Обзор средств обеспечения безопасности систем голосовой связи. Защита инфраструктуры сети обработки голосовой связи, системы управления вызовами, приложений и оконечных устройств

При выборе решения для построения системы голосовой связи соображениям безопасности уделяется большое внимание. При внедрении в компании традиционной АТС на базе технологии TDM или современной системы IP-телефонии ИТ-специалисты и администраторы системы голосовой связи должно принять соответствующие меры для предотвращения реализации типовых угроз, например, мошенничества при осуществлении междугородных переговоров и прослушивания телефонных переговоров. Системы унифицированных коммуникаций Cisco могут обеспечить уровень безопасности равный уровню безопасности традиционных решений на базе УАТС, а то и превосходящий его. Голосовой трафик передается по той же IP-сети, по которой передается корпоративный трафик данных; таким образом, если в организации обеспечена безопасность передачи данных, то большая часть работы по обеспечению безопасности системы голосовой связи уже сделана. По результатам независимого тестирования, проведенного Miercom, решения Cisco в области IP-телефонии признаны самыми безопасными в индустрии[1].

Краткое содержание

Системы унифицированных коммуникаций позволяют организациям любого размера повысить производительность работы сотрудников, обеспечить мобильность, а также увеличить гибкость системы телефонной связи. Перед внедрением системы унифицированных коммуникаций многие компании хотят предпринять меры по обеспечению безопасности системы обработки вызовов, приложений и оконечных устройств, которые используются при обработке вызовов, а также инфраструктуры основной IP-сети.

Соображения безопасности постоянно учитываются при разработке и внедрении систем голосовой связи еще со времен частных телефонных линий, когда прослушивание линии являлось постоянной угрозой. Первые случаи взлома систем голосовой связи были зафиксированы в 1970-х годах, когда злоумышленники имитировали сигналы управления вызовами с помощью специальных устройств и осуществляли бесплатные телефонные звонки. Сегодня среди наиболее частых атак на телефонные системы TDM, а также на системы IP-телефонии, можно выделить атаки типа "отказ в обслуживании", мошенничество при осуществлении междугородных переговоров и прослушивание телефонных переговоров.

Но стоит отметить, что сервис IP-телефонии представляет собой не более чем еще один дополнительный сервис, реализованный в рамках сети, и все технологии обеспечения и политики безопасности, которые используются для защиты сети передачи данных, также распространяются на трафик системы IP-телефонии. В этом кроется отличие системы унифицированных коммуникаций и системы IP-телефонии от традиционных систем на базе УАТС, которым часто не хватает недорогих средств обеспечения общей безопасности, которые несложно внедрять по мере изменения условий работы организации.

Одно из основных отличий решений Cisco в области IP-телефонии от решений других производителей заключается в успешном решении вопросов обеспечения безопасности. По результатам независимого тестирования, проведенного Miercom, решения Cisco в области IP-телефонии признаны самыми безопасными в индустрии. На сегодняшний день компания Cisco Systems(r) является единственным производителем решений в области IP-телефонии, получившей высшую оценку Miercom "Secure". Эта оценка отражает способность сервиса IP-телефонии функционировать в условиях проведения хакерских атак[2]. Команда квалифицированных хакеров, работавшая по заданию Miercom, не смогла нарушить функционирование или хотя бы повлиять на качество функционирование сервиса телефонии, несмотря на проведение сложных непрерывных атак в течение трех дней.

В отличие от производителей, которые предлагают устанавливать отдельные устройства для обеспечения безопасности системы голосовой связи, Cisco предлагает полномасштабную интегрированную систему обеспечения безопасности, которая защищает всю сеть передачи данных, включая голосовой трафик. Несколько уровней защиты (инфраструктуры, обработки вызовов, приложений и оконечных устройств) обеспечивают надежную защиту как от уже известных, так и от новых, пока неизвестных угроз.

