Обеспечение безопасности корпоративной сети в среде Web 2.0 и при использовании социальных сетей

Технология Web 2.0 и социальные сети сделали интерактивность реальностью и изменили способ использования веб-ресурсов. Кроме того, эти технологии навсегда изменили ландшафт безопасности как для отдельных пользователей, так и для предприятия в целом. Ниже представлен обзор некоторых общих угроз и проблем, характерных для технологии Web 2.0, а также решения, позволяющие с ними справиться.

Вредоносные программы, угрозы безопасности и мошеннические действия

Пользователи социальных сетей полагают, что можно доверять людям, с которыми они связаны. Если «друг» из чьей-то сети размещает URL-адрес, по которому можно прочитать какую-то новость, то остальные «друзья» считают, что можно безопасно перейти по указанной ссылке. В данном случае они не проявляют такой осторожности, как если бы они получили эту ссылку или сообщение от незнакомого человека по электронной почте. Такое отсутствие осмотрительности не всегда безопасно для предприятия: сотрудники могут невольно распространять вредоносные программы по корпоративной сети во время общения в социальных сетях.

Одна из популярных техник, которой пользуются киберпреступники, состоит в том, что пользователям предлагают нажать кнопку Like на определенной странице Facebook, а взамен обещают, что пользователь увидит шокирующие фотографии или прочитает потрясающие новости. Как только пользователь нажмет кнопку Like на нужной странице Facebook, создатель этой страницы может по электронной почте отправить пользователю предложение перейти по другим ссылкам (которые могут вести на сайты с вредоносными программами), а также может просматривать личные данные пользователя[1]. В первом квартале 2011 г. наблюдался значительный рост количества злоумышленных действий, основанных на использовании кнопки Like: от 0,54% всех случаев распространения вредоносных программных средств в Интернете в январе 2011 г. до 6% в марте 2011 г.[2].

Другая тактика состоит в отправке фальсифицированных запросов о добавлении в друзья, зачастую снабженных привлекательным портретом. Если получатель захочет посмотреть в Facebook страничку предполагаемого человека, то, как правило, он увидит там единственный пост, который содержит ссылку; при переходе по этой ссылке будут совершаться какие-нибудь мошеннические действия[3].

Хотя эксперты Cisco в области безопасности прогнозируют, что запуск эксплойтов через социальные сети с течением времени будет становиться менее популярным у современных киберпреступников[4] — главным образом, потому что это требует значительных ресурсов—огромная популярность социальных сетей означает, что вероятность запуска по этим каналам кампаний, направленных против пользователей, будет оставаться достаточно высокой. Таким образом, предприятия должны учитывать те риски, с которыми они могут столкнуться, если у сотрудников будет неограниченный доступ к средствам общения в социальных сетях.

Соответствие нормативным требованиям и потеря данных

Никогда раньше не было так легко утратить контроль за корпоративными данными. Больше уже нельзя сделать так, чтобы информация не выходила за пределы сети—в настоящее время обычная электронная почта, системы мгновенных сообщений и социальные сети дают сотрудникам компании возможности общаться с людьми, не имеющими отношения к данной организации. Этот риск еще больше увеличивается из-за возрастания количества удаленно работающих и мобильных сотрудников, которым необходим доступ к данным, хотя они находятся за пределами безопасной сети.

К сожалению, из-за этого пользователи могут легко распространять информацию, которая не предназначена для глаз посторонних людей — например, путем прикрепления документов к сообщениям в сети Facebook или создания коротких сообщений (твитов) в сети Twitter о важных корпоративных разработках.

---

[1] *Cisco 2010 Annual Security Report (Ежегодный отчет Cisco по безопасности за 2010 г.):* http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf.
[2] *Cisco 1Q11 Global Threat Report (Отчет Cisco о распространении глобальных угроз в 1-ом квартале 2011 г.):* http://www.cisco.com/web/about/security/intelligence/reports/cisco_global_threat_report_1Q2011.pdf.
[3] Там же.
[4] *Cisco 2011 Annual Security Report (Ежегодный отчет Cisco по безопасности за 2010 г.):* http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

Сотрудники финансовых служб могут размещать информацию, которая будет содержаться в будущих сообщениях о размере прибыли. Сотрудники из сферы высоких технологий могут высказывать предположения о намечаемых приобретениях компании.

Как только эта информация попадает в Интернет, ее уже нельзя изъять оттуда, в отличие от письма, отправленного по электронной почте. Если кто-то прочитал информацию, переслал ее кому-то еще и разместил на своей страничке, она уже навсегда останется в Интернете.

