БЕЗОПАСНОСТЬ

КАК УЦЕЛЕТЬ В КИБЕР

Хочешь себя защитить — ни на кого не полагайся

Как любят шутить специалисты по кибербезопасности, существуют два типа организаций — те, которые уже пострадали от хакеров, и те, которые об этом пока что не подозревают. И, к сожалению, последние новости лишний раз подтверждают правоту этих слов. Например, компьютерным взломщикам удалось выкрасть у таких гигантов, как *Target*, *Home Depot* и *JPMorgan Chase*, всю информацию о кредитных картах вместе с персональными данными миллионов граждан. Но и это еще не все. Специалисты по кибербезопасности вдруг обнаружили фундаментальные изъяны в тех кирпичиках, из коих состоит Интернет, — вспомним хотя бы про ошибку *Heartbleed* в известном криптографическом пакете *OpenSSL*. А компания *Sony Pictures Entertainment* вообще была вынуждена вернуться к использованию шариковой ручки и бумаги после того, как злоумышленники нанесли по ее серверам массированный удар. В тот раз компьютерным мошенникам удалось получить доступ к персональной информации более чем 80 млн клиентов компании *Anthem*, которая занимается страхованием в сфере медицины. И это лишь наиболее известные примеры.

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- В ближайшие годы интенсивность кибератак увеличится, причем эта угроза нависла не только над правительствами и крупными корпорациями, но также над всеми, кто пользуется современными технологиями.
- Понятие кибербезопасности расширило свое толкование: теперь под ударом находятся не только секретная и прочая виртуальная информация, но и вполне реальные оборудование и устройства, инфраструктура и процессы — т.е. технологии, лежащие в основе нашей современной жизни.
- Поскольку государственные структуры и высокотехнологичные компании не в состоянии в одиночку обеспечивать безопасность киберпространства, необходимо создать коллективную «иммунную систему», неотъемлемой частью которой станут хакеры.
- Кроме того, свое веское слово должны сказать рядовые граждане. Каждый пользователь, подключенный к Сети, обязан внести свою лепту в создание коллективной «иммунной системы», практикуя своеобразный киберэквивалент личной гигиены.

ОБ АВТОРЕ

Керен Элазари (Keren Elazari) — израильский эксперт в области кибербезопасности; сотрудничала с ведущими производителями антивирусного ПО, государственными организациями и компаниями из списка *Fortune 500*. Ее выступление на конференции фонда *TED*, посвященное хакерам и собравшее более 1,2 млн просмотров, переведено на 24 языка и вошло в список самых новаторских идей *TED*.

ВОЙНЕ

Керен Элазари

В ближайшие годы интенсивность кибератак почти наверняка увеличится, и эта угроза, будто дамоклов меч, висит над всеми пользователями. В наше время почти каждый житель планеты так или иначе подключен к киберпространству (через мобильные телефоны, ноутбуки, корпоративные сети) — словом, все мы стали уязвимы. Заметим, что компьютерные сети, серверы, персональные компьютеры, виртуальные счета стали мишенью не только для преступников, но и для некоторых правительственных структур, которые любят держаться в тени. Получается, что любая корпоративная сеть, любой персональный компьютер легко может стать орудием в руках не только обычных хакеров, но и тех, кто шпионит в киберпространстве за деньгами налогоплательщиков. Зараженные компьютеры — тоже орудие; их с успехом можно использовать для проведения сетевых атак; в этом случае компьютеры становятся частью «ботнета» — зараженной сети, состоящей из «зомби»-устройств, которые на часок-другой берут напрокат хакеры для проведения *DoS*-атак и рассылки спама.

В ответ на подобные угрозы США и другие страны решили навести в виртуальной среде железный порядок, создав для этой цели множество всяких бюрократических структур и секретных агентств. Однако от подобного подхода толку не будет. Наоборот, он лишь способен усугубить ситуацию (о причинах мы расскажем ниже). Кибербезопасность напоминает здравоохранение, ведь важную роль в ее обеспечении тоже играют правительственные учреждения — что-то вроде медицинских центров по контролю и профилактике заболеваний в США. Однако даже правительственным структурам в одиночку, без помощи рядовых граждан, не под силу предотвратить эпидемии.

