Защита от угроз Web2.0

Значение термина Web 2.0 до сих пор является предметом споров. Оригинальная концепция Web 2.0 приписана Tim O'Reilly и компании MediaLive International и зафиксирована в "Web 2.0 Article" в 2005 году. В общей вольной трактовке его можно представить как термин Интернет-культуры, означающий эволюцию WWW, вызванную развитием опыта ее пользователей и переходом на активный контент с соответствующим смещением баланса функциональных возможностей и мощностей от Web-серверов к Web-клиентам. Такие технологии, как Weblogs, wikis, RSS-feeds, WEB APIs, сервисы класса eBay, Gmail и тп, плюс задействованные в WWW семейства новых форматов и языков, говорят сами за себя.
Повсеместное использование активного контента и усложнение приложений практически вызвали взрыв распространения вредоносного программного обеспечения с одновременным снижением скорости его обнаружения и, соответственно, ростом числа успешных атак. CERT и x-Force отмечают их 30-40% ежегодный рост, констатируя, что 80% проблем обусловлены уязвимостью Web-приложений. При этом активно и эффективно автоматизируются как средства обнаружения и использования их уязвимостей (например, проект Metasploit), так и средства их автоматического тиражирования на открытых ресурсах типа форумов, гостевых книг, блогов и тп (например Xrumer). Результаты на лицо: ежедневно фиксируется до 400 тысяч новых зомби. Отчет Gartner Group указывает на современные Web-шлюзы как на самую уязвимую брешь в сегодняшних корпоративных сетях, тк многие из них используют устаревшие технологии, пригодные лишь для предыдущего поколения WWW - Web1.0.

Компания Secure Computing Corporation (SCC), один из известных профессиональных участников рынка сетевой безопасности, с начала этого года активно продвигает свою инициативу против угроз безопасности Web2.0 (**S**ecure **W**eb2.0 **A**nti **T**hreat initiative). Основная ее цель – помощь в защите корпоративных информационных ресурсов от угроз, обусловленных средой Web 2.0. Недавно проведенное компанией Forrester Consulting по заказу SCC исследование относительно рисков в среде Web 2.0 показало, что хотя угрозы реальны и компании осведомлены о них, они не предпринимают каких-либо достаточных действий для собственной защиты.

Основываясь на рекомендациях Forrester Consulting, собственном многолетнем опыте и опыте клиентов, а также на данных, полученных от своей глобальной репутационной системы TrustedSource, компания Secure Computing выработала семь основных требований, исполнение которых при проектировании системы безопасности обеспечит наиболее эффективную защиту от угроз Web2.0. Данные требования выражают определенный результат их SWAT-инициативы. Возможно они покажутся достаточно очевидными, но эффективная политика, как правило, лаконична и проста для понимания.

1. Для фильтрации почтовых сообщений и URL-ссылок для всех доменов, в том числе и еще не категорированных, *используйте системы подсчета репутации в реальном времени.*

Только тематическое категорирование URL-ссылок в плане защиты от Web-угроз уже малоэффективно. Репутационные системы нового поколения обеспечивают возможность вычисления актуального на текущий момент уровня риска от контакта с каждым зафиксированным ими подозрительным сетевым объектом. Они идентифицируют такие объекты, как источники спама, зомбированные машины и ботнеты на их основе, устанавливают инфицированные Web-сайты и отдельные URL и, даже, фиксируют ложные DNS-сервера. Специализированные центры ведут целенаправленную и активную работу по расширению как охвата, полноты и точности анализа, так и набора идентифицируемых объектов. Например, на дата-центрах TrustedSource.org (Secure Computing) ежедневно анализируются миллиарды почтовых сообщений и миллионы Web-сайтов. Обнаруживается до 18 тысяч зомбированных машин в час по всему миру. Охват системы – более 7000 сенсоров в 82 странах.
Учет в политике безопасности репутации объекта доступа совместно с его категоризацией позволяет не только значительно увеличить эффективность защиты от внешних угроз с точки зрения их своевременного выявления, но и повысить производительность системы доступа. Даже некатегорированные объекты, подпадающие под установленный вами по скользящей шкале пороговый уровень риска, будут блокированы уже на этапе попытки установления соединения.

Принимая во внимание комплексность современных атак, репутационная система должна как минимум просчитывать репутации как Web, так и почтовых Интернет-ресурсов. Направленная атака зачастую начинает развитие с рассылки закамуфлированных под “полезные” почтовых сообщений, содержащих URL-ссылки на заранее подготовленные ресурсы с вредоносным кодом. Камуфляж может быть весьма действенным, в частности, если это результат ”социальной инженерии” атакуемого объекта. Последующее обращение по ссылкам ведет к эскалации атаки. Безусловно, системы на основе оценки репутации - это не панацея, а один из эффективных современных механизмов в многоуровневой системе обеспечения безопасности.

2. Используйте средства защиты от вредоносного программного обеспечения с механизмами как локального анализа поведения кода в реальном времени - для защиты от новых, пока не выявленных угроз, так и сигнатурного анализа - для защиты от уже известных угроз.

Необходимость в проактивной фильтрации почтового и Web трафиков уже давно не вызывает сомнения и широко применяется. Сигнатурным системам обнаружения вредоносных кодов заведомо сложно своевременно справляться со своей задачей.
Примером динамической природы угроз Web2.0 может служить программа генератор-мутантов VoMM (eVade o’Matic Module), вошедшая в открытый проект Metaspoit. Суть ее проста - с помощью ряда методов автоматически модифицируется код известных эксплойтов, делая их неразличимыми для сигнатурных антивирусов.
Проактивное сканирование подразумевает эвристический анализ поведения мобильного кода: ActiveX, BHO, Java аплеты и приложений, Java и VB Script в разных формах, VB в офисных документах и тп, а также исполняемых модулей Windows и DLL. Анализируются HTML и скрипты на предмет попыток переполнения буфера, внедрения shell-кода и тп.
Проактивная фильтрация, безусловно, не устраняет потребность в использовании различных баз данных. Более того, результаты обнаружения новых вредоносных кодов настоятельно рекомендуется автоматически перенаправлять на репутационную систему для дальнейшего анализа и от этого будут в выигрыше все ее участники. Таким образом, хотя любая из баз заведомо имеет ограничения и по объему, и по актуальности содержащейся в ней информации: что сигнатурная антивирусная, что URL-категорий или репутационная, но вопрос состоит в том, чем она наполняется и в каких целях эти данные используются. То есть комплексная защита подразумевает сочетание как различных технологий, так и данных для достижения максимального эффекта.

3. Используйте на шлюзе доступа двухстороннюю фильтрацию и контроль приложений для всех видов Web-трафика, включая протоколы от HTTP до IM и шифрованный трафик.

То есть весь доступный защитный функциональный набор должен применяться как к входящему, так и к исходящему трафику. Достаточно очевидно, что только такой подход позволит обеспечить эффективную защиту как от внешних, так и от внутренних угроз.

4. Задействуйте защиту от утечки информации по ключевым протоколам Web2.0 и Email.

Эту задачу защиты вашей интеллектуальной собственности и обеспечения соответствия требованиям аудиторских проверок рекомендуется решать в 4 этапа:

- Определение политики – знание, что и кому разрешено.
- Обнаружение нарушения – установление содержимого сообщения и наличия в нем информации, подлежащей защите.
- Автоматическое реагирование – применение адекватных мер безопасности на основании информации о важности содержимого и его отправителе.
- Отчетность и аудит – фиксация и протоколирование происшествия.

Таким образом, помимо контроля разрешения доступа к различным приложениям (Web-сайты, блоги, wikis, IM, P2P, почтовые системы и т.п.) требуется анализ исходящих соединений и на предмет утечки информации. С учетом широкого применения HTTPS для внутрикорпоративного информационного обмена, безусловно, должна присутствовать и возможность только выборочной дешифровки трафика

для соблюдения внутренних требований конфиденциальности (например, по доступу к внутренним финансовым системам).

5. Обеспечьте внедрение кэширующих прокси с учетом не только вопросов производительности, но и безопасности.

К кэшируемым объектам следует применять все виды фильтрации при каждом пользовательском запросе на их получение, так как с момента занесения объекта в кэш могут измениться его репутация, контрольные сигнатуры или внутренняя политика в отношении данного объекта. Если прокси не позволяет отслеживать такие изменения, повторно закачивает объект под каждое изменение или дублирует объекты для каждой политики, то, очевидно, это скажется на эффективности его использования или с точки зрения производительности и ресурсоемкости, или безопасности.

6. Проектируйте инфраструктуру безопасности из расчета возможности обеспечения многоуровневой защиты с минимальным количеством задействованных для ее реализации устройств.

