Леонид Бараш

Безопасная сеть без границ

Бурный рост количества мобильных рабочих мест, виртуализация сервисов и проникновение облачных вычислений в корпоративные системы стирают как внешние, так и внутренние границы организаций.

Филипп Роггебанд: «Наиболее опасными сегодня являются атаки на базе бот-сетей»

Ответом на эти тенденции является новая концепция Cisco Systems «Безопасная сеть без границ», представленная на ежегодном форуме компании, состоявшемся 14 апреля в конференц-холле киевского «Президент Отеля». В нем приняли участие около 560 представителей украинского бизнеса и государственных организаций.

Пленарную часть открыл доклад менеджера по продуктам обеспечения безопасности Cisco на развивающихся рынках Филиппа Роггебанда (Philippe Roggeband), посвященный актуальным интернет-угрозам.

Сегодня пользователи должны иметь возможность доступа к корпоративным сетям с различных устройств и ОС. Все большее распространение получают совместная работа, Web 2.0 и социальные сети, и в совокупности это приводит к открытию инфраструктуры корпорации. К тому же и киберпреступники становятся все профессиональнее. Атаки выполняются с использованием социотехнологий, разрабатываются хитроумные методы и модели финансового мошенничества. Одним из главных объектов атак являются социальные сети.

Алексей Лукацкий: «Концепция предусматривает защиту от любых угроз, включая вирусы, спам, сетевые „черви" и бот-сети»

Cisco провела классификацию атак, использовав для этого аналог квадранта компании Gartner. В левой нижней четверти были помещены давно известные атаки, названные «собаками». К ним, к примеру, относятся DDoS, Instant Messaging и Phishing. В правой сосредоточились «дойные коровы» – скажем, письма с предложением что-нибудь купить и т. п. Все эти атаки не имеют особой перспективы – от них научились защищаться. А вот атаки на социальные сети (типа червя Koobface) и «восходящие звезды», использующие бот-сети новейшего поколения и Web exploits, имеют большой потенциал. Как же Cisco этому противодействует?

Сегодня методы защиты от атак основаны главным образом на двух элементах: сигнатуре и анализе поведения трафика. К этому Cisco добавила еще одну характеристику – репутацию сайта.

За последние несколько лет компании удалось создать аналитический центр безопасности Cisco, собирающий информацию о зараженных веб-узлах и компьютерах. Сегодня по всему миру имеется около 700 тыс. датчиков, которые собирают информацию для построения рейтинга репутации сайтов. Встроенное в продукты компании ПО позволяет проверить ее уровень и в случае низкого значения последнего – предотвратить загрузку элементов.

Кроме того, Cisco по-новому группирует свои продукты. В прошлом году на аналогичном мероприятии Cisco говорила о Self Defending Networks, о реактивном подходе к безопасности. Компания строит комплексы из трех элементов инфраструктуры. Два верхних поддерживают работу пользователей (многопотоковое видео, Веб, совместная работа, облачные вычисления, виртуализация). Cisco выпустила соответствующие продукты для единой вычислительной системы (Unified Computing System) и ЦОД. Однако и вне корпорации нужна надежная инфраструктура. Ее и обеспечивает базовый элемент, реализующий концепцию «Сети без границ» (Borderless Networks).

О сущности новой концепции Cisco рассказал в своем выступлении бизнес-консультант по безопасности Алексей Лукацкий. Она была разработана в рамках общей стратегии корпорации в сфере информационной безопасности, предусматривающей защиту клиентов от любых угроз, включая вирусы, спам, сетевые «черви» и бот-сети.

Концепция предполагает укрепление информационной безопасности предприятия в четырех критически важных областях: на уровне оконечных корпоративных устройств (мобильных или фиксированных), на границе Интернета, в ЦОД, а также с помощью политики, учитывающей особенности контента и местоположения.

Первыми работающими элементами этой архитектуры стали решения Cisco AnyConnect Secure Mobility и расширенное Cisco TrustSec, которые предоставляют компаниям функции идентификации и точного управления политиками, максимально повышая уровень информационной безопасности и защищенности.

На современные мобильные устройства невозможно установить весь комплекс средств защиты, обычно имеющийся на настольном ПК. Эти функции берет на себя AnyConnect Secure Mobility. Предусмотрено два сценария: либо трафик пользователя перенаправляется на корпоративный периметр, где он проверяется и фильтруется, либо проходит через облако ЦОД, разбросанных по всему миру.

Cisco рассматривает сеть как платформу для бизнеса. Такой подход, который сегодня транслировался в концепцию «Сеть без границ», позволяет компании сохранять позиции в этом сегменте.

Отдельный бизнес-поток конференции был посвящен интеграции систем безопасности с ИТ- и бизнес-процессами организаций. На нем поднимались вопросы измерения эффективности таких систем, их соответствия стандартам и перспектив виртуализированной безопасности.

Были также рассмотрены практические примеры построения систем защиты с участием представителей системных интеграторов и компаний-заказчиков.

• Киберпреступность – уже бизнес

В кратком интервью Филипп Роггебанд ответил на ряд актуальных вопросов в области инфомационной безопасности.

