assonime

Associazione fra le società italiane per azioni

2/2025

Position Papers

Nis 2: la cybersicurezza come “punto di appoggio” e “leva” sicura per favorire lo scambio dei dati

Priorità della Strategia europea è l’accesso, la condivisione e la circolazione dei dati, in quanto presupposto e volano per l’utilizzo delle nuove tecnologie data-driven e, in ultima istanza, per il recupero della produttività e della competitività delle singole imprese e del sistema[1]. Attraverso misure ed azioni che ora si inscrivono nel Digital Compass, l’Unione continua a rinforzare la “fiducia” nello scambio dei dati, facendo leva anche sulle nuove regole in tema di cybersicurezza.

È questa una esigenza sollecitata dall’attuale contesto digitale in cui il rischio cyber è in costante crescita ed espone le imprese di ogni dimensione e settore a nuovi rischi, come la perdita di dati sensibili, furti di proprietà intellettuale e interruzioni di attività, con conseguenze disastrose sia sul piano economico e legale, che in termini reputazionali. Nel pervasivo processo di digitalizzazione non solo aumenta la “superficie digitale” aggredibile, ma si assiste anche ad una crescente dipendenza da fornitori terzi di servizi digitali per funzioni critiche (ad esempio infrastrutture cloud as a service, piattaforme e svariati servizi in outsourcing). Vi sono, poi, significativi livelli di concentrazione nell’utilizzo di tali servizi verso un numero limitato di fornitori terzi, che possono innescare fenomeni di contagio ed elevare il potenziale impatto sistemico di singole minacce o attacchi cyber.

Secondo il “Cost of a Data breach Report 2024”, elaborato da IBM, il costo medio di una violazione dei dati derivante da attacchi cyber, a livello globale, è passato da 4,45 milioni a 4,88 milioni di dollari nel 2023. L’Italia è il quinto paese al mondo per vulnerabilità cyber secondo la classifica del Report, e ha raggiunto un costo medio di 4,73 milioni di dollari nel 2024, con un incremento del 23% rispetto al 2023, a fronte di violazioni sempre più dannose[2]. La sanità e il settore finanziario sono quelli che risultano più sotto attacco e colpiti. Anche le imprese industriali e quelle del settore tecnologico hanno registrato violazioni particolarmente onerose, seguite da quelle del settore energetico e della farmaceutica.

Per rispondere, dunque, al nuovo panorama dei rischi cyber, caratterizzato dall’intensa digitalizzazione e da crescenti tensioni geopolitiche, l’Europa ha deciso di proseguire lungo il percorso delineato dalla prima direttiva Nis e, con la direttiva “Nis 2”, ha posto un nuovo fondamentale tassello nella definizione di un quadro adeguato di cybersicurezza.

[1] Cfr. Approfondimento Assonime n. 2/2024, “Il governo e la valorizzazione dei dati come leva di competitività delle imprese”.

[2] Secondo il Report, il 40% delle violazioni in Italia ha riguardato dati archiviati su ambienti multipli (tra cui cloud pubblico, cloud privato e on-prem) e il 29% su cloud pubblico.

Recepita in Italia dal decreto legislativo n. 138/2024, la direttiva Nis 2 interviene su diversi fronti[3].

In primo luogo, aggiorna e amplia l’ambito di applicazione, identificando nuovi soggetti e nuovi settori sottoposti agli obblighi di cybersicurezza, dividendo questi in settori altamente critici e critici, e i soggetti in essenziali e importanti, in funzione della importanza per il settore o il tipo di servizi che forniscono, che rileva, in particolare, ai fini sanzionatori.

In secondo luogo, rafforza e definisce in modo puntuale gli obblighi di cybersicurezza imposti alle imprese, regolando anche il tema della sicurezza delle catene di approvvigionamento e dei rapporti con i fornitori. Gli organi di amministrazione e direttivi dei soggetti essenziali e importanti sono gravati della responsabilità di assicurare il rispetto di tali obblighi.

Infine, vengono introdotte misure di vigilanza più rigorose e un sistema sanzionatorio più severo.

Così delineato, il quadro regolatorio promuove una vera e propria “disruption” nella gestione della cybersecurity, che non è più relegata a questioni di stretta sicurezza IT, ma si impone nelle strategie di gestione e nei piani di sviluppo aziendale, acquisendo “centralità” nella organizzazione, governance e attività dell’impresa, con un impatto significativo sulla stabilità finanziaria, sulla produttività e sulla reputazione dell'organizzazione aziendale.

La previsione di chiare responsabilità in capo agli organi di amministrazione e direttivi dell’impresa innesca una “spinta più che gentile”, incentivando gli organi di corporate governance a partecipare attivamente e costantemente al processo decisionale sulla cybersicurezza, in particolare attraverso una relazione diretta e flussi costanti di informazioni, con i soggetti deputati a governare la cybersecurity all’interno dell’impresa.

La cybersicurezza esprime perciò una nuova dimensione su cui esercitare la *business judgment rule* in seno agli organi di governo societario di ogni impresa, in tema, ad esempio, di adeguatezza degli investimenti in cybersecurity e della qualità dei presidi tecnologici e organizzativi per far fronte alle minacce cyber. Il coinvolgimento pro-attivo di tali organi contribuisce, inoltre, a promuovere una cultura aziendale orientata alla correttezza nei rapporti e, dunque, alla sicurezza delle relazioni, trasmettendo un

[3] Per un’analisi del decreto legislativo n. 138/2024, cfr. circolare Assonime n. 1/2025.

segnale forte, all’interno dell’organizzazione, sull’importanza della cybersicurezza e, all’esterno della stessa, in termini di rinnovata reputazione e credibilità sul mercato.

Da questo punto di vista, la Nis 2 ravviva il tema della formazione e, più ampiamente, della alfabetizzazione in materia di sicurezza informatica, in quanto cruciale per una gestione corretta ed efficace della cybersicurezza. Come ribadito in più occasioni dall’ENISA, Il fattore umano è spesso considerato l’aspetto più vulnerabile di un sistema di sicurezza informatica, per cui negli ultimi anni si è dato crescente rilievo all’igiene informatica, che è fondamentale per prevenire numerosi incidenti di sicurezza.

In conclusione, ciò che viene richiesto come “punto di appoggio” e “leva” sicura per lo scambio dei dati è un vero salto culturale e un deciso spostamento di baricentro, nel senso che non basta interpretare ed applicare gli obblighi previsti dalla normativa Nis 2 in modo formale, ma si tratta di far proprio un nuovo approccio che ponga gli aspetti di cybersecurity tra le priorità da considerare negli assetti organizzativi e in ogni fase di sviluppo imprenditoriale.

Proprio in un nuovo modello di “cybersecurity integrata” in ogni operazione e processo dell’impresa, risiede la “chiave di volta” perché sia possibile, da una parte, tutelare i dati all’interno dell’impresa, e dall’altra, valorizzarli e condividerli all’esterno per sfruttare appieno e con fiducia il loro valore.