Опасная цифра

Переход на «цифру» несет банкам не только дополнительные конкурентные преимущества, но и риски. Новые технологии часто недостаточно защищены, а масштабы DDoS-атак продолжают расти. Последствия от простоя бизнеса в результате инцидентов все серьезнее. Прежние же методы защиты уже не могут обеспечить достаточный уровень безопасности.


ЕВГЕНИЙ ПАВЛЕНКО

— тенденция —

Современную инфраструктуру банков защищать все труднее и все дороже. DDoS-атаки становятся мощнее, требуя более быстрой реакции. По данным опроса A10 Networks, во время каждого такого нападения в 2017 году были задействованы сотни тысяч устройств интернета вещей (IoT). Это уязвимое подключенное оборудование потенциально может служить точкой доступа к другим системам. Кибератаки на IoT-устройства могут привести к ущербу для физической инфраструктуры, нарушить работу важных сервисов.

К 2021 году количество IoT-устройств и IoT-датчиков в мире вырастет более чем вдвое и превысит 46 млрд (прогноз Gartner). При этом, по оценкам Hewlett Packard, у 70% таких продуктов есть уязвимости. По данным Счетной палаты США, среди основных факторов распространения угроз IoT — отсутствие контроля безопасности из-за невозможности спрогнозировать потенциальные проблемы, а также применение идентичного ПО в различном оборудовании. Это значит, что одна дыра в таком ПО может привести к взлому огромного количества устройств.

«Цифровизация, в основе которой лежит всеобъемлющее применение новых технологий, неизбежно сопряжена с рисками,— отмечает Тим Клау, руководитель направления по развитию технологий, анализа и контроля рисков PwC в России.— Среди ключевых можно отметить угрозы в области кибербезопасности и защиты конфиденциальных данных, которые будут расти в геометрической прогрессии по мере стремительного распространения, например, подключенных устройств. Они могут стать мишенью для киберпреступников, желающих получить доступ к жизненно важным системам, конфиденциальным данным, либо стать инструментом для проведения DDoS-атак».

В наших широтах

В российском банковском секторе угроза отказа в обслуживании также нарастает. Количество зарегистрированных в 2016 году Центробанком России DDoS-атак на банки увеличилось почти в два раза. Было зафиксировано множество случаев использования в этих целях интернета вещей. Правда, пока, по словам представителей ЦБ, результативность таких атак в кредитно-финансовой сфере не очень высока, по крайней мере выявленные инциденты до сих пор не носили критического характера.

По данным опроса, проведенного по заказу Qrator Labs, в 2016 году около половины респондентов из топ-200 банков по размеру активов сталкивались как минимум с одной DDoS-атакой. Более 50% опрошенных также отмечают, что за последний год уровень угроз DDoS вырос.

Известно, что в 2016-м были атакованы веб-сайты многих крупных банков, в том числе из топ-10. В частности, в Сбербанке заявляют, что за последние три года подвергались DDoS-атакам более 100 раз. Для противодействия использовались внутренние ресурсы, однако у организации есть и внешние системы защиты, включая операторский сервис «Ростелекома».

Как показал опрос Qrator Labs, чаще всего представители финансового сектора сталкиваются с фишингом. По итогам проведенного опроса 30% респондентов отметили, что такие атаки были одним из самых распространенных видов в 2016 году, тогда как в 2015-м об этой угрозе говорил лишь 21% респондентов.

Дополнительным фактором влияния стал резко возросший в последний год интерес к блокчейн-индустрии и ICO (Initial Coin Offering — первичное предложение криптомонет, аналог IPO в криптовалютном мире).

Симметричный ответ

На фоне роста числа атак банки наращивают свою защиту. Глобальный рынок средств защиты от DDoS, по данным IDC, к 2020 году увеличится до $1 млрд при среднегодовых темпах роста 11%. За тот же период российский сегмент вырастет до $32 млн (+14,4%). В эту оценку аналитики включают затраты на аппаратные решения и услуги.

Более трети респондентов Qrator Labs из финансовой отрасли подтвердили, что в 2016 году увеличили бюджет на информационную безопасность (ИБ), еще 39% сохранили его в прежнем объеме.

В числе наиболее существенных последствий от инцидентов в сфере ИБ более половины опрошенных отмечают финансовые и репутационные риски. Около четверти респондентов ссылаются также на повышение риска отзыва лицензии (годом ранее его фиксировали более 60%).

