BIZ KV:A КОМПЬЮТЕРНЫЕ ВЕСТИ www.kv.by

No. 003 (3)
31 августа 2012 года

ООО “РГ “Компьютерные Вести” • Тираж: 11220 экз. • Адрес: Минск, ул. Мельникайте, 2, оф. 710 • E-mail: info@kv.by • Тел. редакции (017) 203-90-10 • Размещение рекламы: adv@kv.by

Защита ноутбуков от утечек информации

Почему уходит сисадмин?

Страхование рисков ИТ-компаний при работе с зарубежным заказчиком

Многофакторная аутентификация

Социальные ресурсы

Учебный центр IBA:
Учиться Cisco никогда не поздно

Ни в одной другой отрасли знания не ценятся так, как они ценятся в ИТ. А что может быть лучше знаний, полученных непосредственно из первых рук, особенно если эти знания подтверждаются международными сертификатами? Авторизованные учебные курсы, не только дающие знания в области технологий, но и готовящие к сертификации, давно перестали быть диковинкой для жителей Беларуси. Вот и курсы Cisco, для прохождения которых ещё недавно нужно было ехать за пределы нашей страны, успешно изучаются в Учебном центре компании IBA.

Сотрудничество Учебного центра IBA и Cisco началось довольно давно — ещё в 2008-м году. Именно тогда на его базе открылась Академия Cisco, ставшая третьей по счету в Республике Беларусь. Несколько лет спустя, в 2010, году Учебный центр IBA стал Cisco Learning Partner Associate — партнером компании Cisco по обучению с компетенцией базового уровня. А уже в 2011-м году — Центром поддержки Академий Cisco и Центром обучения инструкторов. Только шесть из белорусских академий Cisco сегодня могут похвастаться подобным статусом.

На сегодняшний день Учебным центром IBA взята новая высота: сегодня это единственный в Беларуси учебный центр, который имеет статус как Академии Cisco, так и Авторизованного учебного центра Cisco с правом проведения обучения как по программам академии Cisco, так и по авторизованным “коммерческим” курсам. Что это означает? Дело в том, что стать специалистом в области Cisco можно двумя путями: закончить академию Cisco, либо пройти курсы по той же программе. Первый вариант предусматривает занятия в очно-заочном режиме в течение 6 месяцев, всего 280 учебных часов. Второй — это интенсивное изучение той же программы в течение пяти (десяти) дней, по восемь академических часов ежедневно.

Впрочем, конечно, главное в работе учебного центра — не завоеванные им регалии, а то, какие знания можно в нем получить. Учебный центр компании IBA сегодня проводит обучение по полному спектру академических курсов Cisco, включая курсы и сертификацию по программам CCNA, CCNP (Cisco Routing&Switching), по информационной безопасности CCSP, дизайну и проектированию сетей, технологиям Voice (CCVP), технологиям Service Provider CCIP. Обучение проводят преподаватели, успешно прошедшие сертификацию самой компанией Cisco. Сегодня в Учебном центре IBA работают два сертифицированных тренера по курсам Cisco и один инструктор академии. Именно они позволяют преодолеть все сложности и подводные камни, которые стоят на пути слушателя курсов, и помогают ему получить заветный сертификат международного образца.

В ходе обучения слушатели получат не только теоретические знания, но и массу практических навыков благодаря обширному циклу лабораторных и практических занятий. В отличие от других учебных центров, в IBA слушатель имеет возможность работать непосредственно с оборудованием производства компании Cisco, и иметь к нему прямой, а не удаленный доступ.

Высокое качество знаний, получаемых в Академии Cisco Учебного центра IBA, подтверждается теми высокими результатами, которые её выпускники демонстрируют на международных олимпиадах, проводимых среди слушателей курсов Cisco. В этом году Николай Петров, студент академии Учебного центра IBA по программе CCNA, занял второе место в престижном соревновании NetRiders CCNA-2012 в рамках Сетевых академий Cisco стран СНГ. Кроме того, в 2011 году на базе самого Учебного центра IBA прошла первая в Беларуси Олимпиада Cisco по сетевым технологиям для студентов.

> **“Учебный центр IBA — единственный в Беларуси учебный центр, который имеет статус как Академии Cisco, так и Авторизованного учебного центра Cisco с правом проведения обучения как по программам академии Cisco, так и по авторизованным “коммерческим” курсам.”**

За годы работы Учебного центра IBA через авторизованные программы обучения Cisco прошло множество специалистов из разных белорусских компаний. Сегодня бывшие студенты курсов успешно применяют полученные на них знания в Национальном банке Республики Беларусь, Белгазпромбанке, Белагропромбанке, Белгосстрахе, ЗАО “Второй национальный телеканал”, ЗАО “Атлант”, ОАО “Мапид”, ОАО “Лукойл”, Viaden Media, СООО “НТС”, ООО “Деловые технологии”, РУП “Белтелеком” и других предприятиях и организациях.

Таким образом, результаты работы Учебного центра IBA говорят сами за себя. Выбор, где изучать учебные программы Cisco, конечно, за вами, но лучше учиться у лучших, не так ли?

Страхование рисков ИТ-компаний при работе с зарубежным заказчиком

Вадим СТАНКЕВИЧ

Любая компания в любой сфере бизнеса всегда подвержена ряду рисков. ИТ-компания, реализующая какой-либо проект для заказчика, не является исключением. Для минимизации рисков в мировой практике применяют такой инструмент, как страхование, который позволяет защититься от различных форс-мажоров.

Страхование ИТ-рисков как таковое

Вообще говоря, страхование в ИТ в развитых странах — вещь более чем распространенная и хорошо развитая, как, впрочем, и сами информационные технологии. Ведь риски в ИТ возникают не только там, где есть заказчик и подрядчик, которые пытаются договориться и создать ИТ-систему или программный продукт. Риски, связанные с ИТ, несет любая организация: это риск потери информации или её утечки, риск остановки бизнес-процессов из-за аппаратного или программного сбоя, риск заражения вредоносными программами... От всего этого западные компании успешно страхуются, а вот на постсоветском пространстве пока такого рода страхование в диковинку.

К сожалению, и в России, и в Беларуси, и в других странах, за исключением, пожалуй, Прибалтики, пока о развитии подобного рода страхования говорить не приходится. Не то чтобы на него не было спроса — здесь препятствием являются, скорее, сами страховщики. Они находят множество препятствий для включения подобного вида страхования в свои пакеты услуг.

Первая причина — это необходимость определения вероятности наступления страхового события для расчета страховых тарифов. Вполне понятно, что для её определения нужно, как минимум, знать, как вообще налажена работа ИТ-отдела в конкретной компании и как работает её система информационной безопасности. В большинстве компаний сведения о последней — тайна за семью печатями, которую весьма проблематично будет открыть посторонним, даже если они страховщики.

Впрочем, даже если дать страховщикам доступ к системе информационной безопасности, те вряд ли смогут что-либо понять, не привлекая соответствующих экспертов. И здесь мы видим проблему номер два: эксперты по информационной безопасности ничего не понимают в страховании, равно как и страховщики предельно далеки от информационной безопасности. И где взять тех, кто разбирается в обеих дисциплинах, пока что не очень понятно.

