Кибергигиена — залог здоровья

Центр кибербезопасности компании «Октава Кіберзахист» официально открылся чуть менее полутора лет назад. «СиБ» расспросил ее директора Александра Волощука о том, что изменилось за это время, что интересует заказчиков и каких угроз нам ждать в ближайшем будущем.

Александр ВОЛОЩУК,
CEO «Октава Кіберзахист»

— Как устроен ваш SOC и сколько в нем сотрудников?

— В SOC компании «Октава Кіберзахист» посменно работают 11 технических специалистов, это три линии поддержки. Первая линия сейчас работает не круглосуточно. Но это пока, потому что все услуги будут формироваться под конкретные запросы клиентов.

Рынок путает SOC и SIEM. Но если вы установили SIEM и фиксируете в день 600 событий, из которых отрабатываете 3–4, это сомнительный результат. Люди и процессы так же важны, как и технологии. Например, когда у коммерческого SOC нет операционного директора, то центр таковым может и не являться, потому что процессная составляющая — четкие SLA, отработка, накопление, база знаний — все это является неотъемлемой частью SOC, который работает на рынке, а не обслуживает одного клиента.

Сказывается и большой дефицит специалистов для SOC, об аналитиках нечего и говорить — готовых очень тяжело найти, они в основном уже заняты и никуда уходить не собираются. Мы выращиваем специалистов внутри компании, начиная с первой линии.

— Какие технические решения используются в вашем SOC?

— Лидирующим производителем остается Cisco. При этом за полтора года наполнение SOC достаточно сильно изменилось. В нашей лаборатории — фактически ее можно назвать модным словом «киберполигон» — разворачивались и Splunk, и ArcSight, и ряд других решений. Одних SIEM наши специалисты протестировали 5 или 6. Из современных технологий внимательно смотрим в сторону Threat Intelligence. Сейчас мы пытаемся создать набор инструментов, который позволит автоматизировать работу персонала, уменьшить время реагирования и повысить качество отработки, избавиться от «белого шума», чтобы выделять инциденты из потока событий. Для этого есть целый набор утилит, в том числе и решений с открытым исходным кодом, поскольку не всегда коммерческие оправдывают свою стоимость.

Всевозможные отладчики, анализаторы, системные мониторы — инструментов используются десятки. Одни более активно, другие менее, но каждый служит своей цели. Отсюда и вырастают требования к специалистам-аналитикам: сфера знаний очень широкая и непростая. Они работают с инструментами, по уровню компетенций недоступными даже операторам второй линии поддержки. Разработчика или администратора найти гораздо проще.

— Что включают в себя услуги, есть ли какой-то базовый пакет?

— Наиболее распространенная услуга — это аудит и мониторинг существующих средств, которые есть у заказчика. В большинстве своем, надо отдать должное, они все-таки имеются. Если брать периметральную защиту и антивирус, то в среднем операторы фиксируют в день до сотни событий. Естественно, инцидентами становятся единицы. При необходимости мы можем не только проводить аудит, но и и разворачивать продвинутые инструменты информационной безопасности. Конечно, есть развитие и в других направлениях, но рынок диктует свои предпочтения, поэтому мониторинг — самая классическая, экономически выгодная и массовая услуга.

— А услугу блокирования — Response — предлагаете?

— С Response дело обстоит достаточно сложно. За время нашей работы выяснилось, что заказчики пока не готовы к этому уровню услуг. Единичные случаи есть, но как массовый сервис в Украине реагирование пока не пользуется спросом. Хотя есть причины считать, что в ближайшее время ситуация изменится.

— Есть ли клиенты, которые выбирают только аудит?

— Есть определенный процент заказчиков, которым после аудита выдаются рекомендации по модернизации их информационной системы. Она может состоять из компонентов, к которым мониторинг применять не стоит. Мы просчитываем и формируем для заказчиков оценочные бюджеты, чтобы создать систему, которую вообще есть смысл мониторить. Когда аудит проведен и рекомендации выполнены, то большинство компаний доходят до подключения к SOC. Некоторые не готовы вкладывать

в кибербезопасность даже после прохождения аудита. Возможно, он им нужен просто для оправдания бюджета.

Тем не менее грамотность бизнеса растет, это видно по количеству (пускай пока не качеству) конференций, в названиях которых есть слово «кибербезопасность». В результате интерактивного опроса, который проводился на одной из них, угрозой номер один был назван риск хищения конфиденциальных данных. Мы тоже по мере сил пытаемся доносить необходимость, если использовать модный термин, повышения «кибергигиены».

