Серия для руководителей

Security Essentials для ИТ-директоров

Уверенное использование инноваций

IBM

Ежедневно в корпорации поступают новые потоки данных, заставляя применять имеющийся на данный момент анализ и принимать более разумные решения. Сотрудники компании, клиенты и подрядчики — все тесно взаимосвязаны множеством технологий, как никогда раньше. При этом такие разрастающиеся и накладывающиеся друг на друга сети создают большие проблемы в плане безопасности. Сложность просто ошеломляет, и количество возможных точек атак практически безгранично. ИТ-директоры (CIO) постоянно борются с растущим количеством нарушений и возникающих вопросов. Можно ли обеспечить высокий уровень безопасности в эру «гиперсоединений»? Ответ — да, но это требует фундаментальных перемен в процессах и поведении. Компания IBM внедрила свою собственную стратегию внутри компании и определила десять основных условий, необходимых для обеспечения безопасности в XXI веке.

Когда в Нью-Йорке восходит солнце, вице-президент по продажам встает с постели, включает свой смартфон и видит, что в Малайзии внезапно появилась возможность крупной сделки. Эта новость порождает целый ряд коммуникаций. Перед завтраком шесть членов международной команды проводят телеконференцию, при этом один из них общается по Skype из Стокгольма. Три подрядчика звонят на мобильные телефоны. В течение дня электронные письма несколько раз огибают Землю, при этом около половины из них — в корпоративной сети, а остальные — Gmail и Yahoo. К тому моменту, когда в Нью-Йорке наступает вечер, сделка уже закрыта. В течение нескольких следующих часов некоторые участники этого события добавляют друг друга в друзья на LinkedIn.

91%

пользователей корпоративных смартфонов подключается к корпоративной электронной почте, но только от одного из трех требуют установить защитное программное обеспечение для мобильных устройств.

Источник: Лаборатория Касперского
http://usa.kaspersky.com/sites/usa.kaspersky.com/files/Enterprise%20Mobile%20Survey.pdf

Не секрет, что сегодня руководители могут мгновенно привлекать интеллектуальную мощь и гигабайты данных и использовать их для принятия более быстрых и гораздо лучших взвешенных решений. Однако эти самые сильные стороны взаимосвязанных сетей, их скорость и открытость, и быстрый доступ из любой точки мира, также делают их уязвимыми. И работа по защите корпоративной сети становится бесконечно сложной: информация буквально выливается из тысяч устройств и через десятки общественных веб-ресурсов. Исследование, проведенное Лабораторией Касперского, показывает, что 91% пользователей корпоративных смартфонов подключается к корпоративной электронной почте, но только от одного из трех требуют установить защитное программное обеспечение для мобильных устройств. В таких условиях доступ становится простым для всех заинтересованных — и в число таких «заинтересованных» зачастую входят преступные организации.

Преступные организации теперь рассматривают подключенные к Интернету компьютеры и мобильные устройства как превосходную недвижимость, первоочередной актив. Заражая устройства сложным в обнаружении вредоносным ПО, они расширяют свою операционную базу. Для воров корпоративные сети битком набиты цифровыми сокровищами, включая пароли, идентификаторы пользователей, бизнес и персональную информацию. Цифровые взломщики также нацеливаются на стратегические

активы, от государственных министерств до сетей связи. Выход из строя некоторых таких активов может разрушить бизнес-деятельность. По оценке Gartner, от 20 до 30 процентов компьютеров потребителей взломаны ботнетами и вредоносным ПО, которые могут использоваться как инфраструктура для криминальной деятельности. С учетом того, что многие фирмы задумываются о возможности использования личных устройств в корпоративных целях, потенциальное заражение является крайне насущной проблемой.

20–30%

компьютеров потребителей заражены вредоносным ПО и работают на преступников «на полставки».

Источник: http://www.computerweekly.com/opinion/CW-Security-Think-Tank-How-to-prevent-security-breaches-from-personal-devices-in-the-workplace

Один-единственный зараженный компьютер может стать причиной серьезного ущерба. Одним из наиболее ярких современных примеров является Stuxnet, крайне изощренный «червь», созданный для разрушения промышленного программного обеспечения и оборудования. Весной 2009 г. «червь» начал распространяться по компьютерам, большая часть которых находилась в Иране. Кто-кто, казалось, занес его через зараженный флэш-накопитель. «Червь» был создан, чтобы поражать машины, на которых было установлено ПО Siemens, и ему удалось посеять разрушение во множестве промышленных и корпоративных систем.

