

## WHITE PAPER

GIUGNO 2008

TELEFONIA E INTERNET

# CONVERGENZA SOTTO CONTROLLO

In Europa Occidentale un'azienda su tre si sta informando su questa opportunità. Le infrastrutture di rete, i server, i client, saranno tutti coinvolti in questa evoluzione. Security e QoS (la qualità del servizio in senso specifico) sono gli elementi essenziali per muoversi con successo verso l'integrazione di IP e telefonia.

**ARKON**  
NETWORK SECURITY



ADAPTIVE SECURITY



# PROTEZIONE CONTRO LA VULNERABILITÀ DELLA TELEFONIA INTERNET

## È NECESSARIO AVERE IDEE CHIARE SULL'EVOLUZIONE DEL MERCATO E DELLE TECNOLOGIE

**I**n Europa, meno di due imprese su dieci utilizzano tecnologie VoIP – Voice over Internet Protocol. Solo la metà delle centraline attualmente in uso comunque sono in grado di supportare la connettività IP in affiancamento alla telefonia tradizionale.

La coesistenza fra i sistemi voce tradizionali (telefonia TDM - Time Division Multiplexing -) e VoIP, iniziata da poco, è destinata a durare parecchi anni. Il processo evolutivo potrà essere attuato centralmente, oppure potrà essere demandato all'esterno ad un operatore pubblico, oppure, ancora, l'impresa potrà realizzare sistemi misti. È proprio questo il terreno su cui si attua la convergenza fra telefonia e IP, centrata su centraline (PBX) con funzionalità di gestione delle chiamate (CTI, ACD, unified messaging), telefoni tradizionali (sia fissi che mobili) e softphones, cioè client software telefonici installati su PC.

I fornitori di apparecchiature e gli integratori di sistemi provengono da due culture tecnologiche distinte: il mondo della telefonia (voce), basato su numerosissimi protocolli specifici e il mondo dell'informazione digitale (dati), fondato sull'operatività integrata di apparecchiature di fornitori disparati, supportate da frequenti aggiornamenti del soft-

ware. Per le applicazioni VoIP, sono stati adottati diversi protocolli, come HTTP o alcuni protocolli proprietari. Per tutte queste ragioni, la protezione della telefonia IP richiede l'analisi approfondita di protocolli e pacchetti, e non può essere limitata al semplice controllo e filtraggio delle porte e degli indirizzi IP, cioè nel modo in cui operano i firewall tradizionali.

Le vulnerabilità VoIP devono essere risolte sia internamente che esternamente, senza rinunciare a funzionalità e protezioni di base, quali: gruppi di continuità (UPS), linee telefoniche di backup, ridondanza sugli elementi critici e sulle connessioni alla rete pubblica.

### PROTEZIONE FULL SPECTRUM

La protezione della convergenza richiede un approccio a quattro livelli distinti. In primo luogo: tenere sotto controllo un sistema VoIP. Il traffico di rete deve essere gestito e segmentato per tipologia. Il traffico voce "ufficiale" gestito dalle centraline aziendali, deve essere separato da quello gestito tramite strumenti e protocolli "non ufficiali", tipo Skype. È necessario quindi analizzare in profondità il contenuto di pacchetti IP.

Secondo elemento, la reattività: il sistema



#### GESTIONE DEL TRAFFICO

*Le funzionalità ad altissimo livello delle appliance Arkoon 360 consentono di analizzare e filtrare tutto il traffico delle reti convergenti VoIP. Il traffico viene segmentato tramite l'applicazione di regole predefinite, le chiamate illecite vengono troncate o bloccate in piena interattività con le centraline telefoniche aziendali, politiche di QoS e di security possono essere implementate a livello aziendale. Il traffico VoIP "intersite" viene incanalato in tunnel VPN per ulteriore sicurezza e le centraline PBX remote possono essere altresì facilmente controllate: questo consente l'applicazione e la diffusione di politiche di sicurezza coerenti ad ogni livello dell'azienda.*



deve essere in grado di interrompere le chiamate in uscita e in entrata nella fase stessa in cui sono generate o ricevute: un problema che si verifichi a livello autenticazione, ad esempio, o la modifica del codec durante una chiamata possono rappresentare un rischio grave in termini di sicurezza.

