Современная корпоративная система ИБ

Обзор современных технологий и решений обеспечения корпоративной информационной безопасности.

Сергей Савельев – директор Департамента информационной безопасности компании "ТехноСерв А/С"

Введение

Тема обеспечения информационной безопасности (ИБ) – одна из наиболее значимых при построении корпоративной IT-инфраструктуры. Цель публикации, помимо краткого анализа ставших уже классическими решений – дать представление о последних тенденциях и появившихся на рынке технологиях, позволяющих расширить корпоративную ИБ и вывести ее на новый уровень.

Тенденции, требования рынка ИБ

Несмотря на значительные инвестиции, которые вкладывают компании в свою ИБ, по данным Enterprise Strategy Group[1], менее одной компании из пяти (18%) считают, что их информация находится в безопасности. По данным исследований IDC[2], уже в этом году общемировой рынок продуктов и сервисов, связанных с безопасностью данных, достигнет $50 млрд.

Децентрализация технологий ИБ

Современная корпоративная IT-инфраструктура значительно отличается от той, которая была, например, 5–10 лет назад. Сейчас все большему числу сотрудников многих компаний необходимо подключаться к корпоративной сети из множества мест (офиса, дома, ресторана, движущегося автомобиля, поезда или самолета), используя самые разнообразные устройства (стационарный компьютер, ноутбук, мобильные устройства), и уже небольшие компании все чаще имеют несколько офисов с единой базой данных.

Большинство решений по защите, которые компании развертывают, сегодня фактически не защищают информацию. Инструменты типа систем сетевой защиты (firewalls) и антивирусного программного обеспечения защищают прокси-серверы, сети, ноутбуки. Они формируют и защищают периметры. Такие периметро-ориентированные подходы к защите игнорируют факт, что информацию необходимо защищать везде и в течение всего ее жизненного цикла. И когда данные перемещаются вне защищенных периметров (периметр не следует понимать как чисто физическую границу), возможны многочисленные нарушения. В то же время защита периметра абсолютно необходима, но этого уже недостаточно (рис. 1). Стали требоваться решения, обеспечивающие безопасность информации при полной автоматизации условий входа в сеть и защиту критических ресурсов сети для любых категорий пользователей, независимо от точки и способа подключения (политика защиты по каждому подключению должна в каждом случае определяться индивидуально, разрешая доступ только к определенным ресурсам, на основании установленного профиля доступа для конкретного пользователя, его местоположения и данных о том устройстве, с которого осуществляется доступ, наличие антивируса, файервола, обновлений и т.д.). При этом, если раньше число клиентов корпоративной сети (фактически LAN) измерялось сотнями, то в настоящее время – это могут быть тысячи и десятки тысяч (и это уже совсем не локальная сеть).

ЗАЩИТА, ОРИЕНТИРОВАННАЯ НА ПЕРИМЕТР

Цель: построение и защита периметров

Инструменты: VPNs, системы сетевой защиты (firewalls), IDS/IPS, anti-malware, защита оконечного устройства (endpoint protection)

ИНФОРМАЦИОННО-ЦЕНТРАЛИЗОВАННАЯ ЗАЩИТА

Цель: управление и защита информации

Инструменты: идентификация и управление доступом, шифрование данных, управление правами, защита от мошенничества, управление ИБ

Рис. 1. Два подхода к управлению защитой информации.

Сущность информационно-централизованной защиты относительно проста. Реально это сводится к управлению отношениями между людьми и данными. Весь процесс полного обеспечения защиты данных состоит из нескольких этапов: 1) управление доступом: установление "соединения" и проверка на идентичность прав доступа; 2) обеспечение защиты самих данных: шифрование и управление ключами. При этом сама защита должна быть встроена в IT-инфраструктуру и должна быть бесшовной и прозрачной, уровень защиты данных должен соответствовать рискам бизнеса в случае их потери, а аудит данных должен удовлетворять регулирующим актам/нормам.

Сегодняшние требования безопасности данных не только шире, но и намного глубже. Например, сервисный персонал, занимающийся транспортировкой бэкапных лент или обслуживанием серверов, в случае злоумышленного доступа к данным раньше получал и доступ к информации, теперь вся хранящаяся, например, критичная бизнес-информация независимо от местоположения и времени должна быть защищена, т.е. персонал, допущенный к работе с носителями данных, не должен иметь доступ к самой информации.

Информация должна защищаться/шифроваться не только при хранении, но и при передачах как в локальных, так и глобальных сетях. Простой опыт показывает, что петля из оптического кабеля без больших усилий позволяет "снимать" всю информацию, которая по нему передается. Такие факты в условиях отсутствия шифрования данных, например, при их репликации и/или передачах в глобальных сетях могут полностью нивелировать все усилия по защите данных в датацентрах.

