Telefonia IP, l'altro lato della sicurezza per la protezione dei dati

a colloquio con Roberto Puricelli, fondatore e amministratore di DigitelNET srl
a cura della Redazione

Nell'era della convergenza dei sistemi, anche la telefonia VoIP diventa protagonista della sicurezza globale dell'utente finale. Qual è il vostro punto di vista in merito?
Partiamo dalla constatazione che oltre il 95% delle conversazioni telefoniche si basano oggi su protocollo VoIP (Voice Over Internet Protocol). Anche se l'utilizzatore finale utilizza sistemi telefonici tradizionali (non IP), il segnale viene convertito in VoIP per potersi interconnettere col mondo.
Oltre a questo, il fenomeno dell'Internet of Things (IoT) è ormai un'importante realtà. Si prevede che, entro il 2020, i dispositivi collegati in rete saranno quasi 30 miliardi ma i dispositivi per il monitoraggio che andremo a utilizzare saranno gli stessi che utilizzeremo sul posto di lavoro, siano essi smartphone, tablet o qualsiasi altro strumento che ci proporrà il mercato entro tale data. In altre parole, lo strumento che utilizzeremo per modificare la temperatura della nostra abitazione, per sapere le scadenze degli alimenti posti nel nostro frigorifero o per sapere esattamente dove sono i nostri figli in quell'istante, sarà lo stesso che utilizzeremo per collegarci al CRM aziendale, al sistema di posta elettronica o per fare una video comunicazione con interlocutori oltre oceano. In questo modo, si moltiplicheranno tra loro le possibilità di esposizione ai rischi informatici tra la sfera privata e quella professionale. Per questi motivi, la sicurezza dei sistemi di telefonia IP è un anello determinante per la sicurezza dell'intero sistema informatico delle aziende.

Quali sono, dunque, le attenzioni che il responsabile di un'azienda deve mettere in atto oggi e nel prossimo futuro?
Gli analisti del nostro settore insistono sul fatto che nei prossimi 3 anni assisteremo a uno sviluppo tecnologico

che sarà paragonabile allo sviluppo che abbiamo vissuto negli ultimi 30 anni. È ormai risaputo che destinare risorse economiche per l'acquisto di hardware non è vantaggioso. Normalmente, passano mesi dal momento in cui si destina un budget per rinnovare l'infrastruttura hardware aziendale al momento in cui tali apparati vengono messi in funzione e, nella maggioranza dei casi, quegli apparati saranno messi fuori mercato dal produttore stesso pochi mesi dopo.
Inoltre, spesso non si tiene conto di costi occulti come gli aggiornamenti software, il consumo elettrico e quello per il raffrescamento dei Ced, i sistemi di ridondanza necessari per garantire la continuità di lavoro all'azienda, i sistemi di continuità, la manutenzione di tutti i dispositivi sopra citati, oltre ai costi di formazione degli addetti. Per di più, tutti questi sistemi devono essere messi in sicurezza con i criteri del nuovo regolamento europeo GDPR 679/16 per il trattamento dei dati. Quindi, entro maggio 2018, anche i dispositivi mobili e fissi

messi a disposizione dei dipendenti devono essere messi in sicurezza.
Per far fronte a questo scenario, l'azienda deve avere sistemi avanzati ma, come abbiamo visto prima, gli acquisti nel settore IT diventano presto obsoleti. L'azienda dinamica e flessibile oggi predilige soluzioni IAAS (Infrastructure as a Service) in cloud o con una soluzione mista "hybrid cloud". In questo modo, il cliente può dedicare tutte le energie per il proprio business, senza occuparsi di obsolescenze, aggiornamenti, formazione ecc.
Backup e business continuity sono parole sempre più presenti nella soluzione hybrid cloud, le aziende scelgono di "salvare" i propri dati e informazioni in ambienti esterni, per garantire continuità alla produttività aziendale.
Le domande che le aziende devono porsi alla luce dei più recenti attacchi informatici su larga scala sono: *quanto tempo posso rimanere senza sistema informatico attivo? Che danno mi può provocare la perdita dei dati? Dal momento che le risposte saranno di sicuro il meno possibile e un danno incalcolabile, l'ultima domanda sarà: la mia azienda ha implementato o sviluppa progetti per prevenire questa criticità?*

Cosa propone DigitelNET ai propri clienti per rispondere a queste domande?
Le aziende, anche con un basso numero di addetti, hanno bisogno di garanzie di funzionamento perché un'interruzione nell'operatività dell'infrastruttura di rete si tramuta in un danno economico e d'immagine verso i propri clienti. Figuriamoci se, oltre al fermo dell'infrastruttura di rete, l'azienda subisce un furto di dati sensibili o di progetti per cui l'azienda ha investito migliaia di ore uomo, magari in fase di brevetto! Ricordiamo anche che ci sono società che realizzano fatturati importanti senza nemmeno aver la sede in quel paese, lavorando in modalità "home worker" con i propri strumenti collegati da remoto alla sede centrale.
Per rispondere in modo adeguato a queste esigenze, le aziende chiedono garanzie di competenza e affidabilità.
Per questo motivo, la strategia di DigitelNET è sempre stata quella di non utilizzare software o sistemi open source e di investire continuamente in formazione per proporsi sul mercato come system integrator in grado di seguire il cliente dall'analisi allo sviluppo, all'integrazione con i sistemi esistenti e all'assistenza H24.

Con quali tipologie di interlocutori della filiera interagite ora ed intendete interagire prossimamente?
La scelta dei partner è diventata strategica. DigitelNET ha siglato importanti accordi con i maggiori brand di riferimento in merito ad analisi di rete, sicurezza informatica, unified communication, networking, wifi.
DigitelNET non vuole e non può sostituirsi a chi da anni progetta e sviluppa soluzioni per la sicurezza informatica e software per la comunicazione, ma i nostri presales sono attenti ai protocolli e ai prodotti che ogni giorno integrano un mercato in continua evoluzione, avendo ben presente che il nostro ruolo è quello di analizzare le criticità e i fabbisogni dei clienti per indirizzarli verso un percorso che garantisca una flessibilità tecnologica sicura, con la ricerca dei sistemi più idonei e la completa integrazione all'infrastruttura esistente.
Se parliamo di cyber security, dobbiamo essere consapevoli che i pirati informatici possono sviluppare malware, ransomware, eccetera in grado di oltrepassare le barriere difensive. Le aziende di cyber security sviluppano soluzioni sempre più sofisticate, ma non sempre i brand più famosi offrono le soluzioni più adeguate. Spesso questi operatori dedicano più risorse in marketing e strategie commerciali che in ricerca e sviluppo.
In conclusione, il nostro lavoro è la ricerca e la verifica di soluzioni stabili e sicure per offrire ai clienti finali risposte perfettamente adeguate, integrabili e fruibili.

digitelNET

CONTATTI: DIGITELNET
Tel. +39 0331891118
www.digitelnet.it