Мир наживы и киберчистогана

— технологии —

с13

Василий Дягилев, глава представительства компании Check Point Software Technologies в России и СНГ, рассказывает: «Основные убытки приносят махинации в финансовой сфере и простой тех или иных систем, которые выведены хакерами из строя. Ущерб от действий хакеров может распространяться на целые страны. Мы уже видели пример, как из-за хакеров меняется курс национальной валюты, как было в результате атаки на один из российских банков в 2015 году. Злоумышленники сломали систему, посылающую заявки для торговли на валютной бирже, разместили заявку на очень большое количество валюты — это привело к скачку курса рубля. Конечно, впоследствии ситуация выправилась, однако такие случаи становятся нашей реальностью».

Но речь идет не только о финансовых и репутационных потерях, которые иногда уничтожают бизнес отдельных компаний подчистую. Есть угрозы и более серьезные, связанные с физической безопасностью людей. Давайте представим, что, как в голливудском триллере, некий злобный хакер взял под контроль управление всеми железными дорогами. К сожалению, такой сценарий уже сегодня вполне реален. Эксперты из группы SCADA StrangeLove изучили систему защиты поездов SIBAS, которая широко распространена в странах Европы. Результаты оказались тревожными. Обнаружилось несколько уязвимостей, которые позволяют управлять устройствами без аутентификации и создавать хакерские инструменты для дистанционного контроля над оборудованием. Серьезная уязвимость обнаружилась в системе, отвечающей за распределение маршрутов поездов. Если хакеры получат доступ к этому программному обеспечению, они смогут физически переключить стрелку на рельсах и пустить поезд по ложному маршруту. Последствия этой ситуации могут быть весьма серьезными.

В эпоху подключения всего к интернету самой страшной угрозой ближайших лет становятся именно атаки на критически важную инфраструктуру. Сергей Петров, член правления корпорации «Галактика», рассказывает, что кибератаки на промышленные объекты становятся все популярнее в связи с растущим уровнем автоматизации процессов. «Как правило, корпоративный сегмент основное внимание уделяет сохранности конфиденциальных данных, а обеспечение бесперебойной работы уходит на второй план. В этом главное отличие от промышленных предприятий, где цена минуты простоя, как и любой ошибки, очень велика. Если раньше физической изоляции между производственными системами и внешними сетями хватало для хорошего уровня защиты, то теперь этого недостаточно. Это же касается транспортного сектора, энергетических и телекоммуникационных компаний, поскольку все эти предприятия все больше зависят от автоматики, робототехники, цифровых сетей и взаимозависимых устройств»,— объясняет он.

Широкое проникновение в работу предприятий облачных вычислений, систем бизнес-аналитики и интернета вещей приводит к сращиванию информационных и операционных технологий, что потенциально предоставляет злоумышленникам доступ к компонентам систем и критически важным процессам. Кибератаки связаны с большими репутационными рисками и приводят к ухудшению финансовых показателей компании, краже интеллектуальной собственности, потере конкурентных преимуществ, а на национальном уровне — к ослаблению экономики страны. «Важным моментом является и тот факт, что большинство используемой техники и софта в России — это продукты зарубежных корпораций. Сегодня большинство промышленных предприятий не осознают этих рисков, а тем временем в иностранных ИТ-системах обнаруживаются все новые уязвимости, которыми пользуются злоумышленники»,— добавляет Сергей Петров.

По прогнозам «Лаборатории Касперского», в ближайшие годы наиболее опасными видами киберпреступного бизнеса будут DDoS-атаки и троянские программы-шифровальщики, вымогающие деньги за расшифровку. Это основные сервисы, которые сейчас предлагаются в русскоязычной киберпреступной экосистеме. Также начинает развиваться сфера промышленного шпионажа и «конкурентной» разведки, когда основной целью преступников становятся не деньги компании, а ценная информация, такая как контракты, деловая переписка и т. п.