Terzo aspetto: la "co-operative security". L'informazione deve poter essere scambiata in tempo reale fra nucleo infrastrutturale di rete e centraline telefoniche e loro periferiche, al fine di bloccare chiamate illecite, spamming, war dialing, ecc.

Infine, occorre implementare politiche di qualità del servizio (QoS) che assicurino una appropriata priorità al traffico VoIP. Questo, tuttavia, potrà avvenire solo quando siano stati adeguatamente risolti i problemi di sicurezza, in modo da assicurare che la QoS sia applicata esclusivamente al traffico VoIP autorizzato e solo ad esso ne siano dedicati i benefici.

# CONVERGENZA VOCE-DATI: LE SETTE MINACCE DA NEUTRALIZZARE

UNA VOLTA IDENTIFICATE CHIARAMENTE LE VULNERABILITÀ, LA CONVERGENZA VOCE-DATI POTRÀ ESSERE CORRETTAMENTE PIANIFICATA E GESTITA

L'integrazione fra la telefonia tradizionale e le infrastrutture ed i servizi Internet apre la strada verso interessanti nuove opportunità per le aziende. La riduzione dei costi delle comunicazioni può essere felicemente combinata con produttività ed efficienza maggiori, ad esempio tramite il consolidamento operativo dei call center nella gestione interna. L'integrazione VoIP offre una maggiore flessibilità in quanto garantisce la connessione continua fra azienda e collaboratori, sia che operino on site, da home office o "on the road". Strumenti di gestione delle presenze assicurano che le chiamate raggiungano automaticamente i destinatari, ovunque questi si trovino: tramite linee telefoniche fisse o mobili o tramite i softphones installati sui loro PC. Questo significa maggiore interattività, garanzia di risposta e maggiore efficienza.

Sia nel caso di trasloco in una nuova sede o dovendo sostituire le centraline telefoniche non più in grado di rispondere alle loro esigenze, un numero sempre maggiore di aziende prendono in considerazione le soluzioni VoIP. Tuttavia, la convergenza voce - dati - solleva un nuovo interrogativo: come



La "voce" deve essere considerata un'applicazione critica e le aziende devono considerare la voice security allo stesso livello di serietà con cui proteggono la sicurezza di altre applicazioni. Al fine di garantire una comunicazione "voce" sicura e affidabile è vitale disporre di infrastrutture affidabili e semplici da gestire. I miglioramenti in termini di sicurezza devono procedere di pari passo con i miglioramenti nella QoS.

minimizzare i rischi per la sicurezza, insiti nella telefonia IP? Un insieme di vulnerabilità (riportate nella tabella qui sotto) costringe l'azienda ad adottare misure adeguate per prevenirle. L'analisi accurata dei rischi e del loro potenziale impatto sull'attività aziendale è indispensabile per identificare le risposte appropriate. Possono essere identificate tre categorie di minacce: abuso delle infrastrutture, ad esempio in caso di chiamate non autorizzate; tentativi di intrusione, ivi compresi gli attacchi ini-

bitori dell'attività (DoS, Denial of Service); furto di informazioni, ivi compresi lo spionaggio sulle comunicazioni e il furto di directories. La specializzazione di Arkoon è la sicurezza: Arkoon è in grado di assicurare un percorso sicuro e controllato nella migrazione VoIP, senza compromettere gli investimenti pre-esistenti. L'approccio multilayer di Arkoon garantisce una convergenza voce-dati sicura, eliminando i rischi di intrusione, DoS o fuoriuscite indebite di informazioni.

