БЕЗОПАСНОСТЬ VoIP-соединений

Д.Балашов, руководитель службы технической поддержки ООО "АйПиМатика"

Современные тенденции ведения бизнеса требуют все больше возможностей и сервисов для организации услуг связи, что способствует активному распространению VoIP-оборудования и интенсивному росту услуг и трафика VoIP. Автор обсуждает актуальную проблему обеспечения безопасности VoIP-соединений и дает пошаговую инструкцию по ее решению.

Услуги передачи голоса через Интернет (Voice over Internet Protocol, VoIP) год за годом становятся все более востребованными. Объемы рынка предоставления услуг унифицированных коммуникаций неуклонно растут как в России, так и во всем мире. Внедрение различных систем унифицированных коммуникаций выгодно для организации не столько с экономической точки зрения, сколько с точки зрения разнообразия функций, возможности интеграции в бизнес-процессы и удобства повседневной работы. Но, несмотря на все возможности современных средств унифицированных коммуникаций, количество хакерских атак на корпоративные системы связи растет с каждым днем.

Телефонные станции очень часто становятся объектом хакерских атак. Это вызвано тем, что злоумышленник имеет возможность очень быстро заработать деньги, пропуская звонки через взломанную станцию и терминируя серый телефонный трафик. И если взлом любых других интернет-серверов куда сложнее конвертировать в деньги, то взлом IP-АТС дает возможность получить деньги буквально на следующий день. В результате абоненты получают огромные счета за разговоры с какими-нибудь экзотическими странами. В первую очередь, к сожалению, взломам способствует человеческий фактор:

- неквалифицированные действия инсталляторов IP-АТС;
- слабые пароли на телефонные номера или их отсутствие;
- использование стандартных паролей на управление телефонной станцией;
- использование устаревших версий ПО;
- отсутствие защиты IP-АТС от перебора паролей;
- отсутствие системы управления сетевым доступом (Firewall);
- некорректная конфигурация IP-АТС, позволяющая пропускать неаутентифицированные звонки.

Современное коммуникационное оборудование является одним из важнейших инструментов ведения бизнеса, который обеспечивает компанию таким неоспоримым преимуществом, как качественная и надежная текстовая, аудио- и видеосвязь. Подходить к вопросу выбора, инсталляции и последующего обслуживания данного оборудования нужно комплексно и серьезно, обеспечив необходимую защиту своим деловым коммуникациям. Рассмотрим этот вопрос по шагам.

Шаг 1

Первым шагом при построении системы безопасности для IP-телефонии является осознание возможных рисков. В общем случае они могут быть разделены на четыре группы:

- перехват коммуникационной сессии, присвоение чужих прав, нарушение конфиденциальности и искажение содержания;
- вторжение в сеть организации через бреши, появившиеся вследствие разворачивания IP-телефонии;
- использование IP-АТС обманным путем или через неавторизованный доступ;
- злоумышленные действия, направленные на ухудшение голосовых сервисов.

Шаг 2

Необходимо обратить внимание на средства защиты и компоненты коммуникационной системы или решения IP-телефонии, которые планируется внедрить в организации. Основные компоненты, особенно часто подвергающиеся атакам, должны иметь защиту:

- на уровне операционной системы: межсетевой экран и ограничение прав доступа;
- на уровне IP-АТС: защищенная конфигурация и систематическое обновление ПО;
- на уровне сторонних компонентов, которые следят за безопасностью коммуникационной системы: системы автоматического слежения за логами и оповещения администратора в случае угрозы;
- на уровне VPN для защиты передаваемого трафика: использование OpenVPN для передачи голоса, а также управления IP-АТС;
- на канальном уровне в случае невозможности использования защищенного канала (VPN): шифрование служебной сигнализации TLS и передаваемого голоса SRTP.

Шаг 3

Следует помнить, что весьма важна также правильная установка и настройка защиты некоторых компонентов. Сервер управления вызовами (IP-АТС) – это критический ресурс в коммуникационной системе организации. На нем находится вся информация о пользователях, маршрутизации, сервисах, и он может управлять доступом к другим серверам. Никогда не делайте IP-АТС полностью открытой извне – обязательно удостоверьтесь, что она находится за межсетевым экраном. Любой доступ к системным службам должен быть организован только через VPN. Азы безопасности начинаются с того, чтобы предоставить доступ извне как можно меньшему количеству сервисов. Если сотрудники, работающие удаленно, не могут использовать VPN, необходимо оставить открытыми SIP-порты, но обязательно обеспечить безопасность данных соединений.

Чаще всего SIP-пользователи находятся в локальной сети с постоянными IP-адресами или централизованно управляемыми при помощи DHCP. В качестве дополнительной меры безопасности можно явно указывать адрес для подключения конкретного внутреннего абонента. Если политикой безопасности вашей компании разрешено удаленное подключение к системе, можно повысить защищенность путем задания явно разрешенных или запрещенных хостов или сетей.

Для удаленного администрирования IP-АТС с необходимостью доступа к таким системным службам, как HTTP и SSH, обязательной мерой, существенно повышающей уровень защиты системы, является смена стандартных портов.

Оставив доступными извне только необходимые службы, следует также ограничить возможность сетевых подключений к ним с использованием межсетевого экрана. Хорошей практикой является использование нескольких сетевых интерфейсов в IP-АТС, где SIP-протокол доступен только для внутренних сетевых адресов, а объединение офисов осуществляется по протоколу IAX2 с явным открытием на межсетевом экране IP-адресов офисов и фильтрацией для всех остальных. В такой конфигурации у злоумышленника отсутствует физическая возможность атаковать коммункационный сервер организации с использованием уязвимостей протоколов.

Шаг 4

Необходимо предусмотреть мониторинг атак на IP-АТС и контроль конфигурации управляющей коммуникационной платформы на наличие встраиваемых вредоносных кодов:

- централизованное логирование. В случае успешной попытки захвата сервера злоумышленник может удалить следы попыток взлома для сохранения незаметного контроля над ним. Однако при использования внешнего syslog-сервера это сделать не удастся (необходимо будет также взломать и syslog-сервер), и у системного администратора останутся все зафиксированные проявления аномальной активности, которые затем можно будет использовать для реконструкции процесса взлома и в качестве доказательств;
- контроль конфигурации. Необходимо создать резервную копию настроенной и отлаженной системы управления коммуникациями, периодически сканируя файлы и сравненивая их со старыми отпечатками. Данная мера позволяет выявить следы замены системных утилит и встраивания вредоносных блоков. В идеальном случае база с резервными копиями системы должна находиться на другом сервере.

Шаг 5

При создании плана набора следует разграничить пользователей по возможности доступа к различным направлениям вызовов. Например, внутреннему номеру рядового менеджера может быть разрешен набор городских номеров, но запрещен вызов междугородних и международных направлений. Если план набора разработан неаккуратно, пользователи из-за ошибок инсталляции могут получить возможность мошенничать в корпоративной системе.

Немаловажно грамотно настроить доступ внутренних абонентов к междугородним и международным направлениям связи, а также правильное отображение локального и внешнего номеров организации с помощью Caller ID. Caller ID – это идентификатор абонента в виде "Имя абонента" <номер абонента>. Пользователи могут не догадываться о том, насколько просто поменять Caller ID, если он четко не привязан, и осуществить атаку по типу Caller ID spoofing (подмена Caller ID) для получения каких-либо преимуществ или нанесения вреда. Администратору АТС следует назначать абонентам Caller ID. Также необходимо подменять внутренний Caller ID на исходящих звонках на SIP-провайдера. При терминации VoIP-звонка в телефонной сети общего пользования провайдер все равно подставит свой номер, но если не скрывать свой номер перед звонком SIP-провайдеру, он может получить полное представление о внутренних номерах компании, сделать вывод об иерархии и активировать выборочную запись разговоров. Поэтому перед отправкой звонка рекомендуется на линии, ведущей к провайдеру, настроить отображение внешнего номера организации.

Всегда следует помнить, что тот, кто принимает трафик на терминацию, обладает возможностью несанкционированной записи телефонных разговоров. Сокрытие внутренних пользователей позволяет "сровнять" весь телефонный трафик, однако, возможность его записи все равно остается. Общей рекомендацией является работа с надежными провайдерами, которым можно в определенной степени доверять. Когда необходимо обеспечить гарантированные защищенные переговоры, следует использовать устройства с поддержкой шифрования, подключенные к IP-АТС организации.

Конечно, вышеприведенные советы носят лишь общий характер. В рамках одной публикации невозможно углубиться в проблему досконально. Вслед за общими вопросами безопасности VoIP-соединений, специалистами ООО "АйПиМатика" была проведена большая работа по изучению специфики применения оборудования компаний Yealink и Yeastar. Данный вопрос стал традиционно освещаться на обучающих курсах ООО "АйПиМатика", а для всех желающих был проведен специальный вебинар на эту тему. Узнать подробности вы можете на сайте www.ipmatika.ru или по многоканальному телефону 8 (495) 926-26-44. ■