



White Paper

Sicurezza nelle reti VoIP

Indice

1	La VoIP	3
2	La VoIP in azienda	3
2.1	<i>L'utilizzo di software Client VoIP gratuiti.</i>	3
2.2	<i>L'utilizzo di servizi VoIP di breakin/breakout</i>	3
2.3	<i>La sostituzione del PBX tradizionale</i>	3
2.4	<i>L'introduzione di architetture di PBX trunking</i>	3
2.5	<i>La remotizzazione del PBX, attraverso softswitch VoIP.....</i>	4
2.6	<i>L'introduzione di servizi di Extended Mobility</i>	4
3	Problematiche di sicurezza nelle reti VoIP	4
3.1	<i>Protocolli VoIP.....</i>	5
3.2	<i>Reti VoIP ed architetture di sicurezza tradizionali</i>	5
4	Best Practice di sicurezza nelle reti VoIP	6
5	Conclusioni	7
	Note sul documento.....	8

1 LA VoIP

La rete di telefonia pubblica è una delle reti più antiche ancora operative dato che la sua storia comincia nel XIX secolo con l'invenzione del telefono. Dopo una prima fase di forte innovazione avvenuta negli anni 60-70, la rete telefonica è entrata in una fase di maturità e non ha subito innovazioni di rilievo fino all'inizio degli anni 90.

Proprio gli anni 90 vedono la diffusione a livello mondiale di Internet come reti dati pubblica e, dato che la voce non è nient'altro che un particolare tipo di dati, si è subito pensato di veicolare la voce sulla rete Internet ideando famiglie di protocolli che fanno riferimento ad applicazioni di VoIP (Voice over IP).

L'impatto della VoIP ha determinato un vero e proprio crollo delle tariffe della telefonia di rete fissa dato che il flusso dei dati voce non è particolarmente significativo rispetto alle capacità attuali della rete Internet.

Il trasferimento della Voce su IP presenta però la bassa probabilità di avere in alcuni momenti una qualità inferiore per effetto delle caratteristiche differenti legate alla natura delle reti di telefonia pubblica e di Internet.

Se si accetta una bassa probabilità di avere talvolta un qualità della conversazione vocale magari inferiore a quella della rete telefonica pubblica ma comunque soddisfacente, la VoIP presenta interessanti applicazioni sia in ambito residenziale che in ambito business.

2 LA VoIP IN AZIENDA

Con il progressivo miglioramento della qualità e dell'affidabilità delle applicazioni VoIP, il mercato business si è indirizzato verso queste tecnologie con lo scopo di ridurre i costi complessivi di esercizio soprattutto in un quadro economico come quello attuale dove questa problematica riveste particolare importanza.

Le applicazioni VoIP possono essere introdotte in azienda secondo diverse modalità:

2.1 *L'utilizzo di software Client VoIP gratuiti.*

Skype è la più famosa compagnia al mondo a realizzare comunicazioni VoIP utilizzando un software di peer-to-peer. Il software è disponibile gratuitamente per il download sul sito <http://www.skype.com/> e permette dopo una iscrizione di comunicare gratuitamente con altri utenti che abbiano installato sul PC lo stesso software ed ovviamente siano dotati di casse e microfono (VoIP On-Net).

2.2 *L'utilizzo di servizi VoIP di breakin/breakout*

Un'altra modalità per introdurre applicazioni VoIP in azienda è di utilizzare tecnologie VoIP per effettuare le chiamate dalla rete telefonica privata aziendale verso la rete telefonica tradizionale (PSTN).

In tal caso basta collegare il tradizionale centralino PBX aziendale alla rete IP e collegarsi ad un provider VoIP di servizi di Breakin/Breakout. A tal proposito bisogna ricordare che quando si fa riferimento a questi due termini particolari si intende:

- Breakin Call: la chiamata da rete telefonica a rete IP
- Breakout Call: la chiamata da rete IP a rete telefonica tradizionale

2.3 *La sostituzione del PBX tradizionale*

Una modalità per introdurre tecnologia VoIP in azienda è anche quella di sostituire o estendere il centralino telefonico tradizionale (PBX) con un nuovo centralino in tecnologia VoIP (softswitch), che in realtà non è nient'altro che un server entry-level su cui vengono installati applicativi di gestione centralini.

