Наталья Зосимовская, Ведущий специалист департамента маркетинга компании «Информзащита»

Аутсорсинг ИБ или корпоративный центр мониторинга и управления инцидентами (SOC)?

С каждым годом инфраструктура безопасности компаний с растущим бизнесом становится все более сложной. С одной стороны, это позволяет обеспечить необходимый уровень информационной безопасности, автоматизировать критически важные бизнес-процессы, выполнить требования регуляторов, но с другой стороны приводит и к ряду проблем. Во-первых, использование широкого спектра различных технологий безопасности приводит к необходимости осуществлять управление большим количеством различных устройств. Для осуществления этих работ требуется штат специалистов. При остром дефиците квалифицированных кадров решение подобной задачи сильно осложняется и приводит к тому, что имеющихся специалистов нагружают все большим и большим количеством обязанностей и задач. Но надо понимать, что возможности даже суперспециалиста не безграничны и заниматься всеми задачами одновременно с одинаковой эффективностью просто невозможно. В итоге сотрудники выстраивают приоритеты по задачам, часть которых уходит на второй и третий план, что естественно увеличивает риски внутренних и внешних угроз и может привести к серьезным инцидентам.

Если говорить об инцидентах безопасности, то работа с ними требует определенных инструментов и специфических навыков и знаний. Так для получения общей картины происходящего в сети, выявления инцидентов безопасности, централизованного хранения собранных событий и последующего их анализа требуется система сбора, обработки и хранения событий. Помимо этого должны существовать и выполняться стандарты и руководящие процедуры, а также регламентированные правила выявления, реагирования и расследования инцидентов. Зачастую подобные инструменты и процедуры в организация отсутствую или существуют и выполняются в недостаточной мере, что значительно повышает «время реакции» и снижает своевременность, и адекватность принимаемых мер.

Решить вышеперечисленные проблемы можно несколькими способами. При этом стоит отметить, что каждый из этих способов требует порой серьезных инвестиций. Можно попытаться набрать необходимое количество специалистов, обучить их и продолжать работу уже не в авральном режиме, распределив выполнение необходимых задач между всей командой. Но как говорилось выше, сейчас наблюдается острый дефицит квалифицированных кадров на рынке специалистов по ИБ, поэтому процесс набора персонала, а также его обучения может затянуться во времени, а задачи решать нужно сейчас.

Следующий вариант это передача части функций по мониторингу и управлению средствами защиты на аутсорсинг. На сегодняшний день компания «Информзащита» является единственной российской компанией создавшей полноценный Security Operations Center, позволяющий в круглосуточном режиме осуществлять удаленный мониторинг, а при необходимости и управление средствами защиты клиента. Центр работает с широкой номенклатурой оборудования известных вендоров, таких как Check Point, Cisco, IBM ISS и др. В ближайшей перспективе Центр планирует брать на аутсорсинг и продукты собственного производства «Информзащиты». Подобная организация круглосуточного мониторинга позволит компании переложить наиболее рутинные и трудоемкие задачи на аналитиков и инженеров SOC компании «Информзащита», что в свою очередь высвободит временные и человеческие ресурсы служб ИБ и ИТ для решения задач, стратегически более важных для бизнеса компании. Кроме того, удаленный мониторинг событий информационной безопасности, оперативные оповещения о выявленных инцидентах информационной безопасности и выдача рекомендаций по их устранению позволит значительно повысить уровень защиты сети компании, т.к. данные услуги будут осуществляться в круглосуточном режиме высококвалифицированными аналитиками SOC и с гарантированным временем реакции на события безопасности.

Если по определенным причинам компания не готова передать на аутсорсинг свои средства защиты, но потребность осуществлять мониторинг и управление инцидентами является актуальной задачей, то возможным вариантом решения может стать создание своего собственного центра мониторинга и управления инцидентами. Подобный центр позволит обеспечить централизованный контроль уровня информационной безопасности компании, а также осуществлять своевременную реакцию на инциденты, хранить собранные с различных источников события, создавать комплексные отчеты об угрозах, инцидентах, уровне безопасности компании для различных групп пользователей.

В заключение хотелось бы сказать, что принимать решение, создавать ли собственный центр управления ИБ или передавать на аутсорсинг мониторинг и управление средствами защиты — это выбор каждой компании, на который влияет бюджет, целесообразность и здравый смысл. В принципе принятие решения о покупке системы мониторинга и корреляции или же возложении данных функций на чужие плечи зависит от следующих критериев: размера компании, задач, которые она хочет решить, наличия финансовых и человеческих ресурсов, осознания необходимости использовать продукты и услуги такого класса, обязательности требований регуляторов и так далее.

Вполне естественно, что небольшой компании, с ограниченным набором сетевых устройств, не имеет смысла разворачивать у себя полнофункциональную систему мониторинга и управления инцидентами, т.к. во-первых, это дорого, а, во-вторых, нужны люди, которые будут ею заниматься, которых, к слову, еще надо обучить работе с подобной системой. Гораздо более логично передать на аутсорсинг мониторинг и управление средствами защиты и приобрести высокоуровневый сервис от профессионалов. При этом еще и высвободить временные и человеческие ресурсы для решения более важных для бизнеса задач.

С крупными компаниями ситуация сложнее. Их бизнес напрямую зависит от стабильности существующих бизнес-процессов. И порой незнание того, что происходит в сети, а также несвоевременная реакция на ту или иную угрозу может в результате очень негативно отразиться на деятельности компании и ее репутации. Поэтому создание центра управления безопасностью, осуществляющего сбор, мониторинг, анализ и работу с инцидентами безопасности, будет очень серьезным подспорьем в организации устойчивости бизнеса в целом.