Новый виток гонки безопасности

"Компании становятся все более распределенными, и традиционные подходы к безопасности перестают действовать. На смену традиционным должны прийти новые, прогрессивные методы. Компании и организации больше не могут полагаться на отдельные точечные продукты, работающие на одном уровне. Им нужны унифицированные системы безопасности, работающие на всех уровнях – от сети в целом до конечных устройств – и выполняющие задачи централизованного анализа и управления. Другими словами, современное предприятие должно иметь комплексную интегрированную систему безопасности. Эта система должна постоянно следить за функционированием сети, распознавать угрозы, откуда бы они ни исходили, и координировать действия по ликвидации угроз. Такие системы действительно способны повысить доступность сетей, обеспечить безопасный обмен данными, повысить эффективность работы и помочь системным администраторам и руководителям компаний обрести душевный мир и спокойствие". Такими видит современные системы информационной безопасности вице-президент компании Cisco Мик Скалли.

Сеть как платформа

Давайте вспомним, что представляли собой локальные вычислительные сети на заре своего появления. Образно говоря, они были "ногами", быстро переносящими данные от одного компьютера к другому. Весь интеллект был сосредоточен в узлах сети, в различных программных приложениях. С точки зрения безопасности все было аналогично: антивирусы, VPN, IPS, МСЭ поставлялись только в виде ПО, которое ставилось на обычный универсальный компьютер. Со временем сети становились более интеллектуальными (у компании Cisco,в частности, даже появилась стратегия Intelligent Information Network), и к "быстрым ногам" добавились "мозги": теперь можно было "спустить" логику обработки трафика с уровня приложений на уровень сети. Система безопасности также стала интегрированной, на рынке появилось сетевое оборудование со встроенными межсетевыми экранами, системами предотвращения атак, механизмами контроля содержимого и т.д. Все эти функции ни в чем не уступали своим "выделенным коллегам", а по скорости зачастую их превосходили, достигая мультигигабитных показателей.

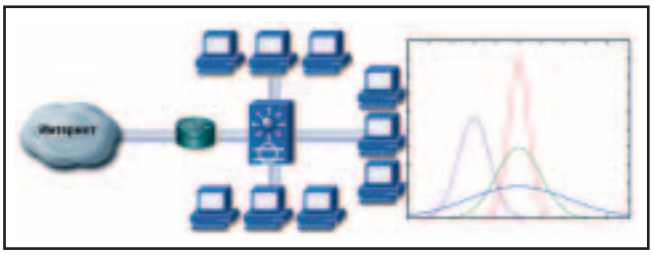
Эволюция стратегии Cisco

Однако, это не значит, что выделенные решения перестали быть востребованными. Существует ряд применений, где эти решения по-прежнему актуальны. В первую очередь, их использование целесообразно в критичных инфраструктурах, где выполнение сетевых задач и функций обеспечения безопасности должно быть разнесено по разным устройствам. Вторая сфера применения выделенных устройств – те организации, в которых безопасностью управляет не ИТ-служба, а отдел защиты информации. В этом случае, во избежание конфликта по доступу к единому устройству, на которое возложены и задачи ИТ, и задачи безопасности, рекомендуется применять отдельные межсетевые экраны, системы предотвращения атак и т.п. И, наконец, третий случай – необходимость использования в организации расширенных механизмов защиты, работающих на прикладном уровне: сканеров безопасности, PKI и т.д.

Специалисты отмечают, что практически все востребованные на сегодняшний день защитные технологии уже разработаны: межсетевые экраны (включая прикладные), системы предотвращения атак, системы безопасности баз данных и ERP-систем, системы безопасности IP-телефонии и систем хранения данных и т.д. Однако все эти технологии и продукты, их реализующие, разрознены и не связаны между собой. В итоге, потребитель вместо того, чтобы защищать свои ресурсы, вынужден заниматься шитьем лоскутного одеяла и управлять "зоопарком", что является крайне трудоемким и неэффективным занятием. Именно поэтому новые решения Cisco, анонсированные в феврале этого года, были направлены, в первую очередь, на решение четырех ключевых задач, стоящих перед любой организацией в области ИТ и информационной безопасности, так и с точки зрения ИБ: интеграции, автоматизации, унификации, адаптации.

Адаптация

Большинство современных средств защиты строятся по принципу "жесткой организованности", при котором сначала четко определяется политика безопасности, затем она реализуется с помощью конкретных средств защиты и в дальнейшем строго исполняется. Однако жизнь



Обнаружение аномалий

не стоит на месте. Не остаются неизменными и угрозы, к отражению которых сеть должна быть готова. Рассчитывать на оперативное реагирование в этом отношении со стороны человека не приходится, поскольку обновлять политику безопасности и распределять ее на сотни устройств со скоростью, соответствующей изменению возникающих угроз, невозможно. Поэтому компания Cisco несколько лет назад начала внедрение в свои решения первых механизмов адаптивности. В частности, системы предотвращения вторжений Cisco IPS стали оснащаться функциями обнаружения аномалий, не требующих знаний о конкретных видах атак, а использующих механизмы адаптивного изучения поведения сетевого трафика и обнаружения в нем отклонений от эталонных значений. При этом такие механизмы могут функционировать как на уровне сети, как в Cisco IPS, так и на уровне отдельных узлов, как в Cisco Security Agent (CSA). Среди новых функций в решениях Cisco можно отметить динамическое определение рейтинга каждой угрозы в зависимости от степени ее опасности и внедрение автоматических фильтров событий и вариантов реагирования для конкретной операционной системы.

