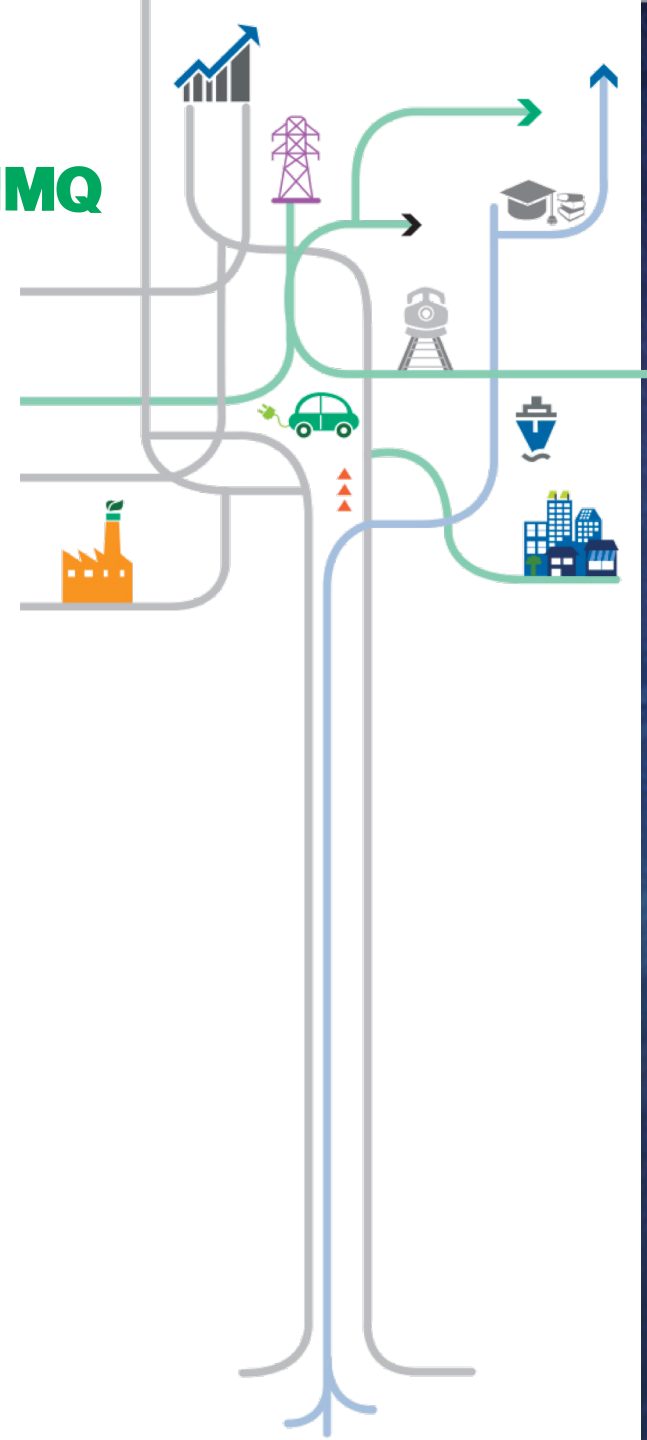
ANIE FEDERAZIONE
Technologies for our future

CONFINDUSTRIA

Associazione IMQ



ARTIFICIAL INTELLIGENCE
E
MACHINE LEARNING
APPLICATI ALLA CYBERSECURITY

Giulio Iucci
Presidente ANIE Sicurezza

IL NUOVO SCENARIO

LA SICUREZZA CYBER

Tutti gli apparati ed i singoli sottosistemi sono, costantemente ed in tempo reale, connessi tra loro ed a loro volta **connessi con gli utenti**, come parte di un unico grande **"organismo"** che può essere "attaccato" non, come in passato, solo direttamente nelle sue "infrastrutture critiche", ma violando qualsiasi suo componente anche apparentemente residuale che faccia poi da "bridge" per entrare nel cuore dell'obiettivo principale.

È necessario quindi conoscere e comprendere quali siano le criticità portate dalla convergenza tecnologica con relativa connessione globale, utilizzarne tutti i vantaggi, minimizzando i rischi che, in ogni caso, non potranno essere azzerati, ma mitigati adottando le **misure tecnologiche, architetturali e procedurali coerenti e proporzionate al contesto ed al bene da proteggere**, sia esso materiale, immateriale o umano.

LE CRITICITÀ

TUTTO È CENTRALE E PRIMARIO, NON ESISTE LA PERIFERIA ED IL RESIDUALE.

Il concetto di sicurezza fisica che prevede sistemi più critici e sensibili, deve essere rivisto in un nuovo paradigma: **tutti i sistemi connessi**, anche residuali, devono essere considerati **potenzialmente critici e sensibili.**

Occorre innanzitutto determinare le **nuove vulnerabilità** introdotte e poi proteggere ciascun elemento che fa parte del sistema e i canali di comunicazione tra essi.

