УГРОЗЫ ТРАДИЦИОННОЙ КОРПОРАТИВНОЙ ТЕЛЕФОНИИ

При построении корпоративных телефонных сетей основной упор обычно делается на том, как телефония может помочь бизнес-процессам компании. Однако, рассматривая использование телефона для расширения бизнеса, совершенно упускается из виду, что телефон может стать и источником потерь в бизнесе, причем очень и очень существенных. И спектр угроз, которые приводят к этим потерям, очень широк – начиная от прослушки и несанкционированного подключения и заканчивая выведением АТС из строя шквалом телефонных звонков. Рассмотрим их более подробно.

ПРОСЛУШИВАНИЕ

Несмотря на право любого гражданина России на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, гарантируемой статьей 23 Конституции, и наличие в российском Уголовном Кодексе статьи 138, карающей за ее нарушение, все равно находятся желающие проникнуть в тайны чужих разговоров. Перехват телефонных переговоров – это самый распространенный способ промышленного шпионажа. Связано это с двумя причинами. Во-первых, его просто осуществить – и не обязательно с заходом в помещение с телефонным аппаратом. Перехват можно осуществить на всем протяжении телефонной линии, а для сотовой связи – во всей соте.

Если речь идет о классической телефонии, то подключение к линии может быть контактным и бесконтактным. По данным экспертов самым опасным является простое контактное подключение к телефонной линии. Затем примерно одинаковую опасность несет использование жучков и бесконтактное подключение (индукционное и емкостное). Гораздо более сложным является перехват в стандартах AMPS (DAMPS), NMT и GSM. Наименее вероятным считается перехват спутниковой телефонной связи.

Вторая причина легкости телефонного перехвата – невысокая стоимость этого мероприятия. Купить телефонный жучок, радиозакладку или иное устройство съема информации можно на любом радиорынке и даже в Интернет-магазине – нижняя ценовая планка 10-30 долларов (но без гарантии качества). Достаточно в поисковой Интернет-системе ввести ключевую фразу «телефонный жучок» и вы получите несколько тысяч сайтов, предлагающих те или иные услуги, связанные с такими устройствами. При желании в Интернете можно найти и специалистов, готовых предложить свои услуги в данной области.

Дополнительное удобство для злоумышленников представляет тот факт, что во многих случаях радиозакладки не требуют дополнительных источников питания и тем более их замены, т.к. «питаются» от самой телефонной линии. К тому же не надо забывать, что и сами телефонные линии представляют угрозу, т.к. могут использоваться для прослушивания помещений, через которые эти линии проходят за счет различных электромагнитных наводок и излучений.

НЕСАНКЦИОНИРОВАННОЕ ПОДКЛЮЧЕНИЕ К ЛИНИИ И МОШЕННИЧЕСТВО

Мошенничество (toll fraud) наряду с прослушиванием разговоров является одной из самых востребованных хакерами угроз. Осуществляться она может различными путями (достаточно вспомнить телерепортажи о вьетнамских «бизнесменах», организующих пункты дешевой междугородней и международной связи) вплоть до взлома биллинговых систем. Но самым простым и распространенным является несанкционированное подключение к телефонным каналам связи для осуществления звонков за счет ничего неподозревающего абонента. Такого рода действия могут быть осуществлены очень легко – достаточно

подключения спаренного телефона или получения доступа к распределительной коробке. И вот уже за все чужие разговоры платить будете вы, и выставляемые счета могут содержать просто астрономические суммы.

ДРУГИЕ УГРОЗЫ

Существуют и другие, менее распространенные, но не менее опасные угрозы традиционным телефонным сетям. Например, вывод из строя телефонной сети путем наводнения ее огромным числом звонков. Такие проблемы регулярно возникают в канун Нового года, когда телефонные линии раскаляются от желающих поздравить своих родственников и друзей с всенародным праздником. При определенных ситуациях запредельную нагрузку на телефонную сеть может организовать и обычный хакер. Существуют и другие угрозы. Например, перемаршрутизация звонков на другие телефонные номера, сброс собеседника с линии или «прорыв» сигнала «занято». Они более сложны в реализации, но не становятся от этого менее опасными.IP-телефония не защищает от подмены телефонов и серверов управления

СРЕДСТВА ЗАЩИТЫ

Самой простой мерой защиты от прослушивания является следование известной фразе «Это не телефонный разговор». Но к сожалению ее мало кто может воплотить в жизнь. Да и проблему мошенничества и несанкционированного подключения она не решает – нужны специальные технические средства, которые, к счастью, представлены на российском рынке достаточно широко. В первую очередь, это специальные устройства, контролирующие, а зачастую и блокирующие, несанкционированное подключение к телефонным сетям. Эти устройства «ставят» помехи, нейтрализуя тем самым подслушивание разговора. Большинство из них предназначено для защиты только проводных линий и только на участке «телефон-АТС».

Другим классом защитных средств являются сигнализаторы и тестеры, которые определяют наличие на линии посторонних радиоэлементов, присущих устройствам несанкционированного съема информации. Работают они по принципу светофора, сигнализируя красным и зеленым светодиодами состояние телефонной линии: зеленый – «Все чисто, можно разговаривать», красный – «Тревога! Вас подслушивают».

