Cybersecurity

Background DEEPTECH – Intelligenza artificiale e Cybersecurity

Prof. Ing. Domenico Capriglione
Dipartimento di Ingegneria Elettrica e dell'Informazione

AGENDA

- INTRODUZIONE ALLA CYBERSECURITY
- UNO SGUARDO ALLE RECENTI DIRETTIVE, NORME E REGOLAMENTI
- TIPOLOGIA DI ATTACCHI INFORMATICI: ESEMPI E RUOLO DEL IA
- POSSIBILI CONTROMISURE

AGENDA

- **INTRODUZIONE ALLA CYBERSECURITY**
- UNO SGUARDO ALLE RECENTI DIRETTIVE, NORME E REGOLAMENTI
- TIPOLOGIA DI ATTACCHI INFORMATICI: ESEMPI E RUOLO DEL IA
- POSSIBILI CONTROMISURE

Cybersecurity – TRIADE CIA

I tre principi chiave della sicurezza informatica

CONFIDENZIALITA’	• Assicura che l’informazione è protetta da utenti, entità e processi non autorizzati.
INTEGRITA’	• Assicura che il dato e/o l’informazione non è stata modificata da terze parti
DISPONIBILITA’	• Assicura che un servizio e/o dati sono sempre disponibili per gli utenti e/o servizi legittimi

Cybersecurity: da dove iniziare

Cybersecurity	• Tecniche, regole, policy, comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete, ma anche di utenti.
Cyber Spazio	• In senso ampio rappresenta l'intero dominio di componenti elettriche ed elettroniche coinvolte nella comunicazione, elaborazione, salvataggio e calcolo dei dati sensibili. Sono tutte le componenti tecnologiche.
Vulnerabilità	• Rappresenta le vulnerabilità che possono essere sfruttate da un hacker per eseguire attività fraudolente e malevoli in maniera non autorizzata. Sfruttano falle di sistema, bug, vulnerabilità degli utenti.
Cyber Attacco	• Rappresenta l'effettivo sfruttamento di una vulnerabilità.

Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Le 10 peggiori password

- ❑123456
- ❑Password
- ❑12345678
- ❑Qwerty
- ❑12345
- ❑123456789
- ❑Accesso
- ❑1234567
- ❑Calcio
- ❑tiamo

Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

alcuni motivi per scegliere generatori di password complesse

Password

- Gli hacker dispongono di sistemi per decifrare una password in pochi secondi: gli attacchi di «forza bruta» consentono ai criminali informatici di testare rapidamente milioni di password
- La maggior parte delle persone crea password facili da indovinare (parole comuni, nomi o schemi prevedibili)
- Le password generate in modo casuale sono molto più sicure (una password realmente casuale, con lettere maiuscole e minuscole, numeri e simboli, è molto più difficile da decifrare di una creata da una persona)

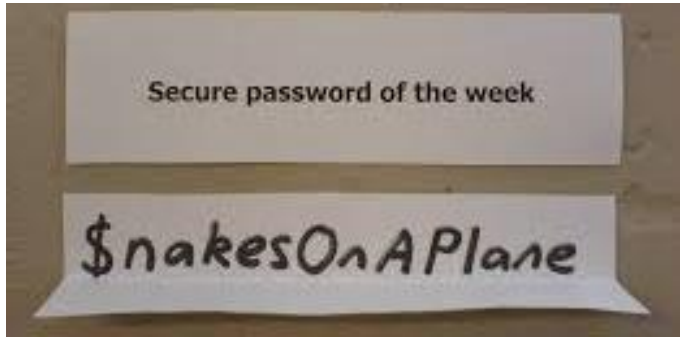
Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Generatori online di password complesse

- Avast
- Roboform



Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Password manager

- NordPass
- Roboform
- Keeper
- ProtonPass
- Norton
- BitDefenderPM
- ....