Наконец, на западе все бизнес-процессы в большинстве компаний стандартизованы, и их результаты легко прогнозируемы. Также легко прогнозируемы и возможные риски. На постсоветском пространстве ситуация несколько иная, да и действующие стандарты отличаются в ряде случаев от западных. Соответственно, и изобретать страховой велосипед придется тоже с нуля.

Вот, в общем-то, и получается, что страховать ИТ-риски сегодня в Беларуси, как, впрочем, и в России, пока не спешат.

Страхование рисков поставщиков ИТ-услуг

Впрочем, для нашей страны намного актуальнее, в свете нацеленности на развитие экспорта ИТ-услуг, страхование исполнителей (т.е. белорусских ИТ-компаний) от рисков, связанных с проблемами при оплате их работы заказчиком. Речь идет не только о тех случаях, когда заказчик пытается “кинуть” исполнителя, но и о всевозможных финансовых затруднениях у заказчика. Или же проект попросту не понравится заказчику, и он откажется платить.

Для этого рода страхования характерны все те негативные моменты, которые были перечислены выше, за исключением, пожалуй, отсутствия стандартизации бизнес-процессов — большинство белорусских софтверных компаний применяют хорошо известные и хорошо зарекомендовавшие себя методологии разработки ПО, которые прекрасно “обкатаны” на западе. Но специали-

Страхование рисков ИТ-компаний при работе с зарубежным заказчиком

стов по страхованию по-прежнему нет, и это, как оказалось, далеко не единственная из возникших трудностей.

Согласно общепринятой практике, страхование рисков по договорам ложится целиком и полностью на плечи компании, реализующей для кого-то какой-то проект. Именно этот нюанс сегодня и является основным "стоп-краном" на пути страхования для ИТ-компаний в нашей стране. Как говорят в Министерстве финансов Беларуси, если страхователем будет являться разработчик, то в таком случае объектом страхования будет выступать его ответственность по договору, а в соответствии с частью первой статьи 824 Гражданского кодекса Республики Беларусь "*страхование ответственности за нарушение договора допускается в случаях, предусмотренных законодательством*". А в настоящее время законодательством страхование ответственности по такого рода договорам не предусмотрено.

Свою ложку дегтя в общий котел вносит и тот факт, что заказчик разработки находится за рубежом, и, соответственно, необходимо в вопросах обеспечения страхования сообразовываться с иностранным законодательством, которое заметно отличается в разных странах и при этом крайне редко похоже на белорусское.

Впрочем, несмотря на законодательные сложности, у белорусских ИТ-компаний есть возможность несколько снизить свои риски, связанные с выполнением проектов для зарубежных заказчиков — это использование добровольного страхования гражданской ответственности за причинение вреда в связи с осуществлением профессиональной деятельности риски ошибок и упущений при разработке программного обеспечения. Но и к такому виду страхования сами компании, продающие страховки, относятся весьма и весьма настороженно.

Страховщики, конечно же, опять же, находят свои доводы в поддержку такого отношения к страхованию рисков ИТ-компаний. Одна из главных причин — трудности в поисках виноватого. То есть, невозможность определить, по чьей вине провалился проект, если он оказался провальным — заказчика, недостаточно четко сформулировавшего свои требования, или исполнителя, не сумевшего реализовать всё так, как нужно заказчику. Собственно, здесь мы имеем ту же самую проблему, которая упоминалась выше в связи с оценкой систем информационной безопасности — много ли вы знаете программистов и менеджеров проектов, разбирающихся в страховании?

Ещё одна сложность — это оценка стоимости ИТ-проектов, от которой и приходится, в конечном итоге, "плясать" страховщикам. Поскольку нередко при оценке сроков представители компании-аутсорсера занижают цифры, чтобы их предложение выглядело более выгодно для заказчика, то и цена проекта оказывается заниженной, из-за чего в дальнейшем также могут возникнуть разногласия между сторонами, вплоть до разрыва контракта. Поскольку оценка стоимости ИТ-проекта — вещь сама по себе достаточно сложная, то страховщики смотрят на неё с ещё большей опаской.

> **"Самим ИТ-компаниям необходимо активно обращаться к страховщикам, чтобы те, увидев интерес с их стороны, могли способствовать изменениям в законодательстве со своей стороны."**

Соответственно, ситуация со страхованием рисков ИТ-компаний, работающих в аутсорсинге, полностью аналогична ситуации с другими ИТ-рисками. Однако о каком развитии информационных технологий в Беларуси можно говорить всерьез, если страховые компании боятся страхования ИТ-рисков? Проблема нуждается в решении.

Пути разрешения ситуации

В современных белорусских условиях можно говорить о формировании со стороны ИТ-компаний устойчивого спроса на страхование своих рисков при работе с зарубежными заказчиками. Сегодня практически все белорусские страховые компании, предлагающие страховые услуги для бизнеса, имеют в своём портфеле такую услугу, как "Добровольное страхование гражданской ответственности за причинение вреда в связи с осуществлением профессиональной деятельности". Тем не менее, вполне очевидно, что этого недостаточно для полноценной защиты ИТ-компаний от рисков при реализации проектов. Гораздо более подходящим видом страхования для них могло бы стать страхование ответственности по договору то исполнителей услуг, для чего, как говорилось выше, нужны изменения в национальном законодательстве. Они могли бы быть реализованы в рамках реализации программы ускоренного развития экспортно-ориентированной ИТ-индустрии, которая принята в Беларуси на ближайшие годы.

Самим ИТ-компаниям также необходимо активно обращаться к страховщикам, чтобы те, увидев интерес с их стороны, могли способствовать изменениям в законодательстве со своей стороны. Опять же, проявление самого живого интереса к проблеме со стороны ИТ-компаний дало бы толчок к появлению специалистов по страхованию ИТ-проектов — стажировкам страховщиков в западных компаниях, перениманию опыта и т.п. Это позволило бы улучшить ситуацию и со страхованием других ИТ-рисков.

В целом, ситуация сегодня такова, что необходимо приложить ряд усилий, прежде чем страхование рисков ИТ-компаний станет такой же привычной вещью, как, например, страхование грузоперевозок. Что ж, сегодня у ИТ-компаний есть всё, чтобы этого добиться.

Обсудить

Защита ноутбуков от утечек информации

Роман ИДОВ, аналитик компании SearchInform

Количество используемых организациями портативных компьютеров в виде ноутбуков и нетбуков растёт в последнее время просто в геометрической прогрессии. Поэтому особенно актуальной становится проблема защиты всего этого компьютерного парка от различных информационных угроз, начиная с вредоносного ПО и заканчивая утечками информации.

Почему лэптопы популярны?

Пожалуй, начать разговор о защите лэптопов стоит с общей характеристики их положительных и отрицательных сторон для организаций. Существует множество преимуществ лэптопов перед настольными компьютерами, которые в последнее время заметно сдали свои позиции в офисах и даже в домах сотрудников.

Очевидно, что главным козырем лэптопов сегодня является их мобильность — в условиях, когда должна быть возможность брать с собой компьютер в командировки, на презентации, на совещания, это ценное качество ноутбуков выходит на передний план. Конечно, далеко не каждому сотруднику нужны подобные возможности рабочего компьютера, но они наиболее актуальны как раз для тех, кто работает с наиболее важной информацией — то есть, для руководящих сотрудников. А значит, именно ноутбуки нуждаются в наиболее серьезной защите.

