

SOPHOS NAC: КОНТРОЛЬ ДОСТУПА К СЕТИ УСТРАНЕНИЕ ПРОБЕЛОВ В СЕТЕВОЙ БЕЗОПАСНОСТИ

Сегодня мы наблюдаем повышение общего уровня осведомленности ИТ-менеджеров об информационных угрозах, что приводит к принятию множественных мер по построению систем информационной безопасности и повышению связанных с этим затрат. Однако в диверсифицированном информационном пространстве, в условиях применения множественных гибридных решений, многие реально не контролируют работу своих пользователей и связанные с этим опасности. В стремлении к увеличению гибкости работы доступ к сети и корпоративным информационным ресурсам открывается третьим лицам (партнерам, подрядчикам и т.п.), средства безопасности которых неподконтрольны самой организации. Что касается служащих компании, то права администратора, назначаемые им для более производительного использования компьютеров, часто компрометируют систему защиты, предоставляя возможность отключения критически важных служб безопасности, таких как антивирусное программное обеспечение, системы слежения за авторизацией используемого программного обеспечения и т.п.

Мы наблюдаем технические сложности по реализации политик безопасности, заключающихся в отсутствии возможностей принудительного применения мер защиты, контроля за их состоянием и своевременного получения отчетных данных в требуемом объеме. Такие пробелы в корпоративной защите подвергают компанию целому ряду угроз – и речь уже идет не только о различных вредоносных программах, хакерах и злонамеренных пользователях, а о потере интеллектуальной собственности, например, базы клиентов, баз ERP, бухгалтерской и других систем, которые могут оказаться просто фатальными для бизнеса.

ДЛЯ ЗАЩИТЫ СВОИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПАНИИ ДОЛЖНЫ ИСПОЛЬЗОВАТЬ ЖЕСТКИЙ ПОДХОД, ОСНОВАННЫЙ НА ПОЛИТИКАХ БЕЗОПАСНОСТИ, РЕАЛИЗАЦИЯ КОТОРЫХ ДОЛЖНА БЫТЬ ПОДКРЕПЛЕНА НЕ ТОЛЬКО С НОРМАТИВНОЙ, НО И С ТЕХНИЧЕСКОЙ ТОЧКИ ЗРЕНИЯ.

Чтобы обеспечить максимальную окупаемость вложений, ИТ-менеджерам необходимы универсальные решения, работающие в уже существующих инфраструктурах и позволяющие осуществлять контроль над вредоносным ПО и действиями неизвестных или нарушающих требования политик безопасности пользователей. Ключевым фактором успеха является возможность задания, во-первых, уникальных политик, которые могут применяться к группам пользователей, а во-вторых, принадлежности пользователей к этим группам в соответствии с деятельностью организации.

Контроль доступа к сети

Имеющиеся программные и аппаратные продукты безопасности, по большей части, великолепно справляются с задачей защиты находящихся в сети и управляемых компьютеров – однако, эти продукты успешно решают лишь те проблемы, которые им известны. Слишком часто неожиданные угрозы, возникающие в сети, исходят от таких неуправляемых источников как системы с неустановленными обновлениями ПО, компьютеры, неподконтрольные организации, или, что еще хуже, управляемые компьютеры, но которые просто неправильно настроены или неправильно используются.

К КОНЦУ 2007 ГОДА, 80% ПРЕДПРИЯТИЙ ВНЕДРЯТ ПОЛИТИКУ И ПРОЦЕДУРЫ КОНТРОЛЯ ДОСТУПА К СЕТИ.

ДЖОН ПЕСКАТОР (JOHN PESCATORE), GARTNER INC

Поэтому доступ к защищенной, управляемой корпоративной сети должен обеспечиваться путем определения уровня безопасности подключающегося компьютера еще до того, как будет разрешено его подключение, а также постоянной проверки его соответствия требованиям, когда он уже работает в сети.

Технология контроля доступа к сети NAC (Network Access Control) является многообещающим ответом для решения вопроса соответствия требованиям безопасности всех компьютеров – управляемых и неуправляемых, пытающихся подключиться к сети, будь то удаленно или через локальную сеть.