2.4 *L'introduzione di architetture di PBX trunking*

Il PBX Trunking è un'applicazione delle tecnologie VoIP che prevede l'utilizzo di softswitch VoIP con architetture analoghe a quelle necessarie per utilizzare servizi di Breakin/Breakout. In questo caso sfruttando la rete IP

aziendale che collega in VPN le varie sedi dell'azienda vengono sostituiti o affiancati ai centralini tradizionali posti nelle varie sedi gateway con schede PBX o router che:

- instradano le chiamate tra le sedi all'interno della rete IP
- fanno uscire le chiamate esterne sulla rete tradizionale dal punto più conveniente massimizzando le chiamate urbane e minimizzando quelle interurbane

2.5 La remotizzazione del PBX, attraverso softswitch VoIP

Un caso particolare delle architetture di PBX trunking è la remotizzazione del PBX. In questa architettura vengono infatti eliminati dalle varie sedi i PBX tradizionali ed attraverso IP phone gli utenti sono collegati direttamente al softswitch posto nella sede centrale attraverso la rete IP aziendale.

2.6 L'introduzione di servizi di Extended Mobility

Una evoluzione delle architetture di remotizzazione del PBX è rappresentata dalle architetture di Extended Mobility. In questo caso sfruttando architetture VoIP abbinata a infrastrutture di VPN con Client mobili è possibile realizzare di fatto un ufficio mobile.

Il singolo utente infatti accedendo alla VPN aziendale, diventa in pratica un utente della LAN aziendale anche dal punto di vista dei servizi VoIP e quindi può essere raggiungibile tramite il suo numero di telefono ovunque si trova (in viaggio, a casa, ecc...).

3 PROBLEMATICHE DI SICUREZZA NELLE RETI VOIP

Come accade con molte nuove tecnologie, la VoIP introduce in azienda sia opportunità che rischi legati alla sicurezza. Costi inferiori e maggiore flessibilità sono tra le promesse della VoIP nelle aziende, ma la tecnologia presenta ai Security Administrator molte sfide nell'ambito della sicurezza.

Dato che la voce viaggia in pacchetti IP i Security Administrator potrebbero erroneamente pensare che inserendo il traffico voce nella loro rete IP la rete rimarrà sicura. Sfortunatamente la VoIP aggiunge un numero elevato di elementi e di complicazioni alla tecnologia di networking esistente determinando così anche problemi legati alla sicurezza.

Le reti VoIP prevedono una ampia varietà di apparati che includono i normali apparecchi telefonici, le unità di audio conferenza e gli apparati mobili. Oltre ai terminali utente, le reti VoIP includono un'ampia varietà di altri componenti, quali:

- softswitch
- gateway
- router
- firewall.

Gran parte di questi componenti sono presenti nelle normali reti dati, ma le richieste di performance della VoIP possono determinare la necessità di aggiornamento del software e dell'hardware di networking.

L'implementazione di alcune misure di sicurezza può causare un marcato deterioramento della QoS, per effetto dei delay o dei blocchi delle chiamate prodotti dai firewall, oppure della latenza e del jitter (variazione del delay) introdotto dalla cifratura.

A causa della natura time-critical della VoIP ed alla sua bassa tolleranza alla perdita di pacchetti, molte misure di sicurezza implementate nelle reti dati tradizionali potrebbero essere semplicemente non applicabili alle reti VoIP nella loro forma attuale.

3.1 Protocolli VoIP

Gli attuali sistemi VoIP usano o un protocollo proprietario o due standard, H.323 e il SIP (Session Initiation Protocol). In aggiunta a SIP ed H.323 ci sono anche altri standard, MGCP, IAX2 e Megaco/H.248, che possono essere usati in implementazioni estese di gateway VoIP.