Виртуальные просторы

Когда мы говорим о защите виртуального пространства, то прежде всего следует иметь в виду, что единого, монолитного «киберпространства» не существует, поскольку оно представляет собой огромную и взаимосвязанную систему систем, которая постоянно развивается и эволюционирует. Чтобы лучше себе это уяснить, давайте вернемся к работам профессора математики из Массачусетского технологического института Норберта Винера, написанным полвека назад. В 1948 г. для названия новой научной дисциплины он позаимствовал у древних греков слово «кибернетика», определив его как «управление и связи в животном

и машине». В греческом языке словом *kibernētēs* называли кормчего, рулевого, который управлял судами, бороздившим Средиземное море. Таким образом, под киберпространством следует понимать множество взаимосвязанных между собой электронных и цифровых устройств, обеспечивающих управление и передачу информации между всей совокупностью технических средств, без которых наша современная жизнь просто немыслима. Киберпространство состоит из огромного множества систем, управляемых дистанционно, и технических средств связи начиная от инсулиновых дозаторов, использующих беспроводные соединения на определенных частотах, и заканчивая спутниками *GPS*.

С юридической точки зрения киберпространство — не публичная собственность (вроде международных вод или Луны), оно неподконтрольно государственным структурам, в том числе военному ведомству. Компьютерные сети и технологии, из которых состоит киберпространство, принадлежат транснациональным компаниям, обслуживающим все это огромное хозяйство.

Количество и разнообразие технологий, из которых состоит виртуальное пространство, растет быстрыми темпами. Так, по прогнозам компании *Cisco Systems*, занимающейся производством сетевых технологий, к 2020 г. к Интернету будет подключено 50 млрд устройств, бóльшая часть которых обслуживают потребности промышленности, в частности министерства обороны и аэрокосмического комплекса. При этом каждый новый девайс, подключенный к виртуальному пространству, становится потенциальной мишенью для киберпреступников, которые уже научились выявлять слабые звенья сети. Так, например, хакеры получили доступ к крупной американской розничной сети *Target*, взломав ее кассовые терминалы и похитив персональные данные о платежных картах миллионов клиентов. Однако сначала они выбрали более доступную цель — компанию *Fazio Mechanical Services* (одного из подрядчиков *Target*, занимающегося обслуживанием системы кондиционирования). То же самое сделали и китайские хакеры, которые, как считается, в 2011 г. нелегально просочились в компьютерные сети подрядчика Министерства обороны США — корпорации *Lockheed Martin*. Как им это удалось? Первым делом они вскрыли систему безопасности компании *RSA*, раздающей ключи шифрования корпорации *Lockheed Martin*. *RSA*, в свою очередь, пострадала всего лишь по той причине, что один из сотрудников материнской компании — *EMC* — взял да открыл полученный по почте безобидный с виду файл в формате *Excel*.

