

I rischi Cyber per la Pubblica Amministrazione: scenari evolutivi e come proteggersi

- ▶ Scenari evolutivi del rischio Cyber per le Pubbliche Amministrazioni
- ▶ Come proteggersi nel contesto attuale
- ▶ Il ruolo dell' RTD

- ▶ Scenari evolutivi del rischio Cyber per le Pubbliche Amministrazioni
- ▶ Come proteggersi nel contesto attuale
- ▶ Il ruolo dell' RTD

Trasformazione digitale

La **digitalizzazione e la trasformazione digitale** stanno avendo un impatto significativo sulle Pubbliche Amministrazioni, le città stanno diventando sempre più «smart», aprendo la strada a sistemi che possono auto-evolversi e raccogliere dati in modo automatico, senza alcun intervento umano.

- Questa evoluzione trasforma le città in smart city, in grado di **sfruttare le tecnologie digitali** per migliorare l'efficienza operativa, la sostenibilità e la qualità della vita dei cittadini.
- Elemento fondamentale è la **connessione di tutti i sistemi informativi** all'interno della città (es. dispositivi IoT e applicazioni mobili), creando un **ecosistema interconnesso**.



Introduzione ai rischi cyber

Da un lato la **trasformazione digitale** sta **migliorando l'efficienza** dei servizi verso gli utilizzatori, dall'altro **l'interconnessione dei sistemi** sta esponendo a **rischi di attacchi informatici**.

Rischi Cyber



Fughe di dati



Aumento dell'impatto di un evento avverso legato ad un'infrastruttura critica



Distacco della classe dirigente dal contesto reale, dovuto all'automazione



Imprevedibilità dell'evoluzione della tecnologia

Trasformazione digitale

La **digitalizzazione e la trasformazione digitale** stanno avendo un impatto significativo sulle Pubbliche Amministrazioni, le città stanno diventando sempre più «smart», aprendo la strada a sistemi che possono auto-evolversi e raccogliere dati in modo automatico, senza alcun intervento umano.

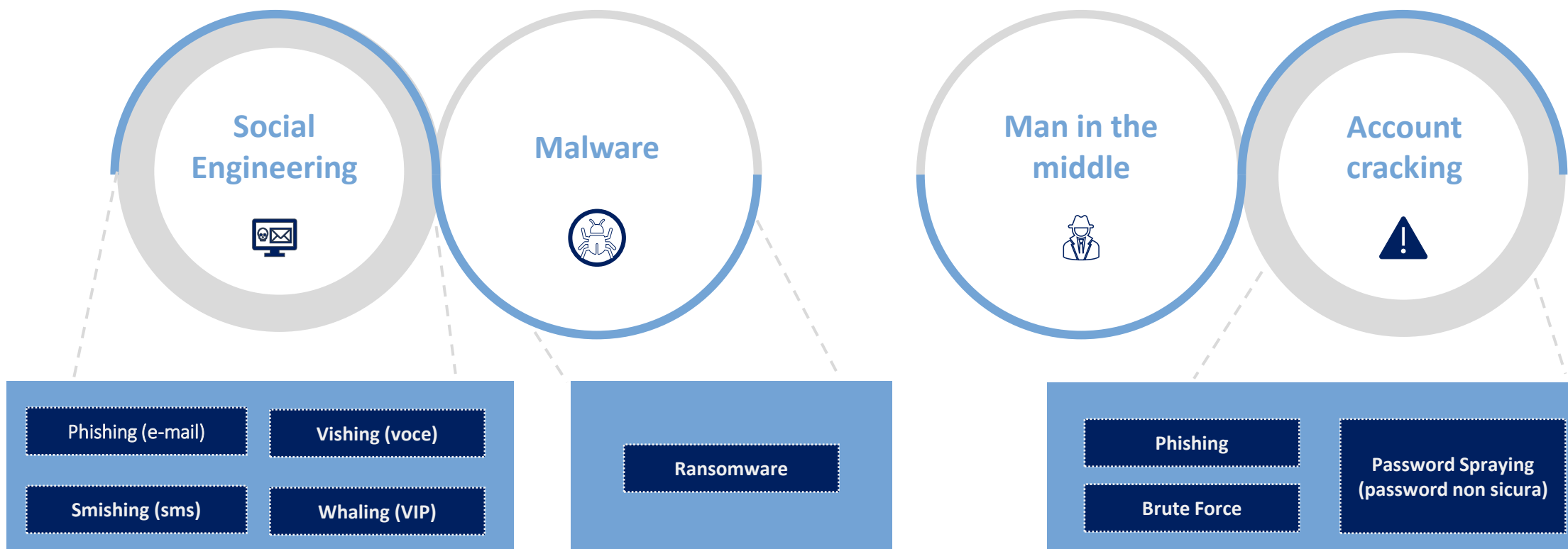
- Questa evoluzione trasforma le città in smart city, in grado di **sfruttare le tecnologie digitali** per migliorare l'efficienza operativa, la sostenibilità e la qualità della vita dei cittadini.
- Elemento fondamentale è la **connessione di tutti i sistemi informativi** all'interno della città (es. dispositivi IoT e applicazioni mobili), creando un **ecosistema interconnesso**.



