WHITEPAPER

STANDARDIZZAZIONE, CYBERSECURITY E RESPONSABILITÀ INDIVIDUALE

Note a margine dell'attuazione della direttiva NIS 2 in Italia

AVV. GIUSEPPE SERAFINI

INDICE ARGOMENTI

1 IMPORTANZA DELLA STANDARDIZZAZIONE NELLA SICUREZZA INFORMATICA

2 LA DIRETTIVA NIS 2 E LE NUOVE RESPONSABILITÀ PER LE ORGANIZZAZIONI

3 IL NIST CSF 2.0 E LA SUA RILEVANZA PER LA DIRETTIVA NIS 2

4 STRUMENTI DI SUPPORTO: PIATTAFORME DI ENISA E CISA

5 STANDARDIZZAZIONE E RESPONSABILITÀ ORGANIZZATIVA

6 RESPONSABILITÀ INDIVIDUALE E COLPA NEL CONTESTO INFORMATICO

7 CAUSALITÀ E RESPONSABILITÀ NELLE DECISIONI GIURIDICHE

Nell'era digitale, la sicurezza delle informazioni è una priorità critica per le organizzazioni e le persone fisiche, il crescente numero di minacce informatiche, come violazioni dei dati e attacchi ransomware, rende necessario un approccio sistematico e uniforme per proteggere le infrastrutture digitali.

La standardizzazione in materia di sicurezza delle informazioni svolge un ruolo cruciale in questo contesto, fornendo linee guida e best practice che non solo migliorano la sicurezza, ma determinano anche il grado di responsabilità delle organizzazioni e delle persone fisiche in relazione alla commissione di illeciti o reati informatici.

In questo ambito, la Direttiva NIS 2 (Network and Information Security) dell'Unione Europea, adottata nel 2022, rappresenta un importante sviluppo normativo che rafforza il senso delle considerazioni appena svolte, ampliando il campo di applicazione e introducendo nuovi obblighi per garantire un elevato livello di sicurezza in tutta l'UE.

Come è noto, la standardizzazione nel campo della sicurezza delle informazioni implica l'adozione di norme, politiche, protocolli e procedure uniformi che aiutano le organizzazioni a gestire, proteggere e rispondere a incidenti di sicurezza.

Standard come la serie 27000, che fornisce un framework per un sistema di gestione della sicurezza delle informazioni, e copre vari aspetti della gestione della sicurezza, sono ampiamente riconosciuti e adottati a livello globale, anche perché non solo definiscono le misure tecniche necessarie per proteggere le informazioni, ma stabiliscono anche processi per la gestione del rischio, la formazione del personale e la risposta agli incidenti.

Attraverso l'adozione di tali standard, le organizzazioni possono dimostrare di aver adottato misure adeguate e proporzionate per proteggere le proprie infrastrutture digitali e i dati personali, il che può influenzare significativamente la determinazione del grado di responsabilità in caso di violazione.

Rispetto alla Direttiva NIS originale del 2016, la NIS 2 amplia il campo di applicazione includendo un maggior numero di settori e organizzazioni che operano in infrastrutture critiche. Inoltre, introduce requisiti più rigorosi in termini di gestione del rischio e misure di sicurezza, e rafforza il regime di vigilanza e di applicazione delle norme.

Uno degli aspetti chiave del Decreto di recepimento è l'obbligo per le organizzazioni di adottare misure tecniche e organizzative adeguate per gestire i rischi per la sicurezza delle reti e dei sistemi informativi.

Questo implica, dal punto di vista di chi scrive, la necessità di conformarsi a standard riconosciuti a livello internazionale, il che sottolinea ulteriormente l'importanza della standardizzazione. Le organizzazioni che non riescono a conformarsi a questi requisiti potrebbero essere soggette a sanzioni significative, e la loro responsabilità in caso di incidente potrebbe essere aggravata dalla mancanza di conformità.

Il NIST Cybersecurity Framework (CSF) 2.0, la versione aggiornata del framework di sicurezza informatica sviluppato dal National Institute of Standards and Technology (NIST), introduce miglioramenti e aggiornamenti chiave per aiutare le organizzazioni a gestire meglio i rischi cibernetici. Il framework, che è riconosciuto a livello globale, è particolarmente rilevante in relazione alla Direttiva NIS 2, poiché offre un approccio strutturato e scalabile alla gestione della sicurezza informatica.

