UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Direttiva Nis2 : Il ruolo del System Integrator

Umberto Aquilini

Account Manager

Elettrica srl

u.aquilini@elettricasrl.com

Venerdì 12 Aprile 2024

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Nis 2 in pillole

La direttiva sulla sicurezza delle reti e dei sistemi informativi, Network and Information Security Directive 2 (NIS2) dell'Unione europea delinea i requisiti di cybersicurezza per le organizzazioni operanti nell'Unione Europea (UE) al fine di garantire un livello elevato e comune di protezione tra gli Stati membri.

La direttiva affronta le limitazioni della precedente direttiva NIS inizialmente istituita nel 2016 con requisiti più rigorosi, un'estensione dell'ambito di applicazione delle entità e dei settori che devono conformarsi e maggiori sanzioni per l'inosservanza.

A chi si rivolge la Nis 2?

A seconda delle loro dimensioni e del settore in cui operano, le organizzazioni rientrano nelle categorie "**Essenziali**" o "**Importanti**". Entrambe devono rispettare le stesse misure di sicurezza, ma le Entità Essenziali sono monitorate proattivamente e sono soggette a sanzioni più gravi in caso di inosservanza. Poiché NIS2 è una direttiva europea, spetta a ciascuno Stato membro dell'UE recepirla nella propria legislazione nazionale e farla rispettare. I requisiti chiave sono gli stessi, ma le leggi locali definiscono procedure e linee guida di attuazione specifiche, puntando agli stessi obiettivi in tutta l'UE: garantire che le organizzazioni che fanno parte della catena di fornitura delle infrastrutture critiche comprendano la loro esposizione ai rischi informatici, applichino le best practice di cybersicurezza e siano in grado di rilevare, gestire e segnalare gli incidenti in tempi molto brevi.

Essential Business Sectors

Energy

- Electricity
- Gas
- Oil
- Hydrogen
- District Heating & Cooling

Transport

- Air
- Rail
- Water
- Road

Health

- Healthcare Providers
- Pharmaceutical Industry

Space

- **Drinking Water**
- **Waste Water**
- **Public Administration**
- **Digital Infrastructure**
- **Banking**
- **Financial Market Infrastructures**
- **ICT Service Mgmt (B-to-B)**

Important Business Sectors

Postal & Courier Services

Waste Management

Digital Providers

- Online Marketplaces
- Online Search Engines
- Social Networking Service Platforms

