управління безпекою та головні переваги побудування на підприємстві.

Ключові слова: центр управління безпекою, моніторинг IT-систем, інформаційна безпека, захист від вразливостей, кібератака

Аннотация: рассмотрено важность создания центра обеспечения безопасности, что такое центр обеспечения безопасности и главные преимущества построения на предприятии.

Ключевые слова: центр безопасности, мониторинг IT-систем, информационная безопасность, защита от уязвимостей, кибератака

Abstract: The importance of creating a security operation center, what is a security operation center and the main advantages of building in the enterprise are considered

Key words: security operation center, IT-systems monitoring, information security, vulnerability protection, cyberattack

Майже щодня ми чуємо чи читаємо про кібератаку чи порушення безпеки в організації, що спричиняє величезну втрату даних та грошей. Власники бізнесу стають розумнішими, і вони починають вживати суворих дій щодо кібератак. Будь-якому адміністратору важливо зберігати онлайн-активи та інфраструктуру в безпеці, оскільки вони можуть бути мішенню для кібератаки, якщо з’являться якісь порушення в системі. Сьогодні організації починають розширювати свої можливості виявлення вразливостей, вкладаючи кошти в Центр Управління Безпекою (SOC), який виявляє недоліки в їх IT-інфраструктурі,

що можуть призвести до кібератак. Вдосконалення позиції безпеки IT в організації повинно бути головним питанням власника.

Центр управління безпекою (SOC) — це внутрішня організація команди спеціалістів IT-безпеки, головне завдання яких — щодня контролювати та постійно аналізувати позиції безпеки організацій. Команда з питань безпеки аналізує IT-системи та виявляє недоліки чи загрози через довірений набір процесів та технологічних рішень. Вони також несуть відповідальність за виявлення та вирішення загроз інформаційним активам організації. Команда SOC тісно співпрацює з групами реагування на інциденти в організації, щоб швидко вжити заходів при виявленні. Команда SOC також складається з аналітиків безпеки та експертів, які здійснюють нагляд за операціями з безпеки.

Центр управління безпекою може виявити потенційну атаку, вивчивши механізми атаки та яку частину IT-системи вона поставить під загрозу. Організації, які мають SOC, здатні виявити недоліки в своїх IT-системах і, таким чином, можуть уникнути нещасного випадку.

IT-лідери починають приймати важливі рішення щодо забезпечення своїх IT-систем і тепер зосереджуються на людському впливі, а не на технологічному для вивчення та зменшення загроз. Члени команди постійно контролюють та аналізують відомі та існуючі загрози для вивчення виникаючих ризиків. Технологічні системи, такі як брандмауери, можуть запобігти елементарним атакам, але людський аналіз може «врятувати життя». SOC потрібно оновлювати новітніми технологіями, наприклад, такими як інтелектуальні системи загроз, що може бути корисним для вдосконалення рішень та механізмів захисту. SOC збирає всі дані всередині організації та співвідносить їх з інформацією із зовнішніх джерел, таких як стрічки новин, повідомлення про інциденти, повідомлення про загрози та повідомлення про вразливості, які надають уявлення про вразливості та допомагають залишатись в курсі нових кіберзагроз. Команда SOC повинна випереджати інциденти, вводячи дані розвідувальних даних про загрози в інструменти для збереження оновлених процесів для розрізнення між реальними загрозами та не загрозами. Високоякісний SOC використовує автоматизацію безпеки, щоб стати більш ефективним.

Завдяки висококваліфікованим експертам з безпеки, що мають автоматизацію безпеки, організації мають змогу посилити свої аналітичні сили для посилення заходів безпеки та захисту захищених порушень безпеки та кібератак. Здебільшого організації, які не мають власних ресурсів або можливостей, користуються послугою SOC-as-a-Service.

Однією з головних переваг роботи центру безпеки є те, що він покращує виявлення аварійних ситуацій через постійний моніторинг та аналіз. Завдяки цій діяльності команда

SOC може аналізувати мережі, сервери та бази даних, що забезпечує своєчасне виявлення інцидентів безпеки. Відслідковуючи 24/7, SOC може надати організаціям перевагу захищатись від вторгнень незалежно від типу атаки в будь-який час.

Сьогодні організаціям важливо забезпечити належний захист їх IT-інфраструктури, оскільки вона містить дуже цінну інформацію і є невід'ємною частиною компанії. Служби SOC надають глибокий погляд на позицію безпеки організації та рекомендують виправлення та зміни для забезпечення здорової IT-інфраструктури. Втратити свої дані у разі кібератаки може бути дуже дорогою справою, але якщо у вас є послуга SOC, то вона активно визначає інциденти та забезпечує оптимальну безпеку.

СПИСОК ЛІТЕРАТУРИ

1. Остапчук В.В. Комплексна система захисту інформації на підприємстві Seton Hungary KFT; наук. керівник О.С. Сафронов // Сучасні інформаційні технології та телекомунікаційні мережі: тези доп. 53-ї наук. конф. молодих дослідників ОНПУ-магістрів. — Одеса, 2018. — С. 16
2. Передумови до створення SOC. [Електронний ресурс]. URL: https://www.anti-malware.ru/practice/methods/preconditions outsourcing-soc
3. Родичев Ю.А. Нормативна база та стандарти в області інформаційної безпеки — Санкт-Петербург: Питер, 2017. — 254 с.
4. Сафронов О.С., Венедиктов Ю.І., Барабанов М.О. Життєвий цикл системи управління інформаційною безпекою організації // Тези доповідей V міжнародної конференції «Управління проектами у розвитку суспільства» — Київ, 2008. — С. 46-47
5. Сафронов О.С. Аналіз застосовності стандарту ISO / IEC 31010: 2009 «Методи оцінки ризиків» для завдань інформаційної безпеки // Матеріали XII міжнародної науково-технічної конференції «АВІА-2015». — К.: НАУ, 2015. — С. 54-57
6. Сафронов О.С. Аналіз ризиків інформаційної безпеки на основі стандарту ISO / IEC 31010 // Праці XV міжнародної науково-практичної конференції «Сучасні інформаційні та електронні технології». — Одеса: 2015. — С. 135-136
7. Системи для аналізу захищеності інформаційних систем [Електронний ресурс]. URL: https://www.anti-malware.ru/security/security-check
8. Стрєльцов О.С. Система контролю та управління доступом співробітників підприємства; наук. керівник О.А. Сиропятов // Сучасні інформаційні технології та телекомунікаційні мережі: тези доп. 53-ї наук. конф. молодих дослідників ОНПУ-магістрів. — Одеса, 2018. — С. 16
9. Cisco OpenSOC — open source рішення для створення власного центру моніторингу кіберзагроз. [Електронний ресурс]. URL: http://habrahabr.net/thread/1370