

## Sicurezza dei Sistemi Informativi

La sicurezza informatica è uno dei processi a cui le imprese e le organizzazioni in generale dovranno dedicare sempre più attenzione e risorse, anche a causa di alcuni fattori ineludibili:

- Internet: le risorse e le reti interne alle imprese ormai sono o saranno collegate all'esterno, anche grazie alla diffusione sempre più capillare della connettività a larga banda. Basta questo a introdurre una serie di rischi per i Sistemi Informativi interni.
- Sia su Internet che con altri mezzi l'informatizzazione prevede lo scambio di dati e informazioni, anche molto importanti e riservati, con attori esterni all'organizzazione (clienti, fornitori, Pubbliche Amministrazioni) e anche tra unità produttive della stessa azienda geograficamente distanti tra loro.
- Vincoli normativi e standard internazionali che coinvolgono la gestione e la sicurezza dei Sistemi Informativi: dalla normativa sul trattamento dei dati di terzi (D.Lgs. 196/03, la cosiddetta "legge sulla privacy") alle prescrizioni di Basilea II, alle normative ISO serie 27000 che tenderanno ad assumere la stessa importanza della serie 9000 sulla qualità e 14000 sull'ambiente.



**La sicurezza è un processo, non un prodotto.** La corretta gestione della Sicurezza Informatica non si conclude con l'acquisto di un singolo prodotto che pretende di eliminare tutti i rischi (sia esso un firewall, un antivirus o un sofisticato sistema per la rilevazione delle intrusioni) ma è un processo come gli altri che sono gestiti in azienda. Inoltre è un processo che coinvolge per sua stessa natura competenze sia tecniche che gestionali: l'aspetto umano e organizzativo è una componente essenziale della sicurezza, riconosciuto anche dagli standard.



**La nostra offerta** integra appunto forti competenza tecniche e di gestione, con la possibilità per i clienti di scegliere un supporto completo oppure un singolo servizio in modo modulare, in accordo con le rispettive esigenze e con gli altri attori eventualmente coinvolti.

**Progettazione ed implementazione di sistemi per la sicurezza** Sistemi per la sicurezza perimetrale (firewall, filtraggio dei contenuti, server proxy), Sistemi di rilevazione delle intrusioni (IDS), reti private virtuali (VPN), comunicazioni sicure e crittografia, disaster recovery, posta elettronica sicura.

**Analisi delle vulnerabilità (vulnerability scanning)** Verifica delle vulnerabilità presenti nei sistemi IT del cliente effettuata con strumenti per lo più automatizzati dall'interno e dall'esterno. Copre i livelli software presenti, dai Sistemi Operativi alle applicazioni, al software di sistema degli apparati di rete. Il risultato dell'attività è un report tecnico contenente l'elenco

delle vulnerabilità rilevate e i passi da compiere per correggerle. Il destinatario naturale del report è il reparto tecnico ICT (CED).

**Valutazione delle vulnerabilità (vulnerability assessment)** Questo servizio aggiunge alla scansione automatizzata una valutazione dei risultati da parte del consulente alla luce dell'infrastruttura di rete esistente. Inoltre comprende una analisi della architettura della rete e dei sistemi.

**Analisi dei rischi (risk analysis)** Le vulnerabilità dei sistemi fanno nascere dei rischi, che vanno valutati con metodologie appropriate, per il business dell'organizzazione. Questa valutazione non è più strettamente tecnica e per avere valore deve coinvolgere oltre alla struttura tecnica anche il management. Il risultato è una analisi dettagliata dei rischi per il business e degli impatti economici e di altro tipo per la sua continuità.

**Penetration test** Test di penetrazione dall'esterno, applicando il metodo che userebbe un eventuale aggressore. Valutazione dei risultati.

**Security assessment** La valutazione globale della sicurezza non comprende solo la sicurezza informatica ma anche quella logica, fisica, infrastrutturale, organizzativa... Comprende anche elementi di processo. I modelli di riferimento sono CobIT di ISACA, OSSTM, ITIL. I referenti aziendali idealmente coinvolti sono di livello direzionale.

**Auditing ISO 27001 di parte seconda.** Analisi della conformità agli standard internazionali ISO in materia di sicurezza informatica, valutazione dei passi da intraprendere per allinearsi agli standard e ottenere la certificazione ISO 27001. L'auditing è una procedura che dovrà essere implementata nel Sistema di Gestione del Sistema Informativo aziendale, in accordo con lo standard.

### **Servizi collegati:**

- Progettazione di impianti speciali (reti dati anche in ambito industriale) e data center: la sicurezza e la continuità del business partono dal livello base dell'infrastruttura
- Videosorveglianza digitale (progettazione degli impianti, fornitura e installazione del software, implementazioni, consulenza): la sicurezza fisica è contemplata dagli standard in materia di sicurezza dei Sistemi Informativi

*Contatti per maggiori informazioni:*

#### **StudioAG - ICT Consulting & Engineering**

Via Giacomo Zanella, 166

I 36010 Cavazzale – VI

Tel. +39 0444 945523

Fax. +39 0444 298549

**info@studioag.eu**

www.studioag.eu

Membro ISACA - Informations Systems Audit and Control Association

Membro CLUSIT - Associazione italiana per la sicurezza informatica