Второй плюс лэптопов — это батарея, которая, в отличие от подавляющего большинства устанавливаемых в офисах ИБП, позволяет работать в случае отключения питания не двадцать минут, а около двух часов. Во многих организациях ноутбуки уже, в принципе, и используются как настольные компьютеры с очень большим временем автономной работы в случае перебоев с электричеством.

Стоит отметить, что в последнее время многие из тех, кто часто работает с компьютерами в “полевых” условиях, отдают предпочтение не ноутбукам, а нетбукам. К ним применимо всё то, что говорилось выше и будет сказано ниже про ноутбуки, за исключением, пожалуй, отдельных видов рисков, о которых будет говориться отдельно.

Информационные риски

Информационные риски для лэптопов можно разделить на две категории: специфичные для мобильных устройств и неспецифичные для них. Начать стоит со второй группы, поскольку о ней мы поговорим коротко, поскольку она хорошо известна как специалистам по информационной безопасности, так и обычным пользователям.

Основные неспецифичные для мобильных компьютеров риски заключаются в порче, потере или утечке информации вследствие таких причин, как действия вредоносного программного обеспечения, сбои в работе ПО или аппаратного обеспечения, халатность пользователя и т.д. Отдельно стоит выделить группу организационных рисков, связанных с умышленным распространением конфиденциальной корпоративной информации или с её порчей. В свете того, что такие риски в последнее время значительно увеличились, их минимизации необходимо уделить особое внимание.

Что касается специфических для ноутбуков и нетбуков рисков, то здесь, в первую очередь, следует выделить риск утраты информации, характерный для всех мобильных носителей. Они, как правило, используются в гораздо более неблагоприятных условиях, чем стационарные настольные компьютеры, а потому гораздо чаще выходят из строя. Кроме того, в отличие от стационарного компьютера, мобильный очень легко потерять, также есть риск кражи служебного ноутбука из автомобиля, в аэропорту, на вокзале и т.д.

Из этого вытекает и второй риск, связанный с утечкой конфиденциальной информации через ноутбуки. Если кто-то что-то теряет, то кто-то что-то и находит. Нередко находящаяся на лэптопе информация стоит в десятки раз дороже самого лэптопа, и его потеря может привести к катастрофическим для компании последствиям. Отдельно стоит упомянуть и умышленную передачу закрытой корпоративной информации за пределы компании — часто сотрудники используют для этого служебные ноутбуки, передавая данные третьим лицам из дома или в командировках.

Таким образом, как несложно увидеть, в среднем риск утраты или утечки информации для корпоративных лэптопов заметно выше, чем для десктопов. Тем не менее, в большинстве своём риски носят неспецифический характер, что, впрочем, сложно сказать об инструментах защиты, на которых мы далее остановимся подробнее.

Физическая защита

Поскольку ноутбуки подвержены не только виртуальным, но и вполне реальным угрозам, таким, например, как кража, то и методы защиты от таких угроз будут чисто физическими. Сегодня существует достаточно большое количество приспособлений, с помощью которых можно снизить вероятность “угона” лэптопа.

Самое простое и при этом одно из самых эффективных средств защиты ноутбука или нетбука от кражи — это обыкновенный замок, с помощью которого компьютер пристегивают тросом к какому-либо достаточно большому и устойчивому предмету. Замок этот, конечно, имеет специальную форму, и называется обычно замком Кенсингтона. Впрочем, хрупкость ноутбучных корпусов зачастую является причиной того, что при попытке кражи “пристегнутый” ноутбук попросту лома-

Защита ноутбуков от утечек информации

ется.

Как и для автомобилей, для ноутбуков существуют специальные противоугонные сигнализации, которые сообщают владельцу устройства о попытках несанкционированного физического доступа к нему. К сожалению, эффективность подобных средств не так высока, как в случае с автомобилями.

Остальные средства физической защиты предназначены, скорее, для возврата пропавшего ноутбука владельцу, нежели для предотвращения кражи. К таким средствам относятся специальная маркировка, наносящаяся на устройства, радиомаячки и т.д. К сожалению, они вовсе не гарантируют возврат украденного устройства, и тем более бессильны предотвратить утечку данных.

Многие дорогие модели ноутбуков оснащаются специальными биометрическими устройствами (обычно используются сканеры отпечатков пальцев), которые предназначены для защиты не столько самих ноутбуков, сколько находящихся на них данных. Хотя такое оборудование заметно повышает стоимость ноутбука, оно действительно чрезвычайно эффективно от случайных краж. Если же ноутбук украли ваши конкуренты, охотящиеся за вашими корпоративными секретами, будьте уверенны, что сканер отпечатков пальцев их не остановит.

Классическая программная защита

Большей частью средства защиты не отличаются от аналогичных для настольных компьютеров, поскольку подавляющее большинство лэптопов работает под управлением тех же самых программных продуктов, которые “рулят” и настольными ПК. Исключение составляет, разве что, небольшая прослойка Android-нетбуков, так и не получивших большого распространения на постсоветском пространстве.

Тем не менее, даже такие привычные средства защиты, как антивирусы и файрволы, нередко предлагаются производителями в специальной “ноутбучной” редакции, которая, по заверениям разработчиков, специально оптимизирована для работы на ноутбуке с учетом нагрузки на системные ресурсы и энергопотребления. Сложно сказать, насколько такие решения действительно помогают растянуть на более долгое время заряд батареи ноутбука, но однозначно можно сказать, что в тех случаях, когда батарея используется нечасто и играет, скорее, роль ИБП, переплата за такую оптимизацию нецелесообразна.

Для защиты от кражи информации существуют разнообразные средства ограничения доступа к ноутбукам и шифрования находящихся на них данных. Обычно это те же самые средства, которые применяются для защиты настольных ПК — к примеру, в российских компаниях распространена практика установки на ноутбуки решений, предлагающих автоматическое шифрование разделов жесткого диска, на которых сотрудники должны держать критически важную информацию. Достаточно интересным, хотя и редким решением являются ноутбуки с жесткими дисками, контроллеры которых позволяют шифровать находящуюся на диске информацию.

Для защиты компании от утраты критически важной информации, находящейся на ноутбуках, очень важно использовать системы резервного копирования. Их важность значительно возрастает по сравнению с

Защита ноутбуков от утечек информации

Теми случаями, когда используются настольные компьютеры, поскольку, как говорилось выше, ноутбуки подвержены гораздо большему числу физических угроз, которые могут привести к потере важной для организации информации.

Endpoint-защита

Пожалуй, одной из немногих защитных систем, которая заметно отличается для ноутбуков и для настольных ПК — это DLP, система защиты организации от утечек информации. Как уже отмечалось выше, ноутбуки часть используются сотрудниками дома или в командировках, то есть, вне защищенной с помощью DLP-системы корпоративной сети. Казалось бы, в таких условиях совершенно отсутствует возможность проследить, что происходит с конфиденциальными корпоративными документами, находящимися на ноутбуке. Однако, к счастью, существуют решения, позволяющие решить подобную задачу.