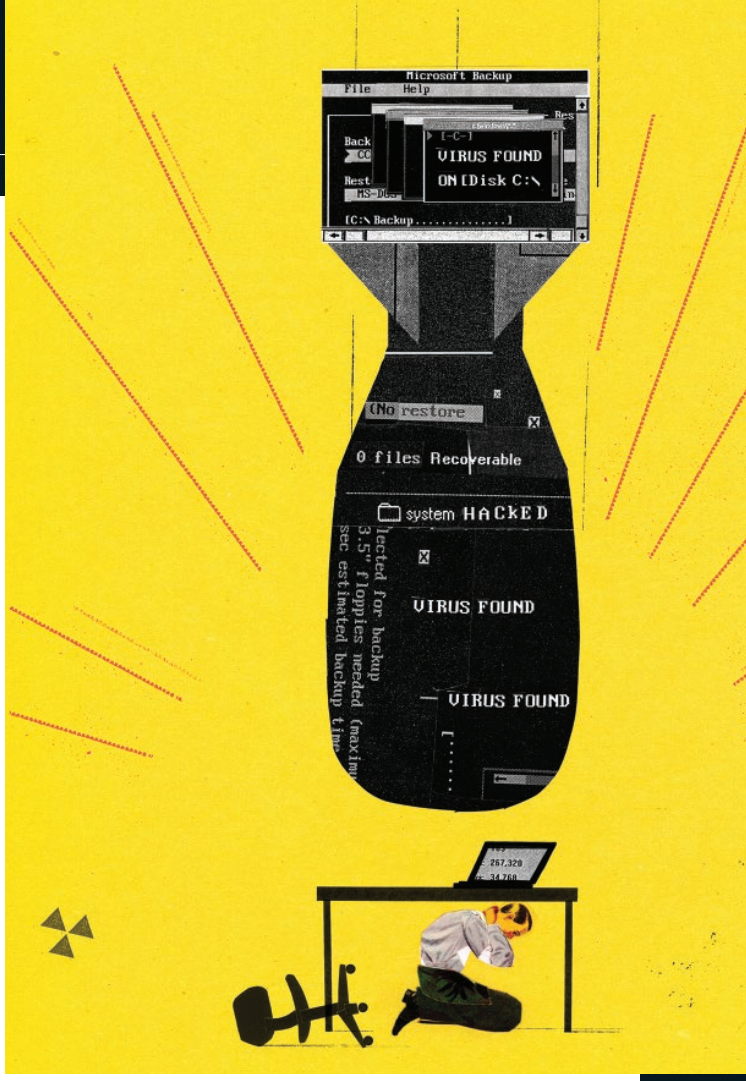

Illustration by Justin Renteria

Теперь перейдем к Интернету вещей, точнее — к составляющим его разнообразным устройствам и гаджетам (так называемым «вещам»). Каждый из таких объектов представляет собой не только своеобразное окно-лазейку, через которое научились проникать киберпреступники, но и самостоятельную мишень. Так, уже в 2008 г. специалисты по защите информации продемонстрировали, что хакеры спокойно могут получать несанкционированный доступ к имплантируемым электрокардиостимуляторам. С тех пор прошло несколько лет, и преступники отточили свое мастерство. Они научились через беспроводное соединение в удаленном доступе управлять имплантированным дозатором инсулина (напомним, что многие современные медицинские устройства, вживляемые в тело человека, комплектуются встроенным компьютером, который оборудован специальным модулем для обеспечения беспроводной связи). Получается, что злоумышленник теперь способен дистанционно управлять не просто имплантатами, а самой жизнью пациента.

Но и это еще не все. Под ударом оказалась также промышленная инфраструктура. Об этом мы все с ужасом узнали в 2010 г., когда выяснилось, что печально известный червь *Stuxnet* смог разрушить центрифуги на секретном заводе по обогащению урана в иранском городе Нетенз. Как полагают эксперты, *Stuxnet* стал плодом интенсивного и весьма дорогостоящего сотрудничества между США и Израилем. Этот червь ознаменовал собой начало новой эпохи: впервые в истории компьютерный вирус оказался способен нарушить работу аналоговых электронных устройств и разрушить промышленную инфраструктуру. Последовавшие следом виртуальные атаки еще раз продемонстрировали разрушительную силу беспощадных червей, подобных *Stuxnet*. И вот еще один пример: в декабре прошлого года Федеральное управление по информационной безопасности Германии сообщило о том, что хакерам удалось взломать систему управления печами на металлургическом заводе этой страны, что привело к отказу механизма отключения доменной печи и нанесло «огромный ущерб всему производству». А буквально за три месяца до этой диверсии китайские хакеры атаковали сайт Национального управления океанических и атмосферных исследований США *(NOAA)*, которое занимается метеонаблюдениями и прогнозом погоды.