- **Какие типы атак сегодня наиболее распространены и опасны для компаний?**

  Я думаю, самые опасные атаки те, о которых вы не подозреваете. Атаки, блокирующие сеть (DDoS), кажутся серьезными. Но о них тут же узнаешь, а значит, можешь что-то предпринять. А вот куда страшнее, особенно для корпораций, так называемые бот-сети. Множество ПК сотрудников может быть заражено и объединено в бот-сеть, которая участвует в атаке на чужие ресурсы. В конечном счете ответственность могут возложить на компанию. Вот это, пожалуй, самое опасное – угрозы, о которых мы не узнаем вовремя.

- **Есть ли разница в структуре атак на зрелых и развивающихся рынках?**

  Есть, и она обусловлена рядом факторов. Они могут быть связаны, например, с пропускной способностью сетей, при этом внутри стран с развивающейся экономикой могут быть большие различия. В эту группу попадают и Украина с ее достаточно развитой инфраструктурой связи, массовым доступом к Интернету, и Камерун, где он в основном осуществляется через телефонную сеть по коммутируемому каналу со скоростью 24 Кб/с. Ну и хакер себя ведет соответственно: если есть скоростной доступ, он может организовать массированную атаку вслепую в надежде, что в кого-то попадет. Если сети с малой пропускной способностью, тогда атаки становятся более изощренными, нацеленными на конкретный объект.

- **Каковы особенности современной киберпреступности?**

  Прежде всего методы стали более профессиональными, а киберпреступность – более организованной. Нанимают лучшие умы за большие деньги, а они там действительно немалые. И главный стимул деятельности кибепреступников изменился радикально: если раньше это была погоня за славой, то теперь все упирается в деньги.

  Если говорить о профессионализме, то качество вредоносного ПО чрезвычайно повысилось. Например, создано так называемое самомутирующее вредоносное ПО. Или возьмем программы для зомбирования, на основе которых строятся бот-сети, – они используют незагруженные циклы работы ЦП, и вы не видите, чтобы что-то замедлялось.

  Ну и наконец, вопрос уже не технического характера. Помимо просто загрузки вредоносного ПО на ПК, организованная киберпреступность стала предлагать услуги. Скажем, заключается договор на техническое сопровождение, и если у вас это вредоносное ПО вдруг перестало работать, присылается заплатка или новая версия. У этих, так сказать, фирм появляются свои центры обработки вызовов. Их модель бизнеса заимствована из других отраслей экономики, т. е. кто-то создает, кто-то развертывает, а кто-то использует, и это три разных лица.

- **В чем должна заключаться стратегия информационной безопасности компаний? Каковы ее организационные и технические аспекты?**

  В деятельности практически всех компаний есть какие-то общие методы – например, решать проблемы по мере их поступления. Они реагируют на то, что я называю угрозой месяца. Находят наиболее распространенную угрозу, устанавливают какой-то кусочек программы, позволяющей ее подавить, и успокаиваются. В итоге получается масса каких-то кусочков, которые не объединяются в комплекс.

  Мы говорим, что стратегия должна включать следующие английские слова на букву «P». Policy – должен быть установлен свод правил безопасности, Protection – нужно решить, что и от чего мы защищаем, и обязательно определять некое разумное соотношение риска и затрат. Третье «P» – это Processes. Что это означает? Вы установили своды правил, а теперь надо обеспечить их реализацию. Какие кому давать права доступа, к каким ресурсам, что делать при нештатной ситуации, короче, как перевести политику на язык действий? И следующая буква «P» – People. Главное – это защита от «дурака» с добрыми намерениями. У вас на фирме могут работать люди, которые просто не отдают себе отчета в своих действиях. Посещают какие-то узлы в Интернете, нажимают кнопку «загрузить», не понимая, какие риски с этим сопряжены. Здесь самое лучшее – придумать план просветительских мероприятий, чтобы сотрудники понимали, насколько рискованно то, что они делают.

  Последнее – это Products – продукты, применяемые для информационной безопасности. Они не должны использоваться изолированно друг от друга. Мы говорим о некой сложной архитектуре и комплексе, которые обеспечивают исполнение процессов, в свою очередь, реализующих свод правил политики таким образом, что людей удерживают от необдуманных действий.

- **Сегодня некоторые средства безопасности предлагаются как сервис. Каковы достоинства и недостатки этого метода по сравнению с использованием собственной системы?**

  Тут следует начать с того, что многие из наших продуктов ориентированы на, так сказать, вычистку информационного наполнения. Например, контролировать электронную почту так, чтобы вирусы или спам вообще не доходили до абонента. Или же то, что у нас в инфраструктуре называется Managed services, т. е. службы, переданные на подряды оператору. Оборудование может физически находиться на объекте как потребителя, так и оператора, но в любом случае все управление им осуществляет оператор. Сегодня в вычислительном облаке нет ни межсетевого экрана, ни средств предотвращения вторжений, поэтому нужно прибегать к подрядной эксплуатации. Это, во-первых, дешевле для заказчика, во-вторых, снимается вопрос администрирования и обучения сотрудников. Есть здесь и недостаток, потому что не все средства безопасности реализованы на этой базе – правда, их перечень будет постоянно расширяться. Ну и еще один недостаток (а может быть, и достоинство) – это то, что к оператору, управляющему всеми этими ресурсами, нужен очень высокий уровень доверия.