Владимир Безмалый

Пути развития технологий защиты

Мы вступили в новую эру, которую уже успели окрестить эрой post-PC, в связи с чем всем специалистам по информационной безопасности хочется понять, как изменится характер угроз и каковы будут векторы защиты. Сегодня все чаще самими важными из них являются защита данных, повышение общей эффективности систем безопасности и управления ИТ-инфраструктурой, а также защита мобильных пользователей.

А не так давно самой большой опасностью, приводящей к потере данных, считались вредоносные программы. Кое-кто считает так до сих пор. Вкладывались и продолжают вкладываться огромные деньги в надежные антивирусные решения. Безусловно, инструменты, надежно защищающие от вредоносных программ, предлагающие средства контроля и блокировки и имеющие централизованное управление с помощью консолей управления необходимы. Антивирусные решения — очень важная часть стратегии ИТ-безопасности большинства компаний. Однако вряд ли одно их наличие можно назвать достаточной защитой.

Как показало исследование, проведенное «Лабораторией Касперского» совместно с агентством B2B International в 14 странах мира, включая Россию, в 2011 году, 9 из 10 компаний сталкивались с внешними киберугрозами. 91% компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. В России этот показатель еще выше — 96%. Более того, ситуация становится только хуже: почти половина участников исследования утверждают, что количество кибератак за этот период увеличилось, и лишь 8% говорят о незначительном снижении их числа.

Многие организации пострадали от киберпреступников: например, треть вирусных атак (а в российских компаниях — почти половина) закончилась потерей данных, при этом для 10% компаний это была важная для бизнеса информация.

Перечисляя киберугрозы, которые представляются самыми значительными, большинство участников исследования во всем мире ставят на первое место вирусы, шпионское программное обеспечение и другие вредоносные программы (61%). Спам назвали источником угрозы 56% респондентов. Третье место (36%) заняли фишинговые атаки, за ними идут сбои, вызванные проникновением в корпоративную сеть (24%), и DDoS-атаки (19%) (см. рисунок 1).

Опрос российских ИТ–специалистов показал, что чаще всего сбои в системе безопасности приводят к потере данных о платежах (13%), интеллектуальной собственности (13%),

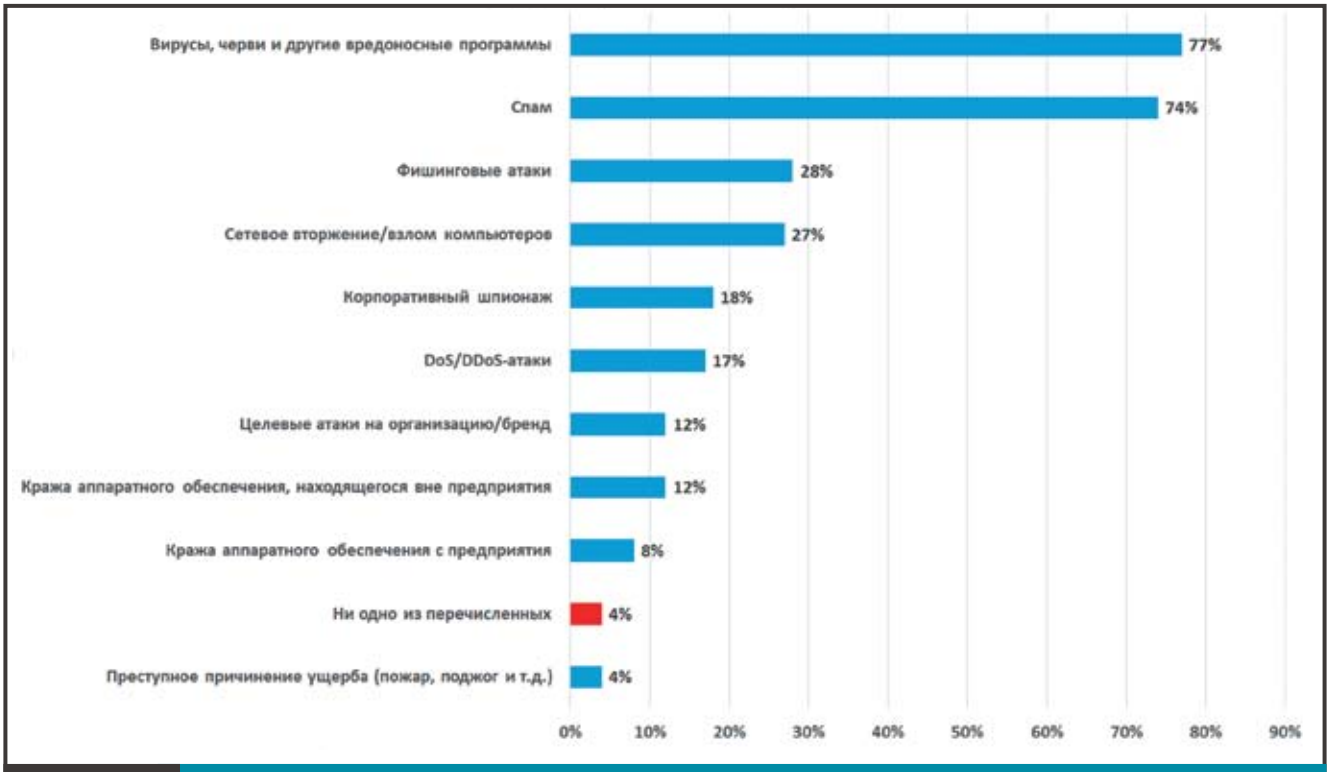

Рисунок 1 Типы внешних угроз, с которыми сталкивались российские компании

клиентских баз (12%) и информации о сотрудниках (12%). Вместе с тем 31% российских организаций не используют антивирусную защиту в полной мере.

Самые популярные меры, применяемые для защиты от киберугроз в компаниях во всем мире и в России (рисунок 2), — антивирусная защита, клиентские межсетевые экраны, установка обновлений (в том числе устраняющих уязвимости в программном обеспечении) и резервное копирование данных. Тем не менее 31% компаний в России не полностью внедрили антивирусную защиту (для сравнения — в Великобритании и США антивирусная защита внедрена в 92% и 82% компаний соответственно). Одна российская компания из ста не имеет вообще никакой защиты (в мире — 3% организаций).

Поскольку сотрудники недостаточно информированы об угрозах ИТ-безопасности, компании предпочитают ограничивать их общение в соцсетях. В 84% компаний в России сотрудники не имеют доступа к сайтам и приложениям социальных сетей или доступ к подобным ресурсам ограничен. В мире этот показатель несколько ниже — 72%.

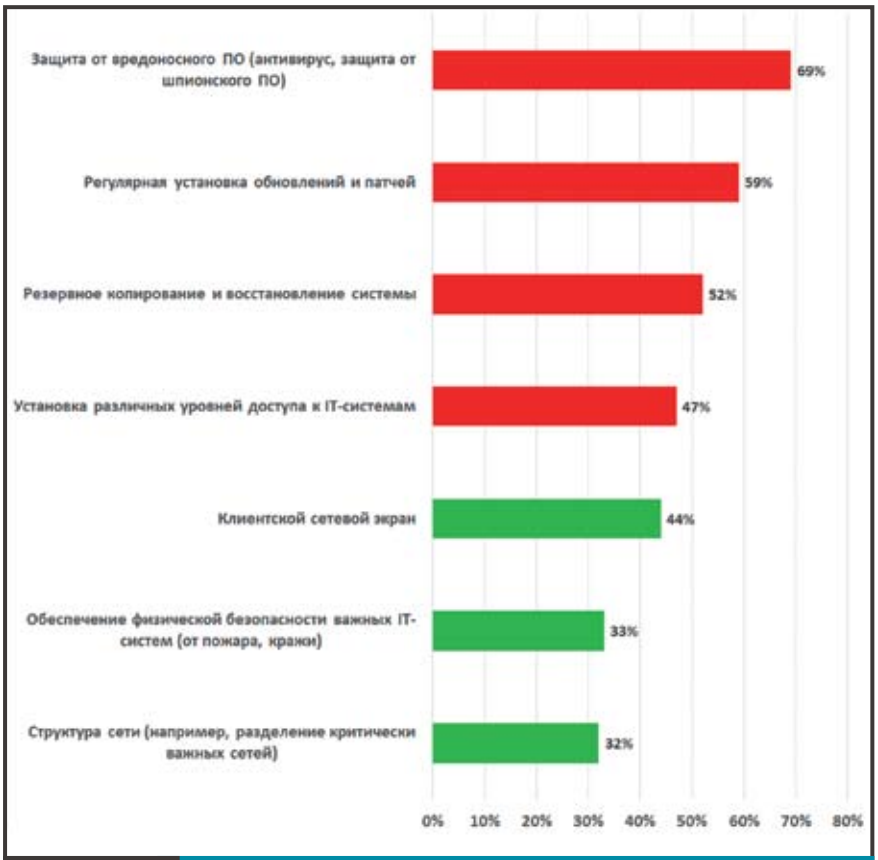

Рисунок 2 Наиболее широко применяемые в России меры по обеспечению информационной безопасности

По данным исследования, проведенного в 2012 году (рисунок 3),

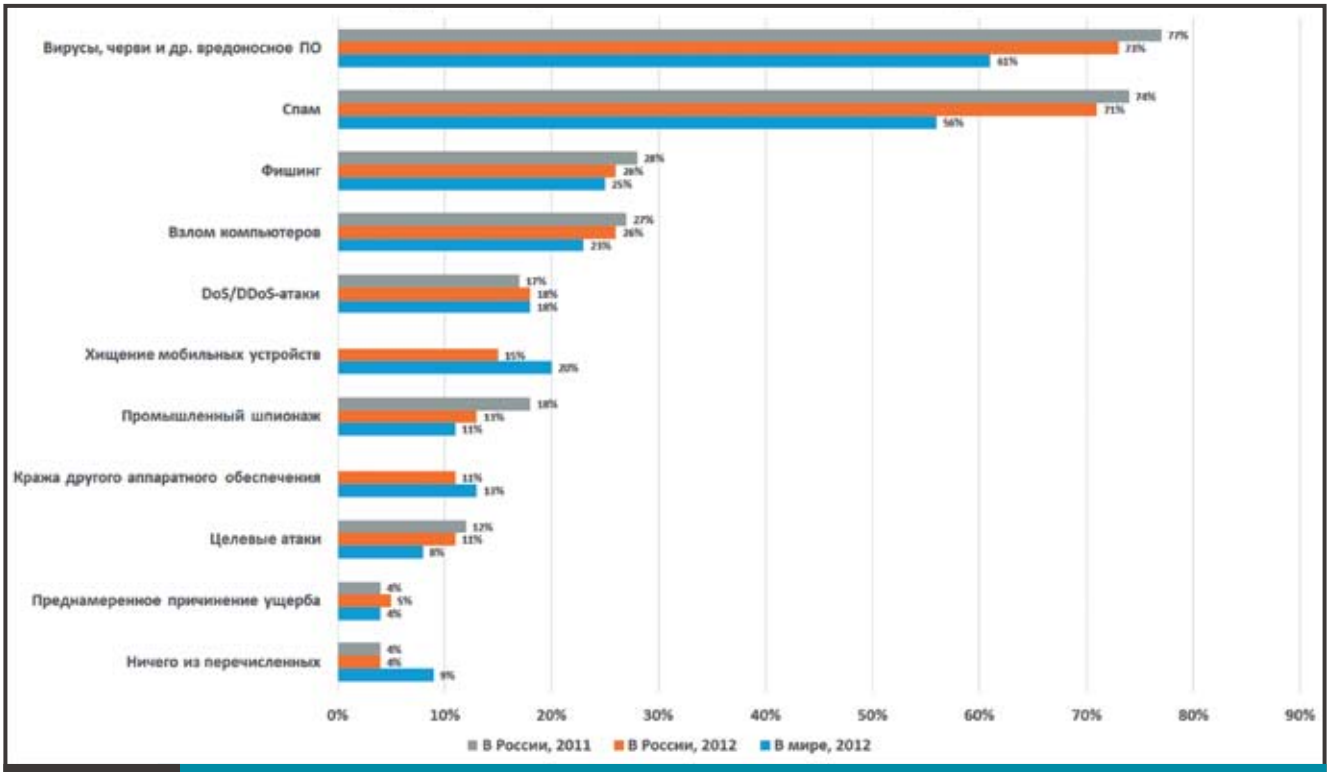

Рисунок 3 Киберугрозы, с которыми сталкиваются компании в России и в мире

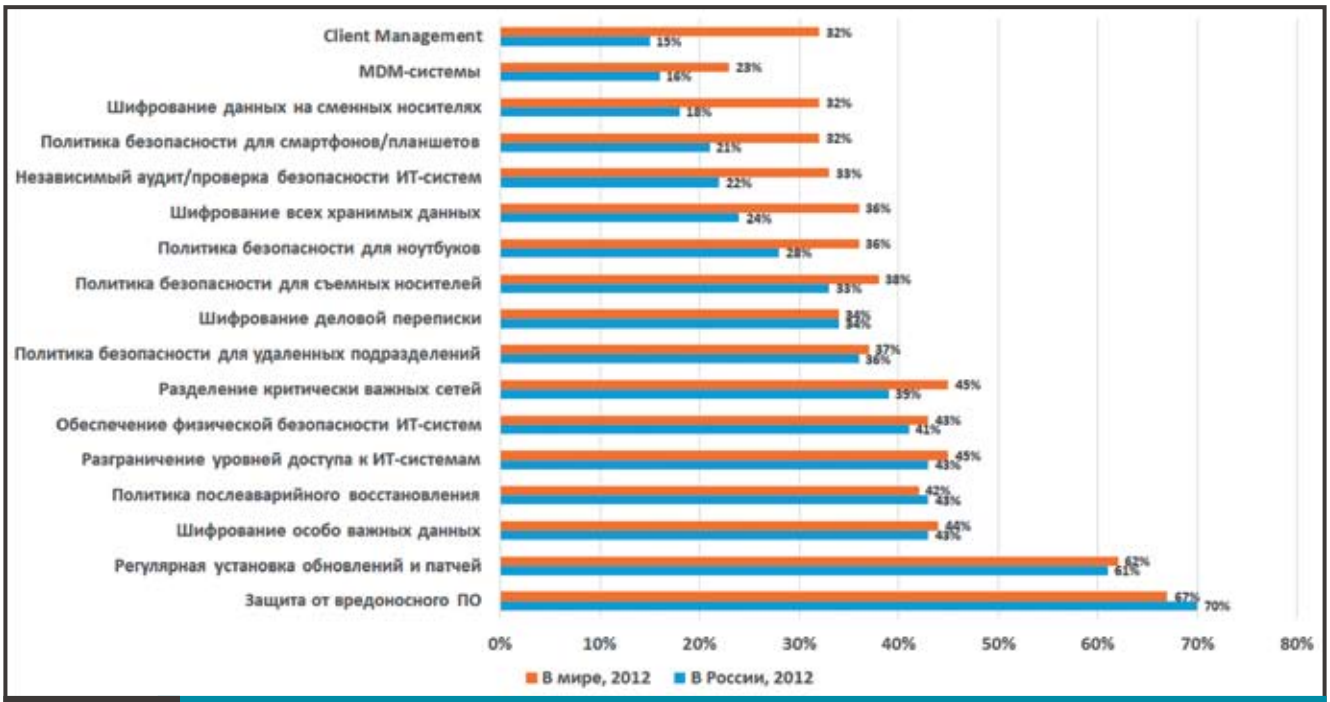

Рисунок 4 Меры по обеспечению информационной безопасности

44% российских ИТ-специалистов включили киберугрозы в тройку наиболее актуальных угроз для бизнеса, и в итоге они заняли вторую позицию в общем списке. При этом треть респондентов отметила значительное увеличение количества киберугроз в течение последнего года. Более того, 36% опрошенных уверены, что в ближайшие несколько лет актуальность этой проблемы будет только возрастать. Это весьма вероятно, учитывая растущее количество вредоносного программного обеспечения и постоянное появление новых видов атак.

Вместе с тем исследование показало, что, несмотря на осознание угрозы, которую представляет киберпреступность, многие компании не готовы к борьбе с такого рода опасностями. Так, только 60% опрошенных считают свои компании более или менее адекватно защищенными, что соответствует показателю 2011 года. Не лучшим образом обстоят дела и с защитой от других угроз ИТ-безопасности. В частности, от кражи интеллектуальной собственности недостаточно защищены 42% предприятий России, а 41% уверены, что используемая ими система защиты инфраструктуры не может пресекать попытки промышленного шпионажа. Таким образом, уровень защищенности бизнеса по-прежнему остается недостаточно высоким.

Рассмотрим меры, применяемые сегодня для обеспечения информационной безопасности в России и мире (см. рисунок 4).

Помимо исходящих от злоумышленников внешних угроз, существуют так называемые внутренние угрозы (рисунок 5), зачастую представляющие не меньшую опасность для компаний. Чаще всего ИТ-специалисты сталкиваются с различными уязвимостями в установленном программном обеспечении — этот пункт отметили 49% респондентов. И это неудивительно: целевые атаки на компании чаще всего проводятся с использованием уязви-

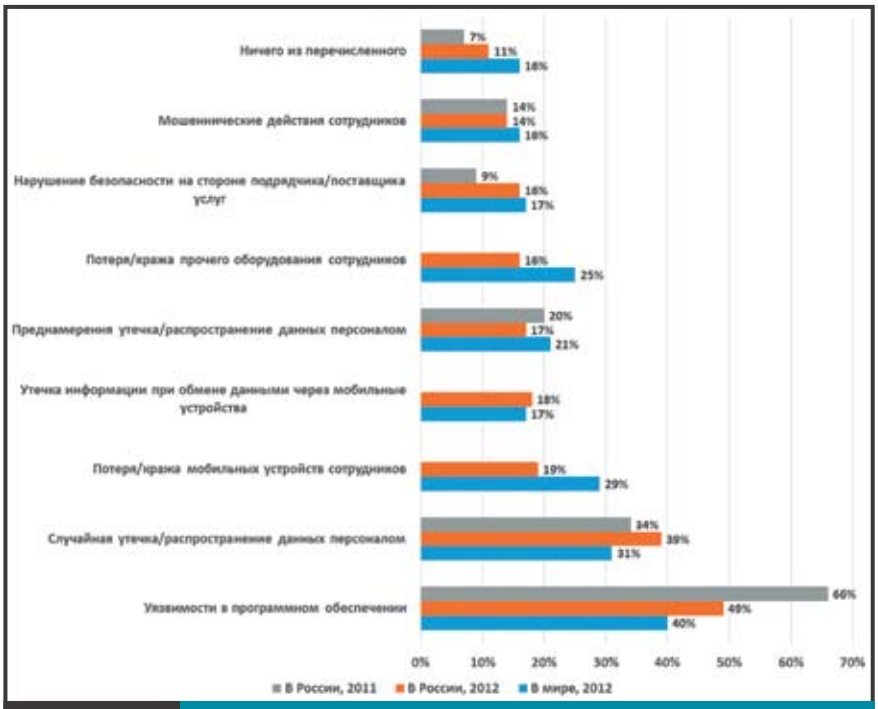

Рисунок 5 Внутренние угрозы

мостей в программах. Справедливости ради стоит отметить, что количество лазеек в программном обеспечении, с которыми пришлось столкнуться российским компаниям, по сравнению с прошлым годом сократилось, однако по-прежнему превышает среднемировой показатель. Другие внутренние угрозы напрямую связаны с действиями сотрудников компаний: 39% российских предприятий сталкивались за последний год со случайной утечкой данных из-за неосторожных действий персонала, 19% — с потерей или кражей мобильных устройств сотрудников.

Таким образом, можно сделать вывод, что киберугрозы сегодня — это не только вредоносные программы. Они гораздо сложнее и разнообразнее, поэтому одной антивирусной защиты уже недостаточно.

Исходя из этого, сегодня компании должны принимать во внимание следующие тенденции и риски.

- Риск использования необновленных приложений и операционных систем сотрудниками компаний. Как известно, такое программное обеспечение имеет немало уязвимых мест, которыми могут воспользоваться злоумышленники.
- В век мобильности, удаленных офисов, работы из дома конфиденциальные данные свободно перемещаются не только в пределах сети компании, но и вне сети — сотрудники переносят данные на сменных носителях, например на флэшке и т. д.
- Смартфоны и планшеты могут использоваться для доступа к корпоративной сети из любой точки мира. 62% сотрудников компаний по всему миру уже пользуются мобильными устройствами для работы, и это число увеличится до 85% в 2015 году.
- Сотрудники сами хотят использовать свои мобильные устройства и персональные компьютеры, чтобы их работа стала более удобной и оперативной.

Рассмотрим подробнее некоторые из этих тенденций.

Уязвимость приложений

Мишень «номер один», которую используют киберпреступники, — лазейки в приложениях. Приложения сторонних компаний загружаются и часто остаются необновленными в течение длительного времени. 75% всех уязвимостей, на которые нацеливаются злоумышленники, находятся в файлах PDF, Java, браузерах и других приложениях. К сожалению, большинство организаций не имеют четкого представления о данной угрозе.

Программы, в которых есть уязвимые места, — это наиболее популярный путь для атак и кражи персональных данных. Модули вредоносного кода, которые используют для инфицирования систем уязвимости в популярном программном обеспечении, применяются во вредоносных программах для кражи персональных данных потребителей, однако они же являются «философским камнем» магии киберпреступлений, когда речь идет о точечных атаках и кибервойнах. Обладатели кибероружия, такого как Stuxnet и Duqu, для проникновения в защищенные ИТ-инфраструктуры с целью совершения вредоносных действий и кибершпионажа использовали модули эксплуатации известных уязвимостей.

В период с января по декабрь 2012 года «Лабораторией Касперского» было проведено исследование уязвимостей на основании данных клиентов, использующих защитные решения «Лаборатории Касперского» для домашних пользователей. Основные результаты (см. рисунок 6):

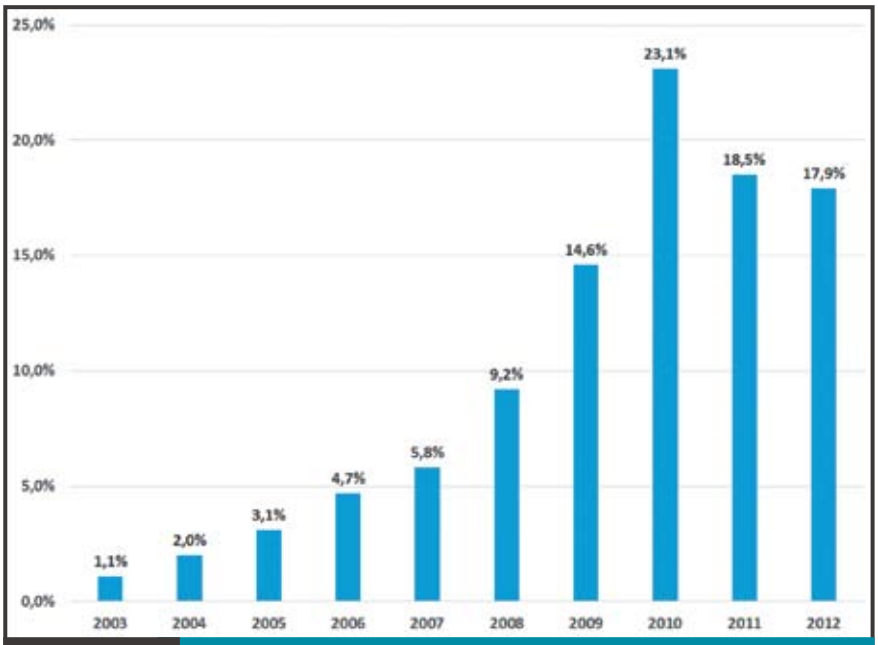

Рисунок 6 Результаты исследований в разные годы

- всего было найдено свыше 132 млн уязвимых приложений;
- в среднем на одного пользователя приходится 12 уязвимостей;
- обнаружено 806 уникальных уязвимостей; только 37 из них найдено по меньшей мере на 10% компьютеров в течение как минимум одной недели в период анализа (это уязвимости, способные привлечь внимание злоумышленников).

Названные 37 уязвимостей были обнаружены в 11 группах программ. Программы с наибольшим числом уязвимостей — Adobe Shockwave/Flash Player, Apple iTunes/QuickTime и Oracle Java.

Дальнейший анализ уязвимостей из этого списка выявил восемь лазеек, которые регулярно используются злоумышленниками в широко распространенных пакетах программ взлома.

Самые серьезные последствия имеют уязвимости в Oracle Java: пять из восьми наиболее активно используемых уязвимых мест обнаружено в Java. Оставшиеся две относятся к Adobe Flash, а последняя к Adobe Reader.

Средний уровень опасности для 37 самых часто встречающихся угроз — 3,7. Показатель рассчитан на основании уровня опасности каждой уязвимости и попадает в промежуток между

средним (ModeratelyCritical) и высоким (HighlyCritical).

Самый тревожный вывод из этого исследования таков: пользователи трех наиболее уязвимых программ (Java, FlashPlayer и Adobe Reader) крайне неохотно переходят на новые, безопасные версии. При дальнейшем изучении использования Oracle Java становится видно, насколько серьезна ситуация: через семь недель после выпуска новой версии обновление выполнили менее 30% пользователей, несмотря на реальную угрозу кражи данных. Для достижения таких же показателей по установке пользователями свежих обновлений наиболее популярных веб-браузеров требуется всего 5–7 дней.

Наилучшей стратегией во избежание потенциальных рисков безопасности в отношении уязвимого программного обеспечения является поддержание всех ваших программ в актуальном состоянии (хотя одного этого недостаточно). «Возраст» уязвимостей показывает, что пользователи не слишком заботятся об этом. И лишь в редких случаях виноват оказывается разработчик программы, поскольку он сам не выпустил обновления.

