BIZ KV:A КОМПЬЮТЕРНЫЕ ВЕСТИ www.kv.by

No. 002 (2)
19 июля 2012 года

ООО “РГ “Компьютерные Вести” • Тираж: 11200 экз. • Адрес: Минск, ул. Мельникайте, 2, оф. 710 • E-mail: info@kv.by • Тел. редакции (017) 203-90-10 • Размещение рекламы: adv@kv.by

DLP и пиар: вещи совместимые

Борьба с пиратством в Беларуси

Концепция BYOC: знакомимся

Человеческий IT-конфликт

Symantec об угрозах

Концепция BYOC: знакомимся

Виктор ДЕМИДОВ

Исследование, проведенное недавно аналитической компанией Forrester Research, показало: в США и Европе уже 53% сотрудников компаний используют на рабочем месте собственные компьютеры. Так на практике реализуется концепция BYOC — bring your own computer — политика использования на работе собственного компьютера.

Выгодно всем

В ходе исследования Forrester Research было опрошено около 10 тыс. сотрудников в сфере IT в компаниях со штатом более 20 человек в 17 странах. 53% сотрудников в США и Европе, следующих концепции BYOC, — это на 5% больше, чем в прошлом году. Причем самый высокий процент приверженцев BYOC оказался среди топ-менеджеров: 77% из них используют собственные компьютеры и 45% — собственное ПО.

По прогнозам экспертов Forrester, на протяжении ближайших трех лет в большинстве западных компаний собственные компьютеры сотрудников станут нормой. Более того, многие компании даже начнут требовать от сотрудников самостоятельно обеспечивать себя техникой — и это станет требованием, прописанным в трудовом контракте.

Но возникает вопрос: каковы в рамках концепции BYOC расходы сотрудников на IT-инструментарий для работы? Это вопрос тоже изучался в рамках исследования Forrester Research. Выяснилось, что среднестатистический сотрудник тратит на аппаратное и программное обеспечение для своей работы более $1200 в год, а у топ-менеджеров эта цифра достигает $4000. Примерно 74% сотрудников сообщили, что самостоятельно купили ноутбук для работы, прочие — выкупили у компании либо используют для работы лэптоп, купленный ранее для личных нужд.

Несомненно, рост популярности концепции BYOC прямо связан со значительным удешевлением ноутбуков в начале 2000-х, когда они по цене приблизились к аналогичным по мощности десктопам. Ну а сегодня производство ноутбуков уже и вовсе в полтора раза превышает мировое производство настольных ПК.

> **“По прогнозам экспертов Forrester, на протяжении ближайших трех лет в большинстве западных компаний собственные компьютеры сотрудников станут нормой.”**

Концепция BYOC (bring your own computer) подразумевает, что компания компенсирует сотруднику существенную часть стоимости оборудования при условии, что он будет работать на этом оборудовании. Система удобна всем: компания гарантирует, что в офисе будет установлена самая современная техника, а сотрудник заботится о компьютере как о своем собственном (в общем, так оно и есть).

Так что первое и самое явное преимущество BOYC — экономия средств. По разным оценкам, компания экономит 15-20% расходов на компьютерную технику. Добавим сюда увеличение производительности труда. Как отмечают многие офисные сидельцы, использование собственного ПК в офисе психологически намного более комфортно, чем работа на “казенном” компьютере. Одновременно снимается проблема забытых дома файлов, “рабочих” и “личных” почтовых ящиков и ряд прочих проблем подобного рода. А все это закономерно повышает производительность.

Ну а если сотрудник работает в удалённом режиме, то компания в выигрыше вдвойне — ведь тогда он из собственного кармана оплачивает не только компьютер с периферией, но и накладные расходы: электричество, аренду рабочего места и т.д.

“Мобилизация” BYOC

Сама по себе концепция BYOC известна и реализуется на Западе уже лет десять, не менее. Но в последние два-три года она буквально обрела новое дыхание — благодаря тому, что в бизнесе начали все более активно использоваться мобильные устройства. В подавляющем большинстве случаев это, разумеется, смартфоны и планшеты. И налицо тенденция к наращиванию функционала мобильного бизнес-ПО.

В 2010-2011 годах очень активно развивался рынок корпоративных IT-решений, способных увеличить мобильность сотрудников. По большей части разработчики бизнес-ПО сейчас предлагают либо узкоспециализированные приложения для мобильных устройств, либо мобильные версии популярного делового софта.

Отраслевые аналитики по-разному оценивают “мобилизацию” мирового бизнеса. Так, IDC прогнозирует, что к 2013 году 35% сотрудников компаний будут работать с использованием мобильных устройств. А по оценке For-

Концепция BYOC: знакомимся

Forrester Research, уже сейчас 75% компаний в мире начали внедрять мобильные приложения. Эксперты агентства Yankee Group подсчитали, что внедренные в бизнес-процессы мобильные технологии дают прирост эффективности управления почти на 27%. Речь идет, в частности, об исключении непрофильных действий сотрудников, приросте количества заказов от клиентов, снижении стоимости сопровождения заказов.