Уроки, которые могут извлечь из этой ситуации руководители по корпоративной безопасности, очевидны. Если «червь» может проделать себе путь в надежно защищенной отрасли в Иране или еще где-то, насколько легче ему будет найти «дыру» в раскиданной по всему миру армии профессионалов, использующих Tweeter, Facebook, смс-сообщения и Skype. И что еще страшнее, если один «червь» может выводить из строя промышленное оборудование, то не смогут ли другие разорвать цепочки снабжения, изменить маршруты транспорта, повредить электросети и вызвать другие катастрофы? Одним словом — смогут.

Чтобы справиться с растущей сложностью этих задач, корпорациям требуется новое **поколение руководителей по безопасности**. Естественно, они должны уметь справляться с бесчисленными технологическими угрозами, но также и быть способными решать стратегические задачи. Какая информация может быть широко распространена? Кто может иметь доступ к определенным сокровищам, и как их следует охранять? Вместе технические и стратегические задачи составляют обескураживающую сложность. И хотя может появиться искушение отреагировать на всю эту проблему столь же сложным решением, дальновидные руководители понимают, что такая эскалация необоснована, недоступна и, наконец, бесполезна.

Единственным верным ответом является изменение способа ведения деятельности компании, на фундаментальном уровне. Оно начинается с **расширения целей безопасности предприятия** от масштаба технического персонала и их машин до каждого человека в компании и до каждого, кто с ней сотрудничает. Это единственно логичное решение: поскольку любой человек может нести потенциальную угрозу взлома, каждый также должен быть частью решения. В конце концов, успех зависит от создания серьезной и постоянной осведомленности: **культуры осведомленности о рисках**.

Культура осведомленности о рисках требует больше, чем просто наличие современных технологий, и выходит далеко за рамки просто «передовых практик». Она представляет собой новый способ мышления, способ, в котором прагматический подход к безопасности используется при принятии каждого решения, каждой процедуры на каждом уровне компании. Она должна изменить способ, как люди обращаются с информацией, начиная от руководителей высшего звена и заканчивая летними стажерами. В такой культуре процедуры обеспечения безопасности данных становятся основной необходимостью, почти как пристегивание ремня безопасности в автомобиле или хранение спичек в безопасном месте.

Она представляет собой новый способ мышления, способ, в котором прагматический подход к безопасности используется при принятии каждого решения, каждой процедуры на каждом уровне компании.

Это не то решение, которое можно отложить. Безопасность предприятий быстро приближается к переломному моменту. Задумайтесь о следующих элементах. В том, что касается криминальных организаций, профессионалы поглотили дилетантов. Это увеличивает угрозу. В то же время, компании увеличили свою производительность и уполномочили работников распространять большие объемы цифровых данных об операциях, маркетинге, продажах и обслуживании клиентов. Это увеличивает уязвимость. И, поскольку практически все бизнесы компаний сейчас управляются цифровыми способами, последствия взлома могут нанести вред всей фирме. В сумме имеем: воры более искусны, у них есть бесчисленное количество цифровых лазеек для проникновения, а внутри в тайнике хранится что-то поистине бесценное.

Когда ставки высоки, путь к безопасности может оказаться сложным и непонятным. Хотя на рынке сегодня нет недостатка в продуктах и услугах по обеспечению безопасности, наши клиенты часто говорят нам, что разочарованы рынком обеспечения безопасности они мечутся от заголовка к заголовку в поисках актуальной информации в свете последнего кризиса безопасности или требований нормативов. Многие не знают, с чего начать или во что верить, и часто описывают безопасность и соответствие требованиям нормативов как инвестицию с невыраженной количественной стоимостью, сомнительным возвратом вложенных средств (ROI), а всю концепцию — как «лежачего полицейского» на скоростной трассе. Такое недопонимание часто ведет к нерешимости — или, что еще хуже, к решению отказаться от инноваций, основанному на страхе.

