ДЕЛОВОЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЕЖЕНЕДЕЛЬНИК
WWW.COMPUTERWORLD.COM.UA

COMPUTERWORLD УКРАИНА

#3-4 (667)
26 ЯНВАРЯ 2009

ISSN 1609-8145

Unitrade Group: конфликт акционеров
с.4

Итоги года украинской ИТ-дистрибуции
с.14

Крейг Барретт (Intel) на CES 2009: «Технологии – инструмент решения проблем»
с.20

Дистрибуция сетевого/телекоммуникационного оборудования в 2008 году
с.16

Business Intelligence: об актуальности и тенденциях
с.28

ФИЛИПП РОГГЕБАНД
МЕНЕДЖЕР ПО ПРОДУКТАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ CISCO В ЕВРОПЕ И НА РАЗВИВАЮЩИХСЯ РЫНКАХ:

«Технологии безопасности Cisco – самое комплексное решение на рынке»
с.10

Филипп Роггебанд,

менеджер по продуктам обеспечения безопасности Cisco в Европе и на развивающихся рынках:

«Технологии безопасности Cisco – самое комплексное решение на рынке»

Вопрос обеспечения безопасности сегодня стоит особенно остро: уровень киберпреступности растет устрашающими темпами, все более важными для успешного функционирования бизнеса становятся такие характеристики, как сохранность и защищенность корпоративных данных. Отвечая на вопросы «ComputerWorld/Украина», Филипп Роггебанд, «гуру» по безопасности компании Cisco, подчеркнул важность всестороннего, глобального подхода к построению системы безопасности и рассказал о тенденциях дальнейшего развития стратегии безопасности Cisco.

Интервью провела Елена Варганич

Наше общение Филипп начал с шутки: «Однажды два человека гуляли по лесу и вдруг повстречали медведя гризли. Один очень испугался, а второй спокойно снял рюкзак, вынул оттуда беговые кроссовки и начал переобуваться. Первый говорит: "Зачем тебе это? Ты все равно не побежишь быстрее медведя гризли!", а второй отвечает: "Мне и не надо бежать быстрее гризли. Главное, бежать быстрее тебя". Другими словами, говоря о защите данных, помните, что, уделяя достаточное внимание информационной безопасности, ваша компания становится менее привлекательной мишенью для злоумышленников: они всегда предпочтут атаковать компанию, защиту которой легче сломать».

CW: Филипп, на недавней конференции Cisco по технологиям безопасности Вы говорили, что в период глобального кризиса компаниям следует в первую очередь заботиться об обеспечении защиты своей ИТ-инфраструктуры, т.к. экономическая нестабильность провоцирует еще более частые всплески киберпреступности. В связи с этим растет ли спрос на технологии безопасности Cisco?

Вы знаете, за последний квартал было отмечено даже небольшое падение спроса, но это объясняется, прежде всего, тем, что люди занимали некую выжидательную позицию. Кризис заставил многих «замереть» и повременить с какими-либо решениями и приобретениями. Но на сегодняшний день мы видим растущее желание людей использовать новые бизнес-модели, работать с унифицированными коммуникациями и веб-порталами. Конечно же, люди все

больше осознают, что внедрение новых бизнес-моделей невозможно без обеспечения повышенной безопасности, а стало быть, без использования соответствующих систем. И мне кажется, что скоро спрос именно на системы безопасности увеличится по сравнению с другими техническими средствами.

CW: Насколько технологии безопасности Cisco востребованы в Украине по сравнению с рынками других стран?

По данным, которые у меня есть, я могу сказать, что показатели продаж систем безопасности относительно сетевых систем в Украине вполне сравнимы с такими показателями на рынках других стран.

Еще могу отметить, что в Украине все еще очень востребованы системы безопасности так называемого первого уровня, файрволы и т. п. Видимо, пока еще не пришло осознание необходимости внедрять системы контроля доступа в сеть или системы защиты оконечных устройств. Движение в эту сторону есть, но пока достаточно медленное.

CW: Расскажите, пожалуйста, о самозащищающейся сети Cisco — Self-Defending Network.

Несколько лет назад, когда мы впервые заговорили о самозащищающихся сетях, это скорее был такой себе маркетинговый ход, обещание на будущее.

Но еще тогда мы определили три вещи. Во-первых, безопасность будет встроена во все, что мы делаем. Во-вторых, будет обеспечено эффективное взаимодействие между этими устройствами в сети. И наконец, в-третьих, мы стремимся к адаптивности для того, чтобы предусмотреть приближающуюся атаку, неизвестную раньше, например «атаку нулевого дня». Когда мы покупаем компании с какими-то решениями и разрабатываем новые средства, мы всегда выдерживаем при этом элемент безопасности, который должен присутствовать во всех наших предложениях.

