ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДЖОН ВИНЭЙТОР (JOHN VENATOR), президент и глава ассоциации Computing Technology Industry

Масштабы угроз корпоративной инфраструктуре, использующей информационные технологии (ИТ), продолжают расти. Безопасность стала важным аспектом организации и промышленных сетей. В статье приводятся и обсуждаются данные опроса ассоциации CompTIA по обеспечению информационной защиты корпоративных сетей, и предлагаются методы ее повышения.

Отделы ИТ сталкиваются с большим количеством вопросов, связанных с обеспечением защиты, начиная от таких внешних угроз, как вирусы, черви, атаки хакеров и шпионское ПО, и заканчивая внутренними угрозами со стороны служащих.

Поскольку незащищенность передающей среды от вирусных атак и количество случаев воровства данных, составляющих большую ценность, выросли за последние годы, увеличилось и понимание необходимости обеспечения информационной безопасности. В результате многие организации выработали многоуровневый подход в этом направлении, позволяющий не только предотвратить, но и реагировать на эти атаки. Однако появившаяся было надежда на программные решения по обеспечению безопасности, с помощью которых удалось автоматизировать многие техпроцессы для отражения атак, так и не переросла в абсолютную уверенность в том, что корпоративные сети получат полную защиту.

В настоящее время возникла большая потребность в организации специального тренинга для ИТ-персонала, а также обучения мерам соблюдения информационной безопасности для всех корпоративных служащих, начиная с заводского цеха и заканчивая президентом компании.

За последние пять лет ассоциация Computing Technology Industry Association (CompTIA) провела исследование того, как происходит обучение служащих предприятия информационной безопасности. Помимо того что произошел определенный сдвиг в понимании большей необходимости изучения этого предмета, следует отметить и то, что персонал ИТ-отдела проходит обучение как по предотвращению атак, так и по минимизации их последствий.

Проведенное в 2007 г. исследование показало, что приложенные компаниями усилия оказались не напрасными. Согласно отчету, у более чем 1000 организаций количество взломов системы безопасности уменьшилось. В меньшем количестве случаев ошибки операторов стали причиной основных повреждений системы безопасности. Проведенное исследование также помогло установить новые угрозы, что указывает на необходимость организаций сохранять бдительность.

БЕЗОПАСНОСТЬ ПРОДОЛЖАЕТ ОСТАВАТЬСЯ ВЫСШИМ ПРИОРИТЕТОМ

Обеспечение мер информационной безопасности становится все более важным вопросом для многих организаций. Об этом свидетельствует наше исследование, которое показало, что руководство 78% опрошенных компаний считает этот аспект высшим приоритетом. Большинство компаний создает письменные документы о комплексной политике безопасности. Количество респондентов, у которых такая политика создана, неуклонно растет с 2004 г.: 62% организаций указывают, что используют эту политику, тогда как два года назад их количество составляло всего 47% (см. рисунок 1).

Кроме того, все больше внимания уделяется совокупности вопросов по обеспечению безопасности работы удаленных и мобильных служащих.

Среди компаний, создавших письменную политику безопасности, у 81% имеются документы по обеспечению компьютерной защиты удаленных и мобильных служащих. Следует регулярно обновлять политику безопасности, чтобы поддерживать ее действенность и возможность решать широкий круг задач, возникающих в процессе деятельности организаций. Решение текущих задач усложняется тем, что диапазон проблем, связанных с обеспечением защитных мер, постоянно изменяется.

Более половины всех респондентов ответило, что шпионящие программы являются одной из самых сложных проблем, с которыми сталкивается современная компания, чего практически не было несколько лет назад.

Более половины всех организаций также ответило, что угрозы безопасности, связанные с использованием портативных устройств, передачи голоса по IP-сетям, беспроводных сетей, а также доступа для удаленных и мобильных пользователей, значительно увеличились за предыдущие 12 мес. С появлением спутникового интернета и мобильного доступа каждое удаленное подключение или точка доступа повышают потенциальную уязвимость сети.