Не нужно много рассказывать о факте, что обеспечение безопасности предприятия — это огромное дело, которое никогда не бывает завершенным. Вдобавок, изменять культуру тяжело. Однако эта работа крайне важна. Надежная безопасность — это залог сохранения бизнеса, и она находится в пределах досягаемости.

Мы в компании IBM постоянно стараемся отыскать баланс между необходимостью инновации и потребностью контролировать риски. Универсальный ответ компании включает в себя технологию, процесс и меры политики. Он включает в себя десять основных практик. В течение следующих месяцев мы распространим ряд официальных документов, где вы сможете ознакомиться с ними подробнее. А сейчас приведем краткое резюме:

Наши основные практики в области обеспечения безопасности

1. Создание культуры осведомленности о рисках
Идея очень проста. Каждый человек может нанести вред компании, открыв сомнительное вложение или не установив на смартфон обновление для системы безопасности. Поэтому в работе по созданию защищенного предприятия должен участвовать каждый. Построение культуры осведомленности о рисках включает в себя описание рисков и целей и повсеместное распространение информации о них. Но самое важное изменение касается культуры. Подумайте о спонтанной реакции, об ужасе, который многие испытывают, когда видят, что родитель болтает по мобильному телефону, пока ребенок бежит по улице. Такая же нетерпимость должна существовать на уровне компании, когда люди видят, что их коллеги не заботятся о безопасности. Руководство, конечно, должно неустанно продвигать это изменение с самого верха вниз, одновременно внедряя инструменты для контроля прогресса.

2. Управление нарушениями и реагирование на них
Предположим, произошли два похожих нарушения безопасности, одно в Бразилии, другое — в Питтсбурге. Они могут быть связаны. Однако при отсутствии соответствующих мощностей службы безопасности, необходимых, чтобы связать эти два происшествия, важная особенность — которая могла бы указать на потенциальное нарушение — может остаться незамеченной. Крайне важны усилия в масштабе компании по внедрению средств интеллектуального анализа и автоматического реагирования. Создание автоматизированной и унифицированной системы позволит предприятию отслеживать свою деятельность и быстро реагировать в случае необходимости.

3. Защита рабочего места
Киберпреступники постоянно зондируют слабые места. Каждая рабочая станция, ноутбук или смартфон представляют собой потенциальную «лазейку» для вредоносных атак. Настройки каждого такого устройства не должны быть оставлены на отдельных лиц или автономные группы Они должны подлежать централизованному управлению и принудительному выполнению необходимых процедур. Все потоки данных на предприятии должны быть классифицированы, для каждого из них следует составить собственный профиль рисков и направлять исключительно в его круг пользователей. Обеспечение рабочей силы безопасностью означает победить хаос и заменить его уверенностью.

4. Безопасность при разработке
Представьте себе, что автомобильные компании изготовили свои автомобили без ремней безопасности и воздушных подушек, а потом добавили их позднее, после несчастных случаев или аварий. Это было бы бессмысленно и одновременно чрезвычайно дорого. Аналогичным образом, одно из самых крупных уязвимых мест информационных систем, а также трат денег, возникает из-за того, что сначала внедряются сервисы, а безопасность для них добавляется потом. Единственным решением является создавать безопасность с самого начала и проводить регулярные автоматические испытания для отслеживания соблюдения нормативов. Это также экономит деньги. Если внедрение функции обеспечения безопасности в приложение стоит дополнительные 40 фунтов стерлингов, добавление ее позднее может обойтись в 100 раз дороже — 4000 фунтов стерлингов.

5. Поддержка чистоты
Это случается все время. Люди держатся за старое программное обеспечение, потому что они его знают, и им с ним удобно. Однако управление обновлениями для множества разных программ может стать практически невозможным. Кроме того, компании-разработчики ПО иногда перестают устранять неисправности старых программ. Киберпреступники также хорошо это знают. В безопасной системе администраторы могут отследить каждую запущенную программу, могут быть уверены, что она последней версии, и имеют универсальную систему для установки обновлений и исправлений сразу после их выхода.