Il NIST CSF 2.0 si basa su cinque funzioni principali: Identificare, Proteggere, Rilevare, Rispondere e Recuperare, che coprono l'intero ciclo di vita della gestione del rischio e l'aggiornamento alla versione 2.0 introduce un focus maggiore su settori emergenti come la supply chain, la sicurezza dell'intelligenza artificiale e la resilienza operativa, tutte aree di interesse anche per la NIS 2.

Secondo chi scrive, l'integrazione delle pratiche raccomandate dal NIST CSF 2.0 all'interno del contesto europeo non solo può facilitare la conformità alla NIS 2, ma può anche migliorare la capacità delle organizzazioni di prevenire, rilevare e rispondere a incidenti di sicurezza informatica, riducendo così il rischio di responsabilità legali e di sanzioni.

Un ulteriore supporto all'implementazione degli standard di sicurezza informatica è offerto dagli strumenti messi a disposizione da agenzie come ENISA (Agenzia dell'Unione Europea per la cybersicurezza) e CISA (Cybersecurity and Infrastructure Security Agency degli Stati Uniti).

Queste organizzazioni forniscono risorse pratiche e strumenti utili per valutare e migliorare la maturità della cybersicurezza, specialmente nelle piccole e medie imprese (PMI). ENISA, ad esempio, ha sviluppato una piattaforma dedicata all'assessment della maturità della cybersicurezza delle PMI, che permette alle organizzazioni di misurare il loro livello di sicurezza informatica in relazione a standard internazionali e best practice.

La piattaforma offre una serie di questionari e guide che aiutano le PMI a identificare le aree critiche da migliorare e a definire piani d'azione concreti, parallelamente, CISA ha rilasciato il "Cyber Security Evaluation Tool (CSET)", un software gratuito che consente alle organizzazioni di eseguire valutazioni dettagliate della loro sicurezza informatica.

Il CSET funziona guidando gli utenti attraverso una serie di domande e scenari basati su standard riconosciuti, come il NIST CSF e la Direttiva NIS 2, per identificare le vulnerabilità e le carenze nelle loro difese informatiche e genera un report dettagliato che evidenzia i punti di forza e di debolezza, offrendo raccomandazioni pratiche per colmare le lacune rilevate.

L'uso combinato di questi strumenti facilita l'adozione degli standard di sicurezza, consentendo alle organizzazioni di migliorare continuamente il loro stato di preparazione contro le minacce informatiche e di dimostrare la conformità alle normative, riducendo così il rischio di esposizione a responsabilità legali.

Da un punto di vista strettamente legale, la standardizzazione offre un criterio oggettivo per valutare il grado di responsabilità delle organizzazioni e delle persone fisiche in relazione alla commissione di illeciti o reati informatici.

Quando un'organizzazione adotta standard riconosciuti e implementa misure di sicurezza adeguate, dimostra una diligenza dovuta nella protezione delle informazioni e delle reti., il che può costituire un argomento di difesa significativa in caso di incidenti, riducendo il rischio di essere considerata responsabile per negligenza. Al contrario, la mancata adozione di standard appropriati può essere interpretata come un segno di trascuratezza o negligenza, aumentando il grado di responsabilità dell'organizzazione in caso di violazione della sicurezza.

La Direttiva NIS 2, con il suo approccio rigoroso alla conformità e alla responsabilità, rende evidente che le organizzazioni devono prendere sul serio la sicurezza delle informazioni e adottare le misure necessarie per proteggere i loro sistemi, in particolare ove si consideri che, anche le persone fisiche, segnatamente i dirigenti e i responsabili della sicurezza informatica all'interno delle organizzazioni, possono essere ritenute personalmente responsabili in caso di mancata adozione di misure adeguate: la legge prevede infatti che i responsabili della gestione della sicurezza siano tenuti a garantire che le organizzazioni siano conformi alle misure richieste.

La responsabilità individuale può derivare, ad esempio, per semplificare, dalla mancata supervisione adeguata, dalla negligenza o dall'ignoranza delle normative vigenti.

