# La Cybersecurity nell'era dell'Intelligenza Artificiale: La Direttiva NIS 2

## Una nuova frontiera per la protezione europea

Prof. Fedeli Massimo

IIS Fermi Sacconi Cpia

7 gennaio 2026

# Agenda

# Il Panorama delle Minacce Informatiche

- Crescita esponenziale degli attacchi
- Aumento di complessità e impatto
- Target: aziende, PA, infrastrutture critiche
- Nuove tecnologie = nuove vulnerabilità

# Ransomware

## Definizione

[-¿, thick, red] (0,2) – (1,3); [-¿, thick, red] (0.5,1.5) – (1.5,2.5); [-¿, thick, red] (1,1) – (2,2); Malware che cifra i dati richiedendo un riscatto per la decrittazione

**Caratteristiche:**

- Richiesta in criptovaluta
- Blocco totale dei dati
- Tempi di recupero lunghi

**Caso Irlanda 2021:**

- Sistema sanitario nazionale
- Ospedali bloccati per giorni
- Interruzione servizi essenziali

# Phishing

## Tecnica di ingegneria sociale

Email fraudolente che imitano comunicazioni ufficiali

**Obiettivi:**

- Credenziali di accesso
- Dati bancari
- Informazioni sensibili

**Esempio:** Email apparentemente dall'IT interno richiede aggiornamento password urgente

# DDoS - Distributed Denial of Service

## Obiettivo

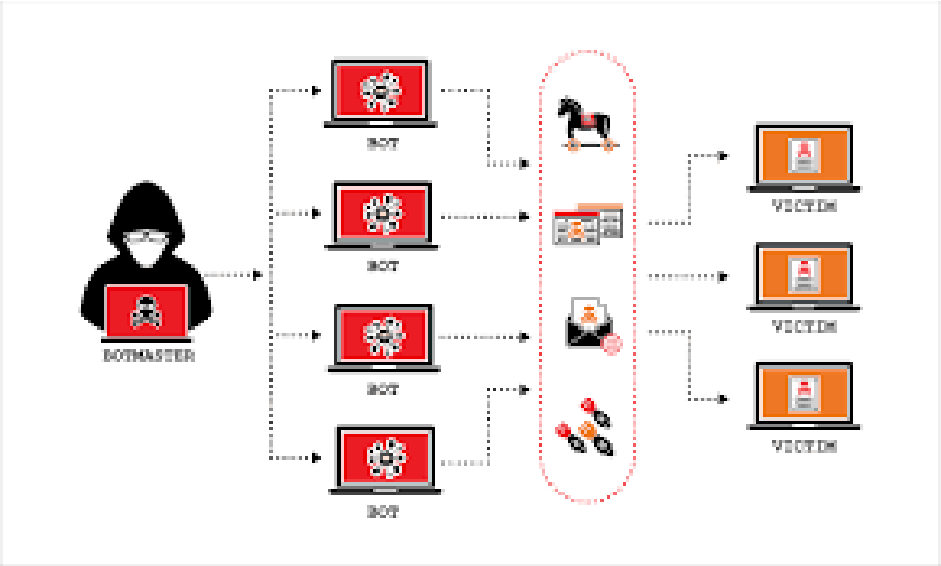
Sovraccaricare un servizio online con richieste massive

**Metodo:**

- Botnet di migliaia di dispositivi
- Richieste simultanee
- Blocco del servizio

**Conseguenze:**

- Inaccessibilità ore/giorni
- Perdite economiche
- Danno reputazionale



# Supply Chain Attack

## Strategia

Attacco al fornitore per propagarsi all'organizzazione principale

**Caso SolarWinds 2020:**

- Software di gestione IT compromesso
- Migliaia di clienti infettati
- Agenzie governative coinvolte

# Il Ruolo dell'IA nelle Minacce

**Automazione degli attacchi:**

- Phishing personalizzato
- Imitazione stili di scrittura
- Analisi vulnerabilità real-time

**Botnet intelligenti:**

- Adattamento dinamico
- Elusione rilevamento
- Selezione bersagli redditizi

# Perché NIS 2?

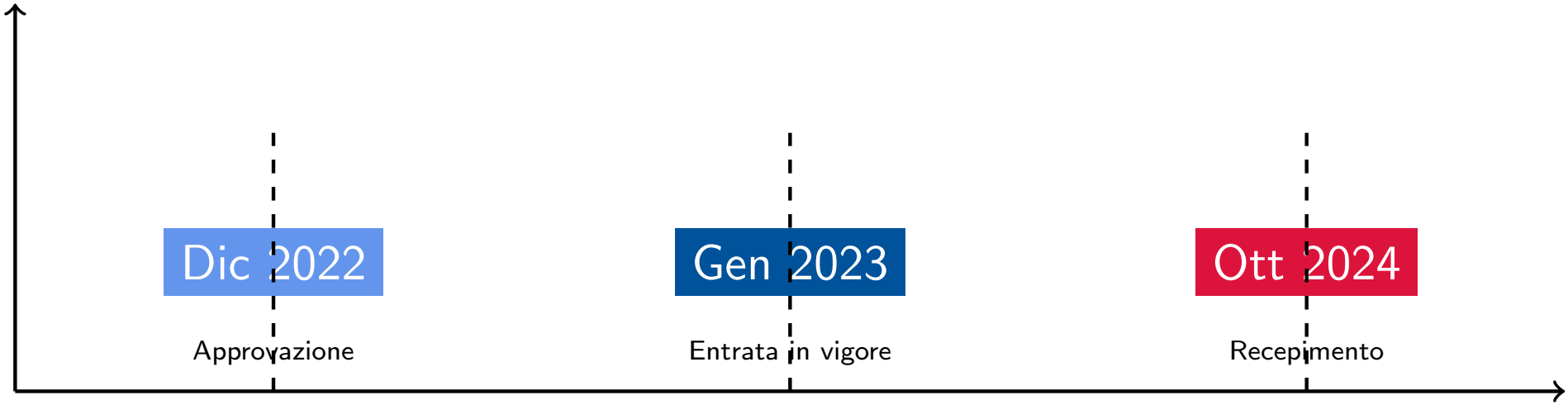
## Problematiche NIS 1 (2016)

