NIS2 - Come e quando

di Antonio Tringali e Alessandro Fontana

Le aziende soggette al Regolamento Network and Information Systems 2 (NIS2, 2022/2555) [1] sono classificate in *essenziali* e *importanti*. Le autorità di controllo possono supervisionare le prime proattivamente, le seconde sono controllate in risposta al contenuto di report su incidenti di cybersicurezza.

La definizione di supervisione è stabilita dagli stati membri dell'Unione Europea. Può consistere in controlli a campione o audit regolari, nonché nella verifica delle politiche di cybersicurezza documentate.

Più in dettaglio, l'art. 32 comma 2 prevede che gli enti di controllo degli Stati membri abbiano il potere di sottoporre i soggetti a:

a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;
b) audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;
c) audit ad hoc, ivi incluso in casi giustificati da un incidente significativo o da una violazione di NIS2 da parte del soggetto essenziale;
d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;
e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cybersicurezza adottate dal soggetto interessato, comprese le politiche di cybersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti a norma dell'articolo 27;
f) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei compiti di vigilanza;
g) richieste di dati che dimostrino l'attuazione di politiche di cybersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Gli Stati membri possono modificare la lista delle aziende essenziali e importanti, per cui se si opera in più di uno Stato dell'Unione bisogna validare la propria classificazione localmente. Gli Stati sono tenuti a definire entro il 17 aprile 2025 un elenco dei soggetti essenziali e importanti, nonché delle aziende che registrano nomi di dominio.

Recepimento in Italia

In Italia per l'applicazione di NIS2 è responsabile l'Agenzia per la Cybersicurezza Nazionale (ACN) [2], come fissato dal decreto di recepimento D.Lgs. 138 del 4 settembre 2024 [3].

All'ACN deve essere notificato un cyberincidente entro 24 ore. Deve poi seguire una notifica più dettagliata entro 72 ore con una valutazione dell'impatto dell'incidente sulle operazioni, sui propri clienti e sugli elementi della catena di fornitura.

La classificazione va fatta conformemente alla *tassonomia cyber* pubblicata da ACN a luglio 2024 [4] e, se disponibili, gli indicatori di compromissione (IoC). Entro 30 giorni deve seguire un report finale dell'incidente che includa sia una sua descrizione sia la risposta adottata.

Un cyberincidente è considerato significativo ai fini di NIS2 quando:

- Abbia causato o sia capace di causare grave distruzione operativa dei servizi o perdita finanziaria per l'azienda considerata.
- Abbia colpito o sia capace di colpire persone fisiche o legali causando danni materiali o non materiali considerevoli.

Il regolamento esecutivo su NIS2 [5] del 17 ottobre 2024 afferma all'art. 3: "il danno è considerato degno di notifica al CSIRT quando ecceda €500000 o il 5% del fatturato nel precedente anno fiscale, quale sia più basso, o siano esfiltrati segreti commerciali". Sono previsti altri casi, ma questi sono i più rilevanti. I requisiti tecnici e metodologici delle misure ricalcano essenzialmente quanto richiesto dalla certificazione ISO/IEC 27001(sicurezza delle informazioni), ma nel caso di un'industria non è possibile ignorare ISO/IEC 62443 (sicurezza operativa).

Ambito di applicazione

Questa è una lista delle classi di aziende interessate da NIS2:

Settori essenziali (Annex I)	**Settori importanti (Annex II)**
Energia	Poste e corrieri
Trasporti	Cibo

Banche	Gestione dei rifiuti
Infrastrutture dei mercati finanziari	Impianti chimici
Salute	Manifattura
Acquedotti	Fornitori digitali
Gestione delle acque reflue	Gestione rifiuti
Infrastruttura digitale	Organizzazioni di ricerca
Pubblica amministrazione	
Fornitori di servizi digitali	
Spazio	

Sono coinvolte dalle medie imprese in su che, secondo la definizione di media impresa data dalla raccomandazione 2003/361/CE [6], sono quelle che occupano più di 250 persone e il cui fatturato annuo superi i 50 milioni di Euro, oppure il cui totale di bilancio annuo superi i 43 milioni di Euro. Vanno valutate con attenzione situazioni in cui il soggetto fa parte di un gruppo, in cui ci sono partecipate e in cui un soggetto non obbligato fornisce servizi IT ad altre aziende del gruppo (si veda in proposito l'art.3 del DL 138, in particolare il comma 10).

