Digeat N.4 - 19 Dicembre 2024

La NIS 2 in Italia: un rinforzo “artigianale” per la cybersecurity

Di Claudio Anastasio

Abstract

L’entrata in vigore della Direttiva NIS-2 in Italia regolamenta la sicurezza informatica in maniera nuova e più stringente, soprattutto per le infrastrutture critiche e i servizi digitali essenziali. La normativa impone nuovi obblighi specifici di sicurezza. Eventi come lo scandalo “Equifax” e “Equalize” evidenziano l’urgenza di tali misure. La NIS-2, ad esempio, avrebbe costretto ad introdurre misure più rigorose per prevenire simili abusi. La nuova direttiva promuove una maggiore collaborazione tra pubblico e privato, introduce sanzioni significative per le violazioni e impone alle organizzazioni di adottare misure tecnico-organizzative più robuste. L’obiettivo è chiaro: proteggere i dati dei cittadini, garantire la continuità operativa e migliorare la competitività del Paese nel panorama digitale.

Indice

L’entrata in vigore del Decreto Legislativo n.138/2024, che recepisce la Direttiva NIS-2 in Italia, segna un punto di svolta nella gestione della sicurezza informatica nel nostro Paese. Questa normativa, più stringente rispetto alla precedente NIS, introduce una serie di obblighi e misure volte a garantire **un livello di sicurezza informatica più elevato** per le infrastrutture critiche e i servizi digitali essenziali.

La NIS-2 amplia notevolmente l’ambito di applicazione rispetto alla precedente direttiva, coinvolgendo un numero maggiore di organizzazioni, incluse le piccole e medie imprese che operano in settori strategici.

NIS-2: un rinforzo operativo concreto

Per sottolineare l’importanza della Direttiva, è utile partire da un esempio concreto di attacco informatico di rilievo occorso nello scandalo “Equifax”, con tutte le sue implicazioni.

Nel 2017, “Equifax”, una delle principali agenzie di credito a livello mondiale, subì **una massiccia violazione dei dati che coinvolse oltre 147 milioni di consumatori**. Gli hacker riuscirono a sfruttare una vulnerabilità nel software di “Equifax”, accedendo a informazioni personali sensibili, come numeri di previdenza sociale, date di nascita e numeri di carte di credito.

Se la NIS-2 fosse stata in vigore al momento dell'attacco, "Equifax", in quanto soggetto essenziale, avrebbe individuato e corretto la vulnerabilità, come quella sfruttata dagli hacker.

Un altro esempio, altrettanto concreto, riguarda il caso di "Equalize", verificatosi in Italia nel 2024 e avente ad oggetto il furto di dati relativi a 800mila persone "spiate". Con l'adozione della NIS-2, anche i log degli accessi da parte delle persone autorizzate (Amministratori di Sistema) sono periodicamente controllati da terze parti e, comunque, i dati sensibili sarebbero stati crittografati, atteso che le chiavi di decodifica non possono essere conservate dagli stessi soggetti (Amministratori di Sistema) che accedono ai dati medesimi. In questo modo, qualsiasi tentativo di abuso nell'estrazione e copia di dati sarebbe stato vanificato.

> Tra le principali novità introdotte con la NIS-2, emerge che le organizzazioni sono state classificate in "soggetti essenziali" e "soggetti importanti"[1], a seconda del loro impatto sulla società e sull'economia in caso di incidente informatico, con obblighi di sicurezza più stringenti.

I soggetti interessati dovranno adottare **misure di sicurezza più rigorose**, come la gestione dei rischi informatici, la formazione del personale, la risposta agli incidenti informatici e la gestione della continuità operativa. In caso di incidenti informatici significativi, le organizzazioni dovranno notificarli alle autorità competenti entro tempi ben definiti. Viene promossa una maggiore collaborazione tra le autorità pubbliche e le organizzazioni private per la gestione delle minacce informatiche e si dovrà istituire una governance della sicurezza efficace, con la nomina di un responsabile per la sicurezza informatica.