В этой публикации, предназначенной для ИТ-специалистов и администраторов систем голосовой связи средних предприятий, представлен обзор современных требований к безопасности систем голосовой связи и существующих решений. В начале документа приводится результаты анализа рисков систем голосовой связи, многие из которых являются общими для TDM-систем и систем IP-телефонии. Далее рассматриваются решения Cisco, позволяющие обеспечить безопасность инфраструктуры системы голосовой связи, системы управления вызовами, приложений и оконечных узлов. В документе приводятся ссылки на web-сайты Cisco, на которых представлена подробная информация о различных компонентах многоуровневого решения Cisco по обеспечению безопасности систем голосовой связи. Организации, заинтересованные в реализации описанных в данной документе решений по обеспечению безопасности сети, могут заказать разработку проекта компании Cisco или партнеру Cisco, при этом в любом случае исполнитель будет следовать тем этапам, которые рекомендованы в документе Cisco Smart Business Roadmap.

Типы угроз для системы голосовой связи

Мошенничество при осуществлении междугородных переговоров

Понятие "Мошенничество при осуществлении междугородных переговоров" относится к ситуации, когда внутренние или внешние пользователи системы корпоративной телефонной системы осуществляют несанкционированные междугородные звонки. Мошенничество при осуществлении междугородных переговоров может осуществляться при использовании в организации как TDM-, так и IP-системы.

Отказ в обслуживании

При проведении атаки типа "отказ в обслуживании" злоумышленники используют программные средства, которые отправляют большое количество не имеющих смысла пакетов на IP-телефоны, серверы обработки вызовов или элементы сетевой инфраструктуры. Целью действий злоумышленников является перегрузка сетевых ресурсов с тем, чтобы вызовы прерывались или их обработка была невозможна. Обычным мотивом атаки является отвлечение ИТ-специалистов для того, чтобы они не обратили внимания на другие атаки.

Подмена абонента

При проведении атаки типа "подмена абонента" злоумышленник подделывает реквизиты доступа легитимного пользователя с тем, чтобы вызовы с телефона злоумышленника казались исходящими с телефона другого пользователя. Например, неизвестный может выдать себя за сотрудника отдела поддержки и позвонить руководителю компании с тем, чтобы узнать его пароль. Если в качестве идентификатора звонящего отображается легитимный телефонный номер, чего нетрудно добиться в рамках как TDM-, так и IP-телефонной системы, жертва может поверить злоумышленнику. Злоумышленники могут подделать IP-адрес своего узла или установить свой DHCP-сервер, отвечающий за распределение IP-адресов.

Прослушивание телефонных переговоров или атака типа "человек в середине"

При проведении атак типа "человек в середине" внутренний пользователь присваивает IP-адрес маршрутизатора или компьютера для прослушивания голосового трафика и данных, вводимых с клавиатуры IP-телефона, например, паролей. После быстрого копирования информации голосовой трафик перенаправляется получателю, так что ни отправитель, ни получатель не могут понять, что разговор прослушивается. Обычными мотивами являются шпионаж или личное преследование. Прослушивание существенно облегчается доступным количеством свободно распространяемых средств для анализа сетевого трафика. Однако прослушивание сравнительно легко предотвращается.

Безопасность инфраструктуры

Для обеспечения безопасности системы голосовой связи используются те же проверенные интегрированные решения Cisco, которые позволяют обеспечить безопасность передачи данных. Организации, внедрившие самозащищающуюся сеть Cisco (SDN), уже обладают фундаментом для построения защищенной системы голосовой связи.

Далее перечислены некоторые из технологий, рекомендованных Cisco для формирования защищенной инфраструктуры, которые могут быть особенно полезны для защиты систем голосовой связи.

Сети VLAN

Технология Cisco VLAN, встроенная в маршрутизаторы Cisco, коммутаторы Cisco Catalyst ® и точки доступа к беспроводной сети Cisco Aironet ®, обеспечивает разделение одной физической сети на несколько логических сетей, например, для разделения сети организации на сети отдела кадров, отдела продаж, отдела маркетинга, инженерного отдела и бухгалтерии. Основным методом обеспечения безопасности системы голосовой связи является создание отдельной VLAN для передачи голосового трафика. Во-первых, трафик голосовой VLAN не будет доступен внутренним или внешним пользователям, подключенным к различным VLAN передачи данных, и трафик данных не сможет

попасть в голосовую VLAN. Во-вторых, ИТ-специалисты смогут назначить для голосовой VLAN особый класс обслуживания, обеспечивающий приоритет голосового трафика над трафиком данных.

