Интегрированная безопасность: фундаментальные перемены в области защиты сетей

В последние годы наблюдаются огромные перемены в области сетевых технологий, где появляются все новые устройства и услуги. Появление новаторских сетевых решений, таких как виртуализация, вычисления в "сетевом облаке" и веб-доступ для сотрудников, партнеров и заказчиков, резко изменило инфраструктуру многих организаций. Кроме того, большое количество компаний переходит к совместной работе в распределенной виртуальной среде, не знающей границ и расстояний. Все это позволяет быстро выводить на рынок новые продукты и услуги. Доступ к сетям становится повсеместным, сотрудники становятся все более мобильными, так как получают необходимые для этого устройства и сети; технологии Web 2.0 и сервисно-ориентированные архитектуры создают новые способы индивидуальной и совместной работы, позволяя по-новому взаимодействовать с заказчиками и партнерами.

Вместе с тем, при всей несомненной пользе этих изменений они создают новые и довольно серьезные проблемы с точки зрения безопасности. Традиционные "точечные" средства защиты не могут обеспечить безопасность в процессе трансформации бизнеса, оставляя без защиты критически важные новые ИТ-ресурсы и не давая возможности внедрить новые услуги, ибо они не в состоянии защитить новые процессы и протоколы. В то же время новые процессы и услуги становятся уязвимыми для принципиально новых угроз, подрывающих работоспособность сетей. Среди новых угроз особо надо отметить кражу идентификационных и репутационных данных и неправомочное использование прикладных и сетевых ресурсов.

Новые угрозы имеют ряд общих характеристик, отличаясь сложностью, целенаправленностью и нацеленностью на новые приложения и услуги. Вот некоторые из этих угроз:

- появление весьма сложных и эффективных "программных роботов" (ботнетов);
- появление первых хакерских продуктов для мобильных телефонов;
- совершенствование методов кражи идентификационных данных;
- совершенствование шпионского программного обеспечения;
- использование уязвимостей веб-приложений;
- атаки по цепочке поставок, заражающие устройства конечных пользователей.

Появление жестких нормативных требований к безопасности еще больше затрудняет защиту сетей. Сегодня многие организации не знают, как удовлетворить все нормативные требования и при этом успешно развивать свой бизнес.

Типичные ошибки в сфере безопасности

Неспособность защитить бизнес-процессы делает любую организацию весьма уязвимой, причем самые опасные угрозы (на которые организация чаще всего не обращает внимания) создаются ее же собственной сетью. Ниже приведен краткий обзор наиболее типичных ошибок в данной области.

Использование "точечных" продуктов и решений

Эта ошибка возникает, когда инфраструктура безопасности состоит из множества традиционных продуктов, приобретавшихся в течение многих лет для решения частных задач. Такие продукты слабо связаны друг с другом, и в результате на предприятии стихийно складывается архитектура безопасности, характеризуемая:

- отсутствием централизованного управления;
- невозможностью оценить общий уровень "здоровья" сети;
- невозможностью сбора и совместного использования критически важных данных о событиях в сфере безопасности;
- полным или частичным отсутствием взаимодействия между продуктами безопасности в части противодействия угрозам и обеспечения прозрачности сети;
- отсутствием реальной интеграции между продуктами безопасности и сетевыми элементами;
- сложностью эксплуатации разнородных продуктов безопасности и управления ими.

Решения, мотивированные страхом

Часто организации принимают решения в области безопасности импульсивно, под воздействием газетных новостей о появлении "страшных вирусов" и катастрафических последствиях потерь данных. При этом в организации, как правило, отсутствует единый стратегический подход к развитию системы безопасности, борьбе с новыми угрозами и разработке единой политики, опирающейся на пере-

Одиннадцатая ежегодная конференция Microsoft®

Microsoft®

Платформа

2010

12-13 ноября

Москва, Центр Международной торговли
Краснопресненская набережная, 12

6 треков

60+ технических докладов

РЕГИСТРИРУЙТЕСЬ

Microsoft

http://msplatforma.ru

довой опыт. Подобный подход может достаточно эффективно противостоять определенному Интернет-червю или атаке DoS, но при этом упускать из виду такие важные вопросы, как отключение неиспользуемых портов, разработка единых правил доступа к пользователям и устройствам, борьба с халатностью и намеренными нарушениями правил со стороны сотрудников, поиск "пиратских" точек беспроводного доступа и т.д. Бороться с острыми проблемами безопасности, конечно, нужно, но не менее важно иметь общую стратегию управления рисками и безопасностью, которая охватывает всю вашу сеть, сетевые услуги и системы безопасности, рассматривая их как одно целое.