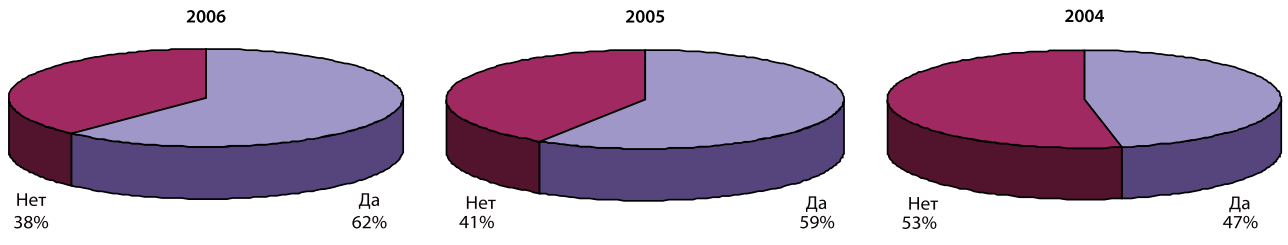
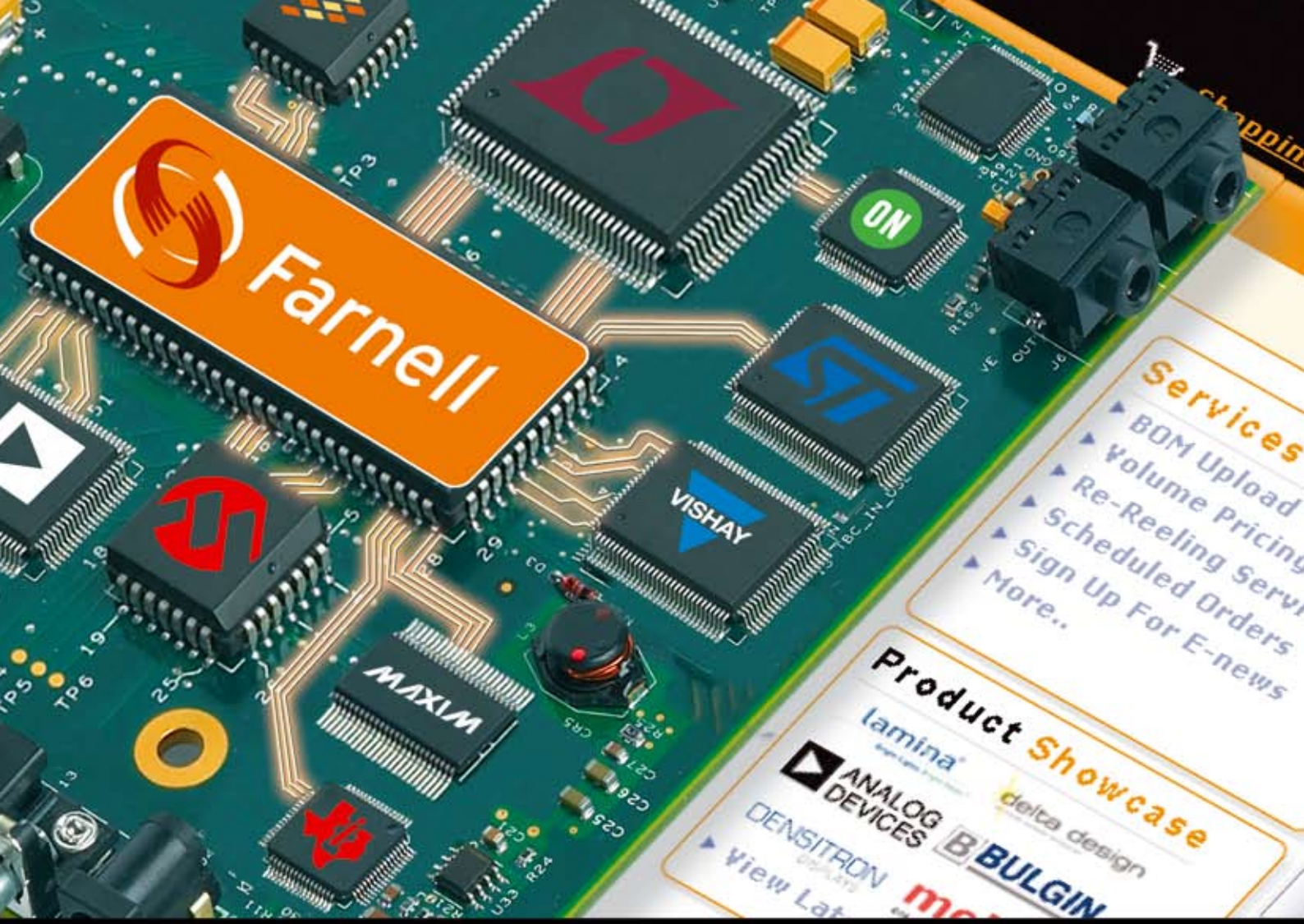