Ниже описаны некоторые способы защиты системы голосовой связи от различных угроз с использованием сетей VLAN :

- **Предотвращение мошенничества при осуществлении междугородных переговоров.** Организации могут устанавливать различные политики управления доступом к голосовой VLAN; например, сотрудники отдела производства могут иметь доступ к сегменту данных, но не иметь доступа к сегменту голосовой связи. Создание отдельной голосовой VLAN также позволяет предотвратить использование сотрудниками сети VLAN другого отдела для выполнения междугородных звонков (такое мошенничество позволяет сотрудникам экономить средства за счет того, что счета за междугородные переговоры попадут в другой отдел).
- **Предотвращение атак типа "отказ в обслуживании".** Многие атаки типа "отказ в обслуживании" должны запускать с персонального компьютера и потому не смогут повлиять на состояние IP-телефонов и серверов обработки вызовов, подключенных к отдельной голосовой VLAN.
- **Предотвращение прослушивания и перехвата телефонных переговоров.** Обычно для прослушивания переговоров злоумышленники используют персональный компьютер со специальным программным обеспечением. При этом компьютер необходимо подключить к VLAN одного из абонентов. Если устройство системы голосовой связи логически выделены в отдельную сеть, злоумышленник не может подключить персональный компьютер к голосовой VLAN.

VPN с поддержкой передачи голоса и видео

Предотвращение несанкционированного доступа к сети является неплохим первым шагом в программе обеспечения безопасности системы голосовой связи. Для введения дополнительного уровня защиты на случай если злоумышленник все же получит несанкционированный доступ к сети, в организации может использоваться криптографическая защита голосового трафика. Технология VPN с поддержкой голоса и видео (V3PN), реализованная во многих маршрутизаторах и специализированных устройствах обеспечения безопасности Cisco, обеспечивает шифрование голосового трафика и трафика данных с использованием алгоритмов IPSec или AES. Шифрование выполняется на аппаратном уровне, таким образом производительность межсетевого экрана не снижается. Также внедрение решения V3PN не влияет на качество голосовой связи, поскольку устройства обеспечения безопасности ASA 5500 Series и решения Cisco в области межсетевых экранов поддерживают механизмы обеспечения качества обслуживания (QoS). При передаче пакетов голосового трафика по VPN-туннелям они обладают более высоким приоритетом, чем пакеты трафика данных.

Ниже описаны некоторые способы защиты системы голосовой связи от различных угроз с использованием технологии Cisco V3PN:

- **Предотвращение мошенничества при осуществлении междугородных переговоров.** Для осуществления мошенничества злоумышленнику необходимо получить сведения о телефонной системе и ее легитимных пользователях, например, MAC- и IP-адреса IP-телефонов Cisco Unified и сервера Cisco Unified Communications Manager. Криптографическая защита этой информации при передаче по сети (особенно после логического выделения голосового трафика в отдельную сеть VLAN и введение механизмов контроля доступа) существенно затрудняет доступ к ней злоумышленника.
- **Предотвращение прослушивания и перехвата телефонных переговоров.** Во многих организациях технология V3PN используется для шифрования голосового трафика, передаваемого через общедоступные сегменты сети Интернет, например, голосового трафика между основным офисом организации и ее филиалами. Маршрутизаторы Cisco, решения в области межсетевых экранов, VPN-концентраторы и адаптивные устройства обеспечения безопасности также обеспечивают шифрование данных, вводимых пользователями с клавиатуры телефонов в процессе телефонных переговоров, например, паролей или номеров кредитных карт, которые вводятся по запросу систем IVR.

Списки контроля доступа

Списки контроля доступа (ACL), которые используются во всех сетевых устройствах Cisco, позволяют ограничить доступ к заданному сетевому ресурсу, например, серверу Cisco Unified Communications Manager, предоставив доступ определенным пользователям или хостам, принадлежащим к определенным сегментам сети. В рамках организации ACL для голосового трафика могут настраиваться для отделов, рабочих групп и даже отдельных пользователей.

