ВСЕОБЪЕМЛЮЩЕМУ ИНТЕРНЕТУ – ВСЕОБЪЕМЛЮЩУЮ БЕЗОПАСНОСТЬ:

новый подход компании Cisco

В этом году центральной темой конференции Cisco Connect стал Всеобъемлющий Интернет (Internet of Everything, IoE). Чем больше вещей мы подключаем к Интернету, тем больше возможностей для бизнеса мы обнаруживаем. Согласно прогнозам, на следующей стадии развития всемирная паутина объединит не только людей и различные устройства, но данные, процессы – вообще все. Это вызовет взрывообразный рост всей ИКТ-индустрии. По прогнозу Cisco, к 2020 году к Интернету будут подключены более 50 миллиардов устройств, что откроет огромные перспективы для технологических компаний. Однако чем больше подключений к Интернету, тем острее становится проблема обеспечения их безопасной работы. Готова ли корпорация Cisco ответить на столь серьезные вызовы? Об этом в эксклюзивном интервью нам рассказал Скотт Харрелл (Scott Harrell), вице-президент подразделения Cisco по разработке решений для информационной безопасности.

Скотт, в чем особенность и сложность современного момента с точки зрения информационной безопасности?

Сейчас происходит немало самых разных событий. Развитие ИКТ-отрасли определяется распространением Всеобъемлющего Интернета (Internet of Everything), постоянно растущим числом пользовательских устройств, облачными вычислениями. Вместе с ними возникают более сложные угрозы, противостоять которым становится все труднее. Cisco стремится защитить компании и организации, помогая им справиться с новыми вызовами с помощью лучших в отрасли решений по информационной безопасности (ИБ).

Очень часто система информационной безопасности отражает нападение, однако в ряде случаев защите удается лишь просигнализировать о том, что вторжение состоялось. В будущем таких вторжений будет все больше. Угрозы непрерывно видоизменяются. Хакеры становятся все более изобретательными, меняют средства атак, делая их все более специализированными, заточенными под конкретную

ситуацию. Чтобы бороться с такими атаками, требуются усовершенствованные инструменты, непрерывно контролирующие ситуацию. Метод противодействия атаке только в тот момент, когда она происходит, больше не приносит результатов.

Нужно отдавать отчет в том, что некоторые из атак злоумышленников окажутся успешными, поэтому системы обеспечения информационной безопасности должны справляться не только с предотвращением вторжения, но и с последствиями атаки. Надо разработать средства борьбы, которые позволят нейтрализовать злоумышленников после их проникновения в систему. Надо оценить масштаб ущерба от успешного нападения и понять, как минимизировать неприятные последствия. Все это существенно меняет стратегию обеспечения информационной безопасности: от стремления предотвратить вторжение необходимо перейти к борьбе с успешно реализованными атаками. Конечно, это не значит, что не нужно предотвращать вторжения – от работы в этом направлении никто не отказывается, и Cisco располагает передовыми решениями для борьбы с нападениями.

Какие решения предлагает компания Cisco, чтобы защитить своих клиентов?

Мы фокусируемся на системах обеспечения безопасности сети и контента. Cisco стремится к тому, чтобы защитить каждое устройство пользователя, подключенное к сети, всю его информацию. И неважно, идет речь о физических пользовательских устройствах или об облачных сервисах. Обеспечивая защиту устройств конечных пользователей, информационную безопасность любых соединений, Cisco создает инструменты для борьбы с вредоносным ПО.

Всеобъемлющий Интернет – это десятки миллиардов устройств, подключенных к сети. Как Cisco собирается их защищать?

С наступлением эры Всеобъемлющего Интернета площадь, которую приходится защищать, значительно увеличивается. Естественно, это повышает степень сложности механизмов обеспечения ИБ. Новые терминальные устройства (в том числе различные сенсоры и пр.) будут все более уязвимы для новых изощренных атак. Новые инструменты для обеспечения ИБ должны быть прозрачны и понятны – пользователь должен видеть, что происходит, и принимать соответствующие меры.

Новые системы обеспечения ИБ позволяют понять, какие угрозы наиболее опасны для компании и могут нанести ей максимальный вред. Далеко не всегда сотрудники отделов ИБ могут справиться со столь изощренными атаками самостоятельно, поэтому система помогает им это сделать автоматически. Обладая полным знанием о работе сети, технологии защиты делают работу ИБ-служб более эффективной.

Есть ли на нашей планете наиболее опасные и наиболее безопасные места в плане киберугроз?