Даже когда производитель программы прикладывает все усилия для обнаружения брешей в защите и своевременно выпускает обновления, для значительной части пользователей это ничего не значит. Известная, опасная и эксплуатируемая злоумышленниками уязвимость на миллионах компьютеров остается не закрытой и через месяцы после того, как была обнаружена и исправлена. Существуют лазейки, которые остаются на компьютерах и через несколько лет после обнаружения и выпуска исправления.

Мы не можем винить в этом пользователей: они не обязаны быть специалистами в сфере информационной безопасности. Что действительно необходимо, так это хорошо налаженный автоматизированный процесс обновления для уже установленного программного обеспечения и на практике большее внимание к безопасности со стороны разработчиков. Исходя из сказанного, компаниям можно предложить следующие рекомендации.

В организации должен существовать постоянно обновляемый список используемого программного обеспечения с учетом версий. Контроль приложений должен вестись централизованно. Так же централизованно должна осуществляться установка патчей и обновлений версий используемого программного обеспечения. Задача ревизии используемого программного обеспечения является достаточно трудоемкой для многих подразделений ИТ. Поэтому важно максимально автоматизировать этот процесс.

В случае если сканирование на наличие уязвимостей проводится впервые, полученный результат зачастую может просто повергнуть в уныние специалистов по информационной безопасности. Ведь многие пользователи и компании даже не задумываются об обновлении приложений, если их все устраивает. Ведь полностью устаревшее программное обеспечение может годами работать в компании.

Решением в данном случае может быть использование программных продуктов, которые позволят вам следить за выходом новых версий установленного программного обеспечения. Другим подходом является шифрование критически важных данных, ведь основная цель атаки — именно хищение таких данных, а шифрование поможет их защитить, даже если заражение уже произошло.

Защита данных. Сегодня многие компании поддерживают удаленную работу сотрудников. Значительная часть сотрудников работает, используя мобильные устройства. Число таких устройств постоянно растет. По данным исследования компании Intel, 5–10% всех ноутбуков будут потеряны или украдены в течение срока их службы. Как мы можем убедиться, что ценные данные защищены, если это произойдет?

Защита мобильных устройств. Пользуясь мобильными устройствами, сотрудники получают доступ к информации компании (в частности, к электронной почте). Как правило, они рассчитывают, что компания позаботится о безопасности данных, и не только о защите от вредоносных программ, но и мерах на случай потери или кражи мобильного устройства. Тем не менее 75% сотрудников не считаются с политикой безопасности компаний.

Рассмотрим основную статистику мобильного вредоносного программного обеспечения за 2012 год.

Основная статистика за 2012 год

Наиболее значимым статистическим показателем за 2012 год стал взрывной рост числа вредоносных программ для Android. Если в 2011 году сотрудниками «Лаборатории Касперского» обнаружено почти 5300 новых вредоносных программ для всех мобильных платформ, то в отдельные месяцы 2012 года число обнаруживаемых ими Android-зловредов превышало этот показатель. А если говорить об общем количестве уникальных вредоносных файлов, то их насчитывается уже более 6 млн. Общее число модификаций и семейств мобильных вредоносных программ в коллекции «Лаборатории Касперского» на 1 января 2013 года показано в таблице.

Темпы роста числа зловредов для мобильных устройств стремительно растут: 40 059 из 46 415 модификаций и 138 из 469 семейств мобильных вредоносных программ попали в коллекцию 2012 года.

Если в конце 2011 года на долю Android приходилось порядка 65% всех мобильных вредоносных программ, то к концу 2012 года доля Android-зловредов в списке практически достигла 94%.

Со времени появления вредоносных программ для мобильных устройств каждый год происходят события, которые определяют очередной этап эволюции мобильных зловредов. И 2012 год можно назвать, пожалуй, одним из наиболее значимых, и вот почему.

- В этом году количество мобильных зловредов резко выросло.
- Произошло окончательное становление Android в качестве основной мишени киберпреступников.
- Мобильные угрозы стали «интернациональными». Сегодня целью киберпреступников являются не только российские или китайские пользователи мобильных устройств, как это было раньше. Инциденты с немалыми размера-

ми ущерба были зафиксированы и в других странах.
- Были получены доказательства того, что мобильные устройства и данные, которые на них хранятся, могут быть целью не только обычных киберпреступников, но и различных организаций, которые стоят за атаками, подобными Red October.

