IQ центров управления инцидентами растет

В прошлом месяце эксперты Федеральной службы безопасности внесли несколько поправок в законопроект «О безопасности критической информационной инфраструктуры РФ». В связи с этим некоторые изменения можно будет увидеть в Уголовном кодексе. Причем помимо наказания самих хакеров законопроект предусматривает, что вину могут понести системные администраторы и руководство пострадавших организаций, поскольку будет считаться, что они не защитили системы должным образом и открыли доступ к конфиденциальным данным. Предусмотрен и срок лишения свободы за подобную халатность – до семи лет, что является достаточно суровой мерой по критериям российского законодательства.
Заставит ли это бизнес задуматься об управлении инцидентами на предприятиях?
Об этом и других вопросах мы решили поговорить с Дмитрием Моисеевым, руководителем практики SOC, «Астерос Информационная безопасность».

– Считаете ли вы, что проявление более жесткой позиции со стороны регуляторов «образумит» российских заказчиков и станет стимулом для более внимательного отношения к управлению инцидентами в сфере информационной безопасности?

– Требования законодательства всегда были и остаются драйвером развития для рынка информационной безопасности. Однако в корпоративном секторе мерилом инвестиций в то или иное направление ИБ является степень влияния соответствующих угроз на критичные бизнес-процессы. Поясню.

Как правило, к основным драйверам для внедрения системы управления инцидентами относятся повышение стабильности деятельности компаний и снижение ущерба от инцидентов ИБ за счет их оперативного выявления и сокращения времени реагирования на них. Возникающие инциденты приводят к нарушениям непрерывности бизнес-процессов компании, финансовым и репутационным потерям. Как показывает статистика, наибольший ущерб приносят именно сложные направленные атаки (targeted attacks), включающие разнообразные инструменты – от социальной инженерии до фрода. Приведу пример. Представьте себе банк. Оператор имеет право доступа к клиентским данным только при звонке клиента и по его просьбе проверить какую-либо информацию. Все звонки записываются. Допустим, администратор видит, что оператор обратился к тем или иным клиентским данным. Для него это действие законно. Но если предположить, что никакого звонка от клиента не поступало, то это уже повод для более детального исследования ситуации. Стандартными и разрозненными средствами защиты такие инциденты выявить очень сложно.

– Еще несколько лет назад крупный бизнес инвестировал в ИБ по прецедентному принципу. Сегодня фактически все компании так или иначе обзавелись антивирусными решениями, системами защиты доступа, сканерами уязвимостей и т. д. Однако утечки данных, факты НСД и другие инциденты, связанные с информационной безопасностью, по-прежнему происходят. В чем вы видите причину?

– Причина большинства инцидентов в области ИБ – человеческий фактор. Умышленно или случайно, по предварительному сговору либо по каким-то иным соображениям человек совершает действия, которые могут представлять угрозу деятельности компании. По сути, фактически все средства защиты направлены на минимизацию рисков ИБ. Следуя этим путем, со временем большинство компаний стали «счастливыми обладателями» арсенала разрозненных решений ИБ, зачастую не интегрированных или слабо интегрированных между собой. Объединить эти решения с учетом логики каждой, провести корреляцию событий ИБ, фиксируемых в прикладных системах, связать между собой и отследить потенциально опасные аномалии – вот ключевая задача SIEM-решений (Security Information and Event Management), на базе которых строится SOC.

Важно отметить, что при правильном подходе к развертыванию SOC компания прежде всего должна четко выстроить процесс управления инцидентами ИБ, что значительно повысит эффективность существующих решений и технологий. А это – минимизация ущерба от инцидентов, реальный контроль над информационными рубежами компании и повышение стабильности и управляемости компании.

– На ваш взгляд, каков сегодня процент компаний, которые осознают необходимость внедрения SOC?

– Действительно зрелых компаний с точки зрения готовности

к инвестированию в инфраструктуру SOC немного. Это в первую очередь лидеры автоматизации – банки, телекоммуникационные холдинги, транспортная отрасль.

Заметьте, дело не в покупке оборудования или программного обеспечения: при наличии грамотных специалистов вы можете развернуть свой центр управления инцидентами и на СПО.

