LA DIRETTIVA NIS2: NUOVI OBBLIGHI E OPPORTUNITÀ

La recente relazione Threat landscape 2021 dell'Agenzia dell'Unione europea per la sicurezza informatica (Enisa) sottolinea che gli attacchi cibernetici sono aumentati nel 2020 e nel 2021. Non soltanto in termini di vettori e numeri, ma anche in termini di impatto, sotto la spinta della pandemia Covid-19. Eppure aziende e istituzioni europee spendono il 41% in meno per la sicurezza informatica rispetto agli Stati Uniti. La Commissione per l'industria, la ricerca e l'energia del Parlamento europeo ha dato il via libera ad ampia maggioranza alla bozza della nuova direttiva, già ribattezzata Nis 2, e all'apertura di negoziati con il Consiglio europeo. La proposta prevede requisiti più stringenti per imprese, amministrazioni e Stati in termini di gestione del rischio, obblighi di segnalazione e condivisione delle informazioni, facendo chiarezza sugli equilibri tra la direttiva e le norme europee in materia di privacy (Gdpr e ePrivacy) che attualmente rappresentano un freno alla condivisione delle informazioni tra i Paesi.

Davide PIERATTONI è ingegnere gestionale e dottore di ricerca in ingegneria industriale e dell'informazione. Già ricercatore di ruolo in sistemi di elaborazione all'Università di Udine, è responsabile della sicurezza delle informazioni di Innova S.p.A. Con oltre 20 anni di esperienza nell'Information Technology, si occupa di sicurezza, privacy e compliance di settore.

Il Consiglio e il Parlamento Europeo hanno raggiunto il 13 maggio 2022 un accordo provvisorio sulla Direttiva NIS2, recante nuove misure per un comune ed elevato livello di cybersecurity in tutta l'Unione, al fine di migliorare ulteriormente la resilienza e le capacità di risposta agli incidenti informatici sia del settore pubblico e privato dei singoli Stati membri, sia dell'UE nel suo complesso. Una volta adottata, la NIS2 sostituirà l'attuale Direttiva (EU) 2016/1148 nota come NIS (Network and Information Systems) sulla sicurezza delle reti e dei sistemi informativi [1].

Ampliamento del campo di applicazione

Nell'attuale bozza [2], il *framework* NIS2 obbliga specifiche categorie ad adottare misure tecniche e organizzative per gestire i rischi sulla sicurezza delle reti e dei sistemi informativi. L'Annex I della nuova Direttiva elenca i **soggetti essenziali**: energia, trasporti, banche, infrastrutture del mercato finanziario, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. L'Annex II invece identifica i **soggetti importanti**: servizi postali e corrieri, gestione dei rifiuti, produzione e distribuzione di prodotti chimici, produzione, lavorazione e distribuzione di alimenti, produzione di apparecchiature medicali e fornitori digitali (intesi come provider di motori di ricerca online, di piattaforme di servizi di social network e di mercati online).

Ai soggetti essenziali si applica un rigoroso regime di vigilanza *ex ante*, mentre i soggetti importanti sono sottoposti a una vigilanza *ex post* che interviene in caso di rilievi o segnalazioni di non conformità.
Le micro- e le piccole imprese – identificate secondo la raccomandazione 2003/361/CE [3] – sono escluse dall'ambito di applicazione della NIS2, ad eccezione dei profili ad alto rischio, quali i fornitori di reti o di servizi di comunicazione elettronica accessibili al pubblico, dei *trust service provider*, i registri dei nomi di dominio di primo livello (TLD), la Pubblica Amministrazione e alcuni altri soggetti, come ad esempio il fornitore unico di un servizio in un dato Paese dell'UE. Sebbene l'accordo tra il Parlamento europeo e il Consiglio mantenga questa regola generale, il testo concordato in via provvisoria include disposizioni aggiuntive per garantire la proporzionalità delle misure in base alla dimensione dell'ente.

Poiché anche le Pubbliche Amministrazioni sono spesso bersaglio di attacchi informatici, NIS2 si applica agli enti della PA a livello centrale; gli Stati membri potranno decidere di estenderla agli enti anche a livello regionale e locale. La direttiva non si applicherà ai soggetti che svolgono attività in settori quali la difesa o la sicurezza nazionale, la pubblica sicurezza, il *law enforcement* e il sistema giudiziario. Anche i Parlamenti e le Banche Centrali sono esclusi dal campo di applicazione.

Giurisdizione e registrazione

Di norma i soggetti essenziali e importanti ricadono sotto la giurisdizione del Paese in cui **forniscono i loro servizi**. Tuttavia alcuni tipi di fornitori digitali (fornitori di servizi DNS, registri dei nomi TLD, fornitori di servizi di *cloud computing*, fornitori di servizi di *data center* e fornitori di reti per la distribuzione di contenuti) sono considerati soggetti alla giurisdizione del Paese in cui hanno la loro sede **principale** nell'Unione, in quanto forniscono servizi transfrontalieri su larga scala. L'ENISA (*European Union Agency for Cybersecurity*) è tenuta a creare e mantenere un registro di quest'ultima categoria di soggetti, garantendo così che essi non debbano ottemperare a una moltitudine di requisiti giuridici diversi.

Rafforzamento della gestione e della cooperazione

NIS2 stabilisce il riferimento per le misure di gestione del *rischio cyber* e gli obblighi di comunicazione in tutti i settori disciplinati, eliminando le divergenze nei requisiti di sicurezza e nell'attuazione delle misure di cybersecurity nei diversi Stati membri. A tal fine, NIS2 definisce i meccanismi per un'efficace collaborazione tra le autorità competenti di ciascuno Stato membro: il **Gruppo di Cooperazione** per sostenere le strategie comuni e lo scambio di informazioni tra i paesi dell'UE, e la **Rete dei CSIRT** (*Computer Security Incident Response Team*) *nazionali* per sviluppare la fiducia tra i Paesi e una cooperazione operativa rapida ed efficace.

NIS2 istituirà formalmente la rete europea delle organizzazioni di collegamento per le crisi informatiche Eu-Cyclone (European Cyber Crises Liaison Organisation Network), per assicurare una gestione coordinata degli incidenti di cybersecurity su larga scala.

Obblighi di notifica

Gli obblighi di notifica di incidenti di sicurezza saranno ampliati, indicando ciò che deve essere segnalato, a quale istituzione ed entro quali tempi.
In continuità con l'attuale NIS, i soggetti devono segnalare alle autorità competenti o al CSIRT nazionale qualsiasi incidente che abbia un impatto significativo sulla fornitura dei loro servizi. Inoltre, secondo NIS2 le entità saranno tenute a segnalare anche qualsiasi minaccia informatica che potrebbe aver potenzialmente provocato un incidente significativo (o *near miss*).

Viene introdotto l'obbligo per i fornitori di notificare ai destinatari dei servizi anche eventuali incidenti che potrebbero influire negativamente sul servizio, incluse le misure o i rimedi che essi possono adottare in risposta a una minaccia identificata dal fornitore.
La notifica deve essere effettuata "senza indebito ritardo". Tuttavia, per la segnalazione alle autorità competenti o al CSIRT, NIS2 introduce un approccio in due fasi: entro 24 ore dalla data in cui sono venute a conoscenza dell'incidente, le entità devono produrre una notifica iniziale, seguita da una relazione finale entro un termine massimo di un mese. Le autorità nazionali competenti o il CSIRT devono rispondere alla notifica iniziale entro ulteriori 24 ore con un feedback sull'incidente e, se possibile, dando indicazioni sulle misure di mitigazione.

Pubblicazione delle vulnerabilità

NIS2 cerca di incoraggiare **pratiche coordinate di vulnerability disclosure**, invitando figure esperte (anche *ethical hacker*) a segnalare le vulnerabilità di prodotti e sistemi in modo da consentire di diagnosticarle e porvi rimedio prima che vengano divulgate e abusate da terzi. A tal fine l'ENISA sarebbe tenuta a sviluppare e mantenere un registro europeo delle vulnerabilità per consentire ai settori essenziali e importanti, nonché ai loro fornitori di reti e sistemi informativi, di registrare e divulgare le vulnerabilità nei prodotti o nei servizi ICT.

Sanzioni

Spicca nella NIS2 la previsione secondo cui gli Stati membri dell'UE sarebbero tenuti a prevedere sanzioni amministrative fino a 10 milioni di euro o al 2 % del fatturato mondiale totale di impresa. I soggetti essenziali che persistono nella non conformità possono anche vedere sospese le autorizzazioni di scopo o esonerate le proprie figure manageriali, fino a quando non siano state adottate le necessarie misure correttive.

La gestione del rischio: un confronto con la norma ISO27001

Il *framework* NIS2 per la prima volta introduce requisiti di *governance* espliciti, che richiedono al management dei soggetti obbligati di approvare e supervisionare le misure di gestione del rischio cyber e di presidiare la formazione sulla sicurezza delle informazioni. Per quanto riguarda la gestione del rischio cyber, la direttiva NIS2 richiede che le misure siano "appropriate" e "proporzionate" in relazione anche alla dimensione dei soggetti; tuttavia, essa aggiunge una serie di elementi minimi di sicurezza che devono essere previsti in ogni caso, e che saranno stabiliti mediante specifiche tecniche e metodologiche emanate dalla Commissione Europea.