По словам Александра Лямина, основателя и руководителя Qrator Labs (предоставляет облачный сервис для защиты от DDoS-атак), кибератаки становятся все более сложными. Часто злоумышленники комбинируют разные средства, чтобы достичь желаемого. Например, отвлекают внимание специалистов компании с помощью DDoS-атаки, в то время как производится взлом веб-приложений. При этом сами по себе DDoS-атаки, приводящие к полной или частичной недоступности интернет-ресурса,— весьма популярный инструмент вымогателей и неэтичных конкурентов. «Организовать такое нападение стоит сегодня от $5 в сутки. В черном интернете можно скачать множество уже готовых к использованию инструментов для DDoS-атак, которыми способен воспользоваться даже школьник. Поэтому популярность метода растет с каждым годом на 25–50%. А в эпоху интернета вещей мы увидим в действии гигантские ботнеты, когда атака будет исходить из каждого умного, но слабозащищенного чайника»,— говорит Александр Лямин.

В качестве примера эксперт приводит атаку на сайт KrebbsOnSecurity, освещающий вопросы кибербезопасности. Вечером 20 сентября на ресурс обрушилось цунами из мусорного трафика со скоростью 665 Гб/сек. (предыдущий рекорд — 363 Гбит/сек). Ресурс удалось защитить с помощью спецсредств Akamai. Эксперты этой компании рассказали, что гигантский ботнет был создан с помощью взломанных IoT-устройств: роутеров, веб-камер, видеорегистраторов, подключенных к интернету и защищенных слабыми паролями. Атака исходила буквально отовсюду.

Сила противодействия

Апокалиптические картины будущего, которые рисуют эксперты, начинают постепенно сбываться. Киберпреступность стала организованным черным рынком, противостоять которому можно только слаженными системными усилиями разных стран.

Андрей Заикин, руководитель направления информационной безопасности компании КРОК, говорит, что для противодействия этой глобальной угрозе используется специализированный класс решений по борьбе с направленными атаками (AntiAPT). Но чтобы обеспечить оптимальный уровень информационной безопасности в корпоративном секторе, нужно предусмотреть целый комплекс мер, который включает в себя также сетевую безопасность, обеспечение защиты приложений (включая АСУ ТП для производственных предприятий), проведение тестирований на проникновение (pentest), повышение осведомленности персонала о рисках и способах их нивелирования и пр. Такими, казалось бы, элементарными вещами, как своевременное обновление программного обеспечения и антивирусов, тоже нельзя пренебрегать. Михал Салат, ведущий вирусный аналитик Avast Software, рекомендует «джентельменский набор» для защиты госкомпаний и бизнеса, состоящий из нескольких уровней, включающих антивирус, брандмауэр, систему обнаружения вторжений. По его словам, также важно регулярно обновлять встроенные программы и ПО, предоставлять работникам соответствующие права доступа на пользование.

Сергей Ложкин отмечает, что в России есть ряд сложностей, возникающих при расследовании инцидентов: «Прежде всего это слабое законодательство, регулирующее высокотехнологичные преступления. В США компании обязаны сообщать об атаках на их ИТ-инфраструктуру, это регулируется законом. В России компании, наоборот, предпочитают замалчивать инциденты, поскольку опасаются потерь для репутации». В РФ тяжело доказать сам факт киберпреступления, в основном подобные действия подпадают под статьи 272 и 273 — это статьи небольшой тяжести с максимальным наказанием до семи лет заключения. В следственных органах, к компетенции которых относится расследование компьютерных преступлений, нет специальных подразделений и специалистов, обладающих глубокими техническими знаниями. «В России до сих пор во многих организациях действует так называемая бумажная безопасность: мы имеем огромное количество правил, которые регулярно обновляются, но при этом плохо работают на практике. Тогда как на Западе правил как таковых нет, но организация обязана сделать все возможное, чтобы сохранить безопасность данных своих клиентов. Если данные утекли, организация будет наказана»,— объясняет эксперт.