Questi standard possono essere usati per facilitare la trasmissione di messaggi tra i gateway e d'altro canto possono facilmente essere usati per implementare terminali senza alcuna intelligenza, in modo analogo ai telefoni attuali collegati ad un centralino PBX.

Benché sembri che il SIP stia guadagnando popolarità, nessuno di questi protocolli è già diventato predominante sul mercato. Infatti i maggiori vendor, incluso Cisco, IBM, Microsoft, Novell, e SUN stanno investendo una frazione sempre maggiore delle loro risorse nello sviluppo di prodotti SIP. Una estensione di SIP, il SIP per Instant Messaging e Presence Leveraging Extensions (SIMPLE), è incorporato in molti prodotti che supportano l'Instant Messaging.

3.2 Reti VoIP ed architetture di sicurezza tradizionali

Le reti VoIP fanno dipendere la loro gestione da un ampio numero di parametri configurabili:

- gli indirizzi IP e MAC dei terminali voce
- gli indirizzi IP di router e firewall
- i parametri di alcuni software specifici VoIP come i Softswitch
- i parametri di altri programmi utilizzati per realizzare l'instradamento delle chiamate.

Molti di questi parametri di rete sono stabiliti dinamicamente ogni volta che il componente di rete subisce un restart, o quando un telefono VoIP è riavviato o aggiunto alla rete.

Dato che sono presenti in una rete VoIP così tanti punti con parametri configurati dinamicamente, esiste una vasta scelta di punti potenzialmente vulnerabili ad un attacco.

3.2.1 SICUREZZA FISICA

Le aziende dovrebbero fare attenzione al fatto che i controlli fisici rivestono una particolare importanza in un ambiente VoIP e dovrebbero comportarsi adeguatamente.

A meno che la rete VoIP non sia cifrata, chiunque fisicamente all'interno della LAN dell'ufficio può potenzialmente connettersi alla rete un tool di monitoraggio ed intercettare le conversazioni.

Sarebbe opportuno che le aziende si assicurino della presenza di adeguate misure di sicurezza fisica e restringano l'accesso ai componenti della rete VoIP. Le misure di sicurezza fisica, inclusive di barriere, lucchetti, sistemi di controllo degli accessi e guardie sono quindi le prime linee di difesa.

3.2.2 I FIREWALL

I firewall sono l'elemento base di sicurezza nella attuali reti IP e solitamente sono la prima linea di difesa nel caso si voglia proteggere una LAN, una WAN, una DMZ o un singolo computer. I firewall lavorano bloccando il traffico giudicato invasivo/intrusivo in base da un set di regole programmate all'interno del firewall stesso.

L'introduzione di firewall in una rete VoIP complica notevolmente le cose, principalmente per effetto delle procedure di setup delle chiamate e del fatto che il traffico VoIP avviene su porte allocate dinamicamente.

Per tali ragioni sarebbe opportuno adottare firewall SIP-aware in grado di tracciare lo stato delle connessioni e di respingendo i pacchetti che non fanno parte della chiamata originaria.

3.2.3 IL NAT

Il NAT (Network Address Translation) è uno strumento che può essere utilizzato per fornire sicurezza ad una LAN e per abilitare la condivisione dello stesso indirizzo IP da parte di molteplici end-point.

I benefici del NAT si attuano però ad un prezzo. Ad esempio, un tentativo di fare una chiamata dall'esterno verso la rete interna diventa molto complesso quando è presente il NAT, dato che crea una situazione del tutto analoga ad una rete fonia dove parecchi telefoni hanno lo stesso numero di telefono (ad esempio una casa con molteplici apparecchi telefonici).

Benché l'uso del NAT possa essere ridotto con l'introduzione dell'IPv6, il NAT rimarrà una componente comune delle reti per gli anni avvenire, e per questa ragione i sistemi VoIP devono avere a che fare con la complessità determinata dal NAT.