Одновременно с увеличением степени защиты данных усложняется и тополо-

[1] Enterprise Strategy Group: "Protecting Confidential Data," March 2006;

[2] IDC: "Worldwide IT Security Software, Hardware, "and Services 2007–2011 Forecast: The Big Picture," Doc. #210018, December 2007

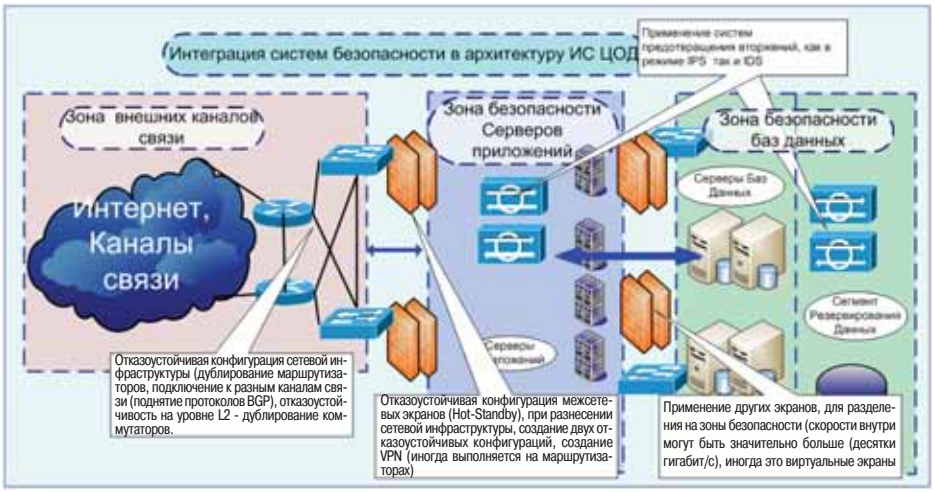

Рис. 2. Архитектура "классической" системы безопасности центров обработки данных.

гия IT-инфраструктуры. Сейчас это множество интерфейсов, протоколов, устройств и каждый со своими методами доступа и, возможно, шифрования. При этом на всех уровнях/этапах/подэтапах должна обеспечиваться полная их совместимость, прозрачность для приложений и пользователей, работоспособность и управляемость.

Обеспечение отказоустойчивости технологий ИБ

Важной компонентой при построении систем ИБ является их отказоустойчивость. Непродуманность этой части решения ведет не только к снижению доступности, но часто и к лишним затратам на оборудование и сервис.

Рассмотрим классическую схему датацентра. Типичная схема его построения – дублированная архитектура на уровне L2 (рис. 2). Это означает, что серверы включаются двумя сетевыми адаптерами в разные сетевые коммутаторы (switch), один из которых работает в резервном режиме, подключаясь в случае выхода из строя основного. Точно также дублируются и маршрутизаторы, и каналы связи (при этом возможно одновременное использование каналов связи). У каждого коммутатора устанавливается межсетевой экран для обеспечения высокой надежности – дублированный. Кроме того, применяются системы IPS/IDS, шифрование каналов связи.

При разделении датацентра на зоны безопасности (как правило, на несколько DMZ-зон, зоны баз данных и др.) на самих серверах часто используются хостовые системы предотвращения вторжений (HIPS) и другие системы безопасности, например, системы анализа уязвимостей, или системы мониторинга и корреляции.

Вроде бы все нормально, однако достаточно ли этого для современного датацентра?

Рассмотрим потоки информации в датацентре. Потоки информации могут быть разными: например, в канале связи между клиентом и датацентром и между сервером приложений и базой данных. Причем, объем потоков может различаться в несколько раз: между клиентом и сервером приложений – мегабиты, а между сервером и базой – гигабиты. Это требует наличия очень мощного межсетевого экрана. Когда мощности не хватает, приходится разбивать систему на сегменты и ставить свои экраны для обеспечения надежности. Дополнительные экраны дублируют инфраструктуру – часто до четырех крат! Системы IPS, обладающие, как правило, невысокой пропускной способностью (обычно до 1 Гбит/с), также требуют кластеризации.

