# Sicurezza in Azienda: Una Visione Globale

## Introduzione

La sicurezza in azienda è un aspetto cruciale per garantire un ambiente di lavoro sicuro, proteggere le risorse dell'azienda e mantenere la fiducia dei clienti. Questa relazione esplorerà i vari aspetti della sicurezza in azienda, includendo la sicurezza fisica, la sicurezza informatica, le politiche di gestione dei dati e la formazione dei dipendenti. Saranno discussi anche i rischi associati alla mancanza di sicurezza e le strategie per mitigarli.

## Sicurezza Fisica

La sicurezza fisica è essenziale per proteggere gli impiegati, gli asset e le informazioni aziendali. Questo include la sicurezza degli uffici, l'accesso ai locali, i sistemi di sicurezza come telecamere di sorveglianza e sistemi di allarme, oltre alle misure per prevenire incendi e altre emergenze. Le aziende devono implementare procedure di evacuazione e formare i dipendenti per situazioni di emergenza.

## Sicurezza Informatica

Con l'aumento delle minacce informatiche, la sicurezza informatica è diventata un focus critico. Le aziende devono proteggere i propri sistemi da malware, phishing, attacchi DDoS e altre minacce. Ciò include l'uso di firewall, antivirus, crittografia dei dati, autenticazione a due fattori e formazione dei dipendenti sulla sicurezza informatica. La gestione delle password e l'aggiornamento regolare del software sono anche pratiche fondamentali per mantenere la sicurezza informatica.

## Gestione dei Dati Sensibili

Le aziende gestiscono enormi quantità di dati sensibili, tra cui dati dei clienti, dati finanziari e proprietà intellettuale. È essenziale implementare politiche di protezione dei dati, compresi protocolli di backup regolari e crittografia dei dati. La conformità alle normative sulla privacy, come il GDPR in Europa, è fondamentale. Le aziende devono anche pianificare la risposta a incidenti di sicurezza dei dati, incluso il processo di notifica alle autorità competenti e agli interessati.

## Formazione dei Dipendenti

I dipendenti sono un punto debole significativo nella sicurezza aziendale. Spesso, gli attacchi informatici iniziano con tecniche di ingegneria sociale, quindi la formazione dei dipendenti è essenziale. I dipendenti devono essere istruiti su come riconoscere phishing, password sicure, l'importanza di non condividere informazioni sensibili e la sicurezza fisica dell'ufficio. La formazione continua è essenziale poiché le minacce e le tecniche di attacco evolvono costantemente.

## Rischi e Mitigazione

La mancanza di sicurezza in azienda può portare a gravi conseguenze, tra cui la perdita di dati sensibili, danni all'immagine aziendale, multe per violazioni della privacy e interruzioni operative. Per mitigare questi rischi, le aziende dovrebbero investire in tecnologie di sicurezza, implementare politiche robuste e formare i dipendenti in modo efficace. La collaborazione con esperti di sicurezza esterni per audizioni e valutazioni di sicurezza può anche rivelarsi preziosa.

## Conclusione

La sicurezza in azienda è un compito complesso che richiede un approccio olistico. Dalla sicurezza fisica alla sicurezza informatica, dalla gestione dei dati alla formazione dei dipendenti, ogni aspetto contribuisce a creare un ambiente aziendale sicuro e protetto. Le aziende che prioritizzano la sicurezza non solo proteggono i propri interessi, ma anche costruiscono fiducia tra i clienti e gli stakeholder. Affrontando i rischi e adottando pratiche di sicurezza robuste, le aziende possono prosperare in un mondo digitale sempre più complesso e minaccioso.

# **Sicurezza informatica aziendale: tutto quello che c’è da sapere**

La tematica della **sicurezza informatica aziendale** è sempre più discussa, specie dall’avvento del GDPR che ha portato tutta una serie di cambiamenti informatici. Il problema di fondo sta nel fatto che sono sempre di più le imprese che oggigiorno sono costrette a confrontarsi con **attacchi di cyber criminali**, **malware**, [**ransomware**](https://www.dssecurity.it/blog/cyber-risk/i-ransomware-una-minaccia-sempre-piu-presente-per-i-cloud/) e altre minacce informatiche provenienti dall’esterno. Non tutte, però, dispongono di una protezione eccellente data dai sistemi informativi aziendali.

## **Che cos’è la cyber security aziendale?**

La **sicurezza informatica aziendale** è la salvaguardia dell’integrità, della riservatezza e della disponibilità di dati e informazioni che vengono gestiti direttamente da un’impresa. Di conseguenza, la protezione degli apparati informatici contro i cyber attacchi è un aspetto di fondamentale importanza. Ma non ci sono solo i dati e le informazioni da tutelare, visto che la tematica in oggetto abbraccia svariate aree. Una di quelle più importanti nell’ottica della normativa sulla sicurezza informatica riguarda la Rete.

Al giorno d’oggi, di tutti gli investimenti effettuati in quest’area, quasi il 50% ha che fare proprio con i servizi collegati. Poi è la volta delle **infrastrutture** e dell’***identity & access management***, sempre più rilevante.

## **Com’è la situazione della sicurezza informatica aziendale in Italia?**

Le imprese italiane non lesinano di certo gli investimenti nel campo della sicurezza informatica: chiaramente, la maggior parte di questi, e nello specifico il 78%, nell’ultimo anno è stato ad opera delle multinazionali. Le PMI che costituiscono la spina dorsale del tessuto industriale del Belpaese risultano ancora un po’ indietro al riguardo.

Tuttavia, è opportuno mettere in evidenza come è con l’**avvento del GDPR** e la necessità di essere conformi alla nuova normativa dell’Unione Europea in materia di ***privacy*** che si sono registrati maggiori investimenti.

La maggior parte degli attacchi informatici, in Italia così come un po’ nel resto del mondo, proviene da **malware**, da **tentativi di phishing** e da tecniche tutto sommato banali, quali **DDoS** e **SQLI**. Il problema di fondo è duplice: i trend dimostrano come di anno in anno, i malcapitati di queste minacce informatiche sono in crescita; dall’altro, gli attacchi di successo vengono realizzati a costi decrescenti.

Il sistema operativo che finisce quasi sempre nel mirino dei criminali informatici è **Android**. Come mai? Trattasi di un sistema aperto, dove spesso gli utenti non scaricano le applicazioni non dallo store ufficiale di Google. Qui, nel complesso, le protezioni si dimostrano scarse. **iOS**, nonostante non possa essere definito una vera e propria roccaforte contro gli attacchi dei cyber criminali, fa già meglio, essendo un sistema operativo chiuso.

In tutto questo, anche in ambito aziendale, i **danni sulla produttività** non mancano di certo. E tra truffe, furti di denaro, estorsioni, violazione di dati sensibili, il conto negli ultimi anni è stato più salato delle aspettative.

## **Sicurezza informatica aziendale: problematiche esterne e interne**

Come mai i malintenzionati riescono ad aggirare i sistemi di sicurezza informatica aziendale? Talvolta, il problema deriva dall’esterno, ma non sono poche le volte in cui le **difese interne** si sono rivelate carenti. Colpa di dipendenti aziendali che hanno sottovalutato il problema. Sono solo in pochi, infatti, quelli che hanno una piena consapevolezza relativamente alla policy sicurezza informatica aziendale. I dipendenti, però, non corrono grossi rischi di finire vittime di **raggiri** o di **truffe**, almeno in prima persona. Tuttavia, possono mettere la propria azienda nel mirino delle minacce informatiche. Ed è proprio per questo motivo che negli ultimi anni si sono diffusi tutta una serie di corsi aziendali, volti a educare i dipendenti delle organizzazioni a migliorare il livello di protezione della sicurezza aziendale. La formazione è stata indirizzata non solo a chi lavora a stretto contatto con l’IT, ma a tutti.

## **Normativa sicurezza informatica: le novità introdotte dal GDPR**

Non c’è il minimo dubbio sul fatto che l’entrata in vigore del GDPR abbia inciso sensibilmente in materia di investimenti nella sicurezza informatica aziendale.

L’intento di fondo del **GDPR** verte sulla salvaguardia dei diritti di tutti i cittadini in materia di **privacy** e, per ovvi motivi, il contesto aziendale ne è parte integrante.

Il principale cambiamento del GDPR è incentrato sulla **maggiore responsabilizzazione del titolare dell’impresa** e del management. Tocca ai vertici aziendali valutare quali sono i rischi che possono verificarsi in materia di privacy di dati e informazioni e quali sono le contromisure adeguate adeguate da prendere tenendo conto che la gestione della cyber security varia in base alle esigenze e alla struttura di ogni azienda. Vi sono, tuttavia, alcuni principi base ai quali tutti possono fare riferimento. Questo significa che qualsiasi policy sulla sicurezza informatica aziendale deve tenere conto delle seguenti fasi:

Per ovvi motivi, la gestione della sicurezza informativa differisce in base alle dimensioni. Vi sono tuttavia alcuni principi base che è bene tenere in considerazione.

Qualsiasi policy sicurezza informatica aziendale deve tenere conto delle seguenti fasi:

1. **Identificazione degli asset da proteggere al meglio**, a fronte di eventuali minacce. Anche queste ultime vanno sempre individuate. Quindi, una volta valutate le vulnerabilità di un’impresa, mediante indagini approfondite sui sistemi interni ed esterni, si acquisisce maggiore consapevolezza relativamente a quello che non va. Presi in esame i rischi a cui l’azienda è esposta, è opportuno passare alla protezione dei dati.
2. **Implementazione di contromisure protettive**, volte a innalzare il livello di sicurezza informatica. In questa fase, si passa al piano strategico, noto come action plan. Il suo fine principale è quello di identificare le necessarie azioni per garantire un livello di protezione soddisfacente se non ottimale.

L’installazione dei **firewall** è il più classico degli esempi al riguardo.

1. **Rilevazione delle minacce informatiche** e azione delle difese. Queste ultime hanno lo scopo di bypassare la fase di difficoltà e di ripristinare il ritorno alla normalità.
2. **Monitoraggio dell’efficienza delle contromisure implementate**. La strategia posta in essere si è dimostrata foriera di risultati positivi oppure le vulnerabilità per i sistemi informatici persistono ancora? Dalla risposta, bisognerà fare le dovute valutazioni e agire tempestivamente, senza sottovalutare nessun rischio.

Affinché tutto funzioni per il verso giusto, è bene che le aziende sviluppino una cultura interna, tenendo conto degli eventuali rischi in rapporto al budget che può essere stanziato.

Minimizzare le probabilità di perdita di dati, a seguito di un attacco informatico, diventa perciò possibile solo con l’implementazione di un sistema di prevenzione attiva e con l’esecuzione di scansioni regolari. La **regolarità dei backup**, di fatto, gioca un ruolo imprescindibile per garantire la necessaria continuità di accesso alle informazioni. Quest’ultimo aspetto è determinante nell’ambito della **sicurezza IT**.

## **L’importanza delle competenze necessarie per migliorare la sicurezza informatica di un’impresa**

Chi lavora nel ramo della sicurezza informatica aziendale sa benissimo che ci sono diverse tematiche fra loro connesse: la gestione del rischio, l’organizzazione dei sistemi informatici, l’attenzione alla sicurezza dei software e i penetraction test sono alcune delle aree trasversali su cui c’è molto da lavorare. Al riguardo, vi sono diversi professionisti e consulenti fortemente specializzati in ognuna delle aree in questione: oltre al percorso universitario in informatica, vi sono tutta una serie di certificazioni sulla sicurezza informatica che vanno per la maggiore. Alternare alla formazione in aula e in laboratorio, l’esperienza sul campo è però fondamentale. Ed è proprio questa la strada che numerose figure nel ramo IT oggigiorno percorrono.

Per quanto riguarda le competenze inerenti all’organizzazione della sicurezza delle informazioni, una delle certificazioni più richieste nel contesto aziendale è la **Lead auditor ISO/IEC 27001**. Basta controllare i bandi di gara per rendersene conto.

Nell’ambito delle c**ompetenze organizzative e tecnologiche**, la **CISSP** (**Certification Information System Security Professional**) è sempre più richiesta, in quanto serve ad attestare le competenze attinenti ai principi dei sistemi di sicurezza informatica, relativamente alla progettazione e alla gestione.

## **Conclusioni**

Internet rappresenta il principale veicolo per attaccare le aziende e, almeno potenzialmente, tutti i dipendenti risultano esposti al rischio di cyber attacchi. Investire nella sicurezza informatica aziendale è più che mai necessario, principalmente per una questione di produttività e di salvaguardia dei dati sensibili. Un noto consulente per la sicurezza nazionale della Casa Bianca, Richard Clark, ha più volte messo in evidenza che chi spende più soldi per il caffè che per la sicurezza delle informazioni personali, merita di essere hackerato.