«Многие государства, включая РФ, принимают так называемые доктрины кибербезопасности или киберстратегии. Это делается, чтобы урегулировать направление развития безопасности. Государство создает специальные подразделения, которые в разных ведомствах занимаются анализом специфического направления угроз. Такое подразделение есть, например, в Центральном банке. Государство делает много, но все-таки недостаточно, так что понимание опасности должно исходить именно от руководителей бизнеса, которые и принимают решение об уровне защиты данных»,— добавляет Василий Дягилев.

Борис Симис, заместитель генерального директора Positive Technologies по развитию бизнеса, рассказывает, что во многих странах есть отдельный представитель власти, отвечающий за информационную безопасность. В США KPI такого «главного по кибербезопасности» исчисляется в числе прочего и объемом онлайн-платежей. Почему? Когда кибербезопасность ниже среднего уровня, люди просто перестают пользоваться интернет-платежами. «У нас эти задачи распределены между различными ведомствами и нет прозрачности в разделении полномочий между ведомствами в части ИБ»,— говорит эксперт.

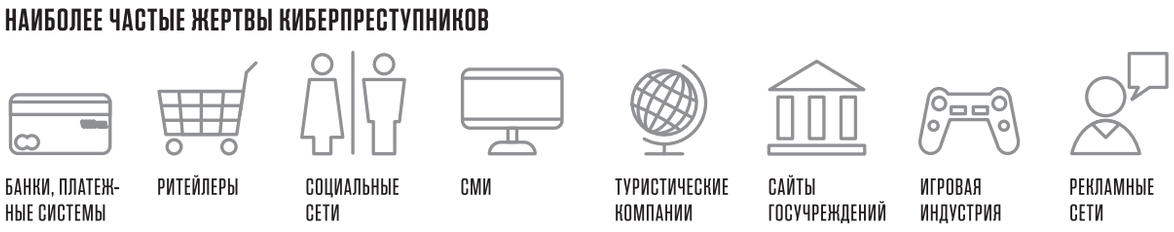
Человеческий фактор — основная причина проблем, связанных с ИБ. Решить ее можно только одним способом — проводя образовательные инициативы, приучая людей к осторожности. Борис Симис рассказывает, что в США и Австралии есть для этого ежегодные «кибермесяцы» (и открывает их глава государства), во время которых проводят специальные образовательные кампании на всех уровнях: от детских учебных заведений до госструктур и медиа. Страны Европы это тоже делают, но, как говорит эксперт, скорее будто «для галочки». В России таких государственных инициатив нет совсем.

