

Особенности борьбы с киберпреступностью

В последнее время Всемирная глобальная сеть, которая объединила миллионы компьютеров, расположенных в разных странах на разных континентах, открыла практически неограниченные возможности для получения и обмена информацией, все чаще используется в преступных целях. Но ущерб, наносимый киберпреступностью, недооценен в современном обществе из-за отсутствия информации о количестве киберпреступлений и понесенных материальных потерях. Отличительными особенностями киберпреступлений, которые значительно затрудняют их расследование, являются отсутствие государственных границ (киберпреступнику ничего не мешает совершить атаку на объект, находясь в другой стране) и значительная удаленность от объекта преступления.

Распространение компьютерных вирусов, пиратского программного обеспечения, аудио- и видеопродукции, мошенничество с пластиковыми платежными карточками, хищение денежных средств с банковских счетов, компьютерный терроризм — это далеко не полный перечень киберпреступлений. Кроме того, появилась тенденция к использованию Интернет-аудитории для формирования общественного мнения или давления как на частных, так и должностных лиц с помощью технологий «черного PR», заимствованных у СМИ. Прослеживается стабильное увеличение числа киберпреступлений. Более того, наблюдается опасная тенденция к объединению киберпреступности с транснациональной и организованной преступностью. По данным исследований, убытки от киберпреступности в мире уже превысили отметку \$100 млрд. и с каждым годом только растут. Так, в 2007 году американские компании потеряли из-за компьютерных атак

вдвое больше, чем в 2006 г., и это только прямые потери, без учета потери репутации и других факторов.

Первым шагом в эффективной борьбе с киберпреступностью стало издание 23 ноября 2001 г. Советом Европы Конвенции по борьбе с киберпреступностью, которая определила, какие действия можно считать преступными. Этот шаг был просто необходим, поскольку преступник мог совершать свои действия через страну, в которой они не были определены законом как преступные, и тем самым оставаться безнаказанным. Но для владельца информации более важен вопрос обеспечения ее защиты, а не наказания нарушителя. Именно для этого используют аудит информационной безопасности (АИБ), комплексные системы защиты информации (КСЗИ) и системы информационной безопасности (СИБ). АИБ необходим и для создания, и для уже существующих систем защиты информации, так как позволяет определить текущее состояние информационной безопасности, а также средства и методы его улучшения. КСЗИ и СИБ — решения, направленные на обеспечение защиты информации предприятия от разглашения, утечки и несанкционированного доступа путем проведения комплекса связанных организационных мер и внедрения технических средств защиты.

Компания «Арт-мастер» проводит АИБ, осуществляет построение СИБ и КСЗИ и отвечает всем требованиям к исполнителю таких видов работ (имеет профессиональный опыт проведения данных работ, сертификаты соответствия ISO/IEC 9001:2000, ISO/IEC 27001:2005, лицензии государственного образца на проведение работ по технической и криптографической защите информации).

Решения Symantec Altiris дополнили дистрибьюторский портфель DataLux

Решения Symantec Altiris дополнили дистрибьюторский портфель программных решений высокой доступности и информационной безопасности корпоративного уровня компании DataLux.

Altiris — высокоэффективные решения по комплексному управлению жизненным циклом ИТ-ресурсов, ориентированные на средние и крупные предприятия. Они помогают компаниям избежать излишних затрат на программно-аппаратные средства, повышают качество услуг и снижают стоимость эксплуатации и управления информационными ресурсами компании.

Решения Altiris ориентированы на три основные области: управление ИТ-ресурсами (Asset Management Suite), управление клиентскими системами и мобильными

устройствами (Altiris Client Management Suite), а также поддержку серверов (Server Management Suite).

«Пополнив дистрибьюторский портфель решениями Symantec Altiris, мы сможем предоставить системным интеграторам эффективные решения по комплексному управлению и защите ИТ-ресурсов компании, — отметил Андрей Якубчик, руководитель отдела проектной дистрибуции компании DataLux. «Продвижение решений Symantec Altiris с использованием опыта и экспертизы специалистов компании DataLux — это еще один шаг на пути к укреплению сотрудничества между нашими компаниями», — добавил Олег Никитский, менеджер по работе с партнерами Symantec в России и СНГ.

Читайте в новом номере

КОРПОРАТИВНЫЕ СИСТЕМЫ
№4 2008 ЖУРНАЛ ПЕРЕДОВЫХ ТЕХНОЛОГИЙ

Подписной индекс 91941

http://enterprise.com.ua Search

НОВОЕ В ТЕХНОЛОГИЯХ

С. Шатохин
Роловый подход Microsoft Dynamics AX 2009

П. Пиларж
Превращение данных в ценную информацию

Е. Коржов
Практические применения анализа текстовой информации

А. Ищенко
Оптимальные офисные решения от Konica Minolta

А. Гладун
Тенденции использования Web-контента корпоративными системами: Web 2.0

БЕЗОПАСНОСТЬ

О. Павленко
Комплекс управления ZENworks Configuration Management

А. Неповека
Подходы к обеспечению информационной безопасности

В. Грам
Проблемы на пути внедрения системы защиты от утечек информации

КОРПОРАТИВНЫЕ СИСТЕМЫ

ТЕХНОЛОГИИ	УПРАВЛЕНИЕ
Где претит вуальность ИТ?	7
Информационные технологии в бизнесской сфере	29
«Датасет» ERP-автоматизация предприятия машиностроения	38
Autodesk Revit — инструмент архитектуру строительного проектирования	39
Web 2.0: использование в корпоративных системах	60
Системы защиты от утечек информации	78

НАСТРОЙКА ИНФОРМАЦИОННЫХ СИСТЕМ 15, 18, 45

Тел./факс: (044) 425 9241 (42, 43, 44, 48)
E-mail: cs_chief@comizdat.com — главный редактор Борис Жданов
cs_editor@comizdat.com — научный редактор Сергей Павлов
www.enterprise.com.ua