In ogni caso, le regole base per misurare **il rischio**, rimangono invariate ed utilizzano gli stessi parametri macro di riferimento per definire **la probabilità** e **l'entità** di ciò che può accadere.

E' quindi sempre importante effettuare con chiarezza **un'analisi di contesto** e definire in dettaglio quali siano **i beni da proteggere** e gli eventuali **offender**.

Tutto ciò anche per dare **equilibrio** e **sostenibilità** ad un'azione di **protezione** e **prevenzione** che sia **coerente** con i reali rischi e conseguenze di un'azione criminosa.

AGENTI INTELLIGENTI

INTERNET OF THINGS – ARTIFICIAL INTELLIGENCE – MACHINE LEARNING

Internet Of Things – È la rete di apparecchiature, sensori e dispositivi, diversi dai computer, connessi a Internet: in generale qualunque dispositivo elettronico equipaggiato con un software che gli permetta di scambiare dati con altri oggetti connessi.

Artificial Intelligence – È la capacità di un sistema hardware di risolvere problemi o svolgere compiti e attività tipici della mente e dell'abilità umane. Si occupa di realizzare macchine (hardware e software) in grado di "agire" autonomamente (risolvere problemi, compiere azioni, prendere decisioni, ecc.).

Machine Learning – È un sistema in grado di apprendere autonomamente e di imparare dai propri errori. Si basa su algoritmi che analizzano dati: imparando da essi possono prendere decisioni e condurre previsioni. Il processo di apprendimento avviene attraverso l'analisi di big data.

LA SICUREZZA INFORMATICA E L'INTELLIGENZA ARTIFICIALE

RAFFORZAMENTO DELLA SICUREZZA INFORMATICA CON L'**AI** IMPERATIVO PER LE ORGANIZZAZIONI

L'intelligenza artificiale (AI) e il machine learning (ML) sono già state implementate in una moltitudine di applicazioni per aumentare la produttività, migliorare le vendite o le performance. Tuttavia, un'applicazione (AI) fondamentale, anche se spesso trascurata, è volta a migliorare la protezione contro gli attacchi cibernetici.

Le organizzazioni contano sull'**IA** per aiutare gli analisti della sicurezza informatica sopraffatti dai continui attacchi. Il 69% delle organizzazioni ritiene che l'**IA** sarà fondamentale per rispondere in maniera adeguata agli attacchi cibernetici e a identificare le minacce critiche.

LO SCENARIO

PER RENDERE LA SICUREZZA INFORMATICA PIU' EFFICACE NELLA RIDUZIONE DEI RISCHI LE ORGANIZZAZIONI RICERCANO SISTEMI DI IA E MACHINE LEARNING.

Se utilizzata in combinazione con i metodi tradizionali, l'**IA** è un potente strumento di protezione contro gli attacchi alla sicurezza informatica.

Nell'era di Internet, con la capacità degli hacker di commettere furti o causare danni a distanza, proteggere i propri beni e i propri dati, è diventato sempre più difficile, con numeri che rischiano di andare fuori controllo.

Solo Cisco ha riferito che, per conto dei propri clienti, nel 2018 ha bloccato sette trilioni di minacce.

Alcune organizzazioni si stanno rivolgendo all'**IA**, non tanto per risolvere completamente i loro problemi futuri, quanto piuttosto per puntellare le loro difese attuali.

LO SCENARIO

LE ORGANIZZAZIONI SI STANNO RIVOLGENDO ALL'IA MENTRE LE MINACCE TRAVOLGONO I CYBERANALISTI

Per comprendere meglio come affrontare le sfide della sicurezza informatica, è stata condotta una importante indagine su 850 dirigenti senior di: IT Information Security, Cybersecurity e IT Operations in sette settori in 10 paesi, da cui è emerso:

- che il traffico globale di affari su Internet si triplicherà entro il 2023
- che l'aumento degli attacchi informatici che possono compromettere le operazioni critiche all'interno di un'azienda richiede capacità talmente avanzate che possono essere fornite solo attraverso l'uso di Sistemi basati sull'**IA**
- che con minacce così crescenti, le organizzazioni hanno bisogno di correre ai ripari con sistemi efficaci e tempestivi

LO SCENARIO

UTILIZZO DELL'**IA** NELLA CYBERSECURITY STA AVENDO UN AVANZAMENTO ESPONENZIALE

La maggior parte delle organizzazioni dichiara che l'**IA** abbassa i costi di individuazione, e la risposta alle violazioni, del 12% in media.

La nuova frontiera della sicurezza informatica, in risposta ai continui attacchi, non può che essere l'IA, perché è con l'IA che gli hacker sferrano i loro attacchi.

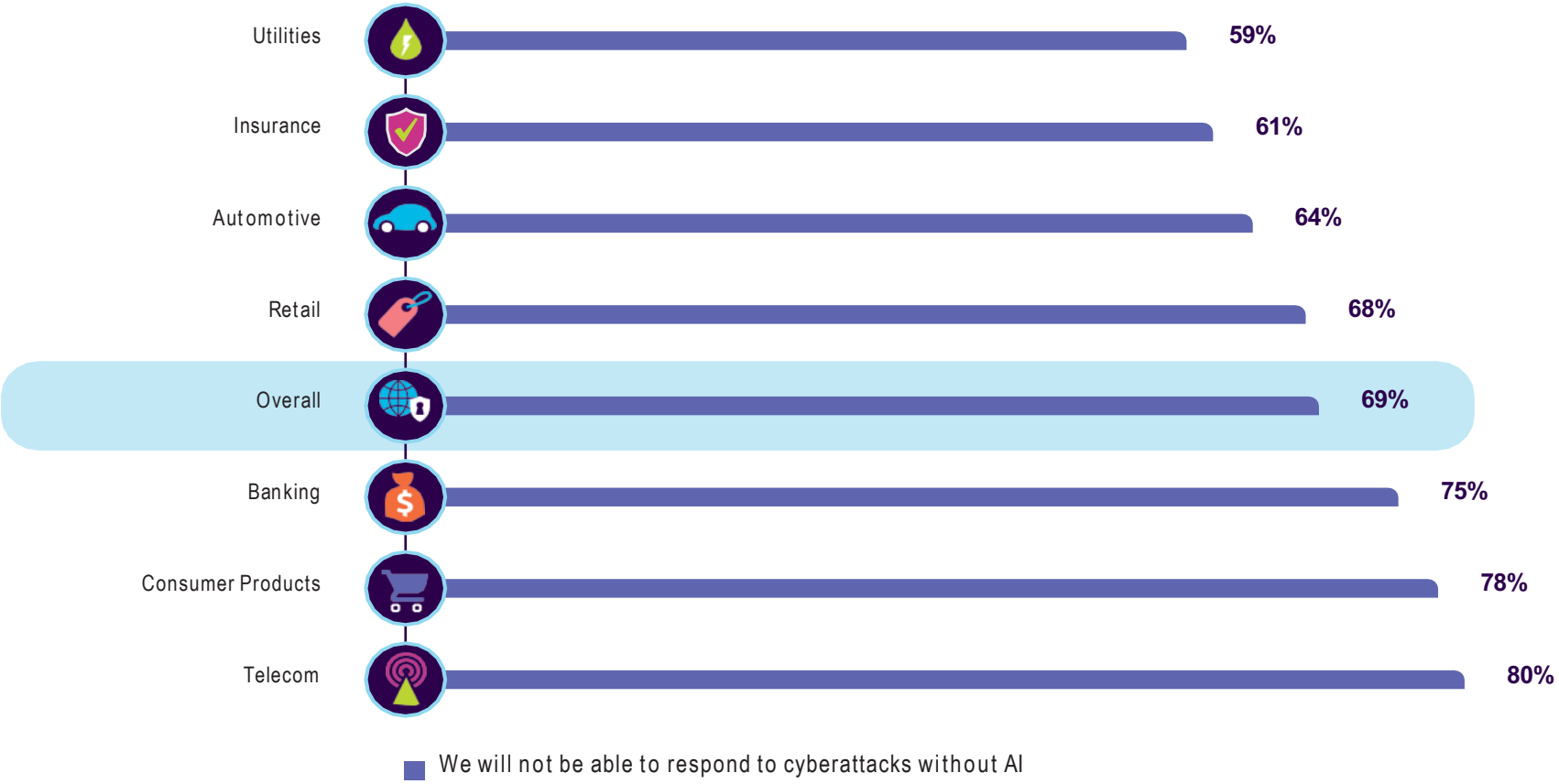
Quasi un'organizzazione su cinque ha usato l'IA prima del 2019. Tuttavia, l'adozione è destinata a salire alle stelle, con due organizzazioni su tre che prevedono di utilizzarla nell'immediato.

Tre Responsabili IT su quattro sostengono che l'uso dell'IA ha permesso alla loro organizzazione di rispondere più velocemente alle violazioni.

Tre aziende su cinque affermano che l'utilizzo dell'IA migliora la precisione e l'efficienza dei cyber analisti.

