Babr24.com

Автор: Артур Скальский ИНТЕРНЕТ И ИТ, МИР 3808 01.02.2013, 16:13 597

Киберугрозы выходят из тени

По данным Ежегодного отчета Cisco по информационной безопасности, интернет-привычки специалистов нового поколения усугубляют распространение опасных угроз.

Согласно результатам Ежегодного отчета Cisco по информационной безопасности (Cisco 2013 Annual Security Report, ASR) и глобального исследования Cisco Connected World Technology Report (CCWTR), информационная безопасность компаний становится уязвимой из-за того, что сотрудники стремятся к повсеместному использованию мобильных устройств, а граница между работой и личной жизнью все более размывается.

Исследование Cisco в области информационной безопасности развеяло популярный миф, согласно которому угрозы возникают главным образом тогда, когда пользователь занимается в сети не вполне приличными делами. Сегодня сетевые злоумышленники фокусируют внимание не столько на порнографических, фармацевтических и игровых сайтах, сколько на обычных сетевых ресурсах с массовой аудиторией, таких как популярные поисковые механизмы, розничные магазины и социальные сети. Более того, отчет Cisco показал, что вредоносный контент можно "подцепить" на сайтах интернет-магазинов в 21 раз чаще, а в поисковых механизмах - в 27 раз чаще, чем на сайтах, специально созданных хакерами. Так, вероятность загрузки вредоносного контента при просмотре онлайн-рекламы в 182 раза выше, чем на порнографических сайтах.

Информационная безопасность бизнеса попадает под угрозу во многом потому, что сотрудники предпочитают работать в привычной для себя манере, повсеместно используя одни и те же устройства и приемы – в офисе, дома, по дороге на работу и домой. Угрозы, создаваемые этой тенденцией, получившей название "консьюмеризация", усугубляются еще одним трендом, раскрытым в отчете Cisco Connected World Technology Report, где говорится о поведении сотрудников поколения «игрек». Большинство (91 процент) из них считают, что эпоха повышенного внимания к вопросам конфиденциальности личных данных безвозвратно ушла в прошлое. Треть поколения «игрек» вообще не задумывается о том, где и как хранится их персональная информация. Эти люди охотно сообщают личные данные, чтобы получить доступ в социальные сети. Более того, все больше специалистов из поколения «игрек» из разных стран предоставляют свои данные сайтам интернет-магазинов с большей готовностью, чем ИТ-отделам компании-работодателя, отвечающим за сохранность и защиту личных данных и устройств.

Окончив колледж и получив работу, представители поколения «игрек» испытывают на прочность корпоративную культуру и политику компании в области безопасности, требуя от работодателя свободы использования социальных сетей, личных устройств и методов мобильной работы. Предыдущие поколения никогда не выдвигали подобных требований. С утра, не вылезая из постели, большинство молодых людей поколения «игрек» заходят в социальные сети, работают с электронной почтой и текстовыми сообщениями (так поступают трое из четырех опрошенных во всех странах, где проводилось исследование). Почти половина респондентов выполняет похожие задачи за обеденным столом, треть - в ванной и одна пятая – за рулем автомобиля. Этот стиль жизни все шире распространяется в корпоративной среде, определяя будущее рабочей среды и новые параметры поиска талантливых сотрудников. К сожалению, исследование показало, что интернет-привычки нового поколения сотрудников создают серьезные угрозы безопасности, с которыми компании никогда раньше не сталкивались.

Основные выводы исследований

Вредоносные программы для ОС Android

• В 2012 году число заражений вредоносными программами для операционной системы Android выросло на 2 577 процентов (ASR).

• При этом доля мобильных вредоносных кодов составляет всего 0,5 процента от общего объема вредоносных кодов в Интернете (ASR).

• Эти тенденции приобретают особое значение ввиду того, что для поколения «игрек» смартфоны стали самым популярным устройством, использующимся чаще, чем ноутбуки, персональные и планшетные компьютеры (CCWTR).

Распространение вредоносных интернет-кодов в разных странах

В 2012 году географический ландшафт интернет-угроз претерпел значительные изменения. В 2011 году Китай занимал второе место в списке стран, наиболее пораженных вредоносными кодами. В 2012 году Китай опустился на шестое место. Скандинавские страны (Дания и Швеция), наоборот, поднялись в этом списке на третью и четвертую позицию соответственно. Первую строчку в списке по-прежнему занимают Соединенные Штаты, где происходит 33 процента заражений вредоносными интернет-кодами (ASR).

Тенденции в области спама

• За период с 2010 по 2011 год объем спама уменьшился на 18 процентов. При этом спамеры стали переходить на «стандартную рабочую неделю» (объем спама в выходные дни сократился на 25 процентов) (ASR).

• В 2012 году большинство спам-сообщений передавалось в рабочие дни. Самым «активным» днем с точки зрения спама, стал вторник (ASR).

• Главным мировым источником спама является Индия. В 2011 году США заняли в этом списке шестое место, а в 2012 году - второе. Третье, четвертое и пятое места заняли, соответственно, Корея, Китай и Вьетнам (ASR).

• Главные цели спамеров, на сегодняшний день, - это реклама фармацевтических средств, таких как Виагра и Cialis, и наиболее фешенебельных марок наручных часов (Rolex и Omega) (ASR).

Защита личной информации

Для оценки влияния угроз информационной безопасности на бизнес, Cisco исследовала поведенческие шаблоны сотрудников поколения «игрек», стремящихся постоянно быть на связи и иметь мгновенный доступ к необходимым приложениям.

• Хотя большинство опрошенных представителей поколения «игрек» (75 процентов) не доверяет веб-сайтам и не считает их надежными хранилищами личной информации, такой как номера кредитных карт и личные контактные данные, недоверие не накладывает никаких ограничений на действия этих пользователей. Они готовы идти и идут на риск, надеясь на "авось" и используя при этом рабочие устройства, подключенные к корпоративной сети, что создает большие проблемы для компаний-работодателей (CCWTR).

• 57 процентов представителей поколения «игрек» не возражают против использования их личной информации розничными магазинами, социальными сетями и другими онлайновыми ресурсами, если это приносит какую-то выгоду или удобство (CCWTR).

Выполнение корпоративных ИТ-правил (политик)

• Девять из десяти (90 процентов) опрошенных ИТ-специалистов указали, что в их компаниях имеются официальные правила использования на работе тех или иных устройств, однако лишь двое из пяти представителей поколения «игрек» знают об этих правилах (CCWTR).

• Хуже того, четверо из пяти сотрудников из поколения «игрек», знающих о корпоративных правилах, не придерживаются этих правил в своей повседневной работе (CCWTR).

• ИТ-специалисты знают, что многие сотрудники не выполняют правил, но не представляют себе масштаба бедствия. Более половины (52 процента) ИТ-специалистов в разных странах считают, что в общем и целом правила безопасности все-таки выполняются. При этом трое из четырех (71 процент) сотрудников из поколения «игрек» правил не выполняет (CCWTR).

• Двое из троих (66 процентов) опрошенных из поколения «игрек» во всех странах заявили, что ИТ-специалисты не имеют права следить за их поведением в сети, даже если это поведение связано с использованием корпоративных устройств в корпоративных сетях (CCWTR).

• Неприятие мониторинга сетевого поведения со стороны корпоративного ИТ-отдела оказалось намного выше,

чем неприятие такого же мониторинга со стороны розничных магазинов. Другими словами, поколение «игрек» гораздо спокойнее относится к отслеживанию работы в сети со стороны совершенно незнакомых лиц (сотрудников розничных магазинов), чем со стороны ИТ-специалистов компании-работодателя, то есть тех, кто по долгу службы обязан защищать сотрудников и корпоративную информацию (CCWTR).

Всеобъемлющий Интернет и безопасность в будущем

В настоящее время самой актуальной тенденцией развития сетей во всем мире считается создание Всеобъемлющего Интернета (Internet of Everything). Чем больше людей, физических объектов и устройств подключается ко "всемирной паутине", тем больше данных передается по корпоративным и операторским сетям. В результате возникают новые зоны уязвимости, требующие более внимательного подхода к вопросам информационной безопасности.

• Число сетевых соединений типа "машина-машина" (M2M) растет в геометрической прогрессии не по дням, а по часам. Оконечных устройств становится все больше, причем возрастает число не только привычных мобильных устройств, ноутбуков и настольных ПК. Возникают соединения типа "каждый с каждым", при которых любое устройство может подключиться к любому облаку или приложению по любой сети.

• К 2020 году, когда к Интернету подключится около 50 млрд физических объектов, количество сетевых соединений вырастет до гигантской цифры в13 квадриллионов (а точнее, 13 311 666 640 184 600). Подключение каждого нового устройства будет увеличивать число сетевых соединений еще на 50 миллиардов.

• Новые сетевые соединения будут генерировать огромные объемы мобильных данных, которые нужно будет оценивать и защищать в режиме реального времени. Мгновенная оценка данных поможет принимать корректирующие действия до того, как хакер, взламывающий сеть, получит полный контроль над ней и сможет нанести непоправимый вред.

• Для специалистов по сетевой безопасности это означает переход к защите любого контента и перенос внимания с оконечных устройств на сетевую периферию.

Информация об исследованиях Cisco

Ежегодный отчет Cisco по информационной безопасности перечисляет самые важные тенденции в данной области, проявившиеся в течение года, и предлагает полезные советы и рекомендации, повышающие уровень безопасности корпоративной технологической среды. Глобальное исследование Cisco Connected World Technology Report дает более подробный анализ угроз, перечисленных в отчете по вопросам безопасности.

В третьем ежегодном отчете Cisco Connected World Technology Report публикуются результаты исследования, проведенного по заказу Cisco независимой аналитической компанией InsightExpress из США. В ходе исследования опрашивались две группы респондентов. Одна состояла из студентов колледжей и молодых сотрудников в возрасте от 18 до 30 лет. Во вторую группу входили ИТ-специалисты, работающие в разных отраслях и разных странах. Всего было опрошено 3 600 респондентов (по 100 респондентов из 18 стран для каждой из двух групп). Исследование проводилось в 18 странах: США, Канаде, Мексике, Бразилии, Аргентине, Великобритании, Франции, Германии, Нидерландах, России, Польше, Турции, ЮАР, Индии, Китае, Японии, Южное Корее и Австралии.

Автор: Артур Скальский © Babr24.com ИНТЕРНЕТ И ИТ, МИР 3808 01.02.2013, 16:13 597
URL: https://babr24.com/?ADE=111852 Bytes: 10763 / 10700 Версия для печати

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта