Associazione Italiana Strumentisti

ISA Italy Section

«LE DIMENSIONI DELLA SICUREZZA INDUSTRIALE»
I percorsi della sicurezza industriale dagli standard ISA/IEC 62443 ai temi della cybersecurity

**Milano, 30 Maggio 2018**

**Auditorio TECNIMONT**

# Le novità introdotte dalla Direttiva NIS per gli operatori di servizi essenziali e digitali

ReD OPEN
BICOCCA RESEARCH GROUP

1998-2018
20 UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA
VENTESIMO ANNIVERSARIO

**Avv. Andrea Palumbo,** Ph.D.
palumbo@htlaw.it

# La normativa di riferimento

Direttiva UE n. 1148/2016

# La Direttiva NIS

Obiettivi della Direttiva

- sostenere e agevolare la cooperazione strategica fra gli Stati membri in relazione alla sicurezza delle reti e dei sistemi informativi
- Imporre l'adozione di una strategia per garantire un livello elevato di sicurezza delle reti e dei sistemi informativi sul territorio degli stati membri
- prevedere obblighi in materia di sicurezza per promuovere una cultura della gestione dei rischi e garantire la segnalazione degli incidenti più gravi

# La Direttiva NIS

Coinvolge con le sue prescrizioni l'attività di:

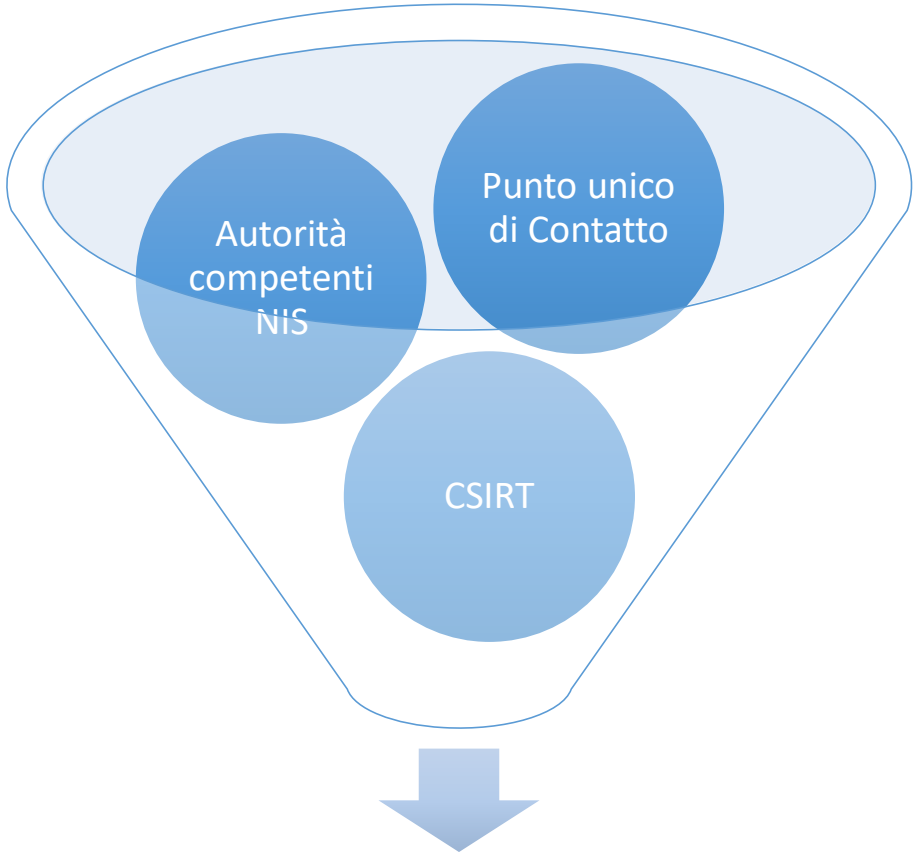
- Attori istituzionali
- Operatori di servizi essenziali
- Fornitori di servizi digitali

# La Direttiva NIS

| | |
|---|---|
| **Attori istituzionali** | **Autorità nazionali competenti NIS** |
| | **Punto di contatto unico (Dipartimento delle informazioni per la sicurezza – DIS)** |
| | **Presidenza del Consiglio dei Ministri** |
| | **Gruppo di intervento perla sicurezza informativa in caso di incidente – CSIRT)** |

# La Direttiva NIS

Attori istituzionali




Cooperazione a livello nazionale

# La Direttiva NIS

Attori Europei

# La Direttiva NIS

Operatori di servizi essenziali – in quali settori operano?

Soggetti pubblici o privati

| **Settore** |
| --- |
| Energia: energia elettrica; petrolio; gas. |
| Trasporti: aereo; ferroviario; per vie d’acqua; su strada. |
| Settore bancario. |
| Infrastrutture dei mercati finanziari. |
| Settore sanitario: istituti sanitari (ospedali e cliniche private). |
| Infrastrutture digitali: IXP; DNS; TLD. |

# La Direttiva NIS

Operatori di servizi essenziali – quali caratteristiche devono avere?

Soggetti pubblici o privati

| **Caratteri:** |
| --- |
| fornisce un servizio essenziale per il mantenimento delle attività economiche essenziali o sociali; |
| la fornitura del suo servizio dipende dalla rete e dai sistemi informativi |
| un incidente informatico avrebbe effetti rilevanti sulla fornitura di tale servizio |

# La Direttiva NIS

## Operatori di servizi essenziali - da chi sono individuati?

| Settore | Autorità nazionali competenti NIS |
|---|---|
| Energia | Ministero dello Sviluppo Economico |
| Infrastrutture digitali | Ministero dello Sviluppo Economico |
| Trasporti | Ministero delle Infrastrutture e Trasporti |
| Bancario | Ministero dell'economia delle finanze |
| Infrastrutture dei mercati finanziari. | Ministero dell'economia delle finanze |
| Settore sanitario: istituti sanitari (ospedali e cliniche private) | Ministero della salute |
| Fornitura e distribuzione di acqua potabile | Ministero dell'ambiente |

Entro il 9 novembre 2018 con verifica biennale

# La Direttiva NIS

Operatori di servizi essenziali – Quali obblighi?

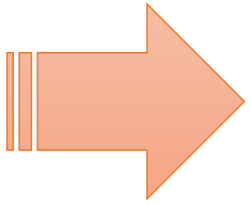
Obblighi in materia di sicurezza

Obblighi di notifica di incidenti

# La Direttiva NIS

## Un nuovo paradigma

Right based approach (approccio basato sulla norma)



Risk based approach (approccio basato sul rischio)

# La Direttiva NIS

**Misure di sicurezza adeguate per:**

- prevenire l'impatto di incidenti sulla rete
- minimizzare l'impatto di incidenti sulla rete
- assicurare la continuità dei servizi

**Notifica di incidenti:**

- al CSIRT e all'autorità competente NIS
- aventi un notevole impatto (sulla base del numero di utenti interessati; dell'ambito geografico dell'incidente; della sua durata)
- senza ingiustificato ritardo

# La Direttiva NIS

## Attività di controllo

All'Autorità competente NIS vengono fornite

Le informazioni necessarie per valutare la sicurezza della reta (comprese le policy di sicurezza)

La prova dell'effettiva adozione di policy di sicurezza attraverso lo svolgimento di audit

1. da parte dell'Autorità competente NIS
2. da parte di revisori abilitati

# La Direttiva NIS

Fornitori di servizi digitali – chi sono?

Soggetti pubblici o privati

| Tipo |
| --- |
| Mercati on line: ossia un servizio digitale che consente a consumatori e professionisti che consenta di concludere contratti di servizi o vendita on line con altri professionisti sia sul web sia sul sito del professionista |
| Motori di ricerca on line |
| Fornitori di servizi cloud |

# La Direttiva NIS

Fornitori di servizi digitali - da chi sono individuati?

Ministero dello Sviluppo Economico

Entro il 9 novembre 2018 con verifica biennale

# La Direttiva NIS

**Misure di sicurezza adeguate alla gestione dei rischi:**

- della rete che utilizzano
- dei sistemi informativi che utilizzano

**Misure di sicurezza adeguate per:**

- prevenire l'impatto di incidenti sulla rete
- minimizzare l'impatto di incidenti sulla rete
- assicurare la continuità dei servizi

**Notifica di incidenti:**

- al CSIRT e all'autorità competente NIS
- aventi un impatto rilevante (sulla base dell'ambito geografico dell'incidente; della sua durata; della portata della perturbazione del funzionamento del servizio; dell'impatto sulle attività economiche e sociali)
- senza ingiustificato ritardo

# La Direttiva NIS

La notifica non è dovuta quando il fornitore di servizi digitali non abbia accesso ai dati precedentemente indicati

# La Direttiva NIS

## Attività di controllo

All'Autorità competente NIS vengono fornite

le informazioni necessarie per valutare la sicurezza della rete e dei loro sistemi informativi (comprese le policy di sicurezza)