Мы продолжаем говорить о самозащищающейся сети, но если бы я работал в отделе маркетинга, я бы говорил не о сети, а скорее об ИТ-инфраструктуре, которая имеет такую самозащиту, либо о самозащищающейся коммуникационной системе. Ведь и IP- телефония, и беспроводные средства должны иметь самозащиту.

Я не буду рассказывать о конкретных видах продукции, потому что на это просто не хватит времени, но в целом скажу, что у нас в каждом продукте, в каждом наборе продуктов обязательно обеспечивается защита сети, оконечных устройств, контента и защита на уровне приложений.

> Я хочу подчеркнуть, что мы переносим безопасность на массивы данных, а не на сами устройства, — ведь только так можно обеспечить комплексную защиту сети

CW: Филипп, о каких нововведениях в концепции самозащищающейся сети Вы могли бы рассказать?

Среди новинок мне хотелось бы выделить репутационные сервисы. На сегодня они в основном используются как антиспам, но в ближайшем будущем, думаю, через несколько месяцев, вы увидите, что они будут использоваться во всех аспектах сетевой безопасности, на уровне файрволов, систем предотвращения вторжений (IPS), конечно, антиспамовых, антифишинговых программ, а также на уровне приложений.

Также хочу отметить, что еще год назад мы объявили о выходе новой технологии TrustSec. В прессе появились об этом кое-какие заметки, но не повсеместно. А на самом деле, я уверен, что эта технология очень важна и будет развиваться. Она фактически базируется на тех компонентах, из которых состоит сеть.

Эта технология позволяет распознавать уровень безопасности трафика, проходящего через сетевое устройство. К примеру, данные могут быть конфиденциальнми, строго конфиденциальнми, высшего уровня секретности, либо общедоступными. Идея в том, что даже маршрутизатор, через который проходит пакет, содержащий определенные данные, «знает», что с этими данными должно быть сделано, у него есть политики с определением, что должно произойти с этим трафиком. Т. е. Cisco TrustSec создает «доверенную сеть предприятия», которая включает в себя коммутаторы, маршрутизаторы и контроллеры унифицированной беспроводной сети, выполняющие функции аутентификации пользователей, распределения ролей, выполнения правил доступа и защиты конфиденциальности сетевого трафика.

Этот наш прошлогодний анонс — только первый шаг, это возможность иметь маленькие «ярлычки», определяющие уровень конфиденциальности данных.

Я хочу подчеркнуть, что мы переносим безопасность на массивы данных, а не на сами устройства, — ведь только так можно обеспечить комплексную защиту сети. Техника сама по себе ничто, если она не соответствует потребностям бизнеса. Здесь мы говорим о необходимости того, чтобы конфиденциальные данные не покидали пределы компании, не попадали к лицам, не имеющим на это права.

Ну и, наконец, я должен упомянуть о соответствии системы безопасности самым новым регуляторным требованиям и положениям.

CW: Каким образом обеспечивается эффективность бизнеса с помощью технологий безопасности Cisco?

Многие люди раньше рассматривали, да и до сих пор еще рассматривают, безопасность как страховку: ты приобретаешь на всякий случай полис, но надеешься, что он никогда не пригодится, и откладываешь подальше. Этот подход, мягко говоря, устарел.

Приведу небольшой пример, который показывает, каким образом применение технологий безопасности помогает сделать бизнес более эффективным, более конкурентоспособным. Современные требования взаимодействия с поставщиками, заказчиками, партнерами показывают, что нужно открывать свои сети перед ними для повышения конкурентоспособности вашего бизнеса. Можно установить, например, портал, через который они могут видеть прохождения заказов, отслеживать интересующую информацию и т. п. Все это будет работать, если есть доверие между сторонами, а доверие возможно только в том случае, когда используются достойные средства защиты. Для действующей защиты нужно обеспечить контроль доступа и шифрование данных. Для того чтобы понимать, что обмен данными производится с конкретным партнером и больше ни с кем, и по определенным стандартам шифрования. Только так на сегодня можно обеспечить такую форму работы компании. Эта модель бизнеса невозможна без использования качественных средств защиты.

CW: Насколько система безопасности Cisco адаптивна к будущим потребностям бизнеса, и с помощью чего это достигается?

