

La protezione dei dati inizia da una corretta progettazione e realizzazione dell'infrastruttura di telecomunicazione

Safety e security a regola d'arte

Eros Prosperi

Vicepresidente di Assotel

Tipicamente si ritiene che, nei sistemi Ict, garantire la sicurezza significhi, semplicemente, dotarsi di un buon antivirus e, nella migliore delle ipotesi, anche di un firewall. Simili componenti sono indubbiamente indispensabili, ma non possiamo dimenticare che la sicurezza inizia da una corretta progettazione e installazione della rete di telecomunicazione. La presenza di errori o carenze a livello infrastrutturale, dovute alla mancanza di competenza o, nei casi più gravi, ad un autentico dolo, possono infatti esporre i dati in transito, così come quelli conservati, al rischio di essere intercettati e/o manipolati. A questo si aggiungono i rischi per l'incolumità delle persone, dovuti a installazioni non correttamente implementate.

Al fine di prevenire simili eventualità è necessaria una progettazione della rete che preveda tutte le strategie adeguate a garantire il più elevato livello di sicurezza e una realizzazione in linea con il progetto. Come risaputo, non esiste la sicurezza assoluta. Ma, in ogni caso, è necessario predisporre infrastrutture sempre più robuste, sia per la propria tranquillità, sia per il rispetto delle normative.

A regola d'arte

Garantire la sicurezza significa quindi, in primo luogo, realizzare infrastrutture in grado di rispondere alle normative stabilite dagli enti nazionali e internazionali, che specificano le caratteristiche costruttive di realizzazione e di utilizzo delle reti elettroniche cablate o wireless. In altri termini, tutto questo implica una realizzazione degli impianti a 'regola d'arte', un concetto non sempre ben definito, ma al quale è necessario fare riferimento per assicurare, oltre alle prestazioni attese dagli utenti, anche un livello di sicurezza in linea con le attuali esigenze del mercato. In generale, eseguire un lavoro a 'regola d'arte' significa rispettare le singole modalità operative attinenti a leggi, prescrizioni, prassi o soluzioni tecniche che soddisfino, in termini di economicità accettabile, la qualità dell'opera, la sicurezza attiva (non arrecare danno ad altri) e passiva (non subire danni), sicurezza attiva e passiva da riferire sia alle maestranze impiegate nell'ope-

Autenticazione

Livello di affidabilità offerta dai sistemi di identificazione univoca.

Integrità e confidenzialità

Livello di garanzia relativa all'alterazione e all'intercettazione dei dati.

Ripudio

Livello di errore nella tracciabilità univoca della richiesta di transazione.



ra e nelle manutenzioni, sia ad ambiti apparentemente non tangibili come i segnali fonia-dati-video e, quindi, delle più concrete informazioni strutturate che essi rappresentano.

Proprio il duplice aspetto di sicurezza attiva e passiva deve essere valutato con estrema attenzione quando la propria rete locale viene collegata a quella pubblica, aprendosi così alle comunicazioni con il resto del mondo, ma anche alla possibilità di violazioni e impieghi illeciti. In particolare, negli ultimi anni, per prevenire simili rischi sono state varate due importanti leggi, non sempre adeguatamente considerate in fase di progettazione e realizzazione. Si tratta, in particolare, della Legge 196/03, relativa alla tutela dei dati personali, che impone al responsabile di queste informazioni di implementare, compatibilmente con i costi, tutte le soluzioni adeguate alla protezione dei dati, soprattutto se considerate sensibili.

Altrettanto importante, ma spesso dimenticata, è la Legge 155/05 relativa alle misure per il contrasto del terrorismo, nota anche come Decreto Pisanu. In particolare, la norma prevede, tra l'altro, che gli accessi alla rete pubblica siano registrati e tracciati, permettendo così alle forze dell'ordine di individuare, in caso di necessità, le persone che hanno commesso crimini attraverso Internet. La Legge 155/05 fissa responsabilità specifiche anche per chi

non ha garantito un adeguato livello di sicurezza della propria infrastruttura. I rischi sono elevati soprattutto per quanti adottano tecnologie wireless che, essendo potenzialmente accessibili a chiunque, potrebbero essere utilizzate proprio per commettere crimini, se non adeguatamente protette.

A fronte di un simile evento, l'autorità di pubblica sicurezza può risalire sino alla rete aziendale e, non potendo individuare il singolo responsabile della violazione, incriminare quanti non abbiano implementato le contromisure adeguate per proteggere la rete da impieghi e accessi illegali.

Chi garantisce la qualità?

