УДК 004.7.056.5
DOI: 10.31673/2409-7292.2020.034448

Бушков В.Г., Соловйов Є. В., Бобровський О.О., Міщан В.Є., Попов В.О.

ФУНКЦІОНАЛЬНА МОДЕЛЬ ОПЕРАТИВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ

У статті розглядається функціональна модель Оперативного центру кіберзахисту (SOC – Security Operation Center), яка поєднує основні політики, процедури та технологічні засоби для протидії кібервпливам на організацію. Визначені основні функції SOC, завдання та способи реалізації. Наведено приклади практичного застосування моделі. Запропонована архітектура типової інфраструктури SOC.

Ключові слова: Оперативний центр кіберзахисту, кібератака, кібербезпека, захист мережі.

Вступ

За вже сформованою світовою практикою Оперативний центр кіберзахисту (SOC – Security Operation Center) – це підрозділ в організації (установі), який відповідає за захист інформації, інформаційних систем та блокування кібератак, спрямованих на порушення інформаційної безпеки [1]. Головною метою функціонування SOC є поліпшення стану інформаційної/кібер безпеки організації шляхом виявлення і реагування на загрози та будь-який вплив на бізнес. SOC збирає дані та управляє подіями безпеки у мережі та мережевому обладнанні, і, шляхом їх аналізу, покращує безпеку системи та мережі. Структура SOC охоплює, як правило, п’ять основних напрямів діяльності [2]: збір даних, реєстрація та архівування записів, аналіз та кореляція подій, реагування на інциденти, взаємодія з менеджментом організації. Разом з тим, таку архітектуру не можна вважати сталою і дослідження у цій сфері постійно тривають. Не зважаючи на вже напрацьований досвід у світі, питання щодо створення ефективної фукнціональної моделі SOC залишаються відкритими.

Аналіз публікацій

У багатьох наукових публікаціях наведено різні архітектури для SOC. Так у [3] запропоновано 8 модулів для SOC: збір журналів, збереження та архівування журналів, аналіз журналів, моніторинг середовищ безпеки для подій безпеки, кореляція подій, управління інцидентами, реакція на загрози, ідентифікація загроз та звітування. У [4] розроблено федеративну структуру SOC, яка контролює широкосмугову мережу. Запропонована архітектура складається з цих модулів: зондування, контролю, аналізу, обробки подій та інтерфейсу користувача. В такій архітектурі можливий аналіз та прогнозування атак. У [5] акцентують увагу на інцидентах безпеки та управлінні подіями за допомогою SIEM-систем. Їх дизайн складається з таких підрозділів: колекція подій, архів подій, аналіз подій та візуалізація. У [6] розроблено центр безпеки, використовуючи аналогію з імунології природного світу. Основну увагу зосереджено на виявленні вторгнень шляхом аналізу інформації журналів, зібраної в мережевих пакетах. Розроблено SOC, що складається з клітинних агентів імунітету. Ці агенти генеруються динамічно, коли відбувається доступ через мережу. Агенти виявляють незаконного зловмисника як автономну сутність. Коли агент імунітету виявляє та автономного порушника то він співпрацює з іншими агентами імунітету та видаляє всі файли та процеси, що виконуються як вторгнення. Запропонована архітектура складається з 6 рівнів: датчики, агенти збору, база даних, модуль аналізу інцидентів, база знань, модуль звітування. У [7] запропоновано ієрархічний центр безпеки оператора мобільного звязку для подолання єдиної точки вразливості. Архітектура має чотири рівні: Перший рівень – рівень датчиків вторгнень і складає NIDS і HIDS. На цьому шарі генеруються сповіщення. Керівником для кожної групи вибирається комп’ютер шляхом голосування. Мобільні агенти збирають та аналізують попередження. Другий, третій та четвертий рівень пов'язані з групою, підрозділом та HMSOC. Кореляція оповіщення та мобільний агент включають етапи модифікації, нормалізації, синтезу, оцінки та звітування.

Метою цієї статті є розробка архітектури SOC, яка б поєднувала кращі практики щодо реєстрації, аналізу та реагування на кіберінциденти.

Організаційна інфраструктура безпеки

Як визначено вище, організаційна інфраструктура, розгорнута на рівні підприємства, є фактичною інфраструктурою, яка використовується для захисту всіх необхідних підрозділів організації. Це пристрої та технології, які розгорнуті на всьому підприємстві у ключових місцях, які виконують фактичну роботу із захисту, виявлення або припинення зловмисної поведінки чи атак. Це може бути брандмауер, який використовується по периметру або всередині мережі, або навіть у сторонніх компаній та постачальників хмарних послуг аж до антивірусного програмного забезпечення на кінцевому комп'ютері користувача. Подивившись на поглиблений підхід до безпеки, можна знайти безліч різних систем, якими повинні керувати та контролювати кваліфіковані фахівці з безпеки, щоб переконатися, що всі вони працюють і налаштовані належним чином.

Далі розглянемо деякі організаційні аспекти безпеки, які потрібні на різних рівнях системи інформаційного захисту організації.

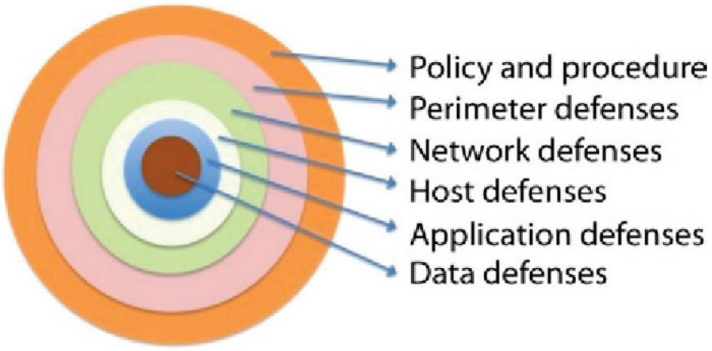

Рис. 1. Організаційна інфраструктура кібербезпеки [1]

Політика і процедури (Policy and Procedure)

Хоча це не зовсім відноситься до технічної сфери проте, політика та процедури мають значний вплив не тільки на те, як працює ваш SOC, але й на те, які функції він може виконувати. Коли у вас є веб-проксі, щоб захистити своїх користувачів від переходу на шкідливі веб-сайти, ваш SOC повинен переглядати ці події, щоб переконатися, що немає заражених систем із шкідливим програмним забезпеченням, яке надає доступ вашій системі до зловмисних веб-сайтів. Ваша організація може також мати політику щодо того, що можна завантажити або те, що працівник може переглядати на своєму комп’ютері. Якщо у вас є політика, згідно з якою ніхто не має права досліджувати певний контент під час роботи на робочому комп’ютері, працівник може нести відповідальність за такі дії, а завданням SOC є належним чином повідомити про це керівництво організації. Існує багато інших політик та процедур, які впливатимуть на роботу вашого SOC і тому формування переліку того, що може ваша організація, і що можна включити до SOC, як частину його відповідальності, має бути закладено у політиці безпеки організації. Політики та процедури стосуватимуться кожного аспекту не лише того, як функціонує SOC, але й того, як пристрої налаштовуються та розгортаються для захисту.

Захист периметра (Perimeter Defenses)

Як правило, у периметрі є кілька різних типів технологій, які використовує організація. Необхідно розуміти, що за периметром знаходиться зона, яка не підлягає контролю з боку організації і починається інший світ: постачальник послуг, діловий партнер або ненадійне з’єднання. Модель безпеки тут полягає у тому, щоб виявити та запобігти потраплянню у мережу організації усього того, що їй легально не призначено.

