DIRETTIVA NIS 2

APPROFONDIMENTO E ADEMPIMENTI

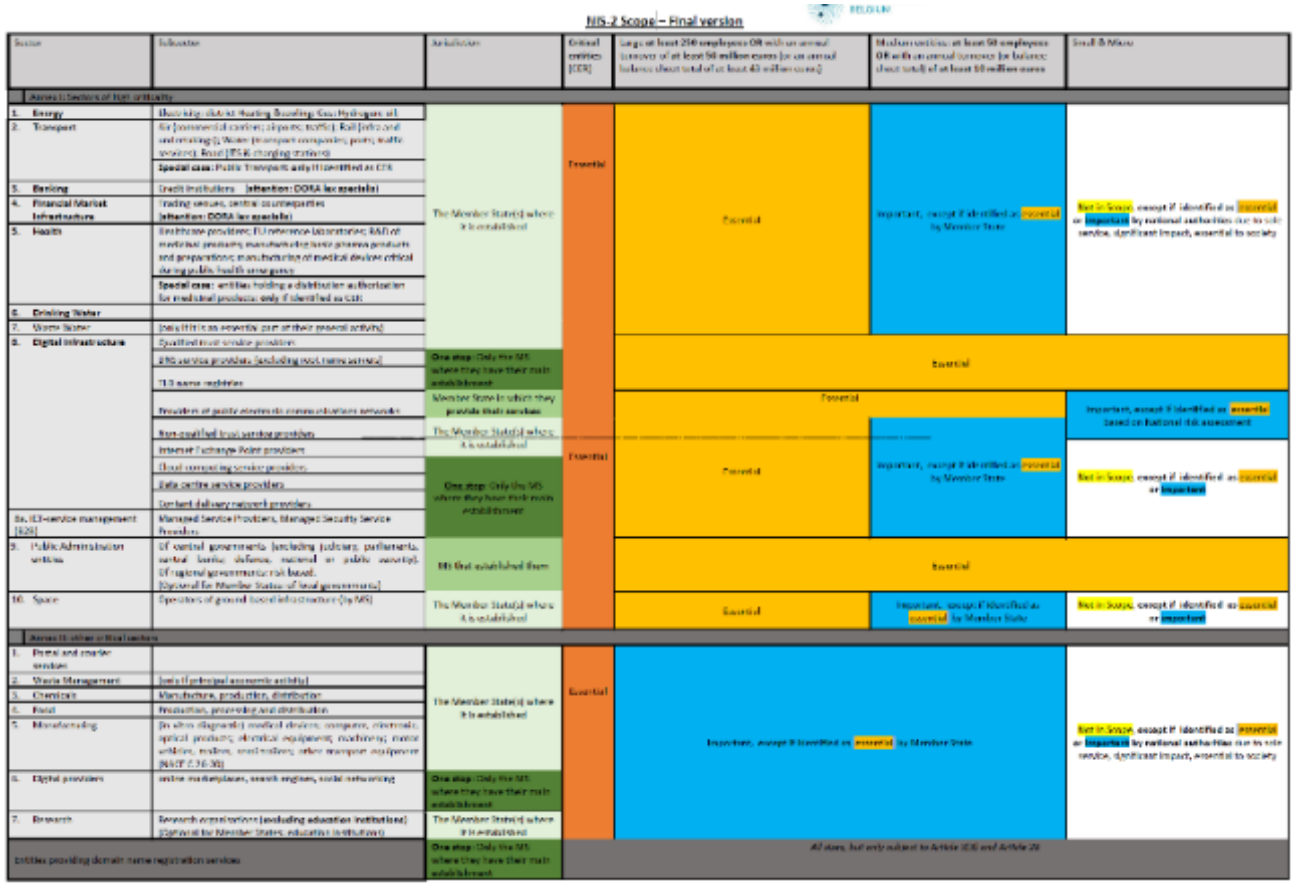
VINCENZO CALABRÒ

COS'È LA NIS 2?