3.2.4 CIFRATURA

Firewall, Gateway ed altri dispositivi analoghi possono contribuire ad evitare che persone esterne compromettano la rete. Un altro livello di difesa sarebbe utile per proteggere i dati stessi. Nella VoIP, come nelle reti dati, questo può essere realizzato criptando i pacchetti a livello IP usando IPSec o a livello trasporto usando RTP sicuro (RFC3243).

Il problema è che parecchi fattori, quali l'espansione della dimensione dei pacchetti, la latenza nella cifratura e la mancanza di QoS nel motore di cifratura possono causare una eccessiva quantità di latenza nella trasmissione dei pacchetti VoIP.

Questo determina un degrado nella qualità della voce e sottolinea ancora una volta il trade-off tra security e qualità della voce.

In alcuni casi può accadere che il traffico VoIP venga veicolato in chiaro su una rete MPLS che prevede l'utilizzo di una infrastruttura di backbone condivisa dal carrier su molteplici utenti.

Il protocollo MPLS, come ogni protocollo, genera degli overhead di trasmissione che variano il dimensionamento complessivo della rete. In particolare l'MPLS determina un aumento del traffico per effetto della label MPLS che incide mediamente per il 19% sul traffico VoIP.

4 BEST PRACTICE DI SICUREZZA NELLE RETI VOIP

Il progetto, l'implementazione e la gestione di una rete VoIP sicura è uno sforzo complesso che richiede una attenta pianificazione. L'introduzione di applicazioni VoIP in una rete già congestionata e sottodimensionata potrebbe essere problematica per l'infrastruttura tecnologica di una azienda.

A causa dell'integrazione di voce e dati su una singola rete, il mantenimento di una rete VoIP sicura richiede uno sforzo maggiore rispetto a quanto richiesto da una rete solo dati.

Non c'è nessuna soluzione facile ed univoca alle criticità evidenziate precedentemente. Ogni azienda deve cercare attentamente con l'ausilio di esperti di VoIP e di sicurezza ICT quale è la soluzione migliore in base alla propria infrastruttura di rete.

In particolare si potrebbe partire con alcune linee guida di carattere generale, riconoscendo che le situazioni reali possono richiedere aggiustamenti:

- Sarebbe opportuno separare voce e dati su reti logicamente differenti. Dovrebbero essere usate per traffico voce e per il traffico dati differenti sottoreti con blocchi separati di indirizzi RFC1918 e con server DHCP separati per ciascuna.
- Sarebbe opportuno usare strong authentication e controllo degli accessi a livello del gateway che si interfaccia con la rete PSTN. Dato che la strong authentication dei Client sul gateway è spesso molto difficile, potrebbero essere utili meccanismi di controllo degli accessi e tecniche di policy enforcement.
- Sarebbe opportuno usare firewall progettati per il traffico VoIP. I filtri Stateful possono tracciare lo stato delle connessioni, respingendo i pacchetti che non fanno parte della chiamata originaria.
- Sarebbe opportuno usare IPSec o Secure Shell (SSH) per tutta la gestione remota. Se risulta fattibile converrebbe evitare del tutto la gestione remota e realizzare l'accesso all'IP PBX da un sistema fisicamente sicuro.

- Sarebbe opportuno utilizzare la cifratura IPSec a livello router e non a livello endpoint se la performance è un problema. Dato che alcuni endpoint VoIP non sono sufficientemente potenti da realizzare la cifratura, potrebbe risultare conveniente introdurre la cifratura in un punto centrale che garantisca che tutto il traffico VoIP in uscita dall'azienda venga cifrato.

5 CONCLUSIONI

La VoIP può fornire un servizio voce più flessibile, ma ci sono significativi trade-off che devono essere considerati. I sistemi VoIP sono più vulnerabili di sistemi telefonici convenzionali, in parte perché sono collegati alla rete dati e determinano debolezze addizionali in termini di sicurezza.

Tecnologie emergenti e mancanza di security practice potrebbero causare un controllo insufficiente e poca comprensione dei rischi. Per tale ragione sarebbe opportuno che le aziende considerino attentamente:

- il loro livello di conoscenza e di addestramento sulle tecnologie,
- la maturità delle security practice, dei controlli e delle policy,
- la qualità delle architetture,
- la comprensione dei rischi di security.