Списки ACL позволяют обеспечить безопасность системы голосовой связи следующим образом:

- **Предотвращение мошенничества при осуществлении междугородных переговоров.** Организации могут использовать ACL для управления списком пользователей, которым предоставлен доступ к системе голосовой связи, и списком местоположений, из которых предоставляется доступ к системе голосовой связи. Например, организация может предоставить доступ к шлюзу системы голосовой связи для осуществления междугородных и международных

звонков только некоторым пользователям, и даже запретить этим пользователям доступ из менее доверенных областей внутренней сети. Запрет доступа из вестибюлей здания может предотвратить международные звонки со стороны постороннего посетителя, зашедшего в здание с ноутбуком, на котором установлено программное обеспечение системы IP-телефонии. Такой запрет позволит предотвратить обнаружение адреса сервера обработки вызовов путем сканирования портов, проведенного посторонним из того же вестибюля или других областей общего доступа. Совместное использование ACL и VLAN позволяет обеспечить дополнительную защиту от мошенничества при осуществлении междугородных переговоров. Представим, что сотрудник одного отдела хочется воспользоваться приложением Cisco IP Communicator, установленным на портативном компьютере, с тем, чтобы выдать себя за сотрудника другого отдела и уменьшить расходы своего отдела на телефонную связь. Технология VLAN не позволяет сотруднику выполнять голосовые вызовы из сети VLAN другого отдела. В качестве дополнительной меры обеспечения безопасности можно настроить ACL пользователя таким образом, чтобы запретить передачу его трафика из сети VLAN одного отдела в сеть VLAN другого.

- **Предотвращение прослушивания и перехвата телефонных переговоров.** Списки ACL позволяют предотвратить передачу голосового трафика через недостаточно защищенные области сети.
- **Предотвращение атак типа "отказ в обслуживании".** Организации могут использовать механизм списков ACL для предотвращения передачи входящих пакетов данных, например, пакетов, которые составляют атаки типа "отказ в обслуживании" в сеть VLAN системы голосовой связи. Можно настроить отдельные списки ACL для входящего и исходящего трафика. В этом случае ACL для входящего трафика блокирует поступление входящих пакетов в сеть VLAN системы голосовой связи, а ACL для исходящего трафика разрешает передачу во внешнюю сеть пакетов, исходящих из сети VLAN системы голосовой связи. Такое разделение позволяет внедрить на IP-телефоны Cisco Unified различные XML-приложения, например, для регистрации времени начала и завершения работы смен.

Безопасность портов

В то время как решения Cisco в области межсетевых экранов обеспечивают контроль и разграничение доступа внешних пользователей, средства обеспечения безопасности портов позволяют реализовать контроль и разграничение доступа внутренних пользователей. Встроенные механизмы обеспечения портов маршрутизаторов и коммутаторов Cisco позволяют ограничивать набор сервисов, доступных пользователям, на основании физического порта, к которому подключены пользователи. Такой подход позволяет защищать систему голосовой связи следующим образом:

- **Предотвращение мошенничества при осуществлении междугородных переговоров.** Первым шагом в предотвращении мошенничества является отказ в доступе тем пользователям, которым не предоставлены соответствующие права доступа. Средства обеспечения безопасности портов позволяют организациям ограничить доступ к сети головой связи до уровня конкретных физических портов. Например, организация может запретить доступ к системе голосовой связи через порты, связанные с областями, в которых у сотрудников обычно нет телефонов, например, с областями содержания заключенных в пенитенциарных учреждениях или с производственными помещениями на промышленных предприятиях. Другой способ контроля доступа с использованием средств обеспечения безопасности портов заключается в перенаправлении пользователя в соответствующую сеть VLAN на основании прав доступа пользователя к системе голосовой связи. Например, неизвестный пользователь может быть перенаправлен в гостевую сеть VLAN, которая характеризуется ограниченным или отсутствующим доступом к системе голосовой связи. Кроме того, список ACL для данного пользователя предотвращает его доступ к системе голосовой связи. Напротив, легитимный пользователь будет направлен в сеть VLAN своего отдела.
- **Предотвращение атак типа "отказ в обслуживании".** Порт не включается до тех пор, пока он не получит подтверждение об уровне доверия пользователю и устройству, с помощью которого работает пользователь. Такой подход позволяет предотвратить несанкционированное подключение постороннего лица к сети из укромного уголка в помещениях организации, например, из подвала или комнаты для переговоров, для последующего запуска атаки типа "отказ в обслуживании". Для защиты от атак типа "отказ в обслуживании" с настольных компьютеров или ноутбуков сотрудников организации необходимо совмещать использование средств обеспечения безопасности портов с решениями NAC, позволяющими убедиться, что на настольном компьютере или ноутбуке установлены последние версии антивирусной программы и программы Cisco Security Agent.
- **Предотвращение подмены пользователя, подмены адреса отправителя или прослушивания телефонных переговоров.** Средства обеспечения безопасности портов позволяют ограничить количество MAC-адресов устройств, которым разрешен доступ к сети через заданный порт. Это позволяет предотвратить ситуацию, в которой нарушитель отключает легитимный IP-телефон от сети, подключает на его место концентратор на два порта или более, а затем подключает к одному из портов несанкционированный IP-телефон или компьютер, на котором установлено соответствующее приложение телефонии. Порт не будет допускать подключения устройств с MAC-адресами, отличными от заданного MAC-адреса.