- NIS 2 (Direttiva UE 2022/2055) è entrata in vigore il 17 gennaio 2023.
- Dovrà essere recepita dall'Italia entro l'ottobre 2024.
- Rispetto alla NIS:
  - Aumentano i soggetti.
  - E' richiesta un'analisi dei rischi.
  - Le misure di sicurezza dovranno essere adeguate al contesto, considerando quindi anche la capacità di spesa.

A CHI SI APPLICA LA NIS 2?

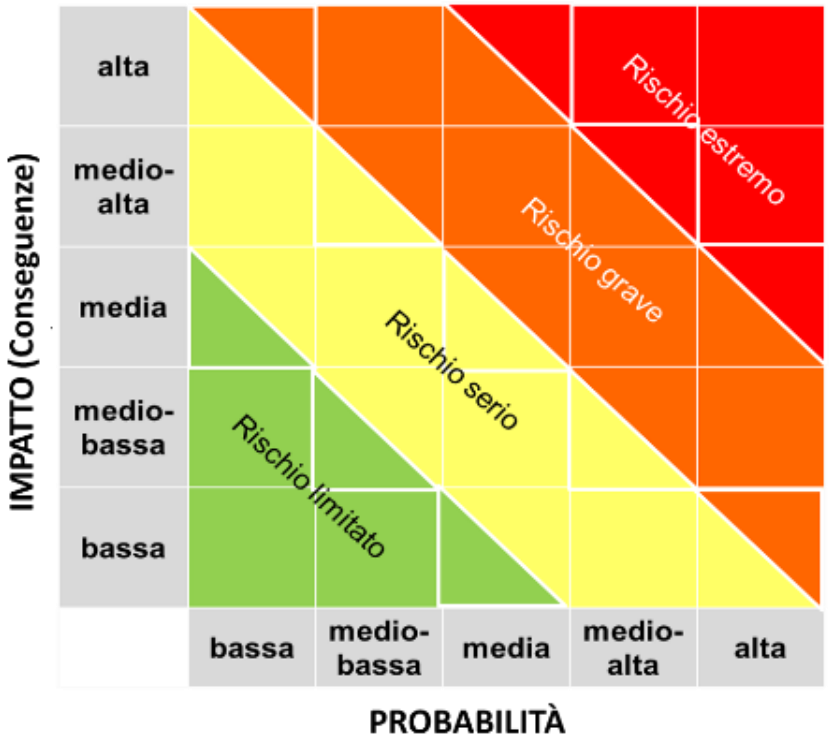
- L'applicabilità dipende da settore e dimensione. La NIS2 è applicabile a:
  - soggetti essenziali (essential entities);
  - soggetti importanti (important entities).
- La differenza pratica riguarda i controlli e le sanzioni.
- Ulteriori soggetti potrebbero essere aggiunti dalla normativa nazionale.
- Le entità dovranno riconoscersi come soggetti a cui è applicabile la NIS 2, non è più l'autorità che le designa come tali. Le entità si dovranno registrare secondo regole che saranno fornite.
- Entro il 17 aprile 2025, gli Stati membri definiscono un elenco dei soggetti.



SOGGETTI A CUI SI APPLICA LA NIS 2

VALUTAZIONE DEL RISCHIO

- NIS2 è multirischio: logico, fisico (in precedenza non richiesto), governo, lock in tecnologico, utilities. E considera l'impatto "sociale ed economico" e richiede un "livello appropriato".
- Gli Orientamenti della Commissione del 13.9.2023 indicano di considerare le seguenti minacce, sempre in una logica di multirischio:
  - sabotaggi,
  - furti,
  - incendi,
  - inondazioni,
  - problemi di telecomunicazione,
  - problemi di interruzioni di corrente,
  - qualsiasi accesso fisico non autorizzato,
  - guasti del sistema,
  - errori umani,
  - azioni malevole, fenomeni naturali.