Chemicals

- Manufacture, Production & Distribution

Food

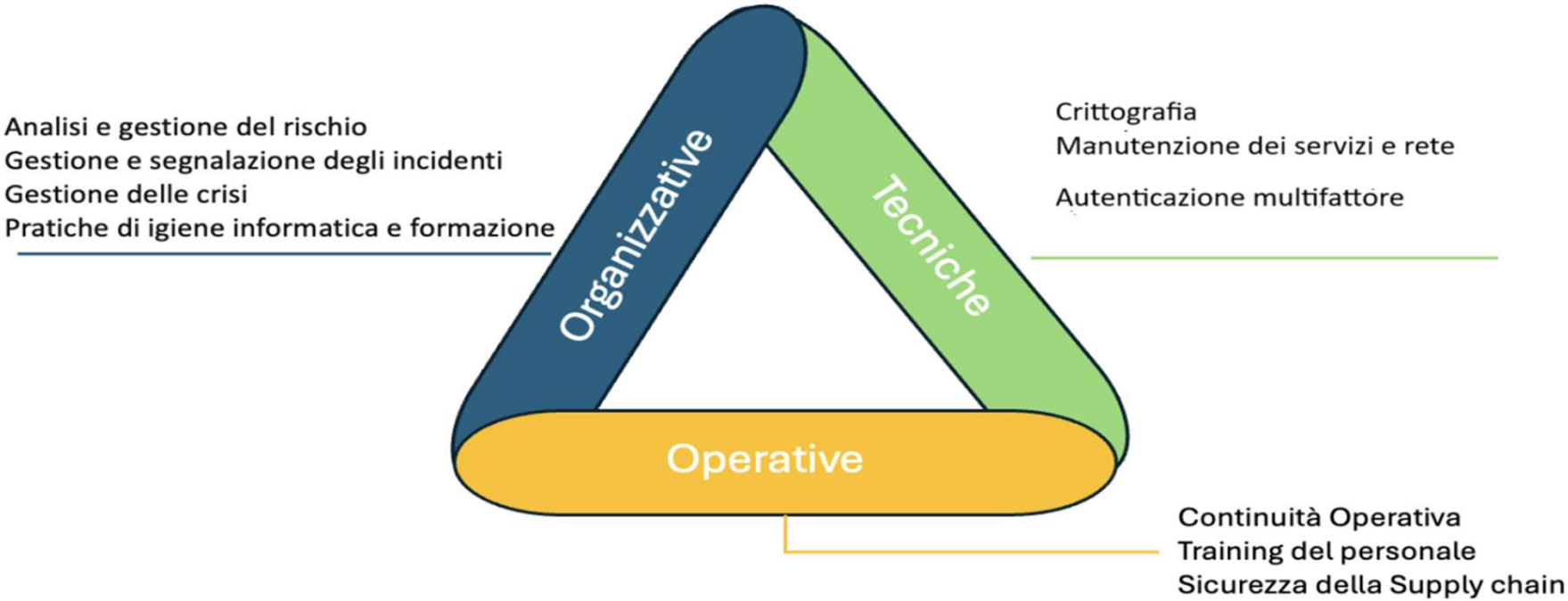
- Production, Processing & Distribution

Research

Manufacturing

- Manufacture of Medical Devices & *In Vitro* Diagnostic Medical Devices
- Manufacture of Computer, Electronic & Optical Products
- Manufacture of Electrical Equipment
- Manufacture of Machinery & Equipment n.e.c.
- Manufacture of Motor Vehicles, Trailers & Semi-Trailers
- Manufacture of Other Transport Equipment

Misure di Sicurezza



Obblighi di notifica

Sebbene la direttiva NIS abbia sempre richiesto alle organizzazioni di segnalare gli incidenti di sicurezza informatica, NIS2 rende obbligatoria la segnalazione degli incidenti "significativi" e descrive un processo chiaro e rigoroso per farlo. Per mantenere la conformità, le entità devono notificare gli incidenti al Computer Security Incident Response Team (*CSIRT*) o qualsiasi altra autorità competente del proprio paese secondo la seguente tempistica una volta verificatosi un incidente.

24 Ore	72 Ore	1 Mese	Su richiesta delle autorità
 Obbligati a segnalare qualsiasi incidente significativo entro 24 ore dal momento in cui ne sono venuti a conoscenza, indipendentemente dal fatto che abbia avuto un impatto diretto sulle operazioni.	 Rapporto aggiornato entro 72 ore dal momento in cui si viene a conoscenza dell'incidente, descrivendo la natura dell'incidente, la sua gravità, gli impatti e gli indicatori di compromissione.	 Una descrizione dettagliata dell'incidente deve essere presentata entro 1 mese, spiegando le possibili cause, le misure di mitigazione in corso e l'impatto transfrontaliero.	 Su richiesta delle autorità di regolamentazione potranno essere richiesti aggiornamenti di natura rilevante.

Il System Integrator: Ruolo, azioni e responsabilita’

Chi e’ il System integrator

Il System integrator e’ una figura professionale o aziendale che progetta, realizza e gestisce operazione Ict complesse integrando componenti hardware, software e servizi.

Coordinando fornitori e tecnologie diverse supporta l’adozione di standard di sicurezza e compliance.

Azioni chiave del System Integrator nella Nis 2

ANALISI DEL RISCHIO E ASSESSMENT

- *Mappatura delle infrastrutture critiche e delle vulnerabilita'*
- *Gap analysis rispetto ai requisiti Nis 2*
- *Redazione di un piano tecnico e normativo*

Azioni chiave del System Integrator nella Nis 2

PROGETTAZIONE E IMPLEMENTAZIONE DELLE MISURE

- Soluzioni di cybersecurity : Firewall, Siem , Mfa
- Business Continuity e Disaster Recovery
- Sicurezza su cloud, endpoint e reti industriali (OT)

Azioni chiave del System Integrator nella Nis 2

INCIDENT DETECTION & RESPONSE

- Implementazione di strumenti per il monitoraggio continuo
- Creazione di play book per la gestione degli incidenti
- Integrazione con i sistemi di notifica verso CSIRT/ ACN

Formazione del personale e Awareness

MANAGED SERVICES

- Fornitura di Security Operation Center (SOC)
- Servizi di aggiornamento e patching continuo
- Threat Intelligence e Vulnerability management

Conclusioni

Il System integrator e’ fondamentale nell’ attuazione nella direttiva Nis2 aiutando le organizzazioni a raggiungere la conformita’ normativa, garantendo l’adozione di soluzioni tecnologiche adeguate e supportando una cybersecurity sostenibile e adattiva

GRAZIE PER L'ATTENZIONE