Rischi Cyber – Minacce informatiche

I principali obiettivi degli attacchi informatici sono i dipendenti non consapevoli e le terze parti, spesso sfruttati come punti deboli per compromettere la sicurezza aziendale.

Minacce informatiche



Rischi Cyber – Evoluzione degli attacchi



Cyber Security

Protezione di un'organizzazione e delle sue reti, programmi e dati da attacchi, danni e interruzioni da minacce interne ed esterne

81%

ATTACCHI SEMPRE PIÙ GRAVI

Degli attacchi rilevati nel 2023 ha avuto un impatto **elevato** (critico o alto) a livello global.

Source: CLUSIT 2024

65%

TREND DEGLI INCIDENTI IN ITALIA

È la crescita degli incidenti informatici in Italia nel 2023 rispetto all'anno precedente.

Source: CLUSIT 2024

11%

ITALIA “NEL MIRINO”

Percentuale degli attacchi informatici sferrati dal cyber crimine a livello mondiale che nel 2023 sono andati

Source: CLUSIT 2024

64%

TIPOLOGIA DI ATTACCANTI

Percentuale degli attacchi rilevati con finalità di cybercrime, seguito dal 36% di attacchi con finalità di hacktivism, in netta crescita rispetto al 2022 (+761%)

Source: CLUSIT 2024

Rischi Cyber – Evoluzione degli attacchi nel settore pubblico

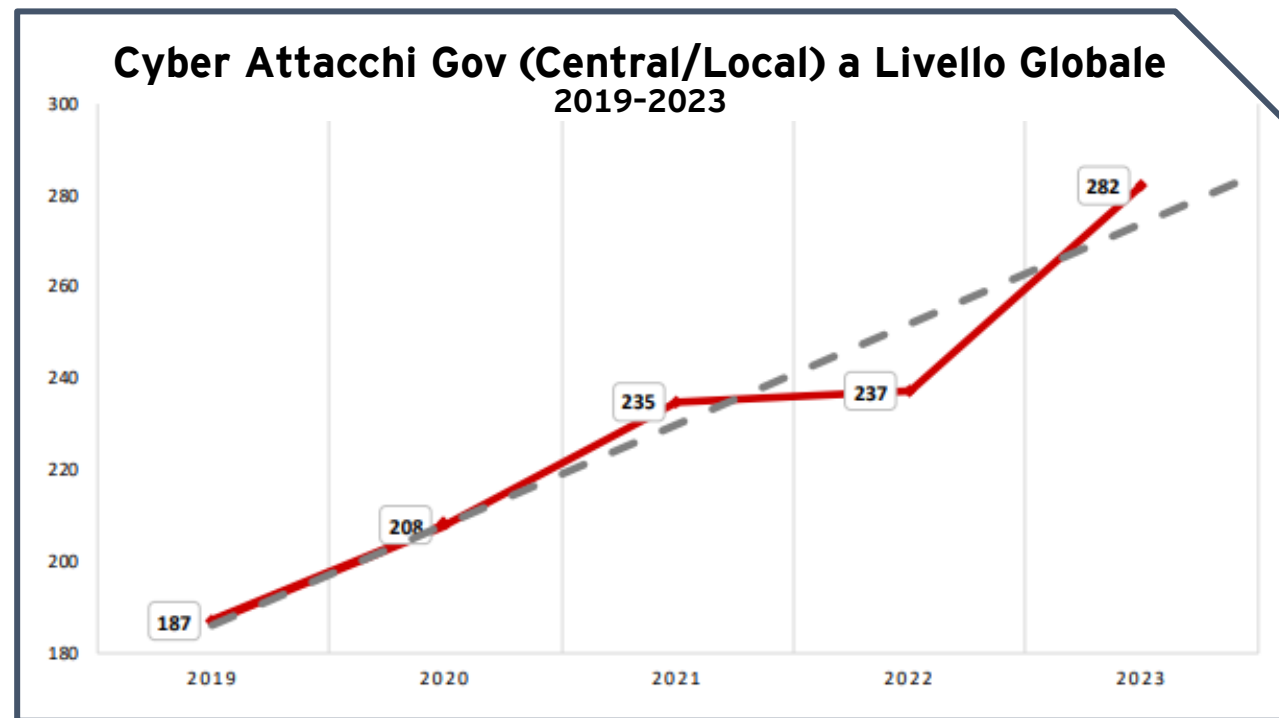


Trend nel Settore Pubblico

- Nel 2023 il settore della Pubblica Amministrazione ha subito il 12% degli attacchi informatici.
- Il settore Pubblico, insieme al settore Finance/Insurance, hanno costituito inoltre il 55% dei casi per quanto riguarda gli attacchi DDoS (interruzione del servizio).

“Il costo globale della criminalità informatica raggiungerà i 10,5 trilioni di dollari entro il 2025”

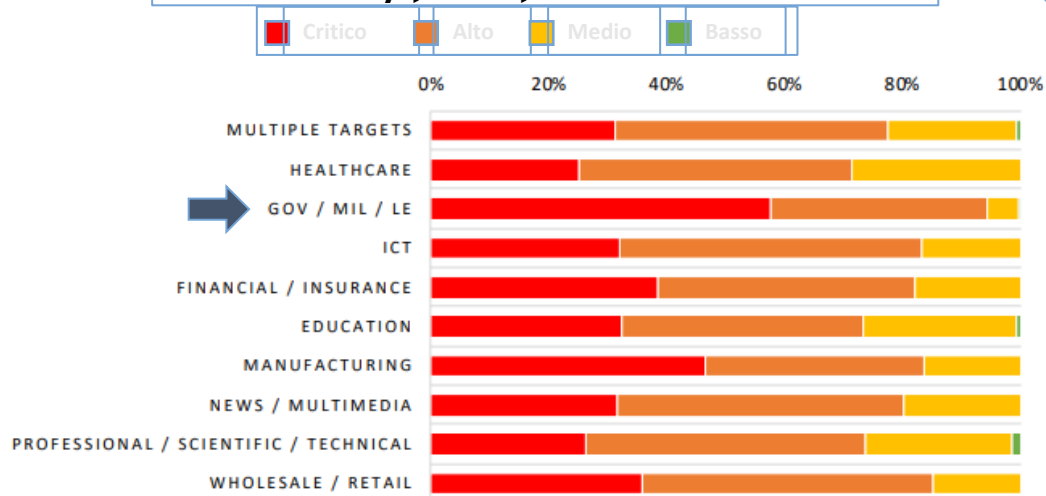
(Jurgen Stock, Segretario Generale dell'Interpol)



Rischi Cyber – Gravità degli attacchi per tipologia di vittima

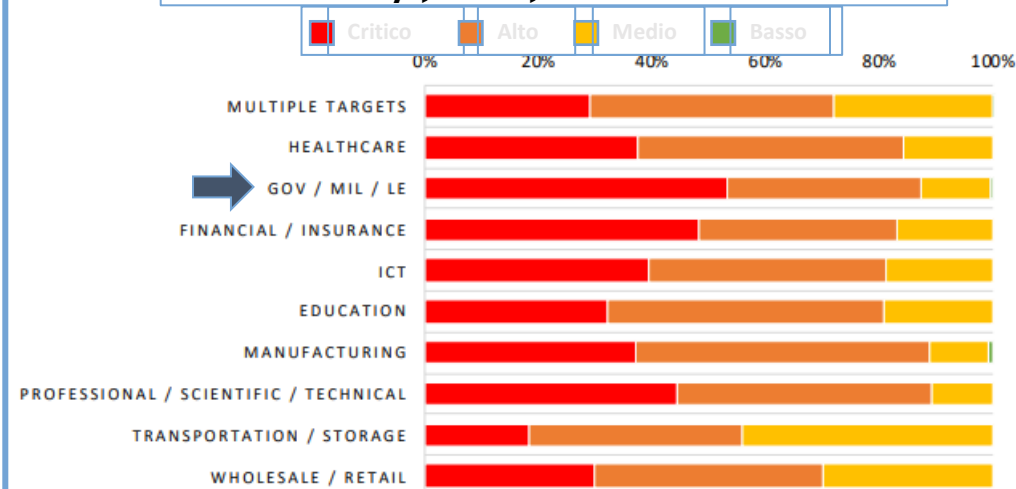
Gli attacchi condotti verso il settore pubblico sono caratterizzati da una Severity maggiore rispetto all'insieme di tutti gli attacchi: ben il 53,2% è infatti classificato come critico e il 40% è classificato alto, trend in linea con gli andamenti del 2022. Si conferma quindi che chi attacca il settore pubblico sia generalmente più preparato, motivato ed efficace nelle sue azioni, puntando a ottenere impatti decisamente più elevati della media.

Severity per Top 10 vittime 2022



Source: 2024 Clusit report on ICT Security in Italy.

Severity per Top 10 vittime 2023



Source: 2024 Clusit report on ICT Security in Italy.

Rischi Cyber – Intelligenza artificiale (IA)

60%

Preparazione contro minacce IA

Sono i leader della sicurezza informatica a livello globale (circa 1100 responsabili su 1800 intervistati), che dichiarano di temere che le proprie organizzazioni non siano adeguatamente preparate a difendersi da minacce e attacchi alimentati dall'intelligenza artificiale.

Fonte: Darktrace



Rischi dell'IA nella cyber security

1. Ottimizzazione degli attacchi informatici

Gli attacchi potrebbero raggiungere livelli di velocità e complessità senza precedenti, oltre a tecniche ottimizzate tramite l'uso dell'IA.

2. Rischi per la privacy

Possibili rischi per la privacy a causa della quantità di dati utilizzati dall'IA.

3. Manipolazione dei dati e data poisoning

I modelli di IA possono essere vulnerabili alla manipolazione dei dati, e quindi potrebbero produrre risultati inaspettati o dannosi.

4. Impersonificazione

Voci e immagini possono essere utilizzate per impersonare individui in truffe e attacchi deepfake.