Таким образом, получается, с одной стороны, большой расход оборудования, с другой – недостаточная пропускная способность устройств в сравнении с требованиями, предъявляемыми в современных датацентрах. Кроме того, информация между системами хранения должна постоянно реплицироваться по защищенным каналам связи и, как правило, это те же каналы связи, что и для связи с клиентами, что вносит дополнительные требования к каналам связи по надежности, приоретизации потоков и др. В результате обычных схем резервирования, защищенных VPN-соединениями между клиентами и датацентром и основным датацентром и резервным, уже недостаточно, когда при пропадании связи они возобновляются по резервным каналам связи.

Более того, когда основной центр выходит из строя и надо перевести всех пользователей на резервный, возникает большой объем проблем по правильной авторизации пользователей в новом датацентре (всем ли туда есть доступ и есть ли актуальная информация о пользователях в резервном датацентре?).

Что же необходимо?

1. Максимальное использование имеющегося оборудования, 50% которого простаивает в режиме ожидания, а производительности средств безопасности нередко не хватает для обеспечения полноценной защиты.

2. Полноценное резервирование всех систем и, по возможности, каналов связи.

3. Возможность резервирования системы управления и централизованное управление устройствами безопасности.

Выбор IT-архитектуры, органически имеющей повышенный уровень ИБ

Современное развитие рынка программных и аппаратных решений только за счет оптимального выбора IT-архитектуры позволяет снять многие проблемы по поддержанию ее информационной безопасности в будущем. Например, использование виртуализации клиентских приложений (VDI-инфраструктуры) не только улучшает ее сервиспригодность, но устраняет большинство уязвимостей на клиентской стороне.

Обзор рынка технологий и решений обеспечения ИБ

Все решения для построения инфраструктур обеспечения ИБ можно разбить на 2 класса: 1) решения, развиваемые уже в течение более 15 лет и ориентированные на интернет-угрозы (системы управления сетевой безопасностью, файерволы, системы защиты от угроз, сканеры, антивирусы и др.); 2) решения, активно развивающиеся только в последние 2 года и ориентированные на предотвращение внутренних угроз и "утечек" информации в глобальнораспределенных ИС в течение всего срока жизни информации, позволяющие значительно расширить ранее поддерживаемый уровень защиты информации (на основе решений первого типа).

Системы управления и мониторинга событий информационной безопасности

Сегодня данный класс решений является ключевой компонентой обеспечения ИБ датацентров. Подключение корпоративных сетей к интернету, построение распределенных сетей, появление огромного количества компьютерных вирусов способствовали активному внедрению технических средств для защиты периметра корпоративных информационных систем. Результаты последних исследований показывают, что сегодня подавляющее большинство компаний имеют такие системы: 90% компаний используют межсетевые экраны и антивирусные программы, а 40% – системы обнаружения вторжений (IDS).

В потоке информации, постоянно поступающей на экран консоли администратора безопасности, есть множество предупреждений и сообщений от установленных в сети средств защиты. Это и диагностика от систем сканирования периметра сети, и обнаруженные попытки подбора пароля на узлах, видимых из интернета, и выявленные атаки "червей", и злонамеренное использование уязвимостей web-сервера, и многое другое. Несколько сотен тысяч событий в день и больше – это, увы, реальность наших дней. А в крупных сетях ежедневная порция информации, которая "сваливается" на администратора, может превысить миллионы сообщений. Например, только один межсетевой экран может генерировать за день более 1 Гбайт данных в Log-файле, а один сенсор IDS за это же время может выдавать до 500 тыс. сообщений. Справиться с такими объемами информации не под силу ни одному человеку.

Ситуация осложняется еще и тем, что далеко не все сообщения, сгенерированные средствами защиты, соответствуют реальным атакам – у всех средств безопасности в той или иной степени случаются ложные срабатывания. Например, по статистике, число ложных срабатываний для сенсоров IDS может достигать 90%. Это

приводит к тому, что администраторы безопасности часто вынуждены рассматривать только события высшего приоритета, оставляя практически все события, кроме наиболее критичных, незамеченными, и, таким образом, пропускать реальные атаки на информационную систему.

Наличие большого количества разных средств безопасности порождает большое количество журналов от разных систем, каждая из которых выдает события на своем языке и, кроме того, выдает много ненужной информации, а также иногда срабатывает на события не совсем адекватно.

В связи с этим, одной из актуальных задач представляется построение единой, централизованной системы мониторинга событий информационной безопасности (Security Information Management), которые позволяют связать все используемые в сети защитные средства в единый управляемый комплекс.