Если говорить коротко, то нет. В любой точке мира есть свои ценности, привлекающие злоумышленников. К сожалению, всегда и везде мошенники стараются присвоить то, что им не принадлежит. Выбор жертвы напрямую не зависит от размеров компаний, от секторов экономики.

Недавно корпорация Cisco выпустила ежегодный отчет по информационной безопасности, где представлен анализ степени защищенности множества компаний. В ходе исследования были рассмотрены их сети, и в 100% случаев – вне зависимости от размера компании,

от ее положения на глобусе – в корпоративных сетях мы обнаружили вредоносное ПО. Это открытие стало настоящим сюрпризом не только для самих компаний, но и для Cisco. Предполагалось, что отдельные системы все-таки должны быть совершенно чистыми, но на самом деле сегодня мы видим лишь разную степень загрязненности информационных систем.

Конечно, компании, работающие в финансовой сфере, более привлекательны для злоумышленников по сравнению с другими организациями. Самые серьезные атаки происходят там, где больше материальных ценностей. Тем не менее у любой организации есть что-то притягательное для хакеров.

Кроме собственных разработок компания Cisco часто приобретает другие компании, имеющие необходимые разработки. Как обстоит дело в области информационной безопасности?

Одно из последних приобретений Cisco – компания Sourcefire, которая была приобретена летом 2013 года. Ее основал в 2001 году Марти Рёш (Marty Roesch), в 1998 году создавший свободно распространяемую сетевую систему предотвращения и обнаружения вторжений Snort. Этот продукт с открытым кодом фактически стал стандартом для систем предупреждения и обнаружения вторжений. На его основе компания Sourcefire создала ряд успешных коммерческих продуктов. За 12 лет лидерства на рынке ИБ Sourcefire удалось создать уникальный коллектив специалистов в области безопасности для совместного строительства лучшей в отрасли системы предотвращения вторжений. Кроме того, в составе Sourcefire работает группа по исследованию уязвимостей, которая объединяет ведущих экспертов, непрерывно исследующих и оценивающих новейшие тенденции хакерской активности, попытки вторжений, вредоносные коды и уязвимости.

Портфель интеллектуальных решений Sourcefire для обеспечения кибербезопасности включает такие продукты, как система предотвращения вторжений нового поколения (NGIPS), межсетевой экран (NGFW), усовершенствованная защита от вредоносных программ (AMP). Решения Sourcefire обеспечивают эффективную, высокоавтоматизированную информационную безопасность, непрерывное изучение и распознавание угроз, а также защиту от них.

Технологии Sourcefire работают в режиме реального времени, обеспечивая прозрачность "расширенной сети", которая включает в себя виртуальные машины, мобильные устройства и оконечные терминалы. Решения Sourcefire обеспечивают непрерывную защиту от угроз и ликвидацию последствий сетевых атак с учетом всей имеющейся информации.

Модель Sourcefire для ПО с открытым кодом усиливает и ускоряет деятельность Cisco, направленную на формирование мощной системы партнеров в области информационной безопасности, способных в реальном времени предоставлять заказчикам интеллектуальные новаторские решения, интегрированные с нашими технологиями и платформами.

Используя достижения Sourcefire, Cisco меньше чем за год разработала решение Advanced Malware Protection (AMP), одну из лучших систем обнаружения угроз инфобезопасности. Этот элемент внедрен во все ИБ-продукты Cisco посредством обновления ПО. Сегодня компания делает следующий шаг для дальнейшего совершенствования своих продуктов, внедряя сервисы Sourcefire Firepower, которые накладываются на межсетевой экран Cisco опять-таки через обновление ПО.

Чтобы использовать новые возможности по предотвращению угроз и сделать эффективный защитный "зонтик", прикрывающий все входы и выходы из сети, система обеспечения информационной безопасности должна быть всеобъемлющей.

Как вы относитесь к тому, что молодежь все чаще использует для работы свои собственные устройства? Это ведь усложняет работу систем обеспечения безопасности?

Запретами ничего не добьешься. Мы видим, как молодежь находит пути обхода запретов работодателей. Надо просто более пристально следить за всеми пользователями, убеждая их в том, чтобы они приняли правильное решение.

Недавно компания Cisco провела внутренний анализ и обнаружила, что многие сотрудники используют облачные системы для хранения своих данных. Вместо того чтобы запрещать эту практику, Cisco приобрела компанию, централизованно предлагающую услуги хранения данных для всех работников. Надо не ограничивать сотрудников, а предоставлять им возможность работать наиболее безопасным образом. ■

Со С.Харреллом беседовал А.Семенов