La classificazione delle organizzazioni

La Direttiva NIS-2, infatti, introduce **una classificazione dettagliata delle organizzazioni**, suddividendole in **soggetti essenziali e soggetti importanti**. Questa distinzione ha un impatto diretto sulle misure di sicurezza da adottare e sugli obblighi di notifica degli incidenti.

I soggetti essenziali sono considerati di vitale importanza per il funzionamento della società e dell'economia. Essi sono esposti a un rischio più elevato di incidenti informatici che potrebbero avere conseguenze significative a livello nazionale o transnazionale. **Rientrano in questa categoria di soggetti tutti i fornitori dei servizi qualificati eIDAS (Reg. UE n. 910/2014)**[2], tra i quali i fornitori di firme digitali, di certificati SSL, di servizi elettronici di recapito certificato qualificato, di identificazione elettronica e di conservazione dei documenti informati in aggiornamento a eIDAS-2[3].

Il Decreto legislativo 138/2024, entrato in vigore il 18 ottobre 2024, ha recepito le disposizioni della Direttiva NIS-2. Sebbene il decreto legislativo abbia fissato una data di entrata in vigore generale, potrebbero esserci scadenze più specifiche per determinate disposizioni o per categorie di soggetti (es. PMI, grandi imprese). La fase di transizione prevede un periodo di tempo per adeguare i sistemi informatici e processi ai nuovi requisiti.

Dal 1° gennaio 2026, entrerà in vigore il sistema sanzionatorio, principalmente di natura amministrativa pecuniaria. L'importo delle sanzioni può variare in base alla gravità della violazione e alla dimensione dell'organizzazione, su base progressiva fino a dieci milioni di euro. Oltre alle sanzioni pecuniarie, potrebbero esserci altre conseguenze, come la sospensione o la revoca di autorizzazioni o licenze, fino all'interdizione dal ruolo per i responsabili dirigenti e amministratori.

> L'attuazione della NIS-2 richiede, pertanto, un adeguamento significativo da parte delle organizzazioni interessate. I tempi per la piena attuazione della normativa sono relativamente brevi (tutti ricompresi in tappe successive nel corso dell'anno 2025), e ciò comporta sfide non indifferenti, soprattutto per la Pubblica Amministrazione.

L’impatto lato Pubblica Amministrazione

L’impatto su quest’ultima, invero, è particolarmente significativo. **L’adeguamento ai nuovi standard di sicurezza potrebbe richiedere la sospensione di attuali contratti di fornitura**, in quanto i fornitori esistenti potrebbero non essere in grado di garantire la conformità alla NIS-2. Di conseguenza, le amministrazioni pubbliche saranno chiamate a **selezionare nuovi fornitori** in grado di offrire servizi e soluzioni conformi alla normativa.

Le conseguenze di questa situazione sono molteplici, con **un aumento dei costi** per la selezione di nuovi fornitori e l’adeguamento dei sistemi informatici per la Pubblica Amministrazione. I processi di gara e di selezione dei nuovi fornitori potrebbero **causare ritardi o sospensioni** nell’erogazione dei servizi ai cittadini. Le amministrazioni pubbliche dovranno, quindi, affrontare una maggiore complessità nelle procedure di acquisto e gestione dei contratti di fornitura in ambito IT.

> L’implementazione della NIS-2 richiede un approccio proattivo per la valutazione iniziale dei rischi, al fine di identificare le vulnerabilità e le minacce più significative. Sarà necessario elaborare una roadmap dettagliata per l’implementazione delle misure di sicurezza, tenendo conto delle risorse disponibili e delle scadenze. Allo stesso modo, si renderà opportuno coinvolgere tutti gli stakeholders, dalla direzione generale al personale operativo, nel processo di implementazione.

