ЗАЩИТА CALLMANAGER

ВВЕДЕНИЕ

Ряд производителей решений по IP-телефонии на своих мероприятиях регулярно заявляют о том, что платформа Windows не может быть использована для построения надежной телекоммуникационной инфраструктуры. Как альтернативу они рассматривают операционную систему Linux для установки серверов управления. Давайте посмотрим, правы ли они? Можно ли построить надежную инфраструктуру IP-телефонии на платформе компании Microsoft? В качестве иллюстрации будем использовать систему Cisco CallManager 4.1.

Механизмы и методы защиты CallManager

Начнем с самого начала – с операционной системы, на базе которой строится сервер управления различных производителей. Уже давно ведутся баталии приверженцев Windows и Unix о том, какая операционка более защищена. Даже несколько лет назад, когда лидерство Unix в области надежности и безопасности казалось безоговорочным, можно было привести множество примеров, когда сеть, построенная на платформе Windows, была устойчивой к разного рода несанкционированным воздействиям. Все это достигалось правильной настройкой операционной системы. Сейчас ситуация изменилась кардинально. Компания Microsoft много внимания уделяет безопасности своих решений и тратит миллионы долларов на тестирование их защищенности. Все это привело к тому, что сейчас защищенность Windows выросла многократно. С другой стороны, активное распространение Linux и попытка ее производителей занять нишу домашней операционной системы привело к снижению уровня ее безопасности. Продемонстрировать это можно очень просто – достаточно подсчитать число уязвимостей, обнаруженных за последнее время в обеих операционных системах (это можно сделать на сайте www.securitytracker.com).

Уже один этот факт говорит о том, что вышеприведенное заявление некоторых производителей не соответствует действительности. Но мы не будем останавливаться только на одном доказательстве и посмотрим другие свидетельства защищенности CallManager. Начнем с того, что само по себе число дыр говорит только о защищенности абстрактной платформы, а не конкретного решения. Сервер управления CallManager устанавливается не на «обычную», типовую ОС Windows 2000 – комплект инсталляции для него существенно отличается от того, что поставляет компания Microsoft на своих компакт-дисках. Реализуется это за счет создания специального защищенного дистрибутива, из которого удалены все ненужные приложения и сервисы, заблокированы лишние учетные записи, настроены права доступа к системному реестру и файловой системе, а также проведены дополнительные настройки не только повышающие защищенность сервера управления CallManager, но и оптимизирующие его с точки зрения надежности, отказоустойчивости и производительности. Надо заметить, что аналогичный защищенный вариант ОС Windows 2000 используется и для других приложения IP-телефонии – IPCC Express, IP/IVR, Personal Assistant и др.

Но каким бы изначально защищенным ни был сервер управления со временем открываются ранее неизвестные уязвимости, которые надо устранять (это справедливо для любой операционной системы). Эффективно решать эту задачу позволяет специальный процесс обновления, в рамках которого инженеры компании Cisco проверяют выпускаемые компанией Microsoft патчи и Service Pack'и, тестируют их на совместимость с CallManager и выкладывают на сайт Cisco Connection Online (CCO) для загрузки всеми заказчиками. Наиболее критичные патчи размещаются на сайте Cisco уже через 24 часа после их выпуска компанией-производителем. Для уведомления всех пользователей CallManager существует специальный список рассылки.

К сожалению, не всегда патчи выходят сразу за обнаружением уязвимости – могут пройти дни и даже недели, прежде чем производитель операционной системы выпустит соответствующую заплатку. Что же делать? Как защитить сервер от возможных атак, использующих еще незакрытую дыру? Реализуется это путем использования двух, взаимодополняющих систем защиты – Cisco Security Agent и антивируса.

Система Cisco Security Agent (CSA) объединяет различные защитные механизмы и функции в одном решении – предотвращение атак, персональный межсетевой экран, защита от вредоносного кода, контроль целостности, блокирование утечки информации через USB-порты и другие внешние устройства (PCMCIA, CD, Floppy, Zip и другие), обнаружение перехватчиков с клавиатуры и т.п. Она позволяет обеспечить всестороннюю защиту CallManager от широкого спектра угроз - сканирования портов, переполнения буфера, троянцев и червей, DoS-атак и других. При этом CSA построен по совершенно иному принципу, чем традиционные антивирусы и системы обнаружения атак и не использует сигнатуры для идентификации несанкционированных действий. Это в свою очередь позволяет защитить компьютер от неизвестных атак, сигнатуры для которых пока не написаны и отсутствуют в базах традиционных средств защиты.