Решения в области контроля доступа к сети должны выполнять следующие функции:

- оценивать уровень безопасности подключающегося компьютера и обеспечивать обратную связь – информацию о его уровне соответствия требованиям безопасности;
- сопоставлять текущий уровень безопасности компьютера с соответствующей политикой, задающей требования к доступу в сеть;
- обеспечивать минимальный уровень доступа к корпоративной сети для автоматической корректировки настроек компьютера (или самонастройки компьютера) в целях удовлетворения требований безопасности;
- осуществлять постоянный контроль за уровнем безопасности компьютеров, которые подключены к сети;
- принудительно устанавливать доступ к сети в соответствии с требованиями среды;
- обеспечивать эффективную отчетность.

Решения NAC могут быть как автономными, так и встраиваемыми во внутреннюю инфраструктуру сети. Выбор подходящего решения для какого-то конкретного предприятия зависит, прежде всего, от сетевой среды, а именно от того, насколько она однородна, каковы основные способы доступа к ней и каков имеющийся в распоряжении бюджет.

Инициативы и решения

Рост и масштабы угроз сетевой безопасности стали причиной разработки комплексных программ и создания альянсов в данной отрасли. Крупные игроки используют эти инициативы, чтобы добиться поддержки со стороны вновь появляющихся поставщиков в части разных подходов к обеспечению соответствия требованиям безопасности на основе политик доступа, внедрения функций оценки уровня безопасности и формирования различных отчетов. Три наиболее признанные инициативы включают технологию защиты сетевого доступа NAP от компании Microsoft, контроль доступа к сети NAC от компании Cisco и совместимые стандарты и решения от Trusted Computing Group, такие как Trusted Network Connect.

Microsoft NAP

Защита сетевого доступа NAP (Network Access Protection) от компании Microsoft представляет собой платформу принудительного применения политик, которая интегрируется как в Windows Vista, так и в операционную систему Windows Server 2008 (Longhorn). Архитектура NAP состоит из компонентов, устанавливаемых на стороне клиента и сервера, которые выполняют конфигурирование и корректирование политик. Платформа проверяет системные требования, заданные в политиках, которым должны удовлетворять компьютеры, подключающиеся к сети. Не удовлетворяющие этим требованиям компьютеры получают доступ только к определенным зонам корпоративной сети – до установки требуемых обновлений. Полный доступ к сети предоставляется только в случае удовлетворения всем требованиям политики.

Cisco NAC

Концепция контроля над доступом к сети NAC (Network Admission Control) от компании Cisco представляет собой сетевой подход к вопросу принудительных мер защиты, при которых политика безопасности интегрируется в инфраструктуру корпоративной сети. Политики безопасности хранятся на серверах политик и применяются на маршрутизаторах и коммутаторах. Программный клиент, установленный на компьютерах, подключающихся к сети, передает сведения о своем статусе безопасности на сервер политик. Компьютеры, не удовлетворяющие требованиям, идентифицируются, и они либо отправляются в карантин, либо их доступ к сети ограничивается.

ОРГАНИЗАЦИЯМ СЛЕДУЕТ ЗАЩИЩАТЬ СВОИ СЕТИ ОТ ПРОДВИНУТЫХ ПОЛЬЗОВАТЕЛЕЙ, КОТОРЫЕ НАМЕРЕННО ПЫТАЮТСЯ ИЗБЕЖАТЬ МЕР БЕЗОПАСНОСТИ ПРИ ДОСТУПЕ К СЕТЕВЫМ РЕСУРСАМ.

NAC также является стратегической программой, в рамках которой компания Cisco предоставляет

ее участникам возможность интегрировать реализованные функции в свои решения. Для крупных предприятий, сети которых целиком и полностью основаны на программных и аппаратных средствах компании Cisco, это может стать правильным решением проблемы доступа к сети.

Группа Trusted Computing Group (TCG)

Задача группы TCG – создание стандартов открытых систем для применения в сетевой безопасности и продвижение стандартов, не зависящих от платформ, устройств и производителей. Спецификация Trusted Network Connect (TNC), разработанная груп-

Sophos NAC

Совместимые системы сетевой авторизации:

- Microsoft NAP
- Cisco NAC
- Trusted Computing Group TNC

пой TCG, определяет основу для обеспечения безопасности, которая предотвращает подключение к сети и заражение со стороны неуправляемых устройств. TNC – это формальное расширение рабочей группы TCG Infrastructure Working Group. Концепция TNC определяет фундаментальные аспекты доверенных вычислений, т.е. взаимодействующих решений от многочисленных поставщиков, использование существующих стандартов в отрасли, включая EAP, 802.1X и RADIUS, а также их применение для неоднородных сетей.