Possono essere infine considerate soggetti obbligati anche Organizzazioni che, indipendentemente dal requisito dimensionale, vengono considerate nell'alveo di applicazione della normativa in esame in ragione del loro ruolo strategico o a causa dell'unicità del proprio servizio.

La gestione della cybersicurezza non riguarda solo l'azienda oggetto della NIS2, ma anche i membri della catena di fornitura di cui si avvale, indipendentemente dal fatto che si trovino in Unione Europea o meno. Se anche uno degli elementi della catena di fornitura non è cybersicuro secondo dati parametri di contratto, l'azienda non è considerata aderente ai principi di NIS2.

Obblighi

Le aziende che ricadono sotto NIS2 devono realizzare che, non proteggendo se stesse, possono mettere a rischio la società civile. Aderire a NIS2 migliora anche la resilienza operativa: una migliore postura di cybersicurezza contribuisce alla creazione di una società più resiliente.

La gestione dei rischi prevede che si produca una dettagliata lista delle azioni per migliorare la propria postura. Qualsiasi iniziativa non può prescindere a priori da una *Business Impact Analysis* che valuti l'impatto sui propri clienti dell'indisponibilità in tutto o in parte del sistema informativo aziendale. Questa evidenzia i flussi critici delle informazioni che sono oggetto di particolare protezione. Idealmente è possibile applicare misure preventive per predire ed evitare situazioni di crisi.

In breve, le aziende coinvolte da NIS2 dovrebbero:

- Registrarsi su un portale fornito da ACN entro il 28 febbraio 2025. Se l'azienda è multinazionale deve adeguarsi in ogni Stato secondo la legislazione vigente.
- Creare il team NIS2: un capo progetto – con la collaborazione di esperti in materia – guida l'audit interno e c'è un'unica persona responsabile della revisione documentale.
- Comprendere i punti ciechi dell'infrastruttura dal punto di vista della sicurezza.
- Eliminare la complessità dell'infrastruttura, consolidando gli stack tecnologici disponibili.

L'obiettivo è la scoperta e la classificazione dei potenziali rischi per le interfacce di comunicazione, l'identificazione dei dati strutturati e non strutturati privati e in cloud a rischio, la definizione della postura di cybersicurezza corrente per fornire un percorso verso la piena conformità al regolamento.

Questo è un possibile percorso da seguire:

1. **Lista delle risorse e degli utenti**: elenca le risorse di rete e il perimetro da proteggere, gli utenti e le loro modalità di accesso alle risorse. Fornisce la base per una prima valutazione delle modifiche architetturali da apportare.
2. **Valutazione dei rischi e implementazione di politiche di sicurezza**: si può compiere una *gap analysis*. Uno degli output è una rappresentazione sintetica tra lo stato attuale e lo stato desiderato, con punti di forza e falle di sicurezza da chiudere, cioè un rapporto per il management esecutivo con le linee guida dettagliate per migliorare la postura.
3. **Formazione sulla cybersicurezza per i dipendenti**: tutti i dipendenti devono essere periodicamente formati sui principi di cybersicurezza, secondo la constatazione che il

70% dei cyberincidenti vede coinvolto il personale. In particolare, il personale coinvolto nella gestione dei sistemi deve avere un addestramento specifico in aggiunta a quello per tutti i dipendenti.

4. **Continuità operativa**: redazione del piano di business continuity, che include la gestione dei backup, nonché di piani di disaster recovery e di risposta alle crisi.
5. **Gestione degli incidenti**: azioni e procedure che mirano a prevenire, rilevare, analizzare, contenere, rispondere e recuperare da un incidente di cybersicurezza. Ciò minimizza il danno verificatosi e consente eventualmente di produrre un rapporto, come richiesto dall'autorità nazionale. La dirigenza deve essere coinvolta durante l'incidente.
6. **Sicurezza della catena di fornitura**: non ci sono obblighi diretti a carico dei fornitori, ma deve essere garantita l'aderenza a un contratto che includa dei livelli di servizio accettabili. Per esempio, un provider di servizi di rete dovrà garantire che questi siano adeguati secondo certi parametri concordati con il cliente.
7. **Sicurezza della rete**: gestione delle vulnerabilità e divulgazione. Le cyberminacce devono essere contenute con *next generation firewall*, monitorando dati strutturati e non strutturati. Le attività su questi devono essere tracciate e deve essere documentato ciò che gli utenti fanno sui dati e sui sistemi sensibili. Idealmente un anno di log dovrebbe essere accessibile per la valutazione delle anomalie. Le risorse informatiche e di rete devono essere poste in sicurezza e tipicamente ci si avvale di Intrusion Detection System ed eventualmente di sistemi di Security Information and Event Management e/o Vulnerability Scanner.
8. **Politiche e procedure di cybersicurezza**: per valutare l'efficacia delle misure di gestione dei rischi per la cybersicurezza.
9. **Politiche e procedure sull'uso della crittografia**: i dati a riposo e in movimento dovrebbero essere criptati. L'informazione sensibile nei database dovrebbe essere pseudonimizzata e dovrebbe essere fatta un'accurata gestione delle chiavi crittografiche.
10. **Sicurezza delle risorse umane, politiche di controllo accessi e gestione delle risorse**: ove applicabile, dovrebbe essere utilizzato il single sign-on e la separazione dei ruoli.
11. **Autenticazione multi-fattore e soluzioni di autenticazione continua**: per comunicazioni sicure (anche di emergenza).
12. **Gestione dei cambiamenti**: per lo sviluppo e la manutenzione dei sistemi.

