# САМОЗАЩИЩАЮЩАЯСЯ СЕТЬ

# Cisco развитие защиты сети

Корпорация Cisco развивает концепцию сети, способной к таким действиям, которые, устраняют ошибки в ее работе. Еще в кибернетическую эру в обиход вошло понятие «помехозащищенная сеть», т. е. сеть, позволяющая не только обнаруживать помехи в каналах связи, но и определенное их количество устранять. Со временем виды помех становились разнообразнее, например, к ним стали относить функциональные сбои, справляться с которыми удавалось с помощью технических решений. В современных информационных системах такие ошибки встречаются значительно чаще. Сейчас Cisco, чтобы удовлетворить растущий спрос на решения для корпораций, позволяющие «управлять ИТ-рисками», защищать данные от вредных воздействий и соблюдать нормативные требования к обработке информации, объявила о расширении своего сетевого решения Self-Defending Network (самозащищающаяся сеть) до более общего системного.

# Безопасность сетей

Системы предотвращения вторжений (IPS). Cisco упростила систему управления своими системами IPS, чтобы сделать их доступными для компаний любого размера. Решение Cisco IPS 6.1 дает заказчику более глубокое представление о "здоровье" его сети и включает в себя новое комплексное приложение Cisco IPS Manager Express для активации функций IPS, мониторинга и отчетности. Кроме программных усовершенствований, Cisco создала новый модуль IPS для продуктов Adaptive Security Appliance с производительностью до 650 Мбит/с и разработала услуги для защиты унифицированных коммуникаций (данные, голос и видео), более эффективного распознавания угроз в одноранговых (peer-to-peer) соединениях и повышения безопасности в среде Microsoft.

Виртуальные частные сети (VPN). Cisco включила технологию шифрованного транспорта GET VPN в систему Cisco 7200 VPN Services Adapter, что позволило увеличить ее производительность на 300 процентов. GET VPN представляет собой технологию VPN нового типа, которая шифрует данные для безопасной передачи по глобальным сетям WAN. Она избавляет от необходимости в туннелях "точка-точка" и дает возможность распространять корпоративные сети VPN на тысячи удаленных офисов с одновременной поддержкой интеллектуальных функций, имеющих критически важное значение для качества голоса и видео, качества услуг, маршрутизации и многоадресной передачи (мультикастинга). Поскольку приложения GET VPN работают, главным образом, в сетях с многопротокольной коммутацией по меткам (MPLS), они позволяют заказчикам гибко распоряжаться функциями защиты своих сетей и выполнять их самостоятельно через операторскую глобальную сеть WAN или передавать на аутсорсинг внешним провайдерам.

# Безопасность оконечных устройств

Cisco Security Agent 6.0. Cisco Security Agent - программный агент, предназначенный для защиты оконечных устройств (серверов, ноутбуков и т.д.). Он помогает распознавать угрозы и управляет доступом к конфиденциальной информации. Версия 6.0 впервые в отрасли включает защиту оконечных устройств от неизвестных атак, функции предотвращения потери данных и антивирусную защиту по сигнатурам в рамках единого хорошо управляемого приложения. Обновление вирусных сигнатур происходит автоматически и не требует дополнительной оплаты.

# Безопасность приложений

Межсетевой экран Web Application Firewall решает проблемы безопасности, вызванные технологией Web 2.0 и социальными сетями. Он защищает конфиденциальную информацию компаний и частных лиц в Web-приложениях. Web Application Firewall поставляется как отдельное устройство или встраивается в шлюз Cisco ACE XML Gateway. Он обеспечивает защиту доступа к приложениям, инспектирует Web-трафик HTML и XML, определяет типовые сигнатуры атак и помогает компаниям удовлетворять требования PCI в области Web-безопасности.

# Безопасность контента

Фильтрация контента. Cisco расширила функции безопасности популярных интегрированных сервисных маршрутизаторов Cisco ISR. Сегодня в мире установлено почти 4 миллиона устройств этого семейства. С сегодняшнего дня они включают функцию фильтрации контента от компании Trend Micro. Это поможет корпоративным заказчикам блокировать доступ к Web-сайтам, которые известны как источники вредоносных программ, ограничивать доступ к непристойному контенту и внедрять приемлемые для сотрудников правила пользования Интернетом.

# Управление безопасностью

Система Cisco Security MARS (Monitoring Analysis Response System) 6.0. Cisco Security MARS позволяет следить за функциями безопасности в реальном времени. Она распознает угрозы, агрегируя информацию, поступающую от устройств Cisco и других компаний, и определяет наиболее оптимальные способы отражения атак. Кроме того, Cisco Security MARS составляет отчеты по собранным данным для удовлетворения нормативных требований. В версии 6.0 появилась система поддержки новых устройств, которая дает пользователям и внешним компаниям возможность встраивать свои устройства в инфраструктуру Cisco Security MARS и тем самым распространять интеллектуальные функции безопасности на всю корпоративную сеть, в том числе на устройства, которые Cisco Security MARS в настоящее время не поддерживает.

# НЕОБХОДИМОСТЬ ПОСТРОЕНИЯ САМОЗАЩИЩАЮЩЕЙСЯ СЕТИ

Корпоративные сети, как и атаки на них, в настоящее время достигли такого уровня сложности, что полностью полагаться на один метод поддержания их безопасности стало невозможно. Это привело к возникновению идеи «глубокой эшелонированной обороны»

В ходе дальнейшего наблюдения можно увидеть, что средства защиты систем такой природы встроены в каждый функциональный блок. Ключевыми возможностями этих средств адаптивной защиты являются:

- непрерывность функционирования,
- ненавязчивость,
- минимизация возможности распространения атак,
- быстрая реакция на еще неизвестные атаки.

Самозащищающаяся сеть Cisco предоставляет решения на основе систем, предоставляющие потребителям новые возможности использования существующей инфраструктуры для сокращения количества источников уязвимостей, минимизации ущерба от атак и повышения доступности и надежности инфраструктуры в целом. Самозащищающаяся сеть также позволяет создавать автономные системы, способные быстро реагировать на вторжения, практически не требуя вмешательства оператора в этот процесс. Такая быстрая ответная реакция необходима для пресечения самых последних видов несанкционированных действий, которые гораздо опаснее своих предшественников.

Самозащищающаяся сеть Cisco продолжает совершенствовать механизм реакции на новые угрозы. На первом этапе (интегрированная защита) выполняется включение механизмов обеспечения безопасности в состав сетевых устройств, таких как коммутаторы и маршрутизаторы. Второй этап (коллективная защита) включает построение связей между элементами сетевой защиты и распространение присутствия сети на оконечные устройства, подключенные к сети. На последнем (на данный момент) этапе построения самозащищающейся сети Cisco происходит внедрение механизма адаптивной защиты от угроз (Adaptive Threat Defense, ATD), позволяющего расширить возможности ответной реакции сети на угрозы на основе новейших технологий Anti-X.