Соответственно, в наши дни понятие «кибербезопасность» следует трактовать намного шире, нежели просто «обеспечение безопасности компьютеров, сетей, серверов» или же «обеспечение сохранности секретной информации» (*Google* и *Facebook* уже и так немало знают о каждом из нас). Основные силы нам следует направить на защиту устройств, образующих собой Интернет вещей, объектов инфраструктуры и процессов. Теперь опасность заключается в том, что технологии, которыми мы ежедневно пользуемся, могут в любой момент дать осечку и нарушить работу вполне реальных объектов — автомобилей, банкоматов, медицинской техники, электрических и телефонных сетей, спутников связи (а то и просто разрушить их). Как бы громко это ни прозвучало, но сегодня кибербезопасность поистине призвана защитить наш образ жизни.

Роль государства

Когда речь заходит о безопасности киберпространства, то здесь мы сразу видим неоднозначную роль государства. Не будем спорить, многие федеральные агентства США, включая Министерство внутренней безопасности, искренне заинтересованы в защите американских компаний и граждан от хакерских атак. Однако некоторые другие госструктуры совсем даже не прочь воспользоваться в своих целях любым уязвимым местом, которыми изобилует мировая Сеть. Например, секретные службы типа Агентства национальной безопасности (АНБ) тратят миллионы долларов на поиск разного рода дыр, намереваясь добраться через эти лазейки до конечных устройств и ПО, чтобы в итоге получить над ними контроль.

Любая уязвимость в системе безопасности — прекрасный подарок для злоумышленника. Взять хотя бы известную всем ошибку *Heartbleed*. Напомним, что в последние пять лет на компьютерах, как правило, используется криптографический пакет *OpenSSL*. *SSL* — это самый распространенный криптографический протокол, сообщающий пользователю о переходе на безопасный веб-сайт (вспомните иконку с изображением замка). Так вот, *Heartbleed* (буквально «Сердце, истекающее кровью») — это ошибка, засевшая, будто заноза, в одном из популярных расширений библиотеки *OpenSSL* под названием *Heartbeat* («Сердцебиение»); кстати, обратите внимание на схожесть названий *Heartbleed* и *Heartbeat*. С помощью уязвимости *Heartbleed* злоумышленник легко получает доступ к криптографическим ключам, именам пользователей и паролям, нейтрализуя любую систему безопасности, выстроенную на основе протокола *SSL*. И вот, представьте себе: *Heartbleed* тихо сидела в библиотеке *OpenSSL* на протяжении целых двух лет до тех пор, пока ее вдруг не обнаружили две независимые группы экспертов (одну из них возглавлял Нил Мехта (Neel Mehta), эксперт из корпорации *Google*, а другую — сотрудники финской компании *Codenomicon*). А уже через несколько дней *Bloomberg Businessweek* сообщал со ссылкой на анонимный источник, что, оказывается, АНБ в течение нескольких лет использовало лазейку *Heartbleed* для шпионажа.

Пришло время, и многие развитые государства мира стали выделять миллионы долларов и нанимать лучших специалистов для того, чтобы отлавливать компьютерные баги, похожие на *Heartbleed*, чтобы затем взять их в оборот для каких-то своих целей. Более того, госструктуры некоторых стран готовы неплохо платить за информацию о всяческих дырах и уязвимых местах в компьютерах, и с этой целью они даже стали выходить на международный уровень. Тем самым они поддерживают на плаву, если можно так сказать, «рынок уязвимостей», на поиске и продаже которых специализируются все больше компаний, таких, например, как

французская *Vupen Security* или американская *Exodus Intelligence* из Остина. Получается, что некоторые государства тратят больше средств на изучение и разработку наступательного, а отнюдь не оборонительного кибероружия. Скажем, Пентагон пользуется услугами целой армии специалистов, занятых выискиванием разного рода брешей; при этом АНБ стало выделять в два с половиной раза больше средств на разработку наступательного кибероружия по сравнению с оборонительным.

Однако из сказанного отнюдь не следует, что, мол, правительственные структуры стали эдакими врагами кибербезопасности, забрызганными грязью. Такие агентства, как АНБ, появились совсем не на пустом месте. Им поневоле приходится собирать секретную информацию, чтобы предотвратить террористические акты; для этой цели они просто вынуждены использовать любые эффективные инструменты. Вот почему, когда мы рассуждаем о роли государственных структур в поиске дыр и уязвимостей, необходимо сохранять объективность и учитывать не только побочные эффекты, но и рациональное зерно. Никогда нельзя забывать о той пользе, которую обществу могут принести только государственные структуры — и больше никто. Например, лишь государство имеет право заставить компании и прочие организации официально сообщать информацию о кибератаках.

Кибербезопасность подобна правилам личной гигиены: чтобы остановить эпидемию, нужно мыть руки перед едой и не забывать о прививках

От подобных мер выиграют, в частности, банки, поскольку атаки на финансовые учреждения в виртуальном пространстве, как правило, следуют по хорошо отработанному сценарию: оказалось, что преступники обычно применяют к разным банкам одни и те же методы взлома. Однако жертвы виртуального нападения не любят сообщать о том, что их атаковали, поскольку в этом случае клиенты решат, что банк вообще не способен обеспечить безопасность операций, и перестанут ему доверять. Вот почему банки совсем не горят желанием делиться с конкурентами информацией о хакерских атаках. Правда, в некоторых случаях им запрещает это делать антитрестовское законодательство — и вот именно здесь государство может сказать свое веское слово. Так произошло, например, в США, где был создан Центр анализа и обмена информацией о финансовых услугах *(FS-ISAC)*, цель которого — оказание содействия международным финансовым организациям. А в феврале нынешнего года президент Барак Обама подписал указ, призванный стимулировать обмен информацией о киберугрозах между компаниями.

Хакеры нам помогут

Уязвимости и дыры будут всегда — до тех пор, покуда существуют программы и программисты. В наши дни высокотехнологичные компании, подгоняемые рынком, с большой скоростью выбрасывают на прилавок все более совершенные гаджеты и девайсы. И вот именно эти компании решили задействовать весьма обширный человеческий ресурс — сообщество хакеров. Согласитесь, необычный ход. Уже в прошлом году хакеры и высокотехнологичные компании стали демонстрировать все больше готовности к сотрудничеству (и откровения Эдварда Сноудена лишь ускорили этот процесс). В наши дни сотни компаний и фирм вдруг осознали, что приглашать хакеров для работы в рамках так называемых программ поиска ошибок и уязвимостей очень даже полезно. Эти программы действительно стимулируют работу независимых специалистов, побуждая их предоставлять очень ценную информацию об уязвимостях и проблемах безопасности. Так, например, корпорация *Netscape Communications*, намереваясь выловить ошибки в своем веб-браузере *Netscape Navigator*, впервые объявила о подобной программе еще в 1995 г. И теперь, 20 лет спустя, мы видим, что меры, принятые этой корпорацией и ее преемником (компанией *Mozilla*) с целью укрепления безопасности, полностью себя оправдали. И теперь появилось множество частных и государственных сообществ, объединяющих профессионалов, которые обмениваются друг с другом информацией о вредоносных программах, угрозах и уязвимостях, — и все для того, чтобы выстроить своего рода коллективную «иммунную систему».

В наши дни киберпространство очень быстро расширяется, затягивая в свои сети даже тех, кто раньше не имел к нему никакого отношения. Теперь производителям автомобилей, медицинской техники, домашних развлекательных систем и всякой всячины придется многому поучиться у компаний, занимающихся кибербезопасностью. Теперь им придется самим оперативно решать вопросы безопасности уже на стадии исследований и разработок,

а не запоздало реагировать на правительственные предписания. Здесь нам большую пользу принесут хакеры. И вот в 2013 г. два специалиста по безопасности Джошуа Корман (Joshua Corman) и Николас Перкоко (Nicholas Percoco) решили к ним обратиться. Они основали движение под названием *I Am The Cavalry*, пытаясь убедить хакеров ответственнее подойти к исследованиям в области обеспечения безопасности, обращая повышенное внимание на такие важные области, как объекты инфраструктуры, автотранспорт, медицинская и бытовая техника. Кроме того, появилась консультативная группа под названием *BuildItSecure.ly*, у истоков которой стоят два выдающихся специалиста в области безопасности Марк Станислав (Mark Stanislav) и Зак Ланир (Zach Lanier). Цель этой группы — создание платформы для разработки безопасных приложений, используемых в Интернете вещей.