ALCUNI DATI

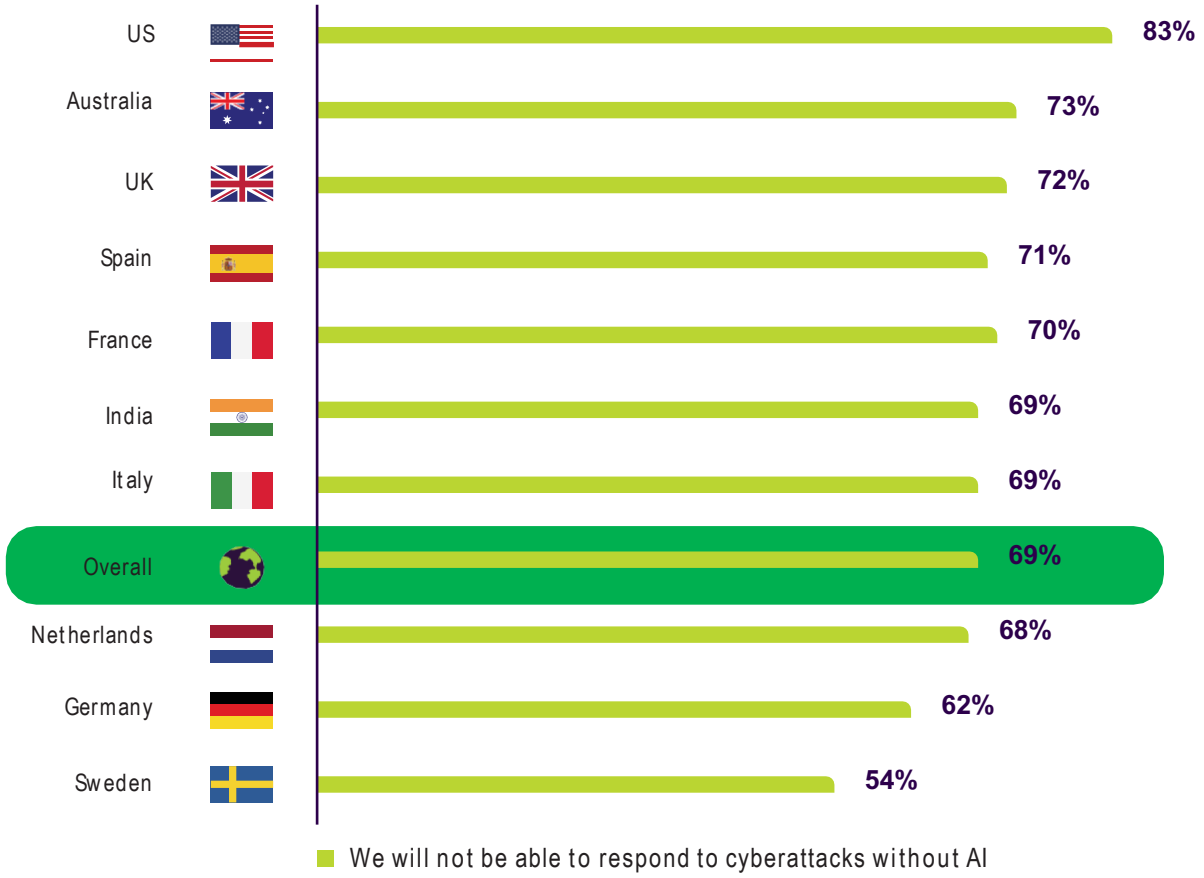
IL 69% DELLE ORGANIZZAZIONI CONTANO SULL'**IA** PER AIUTARE A IDENTIFICARE LE MINACCE E CONTRASTARE GLI ATTACCHI



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

ALCUNI DATI

IL 69% DELLE ORGANIZZAZIONI CONTANO SULL'**IA** PER AIUTARE A IDENTIFICARE LE MINACCE E CONTRASTARE GLI ATTACCHI

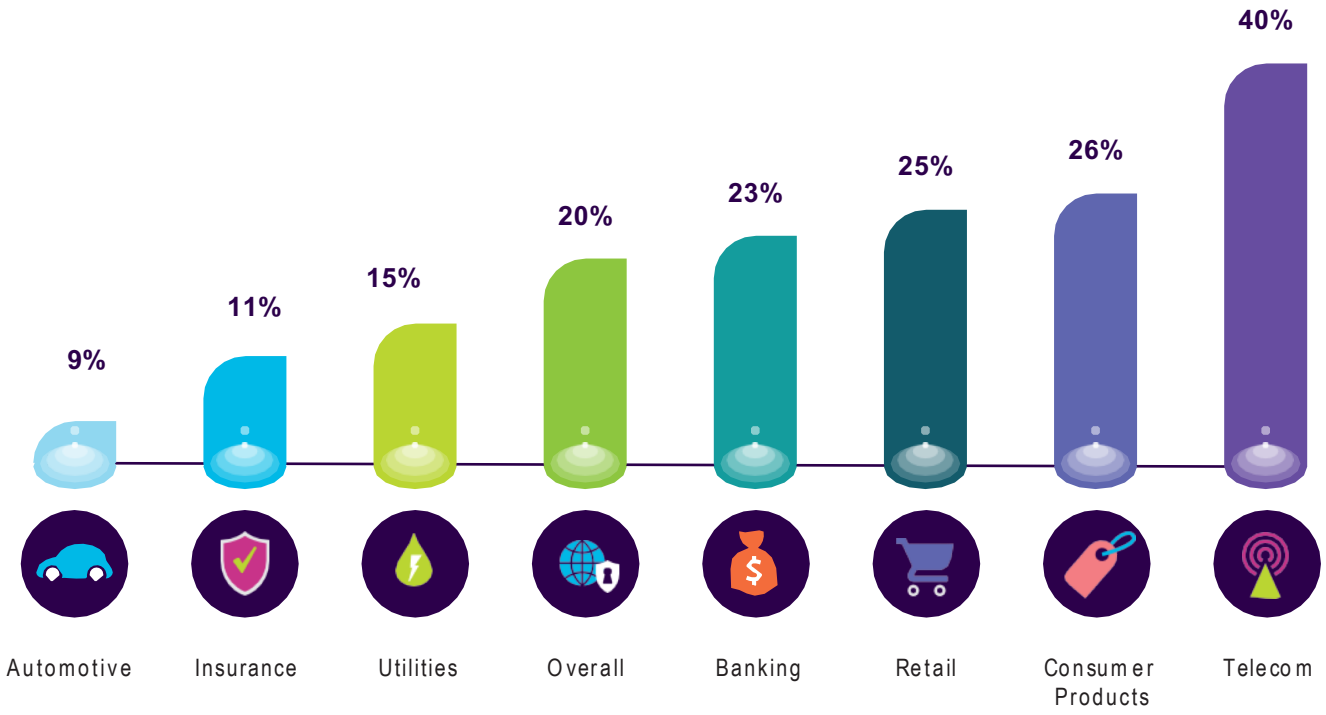


Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

ALCUNI DATI

VIOLAZIONI DIFFUSE DELLA SICUREZZA INFORMATICA

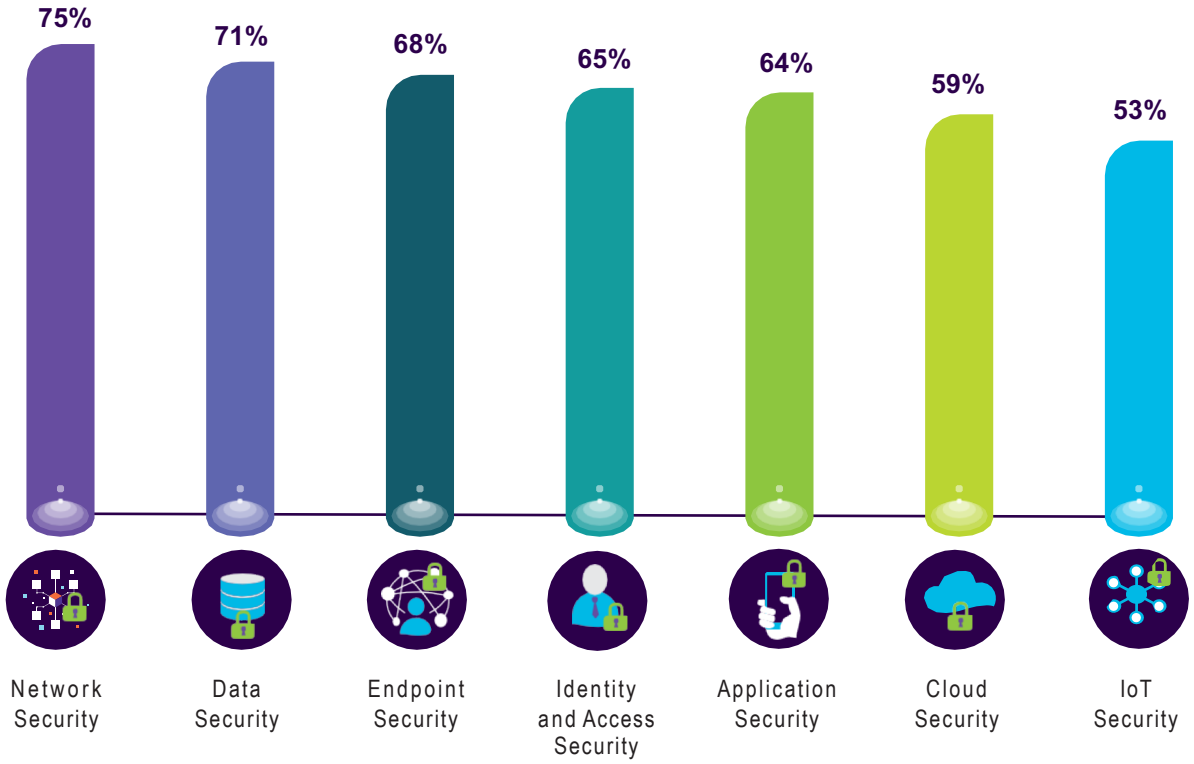
L'industria delle telecomunicazioni ha la più alta incidenza di attacchi con perdite superiori a 50 milioni di dollari



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

ALCUNI DATI

LA SICUREZZA DELLA RETE HA LA PIÙ ALTA DIFFUSIONE DI IA NELLA SICUREZZA INFORMATICA



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

DISEGNARE LE PROCEDURE

Creare la piattaforma dati

Identificare le fonti dei dati e creare piattaforme di dati per rendere operativa l'**IA**

Collaborare

Collaborare all'esterno per migliorare l'intelligence sulle minacce

Creare il Team Cyber-analisti

Addestrare i cyber- analisti ad essere pronti per l'**IA**

Selezionare i casi d'uso ad alto impatto

Selezionare il giusto set di casi d'uso per accelerare e massimizzare i benefici

Implementare la SOAR

Sicurezza, Orchestrazione, Automazione e Risposta rendono l'uso dell'**IA** più efficace e di impatto consentendo una risposta rapida alle minacce rilevate

Installare la governance

Chiarire nei dettagli la governance per l'**IA** per fornire miglioramenti a lungo termine in modo trasparente ed etico

RIASSUMENDO

Un panorama IT *(Information Technology)* / OT *(Operational Technology)* in costante evoluzione e superfici di attacco in continua espansione portano a sfide di sicurezza sempre più complesse. Molte aziende hanno già iniziato a studiare come l'**IA** nella cybersecurity possa contribuire a mitigare questi rischi: i tassi di adozione dell'**IA** nella sicurezza informatica sono in aumento.

Per le aziende che non hanno ancora iniziato a utilizzare l'**IA** nella cybersecurity – così come per le aziende che la stanno già utilizzando - ci sono una serie di passaggi critici per realizzare il potenziale di **IA** nella cybersecurity.

Le organizzazioni devono costruire una roadmap che affronti le infrastrutture, i sistemi di dati, i paesaggi applicativi, le lacune di competenze, le migliori pratiche, la governance e la selezione e l'implementazione dei casi d'uso.

L'adozione di queste azioni consentirà alle organizzazioni di evitare perdite inutili e, in alcuni casi, anche di aggiungere ulteriori fonti di reddito.

LA SICUREZZA DEI SISTEMI

Convenzionalmente si indicano tre caratteristiche fondamentali per la sicurezza dei sistemi: ***riservatezza, integrità* e *disponibilità*.**

Da un contesto di ***computer security*** a uno di ***network security***, anche le proprietà di ***autenticità*** e ***non ripudiabilità*** assumono un ruolo essenziale.

Possono quindi essere definite cinque caratteristiche fondamentali:

01 **Riservatezza**

02 **Integrità**

03 **Autenticità**

04 **Non-ripudio**

05 **Disponibilità**

LA SICUREZZA DEI SISTEMI

01

Riservatezza

Le informazioni/dati memorizzati in un sistema o scambiate tra due entità devono essere **protette da letture non autorizzate** ed essere accessibili solo ai soggetti ed ai processi che ne hanno diritto, in base alle policy definite nel Sistema.
La *segretezza* o *confidenzialità*, si ottiene soprattutto mediante tecniche crittografiche.

LA SICUREZZA DEI SISTEMI

02

Integrità

Le informazioni/dati memorizzati in un sistema o scambiate tra due entità devono essere **protette da modifiche non autorizzate** (alterazione, cancellazione o aggiunta).
L'integrità può essere garantita da meccanismi di *checksum (sequenza di bit utilizzata per verificare l'integrità di un dato)*, da tecniche crittografiche (es. firma digitale, meccanismi di controllo dell'accesso ai dati).

Giulio Iucci

LA SICUREZZA DEI SISTEMI

03

Autenticità

Identificazione certa della provenienza di una informazione/dato: **verificare l'identità dell'origine**. Le informazioni sul mittente devono essere garantite da tecniche crittografiche.
Per l'**autenticazione,** al fine di ottenere l'accesso ad un servizio, è necessario dimostrare preliminarmente la propria identità presso il sistema che ospita tale servizio.

