

Аудит информационной безопасности



■ **Максим Нечаев,**
руководитель отдела технической
и криптографической защиты
информации
ООО «Арт-мастер»

Аудит – необходимый элемент безопасности

Если мы хотим предотвратить какое-то нежелательное для нас действие, то должны понимать, как это действие происходит. Чтобы бороться с утечкой конфиденциальных данных, необходимо, прежде всего, идентифицировать каналы утечки информации. Но если специалистам по информационной безопасности нужно для этого время, то внутренние нарушители уже знают, как можно украсть необходимый им документ. Поэтому наиболее важный вопрос информационной безопасности — «Как именно информация утекает?». Ответ на него сможет дать аудит информационной безопасности.

Аудит информационной безопасности — это системный процесс получения объективных качественных и количественных оценок текущего состояния корпоративной информационной системы в соответствии с критериями информационной безопасности. Важно понимать, что это не единовременное мероприятие, а регулярный процесс, который должен проводиться с заданной периодичностью. Многие руководители организаций заблуж-

В настоящее время, когда все без исключения организации используют информационные системы для передачи, хранения и обработки информации, очень велика вероятность утечки конфиденциальных данных. Говоря другими словами, кража важной информации, халатность сотрудников, саботаж, атаки хакеров могут нанести существенный удар как по финансам, так и по имиджу любой компании. Предотвратить риски поможет грамотно проведенный аудит информационной безопасности.

даются, думая, что, проведя один раз аудит информационной безопасности, выявив каналы утечки информации и приняв соответствующие меры по нейтрализации этих каналов, они полностью обеспечат защиту корпоративной информационной системы. Это не так, ведь современные технологии не стоят на месте, а развиваются очень быстро, следовательно, технологии хакерских атак и способы кражи конфиденциальных данных также совершенствуются. Учитывая это, проводить аудит информационной безопасности необходимо регулярно.

Руководителю организации важно знать, что аудит информационной безопасности поможет его организации избежать материального ущерба, связанного с кражей конфиденциальной информации, а также нематериальных потерь, таких как репутация организации, потеря деловых партнеров и клиентов. Другими словами, грамотно проведенный аудит информационной безопасности поможет снизить риски организации и увеличить уверенность в собственной системе безопасности. Руководителю отдела информационных технологий необходимо знать, что аудит информационной безопасности даст ему перечень каналов утечки информации в организации, рекомендации по нейтрализации этих каналов, перечень угроз и оценку рисков по каждой угрозе, а также поможет сформировать необходимый

комплекс защитных мероприятий и разработать план их реализации.

Каналы утечки информации

По результатам исследования, проведенного аналитическим центром компании InfoWatch, наибольшее количество утечек (50 %) произошло через ноутбуки, КПК, USB-флэшки, CD- и DVD-диски и другие устройства. В результате потери, кражи или выноса носителя конфиденциальной информация оказывается у неизвестных людей, которые распоряжаются ею по своему усмотрению.

Следующий канал утечки информации — Интернет (12 %). В данном случае достаточно легко поймать внутреннего нарушителя и доказать его вину, если использовать сетевую фильтрацию.

Еще 5 % случаев нарушения информационной безопасности произошло из-за неправильной утилизации или потери резервных носителей. По 3 % пришлось на электронные послания и факсы, а также почту. 17 % случаев нарушения внутренней информационной безопасности произошли по другим каналам. В 10 % случаев так и не удалось выяснить, каким образом была произведена кража конфиденциальных данных.

Основная причина нарушения внутренней информационной безопасности — невыполнение или выполнение не надлежащим образом требований должностных инс-

трукций, политик безопасности (если они разработаны), распоряжений либо пренебрежительное отношение к простым средствам защиты информации. Все вышесказанное еще раз подтверждает, что внутренние нарушители могут быть в любом коллективе.

Компетенция определяет профессионализм

Компания «Арт-мастер» работает на ИТ-рынке Украины уже более 8 лет. В 2005 году компания получила сертификат соответствия системы менеджмента качества требованиям международного стандарта ISO 9001:2000, а в 2006 году впервые в Украине система менеджмента информационной безопасности компании была сертифицирована на соответствие требованиям международного стандарта ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Сегодня «Арт-мастер» остается единственной компанией в Украине, которая сертифицирована на соответствие требованиям стандарта ISO/IEC 27001:2005. Представительства компании «Арт-мастер» открыты во всех регионах Украины, что дает возможность качественно и в короткие сроки предоставлять услуги аудита информационной безопасности на всей территории Украины.

Компания имеет лицензии ДСТСЗИ СБУ (с 2007 года — Государственная служба специальной связи и защиты информации Украины) на проведение деятельности в сфере технической и криптографической защиты информации.

Одним из основных направлений деятельности компании является обеспечение информационной безопасности, в рамках этого направления предоставляются услуги аудита информационной безопасности.