Коллективная иммунная система кибербезопасности крепнет буквально с каждым днем — и для экспертов в области безопасности это хорошая новость. Так, в январе корпорация *Google* в дополнение к своей программе поиска багов запустила еще одну программу, в соответствии с которой теперь будут выделяться гранты специалистам по безопасности с целью тщательного тестирования программных продуктов, выпускаемых корпорацией. На этом примере мы видим, что компании не только могут привлекать к работе своих специалистов, но и не прочь воспользоваться помощью хакеров. А правительства некоторых стран этот подход даже одобряют. Например, Центр обеспечения кибербезопасности Нидерландов запустил свою собственную программу, в соответствии с которой хакеры могут теперь сигнализировать об уязвимостях, не опасаясь уголовного преследования.

Однако, не обошлось и без ложки дегтя в бочке меда: подход администрации Обамы к вопросам кибербезопасности отчасти способен ужесточить меры в отношении тех, кто занимается поиском уязвимых мест, ослабив тем самым становление глобальной «иммунной системы». Многие эксперты по вопросам безопасности опасаются, что Закон США о компьютерном мошенничестве *(CFAA)* в нынешней редакции вместе с предложенными изменениями и дополнениями определяет «хакерство» настолько широко, что даже такое простое действие, как переход по ссылке на веб-сайт, содержащий сообщение, распространенное с помощью утечки, теперь может быть приравнено к торговле краденым. Если постоянно ужесточать меры в отношении независимых экспертов в области безопасности, то все наше общество проиграет, а настоящих преступников, пропитанных алчностью или антиобщественными идеями, закон по большому счету не заденет.

Каждый из нас в ответе

Ближайшие годы будут непростыми. Интенсивность кибератак возрастет. Можно ожидать, что с новой силой вспыхнут споры по поводу того, какой объем контроля над виртуальным пространством следует передать государству в обмен на гарантии безопасности. Понятно, что для охраны киберпространства необходимо привлекать специалистов в самых разных областях — технической, юридической, экономической, политической. Но и простые пользователи тоже несут свою долю ответственности: каждый гражданин должен требовать от компаний-производителей более серьезного отношения к обеспечению безопасности и надежности программных продуктов. Однако если государственные структуры не желают об этом беспокоиться, в результате чего общий уровень безопасности понижается, то граждане должны призвать их к ответу. Рядовой пользователь и сам обязан проявлять бдительность и заботиться о своей безопасности, поскольку из-за его беспечности может пострадать глобальная система безопасности.

Как себя защитить? Хотя бы регулярно обновлять ПО, использовать безопасные веб-браузеры, двухфакторную авторизацию электронной почты и аккаунтов социальных сетей. Кроме того, необходимо понимать, что любое устройство, применяемое обычными пользователями, — это маленький элемент глобальной системы, а посему наши вроде бы малозначительные действия способны привести к непредсказуемым последствиям. Иными словами, кибербезопасность подобна правилам личной гигиены: как говорится, чтобы остановить эпидемию, мой руки перед едой и не забывай о прививках. ■

Перевод: И.В. Ногаев

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ

■ Проблемы онлайн-безопасности (круглый стол) // ВМН, № 12, 2008 (Спецвыпуск: Превратности приватности).

■ War and Anti-War: Survival at the Dawn of the 21st Century. Alvin and Heidi Toffler. Little, Brown, 1993.

■ A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Edited by Jason Healey. Cyber Conflict Studies Association, 2013.

■ Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Kim Zetter. Crown, 2014.

■ TED's Who Are the Hackers? playlist: www.ted.com/playlists/10/who_are_the_hackers