## LA PRIMA APPLIANCE UTM VOCE-DATI AL MONDO

Arkoon offre una gamma completa di appliance di sicurezza UTM pronte per l'utilizzo VoIP

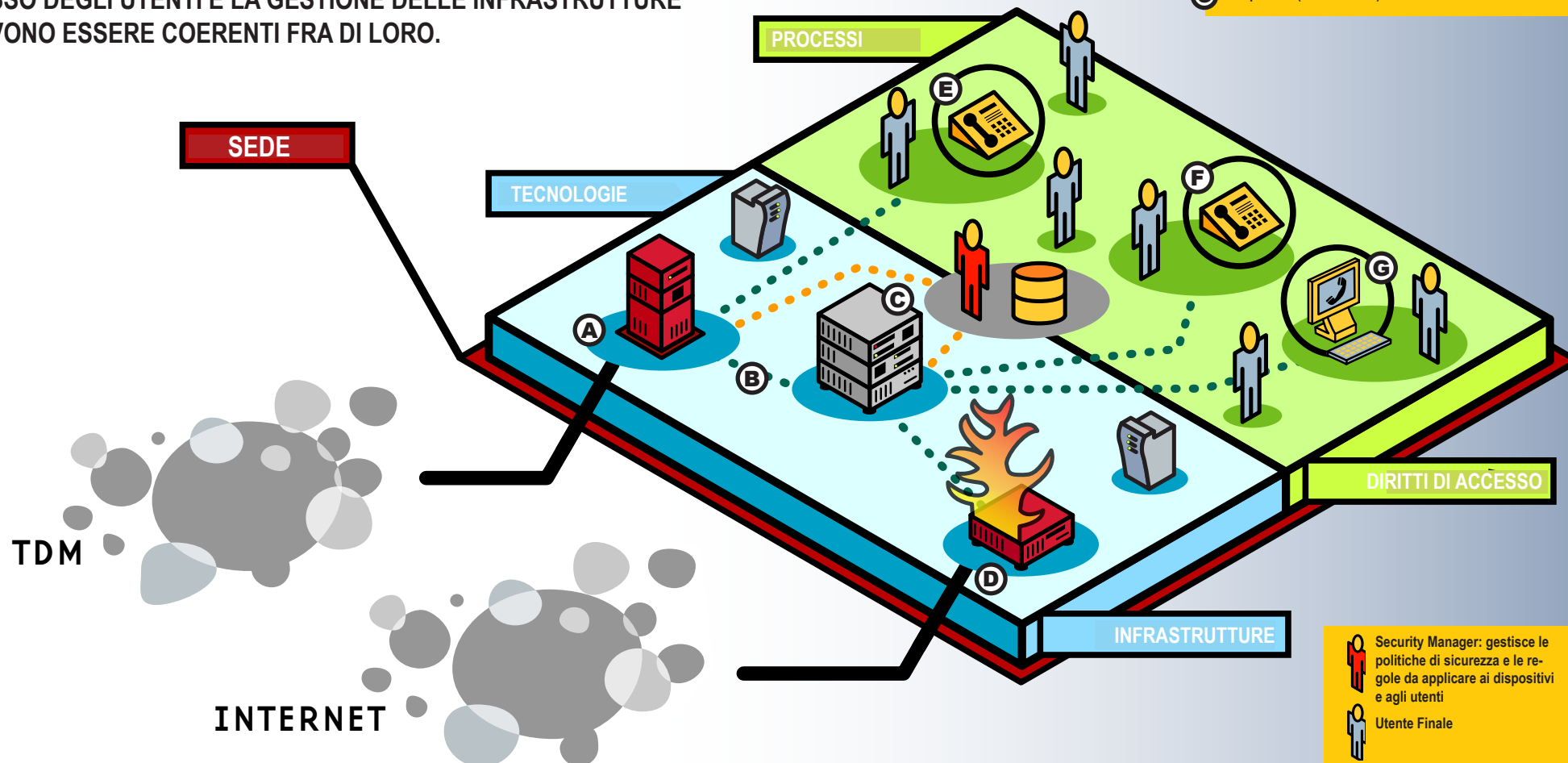


MINACCE	TARGET	VISIBILITÀ	IMPATTO	PREREQUISITI	DIFESE
Denial of Service	I, S	Yes	Qualità del servizio telefonico	Connessione PBX	Firewall + IDPS
Furto di identità	I, S	No	Integrità della comunicazione	Directory	Autenticazione
Pirattaggio "voice mail"	S, C	No	Integrità della comunicazione e/o riservatezza	Filtraggio del traffico	Autenticazione, firewall a livello applicazione
Furto di directory	I, S, C	No	Riservatezza	Filtraggio del traffico	Autenticazione, firewall a livello applicazione
SPIT (Spam over IP Telephony)	I, S, C	Yes	Livello di servizio telefonico, riduzione della produttività	Connessione PBX	Autenticazione, firewall a livello applicazione, IDPS
Abusi nelle applicazioni	S, C	No	Perdita di controllo, drenaggio di risorse	Stesura di politiche di sicurezza	Firewall a livello applicazione
Abuso di infrastrutture	I	No	Perdita di controllo, riservatezza	Gestione basata sul ruolo aziendale degli utenti	Auditing, firewall a livello applicativo

\* I = Infrastructures, S = Services, C = Contents

# GESTIONE INTEGRATA DELLE RISORSE INFRASTRUTTURALI E DIRITTI DEGLI UTENTI

COMUNICAZIONI VOCE-DATI SICURE PRESUPPONGONO POLITICHE GESTIONALI APPROPRIATE. LE PRIORITÀ, I DIRITTI DI ACCESSO DEGLI UTENTI E LA GESTIONE DELLE INFRASTRUTTURE DEVONO ESSERE COERENTI FRA DI LORO.



# TRE PASSI OBBLIGATI PER PROTEGGERE AD OGNI LIVELLO LE COMUNICAZIONI

PROCESSI BEN DEFINITI, MONITORAGGIO E GESTIONE DELLA RETE, E UNA STRATEGIA DI SEGMENTAZIONE RAFFORZANO LA SICUREZZA DELLE INFRASTRUTTURE AZIENDALI, PROTEGGENDONE LA COMUNICAZIONE

1