Рис. 1. **Рост числа компаний, имеющих письменные документы о политике безопасности**



Первоклассный Сервис по Доступным Ценам

- Снижены цены более чем на 36 000 позиций
- Широчайший ассортимент в индустрии компонентов от 800 ведущих производителей
- Впервые доступ к последним технологиям
- Быстрая и надежная доставка, отгрузка в тот же день
- Информационная и техническая поддержка, в которой вы нуждаетесь

Создавайте с лучшими!

Только что издан!
Новый 2008 Каталог

www.farnell.com
Russia-sales@farnell.com
Tel UK: +44 113 387 5369

Farnell

Официальные дистрибьюторы **Farnell**

Совтест Комп.
Москва
т/ф +495 444 3115, 444 3134
E-mail: comp@sovtest.ru
Web: www.farnell.ru

Элим
Санкт-Петербург
т/ф +812 320 8825, 767 0733
E-mail: office@elim.ru
Web: www.elim.ru

Argussoft
Москва
т/ф +495 221 0130, 221-01-37
E-mail: cmp@argussoft.ru
Web: www.argussoft.ru

Саранская Электронная Компания
Саранск
т/ф +8342 48 0119, 48 2870
E-mail: info@farnell-volga.ru
Web: www.farnell-volga.ru

A Premier Farnell Company

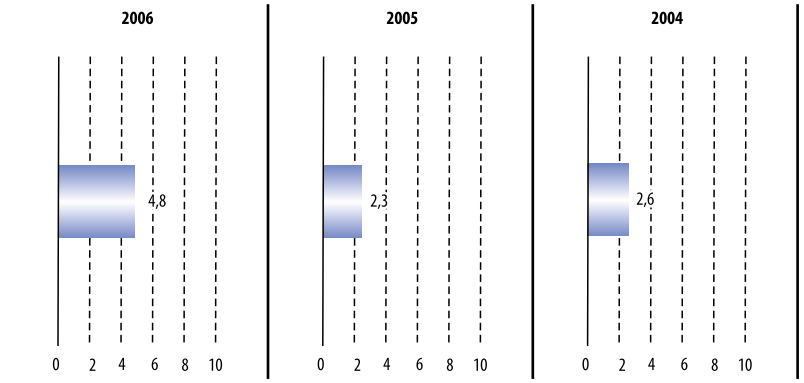


Рис. 2. **Степень серьезности взломов системы безопасности увеличивается**

РОСТ РАСХОДОВ НА ИНФОРМАЦИОННУЮ ЗАЩИТУ

Помимо потребности в организационных изменениях, связанных с созданием письменных политик безопасности, значительно повышается необходимость в финансовых отчислениях предприятия.

В 2006 г. 20% средств ИТ-бюджета организаций было потрачено на обеспечение мер информационной защиты, что на 5% выше того же показателя в 2005 г. и на 8% — в 2004.

Ожидается дальнейшее увеличение этих расходов в 2007 г. Около половины респондентов исследования CompTIA намеревается увеличить расходы на внедрение технологий безопасности. Одна треть опрошенных ожидает увеличения расходов на обучение мерам информационной защиты. Среди тех, кто предполагает увеличить расходы, средний показатель этого роста составляет 19—23%.

Исследование CompTIA также показало, что на каждый доллар, потраченный на обеспечение мер информационной защиты, около 42 центов приходится на приобретение технологии, 17 — на поддержание системы безопасности, 15 — на обучение, 12 — на оценку безопасности, 9 — на сертификацию и оставшиеся деньги — на другие меры.