Однако есть вредоносная активность, которую гораздо проще обнаруживать с помощью традиционных сигнатурных антивирусов. С этой целью на CallManager может быть установлен один из 3-х антивирусов известных производителей – TrendMicro ServerProtect, McAfee VirusScan и Symantec Antivirus.

Дополнительный уровень защиты обеспечивается специальным набором скриптов, которые могут быть запущены на CallManager. Эти скрипты позволяют установить дополнительные ограничения парольной защиты, настроить безопасный доступ к системному реестру, установить права доступа к файлам и каталогам, удалить неиспользуемые файлы и каталоги, закрыть неиспользуемые TCP- и UDP-порты и т.п.

Помимо настроек и механизмов, повышающих защищенность платформы, на которой работает сервер управления CallManager, он сам является центральным звеном инфраструктуры безопасности IP-телефонии. И хотя это выходит за рамки данного материала, перечислим реализуемые CallManager’ом защитные функции:

- .ПО, загружаемое на IP-телефоны, управляемые с CallManager, подписывается ЭЦП, что позволяет защитить его от несанкционированного изменения и модификации (механизм image authentication). Кроме того, все файлы конфигурации, локализации и т.п., регулярно загружаемые на IP-телефоны, защищаются от несанкционированного изменения также с помощью ЭЦП (механизм file authentication).
- Для аутентификации CallManager и IP-телефонов используются цифровые сертификаты (в качестве транспорта обмена аутентификационной информацией используется протокол TLS).
- Для защиты протокола сигнализации используются соответствующие механизмы аутентификации и шифрования – HMAC-SHA-1 и AES.
- Защита телефонных переговоров осуществляется с помощью протокола SecureRTP.
- Для взаимодействия с различными шлюзами (например, MGCP) используются специальные защитные протоколы, например, IPSec.
- Для доступа к центральному корпоративному справочнику, хранящемуся в Microsoft Active Directory или Netscape Server Directory используется специальная версия протокола LDAP – LDAPS (LDAP over SSL).
- И, наконец, в CallManager реализовано несколько различных механизмов защиты от мошенничества.

Однако защищенность CallManager зависит от применения не только указанных защитных механизмов и функций. Решить задачу надежного обеспечения информационной безопасности IP-телефонии невозможно без учета сетевой инфраструктуры, лежащей в основе любой прикладной технологии. Поэтому большую роль играет комплексный подход, заключающийся в правильном дизайне всей сети и эффективном использовании всех имеющихся в ней решений, отвечающих поставленным целям:

- списков контроля доступа и VLAN,
- защитных механизмов BPDU Guard, Root Guard и IP Source Guard,
- Dynamic ARP Inspection и Port Security
- IOS Advanced Security и CISF,
- Cisco Pix и Cisco IDS и т.д.

Заключение

Только такой, комплексный и эшелонированный подход позволит построить действительно надежную и устойчивую к любым несанкционированным воздействиям инфраструктуру IP-телефонии. Не даром компания Cisco Systems единственная, кто получила максимально возможный рейтинг "SECURE" («защищенный») в тестировании решений ведущих производителей этого сегмента телекоммуникационного рынка, проведенном журналом NetworkWorld (http://www.nwfusion.com/reviews/2004/0524voipsecurity.html) в 2004 году.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Cisco CallManager 4.1

http://www.cisco.com/en/US/products/ps5820/index.html

IP Communications Security Solution

http://www.cisco.com/go/ipcsecurity

SAFE: IP Telephony Security in Depth

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_white_paper09186a00801b7a50.shtml

Securing Voice in an IP Environment

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns391/c654/cdccont_0900aecd800dfd34.pdf

Cisco IP Telephony Solution

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns268/networking_solutions_package.html

Cisco Systems
Россия, 113054 Москва
бизнес центр “Риверсайд Тауэрз”
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр “Самал 2”
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр “Горайзон Тауэрз”
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **Cisco Connection Online Web site at http://www.cisco.com/ http://www.cisco.ru/**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe