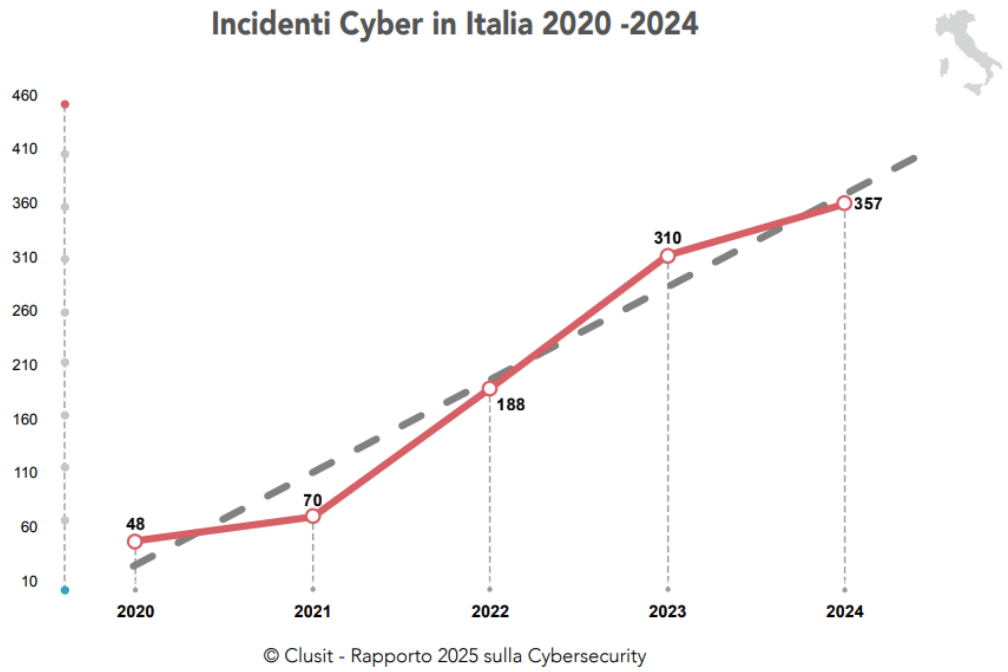
1

Contesto Nazionale

FONDAZIONE PIEMONTE INNOVA

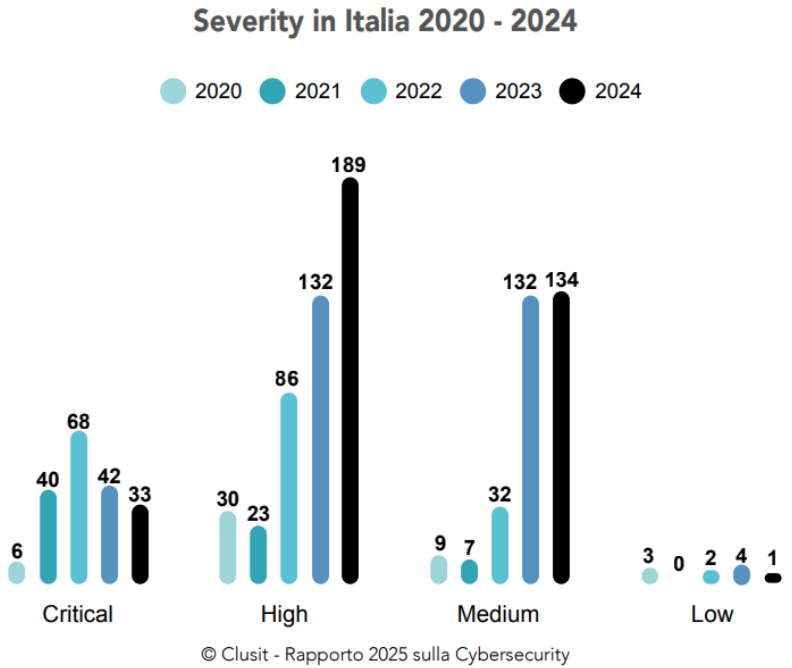
ATTACCHI ITALIA

Cyber attacchi Italia
2020 - 2024:
973 attacchi noti, di cui
357 (**39%**) nel 2024



ATTACCHI ITALIA - SEVERITY

Severity attacchi Italia **2020 – 2024**:
- **189** High
- **134** Medium



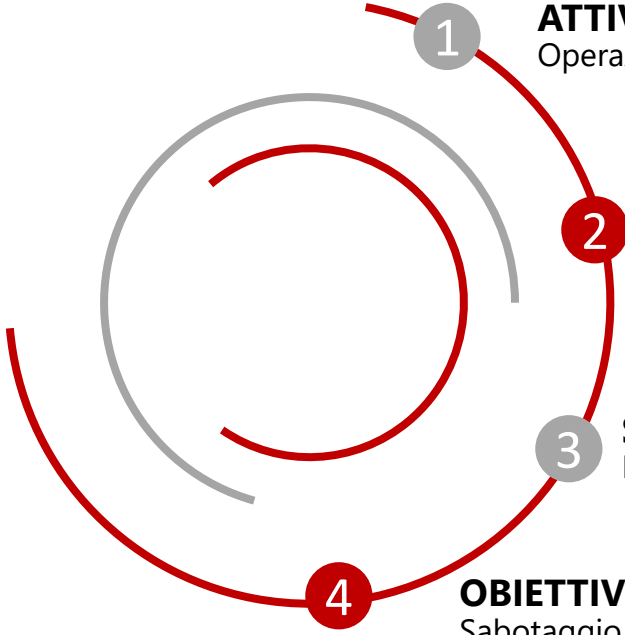
MAPPA ATTIVITÀ A LIVELLO GLOBALE

https://livethreatmap.radware.com

2
Cyberwarfare

FONDAZIONE PIEMONTE INNOVA

DEFINIZIONE



1 **ATTIVITA'**
Operazioni e attacchi informatici

2 **SOGGETTI**
Governi o gruppi affiliati

3 **SCOPI**
Politici o militari

4 **OBIETTIVI**
Sabotaggio infrastrutture critiche
Spionaggio e Disinformazione

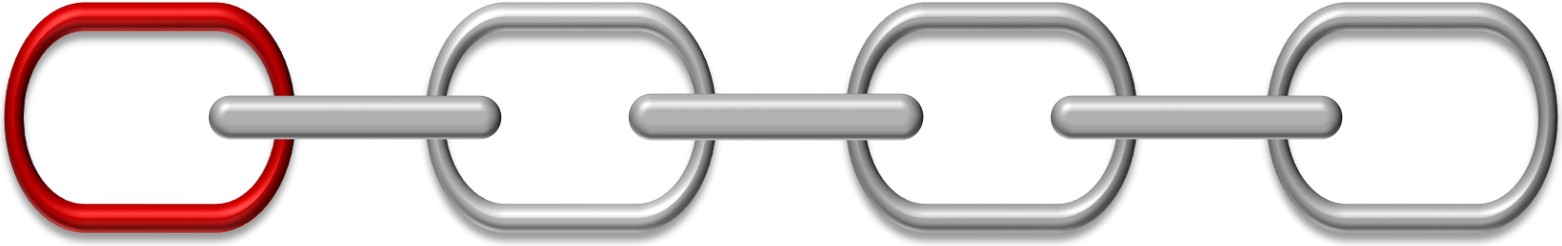
SUPPLY CHAIN

Le **aziende** possono trovarsi ad essere **coinvolte** indirettamente nella **cyberwarfare**

Sfruttamento
Debolezze/vulnerabilità
Infrastrutture digitali

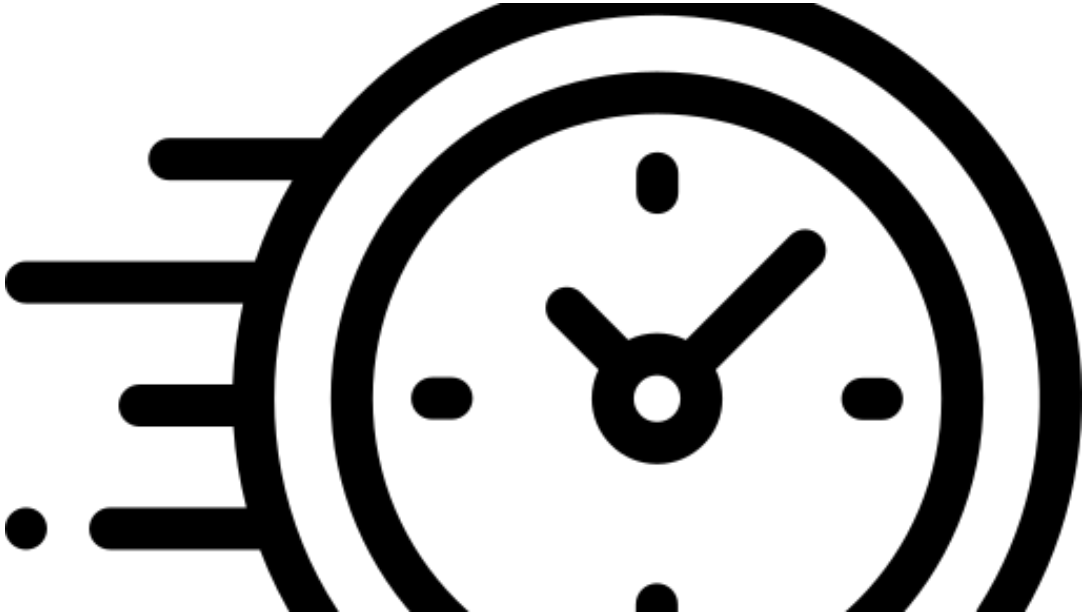
Collaborazione
Organismi di sicurezza

Sicurezza
Nazionale
Internazionale



FATTORE TEMPO

Le aziende sono **sotto attacco** costante:
non è più **questione** di considerare «se» si verificherà, ma **«quando»** si verificherà