На сегодняшний момент рынок систем SIEM переваливает за несколько сотен миллионов долларов. На рынке присутствует несколько десятков компаний, наиболее известны следующие компании (средства): Arcsight (*Enterprise Security Manager)*; RSA enVision (*ранее* – Network Intelligence, *куплена EMC)*; Novell *(Sentinel)*; Cisco *(MARS – Monitoring, Analysis and Response System)*; Symantec *(Security Information Manager)*; NetForensics *(nFX Open Security Platform)*; CA *(eTrust Security Command Center)*; Intellitactics *(Security Manager)*; ActiveWorx; IBM Tivoli Security Operations Manager, IBM Tivoli Compliance Insight Manager; NetIQ *(Security Manager)*; LogLogic; Sensage; Checkpoint *(Eventia)*.

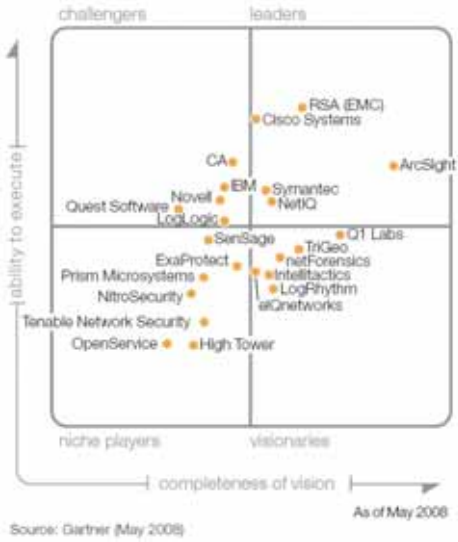

Рис. 3. Позиционирование производителей на рынке ПО управления сетевой безопасностью в соответствии с магическим квадрантом Gartner: *"Magic Quadrant for Security Information and Event Management", май, 2008 г.* .

Система ArcSight управления информационной безопасностью и рисками пока не очень известна на российском рынке, но она занимает ведущие позиции (рис. 3) в мире (по аналитическим данным, ~ 50% всех проектов по построению систем мониторинга сетевой активности в Европе, выполнены с использованием продуктов ArcSight). На сегодняшний день она обладает наиболее мощными механизмами, позволяющими централизованно управлять рисками и реагировать на различные угрозы и попытки несанкционированного проникновения в информационную систему предприятия.

Архитектура решения позволяет создавать распределенные структуры и регулировать отношения между подсистемами как на уровне каналов связи, так и по составу модулей и поддерживаемых систем.

Кроме того, в ней – наиболее простой в управлении и реализующий максимальное количество полезных функций интерфейс. Консоль администратора реализована не только в виде web-приложения, но и в виде отдельного приложения.

Технология функционирования ArcSight ESM предусматривает четырехступенчатую обработку событий безопасности: агрегирование, нормализация, корреляция и визуализация.

Аппаратная платформа для функционирования ArcSight ESM реализуется на основе трехуровневой архитектуры, которая предусматривает установку сервера базы данных, сервера обработки сообщений и консоли управления. Для серверов базы данных и обработки сообщений используют оборудование компании Sun Microsystems или x86-совместимые серверы под управлением ОС Windows 2003 или ОС RedHat Linux. Консоль управления может быть запущена практически на любой ОС, для которой существует java-машина.

Основные преимущества использования ArcSight ESM:

- обзор данных в реальном режиме времени от всех систем и их централизованное хранение;
- классификация угроз по уровням опасности для выявления реальных и игнорирования ложных;
- способность агрегировать данные с огромного количества программно-аппаратных комплексов сети (серверов, межсетевых экранов и др.) различных вендоров;
- чрезвычайно мощная база предустановленных правил корреляции событий безопасности, существенно упрощающая администрирование системы;
- проверка системы безопасности на соответствие стандартам (ISO 27001 (ISO 17799), Sarbanes-Oxley и др.), а также другим нормативным и законодательным актам, включая составленные владельцем системы.

Сетевые решения поддержания ИБ

Это достаточно большой класс решений, представленных на рынке. По применению их можно разделить на: 1) средства обеспечения ИБ в локальных и глобальных сетях при передаче данных; 2) межсетевые экраны; 3) системы обнаружения и подавления атак на сеть/предотвращения вторжений; 4) аппаратно-программные/программные комплексы защиты от спама и вирусов; 5) системы анализа/аудита защищенности и др. По функциональности эти системы в зависимости от позиционирования могут в значительной степени пересекаться; ориентироваться как на внешние, так и на внутренние угрозы; реализовываться аппаратно и/или программно.