«Арт-мастер»: особенности аудита

Компания «Арт-мастер» предоставляет услуги по проведению аудитов информационной безопасности следующих видов:

- экспертный аудит информационной безопасности;

- аудит информационной безопасности на соответствие международному стандарту ISO/IEC 27001:2005.

Результатом экспертного аудита является общая оценка защищенности корпоративной информационной системы организации, которая основана на анализе рисков и перечне обнаруженных уязвимостей. По итогам аудита формируется отчет и разрабатываются рекомендации для нейтрализации выявленных уязвимостей.

В результате аудита на соответствие международному стандарту ISO/IEC 27001:2005 руководитель организации получает описание области действия системы менеджмента информационной безопасности, реестр важных активов, методику оценки рисков, отчет по оценке

рисков, критерии принятия рисков, а также список политик, руководств, процедур и инструкций, необходимых для функционирования системы менеджмента информационной безопасности.

Вывод

Подводя итоги, отметим, что аудит информационной безопасности просто необходим современным, быстрорастущим организациям, так как только он сможет обеспечить своевременное идентифицирование каналов утечки информации, как следствие, своевременное реагирование и принятие решений по обеспечению безопасности корпоративной информационной системы. Вовремя проведенный аудит информационной безопасности поможет избежать ущерба.

Мобильные устройства под защитой Trend Micro Mobile Security 5.0

Вирус уже давно перестал быть угрозой, которой подвержены исключительно персональные компьютеры.

Вирусными аналитиками компании Trend Micro не так давно был выявлен и проанализирован вредоносный код WINCE_INFOJACK.A, нацеленный на Windows Mobile Pocket PC. Кроме того, WINCE_INFOJACK.A изменяет настройки параметров безопасности, которые воздействуют на телефон. Зараженный пользователь может инфицировать другое мобильное устройство через SIM-карту или переданное SMS-сообщение.

В январе текущего года специалистами Trend Micro было обнаружено новое вредоносное ПО SYMBOS_BESELO.A. Вирус заражает телефоны, маскируясь под мультимедийный файл, работающий под Symbian/S60 2nd edition.

Продукт Trend Micro Mobile Security (TMMS) 5.0 обеспечивает комплексную защиту мобильных устройств, поддерживает шифрование данных, идентификацию пользователей, а также снижает вероят-

ность мобильных угроз, таких как бреша в системах защиты и утечки данных, в то же время позволяя администраторам предприятия использовать единую консоль для управления безопасностью корпоративных мобильных устройств.

TMMS 5.0 поддерживает функции шифрования информации и проверки подлинности. В случае потери или кражи мобильного устройства все хранящиеся на нем корпоративные данные остаются зашифрованными до тех пор, пока не будет введен пароль. Кроме того, администратор может удалить все хранящиеся на устройствах данные, не соответствующие корпоративной политике.

Модуль для борьбы с вредоносным ПО способен блокировать вирусы, «черви», троянские приложения, а также SMS-спам. Встроенные брандмауэр и модуль обнаружения вторжений IDS (Intrusion Detection System) обеспечивают защиту от всех

потенциальных угроз для мобильных устройств.

TMMS 5.0 использует консоль OfficeScan Client/Server Edition (OSCE) 8.0, которая также применяется для управления безопасностью клиентских компьютеров и серверов в сетях средних и крупных предприятий. После установки TMMS 5.0 существующие клиенты могут использовать единую консоль для управления безопасностью мобильных устройств, настольных ПК и корпоративных серверов.

Trend Micro Mobile Security 5.0 поддерживает несколько ведущих платформ, в частности, Windows Mobile 5.0 (версии Smartphone и Pocket PC), Windows Mobile 6.0 (версии Standard, Classic и Professional), а также Symbian S60 3rd Edition (Nokia E-Series). Решение представлено в двух версиях. В состав Trend Micro Mobile Security 5.0 Standard входят антивирус, брандмауэр, IDS и средства централизованного обновления. Trend Micro Mobile Security 5.0 Edition, помимо этого, поддерживает шифрование данных и проверку подлинности.

Компания «Арт-мастер»

предлагает следующие услуги в сфере защиты информации:

- ▶ построение комплексных систем защиты информации;
- ▶ проведение государственных экспертиз в сфере технической защиты информации;
- ▶ построение систем менеджмента информационной безопасности в соответствии с требованиями стандарта ISO 27001:2005;
- ▶ проведение аудитов информационной безопасности;
- ▶ предоставление услуг электронной цифровой подписи.



Центральный офис ООО «Арт-мастер»

ул. Сурикова, 3 (лит. А), Киев,
03035, Украина
тел. +380 44 248-97-91, 248-98-27
факс. +380 44 248-98-14
e-mail: post@am-soft.ua
http://www.am-soft.ua