НИКОЛАЙ СМИРНОВ

Ядро безопасности

Разнородные средства защиты информации зачастую плохо взаимодействуют друг с другом, рассыпаясь на отдельные независимые подсистемы. Очевидно, что для обеспечения адекватного уровня безопасности они должны взаимодействовать друг с другом и управляться из единого центра. Ядром такой системы становятся решения по управлению событиями информационной безопасности (Security Information and Event Management, SIEM).

Ландшафт ИТ-систем, используемых компаниями, постепенно усложняется, и сфера безопасности здесь не исключение. Средства защиты постоянно развиваются, количество источников информации растет, и в результате мониторинг событий безопасности становится нетривиальной задачей. Если своевременно не реагировать на возникающие угрозы и не предотвращать их, то даже самые продвинутые системы безопасности будут неэффективными.

Основные задачи решений, относящихся к классу SIEM, — консолидация и хранение журналов событий из различных источников, определение взаимосвязи событий и их обработка по заданным правилам, предоставление инструментов для анализа и разбора инцидентов. Не менее важно автоматическое оповещение администраторов о нештатных ситуациях, ведь миссия таких систем заключается именно в автоматизации процесса обнаружения инцидентов. Таким образом, события должны не только собираться в неком хранилище для последующего разбора инцидентов, но и обрабатываться. В противном случае функционал решения будет урезан, что радикально снизит его ценность для бизнеса.

На рынке SIEM представлено несколько крупных игроков, в том числе IBM Tivoli, Symantec, McAfee, HP ArcSight. Из отечественных решений можно назвать КУБ компании «Код Безопасности» и SafeWork, разработанное ICL КПО-ВС.

«Безусловно, цель каждой компании — добиться целостной картины защищенности и прозрачности механизмов управления возникающими инцидентами. Однако далеко не всем компаниям удается реализовать централизованный подход», — отмечает Владимир Дрюков, эксперт направления Security Outsourcing компании «Инфосистемы Джет». Можно выделить две основные причины этого. Во-первых, высокая стартовая стоимость построения центрального узла информационной безопасности, которым чаще всего является SIEM-решение. Во-вторых, высокая трудоемкость построения самого процесса управления инцидентами, требующая как прямых вложений, так и косвенных затрат. Эти факторы существенно сокращают список компаний, которые могут позволить себе реализацию данного подхода.

Чаще можно наблюдать лоскутную картину защищенности: существуют централизованный анализ и управление всеми сетевыми инцидентами, присутствует DLP-система, контролирующая все утечки конфиденциальной информации, а также ряд разрозненных узкоспециализированных систем. В такой ситуации возможности компании по анализу событий и выявлению инцидентов сильно ограниченны, поскольку даже самое лучшее средство защиты решает свою конкретную задачу и не имеет представления о том, что происходит в инфраструктуре в целом.

В качестве примера можно использовать сценарий утечки информации после успешного подбора пароля. В этом случае инцидент, как правило, распадается на набор событий в разных источниках инфраструктуры: успешная авторизация пользователя в системе после нескольких неудачных попыток, получение доступа к критичным данным в рамках этой же сессии, попытка передачи данной информации за пределы защищенного периметра.

Каждое из описанных событий достаточно легко выявляется с помощью базовых средств защиты, но их разнородность не позволяет отследить их все. При попытке выявления описанного сценария администратор неизбежно сталкивается со следующей проблемой: ни одно из этих событий само по себе не является инцидентом и может вполне легитимно возникать по нескольку раз в день. Это порождает большой объем ручной или полуавтоматизированной работы, которая «замыливает глаза» администратору. В итоге реально возникший инцидент может быть не замечен или обнаружен несвоевременно.

SMB ЖДЕТ ПРЕДЛОЖЕНИЙ

«Многие компании по сей день вполне довольны существующим набором продуктов различных производителей, однако тенденция к централизованному подходу все же налицо», — говорит Денис Гасилин, руководитель отдела маркетинга SafenSoft. Уж слишком дорого стало покупать разношерстную линейку решений, каждое из которых само по себе стоит недешево, да еще и требует правильной интеграции с другими частями системы информационной безопасности.

Естественно, в первую очередь речь идет о крупных корпорациях. Большие компании — большие возможности, но и уровень возможных потерь — информационных, финансовых, репутационных — у них несоизмеримо выше. Именно крупные компании имеют наиболее разветвленную инфраструктуру и остро нуждаются в том, чтобы защищать ее, централизованно управляя системой собственной информационной безопасности.

