DOI: 10.25728/avtprom.2020.07.01

Кибербезопасность сегодняшнего дня – вера в технологии, вера в людей, поиски баланса

В.В. Дрюков (Компания «Ростелеком-Солар»)

Рассмотрены современные проблемы, стоящие перед специалистами по информационной безопасности. Перечислены основные пути, позволяющие предприятиям осуществить противодействие профессиональному злоумышленнику. Отмечено, что все возможные варианты связаны с существенными инвестициями. И компаниям нужно выбрать для себя наиболее комфортную статью расходов.

Ключевые слова: кибербезопасность, инвестиции, злоумышленник, кибератака, уязвимости.

С каждым годом кибербезопасность все активнее входит в нашу жизнь. Для меня лично откровением стал 2018 г., когда моя уже достаточно взрослая мама, учитель физики и астрономии, начала понимать, чем я занимаюсь, — настолько информационный фон, созданный киберпандемиями шифровальщиков, оказался серьезным и массовым. И вообще в последние годы практически за любым крупным аномальным событием в нашей жизни принято видеть признаки кибератаки. Все помнят Олимпиаду 2014 г. и казус, связанный с олимпийскими кольцами. Уже тогда было достаточно много разговоров на тему того, не является ли причиной сбоя скрытая кибератака, а некоторые журналисты искали политические мотивы произошедшего. И уже через четыре года мы увидели фактическое влияние кибератаки на Олимпиаду-2018 г. в Пхеньяне. Резонанс был настолько сильным, что в авторитетном западном издании Wired даже вышла статья с заголовком «Most deceptive hack in history», описывающая атаку и явно указывающая на виновников — группировку Lazarus.

Известно, что кибератака может остановить крупное предприятие любой отрасли, правильно спланированные действия киберпреступников могут спровоцировать blackout в крупном городе или даже области, а фильм «Крепкий Орешек-4», которые многие воспринимали, скорее, как комикс, по сути, демонстрирует возможные последствия от угрозы. Все это заставляет специалистов по информационной безопасности (ИБ) каждый день стремиться быть «быстрее, выше, сильнее» своего противника вне зависимости от времени суток, дней недели и личных дел. Рассмотрим возможные пути достижения этого результата и оценим выбор, который каждый день делает специалист по ИБ, чтобы увидеть атаку злоумышленника заранее и своевременно на нее прореагировать.

Таблица 1. Временные интервалы между публикацией уязвимости (CVE), появлением эксплоита и первой публичной атакой злоумышленников

	CVE	Time	Exploit	Time	Attack
Shellshock	12 Sept 2014	2 недели	24 Sept 2014	1 день	25 Sept 2014
Eternal Blue	n/a	n/a	14 Apr 2017	1 неделя	21 Apr 2017 12 May 2017
CVE-2018-15982	28 Aug 2018	3,5 месяца	5 Dec 2018	1 сутки	7 Dec 2018
Blue Keep	14 May 2019	2 месяца	25 Jul 2019	n/a	n/a

Опередить злоумышленника

Внутри компаний в каждой из отраслей можно видеть некоторое социальное соревнование. Особенно это заметно в кредитно-финансовой сфере и on-line сервисах, где атака злоумышленников, как правило, имеет целью прямую монетизацию. Это достаточно ожидаемо: если злоумышленник работает не по заказу, а стремится атаковать просто компанию определенной отрасли, для него гораздо проще и дешевле направить свои усилия на наименее защищенную и «слабую» жертву. Поэтому компании стремятся подсветить свои вложения и объем усилий для обеспечения кибербезопасности: появляются публикации о внутренних проектах, о подключении к внешнему провайдеру сервисов ИБ. Таким образом различные организации заявляют о своей возможности противодействовать атаке и, казалось бы, рассказывая об используемых инструментах защиты, на самом деле сигнализируют о том, что взломать их не так-то просто.

Говоря о скорости «бега», нельзя оставить в стороне вопрос регулярно появляющихся критических уязвимостей как в базовом, так и в прикладном ПО. Ключевой вопрос: в состоянии ли компания прореагировать на новую угрозу (уязвимость) быстрее, чем ей начнут пользоваться злоумышленники?

В табл. 1 представлена выдержка из большого аналитического исследования интер-

Таблица 2. Время устранения уязвимостей

Отрасль	Время устранения критичных уязвимостей ОС	Время устранения прикладных уязвимостей
Финансовый сектор	42 дня	До 20 дней наложенными средствами, от 90 – исправление
Энергетика и ТЭК	66 дней	Корпоративные сети – от 120 дней, АСУ ТП — ....
Государственные органы	134 дня	.....