Сети предприятий постоянно усложняются — растет использование почтовых служб, интернета, средств оперативной пересылки сообщений, веб-почты, а также беспроводного доступа вкупе с быстрым распространением мобильных устройств, например переносных ПК и КПК, позволяющих работникам получать незащищенные данные вне офиса.

Более 90% опрошенных заявляют, что применяют антивирусное ПО, брандмауэры и прокси-серверы, причем многие приложения используются не только служащими ИТ-отдела. За последний год существенно возросло использование также нескольких других технологий, например системы предотвращения вторжений (49%), управления физическим доступом (38%) и многофакторной проверки подлинности (32%).

Более двух третей организаций, расходующих по меньшей мере часть своего ИТ-бюджета на обучение персонала мерам обеспечения секретности или сертификацию, значительно выросло за последний год на 13% и составило 68%.

Можно предположить, что рост инвестиций оправдан. Только одна треть всех организаций, участвующих в опросе, сообщила о взломе системы информационной защиты в 2006 г. Эта цифра существенно ниже того же показателя в предыдущие годы — 61,8% в 2005 г. и 42% в 2004 г.

Возможно, эти цифры являются серьезным доказательством того, что количество угроз начинает стабилизироваться. Однако несмотря на эту положительную тенденцию, вырос риск оказаться неподготовленным к атаке.

Хотя и уменьшилось количество взломов систем безопасности, степень серьезности ошибки в результате взлома значительно выше по сравнению с двумя предыдущими годами. Респонденты оценили этот уровень цифрой 4,8 по десятибалльной шкале, где степень серьезности растет от 0 к 10. Этот показатель за последние два года был соответственно 2,3 и 2,6 (см. рисунок 2). Таким образом, можно утверждать, что негативные последствия от каждого последующего взлома выросли. Эта общая тенденция для ряда организаций, независимо от их размера.

Снижение производительности труда в результате взлома системы безопасности значительно выше в сравнении с другими издержками. Участвующие в опросе компании оценили это влияние на издержки следующим образом:

– производительность труда — 35%;
– простой сервера или сети — 21%;
– деятельность, приносящая доход — 20%;
– физические активы — 17%;
– судебные издержки или штрафы — 8%.

Опрошенные оценили среднюю стоимость всех взломов системы безопасности в 369388 долл. на одну организацию. 3% компаний заявили о том, что самый серьезный взлом обошелся им в более чем 1 млн долл.

Благодаря возросшей надежности технологии, обеспечивающей политику безопасности, и большему вниманию, уделяемому обучению персонала мерам информационной защиты, снизилось количество взломов, причиной которых был только человеческий фактор.

Если 59% респондентов заявили о том, что причиной самого серьезного взлома в 2005 г. был исключительно человеческий фактор, то в 2006 г. эта цифра уже опустилась до 42%. Этот факт заслуживает внимания, учитывая то, что в настоящее время общее количество взломов стало меньше, чем за последние 12 мес. Общий объем взломов системы безопасности, вызванный человеческим фактором, уменьшается с высокой скоростью.

Из числа взломов, причиной которых стал человеческий фактор, более половины обусловлены несоблюдением персоналом соответствующих защитных мер. Это обстоятельство указывает на то, что организациям необходимо обзавестись средствами по обеспечению информационной безопасности и высококвалифицированным ИТ-персоналом, прошедшим соответствующую подготовку. В то время как большинство компаний увеличивает инвестиции в технологии и политику безопасности, многие организации подвергают себя большому финансовому риску, причиной которого остается человеческий фактор.

При таком большом риске не удивительно, что все большее число фирм внедряет комплексные программы по обучению вопросам безопасности и делает его обязательным. Выгоды от такого обучения вполне очевидны. Среди компаний, организовавших тренинг для ИТ-персонала, 81% считает, что это позволило повысить уровень информационной защиты.

Почти три четверти этих компаний заявили о том, что возросшее понимание вопросов обеспечения безопасности и способность персонала активно определять потенциальные угрозы являются основными преимуществами, достигаемыми за счет обучения. Более половины опрошенных также указало, что тренинги позволяют повысить информационную защиту благодаря способности персонала быстро решать задачи и принимать более совершенные меры.