Выбор продуктов по функциональному признаку без стратегического подхода

Еще одна типичная ошибка – это выбор продукта безопасности, исходя из наличия или отсутствия той или иной функции. При этом упускается из виду тот факт, что продукты непрерывно совершенствуются, в связи с чем один продукт может иметь функцию, отсутствующую в другом, но через полгода ситуация может кардинальным образом измениться. Оценивать продукты безопасности нужно не по отдельным функциям, а по их способности поддерживать критически важные бизнес-приложения, услуги и инфраструктуры. Выбирая тот или иной продукт, необходимо учитывать следующие моменты:

- Может ли это устройство собирать данные с других сетевых устройств и продуктов безопасности? Может ли оно передавать им свои данные?
- Понимает ли это устройство особенности критически важных приложений и услуг, работающих в данной сети (IP-телефония, трафик прикладного уровня, протоколы маршрутизации и коммутации и т.д.)?
- Если изменится протокол, не имеющий отношения к безопасности (например, произойдет апгрейд протокола IP-телефонии), сколько времени уйдет на адаптацию данного устройства к новой версии протокола?
- Способствует ли это устройство достижению необходимой прозрачности сети и поддерживает ли оно централизованное управление защищаемыми сетевыми элементами? Или же устройство дает лишь один узкий взгляд на отдельный аспект функционирования сети?

Оценка любого продукта должна происходить с учетом более широкого контекста управления рисками. Новый продукт безопасности должен максимально соответствовать общим требованиям бизнеса и управления рисками в уникальной среде конкретной компании сегодня и в ближайшем будущем.

Неадекватная политика в области безопасности

Интеллектуальная политика – важнейшая основа любой стратегии в сфере безопасности. К сожалению, во многих организациях такой политики нет, а там где она все же существует, многие ее положения уже устарели или забыты. Ну, а там, где политика разрабатывалась "для галочки", с самого начала никто и не думал ее выполнять. Другая ошибка состоит в том, что политика часто сфокусирована на установке отдельных продуктов. При этом упускается из виду необходимость поддержки корпоративной сети и деловой стратегии. В результате мы получаем политику, которая не решает двуединую задачу поддержки бизнеса и снижения рисков и не определяет требования в области управления, контроля и прозрачности.

Разработка интегрированной стратегии в сфере безопасности

Сеть, как правило, не является однородной, а состоит из множества сегментов (центр обработки данных, "кампусная" сеть в комплексе зданий, граничная сеть, средства удаленной работы, сети отделений и т.д.), каждый из которых имеет свои функции и требования к безопасности. При этом каждый сегмент решает уникальные деловые задачи, использует уникальные решения и подвергается уникальным угрозам. Защитить столь разнородную структуру можно лишь при одном условии: необходимо учитывать специфические требования каждого сетевого сегмента и в то же время соблюдать единую политику безопасности для всей сетевой среды.

Решение этих задач требует полного переосмысления методов безопасности в организации. С этой целью компания Cisco разработала стратегию Security Control Framework. Она представляет собой стандартизированный процесс разработки и реализации политики в области безопасности. Принципы Cisco Security Control Framework используются для выбора технологий и практических методов, которые в наибольшей степени подходят для сетевой среды конкретной организации и для отражения угроз в ее отдельных сегментах.

Cisco Security Control Framework можно использовать в качестве основы для разработки и реализации единой комплексной политики в сфере сетевой безопасности (рис. 1). При этом множество технологий и функций будут работать совместно и давать полное представление о сетевых событиях, соблюдении разработанных правил и появлении аномального трафика. Кроме того, в рамках данного подхода такие инфраструктурные сетевые элементы, как маршрутизаторы и коммутаторы, также используются для непрерывного мониторинга и принятия упреждающих мер.

Учет требований бизнеса и разработка интеллектуальных правил в сфере безопасности

Требования бизнеса и безопасности постоянно меняются, поэтому первейший принцип Cisco Security Control Framework состоит в разработке, непрерывной оценке и коррекции правил (политик) безопасности, которые должны постоянно подстраиваться под меняющиеся требования. Для этого необходимо знать цели и задачи бизнеса вашей компании сегодня и в обозримом будущем, а также правильно определять, что этим целям и задачам угрожает.