6. Управление сетевым доступом
Подумайте о городской преступности. Работа полиции станет гораздо проще, если на каждом транспортном средстве в городе будет закреплен уникальный радиомаркер, а перемещаться можно только по небольшому количеству магистралей, каждая из которых оснащена датчиками. То же самое необходимо и для данных. У компаний, которые направляют зарегистрированные данные через отслеживаемые точки доступа, своевременное распознавание и изолирование вредоносного ПО происходит гораздо легче.

7. Безопасность в облаках

Облачные вычисления обещают невероятную эффективность. Однако она связана с некоторым риском. Если предприятие переводит определенные ИТ-сервисы на облачные вычисления, они окажутся в непосредственной близости от многих других, в число которых, возможно, входят мошенники. В этом смысле облако напоминает отель, в котором определенный процент постояльцев заражен. Чтобы суметь хорошо жить в этих условиях, у гостей должны быть инструменты и процедуры для изолирования себя от других и для отслеживания возможных угроз.

8. Патрулирование по соседству

Предположим, подрядчику нужен доступ к системе. Как вам убедиться в обеспечении системы правильными паролями? Записать их в блокнот? Послать их текстовым сообщением? Такая импровизация рискованна. Культура безопасности предприятия должна распространяться за пределы стен компании и также внедрять лучшие практики среди подрядчиков и поставщиков. Этот процесс сходен с процессом внедрения контроля качества, который был поколение назад. И логика такая же: безопасность, как и превосходное качество, должна внедряться во всю экосистему целиком. Разрушительные эффекты небрежности в одной компании могут потрясти целые секторы общества.

9. Защита «сокровищ» компании

Иногда в «сокровищнице» компании хранятся критически важные сокровища, возможно, ее научные и технические данные, возможно, некоторые документы, имеющие отношение к слияниям и поглощениям, или личная финансовая информация клиентов. Каждое предприятие должно провести инвентаризацию, в соответствии с которой критические данные получают специальное обращение. Каждый приоритетный элемент следует защищать, отслеживать и шифровать, как если бы от него зависело выживание компании. В некоторых случаях так оно и есть.

10. Отслеживание «кто есть кто»

Предположим, сотрудницу, работавшую по контракту, наняли на полный рабочий день. Прошло шесть месяцев, и она получает повышение. Годом позже внезапно появляется конкурент и нанимает ее. Как должна система в течение этого времени относиться к такому человеку? Сначала система должна предоставить ей ограниченный доступ к данным, потом предоставить больше возможностей и, наконец, отрезать ей доступ полностью. Таков жизненный цикл управления идентичностью. Он жизненно необходим. Компании, которые плохо управляют этим циклом, действуют неосознанно и могут быть уязвимы для проникновений. Этот риск можно снизить, внедрив системы тщательной идентификации людей, управляя разрешением и запретом на доступ сразу после их ухода.

Как мне максимально использовать инновации и сохранить уверенность?

Баланс между управлением риском и внедрением инноваций

Присоединяйтесь к беседе

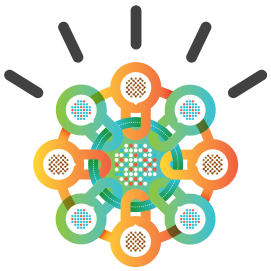
Чтобы прочесть другие статьи, узнать больше или поделиться своими мыслями с другими руководителями, ответственными за безопасность, присоединяйтесь к нам на **ibm.com/smarter/cai/security**.

Об авторе

Кристин Лавджой (Kristin Lovejoy) является вице-президентом по вопросам ИТ-рисков, офис ИТ-директора, IBM. Связаться с ней можно по адресу: **klovejoy@us.ibm.com**.

О Центре прикладных знаний IBM

Центр прикладных знаний IBM объединяет в себе глубокий аналитический опыт и знания, которые могут помочь клиентам выработать курс к новым преимуществам. Центр проводит исследования и создает активы и инструменты, а также практические рекомендации, побуждающие организации действовать.



IBM Восточная Европа/Азия
123317, Москва
Краснопресненская наб., 18
Тел.: +7 (495) 775-8800, +7 (495) 940-2000
Факс: +7 (495) 940-2070

CIE03116-RURU-00