То, что еще год назад казалось незначительным, сегодня оценивается ИТ-специалистами как реальная угроза. Согласно результатам исследования, 32% опрошенных видят в мобильных устройствах серьезную угрозу безопасности бизнеса, а 47% признались, что уделяют гораздо больше внимания безопасности корпоративных смартфонов и планшетов по сравнению с прошлым годом. 5% опрошенных уже сталкивались с утечкой важной информации из-за кражи или утери мобильного устройства сотрудника.

Хотя ИТ-специалисты все больше склонны считать личные мобильные устройства угрозой безопасности, руководители компаний не торопятся запрещать или как-либо ограничивать их использование для работы. Так, неограниченный доступ с личных смартфонов ко всем корпоративным ресурсам поддерживают 31% организаций. При этом уровень внедрения специальных средств для обеспечения безопасности мобильных устройств Mobile Device Management пока крайне низок.

Тем не менее большинство компаний положительно оценивают концепцию Bring Your Own Device (использование сотрудниками личных устройств для работы) либо считают такое направление развития ИТ-инфраструктуры неизбежным. Лишь 8% опрошенных компаний планируют ввести строгий запрет на использование персональных устройств в рабочих целях, а 26% намерены ограничить круг пользователей, имеющих возможность доступа к корпоративной сети с личного планшета или смартфона. В то же время 35% компаний планируют, наоборот, поощрять использование сотрудниками личных устройств для работы. В целом такой подход может принести пользу бизнесу, но только при условии внедрения единой политики безопасности для персональных устройств, а также эффективных решений для контроля и защиты всех мобильных устройств — как принадлежащих компании, так и личных.

Таблица. Общее число модификаций и семейств мобильных вредоносных программ

Платформа	Модификации	Семейства
Android	43600	255
J2ME	2257	64
Symbian	445	113
Windows Mobile	85	27
Others	28	10
Всего	46415	469

Возникает вопрос — что делать, как защититься от новых угроз? Сегодня рынок может предложить решение этих проблем.

Вы можете инвестировать в решения по System Management.

Вы можете приобрести шифрования для защиты данных.

И вы можете вложить средства в технологии Mobile Device Management.

Однако проблема в том, что каждое из этих решений имеет отдельную консоль управления. Это означает новые процессы оценки, выбор новых поставщиков, дополнительный бюджет. Кроме того, компаниям приходится рассматривать новые требования к подготовке новых систем, их развертыванию и т. д. Очень часто сложности возникают при управлении платформами от различных производителей. К сожалению, столько сложностей может привести к тому, что ИТ-специалисты отложат выбор средства защиты или полностью откажутся от нее.

Таким образом, основная проблема на сегодня заключается не в отсутствии доступных инструментов. А в том, что каждый отдельный инструмент усложняет процесс управления безопасностью. К сожалению, именно сложность является основным врагом ИТ-безопасности. Единственным способом решения этих проблем является изменение подхода к безопасности — необходимо уменьшать количество инструментов и консолей управления, то есть требуется инструмент, включающий одну консоль управления, которая позволит легко управлять всеми рисками.

В заключение приведу еще несколько цифр из исследования, проведенного по заказу «Лаборатории Касперского» в 2012 году.
- 50% респондентов признают, что киберугрозы — второй по значимости риск для бизнеса; более ощутимый урон может нанести лишь нестабильная экономическая ситуация (55%);
- 61% опрошенных столкнулись в 2012 году с атаками вредоносных программ, а 35% в результате потеряли данные;
- 40% опрошенных попадали в ситуации, когда уязвимости в программах могли быть использованы для причинения им ущерба, а 25% респондентов уже теряли корпоративные данные из-за незакрытых уязвимостей в программах;
- 23% компаний подтвердили, что потеря данных произошла из-за утраты мобильного устройства (смартфон или планшет);
- 15% потеряли данные из-за кражи мобильного устройства;
- в 13% случаев важная информация попала в чужие руки из-за халатности сотрудника, например в результате отправки сообщения по неверному адресу электронной почты.

Какими бы ни были причины, потеря конфиденциальных данных может нанести ущерб не только самой компании и ее сотрудникам, но и клиентам. Чаще всего встречается утрата информации, содержащей сведения о клиентах, а также финансовых данных (36% случаев). Далее с небольшим отрывом следуют сведения о сотрудниках — кража или утеря таких данных составляет 31% случаев.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor