«А В ФСБ ДРУГАЯ СИСТЕМА СЕРТИФИКАЦИИ»

СЕГОДНЯ НИ ОДИН СЕРТИФИКАТ НЕ ГАРАНТИРУЕТ СТОПРОЦЕНТНОЙ ЗАЩИТЫ ДАННЫХ, УТВЕРЖДАЕТ ДИРЕКТОР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ MICROSOFT В РОССИИ ВЛАДИМИР МАМЫКИН В БЕСЕДЕ С КОРРЕСПОНДЕНТОМ BG ЕВГЕНИЕМ ЧЕРЕШНЕВЫМ. ПАНАЦЕЕЙ НЕ БУДЕТ И ПРОДУКТ, СЕРТИФИЦИРОВАННЫЙ ОРГАНАМИ ФСБ, СТРОГО СЛЕДЯЩИМИ ЗА СОВМЕСТИМОСТЬЮ ШИФРОВАЛЬНЫХ ПРОЦЕССОВ С АЛГОРИТМАМИ ГОСТ. ДАЖЕ ГОСУДАРСТВЕННЫЕ СЕКРЕТЫ УЯЗВИМЫ ДЛЯ АТАК ЗЛОУМЫШЛЕННИКОВ, ПОКА ИМЕЕТ СИЛУ ЧЕЛОВЕЧЕСКИЙ ФАКТОР.

ВЛАДИМИР МАМЫКИН, ДИРЕКТОР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ MICROSOFT В РОССИИ

BUSINESS GUIDE: Почти во всем цивилизованном мире сертификация программного обеспечения имеет международный статус. То есть сертификат на операционную систему, полученный, например, в США, будет действителен и в Европе, и в Азии, и в Латинской Америке. Везде, но не в России. С чем это связано?

ВЛАДИМИР МАМЫКИН: Я считаю, что в России очень правильная практика. Россия в свое время научилась хорошо защищать свои секреты от внешних угроз, поэтому у нас есть чему поучиться. Любая сертифицированная версия Windows, продающаяся в России, в обязательном порядке имеет свой персональный идентификационный номер, голографическую наклейку и набор необходимой документации.

Делается это для того, чтобы версия программного обеспечения, устанавливаемая в том числе на компьютеры государственного сектора, целиком, бит к биту совпадала с оригиналом, прошедшим сертификацию. Иначе где гарантия того, что, установив в своей компании Microsoft Windows XP, вы получите именно ее?

Встает вопрос доверенной загрузки — является ли то, что вы видите на экране, действительно Windows? Быть может, злоумышленник, решив получить доступ к секретам компании, создал и продал вам оболочку, эмулирующую работу системы — установку, загрузку, работу корпоративными ресурсами, и с набором программ по перехвату секретов. И пока вы, как вам кажется, работаете, внедренные программы пересылают ему ваши секреты, пароли, базы данных и так далее. Поэтому сертификация, проводимая ФСТЭК (бывшей Гостехкомиссией),— процедура хоть и сложная, но оправданная.

BG: Такая сертификация дает стопроцентную гарантию защиты от «закладок» и других прочих причин утечек секретов?

B. M.: Нет, конечно, не дает. Важно, в каком окружении находятся ваши системы. Известен надежный способ защиты данных, который сохраняет ваши секреты даже с самыми «дырявыми» программами. Его, кстати, иногда используют.

Для этого достаточно выкопать глубоко под землей бункер со стальными стенами толщиной не менее десяти сантиметров, запереть в нем компьютер с «дырявыми» программами, поставить на входе настоящего вооруженного часового, который будет пускать для работы на компьютере только вас, не давая вам ничего внести и ничего вынести (для этого просто переодевая вас целиком!). И при этом, конечно, никаких сетей и интернета.

Метод дает почти стопроцентную гарантию сохранности секретов. Работать только неудобно. И наоборот, если вы поедете в метро с самым суперзащищенным компьютером, в котором стоят сертифицированные по высшему классу программы, и будете там работать со своими секретами, они тут же станут доступны окружающим пассажирам: они их просто увидят. Поэтому, к сожалению, в современном мире всегда приходится искать некий баланс между защищенностью и комфортом.

BG: Но так или иначе, роль системы весьма значительна. А Microsoft, например, до сих пор очень обвиняют в том, что Windows полна уязвимостей, особенно в сравнении с Linux и Apple MacOS X…

B. M.: Количество найденных уязвимостей системы зависит не только от ошибок разработчиков, но и от степени интереса взломщиков. На сегодняшний день под Windows работает подавляющее количество компьютеров на планете. Разумеется, для получения максимальной выгоды взломщикам намного интереснее ломать Windows, чем Linux.

Но в настоящий момент, согласно независимым экспертам, Linux и MacOS значительно опережают Windows по количеству уязвимостей. Например, по результатам отчета CERT за 2005 год, только в ядре Linux было найдено более 350 уязвимостей, в то время как во всех продуктах Microsoft их было 219 — около 4% от общего числа уязвимостей, найденных в 2005 году. А для MacOS только за три месяца 2007 года руководству Apple пришлось выпускать патчи для латания целых 62 уязвимостей.

Кроме того, как я уже говорил, безопасность складывается из нескольких факторов: ничто не убережет информацию от кражи, если на компьютере помимо операционной системы не установлен антивирус, а пользователь, не задумываясь, открывает вложенные файлы от незнакомых адресатов.

Надо соблюдать, как я люблю говорить, базовые правила «компьютерной гигиены». А в случае работы с действительно конфиденциальной информацией еще и консультироваться со специалистами, той же ФСТЭК.

Ведь на безопасность влияет все: и система, и «железо», и даже место компьютера в комнате. Многие не знают, но во времена, когда компьютеры комплектовались ЭЛТ-мониторами, при наличии специальной аппаратуры можно было считать их сигнал с расстояния в 200 метров, настолько сильно они излучали. Сейчас дисплеи стали существенно более безопасны, однако это совершенно не означает, что с помощью спецсредств наблюдения злоумышленник, находящийся в соседнем здании, не сможет в деталях изучать и даже записывать все, что происходит на дисплее компьютера, стоящего «лицом» к окну.

BG: Помимо ФСТЭК, Windows прошли сертификацию в ФСБ. Чем отличаются эти процедуры?

B. M.: Требования к сертификации в ФСБ, в отличие от требований ФСТЭК, не являются открытыми. В ФСТЭК система сертификации является точным аналогом международной сертификации по «Общим критериям». А в ФСБ другая система сертификации.

Она отвечает за те процессы системы, которые связаны с шифрованием. Ведь именно шифрование обеспечивает гарантированность защиты государственных секретов. В частности, ФСБ проверяет, что алгоритмы шифрования ГОСТ, с помощью которых и можно шифровать государственные секреты, корректно работают с Windows.

Версией Windows, получившей сертификат ФСБ, может воспользоваться любой желающий, однако она в целом предназначена для тех, кому действительно необходим сертификат ФСБ. Для его получения российскими спецслужбами был разработан дополнительный модуль к Windows — Secure Pack Rus, который выполняет контролирующие функции.

BG: А чем занимается Secure Pack Rus?

B. M.: Так как это не наша разработка, то мы не старались особо вникать ее суть. Просто без нее получить сертификат ФСБ было нельзя — что-то там в нашей системе не удовлетворяло их требованиям. А с этим модулем все требования ФСБ выполняются. Вообще говоря, во многих странах есть свои требования к системам, используемым в госструктурах. И не всегда эти требования доступны. Это есть и в Европе, и в Японии, и в США. Это нормально.

BG: Бывали ли случаи, когда в результате проверки Windows специалисты ФСТЭК или ФСБ РФ обнаруживали дефекты системы?

B. M.: Мне о таких случаях неизвестно.

BG: В операционную систему встроены определенные криптографические возможности, позволяющие владельцу компьютера довольно надежно хранить свои данные. В этой связи невольно приходит в голову вопрос о существовании мастер-ключа, с помощью которого теоретически можно открыть любой файл.

B. M.: Подобная аналогия появилась потому, что среди нас много людей путешествующих, часто останавливающихся в отелях. Что происходит, когда вы теряете ключ от своего номера? Приходит портье с мастер-ключом и спокойно открывает дверь. Однако сравнивать электронный ключ с металлическим неправильно. Для обычного замка в принципе можно изготовить универсальную отмычку. А вот сделать универсальный электронный ключ для расшифровывания нельзя в принципе.