Сервер системы контроля доступа Cisco Secure Access Control Server

Сервер Cisco ACS обеспечивает динамическое создание списков ACL для пользователей. В списках ACL указывает перечень действий, разрешенных для конкретного пользователя. Организация может установить правила аутентификации пользователей. Как правило, процедура аутентификации основывается на том, кто пытается войти в систему (имя или идентификатор), что у него есть (электронный ключ или карточка), и что он знает (пароль). Представим себе, что Дженнифер работает в отделе кадров и имеет право пользоваться как сервисом передачи данных, так и сервисом голосовой связи. В то же время Джейсон работает на производстве и имеет право пользоваться только сервисом передачи данных. Не зависимо от того, работает Дженнифер из дома или из офиса, после прохождения процедуры аутентификации она может зарегистрироваться в интранет-сети организации или на IP-телефоне Cisco Unified. Джейсон не сможет получить доступ к голосовой сети даже в том случае, когда он подключается ноутбук с программным обеспечением IP-телефонии к сети VLAN отдела, в котором у всех сотрудников есть право пользования системой голосовой связи.

Сервер Cisco Secure ACS позволяет обеспечить защиту системы голосовой связи следующими способами:

- **Предотвращение мошенничества при осуществлении междугородных переговоров.** Решение Cisco Secure ACS обеспечивает управление действиями, разрешенными для конкретных пользователей. Организация может устанавливать, могут ли пользователи осуществлять местные, междугородные и международные звонки; пользоваться программным обеспечением IP-телефонии, например, Cisco IP Communicator; обладают ли пользователи, работающие из дома или находящиеся в командировке, теми же правами, что и при работе в офисе.
- **Предотвращение атак типа "отказ в обслуживании".** Сервер Cisco Secure ACS функционирует совместно с устройством NAC, которое проверяет состояние системы обеспечения безопасности настольного компьютера или ноутбука перед тем, как разрешить его подключение к сети. Если сотрудник унес ноутбук домой на выходные, там он был заражен вирусами или программным обеспечением для запуска атак типа "отказ в обслуживании", решение NAC обнаружит вредоносное программное обеспечение и заблокирует доступ к сети до тех пор, пока вредоносное ПО не будет удалено.
- **Предотвращение прослушивания телефонных переговоров.** Механизмы аутентификации пользователей, используемые в решении Cisco ACS, позволяют предотвратить подмену пользователя с целью прослушивания телефонных переговоров.

Контроль DHCP-трафика

Один из методов осуществления атаки типа "человек в середине" заключается в том, что злоумышленник подменяет DHCP-сервер для перенаправления всего сетевого трафика через устройство, находящееся под его контролем. Целью таких действий могут являться прослушивание телефонных переговоров или осуществление атаки типа "отказ в обслуживании". Для предотвращения внедрения ложного DHCP-сервера в организации может использоваться функция коммутаторов Catalyst "DHCP Snooping", которая позволяет задавать доверенные порты (через них могут поступать запросы и подтверждения протокола DHCP) и недоверенные порты, через которые разрешено только пересылаться DHCP-запросы. Если злоумышленник пытается послать подтверждающее сообщение DHCP-ACK в сеть через недоверенный порт, то его попытка блокируется, тем самым, срывается атака по внедрению ложного DHCP-сервера.

Решения Cisco в области межсетевых экранов

Решения Cisco в области межсетевых экранов позволяют ограничить набор портов, которые могут использоваться внешними пользователями для доступа к сети с использованием заданных протоколов. Обычно доступ внешних пользователей ограничивается портом 80 для трафика HTTP. Среди функций решений Cisco в области межсетевых экранов присутствует "контроль состояния TCP-соединений". Этак функция позволяет гарантировать, что ни один пакет из сети Интернет не будет передан в локальную сеть организации за исключением тех случаев, когда этот пакет представляет собой ответ на явный запрос или если когда пакет поступает от хоста с адресом, для которого предоставлен доступ в локальную сеть. Такие меры позволяют предотвратить несанкционированный доступ к сети передачи голоса.