валов времени между фактической публикацией уязвимости (CVE) до появления публичного эксплоита[1], а потом от эксплоита до первой публичной (известной) атаки злоумышленников. Оставим пока за скобками ситуацию с BlueKeep, который действительно в свободной природе проявил себя достаточно поздно. В целом статистика достаточно показательная: как правило, с момента публикации информации об уязвимости до появления эксплоита проходит несколько недель, и далее — всего несколько дней до первой атаки с его использованием. Особенно печально ситуация смотрится для уязвимости Adobe (CVE-2018-15982), которая использовалась в атаке уже через сутки после появления эксплоита. И эта скорость злоумышленников продолжает увеличиваться, они все быстрее адаптируют свои инструменты к новым способам атак.

На другой чаше весов находится возможность эти уязвимости оперативно закрыть. И, к сожалению, здесь цифры пока не оптимистичные (табл. 2).

Препятствия на пути офицера ИБ:

• огромный парк рабочих станций, которые никогда не бывают доступны одновременно, а у части еще и невозможна автоматическая перезагрузка;

• необходимость тестирования патчей[2] ОС и оборудования на совместимость с прикладным ПО, специализированными протоколами и т. д.;

• нагрузочное тестирование по ключевым системам, чтобы патч случайно не прикончил быстродействие системы (вспомним историю Spectre/Meltdown);

• простой бизнес-процессов и бизнес-сервисов, который даже в корпоративной среде согласовать непросто, сложность многократно возрастает, когда речь касается уязвимостей в оборудовании АСУТП.

Ключом к тому, чтобы успевать вовремя, является один из важнейших навыков специалиста по ИТ безопасности — коммуникация. Когда он в состоянии донести до руководства все риски от затягивания с установкой обновлений, когда он может выстроить коммуникацию с ИТ-подразделением и технологами таким образом, чтобы устранение самых критичных уязвимостей проходило быстрее, чем их начинают использовать злоумышленники.

Директор по ИБ может избрать альтернативный путь, заключающийся в минимизации поверхности атаки и компенсирующих мерах. В этом случае возникают такие задачи, как полноценная сегментация сети с существенными вложениями в специализированные решения, установка между сегментами систем обнаружения атак, максимально оперативное обновление сигнатур для блокировки или хотя бы выявление попыток эксплуатации уязвимостей. В этом случае можно выбрать менее сложный процессно, но существенно более дорогой финансово путь по противодействию угрозам, что для многих — тоже вариант.

Выше ожиданий атакующего

Одним из ключевых векторов атаки сейчас является фишинг — вид Internet-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Центр мониторинга и реагирования Solar JSOC фиксирует ежегодный рост случаев использования этого инструмента: 4 из 5 сложных атак начинаются с фишинговых рассылок. И с каждым годом они усложняются: от примитивных писем про нигерийских принцев злоумышленники переходят к акциям на Black Friday, бесплатным билетам на значимые мероприятия или лекарствам от новых болезней. Фишинговые письма все больше похожи на настоящие — логотипами, ссылками и всеми прочими атрибутами, и все чаще во вложении или по ссылке мы видим не примитивный троян, а сложное вирусное программное обеспечение, позволяющее злоумышленнику быстро получить доступ к инфраструктуре. Борьба с фишингом имеет два пути.

Первый — инвестиции в технологии. В последнее время заказчики все чаще используют сложные решения класса «песочница» (Sandbox) или Anti-APT, проводящие максимально детальный анализ письма и его вложений с целью выявления скрытого вредоносного ПО. Этот подход при всей своей дороговизне на первый взгляд оправдывает вложения. Но только на самый первый взгляд.

Появилось вирусное ПО, разработанное специально для обхода песочниц. Как правило, такие вирусы мультикомпонентны и используют для своего запуска и сборки легитимные утилиты операционной системы или скрипты, каждый из которых не несет в себе никакой вредоносной нагрузки. Лишь в совокупности уже собранная функциональность позволяет злоумышленнику использовать его в своих целях.

Также встречается вирусное ПО, которое в течение первых нескольких часов после запуска в песочнице лишь фиксирует снимки экрана. Делается это для того, чтобы проанализировать, есть ли между ними какая-то разница, и тем самым определить,

[1] Эксплóит (эксплуатировать) — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

[2] Запла́тка или патч — информация, предназначенная для автоматизированного внесения определенных изменений в компьютерные файлы.