Со стороны бизнес-структур сейчас растёт спрос на продукты, которые обеспечат сотрудникам доступ с мобильного устройства не только к электронной почте, но и к сведениям из корпоративных систем, инструментам совместной работы над документами, планирования и принятия решений.

Как показывает практика, сейчас бизнес-пользователи на своих мобильных устройствах активнее всего используют доступ в интернет и корпоративную почту. Несколько реже планшет или смартфон используется для работы с документами, в том числе мультимедийными.

Достаточно часто компании начинают внедрение мобильных бизнес-приложений с сотрудников коммерческих и маркетинговых подразделений (менеджеров по продажам), специалистов ремонтно-эксплуатационного (обслуживание банкоматов, терминалов, электротехнического оборудования, инженерных сетей) и логистического (экспедиция) департаментов.

> **“Одна из главных проблем BYOC — проблема безопасности.”**

Такой подход вполне логичен, так как в этих областях большинство специалистов работают “в поле” и нуждаются в мобильном доступе к набору приложений для управления взаимоотношениями с клиентами (CRM — Customer Relationships Management) и учетным системам по управлению ресурсами предприятия (ERP — Enterprise Resource Planning).

Но именно мобильные устройства, использующиеся в корпоративных IT-инфраструктурах, чаще всего оказываются личными аппаратами. Намного чаще, чем “полноценные” ПК. И сейчас внедрение технологий BYOC резко ускорилось именно благодаря проникновению в бизнес мобильных устройств.

Проблема безопасности

Одна из главных проблем BYOC — проблема безопасности в связи с тем, что некоторые сотрудники будут уделять недостаточно внимания защите своих ПК от вирусов и других угроз. Потребуется вводить жесткую политику в сфере безопасности. Возникает конфликт: IT-специалисту компании придется хозяйничать на личном ПК сотрудника, что вряд ли этому сотруднику понравится.

Далеко не каждая компания готова допустить, что ценная корпоративная информация будет храниться на персональном и потенциально незащищённом компьютере. Выходом может стать создание зашифрованных “корпоративных” разделов на диске и использовании виртуальных машин. В любом случае это должна быть какая-то стандартная корпоративная процедура.

Кроме того, есть труднорешаемый вопрос увольнения сотрудника, работавшего по схеме BYOC. Ведь уходя со своим ноутбуком, он уносит и информацию, с которой работал. Конечно, скорее всего она продублирована на корпоративном сервере. Но как быть с потенциальной утечкой данных на новое место работы сотрудника? Обыскивать HDD при увольнении? Но это уже вторжение в личную жизнь — компьютер-то личный... В общем, юристам придется еще немало поломать головы, совершенствуя BYOC.

Обсудить

DLP и пиар: вещи совместимые

Роман ИДОВ, компания SearchInform

Не секрет, что любая компания ищет любой удобный повод для написания пресс-релиза и дополнительного упоминания себя, любимой, в печатной прессе и в онлайновых изданиях. Внедрение системы защиты от утечек данных, как показывает практика, тоже нередко используется как информационный повод самыми разными компаниями. Однако так ли хорош этот повод, как кажется на первый взгляд?

Безусловно, внедрение системы защиты от утечек данных, или, как сейчас модно говорить, DLP-системы, — это очень и очень правильный шаг, который клиенты компании могут только приветствовать. Это дополнительный шаг к сохранности персональных данных, о которой столько говорится в российской прессе в последнее время. Это и шаг к повышению дисциплины среди сотрудников, а, значит, и к улучшению качества услуг, оказываемых компанией. Казалось бы — почему бы не написать об этом в пресс-релизе? Тем не менее, помимо позитивных моментов, с точки зрения обывателя факт внедрения DLP-системы несёт в себе и ряд негативных черт.

Давайте вспомним, от чего именно защищают нас DLP-системы. От утечек конфиденциальной информации, обусловленных деятельностью самих сотрудников компании. В пресс-релизе, рассчитанном на широкую публику, неизбежно придётся объяснять, в чём именно заключается роль DLP-системы, и каковы преимущества её внедрения. И как бы качественно не был написан такой пресс-релиз, у его читателя неизбежно возникнет вопрос: если понадобилось внедрять систему защиты от утечек информации, значит, был повод их опасаться? Именно поэтому в пресс-релизах, посвящённых внедрению DLP-систем, совершенно необходимо делать акцент на защите от непреднамеренных утечек, связанных со случайными ошибками сотрудников компании. В качестве примеров таких ошибок могут приводиться ошибки в набираемом адресе электронной почты, отправка сообщений не в то окно ICQ и т.д. Все эти ситуации наверняка будут хорошо знакомы тому, кто будет читать ваш пресс-релиз, и вызовут с его стороны понимание и поддержку действий компании.