Неформальный характер общения в социальных сетях также заставляет пользователей в значительной степени забывать об осторожности при обмене мнениями, в отличие от беседы или даже от использования других электронных сред коммуникации, например электронной почты. Известная сотруднику конфиденциальная информация может незаметно стать общедоступной благодаря социальным сетям. Брошенное мимоходом пренебрежительное замечание о каком-то сотруднике, коллеге или клиенте может очень легко оказаться достоянием намного более обширной аудитории, чем это предполагалось изначально.

Для виновника инцидента это чревато самыми разными последствиями. Один из крайних вариантов – финансовые потери для организации в результате ухудшения репутации бренда и утрате доверия к нему. Более того, в организациях, которые при обработке данных руководствуются подходом Web-2.0, могут не соблюдаться правительственные и отраслевые нормативные требования о наличии эффективных систем и процессов контроля данных. Это может повлечь за собой наложение крупного штрафа регулирующим органом за то, что не обеспечен достаточный контроль или не уделяется должное внимание управлению конфиденциальными данными.

Вероятно, наихудший сценарий связан с возможными юридическими последствиями для организации. В некоторых случаях, когда сотрудники компании делали неосторожные замечания о своей организации в социальных сетях, это приводило к судебным разбирательствам в связи с создаваемыми помехами, клеветой, нарушением конфиденциальности и прав собственности на контент. Однако все более распространенным также становится прекращение в связи с неправомерностью судебных процессов по поводу «неправильного использования» социальных сетей. В самом деле, Национальное управление по вопросам трудовых отношений (США) несколько раз рассматривало использование социальных сетей сотрудниками и политику работодателя в отношении использования социальных сетей, и в ряде случаев было вынесено решение в пользу сотрудников[5].

Сохранение производительности труда в компании

Еще одна проблема, вызывающая законное беспокойство компаний, связана с потенциальным снижением производительности труда сотрудников из-за использования Web 2.0 и технологии социальных сетей. (Хотя следует отметить, что многие работодатели в настоящее время наоборот обращаются к социальным сетям с противоположной целью: приглашать на работу специалистов и измерять их продуктивность.)

В социальных сетях пользователям предлагается множество увлекательных способов взаимодействия, например с помощью игр и викторин, которые отвлекают внимание работников от их непосредственных обязанностей. Поскольку в Facebook разрешено было использовать приложения сторонних разработчиков еще несколько лет назад, то с тех пор было разработано несколько сот тысяч приложений, которые быстро стали частью нашей поп-культуры. (Приведем лишь два примера игр: Words With Friends и Farmville, разработанные компанией Zynga.) Пользователи сети Facebook ежедневно устанавливают более 20 миллионов приложений[6].

Для компаний проблема состоит в том, чтобы найти способ сохранения производительности труда персонала путем ограничения доступа к приложениям в социальных сетях, не ограничивая при этом доступ к бизнес-преимуществам, которые предоставляют социальные сети.

[5] Acting General Counsel releases report on social media cases (Отчет, выпущенный действующим генеральным юрисконсультом об использовании социальных сетей), выпуск Департамента по связям с общественностью Национального управления по вопросам трудовых отношений, 18 августа 2011 г.: https://www.nlrb.gov/news/acting-general-counsel-releases-report-social-media-cases.

[6] Facebook Statistics, Stats and Facts for 2011 (Статистика Facebook: положение и факты, 2011 г.), Digital Buzz Blog, 18 января 2011 г.: http://www.digitalbuzzblog.com/facebookstatistics-stats-facts-2011/.

Противодействие угрозам со стороны Web 2.0 с помощью средств управления использованием веб-ресурсов

Изменение отношения к тому, где и каким образом выполняется работа, а также потенциальные преимущества социальных сетей с точки зрения повышения продуктивности работников все больше затрудняют для организаций возможность сохранения позиции «все или ничего» применительно к контролю доступа персонала к социальным сетям. Веб-сайты социальных сетей стали прибежищем для многих видов человеческой деятельности как в рабочее время, так и в часы досуга. Пользователи общаются с друзьями и коллегами, вместе создают и используют календари событий, распространяют новости компаний, отвечают на вопросы клиентов и многое другое.

Желание общаться и развивать бизнес через социальные сети только увеличивается по мере того, как люди все больше времени проводят за работой вне привычной офисной среды и корпоративной сети. Действительно, результаты исследования Cisco, представленные в отчете о *глобальном развитии сетевых технологий* в 2011 г., говорят о том, что молодое поколение работников и студенты колледжей в разных странах мира склонны считать, что необязательно ходить на работу в офис каждый день (хотя они признают, что у работодателей может быть иное мнение на этот счет).

