

Sicuri di essere sicuri?

La Direttiva NIS 2: un passo importante per la Cybersicurezza a cura dell'Avv. Letizia Maria Ferraris, Presidente CSI Piemonte

Otto anni sono trascorsi dall'entrata in vigore del GDPR.

Grazie alle campagne di sensibilizzazione del Garante Privacy e ai media che hanno evidenziato la gravosità degli incidenti informatici e le conseguenti sanzioni comminate alle aziende, si è diffusa una maggior comprensione dell'importanza del "Regolamento Privacy", volto a proteggere i diritti e le libertà delle persone fisiche dai rischi derivanti dalla connessione in rete (art. 75 Considerando).

Otto anni sono anche passati dalla pubblicazione di un'altra norma europea, di cui poco si conosce, la Direttiva NIS, volta a migliorare e uniformare la cybersicurezza tra gli Stati membri dell'UE.

Negli ultimi anni è stato inoltre proposto un proliferare di compendi legislativi volti ad affrontare i numerosi profili di una società sempre più digitale e a prevenirne i rischi connessi, non ultimo il furto dei dati personali.

Ma le norme ci proteggono davvero? Appare piuttosto che i sofisticati 'scudi informatici' a protezione delle infrastrutture critiche (come quelle degli enti pubblici, che trattano normalmente dati 'particolari') cadano nel nulla anche solo a causa dell'accesso di un fornitore non strutturato, che permette al virus di cogliere di sorpresa i nostri software.

Voglio però pensare positivo: se le nostre vite sono ormai tradotte in dati, l'esistenza di norme attente al dettaglio è di gran valore, ancor più se queste forniscono il criterio per prevenire i pericoli a cui siamo sottoposti quotidianamente.

E così, dopo un periodo di applicazione caratterizzato da luci e ombre, nel gennaio dello scorso anno il Parlamento Europeo ha proposto una nuova versione della direttiva, rivolta a tutti gli Stati membri europei e da recepire entro il 17.10.2024 da un gran numero di categorie di enti e aziende.

La NIS2, nel sostituire la sorella maggiore, rappresenta la prima normativa comunitaria in materia di *cybersecurity* atta a rafforzare la risposta agli attacchi nel web, coeva ad altre iniziative come il *Cybersecurity Act* e il *Cyber Resilience Act*.

Una novità significativa che arriva in un momento storico in cui le minacce sono più insistenti, sofisticate, impattanti e con un tasso di elevata nocività.

Se pensiamo al settore sanitario ove migliaia di dati personali sono spesso stati pubblicati da *hacker* che chiedono riscatti per non rivelare informazioni sensibili... ne troviamo prove e controprove.

Non vi è dubbio che il periodo pandemico abbia accelerato la diffusione delle tecnologie digitali senza un corrispondente adeguamento delle misure di sicurezza. Con l'aumento della digitalizzazione in tutti i meandri della quotidianità era peraltro inevitabile un aumento della cosiddetta "superficie di cyberattacco", che ogni giorno sottopone cittadini, enti e aziende a rischio di danni anche irreversibili, come quelli reputazionali, economici, contrattuali....

Ecco la necessità di innalzare il livello e il perimetro di protezione dei sistemi, armonizzare gli impegni assunti singolarmente con la cooperazione tra i popoli e adottare insieme le misure a tutela dei sistemi informatici, in termini di ‘disponibilità’, ‘confidenzialità’ e integrità’ dei beni o asset di quei sistemi.

Se dunque in questo momento storico l’umanità in ogni sua declinazione (imprenditoriale e amministrativa, sociale e associativa, familiare e personale, di qualsiasi età o estrazione sociale) si sente unita e solidale nella ricerca di soluzioni tecniche, dovrà esserlo anche nella formazione e nella ricerca di consapevolezza e competenze.

C’è tuttavia qualche nodo che potrebbe rendere complesso adeguarsi in tempi rapidi, creare team aziendali idonei, conformarsi a prescrizioni tanto impegnative.

La NIS 2 e gli Enti più piccoli

Se infatti l’obiettivo è colmare i *gap* tra stati e, prima ancora, tra enti, perché escludere quelli al di sotto di centomila abitanti? Anche senza un obbligo di legge specifico, in un’ottica di solidarietà e sussidiarietà giuridica, i capisaldi della formazione, prevenzione e percezione delle minacce dovrebbero assurgere un ruolo imprescindibile nel sostenere enti piccoli o grandi ad applicare regole e principi.

La NIS 2 e il Sistema Paese

Se poi la direttiva intende rafforzare i livelli di *security* informatica, estendendola a settori prima esclusi (alimentare, chimico, servizi digitali, ricerca scientifica...) tale obiettivo non potrà coinvolgere la sola Pubblica Amministrazione, ma dovrà rivolgersi anche a tutti i suoi fornitori.

Il Sistema Paese è interconnesso, non è scindibile: alla caparbietà degli attacchi che non distingue tra loro le organizzazioni, pubbliche e private, grandi o piccole, deve corrispondere una pari capacità di attenzione e organizzazione di contrasto.

Fornitori e clienti costituiscono un tutt’uno di fronte alla creazione di standard di adeguatezza per assicurare la protezione delle infrastrutture critiche nazionali e la doverosa fiducia dei cittadini nei processi digitali.

Vi è poi la continuità operativa da proteggere: solo monitorando le misure di sicurezza lungo tutta la catena (inclusi i fornitori, appunto) anche l’operatività della PA sarà stabile e affidabile, evitando interruzioni nei servizi essenziali e quei furti che, con gravi ripercussioni sulla società civile, interrompono (invece che facilitare) un’efficiente e sicura erogazione di servizi.

I destinatari effettivi

L’adeguamento previsto da NIS 2 prevede infine *policy*, processi e procedure di gestione del rischio, alti livelli di salvaguardia e continuità operativa, fino alla gestione di incidenti e crisi, adottando modelli didattici avanzati, come le simulazioni basate su scenari realistici.

Va da sé che dette caratteristiche richiedano un insieme di competenze che non potranno essere destinate alle sole governance, ma dovranno coinvolgere tutti i processi aziendali e tutti i livelli della gestione del rischio: la ‘sicurezza delle persone fisiche’ e quindi la conoscenza dei processi, non può riguardare solo i top manager.

Insomma, in un contesto di ‘dati continuamente in movimento’ quali siamo diventati tutti noi indistintamente, la NIS 2 potrebbe rappresentare, con le giuste interpretazioni, una delle tappe strategiche per crescere in cultura e consapevolezza digitale.

Non si può che auspicare un impegno condiviso, una linea d'azione integrata e una cooperazione tra pubblico e privato, per garantire nel prossimo futuro un ambiente tecnologico idoneo a tutelare i nostri dati nel cyberspazio.

© 2024 CIVICO20NEWS – riproduzione riservata

Data di pubblicazione: 25/07/2024

Salvato in PDF in data: 23/10/2026

Link all'articolo: <https://civico20-news.it/la-tutela-dei-dati-personali/sicuri-di-essere-sicuri-2/25/07/2024/>