Необходимо отметить, что сегодня подход к системам информационной безопасности таков, что их наличие воспринимается клиентами как что-то само собой разумеющееся. Конечно, DLP-системы с точки зрения пиара пока что выгодно отличаются от тех же антивирусов или файрволов — если вы выпустите сегодня пресс-релиз о том, что защитили свою корпоративную сеть каким-либо файрволом, то вряд ли встретите понимание со стороны журналистов, которые делают новостные материалы. Впрочем, ещё раз повторюсь, системы защиты от утечек данных пока не настолько распространены, и являются в некотором роде диковинкой.

Между тем, именно такое положение DLP-систем в мире средств защиты данных даёт дополнительный козырь при составлении пресс-релизам по поводу их внедрения. Компания, внедрившая у себя систему защиты от утечек данных, выглядит в глазах публики открытой для инноваций и использующей передовые информационные технологии — нужно не забывать подчёркивать это в тексте пресс-релиза.

Многие компании опасаются выпускать пресс-релизы, посвящённые внедрению DLP-систем в их ИТ-инфраструктуру, не желая вовсе афишировать её установку. Опасения эти связаны с представлениями о том, что если сотрудник, желающий “слить” конфиденциальную информацию о компании куда-то на сторону, не будет знать о существовании DLP-системы, то его можно будет поймать с поличным. Руководство компании зачастую желает с помощью DLP-системы выявить нелояльных сотрудников, которые способны организовать утечку конфиденциальной информации за пределы компании. Эти представления, между тем, ошибочны и даже, можно сказать, наивны. Установка DLP-системы, в любом случае, не окажется тайной для тех сотрудников компании, которые будут отвечать за внедрение DLP-системы. Не окажется она тайной и для всех остальных, потому что, как давно известно, если что-то знают двое, это знают и все остальные. В то же время, DLP-система, установленная у вас в компании заставит потенциальных нарушителей политики информационной безопасности три раза подумать, прежде чем совершать какие-либо действия, способные нанести компании ущерб. Публичное заявление об установке DLP-системы продемонстрирует сотрудникам уверенность руководства компании в том, что компания надёжно защищена, и заставит инсайдеров снизить активность или вовсе отказаться от своих планов.

> “Руководство компании зачастую желает с помощью DLP-системы выявить нелояльных сотрудников.”

Таким образом, как можно увидеть, внедрение DLP-системы в информационную среду компании вполне может служить информационным поводом, однако при написании пресс-релиза по нему стоит помнить о некоторых простых правилах, которые позволят вашей компании выглядеть более привлекательно именно благодаря установке системы защиты от утечек информации.

Обсудить

Человеческий IT-конфликт

Виктор ДЕМИДОВ

Проблема взаимоотношений “айтишников” и “не-айтишников” давно уже стала неотъемлемым элементом IT-фольклора. Наверняка многие читатели “КВ” часто посещают и башорговский подресурс IThappens. Однако “веселенькие истории” зачастую скрывают за собой настоящие человеческие драмы, напрямую связанные со взаимным IT-недопониманием.

Сейчас модно разбирать различные проблемы в бизнес-процессах в виде так называемых “кейсов” — конкретных примеров из реальной жизни. Такой “кейс” я и хочу сейчас разобрать — это как раз тот случай, когда для разрешения конфликта, связанного с IT-проблемами, требуется, прежде всего, знание психологии.

Описанную ниже ситуацию я наблюдал своими глазами в одной из белорусских фирм. Я в ней не работал, но выполнял для них некоторые заказы, так что в офисе этой фирмы провел достаточно много времени.

Итак, имеем небольшую фирму (около 50 сотрудников), которая занимается мелкооптовой торговлей. Большая часть штата — “офисные хомячки”, менеджеры по продажам. Из прочих — директор, замдиректора, традиционная секретарша, офис-менеджер, бухгалтерия и сисадмин. Классический сисадмин, поросший бородой и свитером, в серверной комнатушке, заваленной разнообразным IT-хламом.

Практически все продажники в той фирме владели компьютерными премудростями на уровне коечему обученных пользователей. Однако вся их работа была связана с ПК — переписка с клиентами, отчеты в Excel, деловые письма в Word, веб-серфинг в поисках новых деловых контактов...

Сисадмин, замечу, не только следил за работой сервера, локальной сети, пользовательских ПК и оргтехники. Он ещё проводил какую-никакую корпоративную IT-политику. На пользовательских компьютерах верещал регулярно обновляемый “Касперский”, единственным разрешенным браузером была Opera, а почтовым клиентом — The Bat. Доступ в любые социальные сети блокировался до 17.00, посещение сайтов по трудоустройству внимательно отслеживалось и докладывалось начальству.

Однако однажды в фирму пришел работать новый “продажник” — молодой и весьма перспективный торговый менеджер, показывавший заметно лучшие результаты по сравнению с коллегами. При этом новичок оказался еще и изрядно технически подкован. Скажем так, на уровне весьма продвинутого пользователя. Причем он пришел работать с собственным ноутбуком — в отличие от прочих продажников, работавших на уже далеко не новых десктопах, принадлежащих фирме.

Подключая новичка к локальной сети фирмы, сисадмин вкратце изложил ему корпоративную IT-политику. И потребовал поставить перечисленный выше набор — Opera, The Bat и “Касперского”. Однако новый торговый менеджер “оказал сопротивление”. Заявил, что ему комфортнее работать с браузером Google Chrome, почтовой программой Mozilla Thunderbird, а его лэптоп вполне надежно защищен программами от ESET. И с запретами на использование каких-либо веб-ресурсов он также не согласен.

Сисадмин категорически отмел возражения, мотивировав это тем, что менеджер будет работать в корпоративной сети, а значит, должен подчиняться общим правилам фирмы. Новичок напомнил, что ноутбук не фирменный, а его собственный, и ПО на нем он распоряжается исключительно сам. В результате спор пошел на повышенных тонах. Новый сотрудник заявил, что все равно будет работать на том, на чем захочет. Сисадмин ответил, что в таком случае интернет-доступ у него будет на скорости телефонных модемов середины 1990-х, то есть медленный и печальный.

“Разбираться” отправились к замдиректора. Он, довольно молодой парень (28 лет), также был достаточно хорошо подкован в IT-вопросах, хотя корпоративную IT-политику соблюдал беспрекословно. Хотя, конечно, как начальник имел полностью открытый доступ к “ВКонтакте” и “Одноклассникам”.

Однако замдиректора, немного подумав, сообщил, что этот вопрос не в его компетенции. Дескать, корпоративную IT-политику утверждал лично генеральный директор, так что ему ре-

Человеческий IT-конфликт

Ошать. (Интересно, почему у небольших фирм директор всегда не простой, а непременно генеральный?)

Гендиректор был бывшим чиновником, заметно за 60 лет. Свой дорогой ноутбук он рассматривал исключительно как аксессуар большого босса — пользоваться им глава фирмы не умел категорически.

Услышав тему конфликта, но совершенно не поняв его суть, генеральный постановил: есть утвержденная IT-политика, предусматривающая вполне определенное ПО и ограничительные меры. И ради одного сотрудника правила нарушаться не будут.

Финал оказался безрадостным. Молодой талантливый менеджер по продажам был востребован на рынке — и ушел из описанной фирмы, не проработав в ней и трех дней. Именно из-за конфликта с сисадмином, который не смогло или не захотело разрешить начальство.

А теперь давайте посмотрим на роли каждого из участников данного кейса с точки зрения психологии. Причем глубокой науки тут не потребуется — хватит и моего университетского курса психологии.

Итак, молодой *менеджер по продажам*. Видно, что он не только умен, но и понимает свое превосходство над ровесниками/коллегами. Амбициозен и не хочет подчиняться общим для всех правилам. Причем имеет на то моральное основание. А вот дипломатичности ему еще предстоит научиться.

Сисадмин. Имея (негласно) доступ ко всей внутрифирменной документации, он знает, что получает даже меньше, чем офис-менеджер Мария Ивановна — недоучившийся школьный преподаватель младших классов. Это он-то, человек с высшим техническим образованием! А Мария Ивановна сама даже поменять раскладку клавиатуры не может!

Униженный статус сисадмина в фирме приводит к тому, что он подсознательно использует любую возможность проявить власть. Это называется “эффектом вахтера”: чем ниже уровень чиновника, тем сложнее с ним иметь дело. В нашем кейсе именно “эффект вахтера” проявился конфликтом сисадмина с новым продажником. Ведь понятно, что использование Google Chrome и Mozilla Thunderbird никак не угрожали информбезопасности фирмы. Да и закрывать соцсети для амбициозного менеджера незачем — все равно он не будет сидеть в них в ущерб работе, а вот полезные контакты наверняка там наладит. Но сисадмин решил проявить власть — ведь в обычной жизни у него так мало возможностей почувствовать себя влиятельным...