In ambito informatico, la giurisprudenza ha sviluppato criteri specifici per determinare la colpa individuale, che si basano su vari fattori legali e tecnici. Uno dei criteri chiave è il principio della diligenza qualificata, che valuta se l'individuo ha agito con la competenza e la prudenza richieste dal suo ruolo specifico.

Questo principio implica che professionisti con responsabilità in ambito informatico, come i responsabili della sicurezza o i dirigenti IT, devono non solo seguire le best practice e gli standard di settore, come quelli previsti dal NIST CSF o da ISO, ma anche mantenersi aggiornati sulle evoluzioni normative e tecnologiche.

La giurisprudenza considera inoltre il livello di consapevolezza del rischio dell'individuo, ovvero se egli fosse a conoscenza delle minacce specifiche e se abbia preso misure adeguate a mitigare tali rischi; è evidente che l'omissione di misure preventive o la mancata risposta tempestiva agli incidenti possono essere interpretate come negligenza grave, specialmente quando l'individuo ricopre una posizione di responsabilità.

Infine, i giudici esaminano la causalità tra l'azione o l'omissione dell'individuo e il danno subito, determinando se un comportamento più diligente avrebbe potuto prevenire o limitare il danno. Questo processo implica la valutazione di quale ruolo specifico ha avuto l'azione o l'inerzia dell'individuo nel permettere o aggravare l'incidente informatico.

Per esempio, se un responsabile IT ha omesso di applicare un aggiornamento di sicurezza cruciale che avrebbe potuto prevenire una violazione dei dati, i giudici esamineranno se tale aggiornamento fosse una misura ragionevole e facilmente implementabile, nonché se fosse stato previsto dagli standard del settore.

L'analisi della causalità considera anche se un comportamento più diligente avrebbe realisticamente potuto evitare l'incidente o mitigarne gli effetti. In altre parole, il tribunale valuta se, in presenza di una condotta conforme agli standard di diligenza, il danno sarebbe stato evitato o significativamente ridotto.

Se viene stabilito che il danno è direttamente conseguente all'omissione o all'azione negligente, l'individuo può essere ritenuto responsabile civilmente o penalmente per l'illecito informatico. Questo principio di causalità è cruciale poiché non solo stabilisce la responsabilità, ma può anche influenzare l'entità delle sanzioni o dei risarcimenti dovuti.

Alla luce della Direttiva NIS 2, l'adozione di standard riconosciuti diventa non solo una best practice, ma un obbligo legale che influisce direttamente sulla determinazione del grado di responsabilità delle organizzazioni e delle persone fisiche.
Anche perché, oltre alla semplice conformità, la standardizzazione favorisce una cultura della responsabilità all'interno delle organizzazioni; definendo chiaramente le aspettative e le responsabilità per la sicurezza delle informazioni, gli standard responsabilizzano le persone a prendersi cura del proprio ruolo nella protezione dei dati sensibili, questo crea un senso di responsabilità condivisa, in cui ogni attore comprende il proprio contributo alla sicurezza generale dell'organizzazione.

In caso di violazione, questa chiarezza consente di identificare rapidamente i responsabili, garantendo che vengano prese misure correttive e che si apprenda dagli errori.

Sebbene la standardizzazione sia indubbiamente preziosa, è essenziale riconoscerne i limiti; la natura dinamica delle minacce informatiche richiede che le misure di sicurezza rimangano adattabili ed evolvano di pari passo con il panorama delle minacce.

Inoltre, nessuno standard può offrire una garanzia assoluta di protezione, attaccanti evoluti possono ancora cercare di trovare modi per violare anche le difese più solide.

Avv. Giuseppe Serafini

Giuseppe Serafini è Avvocato Cassazionista del Foro di Perugia. Lead Auditor ISO/IEC 27001:2013, ISO/IEC 27701:2019; DPO UNI 11697:2017. Master di II° livello in Cybersecurity. Master di II° livello in Data Protection. Perfezionato in Digital Forensicis, Cloud & Data Protection. Già docente di Informatica Giuridica presso la Scuola di Specializzazione in Professioni Legali di Perugia, e collaboratore della cattedra di Informatica Giuridica della Facoltà di Giurisprudenza di Perugia; Docente in Master di II° livello. Relatore ed autore di numerose pubblicazioni in materia di Sicurezza delle Informazioni e Diritto delle nuove Tecnologie. Associato CLUSIT e Digital Forensics Alumni.