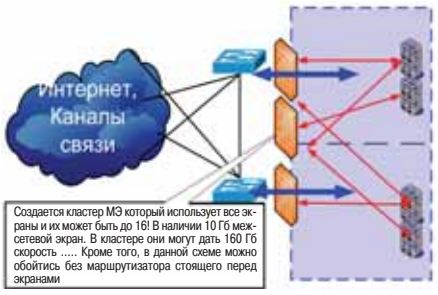

Рис. 4. Межсетевые экраны Stonegate производства компании Stonesoft образуют полноценный кластер, который виден администратору как один МЭ.

Технологии реализации схем отказоустойчивости сетевых систем безопасности ИС

Это одна из наиважнейших компонент при построении систем ИБ корпоративного класса. Данные решения строятся на базе кластеров и служат как для обеспечения доступности межсетевых экранов (МЭ), так и систем управления безопасностью. По опыту инсталляций "ТехноСерв А/С" для обеспечения доступности МЭ наиболее эффективным себя показало решение компании StoneSoft (Финляндия), в котором межсетевые экраны образуют полноценный кластер (виден администратору как один МЭ). В нем устройства работают параллельно и перераспределяют нагрузку между собой (рис. 4). В отличие от решений других производителей, допускается кластеризация различных моделей оборудования, что является существенным фактором защиты инвестиций. Пропускная способность кластера равна суммарной пропускной способности всех компонентов (экранов), входящих в кластер (рис. 5). При этом неважно, какой именно или сколько экранов выйдут из строя. Пока хотя бы один работоспособен, система будет работать.

В этом году аналогичное решение выпустила компания Juniper Networks, которое имеет подобную архитектуру и способно составить конкуренцию в части производительности. Но все же сле-

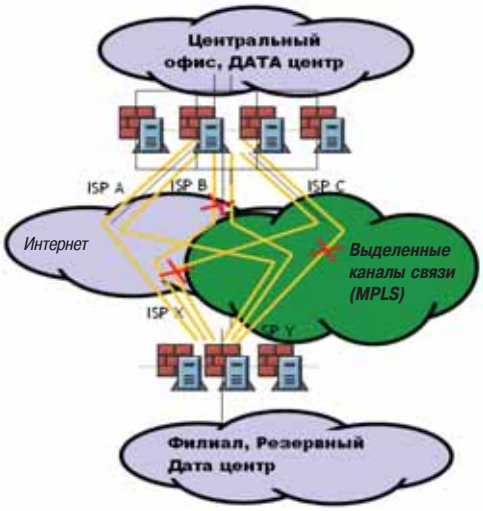

Рис. 5. К каждому кластеру Stonegate (независимо от количества экранов в кластере) можно подключить до 16 каналов связи (например, интернет), которые будут полностью сбалансированы по нагрузке.

дует отметить, что продукты StoneSoft обладают одним из главных преимуществ – наличием открытого крипто-интерфейса к своим VPN-продуктам, что позволило подключить к ним российские сертифицированные крипто-модули. "ТехноСерв А/С" и StoneSoft намерены и дальше продолжать сотрудничество в части встраивания и легализации использования крипто-модулей российского производства.

С появлением распределенных систем безопасности многие столкнулись с необходимостью оперативного управления как собственно системой, так и управления системами доступа пользователей и оперативного мониторинга событий. Решения Stonegate позволяют создать до 5 распределенных систем управления, каждая из которых обладает актуальной и полной информацией о политиках, правилах доступа и др. Вся управляющая информация регулярно обновляется на всех системах управления. При этом резервируется и система сбора журналов безопасности (лог сервера).

Системы предотвращения вторжений также кластеризуются и обеспечивают анализ всех сегментов безопасности на вредоносные воздействия, и при этом можно допустить выход из строя нескольких из них без потери контроля над безопасностью всех сегментов, поскольку вышедшие из строя системы замещаются другими. Системы межсетевого экранирования совместно с IPS становятся не только средством, позволяющим разделить информационную систему на зоны безопасности, не снижая производительности системы в целом, но и средством управления потоками безопасности.

Каналы связи подключаются непосредственно к системе межсетевого экранирования, и при этом никто не решает проблемы маршрутизации информации через нескольких провайдеров связи – кластер это решает автоматически. Причем все системы безопасности резервированы не только сами, но также их система управления и мониторинга. Пропускная способность каналов связи используется полностью как за счет оптимизации прохождения трафика, так и за счет его эффективного сжатия перед передачей по каналам связи, что сильно снижает общую стоимость владения такой системой.

Технологии шифрования и управления ключами

Это один из самых быстро развивающихся секторов ИБ-рынка решений на Западе. Данные технологии делятся на решения по шифрованию для файловых систем и для блокового доступа к данным. Основные поставщики решений: EMC, NetApp, IBM, HDS, Brocade, Cisco, а также некоторые недавно образованные компании, например, Huawei-Symantec.