La confidenzialità e la privacy potrebbero essere un grande rischio nei sistemi VoIP a meno che non vengano implementati e mantenuti forti controlli. A causa della vulnerabilità intrinseca della fonia su una rete a pacchetto, le reti VoIP dovrebbero prevedere un insieme di sistemi di sicurezza.

Le security policy dell'organizzazione dovrebbero prevedere che questi sistemi siano utilizzati. In particolare sarebbe opportuno adottare come componenti in una rete VoIP sicura firewall compatibili con la VoIP ed altri meccanismi di protezione quali la cifratura dei dati.

Una preoccupazione addizionale potrebbe essere la relativa instabilità della VoIP comparata con i sistemi di fonia tradizionali per effetto dell'affidabilità delle reti a pacchetto su cui transita la VoIP. La rete telefonica pubblica è ultra-affidabile contrariamente alla rete IP che è generalmente molto meno affidabile. I servizi telefonici di base potrebbero essere soggetti a grandi rischi se basati sulla VoIP, a meno che non vengano accuratamente progettati, implementati e gestiti.

Particolare attenzione dovrebbe essere prestata anche ai servizi di emergenza dato che il servizio di localizzazione automatico in alcuni casi non è disponibile con la VoIP. Infatti contrariamente a connessioni telefoniche tradizionali, che sono collegate a locazioni fisiche, la rete a pacchetto VoIP permette ad un certo numero di telefono VoIP di essere ovunque. Questo è un vantaggio per gli utenti, dato che le chiamate possono essere inoltrate automaticamente verso la loro locazione fisica. Il trade-off è però che questa flessibilità complica notevolmente la fornitura dei servizi di emergenza, che normalmente forniscono la localizzazione del chiamante all'ufficio che gestisce la singola chiamata.

NOTE SUL DOCUMENTO

INFORMAZIONE SUL COPYRIGHT

Il presente documento è Copyright (2004) di I.NET S.p.A. – BT; è stato redatto da Stefano Quintarelli; è stato concesso in distribuzione gratuita a CLUSIT – Associazione Italiana per la Sicurezza Informatica. Tutti i diritti riservati.

Il documento può essere chiesto in formato elettronico a CLUSIT – Associazione Italiana per la Sicurezza Informatica all'indirizzo di posta info@clusit.it.

RIPRODUZIONE PARZIALE

Porzioni del presente documento possono essere riprodotte liberamente esclusivamente in presenza della INFORMAZIONE SUL COPYRIGHT riportata al paragrafo precedente.

RIPRODUZIONE INTEGRALE

Può essere ridistribuito liberamente in forma cartacea integrale, forma elettronica integrale e può essere riprodotto integralmente liberamente esclusivamente in presenza della presente nota sul Copyright.

ALTRI USI

Altri usi possono essere concessi previa autorizzazione esplicitamente concessa e da richiedersi all'indirizzo di posta elettronica comunicazione@inet.it.

INFORMAZIONI SULL'AUTORE

Stefano Quintarelli (s.quintarelli@inet.it) è Socio Fondatore e Direttore della Pianificazione Strategica di I.NET S.p.A. (parte di BT), e Socio Fondatore di CLUSIT – Associazione Italiana per la Sicurezza Informatica.

Si è occupato di sicurezza informatica a partire dal 1987 quale consulente di grandi aziende e di istituti bancari, come promotore e coordinatore di vari gruppi di lavoro in tema di sicurezza presso l'Università degli Studi di Milano.

E' stato "Assistano Sysop" dell'allora Bulletin Board di John McAfee, ha collaborato con Steve Chang fondatore di Trend Micro, si è quindi occupato di Network Security, fino alla fondazione di I.NET S.p.A.

Ha partecipato, coordinato e organizzato numerosi corsi, convegni e seminari sulla sicurezza informatica sia in ambito nazionale che internazionale; è autore di libri e pubblicazioni specialistiche.