Перший тип пристроїв у цій області – брандмауер. Брандмауери життєво необхідні для SOC, оскільки вони контролюють те, що відбувається і що надходить у вашу мережу. Журнали з брандмауера потрібно збирати та аналізувати, саме там можна знайти проблеми з продуктивністю, пов'язані з атаками на відмову в обслуговуванні, спробами зловмисників порушити правила доступу або заборону доступу до пристроїв через багато інших причин. Журнали брандмауера потрібні щоб допомогти організації визначити справжню IP-адресу зовнішньої системи, яка здійснює доступ до вашої мережі. Коли ви перекладаєте реальні маршрутизовані адреси Інтернету на внутрішні адреси, що не входять до Інтернету, ви повинні мати спосіб пошуку відносин, щоб визначити, хто що робить. Без журналів брандмауера завдання SOC щодо виконання функцій захисту значно ускладнюється.

Важливим елементом також є VPN або системи віддаленого доступу, саме тут працівники організації підключатимуться із-за меж мережі для доступу до внутрішніх ресурсів. Життєво важливо підтримувати цю систему, щоб забезпечити належний доступ користувачам і щоб, коли люди залишають або більше не потребують доступу, його було анульовано або забрано. Отже, моніторинг користувачів, які отримують доступ до цього ресурсу, дуже важливий, але також важливим є фіксація того, хто і звідки отримує доступ до системи. Якщо ви бачите, що хтось входить у VPN з іншої частини світу, перебуваючи тим часом в офісі, то у вас можуть виникнути проблеми. Ваш SOC повинен мати можливість використовувати ці основні системи, щоб отримати цінну інформацію про те, які проблеми безпеки можуть впливати на периметр мережі ваших організацій і хто може отримувати несанкціонований доступ. Окрім розглянутого, звичайно, є багато інших пристроїв, таких як проксі-сервери, які є важливими для захисту периметру.

Захист мережі (Network Defenses)

Наступним кільцем оборонної стратегії організації є внутрішня мережа. Це елемент, який визначає взаємодію всередині мережі в одному або декількох різних сегментах інфраструктури. Елементи, що стосуються безпеки, які ви зазвичай знайдете тут, – це такі речі, як системи виявлення та запобігання вторгненню (IDS), системи контролю доступу до мережі (NAC), а також системи запобігання втраті даних та системи реєстрації поведінки користувачів або аномалій. IDS слід встановлювати скрізь, де є сегмент мережі, який може взаємодіяти з іншим сегментом мережі і трафік даних проходить між цими двома мережами або областями. Це дозволить побачити весь мережевий трафік, який успішно передається та оцінюється за підписами, внутрішніми до IDS, і визначається, чи було щось зловмисним чи ні. Тут можуть бути і атаки хакерів, які намагаються використати вразливі місця. Робота IDS життєво важлива для SOC для перегляду та оцінки, а також для управління та постійного оновлення системи за допомогою останніх підписів для виявлення зловмисного мережевого трафіку. Системи NAC також чудово допомагають запобігти підключенню до внутрішньої мережі систем, які не належать організації. SOC повинен уважно стежити за змінами в мережі та за тим, які пристрої підключені чи не підключені. Зловмиснику не потрібно знаходитись поза мережею в якомусь далекому місці; вони можуть знаходитися всередині організації, намагаючись отримати доступ до даних та ресурсів. Журнали попередження від таких типів систем є важливою інформацією, яку повинен збирати та аналізувати SOC, сюди також можна віднести системи, які намагаються підключитися до будь-яких безпроводових мереж або спробувати видати себе за реальну безпроводову мережу, в якій працює організація.

Захист хостів (Host Defenses)

В цілому захист хосту включає антивірус, засоби керування пристроями для USB або системи запобігання втраті даних хоста. Коли антивірусне програмне забезпечення виявляє присутність вірусу, здійснюється ціла низка дій, одна з яких це очищення вірусу. Але часто бувають виявлені віруси, які неможливо очистити. І тому важливо отримати повідомлення про цю ситуацію, яке надходить до SOC, щоб застосувати дії у ручному режимі і наслідки вірусу не викликали реальних проблем. Часто віруси призначені для викрадення даних або відкриття бекдорів, щоб зловмисникам було простіше отримати доступ до захищених мереж.