находится ли оно на машине активно работающего пользователя или в синтетической среде, где не следует запускать модули с основной вредоносной функциональностью.

Перед лицом подобных атак и достаточно дорогостоящее решение не дает гарантий и не становится серебряной пулей для противодействия угрозе.

Второй путь — инвестиции в обучение сотрудников компании основам киберграмотности, и формирование «последнего редута обороны» из пользователей, на которых и направлены эти фишинговый рассылки. При правильном подходе это дает очень хороший эффект: после обучения вместо каждого седьмогоо пользователя, поддающегося на фишинговую атаку, письма открывает только каждый 12-й. Но ключевым процессом в повышении киберграмотности является даже не столько приобретение соответствующих навыков (которое тоже необходимо), сколько формирование у пользователя потребности в обратной связи. Ведь если из 11 пользователей, которые не открыли фишинговое письмо, хотя бы один не только почувствует неладное, но и сообщит службе ИБ, дальнейшее блокирование и противодействие атаке станет делом техники.

Мы все чаще встречаем компании, выбирающие именно второй путь: инвестиции в процессы и обучение вместо технологий.

Сильнее хакера в технологиях и экспертизе

Третьим трендом, который сложно игнорировать, является существенный рост сложности инструментария, используемого злоумышленниками, и общий рост их экспертизы. Во многом этому способствовали два инцидента с выкладыванием в публичный доступ архивов государственного кибероружия. В итоге даже специалисты невысокой квалификации получили в свои руки готовые инструменты для сложных, практически недетектируемых атак, а заодно познакомились с методами, техниками и тактиками профессионального взлома. Не случайно все современные модели угроз для крупных предприятий в части внешнего нарушителя так или иначе опираются на риски атаки профессиональной группировкой или даже кибервойсками. И техники, и подходы, которые применяются командами высокой квалификации, делают прямое выявление угрозы крайне сложным. Вместо явных «следов» в инфраструктуре опытные злоумышленники оставляют скорее «хлебные крошки», и только при их внимательном и тщательном анализе у специалиста появляется шанс выявить, проанализировать и прореагировать на атаку.

Чем же может ответить сторона защиты?

Во-первых, использованием современных технологий фиксации и сопоставления аномалий. Сейчас часто говорят об использовании искусственного интеллекта и других подходов с нечеткой неформализованной логикой в интересах ИБ. Но пока применимость их в реальных условиях вызывает скепсис у ИБ-сообщества. Любая такая система сначала должна пройти весьма длительный этап «обучения» инфраструктуре. Ей, как растущему ребенку, сначала нужно рассказать, «что такое хорошо, что такое плохо». В условиях цифровой трансформации и ежедневных изменений, происходящих в инфраструктуре любой крупной компании, такое обучение потребует колоссальных инвестиций в виде времени специалистов службы ИБ.

Второе — максимально широкое использование доступных и уже применяемых в компании технологий для обеспечения режима full view или полной наблюдаемости инфраструктуры: подключение всей инфраструктуры в SIEM[3] [1,2] со сбором детальных логов, включая установку Sysmon[4] на Windows-серверы и рабочие станции, контроль сетевого трафика, сбор информации со всех Web-приложений или контроллеров инфраструктуры АСУТП. Это будет способствовать существенному повышению эффективности работы службы ИБ, благодаря тому, что в каждом инциденте или аномалии можно будет дойти до самой сути. При этом финансовых вложений в инструменты защиты потребуется чуть меньше. Однако минус в том, что это дает очень существенную нагрузку на службы ИТ и ИБ в части контроля и поддержания самого состояния full view: развертывание журналирования на каждой системе, мониторинг и устранение сбоев в поступлении событий с каждого из нескольких тысяч источников, выяснение причин пропадания событий на рабочих станциях (причиной которому могут быть не только действия злоумышленника, но и простое отключение машины в связи с отпуском сотрудника или работы ИТ-администратора). Зачастую совокупные инвестиции в фонд оплаты труда сотрудников, которые поддерживают этот уровень защищенности, могут оказаться выше тех финансовых рисков, которые несет компания при киберинциденте, что делает такой подход совершенно не рентабельным.

Другой подход — инвестиции в технологии и экспертизу внутренних специалистов на разработку способов косвенного выявления атаки с использованием уже имеющегося инструментария, анализ всех новых векторов и техник, сбор информации как из открытых источников, так и с ресурсов Даркнета[5]. При

[3] SIEM (Security information and event management) — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) — управление информацией о безопасности и SEM (Security event management) — управление событиями безопасности. Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений, и позволяет реагировать на них до наступления существенного ущерба.