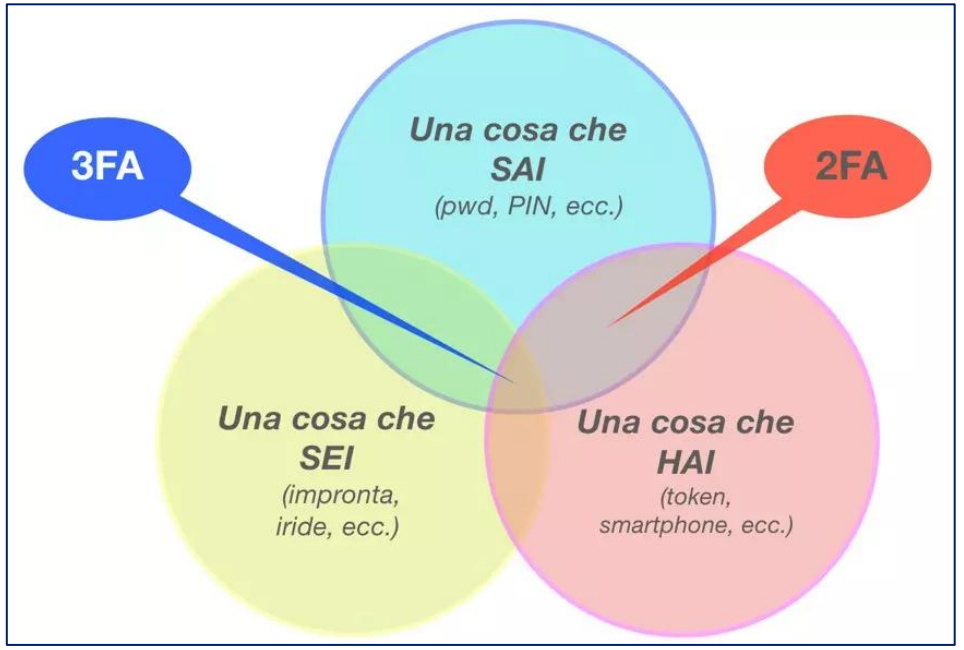
- ✓ Archivia e gestisce in modo sicuro le password degli account online
- ✓ Compilazione automatica delle credenziali di accesso a siti web e applicazioni
- ✓ Misure di sicurezza aggiuntive come **l'autenticazione a più fattori**
- ✓ Mantenere password complesse e diverse per tutti i tuoi account
- ✓ Ricordare una sola master password

Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Autenticazione multifattoriale (MFA)



Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Firewall

Barriere di sicurezza che monitorano il traffico di rete in entrata e in uscita, bloccando le connessioni non autorizzate

Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Antivirus

Software progettato per rilevare e rimuovere virus, malware e altre minacce informatiche

Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Backup dei dati

Copie di backup dei dati importanti consentono il ripristino in caso di perdita o attacco

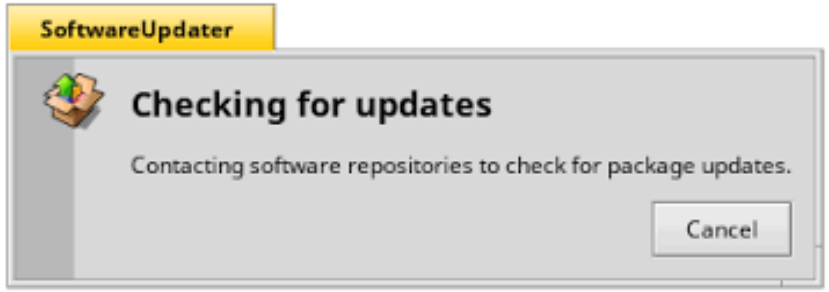
Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Software updates

Mantenere aggiornati i sistemi operativi, i software e le applicazioni per correggere le vulnerabilità di sicurezza



Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Crittografia dei dati

Riservatezza (Confidentiality): assicura che solo i mittenti e i destinatari autorizzati possano leggere i dati
Integrità dei dati (Integrity): la crittografia permette di verificare che i dati non siano stati alterati durante il transito (se un solo bit del messaggio originale viene modificato, la firma digitale risulterà non valida, segnalando una manomissione)
Autenticazione (Authentication): grazie all'uso di certificati digitali e chiavi pubbliche/private, la crittografia conferma l'identità delle parti coinvolte in una comunicazione, impedendo attacchi di tipo Identity Theft

Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

COOKIE: Utilità

- Gestione della sessione (I cookie aiutano i siti web a ricordare chi sei mentre navighi tra le pagine)
- Personalizzazione (preferenze di lingua, contenuti basati sulla posizione, consigli basati sulla cronologia di navigazione)
- Autenticazione (accesso solo gli individui autorizzati possano accedere a determinate parti di un sito web)

Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

Mitigazione del rischio: per ridurre la probabilità e l'impatto di attacchi informatici e violazioni dei dati
Conformità: per garantire il rispetto delle leggi, dei regolamenti e degli standard di settore pertinenti (ad esempio, GDPR, HIPAA, PCI DSS)
Orientamento: fornire linee guida e aspettative chiare per i dipendenti in merito alle migliori pratiche di sicurezza informatica.
Responsabilità: stabilire ruoli e responsabilità in materia di sicurezza informatica all'interno dell'organizzazione.

Cybersecurity: da dove iniziare

Cybersecurity

- Tecniche, Regole, Policy, Comportamenti da adottare al fine di garantire protezione di componenti hardware e software come dispositivi, computer e rete ma anche di utenti.

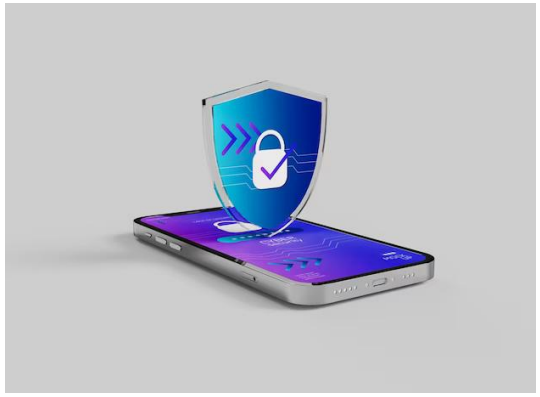
COOKIE: Warning!!