Causa degli attacchi nella pubblica amministrazione italiana

I comuni italiani potrebbero essere un obiettivo attraente per gli attaccanti informatici, motivo per cui è importante identificare ed essere consapevoli dei potenziali scopi principali dietro alla minaccia.



Impatti finanziari, reputazionali e operativi

Il drammatico aumento e l'entità degli attacchi informatici ha comportato effetti sulle finanze, sulla reputazione e sull'operatività degli Enti e delle organizzazioni.

Ancora molti di essi sembrano impreparati a difendersi dal crimine informatico.

Si prevede che gli attacchi informatici siano costati al mondo 8 mila miliardi di dollari nel 2023 e che tale cifra salirà a 9,5 mila miliardi nel 2024 e a 10,5 mila miliardi nel 2025.



Fonte: Statista

IMPATTI FINANZIARI E REPUTAZIONALI

IMPATTO OPERATIVO

Impatti normativi

Tra gli effetti provocati da un potenziale incidente, può esservi anche il risvolto normativo, per cui è necessaria la consapevolezza anche dello scenario normativo al quale essere conformi.



*Fonte:
<https://www.garanteprivacy.it/>

Scenario normativo (I/III)

Negli ultimi anni le istituzioni a livello sia nazionale sia in ambito europeo hanno iniziato a fornire **indicazioni** e **misure tecniche** stringenti atte ad indirizzare una **gestione corretta degli aspetti di sicurezza**.



Strategia Cloud
Italia

Italia Digitale 2026

Piano
Nazionale di
Ripresa e
Resilienza
«PNRR»

Quadro strategico nazionale per la sicurezza dello
spazio cibernetico

Piano nazionale per la protezione cibernetica e la
sicurezza informatica



Qualificazione dei Poli
Strategici Nazionali



L. 28 giugno 2024, n. 90,
«Legge sulla Cybersecurity»



Digital Europe
2021-2027



Piano triennale per l'informatica della PA 2024

Sicurezza Informatica

Adottare una governance della cybersecurity diffusa nella PA

Gestire i processi di approvvigionamento IT coerentemente con i requisiti di
sicurezza definiti

Gestione e mitigazione del rischio cyber

Potenziare le modalità di prevenzione e gestione degli incidenti informatici

Implementare attività strutturate di sensibilizzazione cyber del personale

Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA



AGID

Linee Guida AgID

Misure minime di sicurezza ICT

La sicurezza nel procurement ICT

Configurazione per adeguare la sicurezza del software

Sviluppo sicuro del codice

Adozione di un ciclo di sviluppo di software sicuro

Modellazione minacce e azione di mitigazione conformi ai principi del
Secure/Privacy by Design

Caratterizzazione dei sistemi cloud per la Pubblica Amministrazione



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Scenario normativo (II/III)

Di seguito, una Overview delle misure applicabili ai sensi della recente **Legge 28 giugno 2024, n. 90** «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» e del Decreto Legislativo **4 settembre 2024, n. 138** (recepimento della Direttiva NIS 2) alle **Pubbliche Amministrazioni**.

Legge 28 giugno 2024, n.90



Notifiche incidenti

- Integra gli obblighi già esistenti di notifica degli incidenti (24h);
- Introduce obblighi di segnalazione incidenti entro deadline specifiche (24h, 72h).



Approvvigionamento ICT

- Introduce l'obbligo di tenere in considerazione specifici elementi di cybersicurezza in caso di approvvigionamento ICT.



Riduzione vulnerabilità

- Introduce l'obbligo di implementare interventi risolutivi delle vulnerabilità individuate da ACN entro tempistiche prestabilite.

Struttura e referente Cyber Security



- Introduce l'obbligo di individuare una struttura incaricata di assicurare la sicurezza delle informazioni;
- Introduce l'obbligo di procedere alla nomina di un referente per la Cyber Security, responsabile della gestione e del governo delle tematiche relative alla sicurezza informatica e punto di contatto con ACN.



Robustezza soluzioni crittografiche

- Introduce l'obbligo di verificare se le soluzioni crittografiche in uso rispettano le imposizioni previste dal Garante e dall'ACN.

Decreto legislativo 4 settembre 2024, n. 138



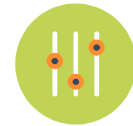
Notifiche incidenti

- Individua tempistiche specifiche per la segnalazione, da parte dei soggetti coinvolti, di incidenti di sicurezza significativi;
- Individua i CSIRT nazionali come enti destinatari delle segnalazioni.



Approvvigionamento ICT

- Permette agli Stati Membri di richiedere ai soggetti rilevanti di approvvigionarsi da Terze Parti certificate a livello europeo e l'esecuzione di Risk Assessment coordinati tra Stati con supporto di ENISA su sistemi, servizi e prodotti critici.



Misure di gestione del rischio

- Impone ai soggetti rilevanti di implementare misure tecniche, operative ed organizzative finalizzate alla gestione dei rischi per la sicurezza di sistemi informatici e di rete;
- Definisce gli ambiti minimi che devono essere coperti da tali misure.