Коли дані передаються з вашої мережі, ви повинні оцінити їх, щоб переконатися, що це санкціоновано, і що їх надсилає автентифікована особа, яка має дозвіл на їх надсилання, і що вони надходять у відоме або надійне місце призначення. Системи запобігання втраті даних можуть працювати на рівні мережі та на рівні хоста; ці системи налаштовані з правилами для виявлення важливих даних, якими володіє організація, та забезпечення їх правильного переміщення по мережі. Правила, з якими працюють ці системи, повинні витримуватися, а попередження про порушення цих правил повинні переглядатися та діяти з боку SOC.

Захист додатків (Application Defenses)

Потрібно також захистити програми, які виконують критичні функції або зберігають важливі для вашої організації дані. Ці програми можуть застосовуватись практично в будь-якій точці мережі організації, від окремих хостів до основних серверів або мейнфреймових комп'ютерів. Це досить велика і широка сфера безпеки, оскільки існує багато різних міркувань щодо захисту різних програм, а також щодо того, як SOC взаємодіє з цими системами захисту. SOC, який виконує регулярне сканування вразливостей, повинен мати можливість виявляти момент, коли програма застаріла, застосовувати оновлення та передавати цю інформацію власнику програми. Віруси, коди оболонки та інша шкідлива логіка можуть скористатися перевагами ваших програм і змусити їх робити те, чого вони не мали б робити. Вміння виявляти, коли файли програм неадекватно модифікуються або коли користувач постійно намагається повторити свій пароль 1000 разів на секунду, – це все те, на що SOC потрібно звертати увагу.

Захист даних (Data Defenses)

Навіть маючи усі рівні захисту все зводиться до даних та ресурсів, що зберігають ці дані. Який вид захисту ви встановите для захисту своїх даних? Чи будете ви використовувати шифрування файлів і томів на своїх пристроях кінцевих точок, захищене сховище на своїх серверах, спеціальний груповий доступ чи навіть фізичний захист? Незалежно від того, як ви вирішили захистити свої дані, хтось повинен спостерігати і реагувати на попередження або змінювати правила системи за необхідності.

Типова інфраструктура SOC для організації наведена на рис. 2.

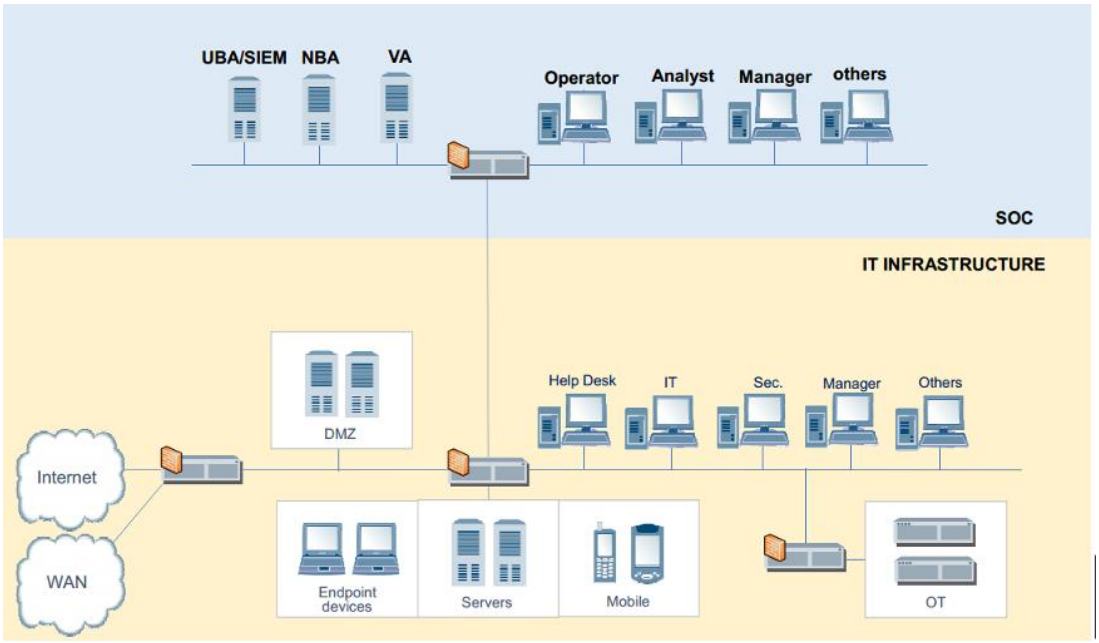

Рис. 2. Типова інфраструктура SOC організації [8].

