Михаил САВЕЛЬЕВ
директор по развитию бизнеса
компании «Информзащита»

ОГЛЯНУТЬСЯ ВПЕРЕД

ЗИМА БЛИЗКО! ПРИБЛИЖАЕТСЯ ЭПОХА НУЛЕВОГО ДОВЕРИЯ

BIS Journal обратился к директору по развитию бизнеса компании «Информзащита» Михаилу Савельеву с просьбой обозначить наиболее яркие, на его взгляд, тенденции в сфере ИБ в 2018 году и сделать прогноз на 2019-й.

2018-Й

Чтобы увидеть, что ждет впереди, порой стоит оглянуться назад. А в этом плане 2018 год принес нам немало:

◆ **Об инцидентах.** С одной стороны, в 2018 году не было таких громких, значимых атак, как в 2017. А с другой — в тени эпидемий шифровальщиков както затерялись и апрельская массовая атака на оборудование Cisco, и появление аппаратных уязвимостей, к которым, к слову, отрасль оказалась не очень готова. В результате чего, соответственно, усилия по их устранению обошлись намного дороже, чем предполагалось.

◆ **О нормативке.** ИБ-отрасль в нашей стране сильно зависима от нормативной базы. А она в 2018 году развивалась стремительно: вступление в силу 187 федерального закона и целого ряда подзаконных актов, выход 167-ФЗ, обновления Положения 382-П и пр., — все это вызвало бурную волну обсуждения как самих документов, так и тянущихся за ними последствий. Надо отметить, что регуляторам удалось взбодрить довольно широкие массы тех, кто либо не задумывался, либо откладывал вопросы безопасности в дальний ящик. Первые полгода прошли в панических обсуждениях, а вторая половина — в процессах составления перечней КИИ и старте процессов категорирования объектов. Я надеюсь, что год, отводящийся на категорирование (а это фаза, на которой находится подавляющая часть активных субъектов КИИ), не станет периодом забвения. Главное, что в головах выстроилось понимание, для чего, зачем и что нужно делать. К слову, я считаю, что регуляторам в рамках 187 закона удалось сформулировать достаточно гармоничный подход к защите объектов КИИ.

◆ **О SOC.** И инциденты, и нормативка (в части ГосСОПКА) стали стимулами к массовому строительству SOCов. И это хорошо тем, что появилось осознание необходимости мониторинга для выявления и оперативного реагирования на инциденты ИБ. Но…

◆ **О кадрах.** Но, оказалось, что катастрофически не хватает специалистов для работы на этих сложных комплексах, о которых говорилось выше. Этот фактор полностью обессмысливает многомиллионные затраты на строительство SOC. Кадровый голод на рынке ощущается остро: сегодня специалисты скорее перетекают из компании в компанию, чем воспроизводятся внутри. Их переманивают всем, чем только можно. Это взвинчивает рынок труда, зарплаты растут, а вот проблемы дефицита кадров пока не решаются.

◆ **Об отрасли.** Главная тенденция на «ментальном» уровне: отрасль ИБ «мудреет». Под этим я подразумеваю как рост компетенций у молодого поколения ИБ-шников, так и захватывающее умы осознание того, что безопасность должна быть неотъемлемым свойством ИТ-решений. Надо сказать, что и извечная пропасть между айтишниками и безопасниками сокращается на глазах — мы чаще начинаем доверять друг другу и сближаться для совместного решения встающих перед нами проблем.

◆ **О рынке.** Меняется расстановка сил. Нельзя не заметить как тенденцию крупных заказчиков к созданию и использованию инсорсинговых компаний, так и выход на рынок таких игроков, как «Ростелеком».

2019-Й

Что определит развитие отрасли ИБ в 2019 году? Если отбросить заведомо футуристические вещи и взглянуть на ИБ прагматически, то отметить хочется несколько главных, на мой взгляд, тенденций:

1. Кадровый голод потребует решения вопроса автоматизации рутинных операций. Тут речь идет и о мониторинге инфраструктурных событий, и о поиске фрода в различных его проявлениях. Обрабатывать руками невозможно не только огромное количество событий, собираемых с инфраструктуры (для этого и появились SIEM и подобные платформы), но и проводить первичную обработку этих событий, не говоря уже об оперативном реагировании на понятные инциденты. Как это будет решено — пока не знаю. Но решения такого рода станут востребованы в ближайшем будущем.

2. Кадровый голод приведет и к росту сервисных услуг в области ИБ.

