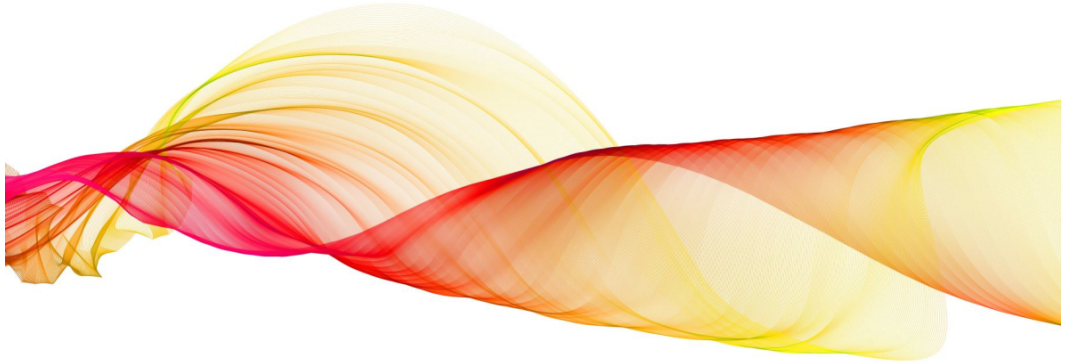
Cybersecurity
Obblighi e opportunità nella disciplina europea



Daniela Redolfi

31 maggio 2024

Cybersicurezza

l’insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche

La disciplina europea in materia di cybersecurity

- Sicurezza delle reti e dei sistemi informativi
- Sistema di certificazione della cybersecurity
- Requisiti di cybersecurity dei prodotti da immettere nel mercato europeo
- Misure intese a rafforzare il rilevamento delle minacce e degli incidenti di cybersicurezza e la capacità di risposta

La legislazione europea in vigore

Regolamento 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Direttiva 2016/1148 *recante misure per un livello comune elevato di sicurezza delle rete e dei sistemi informativi dell'Unione (NIS1)*

Regolamento 2019/881 del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'UE per la cybersicurezza e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione

Direttiva 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (NIS2)

Proposte europee

Com (2022) 454 Regolamento relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica il regolamento UE 2019/1020 (Recillience Act)

Com (2023) 208 Regolamento che modifica il regolamento UE 2019/881 per quanto riguarda i servizi di sicurezza gestiti

Com (2023) 209 Regolamento che stabilisce le misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cybersicurezza e di preparazione e risposta agli stessi (Solidarity Act)

Dalla NIS1 alla NIS2

- Si amplia l'ambito di applicabilità (servizi essenziali e importanti)
- Si elimina la differenziazione – ormai obsoleta – fra operatori di servizi essenziali e fornitori di servizi digitali
- Si riduce la discrezionalità degli Stati membri (nella NIS1 erano i singoli Stati a definire i servizi essenziali)
- Si migliora il coordinamento in termini di misure di sicurezza previste e di risorse disponibili all'autorità di controllo.
- Si rinnova la disciplina relativa agli obblighi di segnalazione degli incidenti
- Si istituisce presso ENISA il registro dei soggetti (fornitori di servizi DNS, soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, …..)

Direttiva NIS2 Soggetti essenziali e importanti

Settori ad alta criticità

Energia (energia elettrica, teleriscaldamento, teleraffrescamento, petrolio, gas, idrogeno); Trasporti (aereo, ferroviario, per vie d'acqua, su strada); Settore bancario; Infrastrutture dei mercati finanziari; Settore sanitario; Acqua potabile; Acque reflue; Infrastrutture digitali (fornitori DNS, registri nomi a dominio, cloud computing, data center, reti pubbliche di comunicazione …) ; Gestione dei servizi TIC (business to business); Pubblica Amministrazione (amministrazione centrale e regionale); Spazio

Altri settori critici

Servizi postali e di corriere; Gestione dei rifiuti; Fabbricazione, produzione e distribuzione di sostanze chimiche; Produzione, trasformazione e distribuzione di alimenti; Fabbricazione (dispositivi medici, computer, macchinari, apparecchiature, auto, altri mezzi di trasporto); Fornitori di servizi digitali (mercati online, motori di ricerca, social network); Ricerca.

Misure di sicurezza

- analisi dei rischi
- gestione degli incidenti e loro segnalazione
- continuità operativa
- **sicurezza della catena di approvvigionamento**
- sicurezza acquisizione e manutenzione
- valutazione efficacia gestione rischi
- formazione
- crittografia
- sicurezza risorse umane
- autenticazione a due fattori o continua

Cosa si attende

entro il 17 ottobre 2024

- Recepimento della direttiva da parte dei singoli Stati
  - Con legge 15/24 il Parlamento ha delegato il governo a recepire la direttiva
- **Atti di esecuzione della Commissione che stabiliscono i requisiti tecnici e metodologici delle misure** per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, nonché i prestatori di servizi fiduciari.
  - Orientamenti in materia di obblighi di segnalazione degli incidenti
  - Orientamenti in materia di informazioni da raccogliere negli elenchi dei soggetti essenziali e importanti

La disciplina in materia di certificazione della cybersecurity

Il Regolamento 2019/881 stabilisce un quadro per l'introduzione di sistemi europei di **certificazione della cybersicurezza** al fine di garantire un livello adeguato di cybersicurezza **dei prodotti TIC, servizi TIC e processi TIC** nell'Unione.

Oggetti di certificazione

Prodotto TIC un elemento o un gruppo di elementi di una rete o di un sistema informativo;

Servizio TIC un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;

Processo TIC un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC

Servizi di sicurezza gestiti *un servizio consistente nello svolgimento di attività legate alla gestione dei rischi in materia di cybersicurezza, tra cui servizi di risposta agli incidenti, test di penetrazione, audit di sicurezza e consulenza, o nella fornitura di assistenza per tali attività*

Obiettivi

proteggere i dati dall'accesso, divulgazione, distruzione, perdita, alterazione

consentire l'accesso ai dati solo a chi ne abbia i diritti

individuare dipendenze e vulnerabilità

registrare i log

verificare i log

verificare che prodotti, servizi e processi TIC non contengano vulnerabilità note

ripristinare la disponibilità in caso di incidente

garantire la sicurezza fin dalla progettazione

effettuare gli aggiornamenti disponendo di meccanismi di aggiornamento protetti

Recillience Act

Requisiti essenziali di cybersicurezza per l'immissione sul mercato dell'Unione di prodotti con elementi digitali

prodotto con elementi digitali: qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware da immettere sul mercato separatamente

Il prodotto con elementi digitali è messo a disposizione sul mercato soltanto se:

- soddisfa i requisiti essenziali;
- i processi messi in atto dal fabbricante sono conformi ai requisiti essenziali

Requisiti

- Requisiti essenziali di sicurezza
- Requisiti di gestione delle vulnerabilità

- Informazioni e istruzioni per l'utilizzatore
- Documentazione tecnica

- Procedure di valutazione della conformità
- Dichiarazione di conformità UE

I prodotti con **elementi digitali critici** sono soggetti a procedure di valutazione più stringenti

Solidarity Act

- **Cyberscudo europeo**, costituito dai centri operativi nazionali e transfrontalieri, con lo scopo di sviluppare capacità avanzate che permettano all'Unione di rilevare, analizzare ed elaborare i dati sulle minacce e sugli incidenti informatici nell'UE, nonché gli obiettivi operativi specifici
- **Meccanismo per le emergenze di cybersicurezza** al fine di migliorare la resilienza dell'Unione alle minacce gravi alla cybersicurezza
- **Meccanismo di riesame degli incidenti di cyber sicurezza**