Конечно, чисто теоретически сисадмин со своим уровнем компетенции мог бы добиться в жизни намного большего. Но отсутствие навыков социальной коммуникации не позволяет ему строить карьеру. Да и вообще, в торговой фирме специалист компьютерного профиля карьеру явно не сделает — это удел менеджеров по продажам. То есть ему стоило бы уйти в IT-компанию и там пробиваться наверх. Вот только данный конкретный сисадмин, как и многие его сородичи, — совершенно не амбициозен. Ему комфортнее общаться с компьютерами, чем с людьми, а потому он продолжит обрастать бородой и свитером на окладе в $350 в безвестной фирмочке.

> “Униженный статус сисадмина в фирме приводит к тому, что он подсознательно использует любую возможность проявить власть.”

Заместитель директора. Классическое проявление не лучших черт белорусского характера. Предпочел действовать по принципу “моя хата с краю” — хотя вполне мог разрешить конфликт, предпочел не принимать вообще никаких решений. Ведь принятие решения означает ответственность за него. Вот он и переложил эту ответственность на плечи начальника. И руки не замарал, и обиженных на него нет...

Ну а *гендиректор*, как я уже говорил, суть конфликта совершенно не понял по причине отсутствия каких-либо компьютерных познаний. Но повел себя в рамках психологической модели советского (или, точнее, “совкового”) начальника. Он подтвердил свое прежнее распоряжение (о корпоративной IT-политике) не потому, что считал его верным, а просто чтобы напомнить подчиненным “кто в доме хозяин”. Так сказать, подтвердить важность и незыблемость своих решений.

Вот такая вот психологическая катавасия в рамках отдельно взятой фирмы. На первый взгляд, дело во взаимном непонимании IT-вопросов, но на самом деле — не очень глубокая психология. Которую стоит учитывать даже при выборе штатного браузера или почтового клиента.

Обсудить

“Корсары” виртуальных морей

Елена ХАРЛАМОВА

Компьютерное пиратство в современном мире приобретает поистине грандиозные масштабы. Как и всякий вид нелегального бизнеса, оно несет создателям поистине баснословные прибыли, что вызывает значительный отток финансов от “белых” производителей программного продукта. Каковы основные виды пиратства и методики борьбы с ними? Об этом и пойдет речь в нашем материале.

— Существует традиционная привычка — сравнивать ситуацию в Беларуси с тем, что было вчера и позавчера, — отметил директор Ассоциации по защите авторских прав в сфере информационных технологий Дмитрий Ананьев. — Целесообразнее было бы проводить подобные параллели с нашими соседями. Ситуация заключается в том, что развитие ИТ — отрасли является одним из государственных проектов. Парком высоких технологий и Инфопарком были подготовлены определенные документы, которые свидетельствуют, что экономическими флагманами стран с высоким уровнем развития являются ИТ-компании. Это тот ресурс, который позволяет превращать интеллектуальную собственность в доход страны. По данным статистики, уровень компьютерного пиратства в развитых странах намного ниже аналогичного в Беларуси. Помимо статистики, оценивался еще и объем черного рынка, который на данный момент составляет $55 млн.

Компьютерные программы не могут стоить четыре доллара за диск. Они ввозятся в нашу страну, растаможиваются. При этом выплачиваются таможенные платежи и налог на добавочную стоимость. Естественно, когда официальные поставщики легально уплачивают необходимые налоги и сборы, цена конечного продукта значительно возрастает. Какие угрозы компьютерное пиратство несет для экономики? Помимо неуплаты налогов и сборов, возникает отток квалифицированных кадров с ИТ-предприятий и оплата в конвертах. На протяжении 10 лет проводились экстраполяционные исследования, которые доказали, что уменьшение объема пиратского рынка создает рабочие места и профильную инфраструктуру. Появляются новые организации, которые обеспечивают создание рабочих мест. При наличии черного рынка подобные организации не создаются.

Помимо экономических угроз, существуют также угрозы для информации. Для пользователей персональных компьютеров были проведены статистические исследования, которые доказали, что при установке нелицензионного ПО возникает угроза полной потери информации, хищения конфиденциальных данных, а также несанкционированной установки вредоносных программ. В 80% случаев при закачке с торрентов нелицензионного ПО, оно содержит программы-черви, которые наносят вред компьютеру. Находясь в дремлющем состоянии, в нужное время они “просыпаются” и передают информацию с компьютера.

Что же касается правового использования компьютерных программ, то подобные программы являются объектом интеллектуальной собственности. Это означает, что обладателю имущественных прав (автору либо правообладателю) принадлежат объекты интеллектуальной деятельности. Правообладателю принадлежит исключительное право использования этой программы по своему усмотрению. Только он имеет право сохранять программу на свой компьютер, импортировать, продавать и сдавать ее в прокат. Иные лица могут использовать ее только с разрешения правообладателя. Для того, чтобы они могли пользоваться программой, необходимо, чтобы с правообладателем был заключен лицензионный договор. По этому договору передаются права от правообладателя к пользователю. При этом последнему передаются только те права, которые указаны в договоре. В ИТ-сфере существует расхожий термин “лицензия”. Под ним понимается договор. И когда существуют различные виды договора, то есть различный объем передаваемых прав, мы говорим, что существуют различные виды лицензий.