Светлана Рагимова

КИБЕРПРЕСТУПНОСТЬ ПРОТИВ ЭКОНОМИЧЕСКОГО РОСТА

УЩЕРБ ОТ ОДНОГО ИНЦИДЕНТА В СРЕДНЕМ В РФ

НАИБОЛЕЕ ЧАСТЫЕ ЖЕРТВЫ КИБЕРПРЕСТУПНИКОВ



92% ОРГАНИЗАЦИЙ В РФ ВЫЯВИЛИ КИБЕРИНЦИДЕНТЫ В 2015 ГОДУ

на 100% ВЫРОСЛО СРЕДНЕЕ ЧИСЛО DDOS-АТАК В 2015 ГОДУ

в 84% СЛУЧАЕВ DDOS-АТАКИ ЧЕРЕДУЮТСЯ СО ВЗЛОМОМ

20–50% ЕЖЕГОДНЫЙ РОСТ ЧИСЛА DDOS-АТАК

100 млн И БОЛЕЕ ЗА ГОД СОСТАВЛЯЕТ ЧИСЛО ХАКЕРСКИХ АТАК

на 75% ОТМЕЧАЮТ 2/3 КОМПАНИЙ РОСТ АКТИВНОСТИ КИБЕРПРЕСТУПНОСТИ

на 173% ВЫРАСТЕТ ЧИСЛО КИБЕРАТАК К 2018 ГОДУ. ПОТЕРИ УВЕЛИЧАТСЯ НА 192%

31% САЙТОВ В РФ СОДЕРЖАТ КРИТИЧЕСКИЕ УЯЗВИМОСТИ

НАИБОЛЕЕ ЧАСТЫЕ ИНЦИДЕНТЫ В ФИНАНСОВОМ СЕКТОРЕ

24% БАНКОВ И ПЛАТЕЖНЫХ СИСТЕМ ПОДВЕРГЛИСЬ DDOS-АТАКАМ

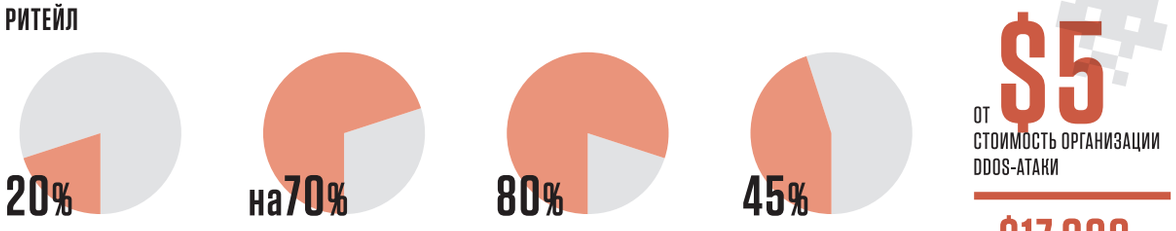
21% ФИШИНГ С ИСПОЛЬЗОВАНИЕМ ЛОЖНЫХ СТРАНИЦ ПОПУЛЯРНЫХ СЕРВИСОВ

17% ВЗЛОМ ПУТЕМ ПОДБОРА ПАРОЛЕЙ ИЛИ ИСПОЛЬЗОВАНИЯ КРАДЕНЫХ ПАРОЛЕЙ

20% ДРУГИЕ ИНЦИДЕНТЫ (ВИРУСЫ, ИНСАЙДЕРЫ, СБОИ В РАБОТЕ ДБО)

27% БАНКОВ УВЕЛИЧИЛИ БЮДЖЕТ НА ИБ

РИТЕЙЛ



20% КРУПНЫХ РИТЕЙЛЕРОВ ПОДВЕРГЛИСЬ DDOS-АТАКАМ В 2015 ГОДУ

на 70% ВЫРОСЛО В СРЕДНЕМ ЧИСЛО АТАК НА ИНТЕРНЕТ-МАГАЗИНЫ

80% РИТЕЙЛЕРОВ ПОДОЗРЕВАЮТ КОНКУРЕНТОВ В КИБЕРПРЕСТУПНЫХ ДЕЙСТВИЯХ

45% ПОДВЕРГЛИСЬ ШАНТАЖУ И ВЫМОГАТЕЛЬСТВУ

ОТ $5 СТОИМОСТЬ ОРГАНИЗАЦИИ DDOS-АТАКИ

ДО $17 000 СУММА ВЫКУПА, ЗАПРАШИВАЕМАЯ ШАНТАЖИСТАМИ

ИСТОЧНИКИ: GROUP IB, QRATOR LABS, WALLARM, «ЛАБОРАТОРИЯ КАСПЕРСКОГО», AVAST SOFTWARE.

ЕВГЕНИЙ ПАВЛЕНКО

Киберпреступность стала организованным черным рынком, противостоять которому можно только слаженными системными усилиями разных стран

От слов к делу

— мнение —

Сочинский инвестиционный форум, кажется, предпоследний крупный съезд бизнесменов и чиновников для обсуждения инвестиций и экономического развития в нынешнем году. За ним должно последовать традиционно приходящееся на более позднюю осень заседание Совета по иностранным инвестициям. Затем рождественский перерыв, и ближе к концу зимы годовой цикл вновь откроет Красноярский экономический форум. Санкт-Петербург, Ярославль, Владивосток, Москва тоже уже планируют «свои» традиционные экономические форумы на 2017 год.

С одной стороны, вроде бы хорошо, что есть так много площадок, на которых можно дискутировать о состоянии экономики России. С другой, лично у меня возникает явный диссонанс между числом этих международных встреч и их реальным влиянием на ситуацию в стране. Россия — страна большая, и у регионов действительно несколько разный экономический фокус. По идее если во Владивостоке обсуждают экономические связи с Азией, то в Сочи должны озаботиться отношениями с государствами региона Черного моря и Восточного Средиземноморья. Но вот парадокс: накануне последнего Восточного форума я был в Южной Корее. Там бизнесмены и дипломаты довольно откровенно говорили мне: «В российском Приморье живут 6 млн человек, а в трех северных провинциях Китая — 120 млн. Ясно, какой рынок будет больше нас интересовать». И даже те корейские инвесторы, которые все-таки пришли в Россию, едва ли не 90% своих средств вложили в европейскую часть РФ. И это лишь один пример того, как сложно России строить отношения с Азией. А если начать вспоминать другие темы вроде отсутствующего до сих пор мирного договора с Японией, политическая картина становится еще более запутанной. И так не только с Восточным форумом.

ГЛЕБ ЩЕЛКУНОВ

Учитывая частоту пребывания в городе «первых лиц», Сочи стал чем-то вроде полуофициальной третьей столицы России. Но с региональной точки зрения ясно: пока не будут окончательно нормализованы отношения Москвы с Киевом, Тбилиси и в какой-то степени с Анкарой, трудно говорить о сотрудничестве в Причерноморье. А война в Сирии делает региональные политические риски для России еще выше.

Можно сказать, что политика часто мешает бизнесу и такое случается не только в России. Это верно. Но все же это не единственная причина, по которой такое число экономических форумов кажется странным и вызывает раздражение иностранных партнеров. Экономика России сегодня — это прежде всего государственные корпорации. Когда я несколько лет назад работал в одной из крупных транснациональных корпораций, то часто слышал от коллег из компаний-инвесторов: «На всех форумах одни и те же лица одних и тех же партнеров: „Ростех“, „Газпром“, „Роснефть“… Мы с ними встречаемся на Санкт-Петербургском международном экономическом форуме, на Совете по иностранным инвестициям. Но мы же знаем: решается все не там, а в Москве».

Международные компании несентиментальны и готовы вести бизнес в России практически при любом политическом режиме. Но они прекрасно понимают: реальные сделки заключаются не на форумах, а в Кремле и Белом доме на Краснопресненской набережной. Главы транснациональных корпораций также знают: для российского руководства их приезд, например, на Санкт-Петербургский форум, этот ставший важной площадкой аналог Давоса, исключительно важен как демонстрация лояльности российской власти. Однако у этих же президентов и председателей совета директоров сверхплотный международный график, в том числе в странах, где экономика не находится в постоянном кризисе почти восемь лет, где государственные корпорации не так могущественны, а правительства не так подозрительны по отношению к инвесторам, как у нас. Кроме того, в России, где понятие «акционеры» до сих пор, мягко говоря, несколько абстрактно, не понимают, что от CEO любой международной компании эти самые акционеры на годовом собрании действительно могут потребовать отчет: зачем он три раза ездил на форумы в Россию, чтобы говорить с одними и теми же людьми, и ни разу не посетил проекты там, где конференций меньше, а бизнеса больше? Каждую такую поездку глава компании должен оправдать конкретными результатами.

Аргументы в пользу проведения форумов известны: чтобы привлечь инвестиции, нужно заявлять о себе как можно чаще и громче. Но дело в том, что все главные партнеры транснациональным корпорациям и так известны. С ними лучше всего встречаться в тиши их московских кабинетов. Именно там и закрывают главные сделки. Каждая из них в нашей стране всегда имеет уникальный характер.

Иностранному среднему бизнесу Россия сегодня менее интересна из-за кризиса, неясных правил игры, произвола чиновников, которые могут взять в оборот даже такого гиганта, как IKEA. Лояльность Кремлю и те и другие будут продолжать демонстрировать, так как знают: без этого в России нельзя. Но делать это четыре-пять раз в год в стране с ВВП, сравнимым с Калифорнией, они едва ли станут. Уж лучше бы инвесторы соревновались между собой за проекты, чем форумы — за приезд инвесторов.

Константин Эггерт,
ведущий программ и комментатор телеканала «Дождь»