Для контроля лэптопов применяются так называемые endpoint-решения (от английского endpoint — крайняя точка). Эти решения отличаются тем, что работают не на удалённом сервере, как обычные компоненты подавляющего большинства DLP-систем, а на самом портативном компьютере. То есть, они работоспособны независимо от того, к какой сети подключен компьютер (и подключен ли вообще). Но при этом endpoint-решения ведут себя поразному внутри корпоративной сети и вне нее.

Находясь в рамках защитного контура, endpoint-модуль на ноутбуке постоянно поддерживает связь с центральными компонентами DLP-системы, передавая им перехваченную информацию и сверяясь с заданными политиками информационной безопасности. Но как только ноутбук отключается от корпоративной сети, модуль переходит в режим автономной работы. В этом режиме он собирает данные о действиях пользователя, сохраняя информацию о переданных документах, написанных сообщениях и других входящих и исходящих данных на самом лэптопе. Затем, когда сотрудник вернётся со своим переносным компьютером в офис, все данные будут переданы для анализа соответствующему компоненту системы защиты, и специалисты по безопасности смогут узнать обо всех нарушениях корпоративных политик, которые потенциально могли привести к утечкам информации.

Конечно, такая защита не так эффективна, как защита корпоративной сети, однако она позволяет своевременно узнавать о возможных инцидентах, связанных с информационной безопасностью, и предотвращать их последствия. При этом модуль, работающий на ноутбуке, может устанавливаться таким образом, чтобы пользователь, работающий за компьютером, ничего не подозревал о его наличии.

Endpoint-системы показывают высокую эффективность в борьбе с заранее спланированными утечками данных, наиболее опасными для любых организаций. Вполне понятно, что сама их архитектура делает их менее эффективными в плане борьбы со случайными утечками информации, однако и сами эти утечки, как свидетельствует статистика, редко приводят к настолько катастрофическим последствиям, как специально подготовленные утечки.

Резюме

Оказывается, защитить корпоративный лэптоп от всего того множества угроз, которые существуют вокруг него, не так уж и сложно, если задаться подобной целью. С другой стороны, вряд ли имеет смысл вооружать ноутбук “до зубов” всеми перечисленными выше средствами защиты — сначала необходимо определить приоритеты, а затем уже закрывать наиболее значимые проблемы.

Обсудить

Почему уходит сисадмин?

Виктор ДЕМИДОВ

Есть вопросы, порожденные техническим прогрессом, на которые пока нет ответов. Нет моделей поведения, нет готовых рецептов решения возникающих проблем, нет даже однозначного отношения к этим проблемам. Один из таких тонких вопросов — взаимоотношения системных администраторов и их работодателей. Сразу предупреждаю: я могу только сформулировать проблему, но не предложить пути ее решения. Тут уже нужно думать всем вместе.

Нужный дядя

Сисадмин-эникейщик — это сегодня одна из самых востребованных специальностей на белорусском рынке труда. Ведь работа любой фирмы, завода или госорганизации сегодня зависит от состояния их компьютерной инфраструктуры. Которую кто-то должен поддерживать в рабочем состоянии и развивать. А ряды офисного планктона непрерывно пополняются "недопользователями", уровень компьютерных навыков которых сводится к "ВКонтакте", ICQ и умению набирать текст в "Ворде" одним пальцем.

Словом, без сисадмина сегодня не обойтись нигде. Вот только директора, люди, в большинстве своем от компьютеров далекие, обычно воспринимают сисадмина как просто технического специалиста — что само по себе вполне оправданно. И без колебаний отдают ему в полное ведение всю IT-инфраструктуру организации. Что уже чревато катастрофическими последствиями.

Ведь в наш информационный век тот, кто контролирует потоки данных — контролирует все. А в описанном (и весьма типичном) случае информационные потоки оказываются в руках человека довольно молодого, с далеко не самой высокой зарплатой и не самым высоким статусом в организации... Лично мне это кажется фактором очень серьезного риска. А вам?

Как показывает практика, уход из фирмы ведущего IT-специалиста оказывается стрессом, вполне сопоставимым со стрессом от ухода, скажем, начальника отдела продаж. Особенно в том случае, если расставание с "айтишником" происходит не по-хорошему. В небольшой фирме с единственным сисадмином его уход может остановить или вообще разрушить весь бизнес. За примерами, к сожалению, далеко ходить не надо, и их не так мало, как может показаться.

Что не нравится сисадмину?

Чтобы узнать из первых уст, почему системные администраторы бывают недовольны жизнью, в принципе, достаточно сходить на "Башорг", в раздел "IT-happens". Но это, так сказать, "сырая" информация. Проанализировав ее, а также опыт специалистов-кадровиков, можно выделить несколько основных причин, по которым сисадмины уходят даже, казалось бы, с самых "теплых" мест.

— Агрессивно-некомпетентные пользователи. Байки про гневно вопящих и брызжущих слюной бухгалтерш, у которых на ровном месте документ не открывается или принтер не печатает, уже давно стали отдельным жанром сисадминского фольклора. Сюда же добавляем начальников, в завирусованных ноутбуках которых папки "важные документы" плотно забиты порнухой. Говорят, у сисадмина, беспрекословно переносящего такое, через десять лет вслед за бородой и свитером отрастает нимб.

— Девальвация профессии. Помнится, лет 10-15 назад специалисты по компьютерной верстке газет и журналов (да и вообще всего полиграфического) были на вес золота. Их холили, лелеяли, всячески обхаживали и платили по принципу "сколько попросит".

Но сегодня верстает, что называется, "жук и жаба" — профессиональные пакеты для верстки стали намного более user-friendly, а двухмесячные курсы подготовки "выплевывают" новых верстальщиков со скоростью пулемета. Как результат — множество безработных специалистов по верстке и оклады на уровне $400.

Так вот: ситуация с сисадминами полностью идентичная, вплоть до уровня зарплат. За минувшее десятилетие количество системных администраторов на рынке труда выросло на порядок, но их профессиональный уровень — значительно снизился (как и средний возраст). Соответственно, значительно упали зарп-

Почему уходит сисадмин?

Зарплаты и престиж профессии.

Не случайно, наверное, все чаще сисадмины жалуются, что их заставляют выполнять функции простых эникейщиков. И это тоже свидетельство девальвации профессии. Действительно, специалиста, получающего $2.000 в месяц, вряд ли кто-то отправит лампочки вкручивать. А получающего $400 — запросто. Перефразирую. Программисту с окладом $3.000 никогда не прикажут сменить картридж в принтере. Сисадмина “стоимостью” $400 за неработающий принтер вполне могут лишить премии. Хотя и первый, и второй, — своего рода “техношаманы”, а сменить картридж могла бы и секретарша.

— Отсутствие перспектив карьерного роста. В абсолютном большинстве организаций штатный сисадмин лишен каких-либо перспектив карьерного роста. Да, в большой компании он может возглавить IT-отдел, став CIO (Chief Information Officer, директор по информационным технологиям). Но таких должностей — очень мало.