Рис. 1. Структура управления безопасностью Cisco Security Control Framework

Процессы Cisco Security Control Framework включают пять основных этапов:

1. ***Планирование.*** Первый этап процесса Security Control Framework – критический анализ целей и задач бизнеса, поддерживаемых сетью, и определение угроз, которым эти цели и задачи подвергаются. Сюда включается оценка угроз и рисков, направленных против определенных активов, текущее состояние безопасности в организации и наличие ресурсов и технологий, способных противостоять угрозам. Необходимо оценить сильные и слабые стороны существующей архитектуры и определить, чего не хватает в этой архитектуре и в информационно-технологическом отделе компании.
2. ***Проектирование.*** Далее необходимо составить подробное описание проекта с указанием выбранных платформ, функций и передовых методов, необходимых для того, чтобы закрыть бреши, вскрытые на предыдущем этапе, и удовлетворить будущие деловые и технические требования.
3. ***Внедрение.*** Этот этап включает установку и подключение платформ и других ресурсов, а также укрепление сетевой инфраструктуры. Обычно внедрение проходит поэтапно по заранее разработанному плану.
4. ***Эксплуатация.*** Эксплуатация нового решения для безопасности включает мониторинг инфраструктуры и управление ею, а также сбор и анализ информации и принятие практических мер для своевременного отражения угроз.
5. ***Поддержка.*** Планы в области безопасности необходимо регулярно пересматривать. Это позволит вовремя обнаруживать бреши и уязвимости, вызванные непрерывным изменением сетевой среды. Для этого используется информация, получаемая в ходе повседневных операций и внеплановых проверок. Оценка рисков и угроз должна проводиться на регулярной основе. Результаты должны использоваться для очередного запуска цикла разработки, позволяющего непрерывно совершенствовать архитектуру безопасности и полнее удовлетворять меняющиеся требования безопасности и бизнеса.

Прозрачность и контроль

Два других фундаментальных принципа Security Control Framework – это обеспечение максимальной прозрачности сетевых устройств и событий и максимальной управляемости пользователей, устройств и трафика, передаваемого по сети. В области прозрачности и контроля Security Control Framework определяет шесть действий, необходимых для разработки любой политики безопасности, выбора и установки любого устройства безопасности, внедрения единой последовательной стратегии безопасности во всех сетевых сегментах, максимального расширения возможностей идентификации и отражения угроз целям и задачам бизнеса, а также для реализации единой политики в области безопасности.

Каждое действие в области безопасности и каждое сетевое устройство должно оцениваться и выбираться с учетом его способности обеспечивать прозрачность событий, пользователей, устройств и поведения сети, а также поддерживать четкое управление устройствами, пользователями и трафиком для отражения угроз в любом сетевом сегменте.

Принципы прозрачности:

- Идентификация и классификация пользователей, услуг, трафика и конечных устройств.
- Мониторинг производительности, поведения, пользовательских предпочтений, событий и выполнения правил.
- Сбор, анализ и корреляция системных событий.

Принципы контроля:

- Защита оконечных устройств, услуг, серверов, приложений и инфраструктуры.
- Изоляция пользователей, систем и услуг для локализации атак.
- Реализация правил (политик) доступа и безопасности и смягчение угроз, возникающих в процессе тех или иных сетевых событий.

Строительство архитектуры безопасности

Одним из примеров реализации принципов Cisco Security Control Framework является Cisco SAFE – новый набор типовых архитектур безопасности, дающий подробную информацию о проектировании и внедрении безопасных и надежных сетевых инфраструктур и политик для их поддержки. Эти данные основаны на принципах Security Control Framework, передовом опыте и результатах, полученных на протяжении тысяч человеко-часов, затраченных на проектирование, тестирование и документирование.

В современной среде атаке может быть подвергнут любой сетевой элемент. По этой причине архитектура Cisco SAFE построена по принципу глубоко эшелонированной обороны. Интеллектуаль-

ные системные средства Cisco SAFE обеспечивают безопасность инфраструктуры, оконечных устройств, сетевых устройств, приложений и прикладных серверов, баз данных, веб-серверов, серверов электронной почты и других серверных систем, коммуникационных устройств и систем хранения данных. Эти задачи решаются за счет встраивания функций безопасности в каждый из перечисленных компонентов. В результате каждый компонент превращается из потенциальной жертвы хакерской атаки в устройство, повышающее общую безопасность и управляемость сети, играющее свою роль в целостной стратегической системе сетевой безопасности и поддерживающее взаимодействие с другими элементами, а также работу системных интеллектуальных средств. И, наконец, средства управления и отчетности SAFE поддерживают единую политику безопасности и стратегию мониторинга, анализа и отражения угроз.