Автоматизация

Хочется обратить особое внимание на тот факт, что основные проблемы у современных организаций, возникающие при построении системы безопасности, связаны не с нехваткой технических средств, а с человеческим фактором (оператор не заметил среди тысяч ложных сигналов тревоги реальную атаку, администратор забыл обновить систему предотвращения атак и т.д.). Автоматизация рутинных задач, внедрение принципов эргономики – насущные требования, в соответствии с которыми развиваются современные системы защиты. Можно утверждать, что политика компании в области информационной безопасности, имеющая целью снизить нагрузку на персонал, отвечающий за безопасность, и переложить ее на саму сеть, оставив человеку "творческие" вопросы принятия решения, обречена на успех. А вот ставка на секретные новинки, ноу-хау, сенсации технологических революций сегодня уже не приведет к желаемому результату – потребителя интересует и удобство, а не технические изыски. К сожалению, этот простой тезис понимают далеко не все производители.

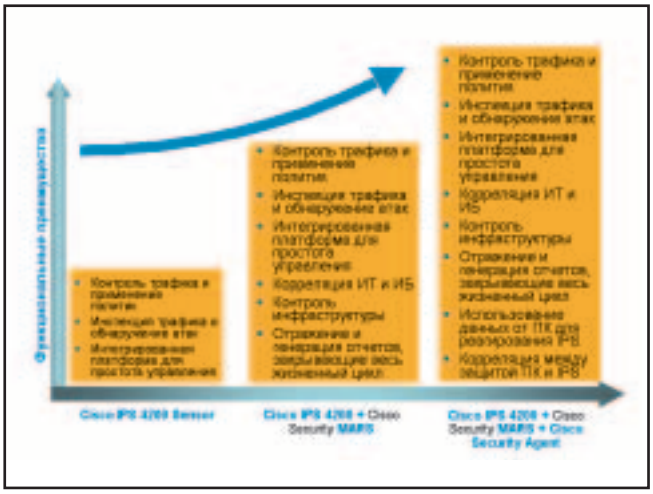
В решениях Cisco реализовано множество механизмов, автоматизирующих рутинные задачи:

- Контроль непротиворечивости правил межсетевого экрана.
- Обнаружение "неработающих" правил.
- Быстрый поиск правил по шаблонам.
- Наследование, копирование и клонирование политик безопасности.
- Выдача в реальном времени рекомендаций относительно средств защиты, которые могут лучше всего отразить реализуемую атаку.
- Групповые операции (обновление, модификация политик и т.д.).
- Контроль изменений на управляемых устройствах, включая откат к предыдущей конфигурации.
- Обновление политики безопасности удаленных устройств даже в условиях их неактивности.
- Автоматическое обновления сигнатур атак и ПО ядра систем защиты.

Интеграция и координация

Интеграция позволяет объединить защитные возможности различных решений и реализовать принцип эшелонированной обороны – проникновение через одну линию обороны не ослабит другие оборонительные рубежи. Кроме того, такая интеграция выводит организацию системы безопасности на новый уровень, когда отдельные продукты начинают взаимодействовать между собой и производят синергетический эффект. На сегодняшний день Cisco реализовала интеграцию для сетевых и хостовых средств предотвращения атак, IPS и сканеров безопасности, систем управления безопасности и серверов аутентификации, антивирусов и VPN-клиентов, межсетевых экранов и IPS а также множество других комбинаций. К примеру, обмен информацией между Cisco IPS и CSA минимизирует число ложных срабатываний и помогает устройствам IPS блокировать атаки до момента их массового распространения. Также появилась возможность интеграции со сканерами безопасности сторонних фирм, расширяющая возможности анализа угроз и принятия адекватных защитных мер.

"Сложная скоординированная работа системы Cisco IPS 6.0 делает ее интеллектуальным корпоративным решением, которое резко снижает уровень угроз и повышает производительность сети, – считает Тами Мартин (Tami Martin), инженер по обнаружению угроз из Argonne Labs. – Скоординированные системы безопасности поддерживают бесперебойную работу, независимо от бурь и штормов, бушующих за пределами сети. Эти системы гарантируют спокойное плавание. Таким образом, Cisco дает нам



Преимущество решения перед отдельным продуктом

не только рост производительности, но еще одно важное преимущество – спокойную работу в безопасной среде".