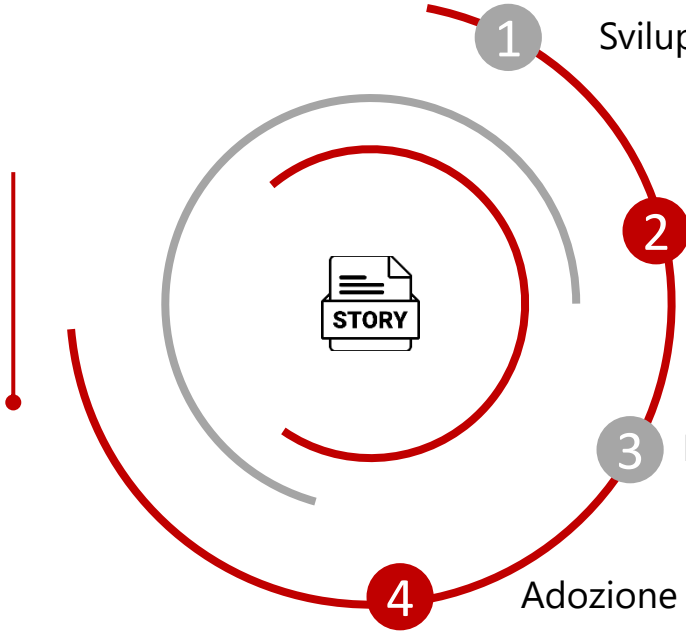


3
Processi

FONDAZIONE PIEMONTE INNOVA

CONTESTO STORICO

Cambio prospettiva nell'**approccio** alla **cybersecurity**



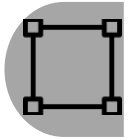
1. Sviluppo cybercrime
2. Nuove normative (Gdpr – Nis II)
3. Rivalutazione difesa perimetro
4. Adozione logica di detect and response

PERIMETRO - EVOLUZIONE

La **sicurezza perimetrale informatica** si concentra sulla **difesa dei confini virtuali** dell'azienda, che costituiscono il cosiddetto perimetro aziendale

PRIMA

Asset interni



Confini fisici azienda

Radicale

trasformazione

ADESSO

Mobilità/Lavoro remoto/Cloud ibridi

Fluido e dinamico

APPROCCIO CYBERSECURITY

Le aziende non possono più limitarsi a logica di difesa del perimetro aziendale, ma devono implementare

- Strumenti
- Processi

Garantire reale sicurezza

attraverso sistemi

- **Verifica** Infrastrutture informatiche
- **Monitoraggio** Infrastrutture informatiche
- **Revisione continua** Infrastrutture informatiche

IMPORTANZA PROCESSI

I **primi effetti** si sono riscontrati sulla **predisposizione degli strumenti**, ponendo l'accento su

Incident Response Plan
Definizione/implementazione processi

Obiettivo 1
Individuare attacchi/Mitigare danni

Obiettivo 2
Eseguire post analysis

Predisposizione processi

Mantenere costante monitoraggio infrastrutture

Definire dinamiche response in caso violazione

INCIDENT RESPONSE

L' **incident response** può essere definito come un insieme di

- Procedure
- Risorse

Utilizzate per

reagire a

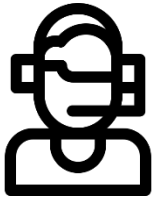
- Incidenti informatici

INCIDENT RESPONSE PLAN - IRP

Un **piano di risposta** agli incidenti è un insieme di

Istruzioni

Aiutano



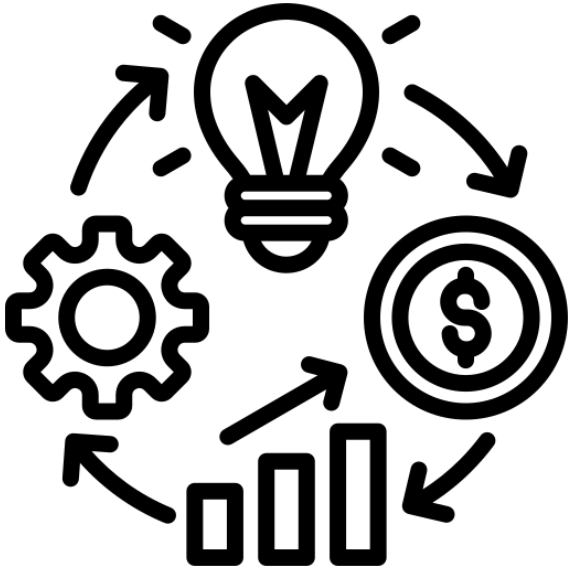
personale a

Rilevare
(Monitorare/Identificare)

