Секция «Компьютерное право и информационная безопасность»

Сравнительный анализ SIEM систем

Наумик В.Ю.[1], *Третьяк М.А.*[2]

1 - Ростовский юридический институт (филиал) Российской правовой академии Министерства юстиции Российской Федерации, Юридический факультет, Ростов-на-Дону, Россия, *E-mail: veronikanaumik@mail.ru*; 2 - Донской государственный технический университет, Факультет информатики и вычислительной техники, Ростов-на-Дону, Россия, *E-mail: ale1431999@gmail.com*

Повсеместное внедрение цифровых решений в различные сферы жизни общества и производства вызвало стремительное развитие информационных технологий, что упростило выполнения рутинных задач, позволив делегировать большинство простых заданий компьютерным системам предприятий, тем самым предоставив возможность сконцентрироваться на выполнении задач компаний, имеющих больший приоритет. Это повлияло на увеличение производительности и увеличило доходы компаний, повысив их ценность для общества и значимость на рынке. Такое положение приводит к тому, что компания становится потенциальной целью для злоумышленников, хакерских группировок и даже государств.

В данной статье проведен обзор и сравнительный анализ SIEM (Security Information and Event Management) систем ArcSight, MaxPatrol SIEM от Positive Technologies, FORTISIEM и RuSIEM. Были изучены особенности работы с ними, методы детектирования угроз, инструменты создания правил корреляции и основной функционал, который понадобится специалисту информационной безопасности для обнаружения вредоносной активности внутри корпоративной сети предприятия. Также мы изучаем требования законодательства к SIEM системам организаций. Задача SIEM систем - упрощение работы специалиста информационной безопасности с журналами аудита, их сбора и анализа событий. SIEM системы являются очень гибкими инструментами в проведении расследований инцидентов информационной безопасности, составлении отчетов и их обработки. Ввиду того, что с каждым днем появляются новые сетевые угрозы, разрабатывается новое вредоносное программное обеспечение, способные нанести существенный ущерб корпоративной сети предприятия, необходимо так же быстро изучать и внедрять более современные и гибкие в настройке и легкие в эксплуатации средства защиты информации. К таким средствам относятся SIEM системы, позволяющие облегчить работу специалиста информационной безопасности, сделав проведение анализа событий еще более быстрым, удобным и надежным, чем использование иных решений.

В средствах массовой информации чаще стали появляться публикации о выкупах персональных данных, похищенных с серверов компаний-жертв, программами вымогателями на крупные суммы долларов. Одним из таких вымогательств, попавших в центр внимания общественности, стал скандал, связанный с атакой на компанию Travelex. Данные этой организации были зашифрованы, а резервные копии данных стерты на ее серверах, и предварительно похищены программой-вымогателем Sodinokibi[5] с требованием выкупа 6.000.000 долларов США, в результате чего компания оказалась на грани банкротства из-за падения акций. Данная атака стала одной из самых резонансных атак связанных с REvil[3] в 2019 году.

Риск компрометация корпоративной сети компании ведет к снижению ее стоимости и надежности. Теряя контроль над критическими данными, компания рискует лишиться

как своего инвестора, так и потребителя. С увеличением объемов организации, возрастает сложность мониторинга активности устройств в ее сети. Для своевременного реагирования на инциденты информационной безопасности сети, возникает необходимость использования инструментов, предоставляющих подробный отчет специалистам, занимающимся вопросом обеспечения конфиденциальности, целостности и доступности данных, о каждом возникшем событии. Таким инструментом является SIEM (Security information and event management) система, предоставляющая возможность поддерживать мониторинг корпоративной сети компании и безотлагательно реагировать на инциденты информационной безопасности.

Системы управления информацией о безопасности и событиями информационной безопасности позволяют решать задачу манипулирования информацией о безопасности потока событий и производить их оценку, выполнять упреждающие действия в случае возникновения инцидента в реальном потоке времени. SIEM система представляет собой комплекс приборов, устройств, программного обеспечения, мер и политик по обеспечению информационной безопасности предприятия обеспечивающие аудит деятельности осуществляющейся в информационной сети защищаемого предприятия.

Осуществление контроля за безопасностью сегментов сети компании обусловлена, как возникновением внешних, так и внутренних угроз, наносящих вред компании. Понимание деструктивного воздействия той или иной кибератаки можно условно охарактеризовать гексадой Паркера, в которой обеспечение защиты информации сводится к соблюдению всех аспектов информационной безопасности, представленных в ней. То есть одновременное соблюдение всех столпов модели обеспечивает надежность компьютерной системы. Мониторинг крупной компании становится трудновыполним без применения современных методов сбора и централизованного анализа журналов аудита доверенных устройств сети.
Для защиты и укрепления финансового рынка РФ был создан ГОСТ Р 57580.1-2017[1]. Данный стандарт устанавливает несколько уровней (минимальный, стандартный и усиленный) защиты информации для компаний, а также требования к каждому уровню. Большинству организаций требуется стандартный уровень защиты, лишь для системно-значимых финансовых компаний требуется усиленная защита информации. Следует отметить, что иные Положения ЦБ РФ не отменяют ГОСТ, а дополняют, например Положение Банка России от 04.06.2020 N 719-П, которое действует с 1 января 2022 года и вводит требования к обеспечению защиты информации ряда финансовых операций[4]. Оно отменяет Положение ЦБ N 382-П.

Способов преодолеть цифровую защиту компаний бессчетное множество и компрометация информационных систем не редкость. Так наиболее уязвимыми являются веб-приложения находящиеся на внешнем периметре сети. Одна только некорректная настройка составляет 81% всех зафиксированных угроз компаний за 2020 год в России. Следом идут отсутствие компетенций в области информационной безопасности среди сотрудников компаний и слабая организация политик управления паролями внутри сети, по данным из отчета компании Rostelecom-Solar JSOC, приходящихся на июнь 2020 - июнь 2021[2].

Таким образом, компании все чаще становятся жертвами хакерских группировок, и необходимо разработать механизмы эффективного противодействия угрозам безопасности.

Источники и литература

1) ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер" (утв. и введен в действие Приказом Росстандарта от 08.08.2017 N 822-ст).
2) Итоги анализа защищенности российских компаний. Date Views 02.02.2022 rt-solar.ru/upload/iblock/a75/Otchet-Solar-JSOC-Itogi-analiza-zashchishchennosti-rossiyskikh-kompaniy-_-web.pdf.
3) Компании-жертвы не заплатили хакерам из REvil 70 миллионов долларов выкупа. Date Views 16.12.2021 d-russia.ru/kompanii-zhertvy-ne-zaplatili-hakeram-iz-revil-70-millionov-dollarov-vykupa.html.
4) Положение Банка России от 04.06.2020 N 719-П "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств"
5) Sodinokibi Ransomware: Following the Affiliate Money Trail. Date Views 12.12.2021 www.bleepingcomputer.com/news/security/sodinokibi-ransomware-following-the-affiliate-money-trail/.