3. Повсеместное строительство SOC начнет перерастать в тенденцию «оцифровки бизнеса», т.е. сбора всех возможных данных о работе систем и процессов. Надо ждать, что вместо хайпа за счет «искусственного интеллекта и машинного обучения» мы начнем учиться выявлять девиации в произвольных бизнес-процессах.

4. Повсеместное строительство SOC повысит популярность и востребованность услуги проведения киберучений, ведь их результаты смогут дать оценку как качеству правил, по которым осуществляется мониторинг (они обязаны видеть действия атакующих), так и слаженности и отработанности действий персонала SOC в процессе реагирования на инциденты.

5. Количество средств защиты должно начать переходить в качество. Мы видим, как большая часть заказчиков начинает решать проблемы не за счет приобретения новых решений по ИБ, а за счет базовых, гигиенических мер (управление уязвимостями, конфигурациями) и максимального использования уже имеющегося инструментария и настроек системного ПО. Сегодня грамотное использование только вышеназванных гигиенических мер может свести риск успешной реализации атак до минимального уровня.

6. Осознание важности работы с персоналом (а он-то и был, и остается самым уязвимым звеном) приведет к очередному витку попыток контроля за ним. Должен родиться не только и не столько поведенческий, сколько некий комплексный анализ действий пользователей.

7. Фокус безопасности станет шире: внимание компаний будет обращено не только на себя. В фокус безопасников неизбежно станут попадать контрагенты и прочее окружение компаний. Вектор целевых атак меняется. Наш IZ: SOC видит, что атаки чаще стали идти не напрямую на организацию, а через третьи руки: партнеров по бизнесу, поставщиков различного рода услуг, разработчиков заказного ПО и т.п. Это является ярким маркером эпохи так называемого «нулевого доверия» — времени, когда под сомнение необходимо ставить абсолютно любую внешнюю коммуникацию.

Атаки чаще стали идти не напрямую на организацию, а через третьи руки: партнеров по бизнесу, поставщиков различного рода услуг, разработчиков заказного ПО и т.п

8. Немалую роль будет играть принятый курс на импортозамещение. К счастью, в настоящее время реестр отечественного ПО активно чистится от псевдороссийских решений. И если государство будет дальше поддерживать этот курс, то интеграционных задач по переходу на отечественные решения хватит на всех.

В «ИНФОРМЗАЩИТЕ»

Компания «Информзащита» стремится развиваться опережающим темпом:

1. Основной потенциал компании — это люди. Наше развитие немыслимо без постоянного приобретения новых компетенций. Залогом успешного решения любой проблемы заказчика является возможность быстро собрать проектную команду, обладающую всеми необходимыми знаниями. Именно поэтому мы активно вкладываемся в развитие наших специалистов.

2. Вопрос кадрового голода мы успешно решаем за счет сотрудничества с ведущими техническими вузами Москвы и активного развития стажёрской программы. Так, по итогам зимней и летней стажировок 2018 года штат компании пополнили около 20 молодых специалистов. Стажировка в компании включает в себя как обучение, проводимое ведущими экспертами «Информзащиты», так и привлечение стажеров к практической работе сначала в роли наблюдателей, а затем — младших специалистов. Практика такого своеобразного «Инкубатора» настолько понравилась всем, что в январе 2019-го к нам пришло более 50 заявок на новый поток стажировки, и мы с удовольствием примем в штат всех, кто себя хорошо зарекомендует в этот период.

3. В компании регулярно проводятся стратегические сессии топ-менеджеров, на которых анализируется динамика и потребности рынка. Сегодня мы, сохраняя фокус на ИБ, работаем над развитием отраслевых компетенций, которые позволят нам глубже понимать бизнес-процессы заказчиков и обоснованно предлагать встраивать в них механизмы защиты. Структурно это выражается в создании отдельных центров компетенции, более глубоко проникающих в предметную область заказчика.

4. Наличие собственного подразделения разработки позволяет нам с легкостью решать различные интеграционные задачи, сопрягать несвязанные системы, создавать и тиражировать новые решения. Некоторые из них мы готовимся выпустить в качестве продуктов.

5. Защищать без понимания того, как осуществляется атака — невозможно. Именно поэтому мы сформировали одну из самых многочисленных и квалифицированных команд «белых» хакеров. Опыт этих ребят позволяет нам на качественно ином уровне строить системы безопасности и анализировать защищенность бизнес-процессов.

6. Мы полностью готовы к сервисной модели обеспечения информационной безопасности. И главным залогом своего успеха на этом поприще мы видим отлаженность собственных процессов и широту компетенций наших специалистов.