В условиях тесного взаимодействия между IPS и CSA задача защиты всей сети решается на уровне системы мониторинга и реагирования CS-MARS, которая собирает всю необходимую информацию на одном устройстве, проводит сложный анализ сетевого поведения, распознает угрозы и координирует свои действия с системой настройки средств защиты Cisco Security Manager. Последняя, в случае необходимости, меняет правила безопасности в масштабе всего предприятия.

"Координация усилий – важнейшее требование безопасности. Системный подход Cisco к защите сетей является уникальным и беспрецедентным, – утверждает Карл Гудмен (Carl Goodman), ИТ-менеджер из калифорнийского банка Premier Valley Bank. – Мы полагаемся на скоординированные решения Cisco для безопасности, необходимые для организованной защиты нашего бизнеса. Поставщик управляемых услуг безопасности HEIT Consulting стал нашим стратегическим партнером. Вместе с Cisco и HEIT мы надежно защищаем внутренние операции и клиентов, а также выполняем требования регулирующих органов. Другими словами, Cisco и HEIT снимают наши проблемы в области безопасности".

Унификация

Унификация в системах информационной безопасности развивается по двум направлениям: унификация управления и выработка единых механизмов борьбы с угрозами. Например, раньше у компании Cisco была только одна платформа для обнаружения и предотвращения атак – Cisco IPS 4200 Sensor. Затем появился сетевой модуль NM-IDS для маршрутизаторов, потом сервисный модуль для коммутаторов Cisco IDSM-2, далее аналогичные механизмы в многофункциональных защитных устройствах Cisco ASA 5500 и, наконец, встроенное ПО IOS IPS в сетевом оборудовании Cisco. Поддерживать, обновлять и управлять таким множеством платформ, решающих одну и ту же задачу, не очень просто как с точки зрения производителя, так и с точки зрения пользователя. Гораздо целесообразней сделать платформу единообразной и стандартизованной (что и делается компанией Cisco). Унификации "подвержены" решения по отражению угроз (IPS), межсетевому экранированию (firewall) и построению VPN, которые могут быть представлены и в виде отдельных устройств и в виде функций маршрутизаторов, коммутаторов и точек беспроводного доступа. Что касается унификации управления, то она заключается в создании единой платформы, которая позволяет с помощью одной системы управлять различными средствами защиты и сетевым оборудованием.

"В результате мы получаем интеллектуальную систему безопасности, действующую в масштабе всей сети. Эта система состоит из устройств и приложений, которые обмениваются данными и координируют все действия в области безопасности, – говорит Мик Скалли. – Она распознает самые разные угрозы: нарушения правил безопасности, бреши в системах защиты, аномальное поведение, – и упрощает управление средствами защиты. Скоординированная интеллектуальная система безопасности обеспечивает простоту и эффективность распознавания угроз и быстрое реагирование на угрозы в реальном времени".

А. В. Лукацкий,
бизнес-консультант по безопасности,
компания Cisco

НОВОСТИ

Microsoft Dynamics AX на Раменском ГОКе

Раменский горно-обогатительный комбинат подвел итоги второго года эксплуатации корпоративной системы управления комбинатом, разработанной на основе Microsoft Dynamics AX специалистами компании "НОРБИТ" (группа компаний ЛАНИТ).

Microsoft Dynamics AX используется на Раменском ГОКе в качестве корпоративной системы управления с января 2006 года. Фактически в опытную эксплуатацию система была передана уже в мае 2005 года, когда был завершен первый этап проекта и автоматизированы ключевые логистические операции комбината – учет выпуска и сбыт готовой продукции, снабжение подразделений и складской учет, а также управление финансами, расчеты с клиентами и поставщиками и бухгалтерский учет в части отражения логистических операций. В полном объеме функциональность бухгалтерского учета была запущена на РГОКе на втором этапе проекта в апреле 2006 года наряду с налоговым учетом, управленческой отчетностью в соответствии с требованиями акционера, а также модулем управления кадрами.

Внедрение Microsoft Dynamics AX на Раменском ГОКе позволило не только создать единую интегрированную систему для ведения данных о хозяйственной и финансовой активности предприятия: благодаря использованию Microsoft Dynamics AX удалось повысить точность планирования поставок готовой продукции и обеспечить оперативное проведение отгрузок.

Возможности системы также позволили вести оперативный контроль уровня дебиторской задолженности по каждому клиенту, вследствие чего возросло качество обслуживания клиентов комбината и были улучшены финансовые показатели. Кроме того, удобный механизм сбора и анализа заявок на ТМЦ, реализованный в системе, позволил повысить эффективность системы снабжения комбината.

В настоящее время в системе работает около 100 сотрудников РГОКа, в том числе специалисты отделов сбыта и закупок, финансовой службы и бухгалтерии, однако с развитием системы, по оценкам ИТ-службы комбината, число пользователей будет увеличиваться. Развитие корпоративной системы РГОКа продолжается, и сейчас комбинат занимается проектом автоматизации расчетов заработной платы в Microsoft Dynamics AX, а в планах – реализация в системе механизмов управления качеством продукции, техническим обслуживанием и ремонтами оборудования, а также интеграция с лабораторией химического анализа сырья.