- Tracciamento e profilazione (problematiche di privacy)
- Furto di identità (problematiche di intercettazione dei cookies)
- Codice dannoso nei cookie (Malicious software – Malware)
- Cookie Zombie (difficilmente cancellabili e rilevabili dagli antivirus)
- Accesso non autorizzato (la memorizzazione espone ad accesso incontrollato dal proprio dispositivo)

Cybersecurity: da dove iniziare

Cyber Spazio

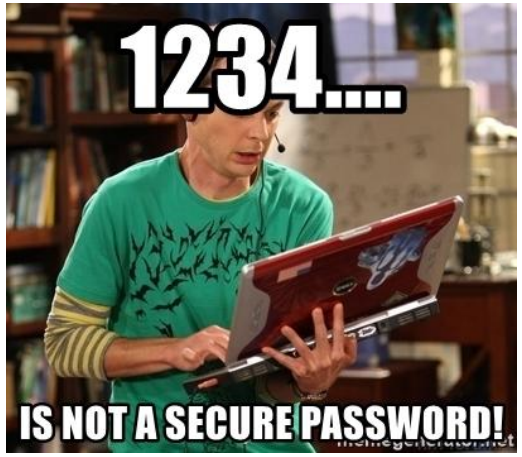
- In senso ampio rappresenta l'intero dominio di componenti elettriche ed elettroniche coinvolte nella comunicazione, elaborazione, salvataggio e calcolo dei dati sensibili. Sono tutte le componenti tecnologiche.



Cybersecurity: da dove iniziare

Vulnerabilità

- Rappresenta l'insieme delle debolezze o falle (di sistema, software o umane) che possono essere sfruttate da una minaccia per eseguire attività non autorizzate, malevole o fraudolente, compromettendo la sicurezza degli asset informatici.



Cybersecurity: da dove iniziare

Vulnerabilità

- Rappresenta l'insieme delle debolezze o falle (di sistema, software o umane) che possono essere sfruttate da una minaccia per eseguire attività non autorizzate, malevole o fraudolente, compromettendo la sicurezza degli asset informatici.

Vulnerabilità Software → Sono errori di programmazione che permettono a un attaccante di far eseguire al sistema azioni non previste (ad esempio SQL Injection, Buffer overflow)

Vulnerabilità di Configurazione → Il sistema è stato impostato in modo errato o superficiale (ad esempio Password di default, software non aggiornati, porte di comunicazione aperte)

Vulnerabilità Umane → In questo caso, la "debolezza" non è nel sistema, ma nella psicologia dell'utente (Phishing, Unawareness, Tailgating)

https://www.cve.org/

Cybersecurity: da dove iniziare

Attacco

- Un tentativo deliberato ed esplicito di sfruttare una vulnerabilità per ottenere un accesso non autorizzato, alterare, distruggere, rubare o rendere inutilizzabili dati e sistemi informatici.

Cybersecurity: da dove iniziare

Attacco

- Un tentativo deliberato ed esplicito di sfruttare una vulnerabilità per ottenere un accesso non autorizzato, alterare, distruggere, rubare o rendere inutilizzabili dati e sistemi informatici.