Tra gli elementi di novità, NIS2 introdurrà requisiti espliciti per gestire i rischi di terzi nelle catene di approvvigionamento e nelle relazioni con i fornitori (*supply chain security*). Inoltre, NIS2 prevede che i soggetti possano (e alcuni soggetti essenziali debbano) dimostrare la propria conformità ottenendo la certificazione della *cybersecurity* prevista dal recente Regolamento UE 2019/881, noto come EU Cybersecurity Act [4].

Nel 2021 l'EU Cybersecurity Act si è concretizzato con le prime proposte da parte dell'ENISA di schemi di certificazione europea *di prodotto* in ambito cybersecurity. Il primo di essi sarà disponibile a breve, riguarda i prodotti ICT e si chiama EUCC (Common Criteria based European candidate cybersecurity certification scheme): esso si basa sullo schema internazionale dei *Common Criteria* ISO/IEC 15408 [5].

Sono in sviluppo un secondo schema che copre i servizi cloud (EUCS) e un terzo sulle reti 5G (EU5G). Gli schemi di certificazione industriali, come ISO27001, BSI C5 (Germania), SecNumCloud (Francia), CSA Cloud Controls Matrix, NIST 800-53, SOC 2 Trust Services Criteria e PCI DSS, non sono di competenza dell'ENISA ma potranno essere proposti e approvati come schemi formali europei di certificazione della cybersecurity per servizi e per processi.

Su questo tema, diviene opportuno un raffronto con gli obiettivi delle certificazioni internazionali per i sistemi di gestione, *in primis* la norma sui sistemi di gestione della sicurezza delle informazioni ISO/IEC27001:2013 [6] e il codice di pratica per la gestione della sicurezza delle informazioni ISO/IEC27002:2022 [7]. Quest'ultimo, aggiornato di recente e con un focus ancora più esplicito sulla cybersecurity e sulla protezione dei dati personali, propone una serie di controlli operativi, intesi come misure che l'organizzazione attua al fine di mantenere o modificare il rischio sulla sicurezza delle informazioni.

I controlli sono classificati in quattro macrotemi che coincidono con i tradizionali pilastri a cui è associata la sicurezza delle informazioni: controlli organizzativi, fisici, tecnologici e delle persone. L'approccio *risk-based* si conferma requisito sistematico, strutturato e proattivo per la *governance* di un'organizzazione secondo ISO27001. Inoltre, il ciclo di pianificazione, preparazione, valutazione e decisione nel gestire gli incidenti di sicurezza delle informazioni, la prontezza dell'ICT per la continuità aziendale, il monitoraggio delle minacce (*threat intelligence*) e la segnalazione di eventi di sicurezza sono gli aspetti più innovativi previsti dal novellato codice di pratica ISO27002 e valutati in sede di certificazione di un'organizzazione.

Tali norme possono pertanto rappresentare un valido riferimento sul piano tecnico e metodologico per il percorso di adeguamento richiesto ai soggetti essenziali e importanti, ma anche per le eventuali garanzie di *accountability* esigibili dai soggetti coinvolti nelle loro *supply chain*.

Conclusioni

L'accordo provvisorio del 13 maggio 2022 sarà soggetto all'approvazione del Consiglio e del Parlamento europeo. La Direttiva NIS2, una volta approvata, entrerà in vigore venti giorni dopo la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea. Gli Stati membri avranno 21 mesi di tempo dall'entrata in vigore della NIS2 per recepirne le disposizioni nel loro diritto nazionale.

L'aggiornamento della Direttiva NIS ha tratto origine dall'avanzamento della *digital transformation*, dei servizi pervasivi e delle tecnologie abilitanti, quali l'IoT, il 5G e le reti mobili di futura generazione. L'incremento dei crimini informatici, la recente pandemia e il conflitto russo-ucraino, combattuto anche nella dimensione cyber, hanno inoltre esposto le debolezze a livello digitale di imprese e Enti pubblici, rendendo tale aggiornamento improcrastinabile. Al di là del contesto in cui la Direttiva NIS2 sta muovendo i propri passi, l'elemento più significativo è la dichiarata volontà delle Autorità europee di consolidare una norma generale con la quale si armonizzano i principi giuridici e gli aspetti organizzativi degli Stati membri, stimolando un approccio operativo alla gestione del rischio. ©

RIFERIMENTI

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union; http://data.europa.eu/eli/dir/2016/1148/oj

[2] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 - COM/2020/823 final; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

[3] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC); https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF

[4] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act); http://data.europa.eu/eli/reg/2019/881/oj

[5] ISO/IEC 15408-1/2/3:2008; Information technology — Security techniques — Evaluation criteria for IT security; https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[6] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements; https://www.iso.org/isoiec-27001-information-security.html

[7] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls; https://www.iso.org/standard/75652.html ◇