Scenario normativo (III/III)

Di seguito, una comparazione che identifica i soggetti della Pubblica Amministrazione rilevanti ai sensi della recente Legge 28 giugno 2024, n. 90 e del Decreto legislativo 4 settembre 2024, n. 138 (NIS 2).

Soggetti della PA	Legge 28 giugno 2024, n. 90	Decreto legislativo 4 settembre 2024, n. 138
Pubbliche amministrazioni centrali	✓	✓ ALLEGATO III
Regioni e Province Autonome di Trento e Bolzano	✓	✓ ALLEGATO III
Città metropolitane	✓	✓ ALLEGATO III
Comuni con popolazione superiore a 100.000 abitanti	✓	✓ ALLEGATO III
Comuni capoluoghi di regione	✓	✓ ALLEGATO III
Società di trasporto pubblico Urbano e extraurbano	✓ Società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti e società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane	✓ Soggetti che forniscono servizi di trasporto pubblico locale ALLEGATO IV
Aziende Sanitarie Locali	✓	✓ ALLEGATO III
Società in house	✓ Servizi informatici, di trasporto ovvero di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali o di gestione dei rifiuti	✓ Società in house, società partecipate e società a controllo pubblico, come definite nel d. lgs. 19 agosto 2016, n. 175. ALLEGATO IV



Nell'Allegato III del Decreto legislativo 4 settembre 2024, n. 138 sono previsti anche Altri soggetti pubblici come Enti di regolazione dell'attività economica, Enti produttori di servizi economici, Enti a struttura associativa, Enti produttori di servizi assistenziali, ricreativi e culturali, Enti e Istituzioni di ricerca e gli Istituti zooprofilattici sperimentali.

- ▶ Scenari evolutivi del rischio Cyber per le Pubbliche Amministrazioni
- ▶ Come proteggersi nel contesto attuale
- ▶ Il ruolo dell' RTD

NIST 2.0 – Cyber Security Framework - Overview

Il **NIST** (National Institute of Standards and Technology) fornisce **linee guida e best practice per la cyber security**, che rappresentano uno strumento di **difesa essenziale** contro le **minacce informatiche**.

Le risorse offerte dal NIST includono:

- Le pubblicazioni specializzate del NIST, come le Guide SP (Special Publication), che forniscono raccomandazioni tecniche dettagliate per l'implementazione di misure di sicurezza, ad esempio sul controllo degli accessi, la gestione delle identità e la gestione delle vulnerabilità etc.
- I test e le misurazioni, che consentono di valutare l'efficacia delle soluzioni di sicurezza implementate, contribuendo a identificare eventuali debolezze e vulnerabilità.
- I programmi di certificazione e di conformità, che garantiscono un livello di sicurezza e di protezione adeguato per le organizzazioni e i loro sistemi.

L'adozione delle linee guida e delle best practice del NIST consente alle organizzazioni di migliorare la loro postura di sicurezza, proteggendo i dati e i sistemi da minacce cyber sempre più sofisticate e mutevoli.



NIST 2.0 – Cyber Security Framework – Funzioni core



Tutte le infrastrutture critiche sono vulnerabili, analizzare e reagire rapidamente permette una risposta efficace agli attacchi



Creare consapevolezza e protezione contro i rischi del ransomware, supportando al contempo lo sviluppo del business



Nessuna azienda è esente da potenziali rischi critici, ma tutti possono sviluppare una resilienza cyber

Governare

Stabilire e monitorare una strategia e le politiche di gestione del rischio di cybersecurity

Identificare

Costruire una struttura di gestione per il rischio di sicurezza informatica per sistemi, persone e dati

Proteggere

Implementare misure di sicurezza dei sistemi appropriate per proteggere i servizi critici

Rilevare

Rilevare potenziali eventi di sicurezza informatica e l'esistenza di Threat Actor

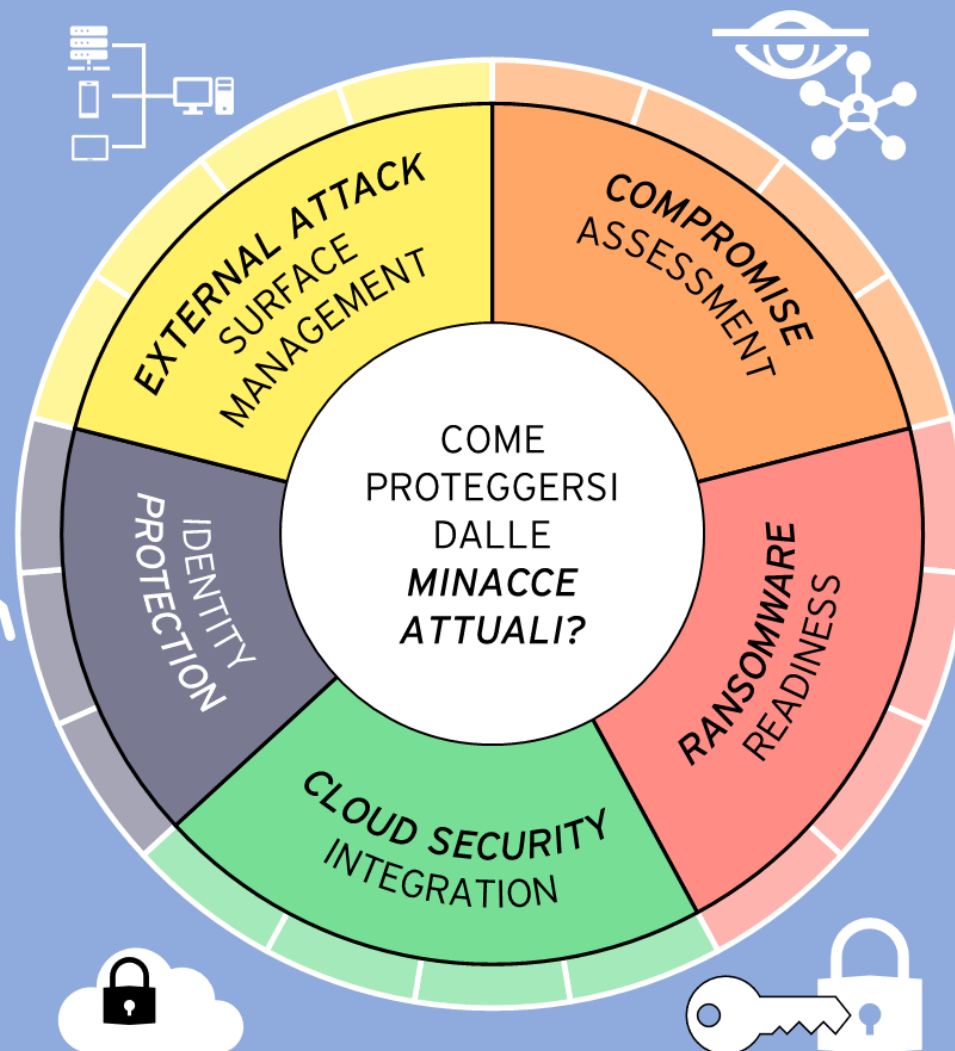
Rispondere

Rispondere ad un incidente di sicurezza informatica

Riparare

Ripristinare le normalità di business e perfezionare le capacità di resilienza informatica

L'evoluzione delle Strategie di Risposta



Essere coscienti del proprio grado di esposizione ed avere visibilità sugli asset esposti, identificando la superficie di attacco esterna dell'organizzazione

Proteggere le identità significa impedire agli attaccanti di sfruttare uno dei vettori più comuni nello scenario attuale

Gestire efficacemente i rischi informatici dell'ecosistema cloud e proteggere il percorso di trasformazione di un'azienda

Svolgere azioni di monitoraggio approfondite, al fine di scovare indicatori di compromissione che potrebbero essere passati inosservati

Il ransomware rappresenta una delle minacce più concrete nello scenario attuale, contro la quale si può fare solamente prevenzione

Cybersecurity Roadmap (I/II)

Al fine di poter apportare **innovazione** nel fornire i servizi ai cittadini e **rispondere in maniera rapida ed efficace ai cambiamenti** imposti anche dall'ambiente esterno, risulta opportuno porsi come obiettivo l'implementazione di **soluzioni più efficaci in ambito sicurezza delle informazioni e protezione dei dati**. A questo scopo potranno essere individuati gli eventuali gap presenti e intraprendere delle nuove iniziative volte alla protezione contro i crimini informatici.



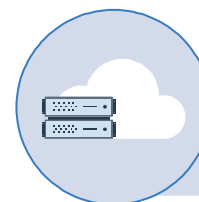
ASSESSMENT & GAP ANALYSIS

Per stabilire il livello di maturità dell'Ente e predisporre una roadmap di iniziative.



INIZIATIVE DI SECURITY GOVERNANCE

Per mitigare i rischi inerenti all'organizzazione e ai servizi erogati, così come per contrastare eventi di cybercrime.



INIZIATIVE IN AMBITO TECHNOLOGY

Per implementare servizi con carattere di innovazione tecnologica.

Cybersecurity Roadmap (II/II)

Di seguito si propone una breve sintesi di ciascun ambito di lavoro.

Assessment & Gap Analysis

- Esecuzione di un Cyber Maturity Assessment sulla base del framework nazionale per la cyber sicurezza e la data protection per comprendere lo stato attuale della postura cyber
- Consolidamento del piano strategico delle iniziative tattiche
- Esecuzione di un assessment di ricognizione per valutare la nuova postura cyber

Iniziative di Security Governance

- Definizione di una metodologia di Analisi del rischio cyber ed esecuzione di risk assessment sulla base della metodologia definita
- Revisione dei processi riguardanti gli aspetti di gestione della sicurezza delle informazioni
- Definizione piano di risposta agli incidenti e piano di ripartenza dei servizi
- Definizione piano di continuità operativa ICT

Iniziative in ambito Technology

- Funzionalità di protezione SIEM+SOC e threat intelligence
- Difesa perimetrale da realizzare con nuovi dispositivi di sicurezza denominati NGFW e WAF
- Attivazione progressiva dell'autenticazione a doppio fattore (2FA)
- Protezioni evolute sul cloud

Avvisi pubblici per il supporto alle Pubbliche Amministrazioni

L'Agenzia per la Cybersicurezza Nazionale (ACN) ha promosso diverse iniziative per supportare le Pubbliche Amministrazioni nel potenziamento della propria resilienza cyber.