За использование компьютерной программы любыми способами, которые не указаны в лицензионном договоре, наступает уголовная либо гражданско-правовая ответственность.

Борьба с компьютерным пиратством: опыт российских коллег

— На сегодняшний день сформирована общенациональная сеть о борьбе с компьютерным пиратством, — рассказывает ведущий специалист Некоммерческого партнерства поставщиков программных продуктов РФ Евгений Воронов. — По последним данным, она включает 144 населенных пункта в России и странах СНГ. Численный состав данной сети постоянно изменяется в сторону увеличения.

Разработка компьютерных программ — это современное высокотехнологичное производство, требующее весомых затрат как интеллекта, так и финансов. Программное обеспечение — это абсолютно возобновляемый ресурс, и ни для кого не секрет, что бизнес информационных технологий, и в частности, развитие рынка ИТ, постоянно совершенствуется. Возникают новые ресурсы, и то, что еще полгода назад было актуально и вызывало восторг, сейчас становится устаревшим. Поэтому разработка программного обеспечения идет в ногу со временем. Развитие информационных технологий — это необходимое условие для развития современного общества.

Чем же опасно пиратство? Если разработчик затрачивает силы, время и средства на исследование рынка, разработку программ, тестирование и оплату, то пират тратится исключительно на тиражирование и продажу. И,

“Корсары” виртуальных морей

соответственно, как и любой нелегальный бизнес, получает баснословные прибыли. Если легальный разработчик может иметь доходность от своего программного продукта 30%, то доходность пиратов составляет 900% — по причинам, указанным выше. Ни о какой конкуренции здесь, безусловно, не может идти и речи.

Важность защиты авторских прав в Российской Федерации осознана на высшем уровне. В 2001 году Владимир Путин, занимавший в то время пост президента России, встречался с представителями ИТ-индустрии. Данная встреча носила позитивный характер, и после нее усилилась борьба с компьютерным пиратством на уровне государства. В частности, была принята новая редакция статьи 144 УК РФ.

Традиционных видов пиратства в России заметно поубавилось. Нетрадиционные же, такие как интернет-пиратство, продолжают процветать. С интернет-пиратами еще не научились окончательно бороться. Причинами его являются мало проработанное законодательство, а также малый рост правоприменения.

Умирающим видом пиратов в России являются лоточники. Связано это с бурным развитием интернет-технологий. Помимо этого, с нелегальными торговцами на лотках начала активно бороться милиция. Большое внимание данному виду пиратства уделяется по-прежнему. Казалось бы, чего проще — купить раскладной стол либо арендовать небольшой павильон в людном месте и активно торговать контрафактом.

Достаточно распространенным видом пиратства, который сегодня сходит на нет, стали предустановщики. В уменьшении их активности следует видеть усиление контроля со стороны правообладателей и правоохранительных органов. Это может быть небольшая фирма, которая занимающаяся реализацией компьютеров, которая, чтобы быть конкурентоспособной на рынке, предлагает покупателю наравне с “железом” установку нелицензионного софта, операционной системы, дополнительных приложений и прочего.

По черным внедренцам ситуация остается прежней. Черными внедренцами называют физических и юридических лиц, которые занимаются нелицензионным распространением компьютерных программ. Качество их услуг весьма низкое, и люди это достаточно асоциальные: либо студенты, либо безработные, которые ссылаются на свое затруднительное материальное положение. Имея порой самые начальные навыки обращения с компьютером, они размещают объявления с предложениями услуг по обслуживанию программ. Число их не уменьшается — в связи с обильным предложением появляется и спрос. Пользователь не хочет приобретать лицензионные продукты, предпочитая воспользоваться услугами данных лиц. В связи с тем, что в России это один из основных видов пиратства, наработана богатая практика борьбы с ними. Выкладывание же в сети нелегального контента, ввиду непроработанности законодательства, приобретает все большие масштабы. В 2004 году ситуацию с черными внедренцами удалось переломить. Навыки борьбы с ними уже отработаны. В России был достаточно громкий прецедент по созданию иммулятора ключа защиты. Разработчики его были осуждены в Благовещенске по статье 273 УК РФ. После этого черных внедренцев стали привлекать к уголовной ответственности не только за нарушение авторских прав, но и за использование и установку нелегального ПО.