## POLITICA UTENTI



La sicurezza è un processo che inizia dalla stesura di politiche aziendali adeguate e dalla loro diffusione nell'azienda. Questo può avvenire in tre stadi distinti. Il primo passo deve essere la definizione di politiche che tengano conto dei singoli ruoli nell'ambito aziendale. I dirigenti di alto livello, i manager commerciali o i responsabili delle produzioni hanno esigenze differenziate. Certi utenti hanno l'esigenza di accedere ad applicazioni specifiche o a risorse condivise, oppure devono poter fare in qualsiasi momento chiamate di lavoro, verso postazioni fisse o mobili, nazionali o internazionali. Sulla base di ruoli-utente chiaramente definiti e strutturati, la politica di sicurezza è in grado di stabilire chi può effettuare chiamate verso quali utenti e quando, dove, come effettuarle. Da questo primo passo, fondamentale e irrinunciabile, inizia la sicurezza aziendale nella telefonia.

2

## POLITICA GESTIONALE

Il responsabile del sistema informativo seleziona collaboratori e infrastrutture secondo criteri che gli garantiscano il pieno raggiungimento degli obiettivi aziendali, riferibili alla sua responsabilità specifica. Deve decidere a chi affidare i diritti di accesso per la gestione del sistema, e precisamente: chi ha accesso a quali apparecchiature, a quale livello, durante quale orario, ecc. Questo passo è altrettanto fondamentale per la sicurezza delle comunicazioni dell'azienda: richiede la definizione delle regole comportamentali dell'utente, ma può comportare altresì restrizioni in termini di accesso e utilizzazione di apparecchiature o risorse. Una politica chiara e precisa risulterà nel raggiungimento di un maggior livello di fiducia sui livelli di servizio attesi da parte degli utenti, parallelamente ad un maggior rispetto delle regole che li assicurano.



3

## POLITICHE DI SEGMENTAZIONE



I network aziendali sono in continua trasformazione per effetto della convergenza voce-dati, ma soprattutto per effetto dell'integrazione tra servizi informatici, Internet e telefonia. La segmentazione del network mediante tecnologie di sub-netting o VLAN consente di contenere lo spazio richiesto dallo scambio di informazioni tra gruppi predefiniti di utenti, alleggerendo il carico sulla banda larga. Un approccio simile permetterà di isolare il traffico "voce" autorizzato da quello "non ufficiale", e di raggiungere il massimo livello di sicurezza e riservatezza nei servizi "ufficiali". Le regole previste dalle politiche aziendali relative agli utenti, alla gestione e alla segmentazione devono essere rigorosamente implementate e rispettate a livello di ogni elemento della infrastruttura del network.

## SEGMENTARE POI OTTIMIZZARE IL TRAFFICO



**NICOLAS BÉLAN,**  
Program Manager Convergence  
di Arkoon

La motivazione più immediata secondo la maggior parte delle aziende che optano per il VoIP è la riduzione dei costi. La sicurezza verrebbe dopo. In realtà, la sicurezza dovrebbe essere la loro prima preoccupazione. Iniziando con la segmentazione della rete, poi ottimizzando il traffico. Altrimenti il miglioramento andrà anche a beneficio del traffico indesiderato e potenzialmente pericoloso. Il traffico VoIP deve essere tenuto separato dal traffico dati: i due mondi non hanno le stesse esigenze. Il traffico voce, contrariamente al traffico email, deve avere una latenza "end to end" molto bassa. Nell'implementazione di sistemi di convergenza è essenziale evitare di mescolare i problemi di sicurezza dei due mondi. Le appliance Arkoon riconoscono il traffico VoIP, segmentano e dunque gestiscono appropriatamente il traffico nei network aziendali. E' altrettanto importante implementare e gestire una politica di sicurezza a livello azienda..

# OPERATORI MOBILI E LAVORATORI HOME OFFICE SEMPRE RAGGIUNGIBILI

COME RISPONDERE ALLE CHIAMATE CHE ARRIVANO IN UFFICIO QUANDO SI È FUORI O QUANDO SI LAVORA DA CASA? ARKOON E PANASONIC HANNO LA RISPOSTA.

**N**el panorama competitivo odierno le aziende hanno l'esigenza di garantire comunicazioni sicure, pur mantenendo la necessaria reattività verso la clientela e il costante miglioramento del servizio. La telefonia IP può fornire una risposta a queste esigenze potenzialmente conflittuali. Con il VoIP, gli operatori mobili sono raggiungibili telefonicamente come se fossero in ufficio. Inoltre, i sistemi VoIP garantiscono economie di scala: i sistemi informativi e i sistemi telefonici convergono e si combinano negli stessi centri di costo. Con un adeguato livello di sicurezza, il VoIP mette l'azienda in condizioni di rispondere più rapidamente e con maggiore accuratezza alle aspettative di clienti e collaboratori.

Panasonic offre una linea centraline IP e di soluzioni di connettività per operatori remoti, due fondamenti della telefonia IP. "Dato per scontato che il VoIP è un mercato condizionato dagli operatori, il nostro target di mercato è rappresentato da imprese da 10 a 200 utenti: a queste Panasonic offre la possibilità di investire gradualmente" spiega Laurent Poirot, Business Manager PBX di Panasonic France. Ed aggiunge che la sicurezza, e più precisamente l'identificazione sicura e affidabi-

le degli utenti, è il parametro essenziale nell'implementazione di sistemi VoIP. Una volta identificato l'utente, il sistema, ad esempio, può mettergli a disposizione la storia completa dei contatti, commerciali o tecnici, avvenuti con l'autore della chiamata. Ovviamente queste informazioni devono essere disponibili solo ad utenti fidati e autorizzati, siano essi locali o remoti. "Troppo spesso ignorata, la sicurezza è in effetti un elemento cruciale per la telefonia IP", aggiunge Poirot.

Per integrare le applicazioni informatiche con la telefonia IP, il telefono IP può essere collegato alla LAN, mediante la porta USB del PC, configurazione questa definita "first party" da Panasonic. La configurazione alternativa, "third party" utilizza una porta Ethernet per ogni client device, e presuppone la riconfigurazione della LAN. In entrambi i casi devono essere presi in considerazione gli aspetti relativi alla sicurezza.