Також варто зауважити, що в міру того, як організація нарощує кількість систем, серверів та мережевого обладнання можуть зростати і чисельність або різко збільшуватись

частота подій та інцидентів. Необхідно це враховувати та планувати зростання ресурсів в цих інструментах.

Висновки

Розгортання SOC - це ретельний баланс між тим, що організація вважає необхідним для зменшення ризиків, та загрозами, які SOC вважає нагальними для захисту організації. Кожен у SOC повинен пам’ятати, чому він тут, щоб захистити організацію та її користувачів найкращим чином, як вони знають, за допомогою найкращих інструментів та можливостей, якими вони можуть скористатися. Незалежно від того, на якому типі SOC чи на чому зосереджена ваша увага, переконайтеся, що ви виконуєте свої основні обов'язки та піклуєтеся не тільки про людей, яких ви захищаєте, але й про тих, хто захищає вас. SOC має значний перелік завдань для виконання, і це постійно зростаючий список. Переконайтеся, що ви правильно визначили цей перелік завдань, сформували всі деталізовані вимоги та отримали відповідні повноваження, щоб взяти на себе ці обов'язки. Ваш SOC повинен знати, хто такі клієнти і чому SOC тут виконує свою роботу. Як тільки ви втрачаєте з виду той факт, що організація сфери послуг повинна відповідати вимогам своїх клієнтів та користувачів, тоді SOC зазнає невдачі у виконанні своєї місії, незалежно від того, наскільки розумна вона чи наскільки технічно здатна захищатись від загроз.

Перелік посилань

1. CVSS Severity Distribution Over Time [Електронний ресурс] // National Vulnerability Database – Режим доступу до ресурсу: https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time (03.07.20).
2. Sarraute C. Penetration testing == POMDP solving? / C.Sarraute, O.Buffet, J.Hoffmann. // arXiv. – 2013. - arXiv:1306.4714.
3. Sarraute C. POMDPs make better hackers: Accounting for uncertainty in penetration testing. / C.Sarraute, O.Buffet, J.Hoffmann // In Proceedings of the 26th AAAI Conference on Artificial Intelligence «AAAI’12». Toronto, ON, Canada, July 2012. AAAI Press. - pp. 1816-1824.
4. Shmaryahu D. Partially observable contingent planning for penetration testing / D.Shmaryahu, G.Shani, J.Hoffmann // 2017 1st Int Workshop on Artificial Intelligence in Security. – 2017. – pp. 33-40.
5. Stefinko Ya. Theory of modern penetration testing expert system. / Ya.Ya.Stefinko, A.Z.Piskozub // Information Processing Systems, -2017. - Vol. 2(148), - pp. 129-133.
6. Durkota K. Computing optimal policies for attack graphs with action failures and costs. / K.Durkota, V.Lisy. // In 7th European Starting AI Researchers` Symposium «STAIRS’14». January 2014.
7. Zhou T. NIG-AP: a new method for automated penetration testing. / T.Zhou, Y.Zang, J.Zhu, et al. // Frontiers Inf Technol Electronic Eng 20, - 2019. – pp. 1277–1288.
8. Sutton R.S. Reinforcement Learning: An Introduction second edition. / R.S. Sutton, A.G. Barto // The MIT Press, Cambridge, MA, 2018. - 445 P.
9. McFarlane R. A survey of exploration strategies in reinforcement learning. [Електронний ресурс] / R. McFarlane // McGill University – Режим доступу до ресурсу: http://www.cs.mcgill.ca/~cs526/roger.pdf (03.07.20).

Надійшла: 12.07.2020 Рецензент: д.т.н., професор Вишнівський В.В.