К унификации системы информационной безопасности стремится и сегмент среднего бизнеса. Переносные носители, документация, переписка — все это важно и ценно, но явно не совсем хорошо в данный момент защищено. К тому же средний бизнес практически всегда работает с большим, а у последнего, в особенности в финансовом или государственном секторе, есть обязательные требования к уровню защиты бизнес-процессов.

Сегмент же малого бизнеса пока остается при своем мнении, удовлетворяясь простыми антивирусами. Возможно, часть проблемы заключается в том, что на рынке очень мало решений для SMB, которые обеспечивали бы полноценную защиту по адекватной для данного сегмента цене. У любого вендора, сделавшего оптимальный продукт за вменяемую стоимость и верно преподнесшего его целевой аудитории, есть все шансы на успех.

Наконец, негативную роль играет и практика замалчивания инцидентов. Компании, подвергшиеся атакам, стараются не афишировать подобные проблемы, тем самым создавая иллюзию безопасности.

ПРОТИВОПОЛОЖНЫЕ ПОДХОДЫ

«Переход от базового обеспечения безопасности к централизованной системе управления инцидентами правильнее всего начинать с "фундамента". Поэтому первым шагом должна стать разработка процесса управления информационной безопасностью и ее угрозами, а также решение сопряженных с ней кадровых вопросов», — рекомендует Дрюков.

Что касается сугубо технической стороны вопроса, то существует два принципиально разных подхода. В некоторых компаниях SIEM является первым элементом построения центра оперативного управления информационной безопасностью (Security Operations Center, SOC). При этом построение SIEM позволяет существенно упростить выявление инцидентов даже в рамках базовых средств обеспечения безопасности и инфраструктурных систем. Впоследствии в ходе развития в состав комплекса включаются другие профильные решения. В некоторых компаниях наблюдается противоположная картина: построение SOC начинается с одного из профильных решений, чаще всего — с DLP. В дальнейшем SIEM входит в состав уже существующего решения как узел централизованного управления и обработки событий

Каждый из этих подходов имеет свои плюсы и минусы. Выбор осуществляется, как правило, исходя из конкретной истории инцидентов компании. Если высокую критичность имеет задача контроля утечек, то построение обычно начинается с DLP.

Однако важно понимать, что безопасность не может быть лоскутной — либо компания защищена, либо нет. С помощью SIEM можно добиться почти полной автоматизации процесса выявления угроз, выводя на новый уровень предоставление сервисов со стороны службы безопасности.

Наконец, логическим завершением должно стать построение процессов расследования инцидентов. Это важнейшая часть системы, о которой очень часто просто забывают. Если инцидент произошел, должен быть инструмент, который позволит этот инцидент расследовать. CIO.RU

Гарант соответствия

Особое значение решения SIEM приобретают для финансовых организаций, вынужденных соответствовать массе регуляторных требований по безопасности. Например, ФЗ-161 «О национальной платежной системе» требует от банков соблюдения жестких сроков по расследованию случаев мошенничества. Выполнить требования возможно только за счет автоматизации управления событиями безопасности. Несмотря на годичную отсрочку вступления закона в силу, банки вынуждены реализовывать такие проекты. Банк «Петрокоммерц» завершил внедрение системы мониторинга корпоративных угроз и рисков безопасности на базе платформы ArcSight ESM. В рамках проекта специалистами Softline было обеспечено соответствие информационной системы требованиям регулирующих органов и международного стандарта PCI DSS. «Мы несем большую ответственность перед нашими клиентами и поэтому должны внимательно отслеживать уровень защищенности нашей системы», — подчеркивает Сергей Кулешов, заместитель начальника управления информационной безопасности банка «Петрокоммерц». Эффективное выстраивание системы безопасности информационных ресурсов банка в соответствии с требованиями международных стандартов в сфере безопасности является важнейшей задачей. Для учреждений такого масштаба защита информационной системы становится одной из ключевых задач обеспечения безопасности бизнеса. В целом можно отметить, что в российских кредитно-финансовых организациях подход к ее решению становится все более системным. Это вызвано как появлением новых программных продуктов и зрелостью компаний, так и ужесточением принятых стандартов безопасности. Решение ArcSight ESM изначально адаптировано под требования банковских стандартов, что существенно снизило риски проекта. В ходе реализации проекта была выполнена настройка специализированных модулей и правил корреляции событий. Любопытно, что системы SIEM могут использоваться банками не только по прямому назначению, но и в качестве средств выявления и предотвращения мошеннических транзакций. Они позволяют осуществить гибкую настройку реакции на события и поэтому обладают практически одинаковыми возможностями по расследованию фактов мошенничества со специализированными решениями класса Anti-Fraud. Более того, работая в реальном времени, они не только выявляют уже совершившиеся операции, но и реагируют на потенциальные риски.