- Applicazione disomogenea
- Ambito troppo ristretto
- Requisiti generici
- Monitoraggio inefficace

**Fattori acceleranti:**

- Pandemia e smart working
- Guerra in Ucraina
- Aumento supply chain attacks

# Timeline NIS 2




**Obiettivo:** Rafforzare resilienza sistemi informatici europei

# Principali Novità di NIS 2

1. **Ampliamento settori:**
   - PA centrale e locale
   - Acque reflue e rifiuti
   - Spazio e satelliti
   - Poste e corriere
   - Produzione critica (microchip, farmaci)
2. **Obblighi di sicurezza specifici**
3. **Notifica tempestiva incidenti**
4. **Responsabilità dirigenziale**
5. **Sanzioni severe**

# Obblighi di Sicurezza Informatica

## Misure obbligatorie

- Analisi rischi e vulnerabilità
- Gestione e risposta incidenti
- Continuità operativa e piani di ripristino
- Sicurezza supply chain
- Crittografia e controllo accessi
- Formazione del personale

# Notifica degli Incidenti

## Tempistiche obbligatorie

| | |
|---|---|
| 24h | Prima segnalazione |
| 72h | Relazione tecnica dettagliata |
| 30 giorni | Relazione finale |

**Esempio:** Ospedale colpito da malware $\rightarrow$ informare immediatamente ACN

# Responsabilità e Sanzioni

**Responsabilità dirigenziale:**

- Approvazione misure sicurezza
- Formazione specifica
- Responsabilità per negligenza

**Sanzioni:**

- 10M€ o 2% fatturato (essenziali)
- 7M€ o 1.4% fatturato (altri)

# L'Agenzia per la Cybersicurezza Nazionale (ACN)

## Istituita nel 2021

Ente pubblico per la protezione e rafforzamento sicurezza cibernetica italiana

**Principali compiti:**

- Strategia nazionale cybersicurezza
- Coordinamento risposta incidenti
- Supporto tecnico-operativo
- Gestione notifiche NIS 2
- Promozione cultura cybersecurity
- Vigilanza e sanzioni

# Recepimento in Italia

## Decreto Legislativo 138/2024

4 settembre 2024 - Entrato in vigore 16 ottobre 2024

**Adempimenti principali:**

- Registrazione piattaforma ACN
- Fornitura informazioni organizzazione
- Comunicazione servizi offerti
- Adempimento entro 28 febbraio 2025

# Obblighi per le Imprese

**Ambito applicazione:**

- Settori ad alta criticità
- Aziende 50+ dipendenti
- Fatturato ¿ 10M€
- Servizi essenziali

# Adempimenti Obbligatori per le Imprese

1. Registrazione ACN entro 28/02/2025
2. Misure gestione rischio
3. Notifica incidenti entro 72h
4. Designazione responsabile cybersecurity
5. Formazione continua personale
6. Gestione supply chain
7. Supervisione organi direttivi

# Benefici Concreti per i Cittadini

**Vantaggi:**

- Maggiore continuità servizi
- Protezione dati personali
- Fiducia servizi digitali
- Prevenzione truffe
- Risposte rapide incidenti

# Esempi di Benefici per i Cittadini

## Servizi Sanitari

Riduzione rischi interruzione appuntamenti e cure urgenti per attacchi ransomware

## Servizi Bancari

Maggiore sicurezza home banking e protezione dati finanziari

## PA Digitale

Fiducia nell'utilizzo servizi online (fascicolo sanitario, portale PA)

# Conclusioni

## NIS 2: Un passo fondamentale

Verso un'Europa più sicura digitalmente

**Imperativo per le organizzazioni:**

- Prepararsi a nuove responsabilità
- Adottare misure sicurezza adeguate
- Contribuire ecosistema digitale resiliente

**Obiettivo finale:** Cybersicurezza condivisa tra pubblico e privato

# Riferimenti Bibliografici


- Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio
- https://digital-strategy.ec.europa.eu/it/policies/nis2-directive
- https://direttivanis2.eu
- https://www.akamai.com/it/glossary/what-is-nis2
- Decreto Legislativo 4 settembre 2024, n. 138
- https://www.confindustriaemilia.it/flex/files/1/1/2/D.90e6cec33a853f3a4ea7/sicurezza_informatica.pdf


# Grazie per l'attenzione!