Compliance normativa nella Governance della sicurezza informatica



La governance della sicurezza informatica è un aspetto cruciale per qualsiasi organizzazione che voglia proteggere i propri dati e garantire la continuità operativa.

La compliance informatica consiste nel rispetto di leggi, regolamenti e standard specifici che disciplinano l'uso, la protezione e la gestione delle tecnologie informatiche all'interno di un'azienda. Questi requisiti sono progettati per assicurare che le organizzazioni tutelino i dati sensibili, garantiscano la sicurezza dei sistemi e operino in conformità con le normative vigenti.

Compliance Normativa e Gestione dei Rischi Informatici

La **compliance normativa** gioca quindi un ruolo fondamentale in questo contesto, le normative impongono standard e procedure specifiche che devono essere seguite per garantire un livello adeguato di protezione delle informazioni.

Sicurezza delle informazioni, Cybersecurity e Data Protection costituiscono i tre elementi fondamentali per una completa gestione degli aspetti della sicurezza informatica.

Oggi, indipendentemente dal settore in cui opera, un'organizzazione deve garantire una gestione efficace e completa della sicurezza delle informazioni. In un'epoca in cui la criminalità informatica è in forte crescita e colpisce aziende di qualsiasi dimensione e notorietà, tale approccio risulta imprescindibile.

Un’adeguata gestione degli aspetti legali e di conformità, supportata da una solida conoscenza giuridica, rappresenta un complemento essenziale alla sicurezza informatica. Trascurare il quadro normativo e le sue interazioni può infatti esporre le aziende a rischi significativi, con possibili conseguenze rilevanti.

Normative rilevanti: GDPR, NIS, ISO/IEC

La **cybersecurity** è, senza dubbio, un aspetto fondamentale della compliance, in quanto strettamente legata alla conformità normativa. Di conseguenza, i sistemi di sicurezza devono necessariamente tenere conto delle implicazioni legali.

Un attacco informatico rappresenta, inevitabilmente, anche una minaccia dal punto di vista legale, come dimostrano le richieste di riscatto, che costituiscono vere e proprie forme di estorsione.

Per operare nel rispetto delle normative e, al contempo, garantire una difesa adeguata contro un attacco informatico, è fondamentale adottare soluzioni progettate e implementate in anticipo. La prevenzione in ambito cibernetico è essenziale, poiché eventuali vulnerabilità nei sistemi di sicurezza IT possono comportare costi elevati. Tuttavia, la preparazione non è importante solo per ragioni economiche, ma anche per assicurare la conformità legale.

Per questo motivo, è indispensabile un approccio strategico e integrato che consideri congiuntamente gli aspetti legali, organizzativi e tecnici. Solo chi possiede competenze specifiche in questi tre ambiti può sviluppare misure di sicurezza realmente efficaci. In caso contrario, mancherà sempre una visione olistica, indispensabile per affrontare minacce complesse.

Oggi, gli attacchi alla sicurezza informatica rappresentano una delle sfide più gravi per le aziende. Durante un attacco, non vi è margine di manovra per improvvisare: la resilienza deve essere immediata.

Di conseguenza, la conformità assume un ruolo sempre più centrale nella gestione aziendale. In questo scenario, il management ha la responsabilità di garantire che l'organizzazione rispetti e applichi le normative sulla protezione dei dati e sulla sicurezza delle informazioni. L'interconnessione tra la tutela dei dati e i potenziali danni, anche reputazionali, impone la necessità di un'infrastruttura IT sicura ed efficiente.

Le normative sulla cybersecurity variano a seconda del settore e della giurisdizione, ma alcune regolamentazioni hanno una portata globale o europea, influenzando direttamente la gestione della sicurezza nei sistemi informatici. Tra le principali troviamo il **Regolamento Generale sulla Protezione dei Dati (GDPR)**, la **Direttiva NIS** e gli **standard ISO/IEC**.

Normative e Standard di Riferimento per la Sicurezza Digitale

Il **GDPR** è uno dei regolamenti più significativi e impattanti nel campo della protezione dei dati personali. Questa legislazione europea impone alle organizzazioni una serie di obblighi da rispettare per assicurare un trattamento sicuro e conforme delle informazioni personali dei cittadini dell'Unione Europea.

Tra i principali requisiti previsti, vi è la necessità di ottenere un consenso chiaro ed esplicito per la raccolta e l'utilizzo dei dati, l'obbligo di adottare misure di sicurezza adeguate a proteggerli e la necessità di segnalare eventuali violazioni entro 72 ore dall'accaduto.

Il regolamento impone quindi obblighi stringenti sulla protezione dei dati personali e sulla gestione della privacy.

La **Direttiva NIS (Network and Information Security)** istituita nel 2016 è una regolamentazione europea che impone alle organizzazioni dei settori critici (energia, trasporti, finanziario, sanitario) di adottare misure di sicurezza specifiche per la protezione delle reti e dei sistemi informatici. Attraverso questa direttiva, infatti, sono state definite sia pratiche precise per la cybersecurity sia anche coloro che le devono adottare, in particolare strutture che si occupano di servizi essenziali.

L'emanazione della **NIS2** rappresenta una versione aggiornata e migliorata della direttiva, con cui l'Unione Europea mira a rendere le aziende, che costituiscono il cuore del tessuto socioeconomico, più affidabili in termini di sicurezza informatica. Questa nuova disciplina amplia significativamente il numero di imprese soggette agli obblighi di protezione, passando da alcune centinaia a decine di migliaia. Le aziende coinvolte devono adottare un approccio strutturato alla sicurezza, che includa l'analisi dei rischi, la gestione degli incidenti, la continuità operativa, la protezione della supply chain e altre misure specifiche.

La NIS2 definisce con maggiore chiarezza le responsabilità del management aziendale, stabilendo anche tempistiche precise per la notifica degli incidenti di sicurezza: gli eventi di particolare rilevanza devono essere segnalati entro 24 ore. Inoltre, impone ai dirigenti non solo di garantire l'attuazione della direttiva, ma anche di supervisionarne l'applicazione. Il mancato rispetto delle disposizioni può comportare sanzioni economiche e, nei casi più gravi, la sospensione temporanea dalle funzioni manageriali.

L'impatto della NIS2 si estende anche agli operatori del settore IT, con particolare attenzione alla sicurezza della supply chain. Le aziende sono infatti tenute a valutare le

vulnerabilità dei propri fornitori e a adottare misure correttive qualora necessario, rafforzando così l'intero ecosistema della sicurezza informatica.

L'obiettivo principale è aumentare la resilienza informatica e garantire una risposta rapida agli incidenti di sicurezza.

Gli **standard ISO/IEC 27001 e 27002** rappresentano un riferimento internazionale per la gestione della sicurezza delle informazioni. Mentre la ISO/IEC 27001 stabilisce i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS), la ISO/IEC 27002 fornisce linee guida dettagliate sulle migliori pratiche per la protezione dei dati aziendali. È importante evidenziare che lo standard **ISO 27001**, che fornisce linee guida per l'implementazione delle migliori pratiche in materia di sicurezza delle informazioni, può rappresentare un framework efficace per conformarsi ai requisiti della NIS2.

Modello di Governance e Responsabilità Aziendali

Il rispetto della conformità normativa non è solo una questione tecnica, ma coinvolge anche il **top management** delle organizzazioni. I dirigenti hanno la responsabilità di garantire che le politiche di sicurezza informatica siano allineate con le normative in vigore e che vengano implementate in modo efficace.

Uno degli obblighi principali è la **definizione di un modello di governance della sicurezza** che comprenda l'assegnazione chiara delle responsabilità, la formazione del personale e l'adozione di misure di prevenzione e mitigazione dei rischi. Inoltre, le aziende devono predisporre un **registro delle attività di trattamento dei dati**, nominare un **Data Protection Officer (DPO)** se richiesto dalla legislazione e assicurarsi che i processi aziendali rispettino i principi di privacy by

design e by default.

Va da sé che, se questi obblighi organizzativi e di monitoraggio non sono sufficientemente adempiuti e la società è quindi danneggiata, vi è anche una **responsabilità personale** degli amministratori delegati.

Il top management infine è anche responsabile della **gestione degli incidenti di sicurezza**. In caso di violazione dei dati, la legislazione impone obblighi specifici, come la notifica tempestiva alle autorità di controllo e agli utenti interessati. Il mancato rispetto di tali obblighi può comportare multe severe e danni reputazionali significativi.

Audit e Verifica della Conformità Informatica

Per garantire la conformità alle normative, le organizzazioni devono implementare **processi di audit e verifica** della sicurezza informatica. L'IT auditing consiste nell'analisi, nella valutazione e nella revisione dei sistemi informatici, delle infrastrutture tecnologiche, delle applicazioni, della gestione e dell'utilizzo dei dati, nonché delle politiche e delle operazioni aziendali. Questo processo viene svolto garantendo il rispetto degli standard riconosciuti, delle policy interne e delle normative vigenti.

Il suo ruolo è fondamentale per individuare e ridurre i rischi legati alla sicurezza informatica, alla gestione dei dati e alla continuità operativa. Attraverso specifiche procedure e controlli, gli auditor IT verificano l'aderenza ai protocolli di sicurezza, identificano eventuali vulnerabilità nei sistemi e suggeriscono interventi per migliorare la protezione delle infrastrutture digitali dell'azienda.

Questi controlli servono a identificare eventuali vulnerabilità e a correggerle prima che possano essere

sfruttate da attori malintenzionati o comportare violazioni normative.

Gli audit possono essere **interni o esterni**. Gli audit interni vengono condotti dal personale dell'azienda o da consulenti incaricati, mentre quelli esterni vengono eseguiti da enti certificatori o autorità di regolamentazione. Entrambi i tipi di audit prevedono l'analisi della documentazione, la verifica delle misure di sicurezza implementate e la valutazione dei processi aziendali in relazione alle normative vigenti.

Attraverso un'analisi approfondita dei protocolli di sicurezza, del flusso dei dati e delle infrastrutture IT, gli auditor individuano le vulnerabilità e i potenziali rischi che potrebbero compromettere l'integrità e la stabilità dei sistemi aziendali.

Per le aziende, la sicurezza informatica non è più un'opzione o un aspetto marginale, ma rappresenta una necessità strategica fondamentale per la loro continuità e crescita. Le violazioni informatiche possono provocare non solo ingenti perdite economiche, ma anche danni irreversibili alla reputazione e alla fiducia dei clienti.

In un mercato altamente competitivo, dove la credibilità è un valore cruciale, garantire la protezione e la resilienza delle infrastrutture IT diventa una priorità assoluta per qualsiasi organizzazione.

Tra gli strumenti più utilizzati per la verifica della conformità ci sono i **sistemi di gestione della sicurezza delle informazioni (ISMS)**, le **piattaforme di monitoraggio della sicurezza**, i **test di penetrazione (penetration testing)** e le **analisi di rischio periodiche**. Questi strumenti consentono di monitorare costantemente l'infrastruttura IT e di individuare tempestivamente eventuali criticità.

L'automazione dei processi di compliance è un ulteriore passo avanti per migliorare l'efficienza della cybersecurity

governance. Attraverso soluzioni software dedicate, le aziende possono automatizzare la raccolta dei dati, la generazione di report di conformità e la gestione delle politiche di sicurezza.

Le imprese devono conoscere le normative applicabili e implementare le misure necessarie per rispettarle, evitando così rischi legali e danni alla propria reputazione.

L'IT auditing e la compliance normativa sono strettamente interconnessi. Gli audit di sicurezza offrono una visione dettagliata delle procedure e delle tecnologie aziendali, evidenziando eventuali carenze o violazioni normative.

Queste analisi sono essenziali per i responsabili della conformità, poiché permettono di individuare criticità e definire strategie mirate per allinearsi ai requisiti normativi.

Sanzioni e Conseguenze della Non Conformità

Il mancato rispetto delle normative sulla sicurezza informatica può comportare conseguenze gravi per le aziende, sia in termini economici che reputazionali. Le sanzioni variano a seconda della legislazione applicabile, ma in generale possono includere **multe significative, restrizioni operative e danni d'immagine**.

Nel caso del **GDPR**, le multe possono arrivare fino al **4% del fatturato annuo globale dell'azienda** o a **20 milioni di euro**, a seconda di quale cifra sia più elevata. Oltre alle multe, le autorità di controllo possono imporre **limitazioni o sospensioni** delle attività di trattamento dei dati, con impatti significativi sulle operazioni aziendali.

Con riguardo alla mancata osservanza degli obblighi della NIS 2, questa prevede che le sanzioni variano in base

all’appartenenza al servizio importante o essenziale.

Le multe per le imprese dei servizi considerati **importanti** possono arrivare **fino a 7.000.000 euro o all’1,4% del fatturato annuo complessivo**, mentre per le **entità essenziali** possono raggiungere i **10.000.000 euro o il 2% del fatturato annuo** complessivo, a seconda di quale importo sia maggiore.

Per evitare condanne, le organizzazioni devono adottare un approccio **proattivo** alla gestione della compliance. Ciò significa implementare un **programma di gestione della conformità**, monitorare costantemente le modifiche normative e adeguare tempestivamente le proprie politiche e procedure interne.

Una gestione efficace della conformità normativa comporta anche l’implementazione di controlli rigorosi sulle autorizzazioni e sulle modalità di accesso ai sistemi informatici. È essenziale mantenere un registro dettagliato con marcatura temporale e validità legale, così da poter tracciare e documentare ogni accesso, facilitando eventuali indagini in caso di data breach.

Inoltre, la gestione della non conformità dovrebbe includere un **piano di risposta agli incidenti**, che preveda azioni specifiche per mitigare gli effetti negativi di una violazione normativa. Un’adeguata comunicazione con le autorità di regolamentazione e una strategia di remediation efficace possono contribuire a ridurre le conseguenze legali e finanziarie di una mancata conformità.

Governance della Sicurezza Informatica: Strategie di Protezione Aziendale

La compliance normativa nella governance della sicurezza informatica è da ritenersi un aspetto essenziale perché porta

ad un miglioramento organizzativo in termini di maggiore **efficienza, efficacia e trasparenza** dell'intera Organizzazione. Il rispetto delle normative come GDPR, NIS e ISO/IEC richiede un impegno costante da parte delle aziende e del top management, con una particolare attenzione alla gestione dei rischi, all'implementazione di controlli di sicurezza adeguati e alla verifica periodica della conformità.

Investire nella sicurezza informatica e nella conformità non solo aiuta a evitare sanzioni e rischi legali, ma rappresenta anche un vantaggio competitivo, migliorando la fiducia di clienti e partner. La chiave per una governance efficace risiede in un approccio strutturato, nell'adozione di tecnologie avanzate e in una cultura aziendale orientata alla protezione dei dati e alla gestione responsabile delle informazioni.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/compliance-governance/