Помимо пассивных средств защиты существуют и активные – генераторы шума и нейтрализаторы. Первые осуществляют зашумление линии, мешая перехватчикам распознавать нормальный человеческий голос. Но с другой стороны, такой способ очень сильно снижает качество переговоров и зачастую делает их попросту невозможными. Более эффективными являются нейтрализаторы, которые создают кратковременное высоковольтное напряжение в канале передачи телефонного сигнала, выводя таким образом из строя несанкционированно (а иногда и санкционировано) подключенные устройства.

Особняком стоят вокодеры (voice coder) и скремблеры, которые осуществляют преобразование передаваемых голосовых данных в «нечитаемый» формат. Одним из способов такого преобразования является шифрование. Очевидно, что такие устройства должны быть установлены у всех участников защищенных переговоров. Выполнены скремблеры могут быть как в виде отдельной «коробочки», устанавливаемой рядом с телефонным аппаратом, так и в виде присадок, накладываемых непосредственно на телефонную трубку. Этот класс защитных средств является наиболее эффективным для защиты телефонных переговоров, независимо от типа используемых каналов связи.

Механизм закрытия голосовых данных может быть встроен в телефон или быть реализован в виде отдельного устройства. В первом случае телефонный аппарат слишком удорожается, во втором – вы становитесь заложником практически полного отсутствия масштабируемости и крайне низкого уровня удобства пользования. Оснастить каждого абонента скремблером или вокодером – задача не из легких, а уж управлять ключами шифрования в такой схеме – тем более. При этом вопрос стоимости также не снимается – цена одного скремблера колеблется от 200 до 500 долларов США (достаточно ввести в поисковой Интернет-системе ключевую фразу «скремблер|вокодер» и вы получите список самых различных коммерческих предложений). Прибавьте сюда стоимость других типов защитных устройств, а также стоимость их установки и вы получите цифру, в 3-5 раз

превышающую стоимость самого телефонного аппарата. И все это для защиты вашей телефонной сети, построенной на традиционных принципах.CallManager незащищен, потому что установлен на платформе Windows

РЕШЕНИЕ ПРОБЛЕМЫ

Можно ли что-то сделать в такой ситуации? Да, можно. Причем необходимо постараться совместить несовместимое – телефонию и безопасность, и сделать это по приемлемой цене. Решением является IP-телефония, совмещающая в себе достоинства обеих ее прародительниц – традиционной телефонии и IP-технологии. Рассмотрим вкратце, как описанные выше угрозы устранены в решениях компании Cisco Systems, которая по данным отчета “WorldWide Enterprise Voice Market: Q2 CY2004” консалтинговой компании Synergy Research Group компания Cisco захватила 4 первых места по продаже различных компонентов IP-телефонии.

Подробно не касаясь деталей реализации самой технологии, отметим, что все защитные технологии уже встроены в любую из моделей Cisco IP Phone 79xx:

- Все телефоны аутентифицируются при подключении к сети, что исключает возможность несанкционированного подключения чужого аппарата. Для подтверждения подлинности телефонов используются протокол RADIUS, сертификаты PKI X.509 и т.д.
- Все переговоры могут защищаться от прослушивания с помощью различных стандартизованных протоколов – IPSec, SecureRTP и т.п.
- Узлы, отвечающие за управление звонками, защищены от DoS-атак, заражения червями, троянскими конями и другими вредоносными программами при помощи антивирусных программ и систем предотвращения атак.
- Управление соединениями (включая сигнализацию) осуществляется в защищенном от несанкционированного доступа виде.
- Телефоны допускают доступ к своим функциям только после предъявления имени и пароля, что предотвращает несанкционированное использование телефонной сети и обеспечивает полную регистрацию всех выполняемых действий, в т.ч. и для целей расследования инцидентов.
- Удобное и эффективное управление правами доступа абонентов к телефонной сети. Например, с помощью интуитивно понятного графического интерфейса можно легко ограничить диапазон номеров, по которым может звонить тот или иной абонент.
- И т.д.

Стоимость использования аналогичных защитных технологий для обычной телефонии составит примерно 600-900 долларов в расчете на один телефонный аппарат. И это без стоимости самого аппарата. А ведь надо не забывать еще и о стоимости внедрения телефонии и устройств ее защиты. Цена же Cisco IP Phone 79xx гораздо меньше указанной суммы. Да и внедрять их гораздо проще. Как говорится, выгода налицо.

ЗАКЛЮЧЕНИЕ

Итак, вы видите, что существующая уже не одно десятилетие традиционная телефония, являющаяся неотъемлемой частью современного бизнеса, к сожалению, не обеспечивает должного уровня защиты переговоров, которые ей доверяются. Разумеется, можно использовать различные «навесные» системы защиты – скремблеры, блокираторы, нейтрализаторы и другие, но в этом случае существенно повышается стоимость владения системой корпоративной телефонии. Гораздо более эффективным вложением средств является внедрение инфраструктуры IP-телефонии, которая не только предлагает доселе невиданные возможности по ведению бизнеса, но и обеспечивает его надежную защиту. При этом защитные функции уже встроены во все компоненты IP-телефонии, начиная от IP-телефонов и голосовых приложений и заканчивая серверами управления и голосовыми шлюзами, а следовательно, не требуют дополнительных затрат на их приобретение и установку.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

IP Communications Security Solution

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_package.html

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

Voice and IP Communications

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

NIST Special Publication 800-24 PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does

http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

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