Современные шлюзы безопасности являются ключевыми точками в определении политик, их реализации и отслеживании исполнения. Это обуславливает повышенные требования к ним. Как было отмечено ранее, современная защита подразумевает объединение в себе как обновляемых баз (сигнатуры и категории URL), так и анализ в реальном времени (проверка репутации и поведение кода). Эффективная реализация механизма кэширования подразумевает тесную интеграцию с механизмами защиты, и, скорее всего, в рамках единого приложения. Требуется исключения таких “мертвых зон” в анализе, как SSL трафик и, конечно, исключение возможности внесения используемыми устройствами дополнительных уязвимостей. Например, за счет операционных систем, на которых они работают. Использование разнородных систем может вызвать целый ряд проблем: их контроль и управление, обеспечение совместимости и надежности, консолидация данных для отчетности и тп. Однако есть и другая сторона медали – если одно устройство позиционируется с поддержкой функционала от межсетевого экрана до комплексного web- и/или email-шлюза, то закономерно возникает вопрос об уровне и полноте реализации каждого функционального набора в частности, а также производительности такого устройства.

7. Используйте развитые средства управления и отчетности, обеспечивающие возможность всестороннего контроля и анализа.

Внедряемые решения должны предоставлять как возможность быстрой и полной оценки текущего состояния подсистем защиты, так и отчетность в реальном времени или за требуемый период времени по интересующим срезам данных для проведения оперативных корректировок настроек или последующего анализа событий. Развитая и исчерпывающая отчетность – это один из ключевых элементов в понимании и оценке рисков, совершенствовании политики безопасности и оценке своего соответствия внешним регулирующим требованиям и стандартам.

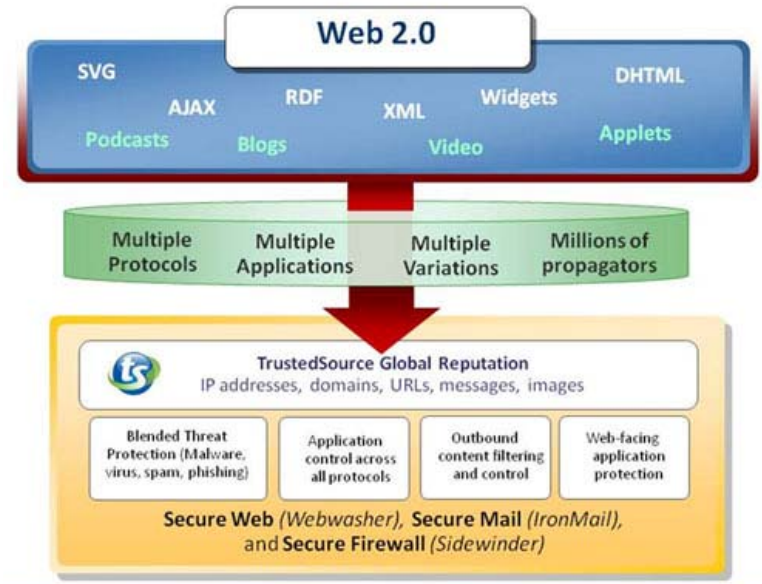

Рис.1 Продукты и технологии Secure Computing для защиты от угроз Web2.0

Следуя вышеизложенным требованиям, компания Secure Computing продолжает активно развивать линейки своих продуктов, каждый из которых в отдельности и без того входит в признанные лидеры на своем сегменте рынка (например, по отчетам Gartner Group, IDC и других признанных аналитиков рынка, а так же оценкам специализированных журналов уровня SC Magazine). В рамках же концепции защиты от угроз Web2.0 все эти комплексные и, в общем-то, достаточно уникальные по своему функционалу продукты позиционируются следующим образом:
Webwasher – web-шлюз, предоставляет исчерпывающее решение обеспечения безопасности по всем аспектам угроз Web 2.0 трафика и, безусловно, полностью соответствует вышеизложенным требованиям.
IronMail – почтовый шлюз, рекомендуемый для совместной работы с Webwasher для защиты от смешанных Web2.0 атак. Обеспечивает комплексную защиту почтовых систем от спама, вредоносного контента и утечки информации любого вида.
Sidewinder - межсетевой экран прикладного уровня. Комплексная защита корпоративных Web-серверов на уровне прокси, включая защиту от сканирования портов и уязвимостей, внешнего взлома и DDos атак.
Все три системы используют глобальную репутационную систему нового поколения TrustedSource. Ознакомиться с ее работой можно на сайте: www.trustedsource.org
В апреле этого года был создан открытый альянс TrustedSource – новая партнерская программа, позволяющая интегрировать и использовать данную технологию в своих продуктах. На текущей момент членами альянса уже являются такие компании как: Brightfilter, Cymtec Systems, F5, Foundry Networks, InternetSafety.com, MarkMonitor, Riverbed Technology и Webroot.

Для получения более подробной информации по продуктам, технологиям и инициативам SecureComputing вы можете обратиться на сайт компании: www.securecomputing.com или в компанию Демос, являющуюся ее официальным партнером в России.

А.Смирнов
Компания Демос
Публикация: LAN 06/06/2008 №06