Решения по управлению ключами предлагаются в виде специализированных серверов/appliance, которые обеспечивают управление устройствами шифрования данных. Реализация последних гораздо шире. Она может быть как чисто программной, так и в различной интеграции со специализированным/стандартным аппаратным обеспечением. Для корпоративных инфраструктур, в основном, используются специализированные appliance или блэйд-модули шифрования (Brocade, Cisco), устанавливаемые в SAN-директора. В отдельных случаях это специализированные порты непосредственно на дисковых системах. Для ленточных устройств (приводы/библиотеки) встроенные механизмы шифрования уже более 1,5 лет, например, поставляются IBM.

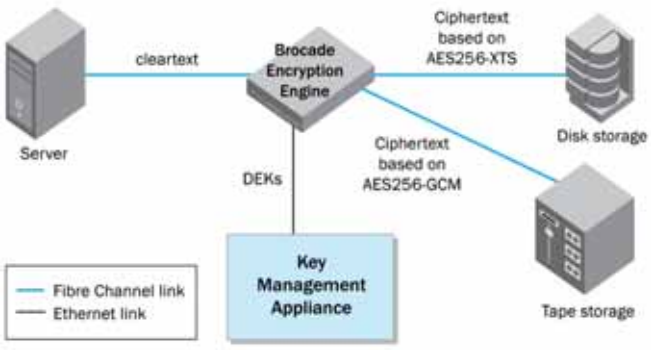

Рис. 7. Общая архитектура решения на базе Brocade encryption device для дисковых и ленточных хранилищ.

Необходимо заметить, что решения по управлению пользовательскими ключами доступа – PKI – на рынке уже лет 15–20. Решения по управлению ключами, связанными приложениями и шифрованием их данных, активно стали развиваться только в последние 2 года.

Сейчас PKI используется практически в каждой системе управления доступом (например производства Oracle, SUN, IBM, Novell, Symantec и др.), которая предоставляет комплексный набор сервисов по централизованному управлению идентификацией пользователей и их доступом к различным информационным ресурсам предприятия, в том числе web-ресурсам и приложениям. Подобные системы полностью реализуют концепцию защищенного доступа к ресурсам предприятия, известную как концепцию AAA (аутентификация, авторизация, аудит). Системы предоставляют средства, существенно сокращающие расходы на администрирование тысяч и миллионов пользователей (в том числе, корпоративного портала), а также на контроль их доступа к информационным ресурсам. Развитые средства авторизации и аудита действий, как пользователей, так и администраторов системы, позволяют существенно повысить уровень безопасности работы с информационными ресурсами.

Решение Brocade класса "data-at-rest" по шифрованию данных

На конец лета 2008 г. это самое высокопроизводительное решение по шифрованию данных в FC-системах хранения на базе специализированных Brocade SAN-коммутаторов (2U, rack-mounted Brocade Encryption Switch) и блэйд-модулей, устанавливаемых в директора класса Brocade DCX Backbone (рис. 6). Каждое из этих решений обеспечивает шифрование потока данных с общей скоростью 100 Гбит/с и со скоростью 50 Гбит/с сжатых данных.

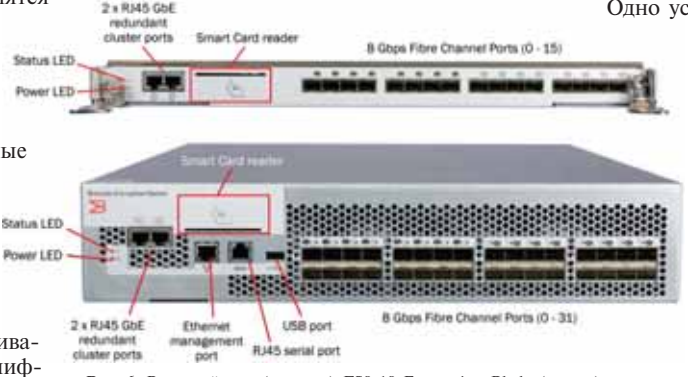

Рис. 6. Внешний вид (спереди) FS8-18 Encryption Blade (вверху) и Brocade Encryption Switch (внизу).

Каждая из конфигураций имеет также два gigabit Ethernet (GbE) порта, которые используются для синхронизации множества устройств шифрования. USB порт облегчает обновление ПО, а RS-232 используются для системных целей. Последний интерфейс – порт управления Ethernet для связи с приложениями управления и хранилищами ключей.