Предотвращение вторжений

Системы предотвращения вторжений (IPS), разработанные Cisco, могут внедряться как автономные устройства-сенсоры или как модули устройств Cisco ASA 5500 Series и Cisco Catalyst 6500 series. Решения IPS дополняют решения Cisco в области межсетевых экранов и позволяют предотвратить несанкционированное использование порта 80 для нарушения безопасности системы голосовой связи или любого другого ресурса сети. Межсетевой экран обеспечивает выполнение политик, регламентирующих протоколы и приложения, которым разрешен доступ через заданный порт. Система IPS анализирует весь трафик в контролируемой сети независимо от его источника и осуществляет поиск вредоносных воздействий. Специалисты ИТ-отдела могут задать допустимое поведения для каждого приложения, например, для Cisco Unified Communications Manager. В отличии от антивирусных решений,

осуществляющих поиск известных сигнатур, сенсоры и модули Cisco IPS осуществляют поиск признаков аномального поведения, никак не связанного с наблюдавшимся ранее. Такой подход позволяет средствам IPS обнаруживать вредоносный трафик даже в тех случаях, когда он формируется совершенно новым программным средством. Специалисты организации могут сконфигурировать Cisco IPS на автоматическое выполнение действий при обнаружении угрозы, например, на сброс порта или отключение сетевого интерфейса.

Безопасность беспроводных сетей

При передаче голосового трафика по беспроводной сети организации можно использовать те же методы обеспечения безопасности, которые используются при передаче по беспроводной сети трафика данных. Так, передаваемые данные защищены от прослушивания с использованием технологии Cisco VPN, которая поддерживает алгоритмы шифрования WPA и WPA2. Другим вариантом является использование алгоритма шифрования AES как одного из приемов криптографической защиты 802.11 в беспроводной сети Cisco Unified.

Для аутентификации пользователей системы голосовой связи, работающих с беспроводной сетью, в рамках решения NAC, для связи с централизованным сервером RADIUS организации может использоваться метод аутентификации 802.1X беспроводной сети Cisco Unified.

Безопасность приложений

В состав семейства приложений системы унифицированных коммуникаций Cisco входят Cisco Unified Communications Manager, Cisco Unity® Unified Messaging и Cisco Unified MeetingPlace®. Ниже перечислены способы, используемые для защиты приложений:

- **Многоуровневая система администрирования.** Большинство администраторов в рамках организации могут обладать правами только на чтение. Права на чтение и запись могут быть предоставлены нескольким доверенным профессионалам.
- **Безопасное управление.** Перед началом управления приложениями системы голосовой связи администраторы должны проходить процедуру аутентификации. Другой метод обеспечения безопасности заключается в том, что администраторы регистрируются с использованием физического интерфейса, который отличается от интерфейса, используемого для обработки вызовов, и недоступен большинству пользователей и посторонним лицам. Кроме того, при пользовании интерфейсом управления Cisco Unified Communications Manager используется протокол HTTPS, а не HTTP, поскольку в протоколе HTTPS применяются 128-битные средства шифрования, обеспечивающие защиту управляющих воздействий от подмены или модификации.
- **Защищенная конфигурация операционной системы.** Специалисты компании Cisco осуществляют тонкую настройку операционной системы Windows на серверах, используемых для внедрения приложений Cisco Unified Communications Manager, Cisco Unity и Cisco Unified MeetingPlace. При настройке выполняется изменение принятых по умолчанию значений параметров ОС и отключение сервисов, которые не требуются для работы выделенного сервера обработки вызовов. Компания Cisco также поддерживает политику по активной разработке обновлений подсистемы безопасности (patch) и придерживается принципа подготовки оперативных исправлений (hot-fix).
- **Использование сигнализации H.323 и SIP.** Эти протоколы обладают встроенными средствами для предотвращения несанкционированного или нелегитимного осуществления или прекращения вызовов.
- **Шифрование носителей информации.** Во избежание кражи информации в решениях Cisco Unity и Cisco Unified MeetingPlace используется шифрование записи голосовых сообщений.