Rispondere
(Contenere/Mitigare)

Recuperare
e **apprendere**

BUSINESS CONTINUITY



Processo aziendale

Continuità
Garantita a tutte le attività aziendali

Prevenzione
Interruzioni sistemi/attività

BUSINESS IMPACT ANALYSIS - BIA

Passaggio chiave nel processo di pianificazione della **continuità di business**, permette la definizione

- Requisiti sistema
- Processi
- Interdipendenze

utilizzando

queste informazioni

- Previsione conseguenze interruzione processi
- Garanzia continuità business

RISK ASSESSMENT – TOM E SPIKE

https://www.youtube.com/watch?v=QkRzrqqDd8E&t=2s

BIA VS RA

Business Impact Analysis

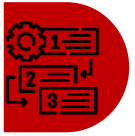
Punto partenza elaborazione strategie

Focus su conseguenze guasti/possibili incidenti

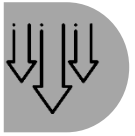
Valutazione impatti diversa natura

Risk Assessment

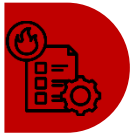
Successivo alla BIA



Focus su situazioni potenzialmente pericolose

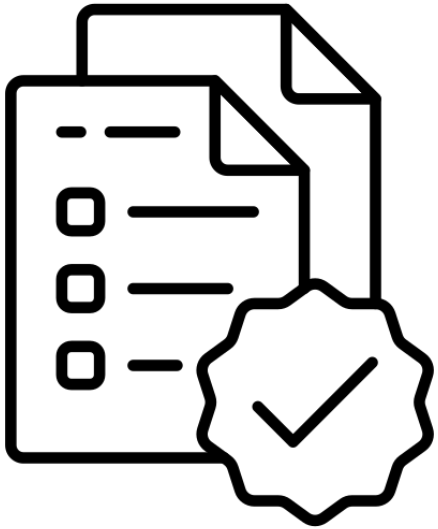


Valutazione probabilità/gravità incidente



BUSINESS CONTINUITY PLAN - BCP

Documento costituito dalle **procedure formalizzate** che guidano le organizzazioni



- **Risposta** ad un incidente
- **Recupero/ripristino** processi critici a un livello di funzionalità accettabile
- Recupero/ripristino entro il **tempo di ripristino** stabilito (RTO)

4
Tecnologie

FONDAZIONE PIEMONTE INNOVA

SISTEMA SICUREZZA DI RETE - SSR

Firewall
software/hardware

Network access control - NAC
autenticazione/autorizzazione

Intrusion detection and prevention system - IDPS

Virtual private network - VPN

Application security

Sicurezza e-mail
filtri antispam

SSR FUNZIONAMENTO

I **sistemi di sicurezza di rete** (SSR) funzionano a **due livelli**

Perimetro
Impedire entrata rete

Interno rete
Controlli risorse interne

Strategia stratificazione

controlli multipli

Difesa in profondità
Defense in depth

FIREWALL

Soluzione e **prima linea di difesa** sicurezza rete che **monitora**

Traffico in entrata

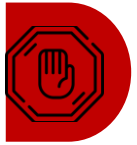
Traffico in uscita

Attraverso serie

predefinita regole per

Consentire eventi

Bloccare eventi



INTRUSION DETECTION SYSTEM - IDS

Un sistema di rilevamento delle intrusioni (IDS) è uno **strumento di sicurezza di rete** che monitora

- Traffico rete
- Dispositivi

per rilevare e avvisare

admin/tool sicurezza su

- Attività dannose note
- Attività sospette
- Violazioni politiche sicurezza

INTRUSION PREVENTION SYSTEM - IPS

Talvolta detti IDPS, includendo stesse funzioni di rilevamento/reporting minacce degli IDS, **monitora traffico di rete** per

- Individuare potenziali minacce
- Bloccarle automaticamente

- Avvisando team sicurezza
- Interrompendo connessioni pericolose
- Rimuovendo contenuti dannosi
- Attivando altri dispositivi sicurezza

GRAZIE

www.piemonteinnova.it

facebook

LinkedIn

YouTube

cyber@piemonteinnova.it

FONDAZIONE PIEMONTE INNOVA