Per la conformità alla NIS-2, le organizzazioni dovranno adottare **nuove misure tecniche ed organizzative per implementare sistemi di gestione degli accessi efficaci**, volti a limitare l’accesso ai sistemi e ai dati solo al personale autorizzato, con segregazione fisica e logica degli accessi alle chiavi di crittografia. Dovranno proteggere le reti aziendali da attacchi esterni attraverso l’utilizzo di firewall, sistemi di rilevamento delle intrusioni e altre tecnologie di sicurezza. Ancora, sarà necessario effettuare regolarmente backup dei dati e testarne il ripristino per garantire la continuità operativa, organizzare programmi di formazione e sensibilizzazione del personale sulla sicurezza informatica, definire procedure chiare per la gestione degli incidenti informatici, dalla detection alla risposta.

Le organizzazioni saranno altresì chiamate ad **elaborare piani di continuità operativa per garantire il funzionamento dei servizi essenziali in caso di incidente informatico**, valutare attentamente i fornitori di servizi IT per verificarne la conformità ai requisiti di sicurezza della NIS-2, monitorare costantemente la sicurezza dei sistemi informatici per identificare tempestivamente eventuali anomalie. Infine, dovranno aggiornare regolarmente le misure di sicurezza, in base all’evoluzione del panorama delle minacce informatiche.

La NIS-2 avrà un impatto significativo, oltre che per la Pubblica Amministrazione, anche sulle aziende e gli operatori fornitori di servizi essenziali. Questi soggetti, infatti, dovranno affrontare sfide importanti per adeguarsi ai nuovi standard di sicurezza. Le aziende dovranno investire in nuove tecnologie e soluzioni di sicurezza per garantire la conformità alla NIS-2, formando adeguatamente il personale sulle nuove misure di sicurezza.

La protezione del cittadino

La NIS-2 ha come obiettivo primario **la protezione dei dati dei cittadini**. Grazie all’introduzione di misure di sicurezza più rigorose, si prevede una **riduzione del rischio di attacchi informatici e di conseguenti violazioni dei dati personali**, anche se per opera di interni dipendenti infedeli, attraverso – come sopra – la **segregazione dei ruoli** tra l’accesso ai dati e le chiavi di crittografia degli stessi (unico modo per aumentare la tutela dei dati anche da parte del personale interno che vi ha accesso per uso improprio, non potendo un’estrazione su dati crittografati essere così facilmente decodificata).

> La Direttiva rafforza la protezione dei dati personali, in linea con il Regolamento Generale sulla Protezione dei Dati (GDPR). Le procedure di gestione degli incidenti informatici più stringenti permetteranno di limitare i danni in caso di violazione dei dati. Le organizzazioni dovranno essere più trasparenti nei confronti dei cittadini in merito alle misure di sicurezza adottate e agli eventuali incidenti informatici.

L'Agenzia per la Cybersicurezza Nazionale (ACN) è l'Autorità deputata alla vigilanza, mediante la tenuta di un registro pubblico dei soggetti e delle organizzazioni sottoposti al regime della Direttiva.

Conclusioni

La Direttiva rappresenta una sfida, ma anche un'opportunità, per le organizzazioni italiane, di rafforzare la propria sicurezza informatica. L'adeguamento ai nuovi requisiti è fondamentale per proteggere i dati dei cittadini, come è emerso dagli ultimi fatti di cronaca nazionale, nonché per garantire la sicurezza dei dati, la continuità operativa e migliorare la competitività delle imprese italiane a livello internazionale.

La NIS-2 porterà a un aumento del livello di sicurezza informatica in Italia, con maggiore protezione dei dati dei cittadini, mai conseguita finora in maniera così stringente ed elevata.

NOTE

[1] A tal proposito, si veda l'art. 3 della Direttiva 2022/2555 (Nis-2)

[2] In tal senso, si veda il Reg. UE n. 910/2014 e, in particolare, gli artt. 20 e ss.; qui il testo integrale.

[3] In Italia, il D. Lgs. N. 82/2005 (Codice dell'Amministrazione Digitale), stabilisce che i soggetti che intendono fornire servizi fiduciari qualificati devono presentare all'AgID domanda di qualificazione, secondo le modalità indicate all'articolo 29. Per consultare il testo integrale si veda qui.