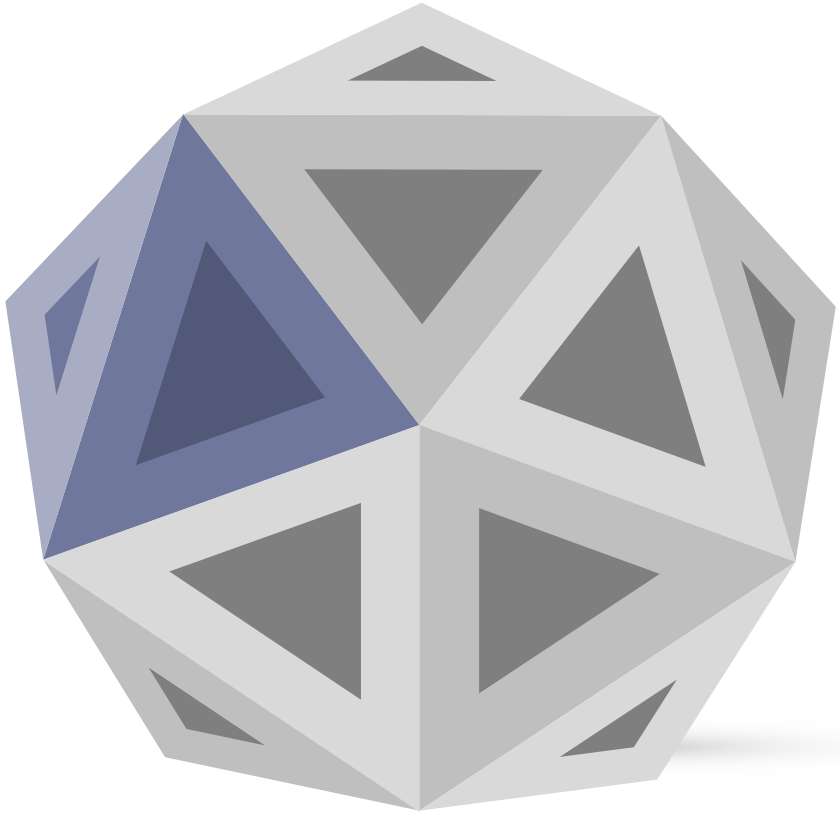
LA SICUREZZA DEI SISTEMI

04

Non - Ripudiabilità

Chi genera ed invia un dato **non deve poter negare** successivamente di averlo generato ed inviato, né deve poterne negare il contenuto. Allo stesso modo, chi riceve un dato, non deve poter negare di averlo ricevuto, né deve poterne negare il contenuto. Nell'ICT la non ripudiabilità è ottenuta attraverso tecniche crittografiche.

LA SICUREZZA DEI SISTEMI



05

Disponibilità

Risorse, servizi e dati di un sistema devono essere **sempre accessibili** agli utenti legittimi. I sistemi devono risultare funzionanti con il livello di prestazioni prestabilito e nessuno deve essere in grado di minacciare il loro funzionamento regolare. Es. attacchi denial of service *(malfunzionamento dovuto ad attacco informatico in cui si fanno esaurire le risorse di un sistema che fornisce un servizio)*, ma anche disastri naturali (cali di tensione, guasti all'hardware).

TIPOLOGIE DI ATTACCHI

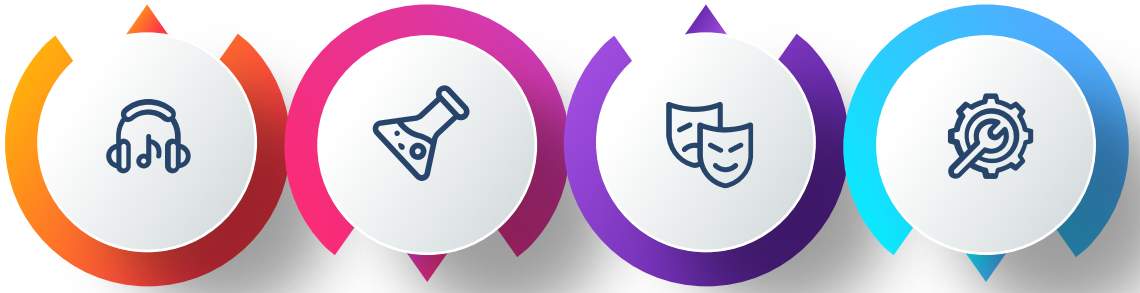
Di seguito vengono forniti alcuni semplici esempi dei più ricorrenti **attacchi** che costituiscono una *violazione delle proprietà di sicurezza* sopra descritte

INTERCETTAZIONI

Violano la proprietà di riservatezza dell'informazione

FALSIFICAZIONI

Violano i requisiti di autenticità e di non-ripudio



ALTERAZIONI

Violano il requisito di integrità

SABOTAGGI O INTERRUZIONI

Minacciano la disponibilità del sistema

Nella Tabella seguente sono elencate le caratteristiche delle principali categorie di attacco.

