NIS2: UN'OPPORTUNITÀ DA NON PERDERE

Da Netalia alcune indicazioni sui temi della direttiva europea e i requisiti da soddisfare.

In vigore da ottobre 2024 la direttiva europea **NIS2** (**Network and Information Security Directive**), che disciplina le imprese e le agenzie governative nel settore cybersecurity, è l'evoluzione della precedente NIS1. Il suo obiettivo è di **rafforzare il livello collettivo di cybersicurezza degli Stati membri dell'Unione Europea**, aumentando i requisiti di applicazione per i settori delle infrastrutture critiche e, nel contempo, espandendo anche le sanzioni per chi non dovesse soddisfarli. "La nuova direttiva riguarda molti settori e in particolare si parla di tutte le organizzazioni che occupano una posizione critica nella società, al fine di rafforzare la resilienza informatica dell'Europa. Ecco che sono interessate anche realtà della produzione alimentare, della gestione dei rifiuti e l'intera catena di approvvigionamento. Inoltre viene fatta una distinzione tra 'aziende essenziali' e 'aziende importanti", spiega **Michele Zunino, Ceo di Netalia**.

Michele Zunino, Ceo di Netalia

Per quanto riguarda le aziende essenziali (sanzionate, se non conformi, con multe di rischio essenziale fino a 10 milioni di euro o il 2% del loro fatturato annuo globale) si fa riferimento ai settori Energia, Trasporti, Finanza, Salute, Acqua potabile e acque reflue, Infrastrutture digitali, Pubblica Amministrazione, Spazio. Per aziende importanti (multe fino a 7 milioni di euro o l'1,4% del loro fatturato annuo globale) si intendono invece quelle di Servizio postale e pacchi, Gestione dei rifiuti, Prodotti chimici (produzione e distribuzione), Alimenti (produzione e distribuzione), Produzione di apparecchiature, macchinari e veicoli parafarmaceutici, elettronici e ottici, Fornitori digitali dei mercati online, motori di ricerca e piattaforme social, Ricerca.

I requisiti da soddisfare

Relativamente ai requisiti la direttiva NIS2 ne aggiunge alcuni, andando a toccare quattro aree particolari: **responsabilità aziendale**, **reporting alle autorità**, **gestione del rischio** e **continuità operativa**. "Il livello dei requisiti varia a seconda delle dimensioni dell'azienda, della funzione sociale o dell'esposizione dell'organizzazione, ma per tutte le realtà sono previste alcune misure minime", prosegue Zunino. Senza voler essere esaustivi, proviamo a riassumerne alcune. Si parte dalla valutazione dei rischi e delle politiche di sicurezza per i sistemi informativi e da un piano per la gestione degli incidenti di sicurezza. Quindi si deve prevedere un piano per la gestione delle operazioni aziendali durante e dopo un incidente di sicurezza, con aggiornamento dei backup, e un piano per garantire l'accesso ai sistemi IT e alle loro funzioni operative, durante e dopo un incidente di sicurezza. E ancora, si devono soddisfare requisiti relativi alla sicurezza intorno alle catene di approvvigionamento e nel rapporto tra azienda e fornitore diretto. Sono poi richieste politiche e procedure per valutare l'efficacia delle misure di sicurezza ma anche sicurezza relativa all'approvvigionamento allo sviluppo e al funzionamento dei sistemi. Ciò significa disporre di criteri per la gestione e la segnalazione delle vulnerabilità.

Non manca anche il tema della formazione sulla sicurezza informatica e sulla 'Computer Hygiene' di base così come l'adozione di politiche e procedure per l'uso della crittografia e, se necessario, dell'encryption. E poi, l'implementazione di procedure di sicurezza per i dipendenti con accesso a dati sensibili o importanti, comprese le politiche per l'accesso ai dati. Per essere conforme alla NIS2 l'azienda deve anche avere una panoramica di tutte le risorse rilevanti e garantire che siano correttamente utilizzate e gestite. Infine, la direttiva prevede l'uso dell'autenticazione a più fattori, delle soluzioni di autenticazione continua, della crittografia vocale, video e testuale e delle comunicazioni di emergenza interne crittografate, quando appropriato.

Il ruolo di Netalia

Non c'è una soluzione as-a-Service per adeguarsi a NIS2, si tratta piuttosto di adottare una visione di filiera che riguarda tutti i processi aziendali e include fornitori, clienti e partner. **Occorre prima di tutto un nuovo orientamento culturale verso la sicurezza informatica**. "Servono partner affidabili, competenti e compliant per rispondere agli interrogativi e diffondere consapevolezza. In tale scenario il cloud di fatto semplifica la mitigazione dei rischi connessi alle violazioni, perché **delega al Service Provider certificato la responsabilità della gestione delle componenti abilitanti**. La nostra offerta 'Cloud Platform' è stata di fatto progettata e realizzata come layer di erogazione dei servizi, attraverso la quale i clienti hanno a disposizione servizi che soddisfano le esigenze di calcolo, custodia e controllo. **Il tutto con supporto del modello di compliance e security by design**", conclude Zunino.

www.netalia.it