MISURE DI SICUREZZA

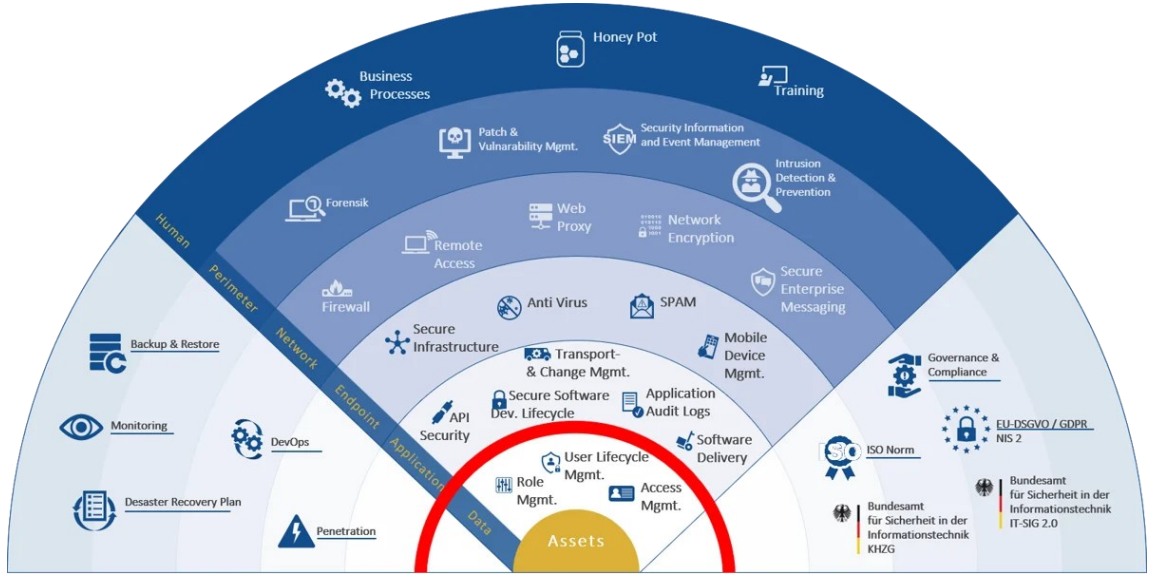
La Direttiva identifica misure di gestione del rischio:

1. Politiche di analisi dei rischi e della sicurezza
2. Sistemi di gestione degli incidenti
3. Soluzioni di business continuity
4. Misure di sicurezza dell'intera supply chain
5. Sicurezza dell'acquisizione, sviluppo e manutenzione dei sistemi e delle reti informatiche, compresa la gestione e la divulgazione delle vulnerabilità
6. Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersecurity
7. Pratiche di igiene informatica basilari e formazione in materia di sicurezza informatica
8. Uso della crittografia
9. Sicurezza delle risorse umane e politiche di controllo degli accessi (log management) e gestione degli asset
10. Uso 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 all'interno dell'entità, ove opportuno.

ATTI DI ESECUZIONE

Entro il 17 ottobre 2024, la Commissione adotta atti di esecuzione che stabiliscono i requisiti tecnici e metodologici delle misure per quanto riguarda i fornitori di:

- servizi DNS,
- registri dei nomi di dominio di primo livello (TLD),
- servizi di cloud computing,
- servizi di data center,
- reti di distribuzione dei contenuti,
- servizi gestiti,
- servizi di sicurezza gestiti,
- mercati online,
- motori di ricerca online,
- piattaforme di servizi di social network,
- prestatori di servizi fiduciari.



SI RACCOMANDA UN RIFERIMENTO NOTO PER L'APPLICAZIONE DELLE MISURE DI SICUREZZA IN GRADO DI FORNIRE LE SEGUENTI FUNZIONI

- valutazione del rischio
- trattamento del rischio e scelta delle misure di sicurezza
- gestione degli incidenti
- miglioramento continuo

GESTIONE INCIDENTI

- NIS 2 (come NIS 1) prevede l'obbligo di notifica al CSIRT e alle autorità competenti (oltre che ai destinatari stessi del servizio) degli incidenti significativi (se hanno causato o sono in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato o se si sono ripercossi o sono in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli).
- Le comunicazioni al CSIRT dovranno avvenire:
  - Entro 24 ore dalla conoscenza dell'incidente con una notifica di preallarme (per attenuare la potenziale diffusione di incidenti e per consentire di chiedere assistenza).
  - Entro 72 ore dalla conoscenza dell'incidente con aggiornamenti rispetto alle informazioni fornite con il preallarme
  - Entro 1 mese dalla conoscenza dell'incidente con una relazione finale a completamento del processo di segnalazione (questo per poter trarre insegnamenti preziosi dai singoli incidenti).
- Il CSIRT, con il NIS 2, ha maggiori responsabilità di coordinamento.

GESTIONE INCIDENTI

- Alcuni soggetti sono soggetti a più normative e quindi a diverse modalità di notificazione degli incidenti.
- Obbligatorietà:
  - Articolo 23, stabilisce quando è obbligatorio notificare;
  - Articolo 30, indica quando la notifica è volontaria (altri incidenti, minacce, quasi incidenti, anche da parte degli altri soggetti).
- Definiti anche i «quasi incidenti». Un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato.
- La NIS2 istituisce la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe).

SUPPLY CHAIN MANAGEMENT

- Degrado del contesto geopolitico e cyberwarfare
- Shortage di risorse e aumento dei costi della logistica
- Attacchi informatici sempre più sofisticati (ed economici…)
- Difficile visibilità e controllo sui fornitori (e sui loro fornitori…)
- Mancanza di competenze e risorse

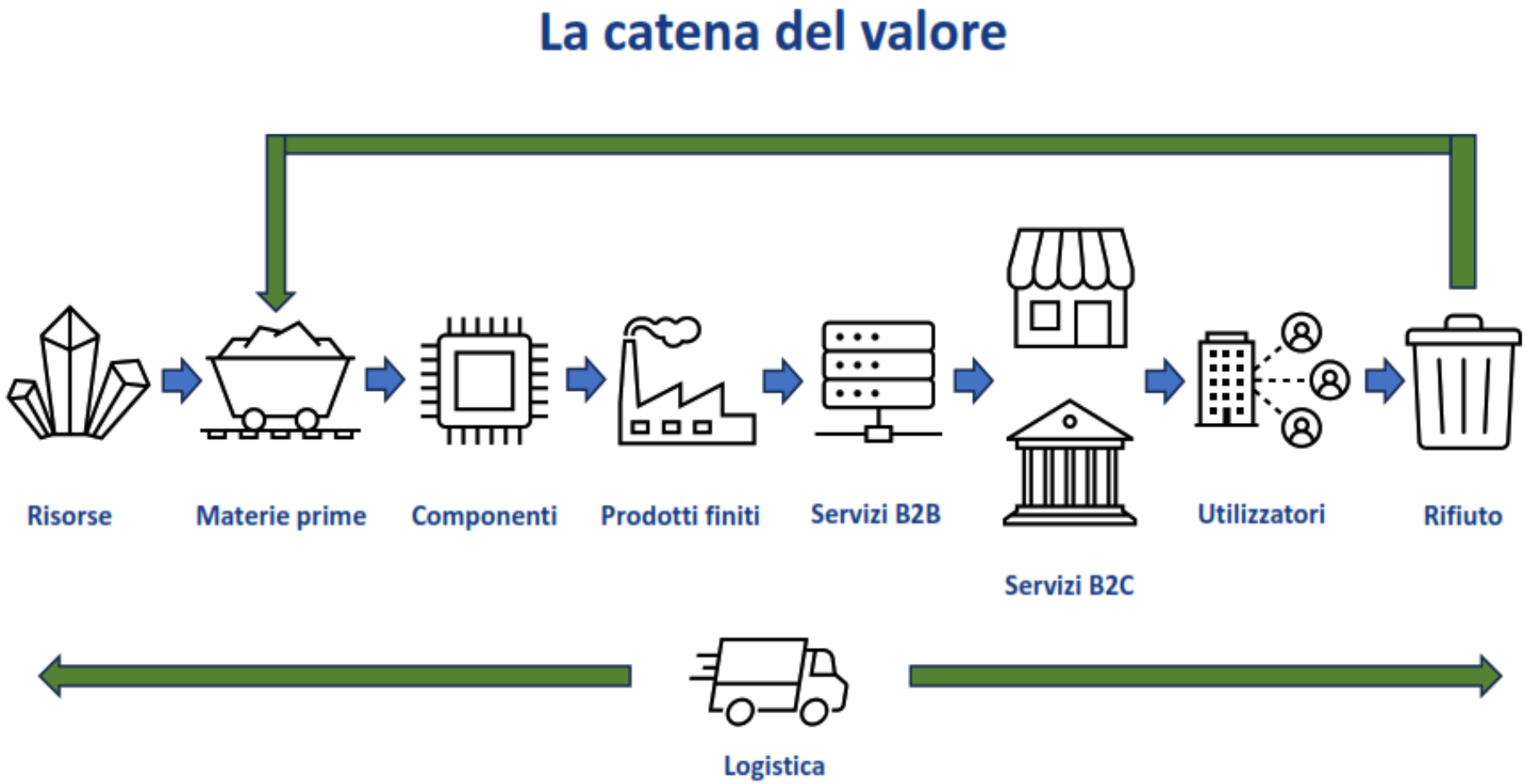
I PILLAR SULLA SUPPLY CHAIN

- Valutare i rischi connessi alla supply chain (approccio olistico)
- Adottare misure di mitigazione
- Cooperazione tra organizzazioni e istituzioni

Effetto Domino

- Gli incidenti sono il risultato finale di una catena di fattori di incidenti.
  Tanti piccoli eventi possono portare ad un grande evento.

VALUTARE IL RISCHIO



GLI IMPATTI

(C) Riservatezza - Confidentiality

Garantire la riservatezza (privacy) dei dati creati, custoditi, trasmessi e diffusi evitandone l'accesso a utenti non autorizzati

(I) Integrità - Integrity

Garantire la protezione del dato da qualsiasi tentativo di manomissione dello stesso, prevenendo alterazione o cancellazione non autorizzata.

(A) Disponibilità - Availability

Garantire la continuità alla fruizione e all'accesso di dati e servizi, impedendo interruzioni nell'erogazione di servizi hardware e software

I PRINCIPALI RISCHI CYBER CONNESSI ALLA SUPPLY CHAIN

