Implementazione NIS2 in ISPRA

Andrea Ranaldi
ISPRA

Il mercato della NIS2!

- Un favoloso programma per la gestione degli assets informatici
- Un magico framework per la sicurezza informatica
- Mai più problemi con la NIS

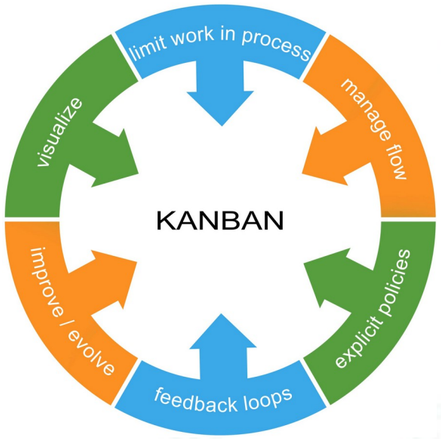
Ma la NIS è tutta qui?

Approccio ISPRA allo studio della NIS2

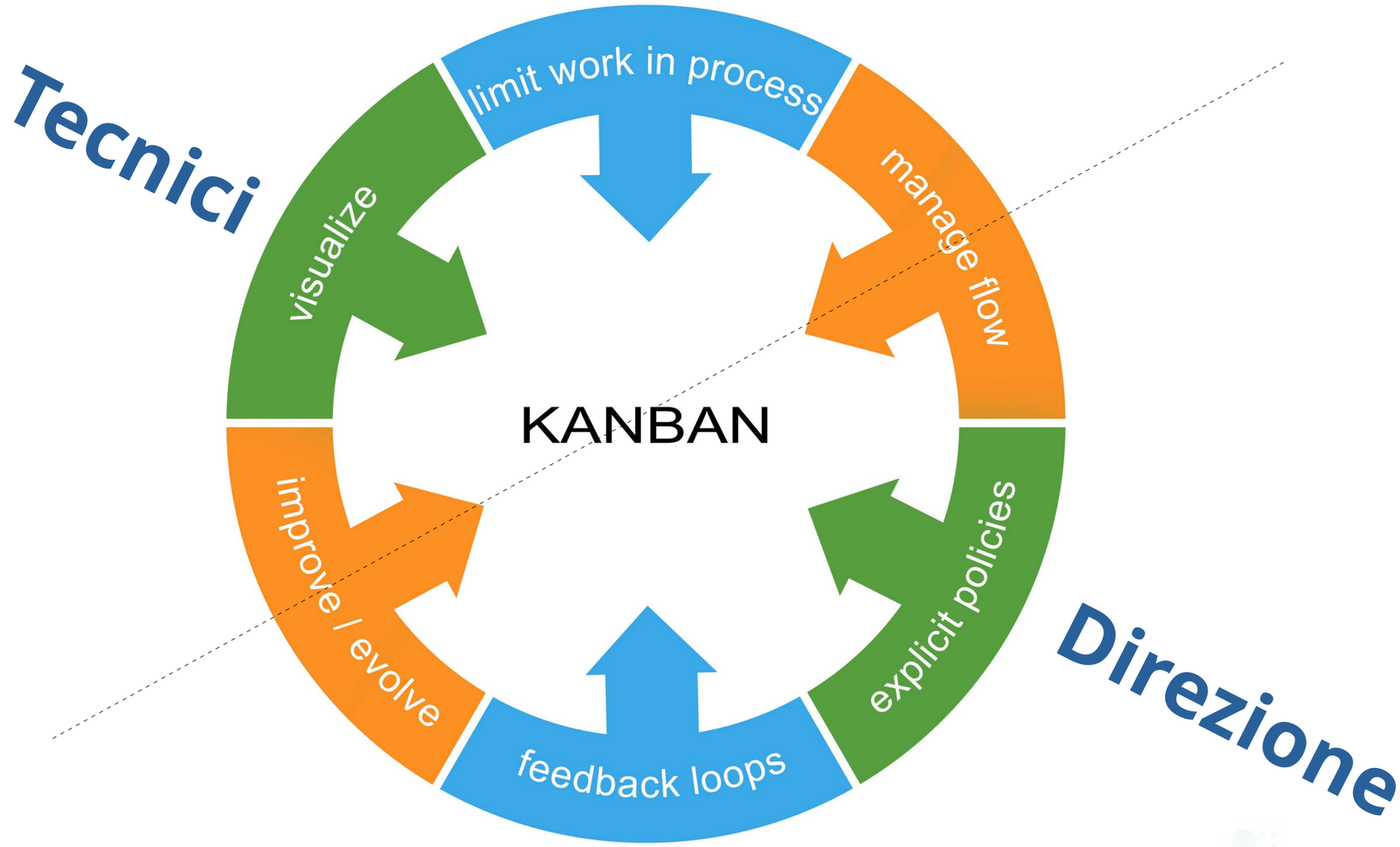
- Studio dei testi di riferimento europei ed italiani da parte dei tecnici
- Analisi degli obiettivi minimi e dei processi necessari
- Engagement della dirigenza per la definizione di processi e obiettivi
- Pubblicazione di processi e responsabilità da parte della direzione
- Formazione degli attori e Analisi dei risultati
- Definizione dei successivi traguardi

...non distante dai principi Kanban

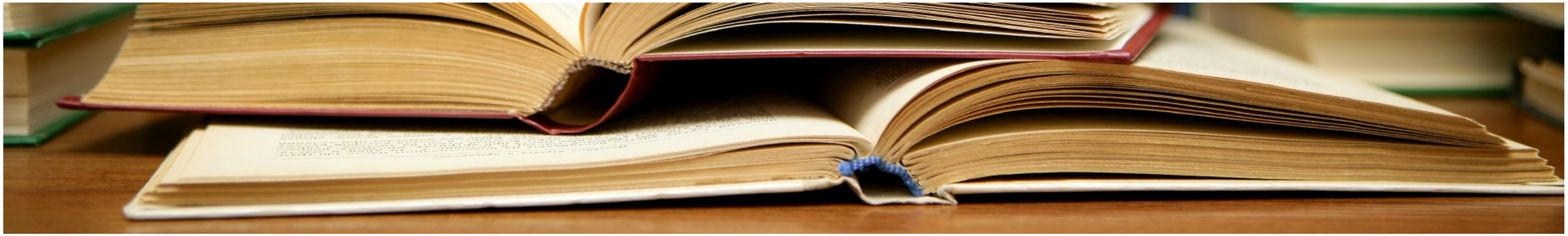
- Studio dei testi di riferimento europei ed italiani da parte dei tecnici
  Visualize
- Analisi degli obiettivi minimi e dei processi necessari
  Limit work in process
- Engagement della dirigenza, definizione di processi e obiettivi
  Manage Flow
- Pubblicazione di processi e responsabilità da parte della direzione
  Explicit policies
- Formazione degli attori e Analisi dei risultati
  Feedback Loops
- Definizione dei successivi traguardi
  Improve / Evolve



Sicurezza: un processo di crescita continua



Partire studiando le leggi



POSSIBILE, UTILE, RICHIEDE POCO TEMPO

- Direttiva UE 2022/2555, NIS2
- Piano di implementazione della strategia nazionale di Cybersicurezza
- Legge 90/2024, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici
- Decreto 138/2024, Recepimento della direttiva (UE) 2022/2555

- Gruppo di Lavoro volontario
- Un incontro settimanale
- 6 settimane per completare tutto

Direttiva UE 2022/2555 - NIS2

Relativa a misure per un livello comune elevato di cibersicurezza nell'Unione

- Non parla con noi ma con gli stati membri
- Dispone gli obblighi per gli stati europei in materia di sicurezza informatica
- Chiede di definire le misure minime per la gestione del rischio informatico
- Definisce come condividere le informazioni di sicurezza
- Definisce gli obblighi di vigilanza
- Definisce le tipologie di soggetti che devono garantire un livello adeguato di sicurezza
- Definisce che le leggi nazionali in materia di sicurezza non possono essere inferiori a quelle europee
- Richiede di programmare e adottare una Strategia nazionale per la cibersicurezza
- **Richiede che la sicurezza dei rischi e della sicurezza sia materia degli organi di gestione dei soggetti**
- Richiede che i soggetti adottino misure tecniche, operative ed organizzative adeguate e **proporzionali ai rischi di sicurezza** previsti per prevenire o ridurre al minimo l'impatto degli incidenti.
- Le misure sono basate su un approccio multirischio che tiene conto dei sistemi informatici, della rete, dell'ambiente fisico
- Obblighi di notifica

Direttiva UE 2022/2555 - NIS2

Relativa a misure per un livello comune elevato di cibersicurezza nell'Unione

Concetti chiave

- Parla agli stati
- Richiede di individuare soggetti e le loro risorse
- Valutazione del rischio delle risorse
- Minimizzare il rischio
- Preparazione e la risposta in caso di inidente
- Approccio alla sicurezza come strategia centrale
- Approccio multirischio
- Proporzione delle misure
- Notifiche degli eventi

Strategia nazionale di Cybersicurezza

Piano di implementazione

Concetti chiave

- Definisce gli obiettivi di sicurezza dello stato
- Definisce come misurare gli obiettivi
- Viene rivalutata al massimo ogni cinque anni
- Deve definire un meccanismo per individuare le risorse e una valutazione dei rischio
- Individua delle misure per garantire la preparazione e la risposta degli incidenti
- È la base per definire gli obiettivi di sicurezza per i soggetti NIS

Legge 90/2024

Disposizioni in materia di rafforzamento della cybersicu- rezza nazionale e di reati informatici