Sophos NAC

В 2007-м году компания Sophos предоставила собственное решение для контроля доступа в сети. Sophos NAC управляет доступом к сети на основе политик безопасности, задаваемых и управляемых администратором. Это гарантирует, что сеть будет защищена при подключении к ней компьютеров как удаленно, так и по локальной сети, по линиям связи или с использованием беспроводных технологий, из зоны ответственности системы безопасности либо с гостевых компьютеров.

Sophos NAC

Совместимое программное обеспечение:

- Cisco®
- Computer Associates®
- Internet Security Systems™
- Sophos
- Trend Micro™
- Zone Labs™
- Microsoft®
- McAfee®
- Symantec™
- Big Fix™
- Lucent Technologies®
- Hewlett-Packard
- Juniper Networks™
- Meetinghouse™

Через веб-интерфейс осуществляется поддержка всего основного ПО систем безопасности, определяются пользовательские приложения, а также одним нажатием мыши выполняется “легализация” патчей для операционной системы (ОС). Администраторы мо-

гут задавать и осуществлять управление уникальными политиками для выделения патчей ОС, приложений обеспечения безопасности и обновления баз сигнатур, а также гарантировать, что неавторизованные приложения не будут запущены на клиентских компьютерах.

Являясь программным решением, система Sophos NAC не зависит от изготовителя оборудования и ПО, и поэтому может быть вполне совместима с уже имеющейся сетевой инфраструктурой (коммутаторами, концентраторами виртуальных частных сетей, серверами DHCP и хранилищами данных). Система Sophos NAC представляет собой готовый самостоятельный продукт и не требует внесения значительных изменений в существующее аппаратное обеспечение, кроме того, существует синхронизация с уже настроенными группами пользователей. Система использует набор заранее определенных правил по выявлению основного ПО систем безопасности, которые не потребуются менять. Простой централизованный режим управления политиками безопасности позволяет задействовать режимы их реализации поэтапно, – начиная с режима “Только уведомление” (Report Only), далее “Восстановление” (Remediate), и заканчивая режимом “Слежение” (Enforce). Так удается избежать подхода “всё или ничего”, но обеспечивается оптимальное управление и простота в развертывании политик безопасности на каждой из стадий внедрения.

Sophos NAC

Совместимое сетевое оборудование:

- Alcatel™
- Aruba Networks™
- Aventail®
- Cisco®
- Checkpoint®
- Enterasys Networks
- Extreme Networks™
- Foundry® Networks
- Hewlett-Packard
- Infoblox®
- Juniper Networks™
- Lucent Technologies®
- MetalInfo®
- Nortel®
- Novell
- RSA Security®
- Sun Microsystems
- 3Com Corporation™

Авторизация нового компьютера в сети производится поэтапно. При подключении определяется принадлежность компьютера к сети компании. Это можно определить не только поиском соответствующей записи в домене, но и поиском специальной программы – агента, через который производится общение рабочей станции с сервером. Агент может быть постоянной программой, установленной на компьютере, либо, если станция гостевая, может быть выполнен в качестве расширения к стандартному браузеру. Если компьютер известен (например, это мобильный компьютер менеджера по продажам), то он проверяется на соответствие политикам безопасности (Sophos NAC policy scan). Если обнаружено несоответствие, то компьютер переключается на карантинный сервер (Remediate), и в сеть не допускается. После «лечения» станции (установки требуемых патчей ОС, либо сканирования антивирусом и т.п.), процесс авторизации повторяется до тех пор, пока компьютер не будет соответствовать всем принятым в компании политикам безопасности.

ции повторяется до тех пор, пока компьютер не будет соответствовать всем принятым в компании политикам безопасности.

Система Sophos NAC обладает развитой системой аудита и отчетов, как в режиме real-time, так и в режиме обработки архивных данных, позволяющем проводить глубокий анализ состояний корпоративной сети.



Sophos NAC Policy Scan: protecting the entire network