Говоря о зрелости компаний, я прежде всего имею в виду готовность менеджмента перестроить или создать с нуля процессную составляющую функционирования SOC, что в ряде случаев связано не только с внедрением и описанием новых бизнес-процессов, реализацией политик и регламентов, но и с «перекраиванием» штатного расписания, набором сотрудников, которые круглосуточно будут осуществлять мониторинг всей информационной инфраструктуры.

Здесь большое значение имеют опыт компании-партнера, ее экспертиза в области классификации возможных событий, исключение из перечня событий, на которые реагировать не нужно. Кроме того, очень важно типизировать инциденты, ранжировать их по степени критичности, описать все эти процессы и роли.

Опытные интеграторы, как правило, предоставляют услуги обучения персонала навыкам распознавания тех или иных аномалий и соответствующим действиям для предотвращения каждой из угроз. Не менее сложен этап при функционировании SOC – постоянная адаптация его процессов и технологий к новым и изменяющимся угрозам ИБ.

– В период рецессии компании интересует вопрос оптимизации и сокращения затрат. Каким образом SIEM может повлиять на минимизацию издержек?

– Помимо минимизации прямого ущерба, который может понести компания в случае невыявления инцидента в силу отсутствия корреляции, внедрение SOC позволяет снизить операционные расходы на процессы управления инцидентами ИБ, в том числе за счет автоматизации самих процессов. Это достигается путем уменьшения доли ручного труда при обработке событий ИБ, даже при увеличении количества используемых средств защиты. Кроме того, SOC дает возможность поддерживать процесс непрерывного совершенствования мер обеспечения безопасности, выявляя слабые места в защите.

Еще один вариант экономного подхода к организации SOC – передача управления системами ИБ на аутсорсинг. Таким образом компания экономит на содержании дополнительного штата высококвалифицированного персонала, высвобождает рабочее время собственных специалистов и получает качество услуги, гарантированной SLA.

> Любой SOC является сложным конструктором, все элементы которого функционируют по правилам, выработанным индивидуально для каждой корпоративной структуры.

– С чем связаны типичные сложности при развертывании SOC?

– Каждый проект по внедрению центра управления инцидентами имеет свои сложности. Многие компании, полагающие, что у них развернут SOC, на деле внедрили некий комплекс средств отслеживания инцидентов ИБ со стандартными правилами корреляции, не адаптировав их к своим уникальным бизнес-процессам и ИТ-инфраструктуре с учетом отраслевой специфики. Использовать SOC исключительно для сбора, хранения и анализа логов – то же самое, что палить из пушки по воробьям. Такое внедрение не приносит пользы. Именно интегратор SOC добавляет ту ценность, которая востребована конкретным бизнесом и соответствует его потребностям, целям и задачам. Любой SOC является сложным конструктором, все элементы которого функционируют по правилам, выработанным индивидуально для каждой корпоративной структуры. Двух одинаковых центров управления инцидентами не бывает.

Типичные сложности, как уже было отмечено, заключаются в неготовности компаний перестраивать систему управления безопасностью под новую технологическую платформу, в значительной мере зависимую от человеческого ресурса.

– Каковы, на ваш взгляд, основные пути развития рынка SIEM в России?

– Технологически рынок SIEM развивается в тренде наращивания производительности. Объемы данных в прикладных системах, подключаемых к центру управления инцидентами, постоянно увеличиваются, что повышает требования к мощности.

Второй тенденцией, которую мы наблюдаем, является наращивание интеллектуальной составляющей SIEM, что особенно важно на этапе распознавания аномалии. IQ центров управления инцидентами растет, в том числе за счет применения эвристических алгоритмов, использующих сложные корреляции событий для поиска потенциально опасных цепочек.

Фокус рынка SOC постепенно смещается в сторону многомерной обработки не только структурированных «больших данных» (BIG DATA), но и неструктурированных, что, с одной стороны, намного сложнее для анализа, с другой – позволяет реализовать полностью контролируемый безопасный периметр.

Еще один важный тренд для современных решений SOC мировых поставщиков – усовершенствование интерфейса. Идя в ногу друг с другом в технологическом отношении, лидеры рынка зачастую соревнуются именно в качестве представления статистической, аналитической и оперативной информации, способностях системы за считаные секунды выводить на экран рабочей консоли инфографику, диаграммы, таблицы. Это позволяет использовать результаты работы SOC не только операторам центра и техническим специалистам, но и менеджменту. ■