ANIE FEDERAZIONE
Technologies for our future
CONFINDUSTRIA

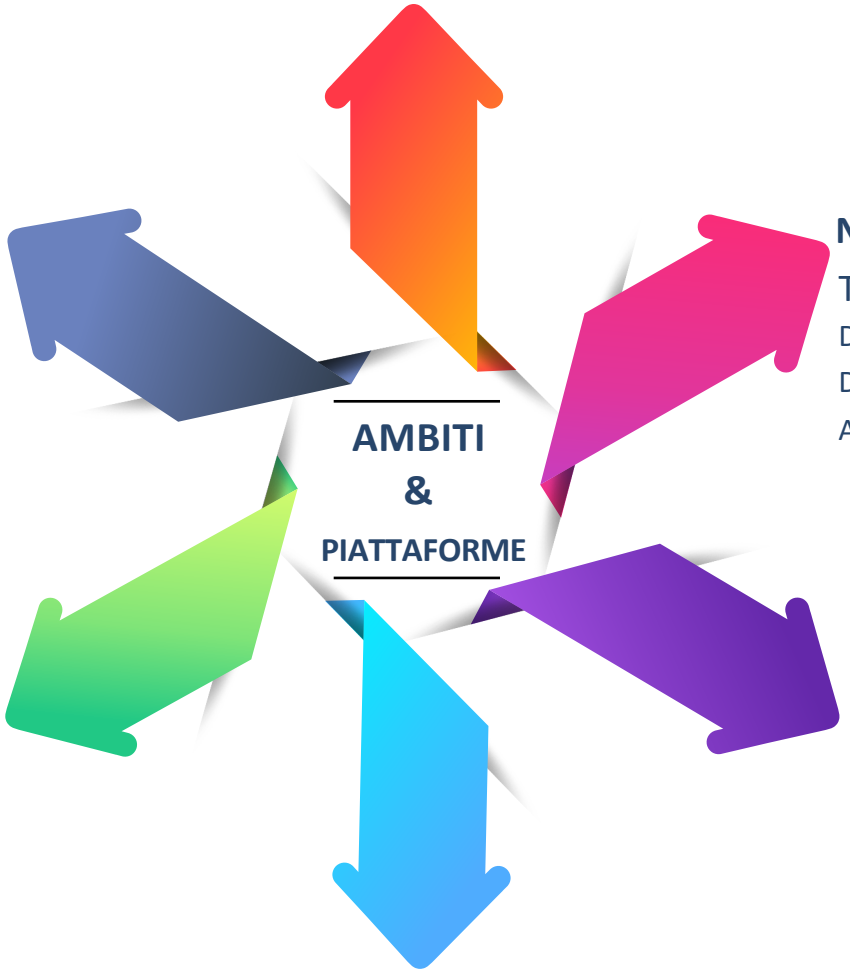
Associazione IMQ

IT (FIREWALL)

PREROGATIVE DI ACCESSO / VALIDAZIONE - SICUREZZA PORTE DI ACCESSO AI SINGOLI SISTEMI

RESILIENZA (BACKUP)

PROTEZIONE E SEGMENTAZIONE
RESILIENZA / BCRS
VIRTUALIZZAZIONE / BACKUP



NETWORK / LINK

TRASMISSIONI SICURE / ALGORITMI DI CRITTOGRAFIA / AUTENTICAZIONE DATI - PROTEZIONE E RICHIESTA ACCESSO RETE DA REMOTO

PROCEDURE

LOGICHE DI ACCREDITAMENTO, DI ACCESSO E DI INTERVENTO.
AGGIORNAMENTI E PENETRATION TEST PERIODICI

ARCHITETTURA DI SISTEMA

SUDDIVISIONE IN ZONE (FISICHE E LOGICHE) ISOLATE TRA LORO E, OVE POSSIBILE, CON IL MONDO ESTERNO

SISTEMI DI MONITORAGGIO

ALLARMI/ANOMALIE - SUPERVISIONE E MONITORAGGIO PSIM - DATA ANALYTICS ARTIFICIAL INTELLIGENCE (PREDITTIVITÀ)

IL TREND DELLA CERTIFICAZIONE

CYBER SECURITY ACT

I LIVELLI DI SICUREZZA:

- FONDAMENTALE (Base) – Autocertificazione volontaria
- SOSTANZIALE – Verifica/monitoraggio da parte di un ente terzo
- ALTO (Servizi essenziali: Energia/Trasporto/Banche/Infrastrutture Sanitarie, Digitali, ecc.) Ente terzo esegue dei test (audit)

ATTIVITÀ:

- RISK ANALISYS
- RISK ASSESMENT
- SCHEMI DI CERTIFICAZIONE (Prodotti – Processi – Servizi)

SCHEMI DI CERTIFICAZIONE:

- Prodotto
- Processo (azienda costruttrice)
- Procedure (back-up, penetration test, ecc.)
- Architettura di sistema
- Rete e connessioni (interne – esterne)
- Resilienza (capacità di resistere) intervenire – mitigare – ripristinare

RIASSUMENDO

ATTIVAZIONE DI **PIANI E PROCEDURE** CHE CONSENTANO UN ELEVATO LIVELLO DI PROTEZIONE, PREVENZIONE E MITIGAZIONE DAI RISCHI DI ATTACCO: ES. PENETRATION TEST, BACK-UP, VIRTUALIZZAZIONE , RESILIENZA, ECC.

LA DIGITALIZZAZIONE PORTA ALLA **CONVERGENZA**: SECURITY / SAFETY / AUTOMATION

VALORE E QUALITÀ. **CERTIFICARE E CONTROLLARE** TUTTA LA FILIERA: RISK ANALYSIS, PROGETTAZIONE, SCELTA PRODOTTI (HW / SW), INSTALLAZIONE, COLLAUDO E MANUTENZIONE, TEST PERIODICI, PROCEDURE OPERATIVE DI INTERVENTO

SISTEMI DIVERSI INTERAMENTE **INTEROPERABILI**, CONESSI TRA LORO E CON L'ESTERNO

È NECESSARIA UNA **PROGETTAZIONE SISTEMICA** GLOBALE CHE SEGUA FERREE REGOLE ARCHITETTURALI, PROCEDURALI, NORMATIVE E TECNOLOGICHE

UTILIZZO DI **NUOVE TECNOLOGIE DI CENTRALIZZAZIONE**, COMANDO E CONTROLLO

IMPORTANTE FISSARE DELLE **BEST PRACTICE** E SEGUIRE DELLE LINEE GUIDA NAZIONALI ED EUROPEE

LE INFRASTRUTTURE E GLI **IMPIANTI SENSIBILI** SONO CONNESSI CON IMPIANTI **PERIFERICI E SECONDARI**

ANIE FEDERAZIONE
Technologies for our future

CONFINDUSTRIA

Associazione IMQ

GRAZIE

Giulio Iucci