Решение по шифрованию Brocade в настоящий момент поддерживает два решения по управлению ключами: NetApp Lifetime Key Manager (LKM) и RSA Key Manager (RKM).

В решениях Brocade используется 256-битный ключ шифрования данных (data encryption key – DEK), что позволяет использовать $1{,}2 \times 10^{77}$ различных ключей. В случае "утечки" данных и случайном выборе ключа, то при современной производительности суперкомпьютеров на это могло бы уйти около 3×10^{51} лет.

Для расшифрования информации используется тот же самый ключ, что и для шифрования данных. Такая технология называется "симметричное ключевое кодирование" ("symmetric key encryption").

Для шифрования данных на ленту и диски используются соответственно два разных механизма – AES256-GCM (Advanced Encryption Standard 256 Galois Counter Mode) и AES256-XTS (рис. 7). AES256-GCM использует один 256-bit DEK и один или более DEKs, которые связаны с каждым ленточным картриджем, томом или ленточным пулом.

Одно устройство шифрования Brocade может масштабироваться по пропускной способности с показателями 34, 68 и 102 Гбит/с. Максимально в одном директоре Brocade DCX или фабрике может быть размещено до 4 устройств шифрования с общей производительностью 384 Гбит/с.

Шифрование данных на лентах и дисковых библиотеках

В апреле с.г. Cisco и RSA объявили о продолжении сотрудничества в этой области и с июня с.г. доступно решение, позволяю-

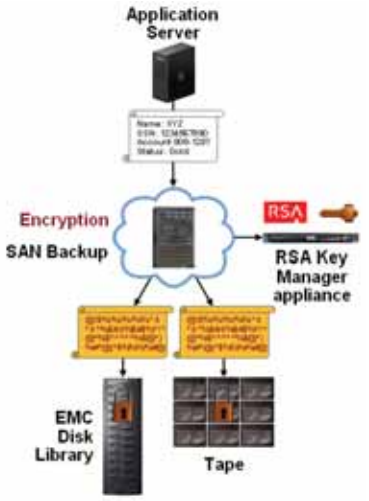

Рис. 8. Шифрование данных на лентах и дисковых библиотеках с помощью Cisco MDS 9000 Storage Media Encryption и RSA Key Manager.

щее шифровать данные, хранимые на магнитных лентах (в том числе виртуальных) с помощью интегрированных систем Cisco MDS 9000 Storage Media Encryption (SME) и RSA Key Manager for the Datacenter (рис. 8). SME представляет собой блэйд-модуль, вставляемый в директора серий Cisco MDS 9500/9200.

Данное решение гораздо менее производительное, чем предыдущее, и позиционируется для компаний, которым необходимо защищать данные на лентах в соответствии с регулирующими требованиями, а также резервные копии от внутренних атак или/и возможных утечек данных при транспортировке лент.

Поддерживается ПО бэкапирования EMC Disk Library, EMC NetWorker и Symantec Veritas NetBackup.

Каждый SME-модуль поддерживает производительность около 4 Гбит/с с возможностью подключения до 8 ленточных накопителей на модуль. Четыре SME-модуля могут быть конфигурированы в кластер.

Также Cisco и RSA будут вместе расширять функции безопасности Cisco TrustSec для шифрования передаваемых данных с помощью платформы Cisco Nexus 7000. Чтобы защитить данные в системе электронной почты, RSA намерена добиться совместимости с технологией Cisco Registered Envelope Service, что позволит шифровать конфиденциальные сообщения электронной почты, обнаруженные в сети RSA DLP Network.

Технология предотвращения потери данных (Data Loss Prevention, DLP)

Данная технология на рынке уже около 3 лет. Но только в последний год она появилась в портфеле решений основных IT-вендоров: IBM, Cisco, EMC, Symantec, в решениях Infowatch и др.

В основном, эти решения ориентированы на предотвращение "утечки" информации вне защищаемых периметров. Суть их в том, что все новые/модифицируемые документы/записи в базах данных постоянно сканируются на предмет наличия в них определенных слов/словосочетаний, задаваемых признаков и др. Помимо этого, также фиксируются все обращения к защищенным источникам информации из этих документов. В случае, если эти условия выполняются (или/и происходят события), то документы/записи помечаются как "чувствительные" и им присваивается определенный класс. В случае необходимости такие документы/записи могут шифроваться на основе интеграции с соответствующими решениями. После этого все манипуляции с этим документом могут осуществляться только в соответствии с заданными правилами/политиками. Например, может быть запрещена пересылка документ с письмом или записывать его на переносимый носитель, печатать, осуществлять скриншоты и др. Количество правил, уровень их сложности могут быть любыми. Многие DLP-системы позволяют работать с кириллицей.