С предустановщиками и лоточниками ведет активную борьбу милиция. Против последних были направлены такие операции МВД, как “Сеть” и “Контрафакт”. Проходили массовые рейды, направленные на выявление компьютерных пиратов. Осуществляются негласные закупки, соответственно, после которых выносятся обвинительные приговоры. Обсуждение данной проблемы ведется на уровне Государственной Думы и правительства РФ. Тем не менее, несколько обвинительных приговоров по по интернет-пиратам все же было вынесено.

Интернет является поистине кладезем информации для пиратов: в нем можно как разместить объявление об услугах черных внедренцев, так и распространить нелегальный контент с прямым извлечением доходов, предоставляя возможность скачивать с торрентов нелегальное ПО. Также можно предоставлять бесплатное скачивание с целью поднятия рейтинга, установку рекламных баннеров и распространять нелегальные программы. Как и любая программа, направленная на то, чтобы взломать программную защиту легального продукта, она несет потенциальный вред. Правоохранителями ведется активный мониторинг подобных действий с последующей передачей информации в компетентные органы. Поскольку компьютерным пиратством занимается Управление “К” БСТМ МВД России, пишутся письма провайдерам, которые, как правило, идут навстречу и закрывают доступ к нелегальному контенту по просьбе правообладателя.

В целом же, компьютерное пиратство на сегодняшний день несет целый ряд угроз, как экономического, так и информационного характера. Поэтому борьба с данным видом преступности должна быть планомерной и комплексной, что прекрасно понимают специалисты.

Обсудить

Виды лицензий:

— однопользовательская: правообладатель разрешает использовать компьютерную программу только на одном компьютере;

— сетевая: правообладатель разрешает использовать компьютерную программу в сети одной организации;

— для коммерческого использования: правообладатель разрешает использовать эту программу в сети одной организации;

— свободная: правообладатель разрешает использование данной программы без оплаты.

Эксперт Symantec: защита от угроз во всем мире примерно одинакова

Беседовал Вадим СТАНКЕВИЧ

Информационная безопасность — тема, сегодня актуальная, как никогда. О ней мы решили поговорить с Александром Суязовым, консультантом по информационной безопасности компании Symantec.

— На Ваш взгляд, оправдана ли нагнетаемая в последнее время вендорами паника по поводу утечек данных? Реально ли они так сильно вредят, как об этом говорят?

— Она может быть оправдана в определенных случаях. Стоимость утечек может оценить только сама компания, так же, как стоят ли потенциальные утечки столько, сколько стоит защита. Есть компании, для которых утечка равносильна уходу с рынка и прекращению бизнеса. Это может касаться, например, фармацевтических компаний, имеющих свои разработки и ноу-хау. Для них утечка — это потеря всего бизнеса. В общем, как и для любой высокотехнологичной компании, имеющей уникальные разработки, которые напрямую касаются бизнеса. В том числе и ИТ-компании, например, разрабатывающие ПО. Малый бизнес, разумеется, значительно более чувствителен к утечкам, так как зачастую ресурсы небольших компаний ограничены, а направлений деятельности мало или оно вообще одно.

— А с чем чаще сталкиваются компании — с утечками из-за каких-то действий сотрудников, или с тем, что данные крадет, например, какой-то троян?

— Для малого бизнеса, разумеется, это действия сотрудников. Маловероятно, что кто-то будет заниматься целенаправленной атакой через трояны, хотя это и возможно. Часто крупные утечки происходят из-за банальностей: потеряли съемный носитель с конфиденциальными данными, распечатали документ и не уничтожили, бывает, даже выбросили старый компьютер, забыв почистить диски. Как ни странно, но сам с таким сталкивался. Если же говорить о людях — многие сотрудники, увольняясь, пытаются прихватить с собой данные, которые, в том числе, помогут им устроиться на новой работе. Про крупный бизнес сказать что-то сложнее. Там, в любом случае, принимаются комплексные меры. Вопрос только в стоимости добываемой информации.

— Достаточно ли сегодня приобрести специальное ПО, чтобы защититься от подобных угроз, или нужны какие-то более глубокие и вдумчивые меры?

— Тут опять стоит отталкиваться от стоимости ваших данных. Если цена стремится к нулю, то достаточно купить антивирус, чтобы обеспечить необходимый уровень безопасности и непрерывность бизнеса. Если вам есть, что терять — необходимы значительно более комплексные меры, и одного ПО будет мало. Вам необходимы люди, понимающие, как его настраивать, понимающие, как интерпретировать события, которые это ПО создает. Вам нужны организационные меры, направленные на повышение защищенности компании, начиная с базового обучения сотрудников (например, не отключать антивирус, смотреть на адрес сайта, куда они зашли, и многое другое).

— ПО для защиты от утечек обычно достаточно дорого стоит. Означает ли это, что оно адресовано лишь крупному бизнесу, а сектору SMB оно и не должно быть интересно?