- Malware e ransomware
- Aumento dei costi
- Potere contrattuale
- Data breach
- Business Interruption
- Vulnerabilità del software
- Difficoltà di monitoraggio
- Perdita di controllo
- Fattore umano: atti dolosi da insider
- Fattore umano: shortage competenze
- Fattore umano: errore
- Attacchi alla supply chain: «island hopping»
- Attacchi alla supply chain: «watering hole»
- Compliance

UN APPROCCIO STRUTTURATO

Come si valuta?

- Definire gli obiettivi
- Identificare le aree di rischio e identificare i fornitori critici su quelle aree
- Definire le soglie di tolleranza
  - Risk appetite (propensione al rischio)
  - Risk tolerance (devianza tollerabile rispetto alla propensione)
  - Risk capacity (massimo livello di rischio sopportabile)
- Analizzare il rischio (Probabilità e Impatti)
- Valutare il rischio rispetto alle soglie
- Identificare gli indicatori di rischio e i parametri di controllo (KRI)
- Identificare gli indicatori di performance e i parametri di controllo (KPI)
- Scegliere l'azione di trattamento dei rischi valutati
- Monitoraggio e revisione periodica

COME MITIGARE IL RISCHIO

Scegliamo i migliori

- Screening e classificazione dei fornitori, con rating di affidabilità
- Diversificare la catena di fornitura ove possibile
- Richiedere attestazioni e certificazioni (es. ISO 27001, ISO 22301)
- Prevedere clausole di notifica, monitoraggio e audit di 2° parte
- Prevedere clausole di garanzia nei confronti dei sub-fornitori

… e manteniamo il Controllo

- Coinvolgiamoli nelle esercitazioni e nei test
- Prevediamo monitoraggi e audit periodici basati sul rischio
- Condividiamo informazioni su minacce, vulnerabilità, rischi, azioni di mitigazione
- Formazione e consapevolezza

GRAZIE

INFO@VINCENZOCALABRO.IT

WWW.VINCENZOCALABRO.IT