L’IT in azienda oggi

Il mondo odierno, permeato di strumenti “connessi” ed accessibili in vari modi, la penetrazione del mondo digitale in ogni aspetto della nostra vita, volenti o nolenti, ci costringe ad un approccio consapevole a questi temi.

La correlazione tra i temi legati al mondo “informatico” e i vari aspetti della nostra vita comporta una deriva fortemente legale e le norme hanno solo preso atto di quella che è l’evoluzione della nostra società verso il digitale.

Detto ciò appare chiaro che tale evoluzione va assecondata e seguita, ma assolutamente non subita.

Siamo fondamentalmente “inconsapevoli digitali” ovvero utilizziamo strumenti ma non abbiamo coscienza del funzionamento degli stessi e delle loro implicazioni.

Crescente attenzione sul tema della Cybersecurity in ambito aziendale che non comprende come farebbe intendere il termine solo aspetti puramente tecnici ma anche (sarebbe più corretto dire in maggior parte) procedurali e organizzativi, di gestione del personale e di tutela legale.

Firewall, IDS (Intrusion Detection System) e antivirus/antimalware non bastano da soli a proteggere le reti aziendali. Per raggiungere questo risultato occorre una strategia che consideri tutte le singole caratteristiche del sistema in oggetto e preveda l'azione combinata di tutti gli strumenti a disposizione, sulla base delle reali esigenze e problematiche di sicurezza dell'azienda.

Per essere del tutto protetto un sistema dovrebbe essere completamente chiuso, ma questo non consentirebbe scambio di informazioni con l'esterno o all'interno di una rete aziendale.

Quindi è necessario garantire un numero minimo di aperture ed è altrettanto importante verificare che i protocolli di accesso impiegati siano esenti da falle riconosciute.

L’evoluzione tecnologica, l’introduzione di IoT (Internet of Things, neologismo riferito all'estensione di Internet al mondo degli oggetti e dei luoghi concreti), l’utilizzo di tecniche di AI (Artificial Intelligence), più o meno spinta, in svariati processi e sistemi non fa altro che aumentare rischi e vulnerabilità.

Quindi, come identificare i bug del sistema? Come controllare che le password proteggano effettivamente gli accessi? Come assicurarsi che il firewall sia efficiente e funzionale? Come verificare che non ci siano vulnerabilità in grado di crashare il sistema minandone la stabilità? Sono presenti sistemi IoT che possano costituire una via d’accesso? E ancora, quanto e in che modo i processi aziendali e i flussi di dati insieme al "fattore umano" influiscono sulla sicurezza dei sistemi?

L'analisi del rischio e delle vulnerabilità del Vostro sistema informatico aziendale è lo step fondamentale per poter pianificare una strategia di sicurezza e organizzare le contromisure di protezione. Permette di identificare quali misure di sicurezza siano effettivamente necessarie.

Prima di lanciarsi in revamping più o meno articolati, introdurre mirabolanti software spesso utilizzati solo in parte, acquistare hardware pluri-premiato e certificato, è necessario analizzare tutta la struttura di rete hw/sw esistente ed i vostri "modus operandi" al fine di individuare i possibili rischi per la sicurezza.

La giusta domanda da porsi è dunque: quanto è importante il dato che produco e custodisco e quanto il mio business verso i clienti dipende dal dato?

Inoltre, parlare di cybersecurity ovvero di protezione del dato implica trattare la protezione del dato personale ovvero tutto ciò che afferisce al Regolamento UE 679/16 (GDPR), affiancato dal Codice della Privacy (D.Lgs. 196/03) e dal D.Lgs. 101/18, che lo completano contestualizzandolo nel tessuto normativo italiano.

Possiamo quindi sintetizzare la nostra visione della gestione della sicurezza dei dati in azienda (o come più ad effetto viene chiamata oggi Cybersecurity) nei seguenti ambiti:

- IT Security (in senso stretto, ovvero nei termini di sicurezza di hardware e software);
- gestione dei processi;
- gestione del personale;
- GDPR compliance;
- NIS 2 compliance;
- compliance specifiche di settore;
- IT Forensics (tutto quanto ruota intorno a dati e informazioni da poter utilizzare in Tribunale).

La spinta alla digitalizzazione ha fatto sì che la figura dell’IT Manager ricopra un ruolo cardine.

L’IT Manager è una figura manageriale, con solide competenze ICT, in grado di concordare e perseguire con la Direzione Aziendale obiettivi di business in ambito IT definiti e misurabili. La sua mission è trasformare l’IT aziendale in un asset strategico, favorendo una progressiva integrazione tra infrastruttura tecnologica e processi di business, per poi assicurare attraverso una adeguata governance i massimi livelli di supporto alle attività imprenditoriali e produttive da parte dell’IT.