Адаптивность системы очень велика, потому что все в ней основано на процессе постоянного обновления. Используются репутационные сервисы, которые пресекают еще незнакомые угрозы. Существует такой сервис, как IntelliShield, который постоянно информирует заказчиков о потенциальных угрозах информаци-

онной безопасности и уязвимостях продуктов ИТ, которые могут затронуть всю ИТ-инфраструктуру компании. При помощи этой системы соответствующие оповещения передаются на устройства безопасности достаточно быстро, что позволяет на корню пресечь ряд вредоносных атак.

Мы всегда стараемся опережать мысли и действия хакеров. Например, пока еще не было атак на уровне протоколов баз данных, а мы уже готовы к таким атакам в нашей системе IPS.

CW: С развитием бизнеса сетевая инфраструктура растет и усложняется. Какие трудности с обеспечением информационной безопасности при этом возникают?

Я считаю, что изначально надо рассматривать безопасность не как что-то такое «техническое», а как что-то на уровне регламента, политики компании. Например, у вас есть отдел продаж, маркетинга, технический отдел. Необходимо просто сразу предположить, кто и с кем должен общаться, для каких целей. Потом очень легко можно будет справиться с ростом компании, провести масштабирование. Проблем не будет, если изначально схему продумать и правильно построить.

Опять же, с самого начала производится шифрование соответствующих каналов обмена информацией между различными отделениями и персонами компании. Другими словами, потом между ними «нажатием кнопочки» устанавливается определенный закодированный канал, и происходит обмен информацией. Заранее, по логической цепи, программным образом выстраиваются все эти каналы, и все функционирует, а потом, если надо, расширяется, наращивается.

Речь идет о том, чтобы обеспечить потребности бизнеса техническими решениями. Поэтому изначально следует продумать, кто и с кем должен быть на связи, установить соответствующие каналы, сформировать конфигурационные файлы и протоколы, которые будут потом передаваться на файрволы, VPN-концентраторы и другие устройства.

> Мы всегда стараемся опережать мысли и действия хакеров. Например, пока еще не было атак на уровне протоколов баз данных, а мы уже готовы к таким атакам в нашей системе IPS

В целом, если логично и разумно сразу все продумать, то потом система будет работать отлаженно.

Если по мере расширения сети в нее вводятся новые компоненты, то система безопасности будет предопределять то, как обеспечить безопасность для этих новых компонентов.

Возьмем, например, автомобиль. Есть руль, коробка передач, педаль газа, — но нужна еще панель приборов, чтобы видеть, что происходит с машиной. Так и наша система позволяет нам видеть, как на приборной панели, какие это атаки, откуда они исходят, что является для них целью и массу других деталей.

CW: То есть, другими словами, критически важным является именно изначальный этап планирования построения системы безопасности?

Да, планирование — это, конечно, важно, но необходимо сразу же, во время того же планирования, вписать систему безопасности в ту инфраструктуру, которая существует. Знаете, я часто говорю, что безопасность — это скорее прилагательное, чем существительное, конечно,

не в смысле грамматическом, а по содержанию нашей деятельности. Вместо того чтобы строить сеть, а потом думать, как ее обезопасить, надо сразу строить безопасную сеть. И если, например, какие-то элементы вводятся, то надо сразу же их внедрять с системами безопасности, а не делать это потом или отдельно.

CW: В Украине мы наблюдаем сейчас постепенный переход от аналоговой телефонии к IP. Какие методы защиты вы предлагаете для IP-телефонии?

У нас есть очень мощные методы защиты, встроенные в сами устройства для IP-телефонии, например, кодирование голосовых видов информации. Вас невозможно подслушать, потому что ваш голос кодируется. На сегодняшний день мы делаем акцент на работе с сигнальными протоколами, потому что именно через них возникает возможность осуществить звонок, провести конференцию. Если хакеру удается проникнуть в этот сигнальный пакет и модифицировать его, то тогда в процессе разговора вас спокойно может прослушивать злоумышленник, внедрившийся в этот пакет. Для предупреждения таких вторжений у нас есть два фронта защиты. Первый — это использование файрволов, для того чтобы распознавать закодированный трафик, а второй — это использование системы IPS, для того чтобы на уровне сигналов распознавать и видеть что-либо модифицированное, измененное, необычное.

Для унифицированных коммуникаций у нас есть платформа ASA (Adaptive Security Appliances), и там есть виртуальная система предупреждения вторжений со всеми теми элементами защиты, о которых я говорил.

CW: Что можно выделить в методах обеспечения безопасности беспроводных сетей?