Александр Суязов

— Дорого — понятие относительное. Если цена утечки — ваш бизнес, то стоимость покажется не очень высокой. Если говорить о DLP системах — они модульные, и даже SMB может выбрать себе модули, которые обеспечат значительное снижение рисков утечек, при этом, не потратив значительную сумму. У меня были проекты по DLP-решениям даже для компаний в 10 пользователей.

— Скажите, а есть ли какие-то региональные особенности защиты? В частности, для белорусских компаний?

— Наверное, могут быть определенные тонкости, связанные с законодательством конкретных стран, но в целом защита от угроз во всем мире примерно одинакова.

— А количество утечек тоже примерно одинаково? Просто, к примеру, об утечках в США сообщают регулярно, а о России и всем постсоветском пространстве новостей на эту тему заметно меньше.

— Дело в законодательстве. В США компании обязаны уведомлять о произошедших утечках лиц, которых эта утечка могла затронуть. К сожалению, у нас такого закона нет.

— А почему “к сожалению”?

— Если компания знает, что каждая утечка обойдется ей в значительную сумму, она старается более правильно строить системы защиты. И мне, как обычному человеку, будет житься спокойнее, если я буду знать,

Эксперт Symantec: защита от угроз во всем мире примерно одинакова

что моя личная информация, например, медицинского характера, будет под надежной защитой.

— Можете рассказать, что такое контроль уязвимостей?

— Уязвимость — это слабость целевых систем, которая приводят к тому, что с ними можно выполнить определенные действия. Уязвимости могут быть в ПО изначально или потому, что ПО было неправильно настроено. Есть специальные системы, выявляющие уязвимости (сканеры уязвимостей, vulnerability scanner), которые позволяют выявлять подобные уязвимости. Далее осуществляется процесс управления обнаруженными уязвимостями. Это больше организационный момент, когда компания принимает решение, какие уязвимости могут повлиять на ее бизнес и какие надо закрыть, а какими уязвимостями можно пренебречь. Ну, и сам процесс закрытия уязвимостей патчами, сторонним ПО или другими способами.

— Но ведь всё равно остаются какие-то уязвимости, для которых еще нет патчей?

— И для таких случаев есть специально ПО, которое не позволяет эту самую уязвимость использовать. Но, разумеется, тут много тонкостей, и каждый случай надо рассматривать отдельно. Довольно неплохой вариант — уходить с определенными сервисами в облака. Компании, для которых это прямой бизнес, уделяют очень много внимания защите своих облачных услуг. И далеко не каждая компания может позволить себе такие траты на безопасность.

— Ведь облачные услуги и задумывались как средство экономии на ИТ?

— Так оно и есть. И это очень актуально для малого бизнеса. Посмотрите стоимость, например, услуг почты Google и сколько будет стоить установить локально сервер, купить ПО, поддерживать это, платить администраторам... А в современном мире необходимо много средств защиты, которые в облачном исполнении обходятся значительно дешевле.

— И насколько велика может быть такая экономия для средств безопасности? На 10%, в разы?..

— Я могу говорить о ценах на наши продукты, которые входят в службу Symantec.Cloud. Например, защита почты от спама, вирусов, фильтрация доступа по типам сайтов обойдется в 70-80 долларов в год на человека. При этом надо учесть, что у нас есть очень жесткие соглашения об обслуживании (если мы пропускаем вирус — вы не оплачиваете услуги в этом месяце). Ну, и, разумеется, надежность. Мы гарантируем доступность этих сервисов 24x7. Теперь можно посчитать, сколько это будет стоить компании. Для высокой доступности сервисов вам необходимы: 2 канала в интернет, 2 сервера, ПО для кластеризации. По моим прикидкам, только 2 сервера обойдутся вам в сумму от 2 тысяч долларов. Тогда получается, что за стоимость 2-х серверов мы можем защищать 30 сотрудников в год, при этом не тратя денег на персонал для поддержки всех этих систем. Поэтому, если мы говорим о небольшом бизнесе — то альтернативы облачным средствам защиты у них практически нет.

— Есть ли у ваших облачных сервисов клиенты из Беларуси?

— Мы только недавно начали предлагать эти услуги в Беларуси. Так что пока нет, но это лишь вопрос времени.

— А есть ли облачные сервисы защиты от утечек?

Мне кажется, компании не готовы отдавать в облака подобные услуги. Есть DLP решения, которые работают с облачными сервисами, но база, в которой хранятся инциденты, содержащие конфиденциальную информацию, стоит в компании. Просто ценность такой базы может быть очень высока.

— Скажите, на Ваш взгляд, что в ближайшее время будет основным трендом в защите для корпоративных пользователей?

— Скорее всего, мобильные устройства. Мы все стремимся к этому. Мобильность, легкость доступа...

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.