Ясно, что традиционные средства контроля за использованием веб-ресурсов больше не могут помочь предприятиям в эффективном управлении безопасностью, производительностью труда, а также в решении проблем управления данными, чтобы не допустить их потерь, и проблем соответствия нормативным требованиям. Попытки реализовать даже хорошо продуманные и приемлемые политики использования только лишь на основе фильтрации URL-адресов – это не просто устаревший прием, но и неэффективный. Несмотря на то, что фильтрация URL-адресов все еще считается разумным первым шагом для нейтрализации рисков, связанных с сайтами социальных сетей, такое решение не является полным. Если использовать только фильтрацию по категориям, то это также не может предотвратить заражения компьютеров пользователей вредоносными программами.

Поскольку современные веб-сайты стали намного более динамичными, существенно более эффективным является сканирование в режиме реального времени, при котором сразу же проверяется весь контент, имеющий данный URL-адрес. Одно посещение единственной веб-страницы может привести к предоставлению контента из нескольких доменов, расположенных в разных местах земного шара. Кроме того, приложения для социальных сетей никоим образом нельзя рассматривать как единое целое. Они могут состоять из сотен микроприложений, причем некоторые законно используются для деятельности компании, а другие серьезно подрывают производительность труда персонала. В результате компаниям необходимы такие рычаги управления социальными сетями, которые бы обеспечивали доступ к определенным компонентам приложения, но блокировали бы другие компоненты. Поскольку разные подразделения компании имеют разные потребности, существенное значение приобретает возможность изменять права доступа в зависимости от функциональных ролей.

Более логичным и реалистичным подходом в среде Web 2.0 будут решения, способные в динамическом режиме идентифицировать веб-содержимое и приложения, а также применять соответствующую политику даже для приложений, встроенных в веб-сайт. Ниже приводятся типы средств управления, позволяющие эффективно проводить политику безопасности, помогающие повышать производительность труда и обеспечивать соответствие нормативным требованиям, а также снижающие риск заражения вредоносными программами и риск распространения других видов угроз безопасности.

Прозрачность и управление веб-приложениями

Чтобы обеспечить реализацию приемлемых политик использования и безопасности для сайтов Web 2.0, которые содержат встроенные приложения, требуемое эффективное решение для обеспечения безопасности должно уметь точно идентифицировать и контролировать отдельные приложения с использованием сигнатур приложений или других методов. Детальный контроль приобретает решающее значение, если учесть объем всех действий, которые можно осуществить в сети Facebook – например, разместить контент, нажать кнопку Like возле статуса какого-либо пользователя, отправить письмо по электронной почте и поучаствовать в чате. При принятии решений корпоративными ИТ-структурами в области управления доступом необходимо также идентифицировать и учитывать микроприложения, которые используются внутри более крупного приложения, например FarmVille в сети Facebook. Чтобы не отставать от перемен, происходящих в Интернете, и эффективно обеспечивать управление и безопасность, необходимо также в динамическом режиме обновлять сигнатуры.

Средства динамического управления использованием веб-ресурсов

Бурный рост количества создаваемых динамических веб-страниц (страниц, которые обслуживаются базами данных), создаваемого пользователями контента и веб-страниц, защищенных паролями, а также популярность социальных сетей привели к созданию миллиардов страниц веб-контента. К 2015 г. примерно 95% сайтов в Интернете будет невозможно категорировать с помощью списков фильтрации URL-адресов.

Это привело к необходимости разработать другой подход к применению средств управления использованием веб-ресурсов: выполнение контент-анализа ранее неизвестных сайтов в режиме реального времени.

Средства управления зашифрованным веб-трафиком

Для контроля данных, которые входят в корпоративную сеть или выходят из нее, совершенно необходимо, чтобы любое решение могло обеспечивать дешифрование SSL-пакетов. Без поддержки SSL-дешифрования в ИТ-структуре остается большое «слепое пятно», в котором заданные политики нельзя реализовать.

Эффективное решение для обеспечения безопасности веб-трафика должно быть таким, чтобы менеджеры по безопасности могли детально определять средства контроля функциональности этого типа. Например, из дешифрования следует исключить сайты банков, в которых открыты счета сотрудников. Однако следует немедленно дешифровывать данные сайта фишинга, который замаскирован под легальную персональную страницу клиента на сайте банка.