— Встречаются ли клиенты, у которых вообще никак не выстроена информационная безопасность и они всецело полагаются на вас?

— Наши основные заказчики — это компании сегмента СМБ. В этом сегменте только формируется понимание, что себя нужно защищать. Хорошо, если клиент пришел сам — значит он, по крайней мере, представляет, что такое кибербезопасность. Обычно приходят, когда уже что-то случилось. Ведь вымогатели продолжают шествовать по компаниям, хотя уже все как будто обожглись. До сих пор у некоторых организаций не приняты даже базовые меры. Впрочем, у большинства компаний есть базовый антивирус и какая-то периметральная защита. Вопрос в том, как этим всем управляют.

— На открытии SOC летом прошлого года говорилось, что вы можете предоставлять в аренду межсетевые экраны Cisco. Есть ли сейчас такая практика?

— Есть, но не массово. Тогда предполагалось, что эта модель будет популярной, но оказалось, что бизнес предпочитает иметь что-то свое. За предоставление именно системы кибербезопасности и продвинутых решений они готовы платить по модели подписки (Managed Service). Если же нужно строить или модернизировать систему, бизнес вкладываетсяв покупку, а не в аренду.

— Есть ли какая-то тарифная сетка для ваших услуг?

—У нас сейчас не используются понятия «пакет», «базовая стоимость». Фактически мы прорабатываем конкретно с каждым заказчиком ценовое предложение: количество устройств, их типы, какие риски выделены, какие активы нужно мониторить. Со временем, когда появится массовая культура киберзащиты бизнеса и собственники поймут, что системно платить за нее дешевле, чем потом бороться с последствиями атак, появится и тарифная сетка. А пока – формируем цену под запросы каждого клиента.

— Что в себя включает SLA?

— Оно стандартно для всех организаций, которые предоставляют услуги. В нем прописано время реагирования, четко распределено категорирование инцидентов. SLA адаптируется под каждого заказчика, потому что отличаются защищаемые ресурсы: например, для интернет-магазина веб-сайт — основная ценность, для кого-то другого — лишь визитная карточка. Объединяет их четкое структурирование того, как быстро и кого мы должны информировать.

— Кто ваши заказчики? Какого рода эти компании, каков их средний размер?

— Подключаться к SOC есть смысл, когда рабочих мест 30 и больше, их может быть и 10, но очень критичных. По сферам деятельности разброс очень большой, ведь каждая компания использует информационные технологии и поэтому может стать клиентом. Почему мы выбрали сегмент СМБ? Крупные корпорации способны заплатить за создание собственного SOC, и им аутсорсинг не очень нужен. Ранее, лет пять назад, считалось, что средний и малый бизнес не так интересен злоумышленникам. Сейчас вектор смещается, и более половины атак направлены на СМБ. Часто этот бизнес интересен не сам по себе, а как подрядчик крупных корпораций, его могут использовать в качестве плацдарма для атак на них. К тому же у СМБ часто нет выделенного специалиста по ИБ, они тратят меньше на безопасность, и их можно назвать легкой мишенью. Это гораздо проще, чем годами топтать дорожку к большой компании, где есть и внутренний SOC, и департамент кибербезопасности.

— С какими атаками вы сталкиваетесь чаще всего?

— Из примерно сотни событий, которые фиксируются в день, около 80% — это срабатывания антивируса и попытки сканирования сети (проведения анализа периметра). Конечно, из них на инцидент тянут 1–2. Бывают необычные события, связанные с отклонением от стандартного поведения пользователя.

— Каких угроз ждать в ближайшем будущем?

— Учитывая, что мы находимся в противостоянии со страной-агрессором и ее потенциал создания угроз очень высок, мы ожидаем новую глобальную кибератаку. Когда, в каком виде — неизвестно, но ее последствия зависят от многих факторов, в том числе от подготовленности как государственной критической инфраструктуры, так и бизнеса, от понимания, что рано или поздно она произойдет. Если компании сейчас боятся рейдерства, черных регистраторов, то точно так же они должны осознавать, что бизнес можно потерять только из-за того, что кто-то не обратил должного внимания на кибербезопасность.

Сейчас есть инициатива создания некой платформы обмена киберугрозами. Мы готовы делиться индикаторами компрометации (IOC), чтобы поднимался общий уровень защищенности. А чем больше чистых IOC будет приходить от наших партнеров-конкурентов, тем качественнее станут и наши услуги. Имеет смысл сотрудничать, потому что оформлять подписки на коммерческие IOC гораздо менее эффективно.

Беседовал **Василий ТКАЧЕНКО**, **СиБ**