NIS2

NETWORK INFORMATION SECURITY

Arriva la **NIS 2**, la nuova direttiva dell'Unione Europea in materia di cybersecurity.

Non facciamoci trovare impreparati!

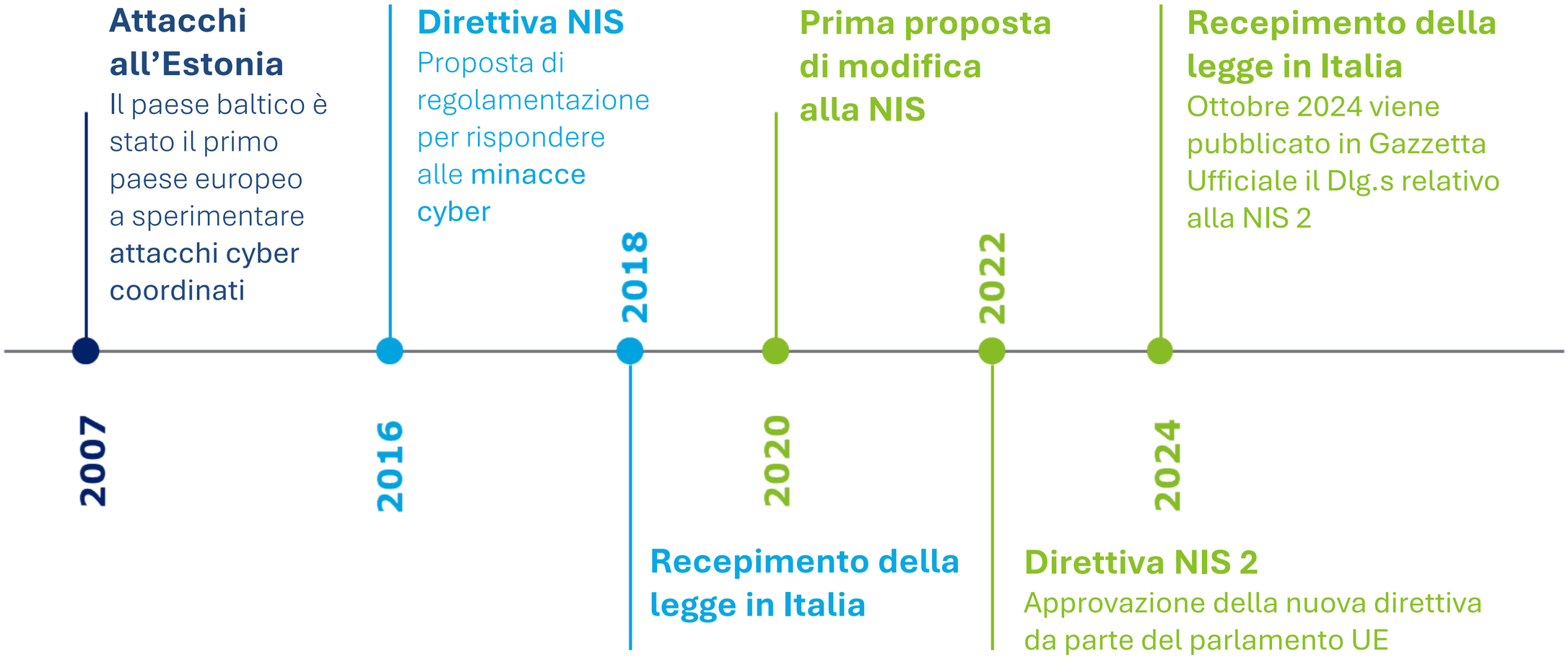
NETWORK INFORMATION SECURITY

NIS2

COMPLIANT

OTS

Genesi della NIS 2



Network Information Security

- Regolamento UE 2022/2555
- Adottata in Italia da ottobre 2024
- Oltre 15.000 aziende in perimetro
- Gestione dei servizi TIC, Pubblica Amministrazione, Spazio, Acque Reflue, Energia, Settore Sanitario, Sostanze chimiche, Alimenti, Servizi Postali e di corriere
- Si applica solo alle medie e grandi imprese (fatturato superiore a 10 Mln€ e/o più di 50 dipendenti)

Nuovi settori a perimetro

SOGGETTI ESSENZIALI & SOGGETTI IMPORTANTI

1. Gestione dei Servizi TIC
2. Pubblica Amministrazione
3. Spazio
4. Acque Reflue
5. Energia*
6. Settore Sanitario**
7. Sostanze Chimiche(fabbricazione, produzione e distribuzione)
8. Fabbricazione***
9. Alimenti (produzione trasformazione e distribuzione)
10. Servizi Postali e di Corriere
11. Gestione dei Rifiuti
12. Ricerca
13. Fornitori di servizi digitali****

** Teleriscaldamento e teleraffrescamento, idrogeno. Nuovi ambiti nel settore elettrico: mercati elettrici, produzione, aggregazione, domanda, offerta e stoccaggio di energia, gestori punti di ricarica.*

*** Laboratori di riferimento dell'UE, ricerca e sviluppo e fabbricazione di medicinali e dispositivi medici considerati critici durante un'emergenza.*

**** Dispositivi medici e medico-diagnostici in vitro, computer, prodotti di elettronica e ottica, apparecchiature elettriche, macchinari e apparecchiature n.c.a., autoveicoli, rimorchi e semirimorchi, altri mezzi di trasporto.*

***** Piattaforme di servizi di social network.*

Nuovi obblighi

La direttiva introduce nuovi obblighi per i soggetti inclusi nel perimetro, al fine di garantire un adeguato livello di misure di cyber security delle infrastrutture critiche.

- **RISK OWNERSHIP**
- **ENFORCEMENT**
- **GESTIONE DEL RISCHIO**
- **SUPPLY CHAIN SECURITY**
- **SEGNALAZIONE DEGLI INCIDENTI**

Nuovi obblighi

RISK OWNERSHIP

- Gli organi di gestione devono avere un ruolo attivo nella gestione dei rischi, in particolare nella definizione della strategia di gestione del rischio Cyber utile ad evolvere e migliorare la sicurezza e resilienza informatica dei soggetti.

- Gli organi di gestione dei soggetti che rientrano nell'ambito di applicazione della direttiva devono approvare le misure di gestione dei rischi di Cyber Security e supervisionarne l'attuazione.

Nuovi obblighi

ENFORCEMENT

- La Direttiva prevede un regime di vigilanza completo (ex-ante ed ex- post) e sanzioni fino a 10 mln di euro o pari al 2% del fatturato annuo globale per i soggetti essenziali; mentre per i soggetti importanti, è previsto un regime di vigilanza leggero (ex post) e sanzioni fino a 7 mln di euro o pari all'1,4% del fatturato annuo globale.

- Gli Stati membri provvedono affinché le autorità competenti dispongano di risorse adeguate per svolgere, in modo efficace ed efficiente, i compiti loro assegnati.

Nuovi obblighi

GESTIONE DEL RISCHIO

- La Direttiva identifica un elenco di misure tecniche, operative e organizzative di gestione del rischio Cyber che tutti i soggetti essenziali e importanti sono tenuti ad attuare.

- Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici.

Nuovi obblighi

SUPPLY CHAIN SECURITY

- I soggetti identificati devono garantire la Cyber Security lungo la Supply Chain. A tal fine, devono valutare il livello di maturità Cyber dei propri fornitori, prendendo in considerazione i presidi e le procedure definite dagli stessi per la gestione dei rischi di Cyber Security.

- I soggetti dovrebbero valutare e tenere conto della qualità complessiva dei prodotti e delle pratiche di Cyber Security dei propri fornitori e prestatori di servizi, comprese le loro procedure di sviluppo sicuro.

Nuovi obblighi

SEGNALAZIONE DEGLI INCIDENTI

- I soggetti interessati dovranno presentare notifica dell'incidente entro 72 ore dalla conoscenza di tale incidente alle autorità competenti o ai CSIRT. Le notifiche devono includere tutte le informazioni necessarie per valutare l'impatto potenziale dell'incidente.

- Gli Stati membri dovrebbero garantire che l'obbligo di presentare una notifica dell'incidente non sottragga le risorse del soggetto notificante dalle attività relative alla gestione degli incidenti, in quanto considerate prioritarie.

Gestione del rischio cyber

Policy di analisi dei rischi e di sicurezza dei sistemi Informatici

Gestione degli incidenti

Continuità operativa e gestione delle crisi

Sicurezza della catena di approvvigionamento (Supply Chain)

Pratiche di «Cyber Hygiene» di base e formazione in materia di Cyber Security
(i.e., principio Zero-Trust, aggiornamenti Software, configurazione dei Device, segmentazione della rete, organizzazione di sessioni di formazione per il personale, incremento della consapevolezza su minacce Cyber e tecniche di Social Engineering)

Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di Cyber Security

Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete

Policy e procedure relative all'uso della crittografia e della cifratura

Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione delle utenze attive

Utilizzo di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti

Supply Chain Security

OBBLIGHI

- Implementare controlli sulla Supply Chain Security
- Valutare e tenere conto della qualità complessiva delle procedure di sviluppo applicativo, maintenance e supporto da parte dei fornitori
- Esercitare maggiore controllo nella selezione degli MSSP (Managed Security Service Providers)

Segnalazione degli incidenti

OBBLIGO DI SEGNALAZIONE INCIDENTI NIS 2

Un incidente è considerate significativo se:

- Ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato
- Si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli

Entro 24 ore da quando il soggetto è venuto a conoscenza dell'incidente:

- Preallarme che indichi se c'è il sospetto che l'incidente sia il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero
- L'autorità o il CSIRT fornisce un riscontro

Entro 72 ore da quando il soggetto è venuto a conoscenza dell'incidente:

- Notifica dell'incidente che aggiorni le informazioni già comunicate in fase di preallarme e fornisca una valutazione iniziale dell'incidente (gravità, impatto, indicatori di compromissione, etc.)

Su richiesta dell'autorità / CSIRT

- Report intermedio con gli aggiornamenti sulla situazione

Entro un mese dalla notifica iniziale:

- Report finale che contenga i seguenti aspetti:
  Analisi dell'incidente - Tipo di minaccia o causa dell'incidente - Misure di mitigazione adottate - Eventuale impatto transfrontaliero

Sanzioni

SOGGETTI ESSENZIALI

Regime di supervisione complete (ex-ante ed ex-post)

(a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali
(b) audit sulla sicurezza periodici e mirati
(c) audit ad hoc
(d) scansioni di sicurezza
(e) richieste di informazioni per valutare le misure di gestione dei rischi cyber adottate
(f) richieste di accesso a informazioni rilevanti
(g) richieste di dati che dimostrino l'attuazione di policy di Cyber Security

Le autorità competenti possono imporre sanzioni fino a 10 milioni di euro o al 2% del fatturato annuo globale dell'organizzazione

SOGGETTI IMPORTANTI

Regime di supervisione leggero (ex-post)

Le autorità competenti, se ricevono elementi di prova, indicazioni o informazioni secondo cui un soggetto importante non rispetta presumibilmente la Direttiva, intervengono mediante misure di vigilanza ex post, prevedendo:

(a) ispezioni in loco e vigilanza ex post a distanza
(b) audit sulla sicurezza mirati
(c) scansionidi sicurezza
(d) richiestedi informazioni per valutare ex-post le misure di gestione dei rischi cyber adottate
(e) richieste di accesso a informazioni rilevanti
(f) richieste di dati che dimostrino l'attuazione di policy di Cyber Security

Le autorità competenti possono imporre sanzioni fino a 7 milioni di euro all'1,4% del fatturato annuo globale dell'organizzazione

Timeline adempimenti Direttiva NIS 2 in Italia

Grazie per l’attenzione!

OTS S.p.A. opera da oltre 25 anni nel mercato italiano, in cui si è velocemente affermata come realtà strutturata e competitiva, proponendosi come fornitore dinamico e flessibile, in grado di offrire un’ampia e articolata gamma di Servizi e Soluzioni ICT.

OTS SpA
20089 Rozzano Milanofiori (MI)
Strada 4, Palazzo Q5, Piano 2
Telefono: +39 02 361611