Безопасность системы управления вызовами

ПО Cisco Security Agent

Программное обеспечение Cisco Security Agent, реализующее функции хостовой системы обнаружения вторжений, может устанавливаться как на серверы приложений системы голосовой связи (серверы Cisco Unified Communications Manager, серверы Cisco Unity, серверы Cisco Unified MeetingPlace и другие), так и на настольные компьютеры. Когда приложение системы голосовой связи пытается выполнить любую операцию, ПО Cisco Security Agent проверяет соответствие операции политике безопасности (администрируется централизованно) и затем, либо разрешает, либо запрещает выполнение этой операции. Уникальной особенностью программного обеспечения Cisco Security Agent является подход к обеспечению безопасности: приложение не пытается обнаруживать несанкционированные приложения и не выполняет поиск сигнатур; напротив, осуществляется контроль несанкционированного поведения, например, изменение состояния недоверенного IP-телефона. Такой подход позволяет обнаруживать и предотвращать действия злоумышленника, которые не наблюдались ранее, т.е. совершенно новые и неизвестные широкому кругу специалистов (0-day) атаки. Кроме того, использование CSA устраняет необходимость в проведении процедур обновления сигнатур, которые могут отнимать много времени и ресурсов.

Приложение Cisco Security Agent позволяет обеспечивать безопасность системы голосовой связи следующими способами:

- **Предотвращение мошенничества при осуществлении междугородных переговоров.** Установка Cisco Security Agent на серверы Cisco Unified Communications Manager позволяет предотвратить внедрение атакующим в программное обеспечение "люков", которые позже могут использоваться для придания доверенного статуса недоверенному устройству. Кроме того, CSA позволяет предотвратить нарушение безопасности сервера с использованием известных и неизвестных вирусов и атак.
- **Предотвращение атак типа "отказ в обслуживании".** Программное обеспечение Cisco Security Agent перехватывает вредоносный трафик, отправленный приложению Cisco Unified Communications Manager, и блокирует передачу такого трафика, обеспечивая доступность системы управления вызовами. При установке на настольные компьютеры программное обеспечение Cisco Security Agent блокирует скрытную установку на компьютер различных приложений, например, приложений используемых для осуществления атак типа "отказ в обслуживании". Защита настольных компьютеров с использованием Cisco Security Agent приносит наибольшую пользу в тех организациях, в которых разрешена маршрутизация между сетями VLAN для передачи данных и сетями VLAN для передачи голосового трафика. В этом случае защищенные компьютеры не смогут стать источниками атаки типа "отказ в обслуживании" на сеть VLAN для передачи голосового трафика.

Защищенная конфигурация операционной системы

Специалисты компании Cisco осуществляют тонкую настройку операционной системы Windows на серверах, используемых для развертывания приложений Cisco Unified Communications Manager, Cisco Unity и Cisco Unified MeetingPlace. При настройке выполняется изменение принятых по умолчанию значений параметров ОС и отключение сервисов, которые не требуются для работы выделенного сервера обработки вызовов. Компания Cisco также поддерживает политику по активной разработке обновлений подсистемы безопасности (patch) и придерживается принципа подготовки оперативных исправлений (hot-fix).

Обеспечение безопасности оконечных устройств

Ниже перечислены некоторые технологии обеспечения безопасности, которые используются в решениях Cisco для защиты IP-телефонов Cisco и других оконечных устройств:

- **Аутентификация устройств и шифрование передаваемой информации.** Маршрутизаторы Cisco выполняют шифрование вызовов с IP-телефонов Cisco Unified, передаваемых на шлюз TDM или аналоговый шлюз, а также информации, которая передается между шлюзами с использованием протокола SRTP. Тем самым обеспечивается защита голосовых вызовов или передачи факсов от прослушивания.
- **Механизм сертификатов X.509 версии 3.** Эти сертификаты, которые используются в работе IP-телефонов Cisco Unified и программного обеспечения Cisco Unified Communications Manager, обеспечивают аутентификацию удаленного устройства. За счет обеспечения надежной аутентификации устройств сертификаты X.509 позволяют предотвратить подключение к сети устройств злоумышленников.