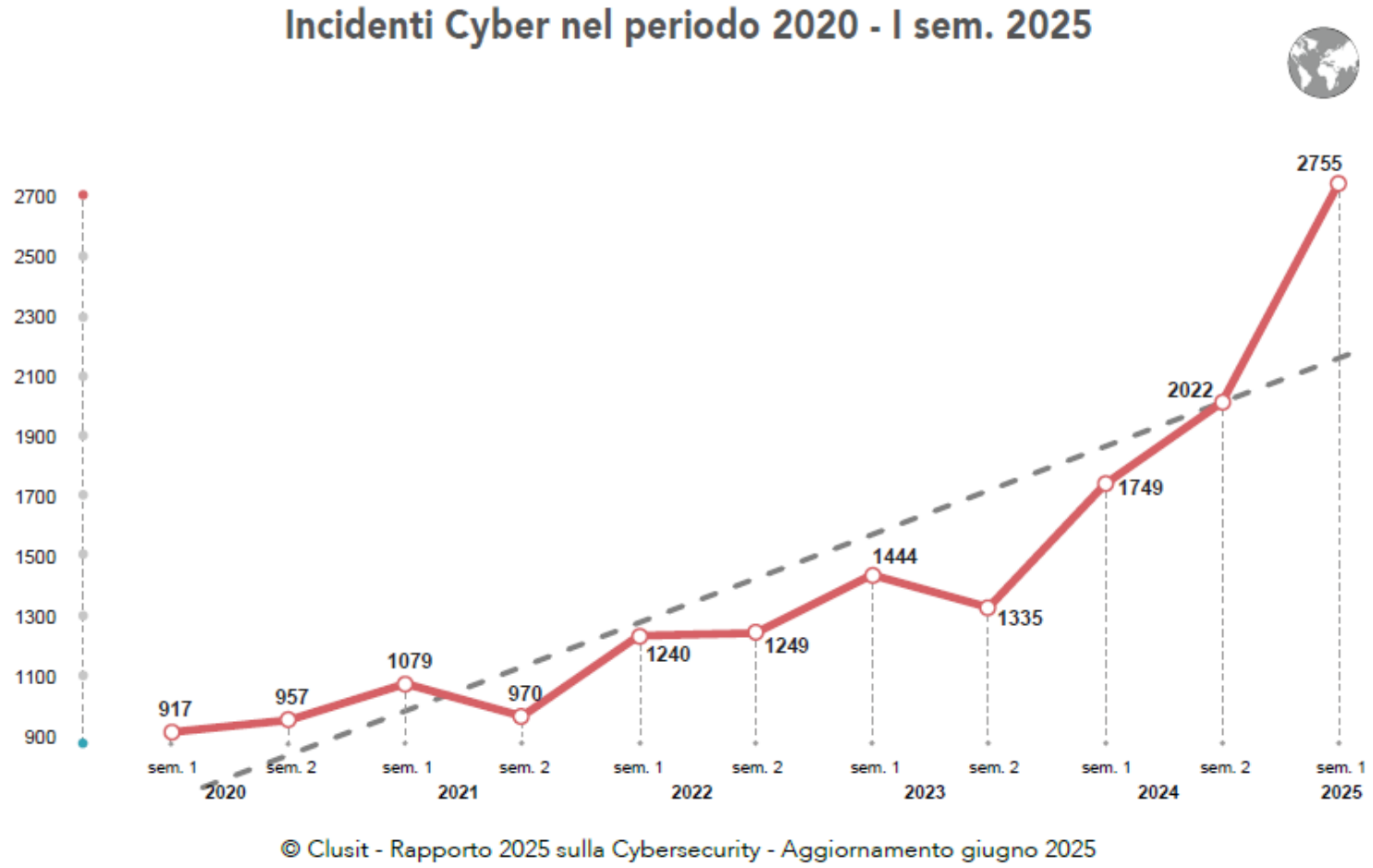
ATTACCHI PASSIVI

L'obiettivo è intercettare informazioni senza che la vittima se ne accorga (es. Eavesdropping o sniffing del Wi-Fi). **Non modificano i dati, violano la Confidentiality (Riservatezza)**.

ATTACCHI ATTIVI

L'attaccante modifica i dati, interrompe i servizi o distrugge i sistemi (es. Ransomware, DDoS, SQL Injection). **Violano l'Integrity (Integrità) o l'Availability (Disponibilità)**.

Analisi dei principali cyber attacchi noti (a livello globale)