Это я вам как профессионал говорю. Как человек, который более 20 лет занимался теорией и практикой шифрования в КГБ. На этом и держится наука криптография, которую используют для защиты своих секретов все без исключения страны мира. Помню такой случай, когда я работал до Microsoft в другой компании, которая также производила средства шифрования жестких дисков.

Приходят как-то к нам военные, показывают захваченный во время какой-то из операций с преступниками жесткий диск, зашифрованный нашей программой, просят расшифровать мастер-ключом. А мы не можем, не можем в принципе! Так как только пользователь, знающий свой ключ шифрования, может расшифровать диск.

Эта ситуация общая. Ни Microsoft, ни другая компания, использующая шифрование в продуктах, не имеют возможности им помочь. В современных условиях, когда длина ключа достигает 512 бит и больше, утерянный ключ означает безвозвратную потерю данных. Время, необходимое на расшифровку, может исчисляться миллионами лет. К этому вопросу автоматически напрашивается еще один — о так называемых недокументированных возможностях, о способности управлять информационными системами вопреки владельцу системы.

BG: Да, есть такой вопрос! Были ли просьбы вставить «закладки» в какой-то из ваших продуктов?

B. M.: Что ж, я могу на него ответить просто, с точки зрения бизнеса. Это будет понятнее и доказательнее. Для крупной транснациональной корпорации вроде нашей совершенно невыгодно встраивать такие функции в продукты. Просто невыгодно! Если договоренность о встройке таких функций с каким-то государством произойдет и о ней узнают другие страны, то такая компания потеряет все рынки сбыта, кроме страны, с которой она договорилась о таком темном деле.

А это убытки такого уровня, в том числе и финансовые, и репутационные, которые никакая транснациональная корпорация не может себе позволить. Да и любому государству намного выгоднее иметь в своих рядах масштабного налогоплательщика. А страну местопребывания сейчас так легко сменить. Кстати, не так давно в Великобритании депутат парламента возмущался, что в Windows Vista не предусмотрено подобных функций, и предлагал их встроить с тем, чтобы спецслужбы могли получать информацию с компьютеров. Мы, разумеется, отказались.

BG: Насколько Windows Vista более защищена по сравнению с той же XP? Совершенно понятно, что речь идет о разных архитектурах, но бизнес лучше понимает язык цифр.

B. M.: Хороший вопрос, но, к сожалению, я не знаю, как на него проще ответить. Появление Vista не означает, что Windows XP SP2 отныне продукт второго сорта или небезопасна. Даже с предыдущей версией операционной системы вы можете получить потрясающую защищенность, если ваши специалисты правильно ее настроят и будут вовремя скачивать необходимые апдейты.

Но у Vista совершенно другая архитектура: в ней заложено гораздо больше средств обеспечения безопасности. Вопрос в том, что все это надо уметь настраивать. Для того чтобы сделать систему максимально неприступной, требуются определенные знания и навыки. Конечно, Windows, в отличие от Linux, устанавливается в автоматическом режиме и начинает работать без дополнительных настроек. Но это не означает, что система Microsoft Windows Server проста — у опытного системного администратора она будет непробиваема, а вот у плохого администратора — весьма средненькой. Полностью защищенных систем не бывает. Поскольку это процесс и в нем всегда есть слабое звено — люди. ■

ИЗВЕСТЕН НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ ДАННЫХ: ВЫКОПАТЬ ГЛУБОКО ПОД ЗЕМЛЕЙ БУНКЕР СО СТАЛЬНЫМИ СТЕНАМИ, ЗАПЕРЕТЬ В НЕМ КОМПЬЮТЕР И ПЕРЕОДЕВАТЬСЯ (ЦЕЛИКОМ!) В СПЕЦИАЛЬНУЮ ОДЕЖДУ. И, КОНЕЧНО, НИКАКИХ СЕТЕЙ И ИНТЕРНЕТА… РАБОТАТЬ ТОЛЬКО НЕУДОБНО