Остальные системные администраторы в некотором смысле обречены. Бухгалтер сталелитейного завода никогда не возглавит этот завод. Водитель НИИ генетики, как бы ни старался, не станет во главе института. Сисадмин торговой компании или фирмы-нефтетрейдера не станет их директором. Профиль не тот. Большинство это понимает, но мало кому это нравится.

— Доступ к ценным и критически важным данным. Самый сложный из мотивов ухода, так как полностью завязан на психологию. Когда сисадмин имеет доступ ко всем данным “двойной бухгалтерии”, финансовым отчетам и бизнес-планам компании, переписке замдиректора с его любовником-геем, номерам счетов и логинам для хостинга — все это развращает, дает ощущение власти и неограниченных возможностей. У не отягощенного моральными принципами сисадмина появляется желание “монетизировать” ценную информацию, уйдя из фирмы. Вот это и есть самое опасное для работодателя.

Забрав самое ценное

Добродушный сисадмин без амбиций, но с бородой, свитером и кофейной кружкой, в которой уже зарождаются новые формы жизни, — типаж, конечно, весьма распространенный. Однако системными администраторами становится все больше “зубастых”, амбициозных, изворотливых — но при этом недалеких молодых людей. Которые вполне адекватно оценивают ценность информации, попадающей им в руки. Наиболее дальновидные начинают собирать ценные данные едва ли не с первого дня работы в организации. Причем вполне открыто — действительно, какое подозрение может вызвать системный администратор, делающий бэкап?!

> **“На днях увольняли сисадмина. Директор говорит ему, мол, сдай системный пароль, и подает бумажку. Админ записывает следующее *******, немного подумав, “а нет, еще одна звездочка”.**
>
> **(с) реальная история на правах анекдота”**

Многочисленные опросы, проводимые в разных странах мира, рисуют безрадостную картину. До 85% сисадминов, уходя из компании, забирают с собой ценные данные. В 27% случаев эти данные представляют собой интеллектуальную собственность, а в 17% — информацию о клиентах. Более того, как утверждает компания Imperva, проводившая соответствующий опрос в Великобритании, 66% респондентов признались, что сознательно приготовятся и скопируют себе данные работодателя, как только по компании поползут слухи об увольнениях. Также 79% опрошенных заявили, что в их организации нет каких-либо правил, обязывающих увольняемого работника стирать собранные данные со своих ноутбуков при уходе. То есть работникам реально ничто не мешает забрать с собой данные компании. К тому же у подавляющего большинства работников (85%) такие данные уже есть на домашних компьютерах или мобильных устройствах. По данным Imperva, эти данные — информация о клиентах (75%) и интеллектуальная собственность (27%).

Как мы видим, сисадмин, решивший уйти из небольшой фирмы, в какой-то момент фактически держит ее судьбу в своих руках. Вот почему для работодателя принципиально важно расстаться с таким сотрудником по-хорошему. Ведь он может не просто продать ценные данные конкуренту. Считающий себя обиженным сисадмин может начать шантажировать сотрудников, “слить” двойную бухгалтерию налоговым органам, уничтожить все учетные записи, стереть или заблокировать данные на жестких дисках всех офисных ПК и серверов, оставить софтверные “закладки” и бэкдоры в системе... словом, на что у него фантазии хватит.

О том, как вести себя работодателю, как строить отношения с IT-специалистами и как их грамотно увольнять мы поговорим в одной из следующих статей.

P.S.

Конечно, в этом мире есть и множество отличных сисадминов, получающих немалые деньги и отрабатывающие их на 100%. Специалистов, которые не суют свой нос в данные пользователей, не припрятывают “про запас” важную информацию и не протоколируют посещения начальником его любимых порносайтов. Хочется думать, что среди читателей “КВ” таких большинство. Но моей задачей было описать проблему в целом. Жаль, что картина получилась не самая веселая.

Обсудить

Многофакторная аутентификация

Использование парольной аутентификации в ИС предприятий и организаций себя изживает. Продолжая применять эту традиционную методику доступа в отношении собственных информационных ресурсов, компании фактически ставят под угрозу рентабельность и, вероятно, само существование предприятия.

Это утверждение имеет смысл и относится, прежде всего, к компаниям финансового сектора, как впрочем, и ряду компаний выполняющих НИОКР в высокотехнологичных секторах рынка. Давайте рассмотрим основания для столь многозначительного вывода.

Согласно стандарту РФ о защите информации, три основных свойства определяют безопасное состояние обрабатываемой информации — её конфиденциальность, доступность и целостность. Вспомним, что парольная аутентификация, а именно она в деле защиты данных является одним из первых барьеров, появившихся в ИТ-системах одновременно с операционными системами, реализующими множественный доступ к информационным ресурсам, без малого 20 лет стоит на первом рубеже контроля. Очевидно, что среди основных достоинств этой методики защиты её привычность и простота. И вряд ли кто-то станет оспаривать достаточность применения во многих организациях парольной аутентификации и уровня безопасности использования информации, при соответствующем организационном подходе. Однако...

80% инцидентов в сфере информационной безопасности случаются вследствие использования слабых паролей — к такому выводу пришла компания Trustwave по результатам собственного исследования, охватившего ряд компаний в 18 регионах мира. Аналитики посвятили исследование уязвимости элементов в системах информационной безопасности, в процессе коего изучили более 300 инцидентов, имевших место в 2011 году. Главное заключение, сделанное в итоге: слабые пароли пользователей в ИС — наиболее уязвимое место, используемое злоумышленниками, как в крупных, так и в небольших компаниях.

Слабый пароль — это плохо, но обратная сторона применения сложных паролей — трудность удержания в памяти человека. Как следствие — небрежность их хранения в виде рабочих записей, а в этом случае уже не имеет значения, будет ли пара логин/пароль записана в личном блокноте сотрудника или закреплена на мониторе липким листком. Зная традицию обращения с такими данными работниками российских компаний, к примеру, для злоумышленника не составит особого труда получить эти сведения... Если еще учесть часто применяемую “синхронизацию” паролей для доступа к различным приложениям и корпоративным системам... И вот, минимум два из трёх столпов информационной безопасности предприятия повержены в цифровую пыль.

Некоторые зарубежные компании, действующие в сфере анализа инцидентов в системах безопасности, делают вывод: несанкционированный доступ к информации ограниченного использования о финансовой активности предприятия, договорах и графиках способен сказаться не то, что потерями — разорением. Ежегодные потери от утечек информации в США оцениваются в миллиардах долларов. Российский отраслевой портал “Информационная Безопасность Банков” в оценке финансового ущерба от возможных злоупотреблений сотрудников ссылается на исследования Ассоциации экспертов по борьбе с мошенничеством (ACFE, США), которая видит эту сумму в размере 6% прибыли банка за год. По наблюдениям ассоциации, потери при подобных инцидентах, в среднем, достигали $100 тыс., а в 14,6% превысили $1 млн.

Исследовательская компания Javelin Strategy в своем ежегодном исследовании, опубликованном в феврале 2012 года, оценила мировой объем мошенничества и утечек данных из компаний и организаций за 2011 год в $18 млрд. Не доверять экспертам нет оснований, а поправку на отставание России в области информатизации и не публичность российских банков и компаний каждый вправе сделать сам.

Невзирая на множество средств вычтехники и широкий спектр технологических решений, выбор методов аутентификации для компаний, планирующих своё будущее, невелик — многофакторная аутентификация (конечно, если в ближайшее время не случится технологический прорыв в управлении вычислительными системами при помощи мысли). Однофакторной или парольной аутентификации для безопасной работы с информационными системами в развитом бизнесе уже не достаточно.

Сильные и слабые стороны многофакторной аутентификации, в общем, известны. К преимуществам можно отнести её способность защитить информацию, как от внутренних угроз, так и от внешних вторжений. Определенной слабостью можно считать необходимость использова-

Многофакторная аутентификация

ния дополнительных программно-аппаратных комплексов, устройств хранения и считывания данных. В то же время, в настоящий момент статистика взломов систем, применяющих двухфакторную аутентификацию, отсутствует или ничтожна.

Многофакторная или расширенная аутентификация уже сегодня применяется рядом российских компаний в сфере финансов при создании сервисов интернет-банкинга, мобильного банкинга, файлообмена и т.п. решений для конечных пользователей. Она основана на совместном использовании нескольких факторов аутентификации (знаний, средств или объектов хранения одной из информационных составляющих легитимной процедуры аутентификации), что значительно повышает безопасность использования информации, по меньшей мере, со стороны пользователей, подключающихся к информационным системам по защищенным и незащищенным каналам коммуникаций.

В качестве примера может послужить процесс двухфакторной аутентификации пользователя, реализованный в настоящее время рядом российских банков: вход в личный кабинет пользователя посредством сети интернет возможен после ввода пароля на странице, после чего (в случае подтвержденной правомерности), следует передача одноразового пароля (в виде SMS) на мобильный телефон, ранее зарегистрированный пользователем.

Аналогичные схемы контроля и управления полномочиями пользователя, его дальнейших действий в корпоративных или других информационных системах, могут быть реализованы с применением самых различных средств и методов, выбор коих достаточно широк, как по технологичности, стоимости, исполнению, так и по возможным комбинациям перечисленных свойств.

Сессия работы пользователя может также контролироваться на предмет соответствия, как IP-адреса последней успешно завершенной сессии, так и MAC-адреса соответствующего сетевого оборудования. Далее могут идти действия подтверждения или отказа в доступе к информационным ресурсам, но доверия к этим двум параметрам контроля быть не может в силу их технологической слабости: IP-адрес можно подменить, а MAC-адрес просто переписать в ходе работы системы, и даже без перезагрузки. Тем не менее, в качестве неких контрольных значений эти сведения могут быть использованы.

Несколько примеров двухфакторной и многофакторной аутентификации

Методика аутентификации при помощи SMS основана на использовании одноразового пароля: преимущество такого подхода, по сравнению с постоянным паролем в том, что этот пароль нельзя использовать повторно. Даже если предположить, что злоумышленнику удалось перехватить данные в процессе информационного обмена, он не сможет результативно использовать украденный пароль для получения доступа к системе.

А вот пример, реализуемый с применением биометрических устройств и методов аутентификации: использование сканера отпечатка пальца, который имеется в ряде моделей ноутбуков. При входе в систему пользователь должен пройти процедуру сканирования пальца, а затем подтвердить свои полномочия паролем. Успешно завершенная аутентификация даст ему право на использование локальных данных конкретного ПК. Тем не менее, регламентом работы в ИС может быть предусмотрена отдельная процедура аутентификации для доступа к сетевым ресурсам компании, которая помимо ввода другого пароля может включать в себя целый ряд требований к представлению аутентификаторов субъекта. Но даже при такой реализации, защищенность системы, несомненно, усиливается.

Аналогичным образом могут быть использованы и другие биометрические аутентификаторы:

— отпечатки пальцев;

— геометрия кисти руки;

— очертания и размеры лица;

— характеристики голоса;

— узор радужной оболочки и сетчатки глаз;

— рисунок вен пальцев.

При этом конечно применяется соответствующее оборудование и программное обеспечение, а затраты на его приобретение и поддержку могут отличаться в разы.

Но! Стоит понимать — биометрические аутентифи-

Многофакторная аутентификация

каторы не являются абсолютно точными данными. Отпечатки одного пальца могут иметь отличия под воздействием внешней среды, физиологического состояния организма человека и т.п. Для успешного подтверждения этого аутентификатора достаточно не полного соответствия отпечатка эталону. Методы биометрической аутентификации содержат определение степени вероятности соответствия действующего аутентификатора эталону. Что касается биометрической аутентификации и удаленного доступа к ИС, то пока у современных технологий нет возможности передать по незащищенным каналам достоверные данные — отпечаток пальца или результат сканирования сетчатки глаза.

Эти технологии в большей степени годятся для использования в корпоративных сетях.

Наиболее популярной технологией, в этом направлении, в недалеком будущем может стать голосовая аутентификация и признаки тому на лицо. Значительное количество разработок в этой сфере имеется уже сегодня, проекты внедрения подобных механизмов управления/контроля нашли место в ряде крупных банков РФ. В качестве примера практического применения систем голосовой биометрической аутентификации, можно указать аутентификацию по ключевой фразе, применяемую в ряде колл-центров, аудио-пароли для доступа к системам интернет-банкинга и т.п., подтверждение действий персонала при осуществлении важных операций доступа к информации, контроль физического доступа и присутствия в помещении.

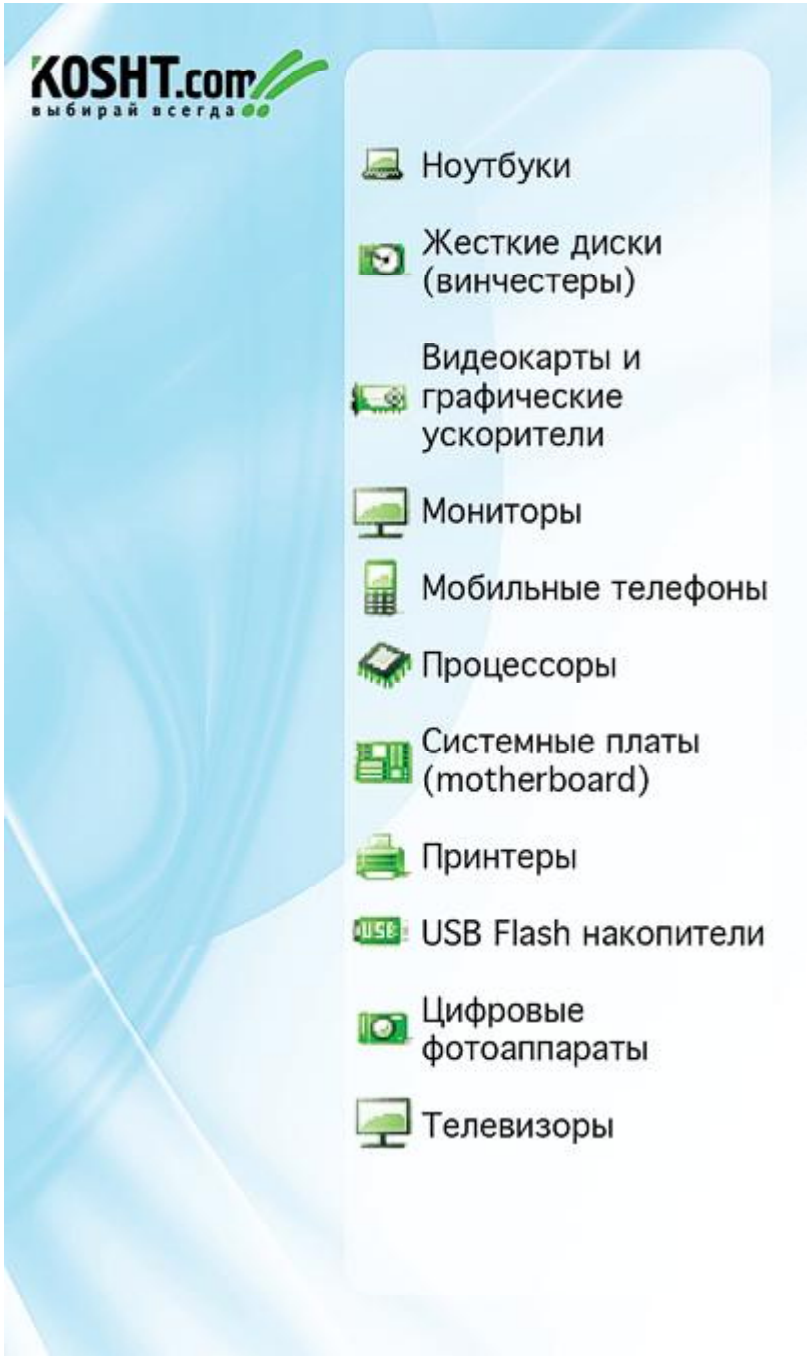
Помимо технологий, связанных с использованием биометрических аутентификаторов, имеются также программно-аппаратные решения, такие как автономные ключи для генерации одноразовых паролей, считыватели RFID-меток, криптокалькуляторы, программные и аппаратные жетоны (токены), электронные ключи различных типов — Touch Memory и ключ/смарт-карта, а также биометрические идентификационные карты. Все перечисленные в рамках статьи системы и методы многофакторной аутентификации, а помимо них еще и системы контроля и управления доступом (СКУД) могут интегрироваться, комбинироваться, отрабатывать поочерёдно и в комплексе. Отсюда можно сделать вывод: на рынке России существует достаточное количество предложений для усиления защиты информационных систем, как от внутренних, так и внешних вторжений. У компаний имеется возможность выбора, ограничиваемая лишь размером бюджета.

Методам защиты, основанным на методиках многофакторной аутентификации, сегодня доверяет большое число зарубежных компаний, среди которых организации хай-тека, финансового и страхового секторов рынка, крупные банковские учреждения и предприятия госсектора, независимые экспертные организации, исследовательские фирмы.

При этом, частные компании и организации в мире, в целом, не очень охотно распространяются о внедрении у себя технологических новинок в сфере безопасности и защиты информации, по вполне понятным причинам. Гораздо больше известно о проектах в государственном секторе — с 2006 года публично известны успешно реализованные технологические решения в государственных учреждениях Канады, Саудовской Аравии, Испании, Дании и ряда других стран.

Материал подготовлен компанией “Индид”

Обсудить



Социальные ресурсы: киберсеть для злоумышленников

Евгений АБАЗОВИК

Еще буквально с десяток лет назад мошенничество в социальных сетях, как впрочем, и иные виды киберпреступлений, воспринималось рядовыми обывателями как нечто диковинное, навеянное западными фильмами о хакерах и фантастическими романами. На сегодняшний день злодеяниями подобного рода буквально пестрит милицейская сводка: взлом аккаунта Вконтакте, кража денег посредством SMS-сообщений уже давно никого не удивляют. Однако подобное безразличие только способствует бурному росту количества интернет-преступлений. И чем активнее работают в этом плане правоохранительные органы, тем изощреннее становятся уловки сетевых мошенников.

К величайшему сожалению рядовых обывателей, бурный всплеск развития информационных технологий способен принести людям не только земные блага: плодами современной цивилизации успешно и весьма активно пользуется все большее количество виртуальных злоумышленников. А Глобальная сеть, обладающая определенными параметрами анонимности, является и вовсе благодатной средой для развития разнообразных криминальных промыслов. Поэтому весьма неудивительно, что именно социальные сети в последнее время создают почву для их бурной и весьма плодотворной деятельности.

Однако, зачастую, виновны в этом сами доверчивые пользователи. По данным исследования, проведенного компанией Symantec, практически каждый из пользователей, ставших жертвой уловок киберзлодеев, ощущает чувство вины. Как правило, жертва зачастую смиряется с произошедшим. Исходя из данных опроса, около 80% интернет-пользователей полагают, что киберпреступники привлекаться к уголовной либо же административной ответственности не будут. И лишь менее половины от общего количества респондентов обращались в правоохранительные органы с жалобой на киберзлоумышленников. Статистика, согласитесь, весьма неутешительная... и в большей мере это связано с тем, что сами жертвы происшествий панически боятся огласки собственных не совсем благопристойных делишек: к примеру, некто решил посмотреть детское порно либо же пошпионить за любимой девушкой путем чтения ее мобильной переписки. Всем известно, что именно подобные предложения в социальных сетях чаще всего являются предтечей совершения компьютерных преступлений.

SMS-шпионаж, о котором было сказано выше, является весьма изощренным видом компьютерного мошенничества. Как правило, к пользователю социальной сети приходит сообщение с предложением подслушать звонки либо же подсмотреть чьи-то SMS. Безусловно, здесь следует помнить о том, что ни один из действующих сотовых операторов не пойдет на то, чтобы осуществлять “слив” конфиденциальной информации организаторам данного теневого сервиса. Технологий перехвата подобного рода на сегодняшний день попросту не существует. А без ведома работников сотовой компании, утечек информации на постоянной основе быть попросту не может. Так что, получив подобное заманчивое предложение, будьте стопроцентно уверены — вас “кидают”.

В целом же, в связи с тем, что социальные сети уже давно превратились в неотъемлемую часть жизни сегодняшних пользователей, мошенничество в сетях приобретает поистине угрожающие масштабы. Субботним утром, наслаждаясь чашечкой кофе, вы с удивлением можете заметить, что у вас украли личность, которую вы пестовали и лелеяли в Facebook. А ваш друг в Вконтакте почему-то ещё раз добавляется в список друзей и присылает сообщение, в котором просит срочно отправить смс на указанный номер. Не стоит удивляться, если после выполнения указанной просьбы с вашего мобильного счёта спишут определенное количество денежных средств. Чего стоит один только нашумевший случай с продажей внутренней валюты — Оков в социальной сети “Одноклассники”. Как бы это ни казалось странным, на удочку мошенников чаще всего попадались взрослые, вполне разумные люди (а как известно, именно они и составляют основной контингент данного ресурса). Виртуальные мошенники тайком узнавали номера мобильных телефонов пользователей данной социальной сети и коды, которые присылались ее администрацией для приобретения виртуальной валюты. При этом деньги списывались со счетов доверчивых абонентов и при этом у них еще и вырастали долги в десятки сотен тысяч рублей перед мобильным оператором. Схема получения кода от социальной сети являлась достаточно простой, поскольку осуществлялась она посредством службы мобильных сообщений одного из крупных отечественных сотовых операторов. Во многом, данный фактор и оказался на руку мошенникам. Министерство внутренних дел обратилось в данную компанию с пись-

Социальные ресурсы: киберсеть для злоумышленников

Мом, где пояснило, что “действующий механизм покупки бонусных единиц позволяет злоумышленникам после активации услуги без согласия владельца абонентского номера произвести до десяти фактов оплат общей стоимостью около 3 млн рублей”. МВД предложило компании изменить механизм взаиморасчетов так, чтобы абоненты для оплаты услуг в интернете отправляли SMS с подтверждением каждого факта оплаты.

Аккаунты, пароли, явки....

Еще одним весьма распространенным способом мошенничества в социальных сетях является кража паролей. Делается это с конкретной, вполне определенной целью: либо злоумышленник интересуется персональной перепиской жертвы, либо же он попросту желает превратить активную страницу в спам-бот, который впоследствии будет использовать уже с собственными целями. Чаще всего в краже паролей и аккаунтов виноваты сами пользователи. Конечно, существуют хакерские сообщества и целые сайты, на которых предлагаются услуги по взлому аккаунтов, но это скорее исключение, чем правило. В том же случае, если вы не управляете крупной компанией, и у вас нет конкурентов, которые хотят прочесть вашу личную переписку, проблема элементарной интернет-безопасности решается довольно просто.

Существует несколько правил, которым нужно обучать людей, перед тем как они впервые выйдут на просторы интернета и зарегистрируются в социальных сетях.

> **“Даже сотрудники крупных IT-компаний, которые знают об информационной безопасности не понаслышке, зачастую становятся жертвами хакеров.”**

1. Придумывайте оригинальный и сложный пароль для почтового ящика, на который вы будете регистрировать аккаунт социальной сети. Изучите систему безопасности почтовой службы, возможно, она предоставляет дополнительные меры защиты, вроде двухступенчатой авторизации и привязки к компьютеру у Gmail.

2. При вводе личной информации, паролей, номера электронного кошелька или кредитной карты всегда проверяйте адресную строку в вашем браузере, особенно если вас по каким-то причинам перенаправляли с первоначального адреса. Фишинг — настоящая чума современной сети. Злоумышленники в точности копируют сайты, однако располагают их на других интернет-адресах, а всю вводимую вами информацию собирают в базу данных, которую затем без труда применяют согласно назначению. Актуальна проблема фишинга и для социальных сетей: к примеру, в Facebook около 9% аккаунтов ненастоящие.

3. Всегда внимательно относитесь к необычным сообщениям со ссылками от друзей в социальных сетях. Рассылка может содержать инструкцию того, как своими руками опустошить собственный кошелёк. Лучше направьте электронное письмо другу с альтернативного сервиса и переспросите, он ли это, а также перепроверьте страницу, с которой вам пришло подозрительное сообщение. Возможно, вашего друга взломали, а теперь хотят добраться и до вашей странички.

4. В Facebook существует функция доверенных друзей, которая позволит вашим друзьям оказать вам помощь, если ваш аккаунт всё же взломают. В Вконтакте есть привязка аккаунта к телефонному номеру, которая повысит степень вашей безопасности от несанкционированного доступа к вашей личной информации.

5. И, конечно же, вам стоит следить за тем, какие файлы, полученные из внешних источников, вы запускаете у себя на компьютере. Старые добрые кейлогеры, отслеживающие каждое нажатие на вашей клавиатуре, всё ещё стабильно пополняют хакерские базы логинами и паролями ни о чём не подозревающих пользователей.

6. Уделяйте внимание тому, насколько легко получить доступ к вашему аккаунту, зная информацию, которую вы разместили на любом другом сайте или форуме. Челночный взлом аккаунтов, когда хакер знает ваш почтовый ящик и мобильный номер телефона, может стать для вас настоящей головной болью. Злоумышленник будет “щёлкать” ваши аккаунты в Twitter, Facebook и где угодно, если вы позволили себе роскошь не озаботиться дополнительными мерами предосторожности, прежде чем публиковать свою личную информацию в интернете.

Ещё раз хочется напомнить, что наиболее лакомым кусочком для мошенников является “угон” аккаунта с привязанной кредитной картой, поэтому необходимо уделять особенное внимание безопасности при операциях с такими аккаунтами.

Следуя этим простым правилам, вы сможете оградить себя от большинства мелких интернет-хулиганов, мошенников и воров. К сожалению, с целенаправленной атакой профессиональных преступников справиться, скорее всего, не выйдет. Даже сотрудники крупных IT-компаний, которые знают об информационной безопасности не понаслышке, зачастую становятся жертвами хакеров и тогда компании несут большие убытки. Так что будьте бдительны — и это вам зачтется!

Обсудить

КВ:\ КОМПЬЮТЕРНЫЕ ВЕСТИ

Издатель: ООО “РГ “Компьютерные Вести”

Адрес: Минск, ул. Мельникайте, 2, оф. 710.

Для писем: 220004, г.Минск, а/я 57.

Телефон/факс: (017) 203-90-10

E-mail: info@kv.by

Редакция может публиковать в порядке обсуждения материалы, отражающие точку зрения автора. За достоверность приведенной информации ответственность несут авторы.

При перепечатке материалов ссылка на “КВ” обязательна.

За достоверность рекламной информации ответственность несет рекламодатель.

Группа компаний "БелХард" приглашает на работу

В связи с ростом масштабов деятельности и открытием новых направлений требуются **специалисты высокой квалификации** в международные проекты на полную занятость:

- **Программисты прикладных систем** J2EE, C#, C++, Delphi, Python,
- **Web-программисты** ASP.NET, PHP, Ruby, Flash и Web-дизайнеры,
- **Программисты мобильных приложений** iOS, J2ME,
- **Руководители проектов, бизнес-аналитики** (разработка ТЗ для АСУП),
- **Системные интеграторы** (сисадмины со знанием Java),
- **Функциональные тестировщики, тест-разработчики**.

Наши ценности — это сильная команда, постоянное профессиональное совершенствование.

Предлагаемые нами условия: достойные вознаграждения, премии за достижения, широкие карьерные перспективы, соц. пакет с льготами от резидента ПВТ, эффективные процессы (ISO, CMMI) и современный инструментарий, разнообразие творческих задач, благоприятная атмосфера в команде.

С нами Вы сможете реализовать себя в актуальных, интересных проектах!

Специальное предложение студентам ИТ-специальностей со знанием английского языка:

- Проводим набор на стажировку с последующим трудоустройством, направления: SW Tester и SW Developer (PHP, Java, C#, IPhone),
- Гибкий график и сокращенная до 30 часов рабочая неделя,
- Стажеры могут быть направлены к нам на преддипломную и производственную практику,
- Наши сотрудники-выпускники вузов получают возможность оформиться на работу в качестве молодых специалистов (по распределению).

Подробная информация о вакансиях, об интенсивно растущих секторах корпорации, бланк резюме: **www.job.belhard.com**.

E-mail для резюме: job@belhard.com.