Gli Enti possono usufruire delle Convenzioni Consip, atte a supportare la Pubblica Amministrazione nell'implementazione delle progettualità in ambito cyber.

Avvisi Pubblici

- Avviso n. 3/2022 – potenziamento resilienza cyber
- Avviso n. 6/2023 - attivazione/potenziamento di CSIRT Regionali
- Avviso n. 8/2024 – rafforzamento delle infrastrutture e dei servizi digitali italiani, e miglioramento delle competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza



Per implementare servizi con carattere di innovazione tecnologica.

Finanziamenti dal Governo

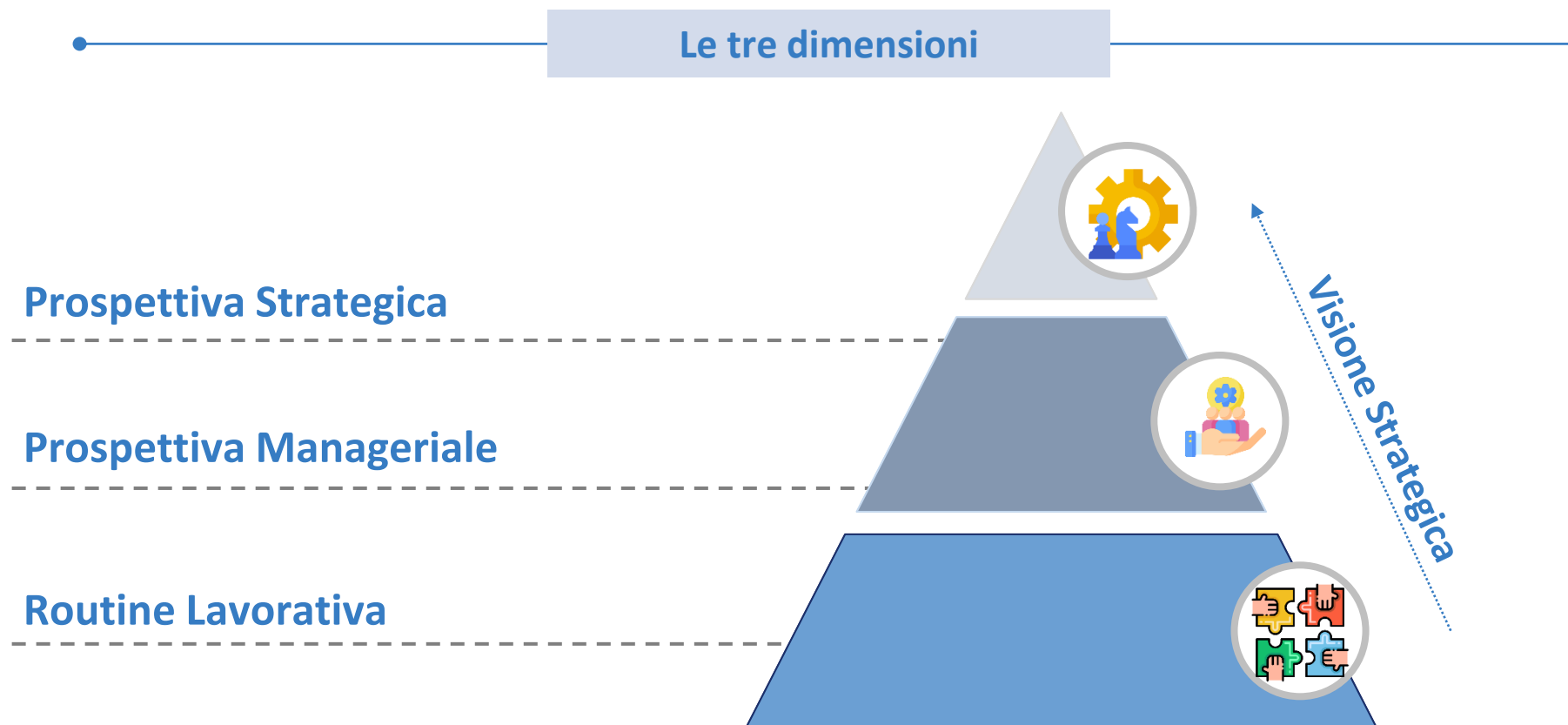
- Misura #55 del piano di implementazione della Strategia Nazionale di Cybersicurezza, per la promozione della digitalizzazione, innovazione, e rafforzamento della sicurezza nella PA



- ▶ Scenari evolutivi del rischio Cyber per le Pubbliche Amministrazioni
- ▶ Come proteggersi nel contesto attuale
- ▶ Il ruolo dell' RTD

Il ruolo dell' RTD – Le tre dimensioni

L'impegno dell' RTD è decisivo nel garantire la Sicurezza Informatica e l'affidabilità dei servizi offerti dall'Ente alla comunità.