In qualità di partner di fornitori chiave di soluzioni CRM (Content Rights Management), Panasonic possiede il know-how per implementare l'interfaciamento fra i CRM e le centraline PBX, che saranno viste come client in rete. I protocolli TAPI 2 e CSTA sono di serie nelle configurazioni di base di tutta la



Processi critici, quali logistica, CRM, servizi diconsegna, sono sempre più dipendenti dalla telefonia IP e, nei sistemi convergenti, l'autenticazione dell'utente è essenziale. Per garantire un rapido ritorno degli investimenti il VoIP deve poter supportare lo scambio di informazioni dati-voce, inoltrare chiamate dati dei clienti, e offrire all'utente remoto una gamma appropriata di funzionalità. Le soluzioni di sicurezza Arkoon supportano integralmente le centraline PBX IP e i server preposti alla convergenza: in questo modo viene garantita la reattività in tempo reale, in coerenza con le priorità aziendali.

LAURENT POIROT

Manager, PBX  
Systems Division,  
Panasonic France



linea di prodotti PBX, fino al modello KX-TDA 600 in grado di gestire le comunicazioni di siti con fino a 1000 utenti.

"Le imprese nel mondo occidentale cercano strade per migliorare reattività, competitività e mobilità. Il VoIP risolve il problema dei collaboratori a distanza". Risolve inoltre i problemi relativi ai fusi orari, permettendo alle aziende di dislocare in modo trasparente il call center a livello globale per rispondere 24 ore su 24 alle esigenze della clientela.

Nelle grandi catene di alberghi, gli strumenti CRM ottimizzano la gestione dei clienti. In altre situazioni il VoIP assicura il collegamento costante degli operatori, fissi o mobili, nella infrastruttura telefonica aziendale, che sono immediatamente in grado di rispondere alle esigenze dei clienti. In qualche caso un server "voce" interattivo con le risorse remote dell'azienda viene previsto nel setup della telefonia IP. Mediante l'inserimento della tecnologia di sicurezza Arkoon, sia le centraline IP PBX sia i servizi aggiuntivi ottenibili con il VoIP beneficeranno dello stesso livello di sicurezza e protezione, tipico di servizi IP più tradizionali.

# GLOSSARIO VOIP

**DoS:** denial of service. Attacco che provoca l'inibizione o il blocco dell'attività operativa

**DMZ:** De-Militarized Zone. Rete separata e protetta dal firewall, in cui sono installati i server, accessibile dall'esterno o dall'interno dell'azienda.

**FIRECONVERGE:** Interfaccia sviluppata da Arkoon per consentire alle appliance di sicurezza Arkoon di scambiare dati con le piattaforme telefoniche per una integrazione completa della sicurezza su voce e dati.



**H.323:** standard ITU, uno dei primissimi protocolli VoIP di larga diffusione.

**IETF:** Internet Engineering Task Force. L'organizzazione per la stesura e la gestione degli standard delle comunicazioni via Internet. Gli standard IETF sono diffusi come "RFCs" (Request For Comments)

**IPBX:** Internet Protocol Private Branch Exchange. Centralina telefonica IP.

**ITU:** International Telecommunication Union. Il principale organismo internazionale per la stesura degli standard di telefonia e telecomunicazioni.

**MGCP:** Media Gateway Control Protocol. Noto anche come Megaco (IETF) o H.248 (ITU), è un protocollo di segnalazione asimmetrica per le comunicazioni IP multimediali.

**PBX:** Private Branch Exchange. Centralina telefonica privata.

**QoS:** Quality of Service. Qualità del servizio, intesa come possibilità di predefinire, per un determinato flusso di dati, i parametri funzionali quali: larghezza di banda, throughput, error rate ecc. È supportata solo nelle appliance di rete più sofisticate.

**RTCP:** Real-Time Transfer Protocol. Protocollo di controllo del flusso progettato per garantire un'adeguata QoS nelle comunicazioni in tempo reale.

**SIP:** Session Initiation Protocol. Protocollo simmetrico per la "negoiazione" di un canale di comunicazione bidirezionale fra due apparecchiature IP.