Per tutte le PMI in cui la complessità dell’IT non giustifichi un IT Manager a tempo pieno, ma la cui Direzione Aziendale non intenda rinunciare alla presenza di una figura manageriale alla guida dei Sistemi Informativi, esiste la possibilità di affidarsi ad un IT Manager esterno “as a service”, la cui presenza è limitata in virtù di precisi accordi presi sulla base delle effettive esigenze aziendali e garantendo costi proporzionati alle reali necessità.

Il partner tecnologico a fianco della TUA azienda

Oltre agli aspetti puramente consulenziali ACS srl è in grado di supportare con facilità le aziende negli aspetti pratici legato agli asset informatici, dalla creazione della rete, alla gestione dei server e dei PC, ecc., ovvero nell'integrazione dei sistemi hardware e software e nella risoluzione di tutte le piccole problematiche quotidiane (ad es. file che non si aprono, installazioni, mancato accesso a cartelle, impossibilità di visualizzazione di pagine web, ecc.) con un help desk di primo livello rapido e puntuale. Siamo abituati a gestire un alto numero di interventi quotidiani e a risolvere con rapidità i problemi che si pongono soprattutto in situazioni di stress che richiedono soluzioni tempestive.

ACS s.r.l. è nata nel 2005 e da allora ha sviluppato il suo percorso di crescita concentrandosi molto sull'aspetto puramente consulenziale avvalendosi anche del supporto legale di alcuni Avvocati esperti in ambito digitale.

Il nostro business si sviluppa su due aree ben definite e una "verticalizzazione".

Area consulenza:

- IT Security (o come più ad effetto viene chiamata oggi Cybersecurity);
- GDPR compliance (Regolamento UE 679/16, D.Lgs. 196/03, D.Lgs. 101/18 e relativi provvedimenti);
- NIS 2 compliance (Direttiva UE 2022/2555);
- compliance IT (famiglia ISO 27000 e standard correlati, audit interni);
- IT Management (organizzazione aziendale e strategia in ambito IT).

Area assistenza:

- system integration (gestione dei sistemi hardware/software, server, ecc.);
- help desk (risoluzione di tutte le problematiche quotidiane dalle più piccole alle più complesse).

Verticalizzazione in abito legale:

- supporto in tutte le fasi del Processo Civile Telematico (PCT), Processo Amministrativo Telematico (PAT), Processo Tributario Telematico (PTT) e Processo Penale Telematico (PPT);
- Consulenze Tecniche di Parte (CTP) in procedimenti penali, civili e amministrativi;
- Informatica Forense e Digital Forensics.

Dal 2005 vantiamo clienti in settori di ogni genere e dimensione:

- PMI;
- cooperative;
- settore sanitario;
- settore legale;
- pubblica amministrazione e società partecipate.

Riferimenti normativi adottati (elenco non esaustivo)

- Codice per la tutela dei dati Personali e Leggi correlate – Regolamento UE 679/2016, D.Lgs. 196/2003 e D.Lgs. 101/2018;

- Sistemi di gestione degli Amministratori di Sistema – D.Lgs. 196/2003;
- Disaster Recovery (Art.50/bis D.Lgs. 235/2010 del 25/01/2011);
- Direttiva UE 2022/2555 (cosiddetta Direttiva NIS 2 - Network and Information Security);
- Attuazione della direttiva NIS 2.

Standard di riferimento adottati (elenco non esaustivo)

- Information Security Management System (ISMS) – ISO/IEC 27001 lo standard internazionale della sicurezza delle informazioni;
- Information Technology — Security techniques — Code of practice for information security controls – ISO/IEC 27002 raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001;
- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – ISO/IEC 27701 standard di riferimento per la protezione dei dati personali;
- Risk Management ISO/IEC 31000 principi e linee guida per la gestione del rischio;
- ENISA (European Network and Information Security Agency) guidelines;
- Information Technology Service Management – ISO/IEC 20000 standard di riferimento per l'organizzazione dei servizi informatici che mira al miglioramento dell'erogazione/fruizione dei servizi IT;
- Societal security — Business continuity management systems — Requirements ISO/IEC 22301 norma internazionale relativa alla gestione della continuità operativa (Business continuity);
- Information Security Incident Management ISO/IEC 18044 linee guida e principi per la gestione degli incidenti relativi alla sicurezza delle informazioni;
- Information Technology – Security Techniques – Guidelines for information and communications technology Disaster Recovery Services ISO/IEC 24762 fornisce le linee guida per il Servizio di Disaster Recovery.