Concetti chiave

- Obbligo di segnalazione degli incidenti
- Richiede ai soggetti l'adeguamento entro 15 giorni per le segnalazioni ACN
- Gli enti devono definire strutture con i seguenti incarichi:
  - Sviluppo delle politiche e delle procedure per la sicurezza delle informazioni
  - Produzione ed aggiornamento di sistemi di analisi preventiva, rilevamento e gestione deli rischio informatico
  - Produzione e aggiornamento di un piano programmatico per la sicurezza dati
  - Pianificazione e attuazione degli interventi di potenziamento per la gestione dei rischi informatici in coerenza con le analisi fatte
  - Pianificazione e adozione delle linee guida emanate dall'ACN
  - Monitoraggio e valutazione continua della sicurezza e delle vulnerabilità
  - Devono definire il referente per la cybersycurezza
- Bisogna nominare un referente per la cybersicurezza che operi nelle strutture, che possieda adeguata competenza e che svolga funzione di contatto con ACN
- Da ad ACN funzioni di agenzia per la crittografia e deve stilare linee guida
- Obbliga i soggetti a seguire le linee guida ACN su crittografia

Decreto 138/2024

Recepimento della direttiva (UE) 2022/2555

Concetti chiave

- il decresto stabilisce le misure per garantire la sicurezza informatica a livello nazionale e comprende
  - La Strategia nazionale di cybersicurezza
  - integra la gestione delle crisi a livello nazionale
  - Conferma l'ACN come: autorità NIS, Punto unico NIS, autorità per le crisi, CSIRT
- Definisce un obbligo di registrazione per i soggetti NIS2 dal 01/01 al 28/02 2025
- Obbligo di Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi a partire dal 01/05
- Incarica le autorità di settore per supportare ACN per l'applicazione del decreto e la produzione delle linee guida
- ACN coopera con i soggetti (se non troppo esoso), vigila e segnala le vulnerabilità
- ACN emette linee guida, raccomandazioni e orientamenti non vincolanti

Leve per l’applicazione delle direttive

Direttiva NIS - Art. 20

- Gli Stati membri provvedono affinché i membri dell'organo di gestione e i dipendanti dei soggetti siano tenuti a seguire formazione, per far acquisire competenze sufficienti ad individuarei i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.

Legge 90, art. 8

- Strutture dedicate alla sicurezza

Decreto 138, art. 23

- Gli organi amministrativi e direttivi dei soggetti NIS:
  - approvano le implementazioni delle misure di gestione dei rischi per la sicurezza informatica come da Art. 24
  - Sovrintendono all'implementazione degli obblighi presenti all Art. 7
  - Sono responsabili delle violazioni del presente decreto
  - sono tenuti a seguire una formazione in materia di sicurezza informatica
  - promuovono l'offerta periodica di formazione ai propri dipendenti atta a ridurre i rischi per la sicurezza informatica
  - sono informatiti degli incidenti e delle notifiche ai sensi dell'Art. 25 e 26

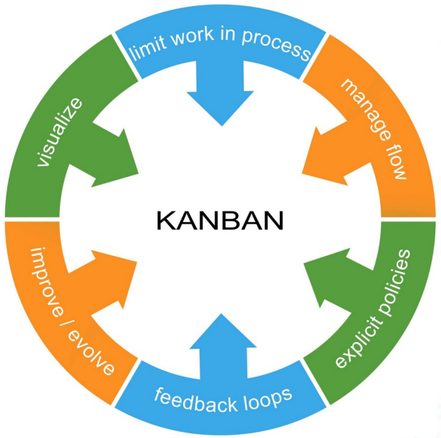
Primo SPRINT

Obiettivi

- Definizione del calendario per le prime attività
- Definizione delle responsabilità e delle strutture definite nella legge 90
- Definizione delle responsabilità e delle figure definite nel decreto 138

Dove siamo

- In attesa della formalizzazione delle nomine



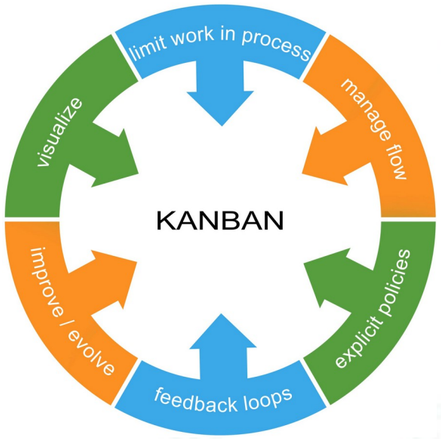
Secondo SPRINT

Obiettivi

- Definizione di una nuova mappa delle risorse

Dove siamo

- Brainstorming
- In attesa di chiusura del primo sprint



Una mappa delle risorse come centro della sicurezza

- Differenziare i servizi (le applicazioni) dai sistemi in cui sono ospitate
- Stabilire le connessioni tra servizi e i sistemi da cui dipendono
- Stabilire le connessioni tra i vari servizi
- Stabilire le connessioni tra i sistemi e le reti
- Stabilire la connessione tra i sistemi virtualizzato e virtualizzatore
- Stabilire la connessione tra sistema ed eventuale hardware fisico che lo ospita
- Identificare i servizi con i conmi DNS a cui rispondono
- Definire le responsabilità di ogni servizio ed ogni sistema
- Creare una mappa a maglie multilivello che ti permetta di individuare rapidamente le risorse collegate ad ogni nodo in caso di incidente
- Identificare il livello di rischio per ogni nodo della mappa

Grazie a tutti, per le domande:

wooclap.com e codice WSGARR24