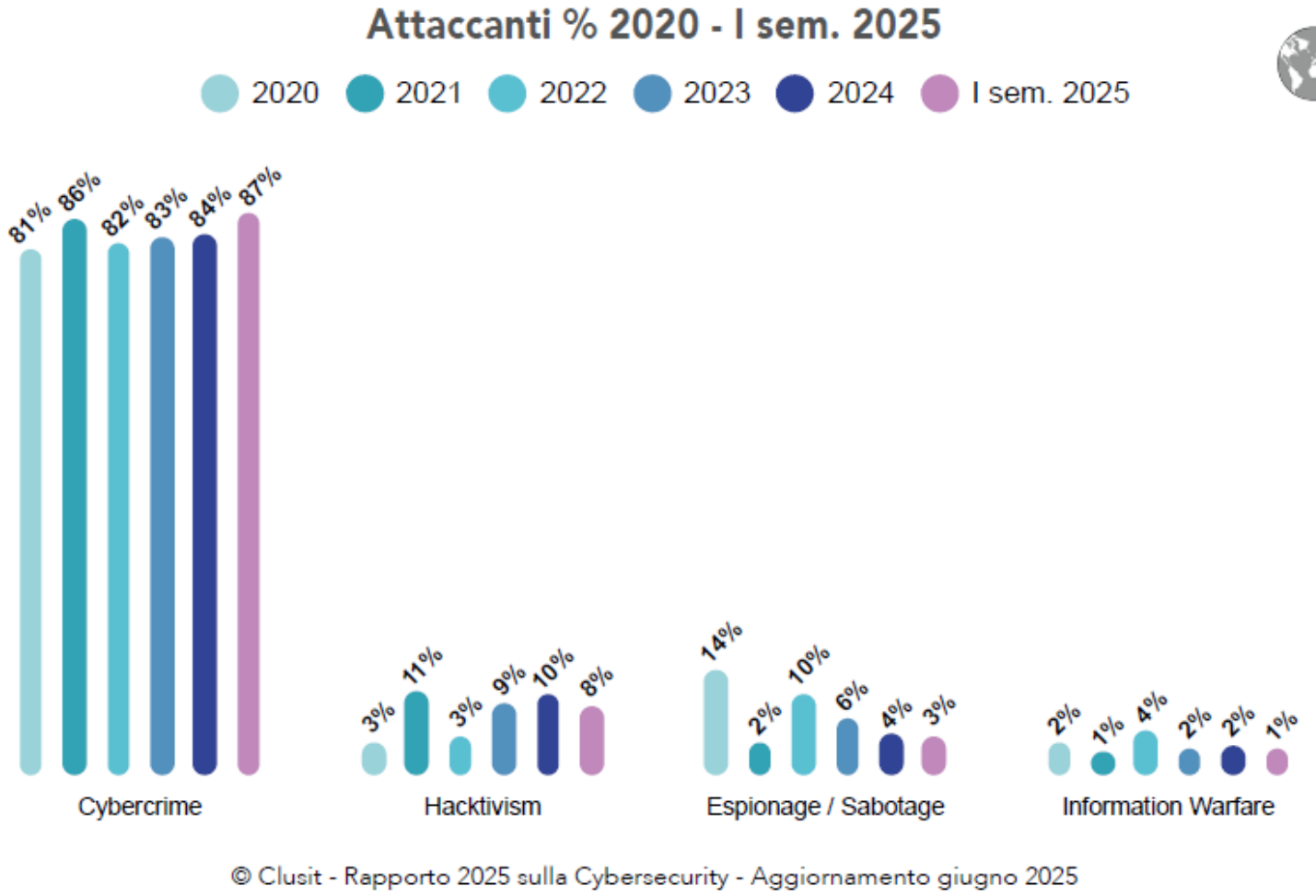


CLUSIT (Associazione Italiana per la Sicurezza Informatica)

https://clusit.it/

≈16000 attacchi **noti,** di particolare gravità ed andati a buon fine

Analisi dei principali cyber attacchi noti (a livello globale)



CLUSIT (Associazione Italiana per la Sicurezza Informatica)

https://clusit.it/

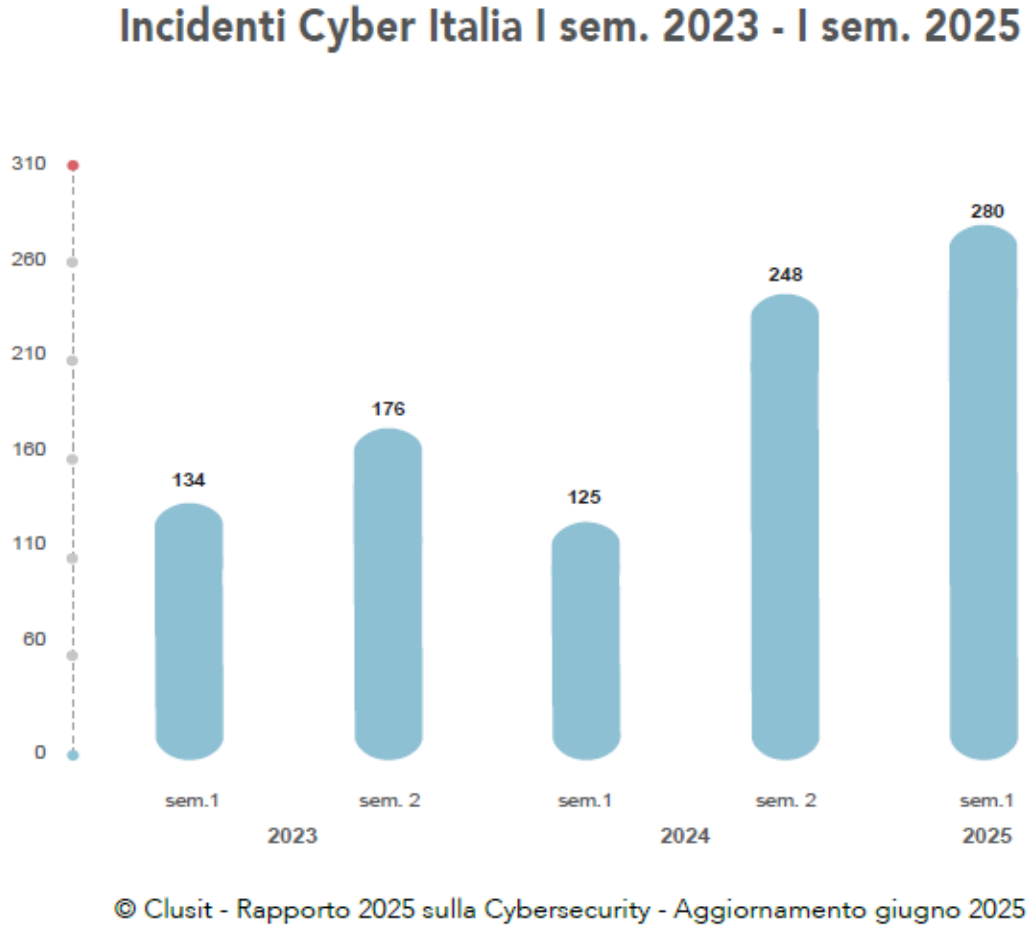
Il peso del cybercrime (reato informatico) a livello globale

Fonte: Cybersecurity Ventures (https://cybersecurityventures.com/)

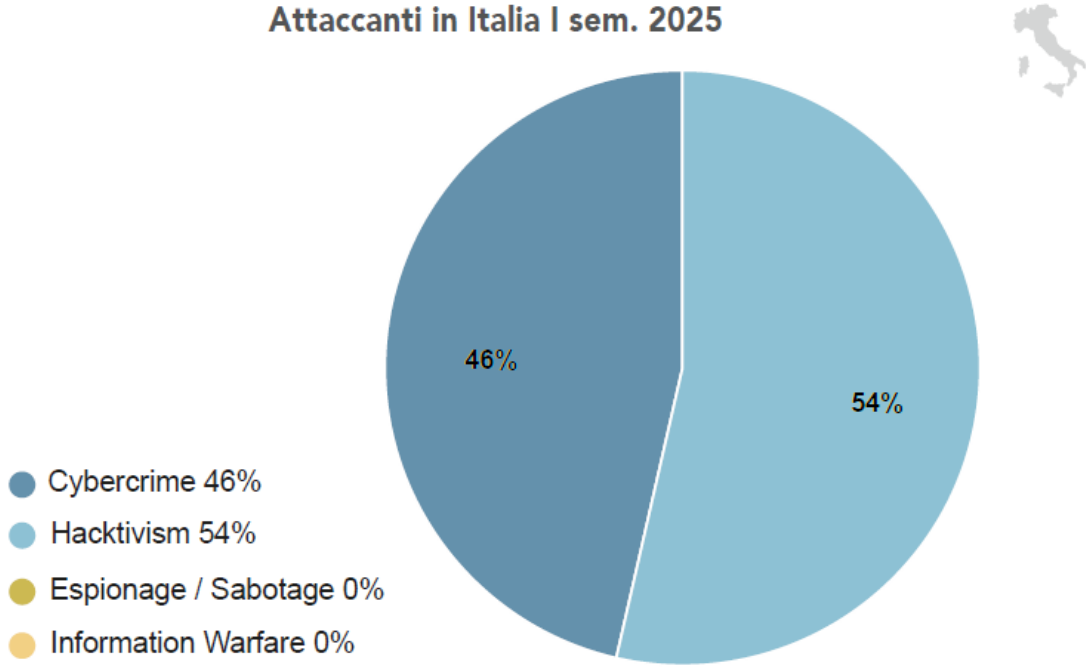
Cybercrime:

- Frode informatica finalizzata a realizzare un guadagno
- Falso in documenti informatici
- Danneggiamento e il sabotaggio informatico
- Accesso abusivo, associato alla violazione delle misure di sicurezza del sistema
- Spionaggio (a scopo politico o industriale)
- Estorsione (caso tipico del ransomware)

Analisi dei principali cyber attacchi IN ITALIA



© Clusit - Rapporto 2025 sulla Cybersecurity - Aggiornamento giugno 2025



Nota: il 10% degli attacchi rilevati a livello globale sono stati condotti verso l'Italia

PERCHE’ ci attaccano ??

- Presa di controllo di un sistema (anche a scopo di sabotaggio) o di un sito web
- Furto di informazioni a scopo di spionaggio industriale
- Disturbo del buon funzionamento di un servizio
- Furto di credenziali e di dati bancari
- Utilizzo delle risorse del sistema dell’utente (data mining)
- ....

Oggi il Cybercrime non è più il «Nerd nel garage»

- **Sviluppatori (R&D)**: Scrivono il codice malevolo, creano i ransomware e cercano le falle "Zero-Day".
- **Specialisti di Social Engineering (Sales & Marketing)**: Psicologi e comunicatori che creano campagne di phishing così credibili da ingannare anche i più esperti. Sono i "venditori" che convincono la vittima ad "acquistare" il malware (cliccandoci sopra).
- **Initial Access Brokers (Logistica)**: Esperti che si occupano solo di "bucare" il perimetro aziendale. Una volta dentro, vendono l'accesso ad altri gruppi che completeranno l'attacco.
- **Money Laundering Specialists (Finance)**: Esperti finanziari che gestiscono il riciclaggio delle criptovalute ottenute dai riscatti.
- **Customer Support**: molti gruppi ransomware hanno una chat di supporto per le vittime, dove operatori gentili spiegano come comprare Bitcoin e come usare la chiave di decrittazione dopo il pagamento.

I RISCHI PER LE AZIENDE, GLI ENTI e GLI UTENTI

- **Danni diretti e materiali ai sistemi elettronici e informatici**

(es. danneggiamento server, riparazione e/o sostituzione componenti)

- **Interruzione delle attività** (es. magazzino, produzione, gestione clienti e fornitori)
- **Furto o manomissioni di dati, informazioni o progetti strategici** (es. proprietà intellettuale)
- **Furto di denaro** (es. pagamenti o distrazione di denaro per via informatica)
- **Danni legali e/o richieste di risarcimento da parte di terzi** (es. perdita o sottrazione di dati sensibili - GDPR)
- **Danni reputazionali e perdita di clienti e fornitori** (es. deterioramento relazioni con clienti, fornitori e finanziatori)

Cyber Security: l'importanza e necessità della sicurezza informatica

- **Le aziende e gli enti** di vari settori (energia, trasporti, vendita, produzione, ricerca, formazione), **utilizzano i sistemi digitali e la connettività** ad alta velocità per fornire un servizio efficiente ai clienti e per gestire operazioni commerciali efficienti dal punto di vista dei costi.
- Un **evento intenzionale di violazione e accesso non autorizzato** a un sistema informatico, a una rete o a strutture collegate comporta **l'esposizione, il furto, la cancellazione o l'alterazione di dati riservati**.

- **Le organizzazioni hanno la responsabilità di proteggere i dati** per mantenere la fiducia dei clienti e soddisfare la conformità normativa (ad esempio il GDPR).
- **Le organizzazioni devono implementare la sicurezza informatica** ottimizzando la difesa digitale tra persone, processi e tecnologie.

AGENDA

- INTRODUZIONE ALLA CYBERSECURITY
- **UNO SGUARDO ALLE RECENTI DIRETTIVE, NORME E REGOLAMENTI**
- TIPOLOGIA DI ATTACCHI INFORMATICI: ESEMPI E RUOLO DEL IA
- POSSIBILI CONTROMISURE

Principali regolamenti e direttive europee

General Data Protection Regulation

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1760885194477

Critical Entities Resilience Directive

https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

Rafforzare la resilienza e la protezione dei servizi essenziali, promuovendo un approccio integrato e coordinato tra le istituzioni nazionali ed europee

Network Information Security Directive 2

https://www.nis-2-directive.com/

https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

Principali regolamenti e direttive europee

Cyber Solidarity Act

https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng

Mira a rafforzare la “resilienza informatica” degli Stati membri, contribuendo alla sovranità tecnologica e all’autonomia strategica della UE in ambito cyber security

Cybersecurity Act

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Certificazione delle infrastrutture critiche, comprese le reti energetiche, l’acqua e i sistemi bancari, oltre a prodotti, processi e servizi, e garantisce che soddisfino gli standard di sicurezza informatica

Digital Operational Resilience Act

https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Mira a mitigare i rischi derivanti dalla trasformazione digitale del settore dei servizi finanziare e a promuovere la resilienza informatica, aiutando le banche, il settore finanziario e i sistemi finanziari a prevenire, rispondere e riprendersi da problemi di cybersicurezza

Cyber Resilience Act

https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

Ulteriori norme internazionali

- NIST Cybersecurity Framework: A voluntary framework for managing cybersecurity risk in the US
- PCI DSS (Payment Card Industry Data Security Standard): Requirements for organizations handling credit card information
- HIPAA (Health Insurance Portability and Accountability Act): Protecting healthcare data in the US

- **ISO 27001: An international standard for information security management systems**
  - **Quadro completo: copre un'ampia gamma di controlli di sicurezza, tra cui misure organizzative, fisiche e tecniche**
  - **Miglioramento continuo: Lo standard promuove una cultura del miglioramento continuo**
  - **Maggiore sicurezza: Riduce il rischio di violazioni dei dati e altri incidenti di sicurezza**
  - **Maggiore fiducia: Crea fiducia con clienti, partner e stakeholder**
  - **Conformità normativa: Aiuta le organizzazioni a conformarsi ai requisiti legali e normativi pertinenti**
  - **Resilienza aziendale: Migliora la capacità dell'organizzazione di resistere e riprendersi dalle interruzioni**

GENERAL DATA PROTECTION REGULATION

GDPR.EU

OBIETTIVI

➢ **Tutela dei diritti individuali**

- Il GDPR mira a garantire agli individui un maggiore controllo sui propri dati personali
- Stabilisce diritti come il diritto di accesso, rettifica, cancellazione e portabilità dei propri dati

➢ **Armonizzazione della protezione dei dati**

- Crea un insieme uniforme di norme sulla protezione dei dati in tutta l'UE, semplificando la conformità per le aziende

➢ **Aumento della responsabilità**

- Rende le organizzazioni responsabili delle modalità di raccolta, utilizzo e protezione dei dati personali

CARATTERISTICHE PRINCIPALI

➢ **Sanzioni severe:**

- Impone sanzioni significative in caso di inosservanza, fino a 20 milioni di euro o al 4% del fatturato annuo globale