Implicazioni

Le aziende devono preparare piani per la gestione di una crisi e per la continuità operativa, che guidino la dirigenza e i team operativi su come dovrebbero reagire a un incidente. La documentazione deve essere disponibile in formato elettronico e cartaceo a chi di competenza.

Per essere pronti a un audit NIS2 bisognerebbe allocare del tempo per simulare le crisi di cybersicurezza (stress test): in altri termini si dovrebbero condurre *adversarial simulation* contro le cyberdifese dell'azienda replicando le tattiche degli attori malevoli reali. Ciò consente la verifica periodica di configurazioni errate e l'identificazione di vulnerabilità sfruttabili, onde applicare opportune mitigazioni.

Tutti i piani devono dettagliare:

1. La risposta a una crisi.
2. La gestione della crisi.
3. Le procedure di emergenza per il ripristino operativo.
4. La pianificazione della continuità operativa.

Per quanto riguarda l'utilizzo pratico di framework, in Italia la Direttiva NIS fu recepita con il D.lgs. del 18 maggio 2018. Ciò ha portato alla creazione del c.d. Framework Nazionale per la Cybersecurity e la Data Protection, il quale dispone una metodologia tutta italiana per realizzare il c.d. *cybersecurity assessment*.

Nel 2021 un DPCM ha dimostrato come a livello normativo il Framework non sia sufficiente, per cui sono previsti ulteriori controlli e misure per avere livelli di sicurezza più elevati per l'ICT; si attendono ulteriori Determine emanate da ACN. Nel frattempo non è inconsueto vedere l'applicazione per le aziende di framework "più pratici" come il NIST CyberSecurity Framework 2.0.

Sanzioni

La violazione dell'articolo 21 (misure di gestione del rischio di cybersicurezza) o dell'articolo 23 (obblighi di reportistica) di NIS2 impone per le aziende essenziali multe fino a 10 milioni di Euro o il 2% del fatturato mondiale, quale delle due corrisponda alla cifra più alta. La multa si riduce a 7 milioni di Euro o l'1,4% del fatturato mondiale per le aziende importanti.

La dirigenza può essere sospesa dalle proprie funzioni fino alla risoluzione dell'incidente, sottoposta a sanzioni disciplinari (nel caso della PA) e infine perseguita civilmente e al limite penalmente, visto che un rischio sulla cybersicurezza può portare al fermo dell'azienda e dei suoi clienti, ma anche a pregiudizio dell'incolumità delle persone (si pensi solo ad un attacco che metta fuori uso dei sistemi di sicurezza). Se l'azienda è essenziale potrebbe anche essere invocata la sospensione di prodotti o servizi.

Riferimenti

[1] **DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555&from=EN

[2] **NIS - Network Information Security**: https://www.acn.gov.it/portale/nis

[4] **D. Lgs. 138/2024**: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2024-10-01&atto.codiceRedazionale=24G00155&elenco30giorni=false

[3] **LA TASSONOMIA CYBER DELL'ACN**: https://www.acn.gov.it/portale/documents/20119/552690/ACN_Tassonomia_Cyber_CLEAR.pdf/9595cc35-1c0b-4007-07b2-8f0468e5b82e?t=1731598519616

[5] **NIS2: Regolamento di esecuzione della Commissione relativo ai soggetti e alle reti critici**: https://digital-strategy.ec.europa.eu/it/library/nis2-commission-implementing-regulation-critical-entities-and-networks

[6] **Raccomandazione 2003/361/CE**:

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:it:PDF