Тем не менее для многих организаций проведение специальных тре-

2J
antenna conceptor

ГЛОНАСС/GPS:
ПРИЕМНИК МНП-М3 + АНТЕННА 2JGLO05

Преимущества приемника МНП-М3
- 16 каналов приема
- каждый из которых работает как по ГЛОНАСС так и по GPS
- миниатюрные размеры 31x40x4мм
- низкое энергопотребление 0,9Вт
- широкий температурный диапазон –40…+70град. С
- невысокая цена

Технические характеристики 2JGLO05:
- диапазон частот: 1572МГц…1610МГц
- усиление: 35dB
- кабель: RG-174 длиной 3 метра (под заказ - любая длина)
- разъём: SMA-male (под заказ - любой)
- рабочие температуры: –40…+85 град. С
- ГЛОНАСС/GPS/GSM исполнение 2JGLO05G
- варианты исполнения с креплением на магнит,на скотч, в отверстие

Макро Групп - официальный дистрибьютор в России

МАКРО ГРУПП
Внедряя Качество

Санкт-Петербург
Тел.: (812) 370 60 70
www.macrogroup.ru

Москва
Тел.: (495) 975 79 18

Ростов-на-Дону
Тел.: (863) 227 03 93

Чебоксары
Тел.: (835) 237 10 76

нингов для ИТ-персонала по-прежнему остается больше исключением, чем правилом. Менее половины всех опрошенных компаний считает ИТ-тренинг обязательным, тогда как только около одной трети сочло необходимым обучение новых сотрудников и служащих ИТ-отдела. В целом, в настоящее время тренинг по мерам обеспечения информационной защиты считается обязательным в той или иной степени у 47% компаний.

Можно считать, что компании, не имеющие официального плана организации ИТ-обучения, подвергают себя значительному финансовому риску. Большинство предприятий согласилось с тем, что обучающие программы не только полезны, но и позволяют избежать крупных финансовых расходов.

Учитывая тот факт, что респонденты тратят в среднем около 90 тыс. долл. в год на обучение мерам информационной защиты, весьма актуальным становится вопрос о прибыли на инвестированный капитал. Согласно исследованию, проведенному для оценки экономической целесообразности проведения ИТ-тренингов, снижение годовых расходов в среднем составляет 352 тыс. долл. на одну организацию.

ОБУЧЕНИЕ УДАЛЕННЫХ И МОБИЛЬНЫХ СЛУЖАЩИХ

Надомная работа на ПК становится все более популярной в государственном и частном секторах. В настоящее время около четырех из пяти организаций (79%) обеспечивают доступ к данным для удаленных и мобильных служащих.

Как уже отмечалось, не удивительно, что за последние 12 мес. существенно выросла необходимость соблюдения мер информационной безопасности удаленными и мобильными служащими. Тем не менее вызывает недоумение факт, что менее трети компаний организовало проведение тренингов для этой категории служащих. В той же мере поражает то обстоятельство, что только 10% фирм планируют организовать тренинг в последующие 12 мес. Большинство компаний либо вовсе не рассматривало данный вопрос, либо не собирается в ближайшее время отправить этих служащих на учебу.

Основной причиной такого поведения является недостаток поддержки со стороны высшего руководства. Таким образом, в настоящее время подобные компании должны понять преимущества организации обучения для удаленных и мобильных служащих как важного компонента эффективной защиты информационных ресурсов корпорации.

Подавляющее большинство — 88% компаний из тех, кто предоставляет обучение для удаленных и мобильных служащих, считают, что количество взломов уменьшилось благодаря возросшей квалификации прошедших обучение работников этой категории. Вполне разумно ожидать, что фирмы, не планирующие подобные тренинги, рискуют в большей степени пасть жертвой атак на систему безопасности.

Таким образом, можно сделать вывод, что возросшие расходы на обеспечение мер информационной защиты и обучение персонала позволяют многим компаниям уменьшить количество взломов. Настораживает внимание то обстоятельство, что вырос уровень серьезности ошибок. Ясно, что по-прежнему остается большой риск повреждения защиты сети.

Поскольку рынок информационных технологий развивается и растут виды угроз, организации должны не только применять современные методы защиты, но и уделять должное внимание обучению персонала. При этом очевидна не только польза от тренингов по мерам обеспечения информационной защиты всех сотрудников предприятия, но и экономия расходов.