«Индустрия постепенно приходит к пониманию того, что, выполняя „до буквы“ требования регуляторов, лицензиаров и сертификационных организаций, пройти большинство проверок можно, а вот построить по-настоящему безопасную систему — нельзя,— комментирует Александр Лямин, генеральный директор Qrator Labs.— Начинать следует с выстраивания эффективных процессов ИБ, а вопросы лицензирования и сертификации должны быть вторичными. Если два года назад многие рассматривали отзыв лицензии как основной риск, то сейчас становится понятно, что он является лишь побочным».

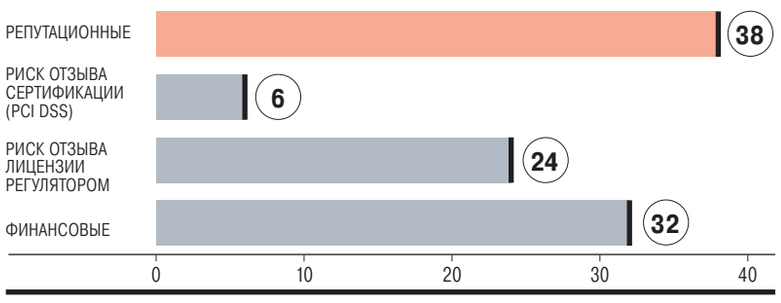
Наращивание ИБ-бюджета в банках — часть стратегии обновления инфраструктуры ИТ в целом. Более четверти респондентов видят необходимость в замене средств защиты при переходе на облачные сервисы, микросервисы и другие нововведения. В этой ситуации часто прежние решения перестают быть эффективными, что подтверждают, в частности, пентесты (оценка безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника). Об этом заявили 53% опрошенных. При этом, следуя актуальным требованиям рынка к минимизации затрат, 13% респондентов отмечают, что в первую очередь ориентированы на миграцию импортных решений на российские аналоги.

Большинство респондентов (68%) считают самым эффективным средством противодействия DDoS гибридные решения (на стороне клиента с участием операторского решения либо распределенной сети). Никто из данной группы опрошенных не подтверждает эффективность решения CPE. Почти две трети опрошенных заявили, что пропускают трафик через внешнее решение постоянно или в случае возникающих инцидентов. Это вдвое больше, чем годом ранее.

Мария Попова

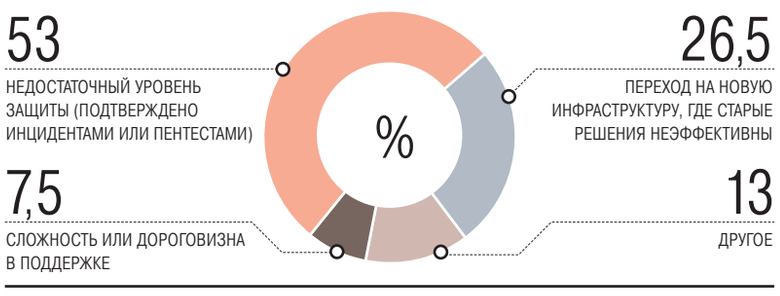
НАИБОЛЕЕ ВЕРОЯТНЫЕ ПОСЛЕДСТВИЯ ОТ ИНЦИДЕНТА ИБ (%)

ИСТОЧНИК: QRATOR LABS, 2017.



ПРИЧИНЫ ЗАМЕНЫ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ЗАЩИТЫ В БАНКАХ РФ

ИСТОЧНИК: QRATOR LABS, 2017.



БИЗНЕС МОЖЕТ БЫТЬ РАЗНЫМ,
НО ОБЯЗАН БЫТЬ
ЦИФРОВЫМ

реклама

Решения для цифровой трансформации бизнеса:
• оптимизация процессного управления
• сквозная интеграция бизнес-процессов
• управление цифровым контентом
• аналитика неструктурированных данных
• роботизированные системы

АйТи

+7 (495) 974-79-79
+7 (495) 974-79-80
115280, Москва, ул. Ленинская Слобода, д. 19, стр. 6
www.it.ru
info@it.ru

Одомашненный интеллект

— потребительский рынок —

с23

Просто избавиться от жуликов

Благодаря развитию технологий компьютерного зрения, применению нейронных сетей и принципов машинного обучения системы безопасности на основе камер видеонаблюдения становятся гораздо более эффективными.

Faceter — одна из систем, которая основана на использовании алгоритмов глубокого обучения, она умеет распознавать лица. Проект основали Роберт Посье, живущий в Йоханнесбурге, и Владимир Черницкий, наш соотечественник из Москвы. Система создана, чтобы снизить уровень преступности и повысить раскрываемость преступлений — весьма актуальная задача для ЮАР и многих других стран. Бета-версия программного обеспечения была разработана в 2016 году и уже прошла тестирование в пилотных проектах в сети пиццерий Debonairs Pizza и крупнейшей сети казино в ЮАР.

Сооснователь и технический директор Faceter Владимир Черницкий рассказал, что бизнес-клиенты и госслужбы могут применять Faceter для контроля доступа в офисы, специализированные помещения и закрытые территории. Домашние пользователи с помощью Faceter будут получать оповещения на смартфон о возвращении членов семьи домой, детекции незнакомцев вблизи жилища. Система может быть настроена на обнаружение источников возгорания, выявление нестандартного шума и прочее. Она умеет отслеживать конкретных людей от камеры к камере и распознавать их даже с изменениями в прическе, в солнцезащитных очках, с бородой или усами.

«Большая часть ПО для видеонаблюдения, которое есть на рынке, оперирует двумя параметрами: время записи и источник,— рассказал „Ъ“ Владимир Черницкий.— Это значит, что пользователь может просмотреть только то, что происходило в определенный момент времени на каждой из установленных камер. Faceter может составить картотеку офисных работников, членов семьи, посетителей ресторана, сформировать отчет о том, кто и когда попадал в область видимости камер, отследить каждый случай появления конкретного человека в определенном месте и выдать все нужные записи из архива. Faceter можно „научить“ реагировать на определенные события. Например, она может отправить СМС родителям, когда ребенок пришел из школы, и передать информацию через API в интегрированные системы».

В будущем Faceter научится распознавать цепочки событий и определять, если происходит что-то нестандартное, например драка, передача денег, похищение человека, взлом автомобиля. А также выявлять потенциально опасные объекты: пламя, спички, оружие, деньги. Предварительная стоимость сервиса — $10–15 в месяц.

Забота о близких

Создать систему для дома, которая могла бы обеспечить полную безопасность жильцов, — довольно сложная задача. Cherry home — одна из таких разработок, которая призвана заботиться обо всех, кто находится в доме. В следующем году система поступит в продажу, сейчас можно сделать предзаказ.

«Такая система должна, во-первых, различать, кто есть кто, и, во-вторых, понимать, что они делают. Сейчас на рынке нет решений, которые хоть сколько-нибудь надежно решали бы даже первую задачу. Например, человек ходил-ходил, потом упал на пол и перестал шевелиться — тогда система распознает это как потенциально опасную ситуацию и оповещает родных или специальные службы. Существующие системы охраны дома, видеонаблюдения и домашние ассистенты сейчас не могут надежно понимать и различать людей, которые находятся перед ними. Мы решили эту задачу. Это позволяет Cherry по-настоящему заботится о людях, а не только о помещении, в котором она установлена»,— рассказал Максим Гончаров, основатель проекта Cherry Labs.

Cherry home — это набор небольших квадратных блоков, которые монтируются на стене. В каждом из них — сенсоры, микрофоны и по паре камер. Программное обеспечение строит модель пространства, определяет в реальном времени, где находятся люди, распознает членов семьи, наблюдает за их движениями. Всех жильцов дома заранее представляют Cherry. Перечень возможных действий ограничен, но достаточен.

«Мы можем различать, лежит человек или стоит, двигается или не двигается, кричит он, смеется или плачет. Мы провели много тестов и хотели сделать систему заботы о семье так, чтобы человек, находясь вне дома, мог оставаться в контакте со своей семьей. Мы фокусируемся на тех, о ком супруги хотят заботиться вместе,— это дети или родители. Система понимает поведение детей и различает ситуации, в которых требуется внимание родителей. Причем не обязательно это что-то негативное: если дети смеются и бегают по комнате, это тоже важное для родителей событие»,— уточнил Максим Гончаров.

Вторая группа пользователей, которым пригодятся «умные» устройства,— пожилые люди. На рынке США уже есть решения, которые позволяют определить, упал человек или нет. В большинстве случаев это различные браслеты, которые надеваются на руку, или тревожные кнопки. Но, по мнению Максима Гончаров, пожилые люди не очень любят такие системы, потому что не хотят себя чувствовать беспомощными. К тому же об этих гаджетах нужно помнить: заряжать, брать с собой, выходя из дома.

Cherry home просто висит на стене. Режим видеозаписи может быть отключен. Система будет просто «понимать», что происходит, узнавать людей по пропорциям их тела (длина рук, ладоней, бедер, туловища, рост и пр.). Разработчики считают, что находиться под таким вниманием людям более комфортно, чем носить на себе тревожную кнопку или браслет.

Но стоимость Cherry home пока нельзя назвать доступной каждому. Стартовый набор из двух блоков для разных комнат и вычислительного модуля обойдется в $900. Этот пакет включает год предоставления сервиса, после окончания данного периода нужно будет платить $10–15 в месяц.

У Faceter и Charry Labs есть сильный конкурент — компания Nest, которая весной представила «умные» камеры Cam IQ. Напомним, что за компанией стоит еще более серьезная фигура: в 2014 году Nest Labs была куплена Google за $3,2 млрд. Команда начинала с производства «интеллектуальных» термостатов и детекторов дыма, давно работает с методами машинного обучения. Cam IQ стоит $299, сервис видеозаписи — $10 в месяц. Ни Faceter, ни Cherry Labs пока не начали активных продаж, и о сравнении технологий говорить рано.

Дом в безопасности

Защита имущества — еще одна насущная необходимость, с которой помогут новые технологии. Обычных камер видеонаблюдения недостаточно, чтобы избежать квартирных краж. Грабители проникают в дома, выводя из строя камеры или по старинке заклеивая дверной глазок, предварительно позвонив в дверь, чтобы убедиться, что за ней никого нет.

Четыре года назад для решения этой проблемы на рынке появился Ring — дверной звонок, который подключается к домашней сети Wi-Fi и в режиме реального времени транслирует видео всего происходящего на телефон владельца. Тот может ответить посетителю как будто из-за двери, даже находясь на другом краю света.

Позже разработчики добавили к системе солнечные панели, камеры слежения, детекторы движения, которые предупреждают об опасности, если их настроить на определенные зоны отслеживания, и сервис хранения видео в облаке. Записанное видео с незваным гостем можно пересмотреть в любое время в любом месте. Ring умеет взаимодействовать с Amazon Alexa. Умный дверной звонок можно купить по цене $179, $199, $249 или $499 в зависимости от качества встроенной камеры и прочего функционала.

В октябре на рынке появился еще один продукт для защиты от воров — Amazon Key. Это видеокамера и электронный замок стороннего производителя (Kwikset, Yale), который может открыть курьер, доставляющий посылку. Стоимость набора — $249,99. По замыслу компании курьер должен оставить коробку или конверт в помещении и удалиться. Пока не ясно, как будет продаваться такое решение: множество пользователей в социальных медиа высказали мнение, что ни за что не пустят чужака в дом даже под видеонаблюдением.

Как видно, на рынке технологий для дома уже довольно много игроков, среди которых и «голиафы», и начинающие стартапы, которые могут повторить библейскую историю пастуха Давида. Случится это или нет, станет ясно уже в ближайшие пару лет.

Кира Васильева

Тематическое приложение к газете «Коммерсантъ» («Информационные технологии»). Учредитель: АО «Коммерсантъ». Адрес: 127055, г. Москва, Тихвинский пер., д. 11, стр. 2. | **Владимир Желонкин** — генеральный директор АО «Коммерсантъ» | **Сергей Яковлев** — шеф-редактор АО «Коммерсантъ» | **Павел Кассин** — директор фотослужбы | **Рекламная служба:** Тел. (495) 797-6996, (495) 926-5262 | **Владимир Лавицкий** — руководитель службы «Издательский синдикат» | **Светлана Рагимова** — выпускающий редактор | **Ольга Еременко** — редактор | **Сергей Цомык** — главный художник | **Виктор Куликов, Наталия Коновалова** — фоторедакторы | **Екатерина Бородулина** — корректор | **Адрес редакции:** 121609, г. Москва, Рублевское ш., д. 28. Тел. (495) 797-6970, (495) 926-3301 | Ограничение: 16+