Il ruolo dell' RTD – Prospettiva strategica



Prospettiva Strategica

La sicurezza informatica non può essere lasciata da parte.
Il successo delle attività è sempre più legato alla digitalizzazione e alla sua protezione.



La **sicurezza informatica** dovrebbe essere considerata come un rischio prioritario per l'Ente



L'impegno per la **sicurezza informatica** è importante



Occorre svolgere un ruolo attivo per **l'implementazione delle strategie di sicurezza informatica** dell'Ente

Il ruolo dell' RTD – Routine Lavorativa



Prospettiva Manageriale

È importante che tutti siano consapevoli dell'importanza della sicurezza informatica per un Ente guidato dal digitale.

La dirigenza dovrebbe:



Diffondere la rilevanza delle **questioni di sicurezza informatica** nell'Ente



Garantire che i nuovi servizi al cittadino che sottendono una componente tecnologica siano sviluppati secondo un corretto approccio di **Security By Design** ed in linea con i regolamenti vigenti



Assicurarsi che lo staff **collabori** in modo proattivo **alle iniziative di formazione sulla sicurezza informatica**

Il ruolo dell' RTD – Routine Lavorativa



Routine Lavorativa

La Dirigenza potrebbe essere l'obiettivo principale degli attacchi informatici. Pertanto, più di ogni altro utente, è necessario che applichi le migliori pratiche di sicurezza nelle attività quotidiane:



Password management



Sicurezza delle e-mail



Aggiornamento dei device



Sicurezza della navigazione web



Uso responsabile degli asset dell'Ente



Queste semplici misure di sicurezza sono essenziali per l'Ente per prevenire ad esempio il rischio di danni finanziari, l'interruzione di servizi di pubblica utilità, il furto di dati sensibili dei cittadini ed il pubblico spionaggio.

Il ruolo dell' RTD - Awareness

La responsabilizzazione, consapevolezza e sensibilizzazione dell' RTD sui temi di cyber security viene rafforzata anche dalle disposizioni presenti all'interno della Legge 28 giugno 2024, n. 90 e del Decreto legislativo 4 settembre 2024, n. 138 (NIS 2) :

Direttiva NIS 2



Management Bodies

*“Gli Stati membri provvedono affinché i **membri dell'organo di gestione** dei soggetti essenziali e importanti siano tenuti a **seguire una formazione** e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cybersicurezza e il loro impatto sui servizi offerti dal soggetto”.*



Legge Cyber Sicurezza



Struttura aziendale cyber

Individuazione, se non già presente, di una struttura aziendale cyber che provveda:

- ▶ Sviluppo politiche e procedure di sicurezza delle informazioni;
- ▶ Definizione ruoli ed organizzazione sistema per la sicurezza delle informazioni;
- ▶ Produzione e aggiornamento piano programmatico per la sicurezza di dati, sistemi e infrastrutture;
- ▶ Potenziamento delle capacità di gestione degli incidenti;
- ▶ Adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'ACN;
- ▶ Monitoraggio e valutazione delle minacce e vulnerabilità dei sistemi.



Referente per la cybersicurezza:

*Individuazione, all'interno della struttura aziendale cyber, di un referente per la cybersicurezza, **dotato di specifiche e comprovate professionalità e competenze in materia di cybersicurezza.***

Il ruolo dell' RTD – Aumentare il livello di Awareness nei dipendenti

Attraverso l'awareness, inoltre, i dipendenti possono diventare un anello fondamentale nella catena di difesa contro le minacce cyber, contribuendo a identificare e prevenire gli attacchi, proteggendo così le organizzazioni e i loro dati sensibili.

Sensibilizzazione sul phishing

Educare gli utenti a riconoscere e evitare email sospette, link fraudolenti e richieste di informazioni personali o di accesso a siti non affidabili.

Gestione delle password

Promuovere l'uso di password robuste e uniche per ciascun account, incoraggiando la pratica di cambiarle periodicamente e di non condividerle con altre persone.

Navigazione sicura

Insegnare agli utenti a verificare la sicurezza dei siti web, utilizzare connessioni crittografate (HTTPS), evitare download da fonti non affidabili e aggiornare costantemente i software per coprire le vulnerabilità.

Dispositivi mobili

Informare gli utenti sui rischi di installare applicazioni non ufficiali, collegarsi a reti Wi-Fi pubbliche non sicure e sulle pratiche per proteggere i dispositivi mobili con password o biometria.

Protezione dei dati

Educare gli utenti sull'importanza di effettuare regolarmente il backup dei dati, evitare l'invio di informazioni sensibili tramite canali non sicuri e utilizzare strumenti di crittografia per proteggere i file sensibili.

Policy

Garantire che gli utenti siano informati sulle politiche e le procedure interne relative alla sicurezza informatica, come l'uso dei dispositivi aziendali, l'accesso alle risorse sensibili e la segnalazione degli incidenti di sicurezza.