Здесь все то же самое, что и в проводных системах, — есть встроенные в устройства для беспроводной связи функции безопасности, которые сразу фиксируют начинающиеся атаки, также есть блокирующие элементы, чтобы не допустить определенный трафик «куда не надо». Сами по себе беспроводные сети не несут какой-либо небезопасности, опасность начинается там, где они соединяются с обычными проводными сетями.

Если кто-то входит в сеть в беспроводных системах, то только после того, как он пройдет виртуальную проверку, «докажет», что этого пользователя можно допустить дальше в глобальную сеть, только после этого он туда пройдет. В беспроводных сетях нет физических преград, например стен, и потому все так организовано.

Сеть необходимо рассматривать глобально, проводная она или беспроводная. Всегда надо обеспечивать взаимодействие между устройствами, из которых состоит эта сеть. Везде необходимы встроенные функции безопасности, у нас единый подход и для проводных, и для беспроводных сетей.

CW: Как обеспечивается безопасность при удаленной работе пользователей, например на дому, с подключением к сети компании?

О, это достаточно распространенная ситуация в настоящее время. Я ведь тоже, например, эти дни в Киеве работаю удаленно из отеля. В этом случае применяются механизмы аутентификации и авторизации, устанавливаются VPN между конечным устройством и VPN-шлюзом. Существует еще контроль доступа в сеть, который обеспечивает отслеживание и контроль в зависимости от того, как долго я не был в сети (может, я уезжал куда-то или еще по какой-то причине не появлялся). В этом поможет NAC (Network Admission Control) — система контроля доступа в сеть. И я уверен, что когда я в отеле соединяюсь с инфраструктурой Cisco, это также безопасно, как если я бы присоединялся к ней физически. Даже если я пройду через ряд небезопасных сетей, я не смогу подсоединится к сети Cisco, пока не буду авторизирован и подтвержден как имеющий право на то, что хочу получить.

> Наши решения по безопасности применимы абсолютно ко всем предприятиям разных профилей и размеров. Мы всегда используем этот принцип у себя в Cisco

CW: Cisco предлагает решения по безопасности для всех сегментов рынка?

Действительно, наши решения по безопасности применимы абсолютно ко всем предприятиям разных профилей и размеров. Мы всегда используем этот принцип у себя в Cisco. Разрабатывая технологию, мы делаем ее способной к масштабированию под разные профили и предприятия. Конечно, запросы по безопасности у маленького магазинчика и крупной корпорации будут разные, но это нам не мешает адаптировать наши технологии к их потребностям.

CW: Филипп, расскажите нам, пожалуйста, о том, как дальше будет развиваться стратегия безопасности Cisco?

Это, конечно же, развитие технологии TrustSec, что очень важно сейчас для нас, дальнейшее развитие репутационных сервисов, их применение во всей сфере сетей безопасности, а не только как антиспам.

Сегодня речь не идет о какой-либо новой линейке продуктов, мы уже имеем продукты, отвечающие любым потребностям. Мы постоянно дорабатываем и улучшаем существующие, развиваем возможности уже разработанных продуктов, для того чтобы они лучше взаимодействовали, «общались» между собой в сети, чтобы можно было обеспечить сохранность и защиту данных в работе этих устройств. Одним словом, речь идет о конвергенции — сближении, соединении разных элементов сети воедино, для того чтобы сеть была единым целым.

Я хочу сказать, что по мере разработки технических средств наша компания предлагает много новых инициатив. Полгода назад проводилась инициатива под названием threat control and containment (борьба и локализация угроз), цель которой — не допустить в сеть вредоносные программы, вирусы и т.д. Еще одна наша инициатива называется data leakage prevention — предотвращение утечки данных. Третью можно назвать compliance — соответствие регламентирующим положениям, политике. На такие подходы сейчас повышенный спрос везде, например, в Европе, США, да и даже на рынках, которые находятся на этапе становления, поэтому наша техническая сфера неразрывно связана с проводимыми нами инициативами.

И я хочу подчеркнуть следующее: многие полагают, что Cisco — это такой себе исключительно сетевой вендор. Будто они там кое-что делают по безопасности, но это, мол, не их основной профиль. Это совсем не так. Я скажу, что у нас 1800 инженеров и разработчиков в сфере решений безопасности, чем не может похвастаться ни одна компания в этой сфере. Да, у других компаний есть, например, крутые файрволы, системы предотвращения вторжения, защита конечных точек, но ни одна из этих компаний не представляет такой комплексный подход в плане систем защиты. И наш портфель систем защиты самый обширный и разнообразный среди всех остальных.

CW