Другой критически важный элемент архитектуры Cisco SAFE – ее модульность, которая помогает защищать сеть, наилучшим образом учитывая уникальные особенности каждого сетевого сегмента и требования взаимодействия между ними. Модульность продлевает срок службы существующего оборудования и обеспечивает защиту инвестиций заказчика. Кроме того, модульный дизайн позволяет включить в состав архитектуры инструментальные средства для облегчения повседневной работы и сокращения текущих расходов.

Принципы Cisco SAFE укрепляют безопасность не только в пределах определенных сетевых сегментов, но и между функциональными сетевыми зонами, что особенно важно в ситуации, когда данные и транзакции передаются в масштабе всей сетевой инфраструктуры. Информация о событиях и состояниях передается между сетевыми устройствами и средствами безопасности, обеспечивая высокую прозрачность и координацию ответных действий, предпринимаемых в рамках единой стратегии.

Принципы сетевой безопасности Cisco SAFE бесплатно предоставляются любой организации, желающей повысить защищенность своей сетевой среды. Вот важнейшие преимущества принципов Cisco SAFE:

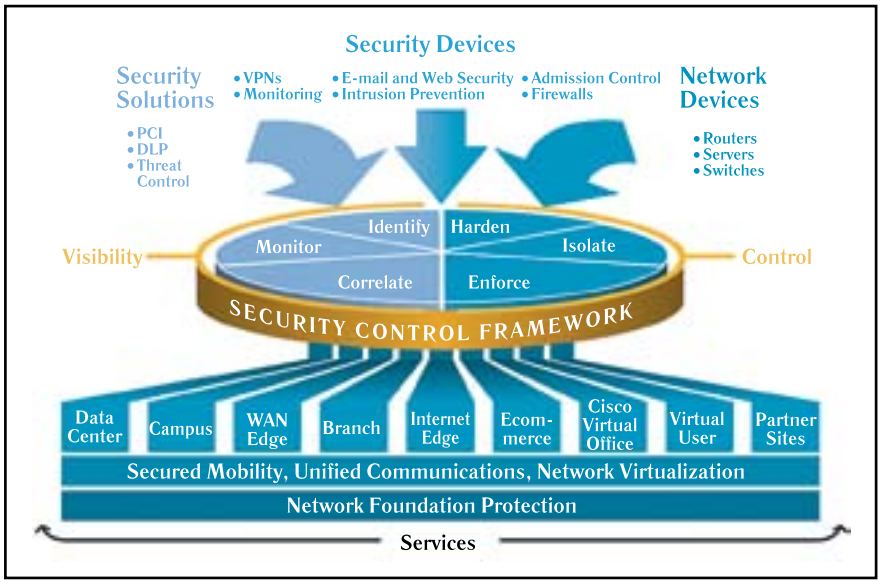

Рис. 2. Использование Cisco Security Control Framework для разработки модульных решений

- ***Подробный дизайн***, основанный на характеристиках Security Control Framework, передовом опыте и практических испытаниях, помогает организациям быстро переходить от концептуального проектирования к практическому внедрению. Кроме того, Cisco SAFE помогает правильно организовать обсуждение вопросов, связанных с разработкой и совершенствованием правил (политик) безопасности. Вместо метода проб и ошибок организация начинает использовать хорошо структурированный подход к защите сетевой инфраструктуры, дающий существенную экономию расходов.
- ***Модульный дизайн*** не только удовлетворяет уникальные требования различных сетевых сегментов в сфере безопасности, но и позволяет непрерывно совершенствовать средства защиты (рис. 2). Большинству организаций не под силу полностью заменить всю инфраструктуру безопасности. Модульный же дизайн Cisco SAFE дает возможность делать это постепенно и поэтапно. Он позволяет оценить существующую систему безопасности, определить, с какого сегмента лучше начинать перестройку и как реализовать единую стратегию укрепления безопасности, обновляя в первую очередь сегменты, в наибольшей мере нуждающиеся в замене. Поскольку все компоненты SAFE являются частью единой стратегии, модернизация каждого из них вносит свой вклад в общее повышение прозрачности, управляемости и защищенности всей сети.
- ***Принцип глубоко эшелонированной обороны*** защищает организацию от более сложных угроз. Современные многовекторные атаки организованы так, что отдельные элементы этих атак способны обойти системы безопасности либо игнорируются ими как не представляющие особой опасности. Целостная система безопасности SAFE позволяет отдельным устройствам не только обмениваться данными друг с другом, но и агрегировать информацию для распознавания и отражения сложных многовекторных атак.
- ***Подробные описания архитектуры и сетевых платформ*** сокращают расходы информационно-технологического отдела, связанные с проектированием, установкой и пуском систем безопасности в эксплуатацию.
- ***Взаимодействие элементов безопасности с сетевой инфраструктурой*** не только повышает уровень защищенности сети, но и увеличивает ее надежность, помогая поддерживать работу ключевых приложений и сетевых услуг.