В июне с.г. корпорация Symantec объявила о выпуске новой версии Vontu Data Loss Prevention с усовершенствованными средствами управления и встроенной поддержкой сканирования баз данных SQL. Решения для предотвращения потери данных (DLP) помогают избежать утечки конфиденциальной информации в процессе ее хранения или использования. Комплекс Vontu Data Loss Prevention позволяет выявлять и защищать конфиденциальную информацию по всему предприятию. Это уже вторая версия продукта DLP с момента приобретения Symantec компании Vontu в декабре 2007 г.

Новая версия Vontu DLP позволяет быстрее проводить сканирование баз данных SQL с целью выявления конфиденциальной информации. Благодаря встроенной поддержке баз данных SQL, таких как Oracle, SQLServer или DB2, появилась возможность выполнять систематические общекорпоративные проверки тысяч баз данных в рамках своей стратегии предотвращения утечки информации, быстро осуществляя инвентаризацию баз данных в процессе аудита или выявляя конфиденциальные данные, которые могли использоваться с нарушением правил.

Системы DLP помогают компаниям решать проблемы, связанные с ревизиями, расследованиями, чисткой и классификацией данных. Благодаря усиленной поддержке глубокого сканирования баз данных SQL Symantec обеспечила самый широкий охват корпоративных хранилищ данных. Vontu DLP поддерживает прямое сканирование всех шести классов систем, в которых могут храниться данные: файл-серверов, распределенных по предприятию настольных ПК и ноутбуков, баз данных, систем управления записями и документами (таких как Documentum и SharePoint), хранилищ сообщений e-mail и веб-сайтов (включая интрасети).

Для оптимального масштабирования Vontu DLP применяет 3 подхода к обнаружению данных. Сканирование при помощи агентов обеспечивает преимущества при сканировании большого числа конечных информационных ресурсов, позволяя обследовать тысячи машин одновременно. Агенты сервера Vontu DLP выполняют распределенное сканирование информационных хранилищ в удаленных региональных отделениях, а централизованное сканирование применяется для обследования крупных, централизованных хранилищ с миллионами документов или записей баз данных.

Vontu Data Loss Prevention теперь поддерживает встроенное сканирование баз данных SQL, которым можно целиком управлять через Vontu Enforce Platform при помощи интегрированных функций для управления планированием, фильтрацией и скоростью сканирования баз данных SQL. В дополнение к этому в решении Vontu Endpoint DLP расширена поддержка операционных систем Windows Server 2003 и Windows Vista и появилась возможность выполнять параллельное сканирование тысяч систем, опираясь на архитектуру агентов Vontu Endpoint DLP.

В апреле с.г. Cisco и RSA объявили о сотрудничестве в этой области. Cisco намерена интегрировать технологию классификации данных из решения RSA DLP Suite с функциями Cisco DLP, работающими на уровне сети, настольных систем и серверов. В свою очередь, RSA встроит в решение RSA DLP Suite функции определения и обязательного исполнения правил безопасности Cisco. Кроме того, система RSA DLP Enterprise Manager будет управлять правилами DLP как в решениях RSA, так и в решениях Cisco. Cisco и RSA также будут сотрудничать в области оконечных сетевых систем, чтобы обеспечить интегрированную защиту хост-машин, управление правилами безопасности и надежную защиту информации, хранимой на настольных системах, мобильных компьютерах (ноутбуках) и серверных платформах. В качестве первого шага Cisco планирует расширить функции DLP в приложении Cisco Security Agent, добавив к ним технологию классификации данных RSA. Управлять новой функциональностью можно будет через центр управления Cisco (Security Agent Management Center) или RSA (DLP Enterprise Manager).

Заключение

При разработке конкретного решения только комплексное использование всех и ряда дополнительных технологий может обеспечить ИБ корпоративной ИС как в пределах датацентра, так и вне этого периметра с учетом задаваемых политик на условия доступа, использования, перемещения, степени защищенности и многими др. Критериями выбора соответствующей компоненты поддержания ИБ могут являться: стоимость, полнота требуемой функциональности, сложность/простота настройки, соотнесенная со стоимостью работ, надежность, совместимость с существующей средой, влияние на производительность системы в целом и многое другое.

Как показывает практика, апробация подобных решений и их дальнейшее эффективное внедрение и использование позволяют существенно экономить владельцам информационных систем за счет более легкой интеграции, в том числе максимально возможно использовать встроенные механизмы безопасности.

Сергей Савельев,
директор Департамента информационной безопасности компании "ТехноСерв А/С"