[4] System Monitor (Sysmon) - сервис, совершающий мониторинг всех процессов в ОС Windows. Утилита содержит подробные сведения о запуске процессов, сетевых соединений, а также изменениях времени создания файлов.

[5] Даркнет — скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов.

общей экономической целесообразности этого подход относительно предыдущих имеет свои ограничения в виде дефицита квалифицированных кадров. Вопросы кадрового голода на рынке ИБ поднимаются чуть ли не на каждой конференции, поэтому остается лишь признать тот факт, что реализацию этого подхода могут позволить себе лишь единицы из числа самых привлекательных работодателей.

Таким образом, на любом выбранном пути по противодействию профессиональному злоумышленнику компании потребуются существенные инвестиции, и компания может выбрать для себя только наиболее комфортную статью расходов: дорогостоящие технологии, которые позволят после долгой докрутки автоматизировать часть работы, вложения в экспертизу специалистов для попытки выявления атак на существующих инструментах или инвестиции в процессы компании, когда проблемы кибербезопасности разделяются и руководством, и ИТ подразделением, и обычными пользователями. В любом из вариантов, в том числе промежуточном — это долгий и тяжелый путь. Но в любом случае стоять долго на месте, как витязь у камня, нельзя, потому что актуальность и критичность проблемы обеспечения кибербезопасности объяснять уже не нужно.

Список литературы

1. *Abdul B. Subhani.* Stay Safe! AbbottPress. 2016. 182 с.
2. *Дрозд А.* Обзор SIEM-систем на мировом и российском рынке. https://www.anti-malware.ru/

Дрюков Владимир Викторович *– директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар». Http:// rt-solar.ru*

DOI: 10.25728/avtprom.2020.07.02

Анализ методики аудита информационной безопасности предприятия с помощью аутсорсинговых компаний

А.А. Басырова, И.И. Лившиц (Университет ИТМО)

Раскрывается понятие аудита информационной безопасности, выполняемого с помощью компаний, оказывающих услуги аутсорсинга (ИБ-аутсорсинг). Представлен анализ существующих методик, а также состояние и тенденции развития современного рынка ИБ-аутсорсинг в РФ и за рубежом. Определено, что целью ИБ-аутсорсинга в современной ИТ-индустрии является сокращение финансовых затрат, применение новой концепции оценки защищенности и снижение времени проведения аудита системы менеджмента информационной безопасности.

Предложено к задачам ИБ-аутсорсинга относить обеспечение защиты конфиденциальной информации, а также прогнозирование рисков ИБ в соответствии с существующими практиками. Это позволит принимать обоснованные управленческие решения на основе объективных отчетов, оперативно выявлять схемы мошенничества, содействовать эффективному выполнению требований регуляторов по обеспечению безопасности объектов критичной инфраструктуры. Важным также представляется обеспечение возможности повышения эффективности контроля использования рабочего времени, исходя из анализа настроения в коллективе. Новизна работы заключается в разработке метода ИБ-аутсорсинга и предоставлении доказательств эффективности (как экономической выгоды) привлечения аудиторских компаний, занимающихся аудитом ИБ.

Ключевые слова: аудит, информационная безопасность, аутсорсинг, методики, уровень защищенности, система менеджмента информационной безопасности, информационные технологии.

Введение

Аутсорсинг аудита информационной безопасности (ИБ-аутсорсинг) — это процесс выполнения внешней оценки степени защищенности ИТ-сервисов компании с выдачей экспертных рекомендаций и минимизация рисков утечки конфиденциальных данных. Сегодня с помощью ИБ-аутсорсинга у многих компаний появляется возможность получить полную и объективную оценку степени защищенности собственных ИТ-сервисов, оперативно обнаруживать уязвимые места в бизнес-процессах, а также разработать план по улучшению системы менеджмента информационной безопасности (СМИБ). По этим причинам тема ИБ-аутсорсинга является устойчивым трендом отечественных и зарубежных компаний. Данный вид аудита затрагивает все области СМИБ, например, сюда можно отнести такие виды активов, как сетевая инфраструктура, операционные системы, системы визуализации, системы управления базами данных, средства защиты информации и критические процессы [1].

Преимущество ИБ-аутсорсинга состоит в том, что с его помощью решается проблема отсутствия возможности у компании собрать в своем штате достаточное число высококвалифицированных специалистов в области ИБ и ИТ. Решив эту проблему, компания смо-