Как системы безопасности помогают бизнесу

Чтобы успешно отражать современные угрозы, организации должны полностью пересмотреть свою стратегию в сфере безопасности и перейти от выбора и установки отдельных продуктов к интегрированному подходу, предусматривающему защиту всей сетевой среды. Единая целостная стратегия безопасности расширяет возможности организации по идентификации, предотвращению и отражению атак за счет максимальной прозрачности сетевых событий и повышения управляемости устройств, пользователей и трафика, передаваемого по сети. По-настоящему эффективная система безопасности помогает организации лучше внедрять критически важные бизнес-приложения и услуги, поддерживающие совместную работу, повышающие производительность труда и удовлетворяющие растущие потребности заказчиков, поставщиков, партнеров и сотрудников.

Более подробная информация о стратегии Cisco Security Control Framework и типовых архитектурах безопасности Cisco SAFE опубликована на странице www.cisco.com/go/safe.

Билл МакГи (Bill McGee), компания Cisco

НОВОСТИ

Новости Dassault Systemes

Федеральное космическое агентство РФ признало соответствующими отраслевым стандартам PLM-решения от компании Dassault Systemes для управления проектированием, разработкой и производством сложной наукоемкой продукции космического и оборонного назначения, включая ракеты-носители, спутники и космические станции.

Для решения ряда задач, стоящих перед отраслью, РОСКОСМОС реализует программу комплексного развития информационных технологий в российской космической индустрии. В рамках партнерства РОСКОСМОС и Dassault Systemes через структуру ФКА – ФГУП "ЭХО" будут интегрированы программно-технические и научно-методические разработки Dassault Systemes в таких областях, как проектирование изделия (CATIA), цифровое производство (DELMIA), управление процессами проектирования и производства продукции и обеспечение совместной работы производителей и поставщиков (ENOVIA).

"Работа с географически распределенными цепочками поставщиков приводит к необходимости эффективной коммуникации в режиме реального времени. Мы надеемся, что технологии 3D в будущем позволят в значительной мере улучшить качество производимой продукции благодаря углубленной интеграции между элементами механики, электрики и программного обеспечения, – говорит Сергей Алексеевич Пономарев, заместитель руководителя Федерального космического агентства. – Мы разделяем идею использования трехмерных технологий и надеемся, что PLM-решения станут одной из основ, позволяющих достигнуть наивысшего качества продукции".

Решения удаленного управления и мониторинга на основе контроллеров Unitronics и GSM/GPRS модемов

UNITRONICS

- Типовые решения для удаленного управления объектами, метрологии с помощью SMS, GPRS или GSM-Data.
- Контроллеры Unitronics разработаны на основе микросхем Infineon Technologies AG и полностью совместимы с GSM/GPRS модемами.
- Возможность защищенного от взлома управления с сервера, удаленного компьютера, мобильного телефона.
- Контроллеры Unitronics совмещают в себе ПЛК, HMI с поддержкой GSM/GPRS и широкие возможности по расширению портов и I/O.
- Бесплатное ПО LadderLogic имеет релейную логику и большой набор готовых функциональных блоков.
- В местных офисах компании Klinkmann Вы можете получить информацию о конкретных решениях на базе Unitronics.

Спрашивайте бесплатный каталог Klinkmann на русском языке в офисах Klinkmann или посетите сайт www.klinkmann.ru.

ПЛК Unitronics Vision - теперь с полной русскоязычной поддержкой

KLINKMANN
www.klinkmann.ru

Санкт-Петербург
тел. +7 812 327 3752
klinkmann@klinkmann.spb.ru

Москва
тел. +7 495 641 1616
moscow@klinkmann.spb.ru

Екатеринбург
тел. +7 343 376 53 93
yekaterinburg@klinkmann.spb.ru

Пятигорск
тел. +7 8793 318441
Pyatigorsk@klinkmann.spb.ru

Самара
тел. +7 846 342 6655
samara@klinkmann.spb.ru

Київ
тел. +38 044 495 3340
klinkmann@klinkmann.kiev.ua

Минск
тел. +375 17 2000 876
minsk@klinkmann.com