Обеспечение безопасности управления

Системы управления сетевыми устройствами используются в организациях, в которых созданы защищенные IP-сети, для ведения журналов событий, отслеживания тревог и проведения мониторинга сетевого трафика. Степень защищенности сети организации может быть повышена за счет защиты средств управления от воздействий со стороны злоумышленников. В противном случае квалифицированные злоумышленники, которые смогли получить доступ к средствам управления сетевыми устройствами, смогут маскировать свои атаки путем очевидно недопустимых пакетов, заполняя тем самым журнал событий и отвлекая внимание ИТ-специалистов от реальной атаки.

Ниже рассмотрены несколько подходов, рекомендуемых для защиты системы управления:

- **Создание защищенных конфигураций платформ.** Обеспечение защищенной конфигурации операционной системы позволяет гарантировать, что доступ к информации системы голосовой связи и возможность изменения этой информации будут предоставлены только легитимным пользователям. Специалисты Cisco обеспечивают защищенную конфигурацию операционной системы Windows, используемой в решениях Cisco.
- **Cisco Security Agent.** Организации, в которых защита настольных компьютеров и серверов обеспечивается с использованием Cisco Security Agent, получают возможность распространения новых политик безопасности при изменении ситуации в сфере информационной безопасности.
- **Контроль и разграничение доступа.** Доступ администратора к интерфейсу управления возможен только после прохождения процедуры аутентификации и после проверки полномочий администратора на выполнение соответствующей задачи.

- **Использование протокола HTTPS.** Управление приложениями системы голосовой связи Cisco осуществляется с использованием протокола HTTPS, а не HTTP, поскольку протокол HTTPS обеспечивает криптографическую защиту сеансов управления (128-битное шифрование).

С чего начать

Создание защищенной сетевой инфраструктуры обеспечивает высокое значение коэффициента окупаемости инвестиций, поскольку одни и те же меры позволяют защитить как голосовой трафик, так и трафик данных. Компания Cisco является разработчиком современных технологий обеспечения безопасности, позволяющих организациям построить надежную основу для системы голосовой связи, отвечающей как современным требованиям по защите информации, так и требованиям завтрашнего дня. Для упрощения процедур защиты системы голосовой связи на базе IP-сети компания Cisco разработала документ Cisco Smart Business Roadmap, требования которого могут быть выполнены как сотрудниками Cisco, так и сотрудниками организаций – партнеров Cisco.

Компания Cisco и ее партнеры предлагают широкий спектр услуг в области обслуживания и поддержки сетей клиентов, позволяющих снизить общую стоимость владения сетью, повысить ее бизнес-ценность и обеспечить надежную работы сети при внедрении системы унифицированных коммуникаций Cisco. Компания Cisco разработала подход "обслуживания сети в течение жизненного цикла", который задает минимальный набор действий, необходимых для успешного внедрения и эксплуатации системы унифицированных коммуникаций Cisco и оптимизации ее производительность за шесть шагов, составляющих жизненный цикл сети:

- **Подготовка.** Для того, чтобы принять обоснованное решение о смене технологии необходимо провести бизнес-анализ возможных последствий, результаты которого должны четко показывать финансовые преимущества для организации.
- **Планирование.** Выполните оценку существующего оборудования с тем, чтобы определить, может ли оно использоваться при внедрении новой системы.
- **Проектирование.** Разработайте подробную архитектуру новой системы, отвечающую техническим требованиям и бизнес-требованиям организации.
- **Реализация.** Выполните интеграцию устройств, не прерывая работу существующей сети и не создавая потенциальных уязвимостей в конфигурации сети.
- **Эксплуатация.** Поддерживайте работоспособность сети, выполняя ежедневные операции по техническому обслуживанию сети.
- **Оптимизация.** Обеспечивайте эффективную работу сети путем постоянного анализа и повышения производительности и функциональности сети.

Более подробная информация о подходе "обслуживания сети в течение жизненного цикла" представлена по адресу: http://www.cisco.com/go/services

Более подробная информация о документе Cisco Smart Business Roadmap представлена по адресу:

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

Более подробная информация об интегрированных сетевых средствах обеспечения безопасности системы унифицированных коммуникаций Cisco представлена по адресу: http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_package.html

Более подробная информация о системе деловых коммуникаций Cisco представлена по адресу: http://www.cisco.com/go/businesscommunications

[1]Miercom, Independent Lab Test Report: Security of Cisco Unified Communications Manager-based IP Telephony Against Malicious Hacker Attacks (на англ. языке), май 2004 г.

[2]Miercom