Средства контроля использования Интернета с учетом конкретного пользователя

Предприятия должны использовать такие политики фильтрации веб-трафика, которые обеспечивают контроль на уровне пользователя или группы. Такой подход наиболее успешен, если разработчик может легко объединить решение с аутентификацией в службе каталогов, например Microsoft Active Directory.

Средства контроля использования Интернета с учетом времени суток

Решения по фильтрации Интернет-трафика также должны быть рассчитаны на использование разных политик в разное время суток. Например, политика безопасности организации может допускать обращение к обычным сайтам социальных сетей по окончании рабочего времени.

Защита от динамических вредоносных программных средств

Традиционные решения с использованием прокси-серверов и фильтрации веб-трафика не обеспечивают адекватной защиты против загружаемого с веб-ресурсов вредоносного кода, эксплуатирующего уязвимости (эксплойтов). Для эффективной защиты необходимо сочетание технологии упреждающей оценки диапазона веб-репутации со сканированием контента на наличие вредоносных программ, вирусов и программ-шпионов с использованием нескольких наборов сигнатур от разных поставщиков, причем так, чтобы это не нарушало работу пользователя.

Пообъектная фильтрация для обеспечения безопасности

Отличительной чертой сайтов Web 2.0 является то, что они содержат множество объектов, поступающих из разнообразных источников. Например, популярный блог BoingBoing.net содержит более 162 различных HTTP-объектов, поступивших более чем из 30 различных доменов. В средах такого типа у хакеров есть экспоненциально растущее количество точек входа в систему, откуда можно запустить эксплойты.

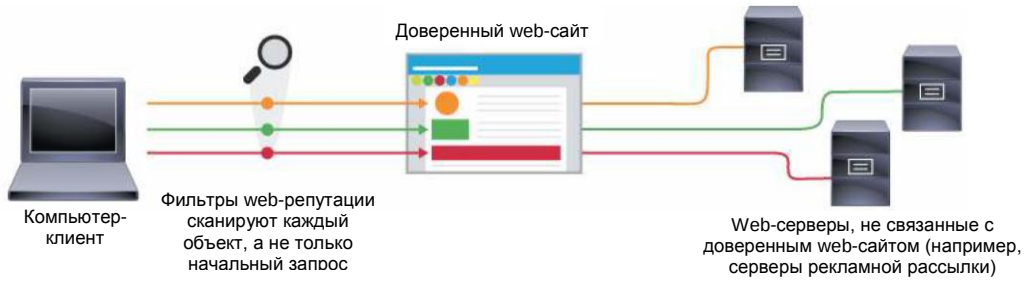
В качестве примера приведем относительно недавний случай мошеннических действий, которые были организованы международной преступной группировкой и в результате которых пользователи потеряли более 2 миллионов долларов США. Киберпреступники создали фальшивое рекламное агентство и разместили рекламу гостиничной сети на веб-сайте городской газеты Миннеаполиса. Сразу после размещения рекламы они изменили компьютерный код рекламы таким образом, что когда пользователь нажимал рекламное объявление, его компьютер заражался вредоносной программой[7].

Для защиты предприятий от угроз этого типа разработчик шлюза может целиком заблокировать веб-сайт до тех пор, пока веб-мастер не уберет с сайта вредоносные программные средства. Однако если такой веб-сайт полезен для бизнеса, то блокировка доступа к нему приведет лишь к многочисленным звонкам в службу поддержки пользователей и увеличению нагрузки на ИТ-департамент.

Второй подход состоит в пообъектной фильтрации веб-сайтов (Рис. 1). При таком подходе на веб-сайте будут заблокированы только вредоносные программные средства. Например, в блоге с фальшивой рекламой будет заблокировано лишь вредоносное рекламное объявление. Для реализации такого подхода необходимо соответствующее решение разработчика на основе архитектуры прокси-сервера.

[7] FBI Busts International ‘Scareware’ Rings (ФБР разгоняет международные группы киберпреступников), Chloe Albanesius, PCMag.com, 23 июня 2011 г.: http://www.pcmag.com/article2/0,2817,2387467,00.asp.

Рис. 1. Фильтрация каждого объекта с помощью решения Cisco Web Security



Средства контроля утечки данных

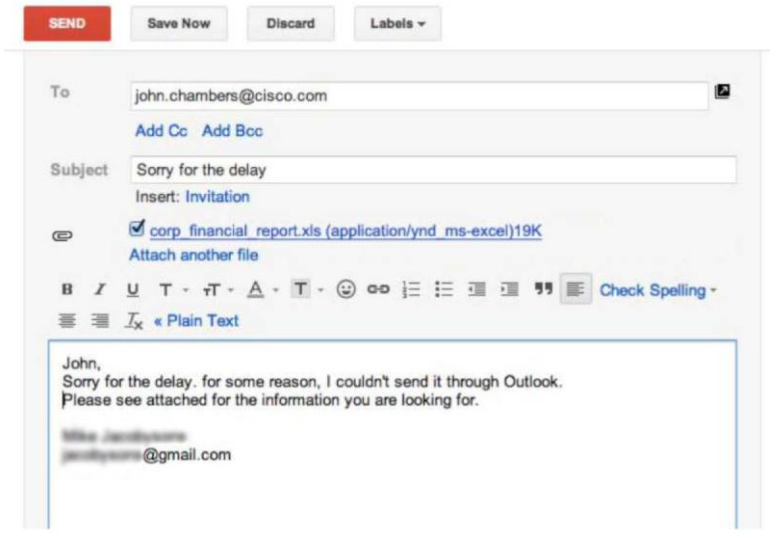
Поскольку Интернет предусматривает двусторонний обмен данными, то и контроль веб-содержимого также должен осуществляться в двух направлениях. Политики и анализ контента должны учитывать всю информацию, выходящую из организации, чтобы предотвратить утечку важных данных.

Обычно корпоративные ИТ-департаменты имеют значительные специально выделенные ресурсы для обеспечения безопасности исходящих сообщений, отправляемых через традиционные корпоративные системы, например Lotus Notes и Microsoft Exchange. Однако организации, в которых разрешен доступ к таким почтовым сервисам как Gmail или Hotmail должны использовать дополнительные средства безопасности.

Конечные пользователи, имеющие доступ к сайтам веб-почты потенциально могут создавать дополнительные бреши в системе безопасности, через которые важная информация может утекать из организации. Например, персонал может использовать веб-почту для общения с клиентами или поставщиками, если возникла какая-то проблема с корпоративной почтовой системой. Или сотрудники могут использовать веб-почту для передачи важной информации из компании ее конкуренту.

Разработчики и поставщики решений, обеспечивающих веб-безопасность, должны предусмотреть указанный тип обмена информацией без непосредственной блокировки сервисов веб-почты (Рис. 2).

Рис. 2. Типичный сервис веб-почты



Решения Cisco

Традиционные средства контроля за использованием веб-ресурсов больше не могут помочь предприятиям в эффективном управлении безопасностью, производительностью труда, а также в решении проблем управления данными, чтобы не допустить их потерь, и проблем соответствия нормативным требованиям. Современным организациям нужны такие решения, которые обеспечат их сотрудникам в любое время и из любого места доступ к необходимым им сервисам Web 2.0. При этом предприятие должно быть защищено от угроз безопасности, которые могут распространяться по таким каналам доступа. Интеллектуальные решения обеспечивают управление динамическим контентом, что позволяет безопасно использовать подход Web 2.0 внутри предприятия, если задать соответствующие параметры безопасности.

Для обеспечения безопасности в современных сетях необходима также прозрачность и контроль сверх того, что предполагает традиционный подход на основе IP-адреса и номера порта. Быстрое распространение веб-приложений, а также способность таких приложений Web 2.0 как Skype переходить на другой протокол означает, что порты и протоколы больше не являются хорошими идентификаторами для приложений. Межсетевые экраны следующего поколения решают эту проблему, обеспечивая прозрачность и контроль в контексте приложения. Однако недостаточно просто классифицировать приложение: как указывалось в этой статье выше, применяя и вводя в действие политику безопасности, необходимо также учитывать микроприложения.

Не существует единого универсального подхода к обеспечению безопасности, и не существует единого способа применения средств и технологий Web 2.0 в организациях, поскольку это зависит от потребностей бизнеса, структуры, персонала и культуры. Поэтому у предприятий должен быть выбор. Cisco предлагает целый ряд инновационных решений, реализованных как физически (на территории клиента), так и в виде облачных сервисов, которые предназначены для того, чтобы обеспечить ИТ-специалистам на предприятии прозрачность и контроль за работой приложений с целью исключения возможных угроз со стороны Web 2.0 и социальных сетей.

С более подробной информацией о решениях Cisco для обеспечения безопасности можно ознакомиться по адресу http://www.cisco.com/go/websecurity.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Компания Cisco имеет более 200 офисов по всему миру. Адреса, номера телефонов и факсов приведены на web-сайте компании Cisco по адресу www.cisco.com/go/offices.