**SOFTPHONE:** Software che, installato su PC, abilita quest'ultimo all'utilizzo come telefono IP.

**SPIT:** Spam over IP Telephony. Chiamate o messaggi indesiderati sulla telefonia IP.

**TDM:** Time Division Multiplexing. Tecnologia di comunicazione propria della telefonia tradizionale. Termine usato genericamente in riferimento a tutti gli aspetti della telefonia tradizionale (Non-IP).

**ToIP:** (Sophie, this doesn't exist in Italian)

**UTM:** Unified Threat Management. Termine coniato dalla società di consulenza del mercato informatico IDC (International Data Corporation) per definire le appliance firewall che incorporano funzionalità di difesa contro attacchi di vario tipo. Tipicamente includono firewall layer 2/3, firewall a livello applicazione, prevenzione e scoperta delle intrusioni, antivirus, antispy, VPN, ecc.

**VLAN:** Virtual LAN. Un metodo di segmentazione logica del traffico di rete su singoli network fisici.

**VoIP:** Voice over IP. Trasmissione di voce via Internet.

**VoIPSA:** Voice over IP Security Alliance. Vedi informazioni dettagliate nel riquadro a fianco.

## ARKOON: MEMBRO VOIPSA

La Voice Over IP Security Alliance è stata creata a febbraio 2005. TippingPoint, azienda del gruppo 3COM, mise in moto il sistema che coinvolse presto altre aziende del settore fra cui Arkoon.

VOIPSA è una organizzazione aperta e non-profit che si è prefissa di aiutare le aziende a scoprire, comprendere ed evitare i rischi inerenti la sicurezza dei sistemi VoIP, attraverso liste di discussione, white papers, sponsorizzazione di progetti di ricerca sulla sicurezza VoIP, così come lo sviluppo di strumenti e metodologie per la sua utilizzazione generalizzata. VOIPSA comprende fornitori di sistemi di telecomunicazione, providers, ricercatori e utenti che hanno uniti gli sforzi per raggiungere gli obiettivi comuni, per far sì che l'adozione di tecnologie VoIP possa essere effettuata con successo e non venga ostacolata dalle minacce di sicurezza correnti o ancora sconosciute.

Attualmente VOIPSA dispone di due gruppi di lavoro.

Il gruppo VoIP Security Threat Taxonomy collabora per l'individuazione generica degli attacchi alla sicurezza delle implementazioni VoIP, dei servizi, e degli utenti. Un elemento significativo nella sfida per una effettiva sicurezza VoIP è rappresentato in primo luogo dall'identificazione delle minacce. L'obiettivo di fondo di questo progetto è fornire un contributo per la diffusione di una cultura della sicurezza in tutti gli operatori del settore, nella stampa e nel pubblico. Il gruppo di lavoro Security Requirements ha il compito di definire i requisiti di sicurezza in tutto lo spettro di un ecosistema VoIP, ivi compresi i componenti di base singoli, i componenti preposti alla tecnologia di sicurezza (SBCs, firewalls, ecc.), progettazione e architettura del network (NAT, VPN, port security, ecc), gestione della rete, end point Access and Authentication, per citarne solo alcuni.

Ulteriori informazioni su : [www.voipsa.org](http://www.voipsa.org)

## PER ULTERIORI INFORMAZIONI

Proteggere la convergenza fra voce e dati significa adottare soluzioni di sicurezza specifiche, capaci di discriminare fra il traffico "voce" e il traffico "dati" e di applicare regole di sicurezza appropriate in coerenza con le politiche di sicurezza aziendali.

CORPORATE HEADQUARTERS  
1, PLACE VERRAZZANO  
CS 30603  
69258 LYON CEDEX 09  
FRANCE  
TEL : +33 (0)4 72 53 01 01

[www.arkoon.com](http://www.arkoon.com) / [info@arkoon.net](mailto:info@arkoon.net)

**ARKOON**  
NETWORK SECURITY



A White Paper Developed by Speedfire mediArchitects

[www.speedfire.com](http://www.speedfire.com) / +33 (0)8 70 27 64 00