La scelta dell'azienda a cui affidare la progettazione e la realizzazione della propria rete locale rappresenta un aspetto particolarmente delicato, in quanto spesso la componente fisica passiva viene erroneamente trascurata a favore delle apparecchiature attive e dei software applicativi. In realtà, secondo la Legge 109/91 e il D.M. 314/92, "l'utente è il soggetto responsabile del corretto affido dei lavori di realizzazione, allaccio, collaudo e manutenzione di impianti di fonia-dati-video direttamente o indirettamente interconnessi alla Rete Pubblica di Comunicazione Elettronica". In altre parole, dal punto di vista legislativo, affidare i lavori di realizzazio-

*La sicurezza della rete
inizia da un'installazione
professionale*

ne della rete ad un'azienda priva di autorizzazione ministeriale di grado adeguato si configura come un reato. In particolare, la Legge 109/91 fissa le disposizioni in materia di progettazione, installazione, allacciamento, collaudo e manutenzione di Impianti e Sistemi d'Utente interconnessi ad una Rete Pubblica di Comunicazione Elettronica, mentre il D.M. 314/92 ne specifica le modalità di attuazione.

Commissionare la realizzazione di un Impianto d'Utente ad un'azienda in possesso del famoso 'patentino' significa, quindi, affidarsi ad una realtà dotata di competenze e solidità certificate a livello ministeriale, disponendo, inoltre, di adeguate garanzie per quanto riguarda la sicurezza nella consulenza, nella progettazione delle soluzioni, nella realizzazione e nell'installazione.

Simili presupposti sono fondamentali per garantire, di conseguenza, anche la sicurezza nella

gestione delle interconnessioni con le reti pubbliche di comunicazione elettronica, nella manutenzione e nell'implementazione delle soluzioni, rispondendo così in modo esaustivo alle normative e alle leggi vigenti.

La forza dell'autorizzazione

L'autorizzazione ministeriale, indispensabile per la realizzazione di qualunque Lan collegata o da collegare alla rete pubblica, rappresenta oggi una garanzia di affidabilità dell'azienda incaricata di realizzare l'infrastruttura di comunicazione. Le realtà certificate, infatti, tutelano la sicurezza a tutti i livelli, partendo proprio dalla progettazione. Infatti le aziende autorizzate devono affidare la progettazione dei sistemi a professionisti iscritti ad adeguati albi professionali e provata esperienza specifica. Nel caso poi di aziende con autorizzazione di primo grado il progettista deve essere inserito nell'organico aziendale. A questa figura si aggiunge un direttore lavori, in possesso di un'esperienza specifica presso case costruttrici o, almeno biennale, presso aziende autorizzate, garantendo così anche la sicurezza nelle realizzazioni.

Infine, la sicurezza nella gestione delle interconnessioni con Rete Pubblica, impostazione, gestione e manutenzione di sistemi e impianti è garantita dalla presenza di tecnici installatori, stabilmente e regolarmente assunti, dedicati all'esecuzione dei lavori e/o alla manutenzione delle apparecchiature terminali e dei sistemi.

La struttura tecnica deve essere, infine, dotata di strumentazione adeguata alle svariate operazioni di test, controllo e verifica necessarie per fornire le opportune garanzie di funzionamento e sicurezza.

Proprio la presenza di figure professionali, oltre ai periodici controlli ministeriali annuali cui è soggetta un'azienda autorizzata dal Ministero, rappresenta un'ulteriore garanzia di sicurezza per quanti utilizzano infrastrutture di comunicazione per svolgere la propria attività.

Safety & Security

Nella lingua italiana, a differenza dell'inglese, non esiste un termine per differenziare la sicurezza delle persone (safety) da quella dei segnali (security). Per questa ragione, in molti casi, si crea una situazione di incertezza e confusione.

Con il termine security, in ambito Ict e Tlc, s'intende la procedura messa in atto per tutelare i dati in possesso di un'azienda e quelli in transito attraverso la rete, che devono essere protetti anche in base a quanto previsto dalla normativa sulla privacy, che punisce quanti non abbiano attuato idonee procedure di difesa.

La safety, invece, fa riferimento soprattutto all'incolumità delle persone e delle cose. Anche questo aspetto assume un'importanza significativa per i teleimpiantisti, sia nell'ottica di prevenire eventuali infortuni sul lavoro di quanti installano, sia per evitare rischi a terzi dovuti ad errate installazioni, quali surriscaldamento degli apparati oppure dispersione di energia su cablaggio strutturato.

ASSOTEL

www.assotel.it