➢ **Responsabili della protezione dei dati (DPO):**

- Impone la nomina di un DPO in determinate circostanze

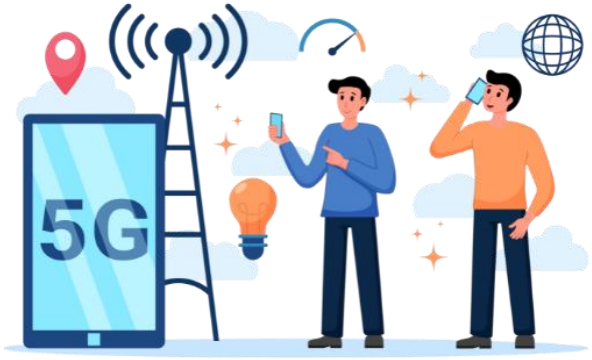
➢ **Notifica di violazione dei dati:**

- Impone alle organizzazioni di segnalare le violazioni dei dati alle autorità di controllo entro 72 ore

Sicurezza delle infrastrutture critiche

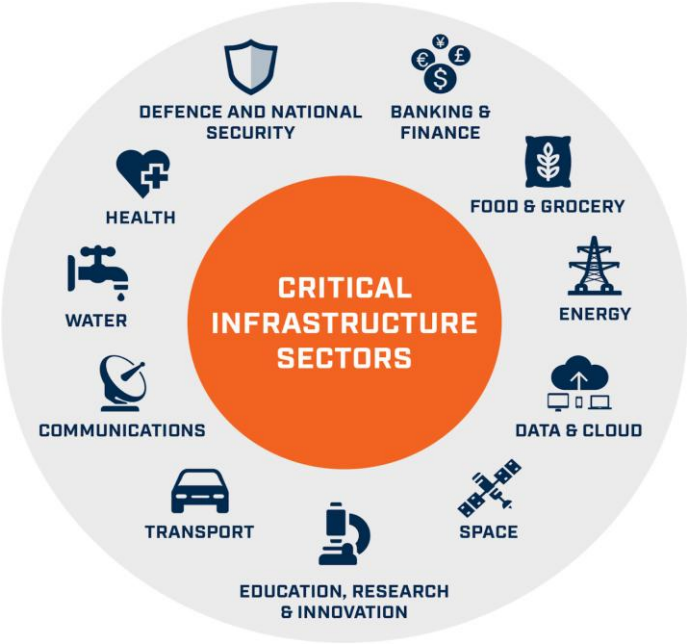
INFRASTRUTTURE CRITICHE: sistemi essenziali per la stabilità e il funzionamento di una nazione, quali:

ENERGIA



TELECOMUNICAZIONI

RETI IDRICHE



TRASPORTI

FINANZE

SANITÀ

Sicurezza delle infrastrutture critiche

DIRETTIVE

Implementata nel 2016, mira a garantire un livello elevato di sicurezza per reti e sistemi informativi, obbligando gli operatori di infrastrutture critiche a segnalare incidenti e a rispettare specifici requisiti di sicurezza

Entrata in vigore nel 2023, rafforza le misure della NIS, estendendo il campo di applicazione a nuovi settori e imponendo standard di sicurezza più rigorosi. Introduce inoltre un approccio multirischio e la collaborazione tra stati membri attraverso il Critical Entities Resilience Group (CERG)

NIS2: A QUALI SETTORI E' RIVOLTA?

- Energia
- Trasporti: Aereo, ferroviario, marittimo e stradale
- Bancario e Infrastrutture dei Mercati Finanziari
- Sanità
- Acqua
- Infrastrutture Digitali
- Gestione di servizi ICT
- Pubblica Amministrazione
- Spazio

Sicurezza delle infrastrutture critiche

DIRETTIVE

Implementata nel 2016, mira a garantire un livello elevato di sicurezza per reti e sistemi informativi, obbligando gli operatori di infrastrutture critiche a segnalare incidenti e a rispettare specifici requisiti di sicurezza

Entrata in vigore nel 2023, rafforza le misure della NIS, estendendo il campo di applicazione a nuovi settori e imponendo standard di sicurezza più rigorosi. Introduce inoltre un approccio multirischio e la collaborazione tra stati membri attraverso il Critical Entities Resilience Group (CERG)

NIS2: OBBLIGHI?

- Formazione
- Gestione dei rischi
- Sicurezza della supply chain
- Continuità operativa
- Notifica degli incidenti

NIS2: AMBITI DI APPLICAZIONE

Articolo 2:

Copre enti pubblici o privati che si qualificano come o superano i massimali per le medie imprese e che operano all'interno dell'UE

Applicazione alle organizzazioni di medie e grandi dimensioni

Disposizioni supplementari per garantire proporzionalità, miglior gestione del rischio e criteri di criticità chiari

Applicazione alle PA centrali e regionali, con possibilità di estensione anche a livello locale

NIS2: AMBITI DI APPLICAZIONE

ORGANIZZAZIONI DI MEDIE E GRANDI DIMENSIONI (+ 50 dipendenti)

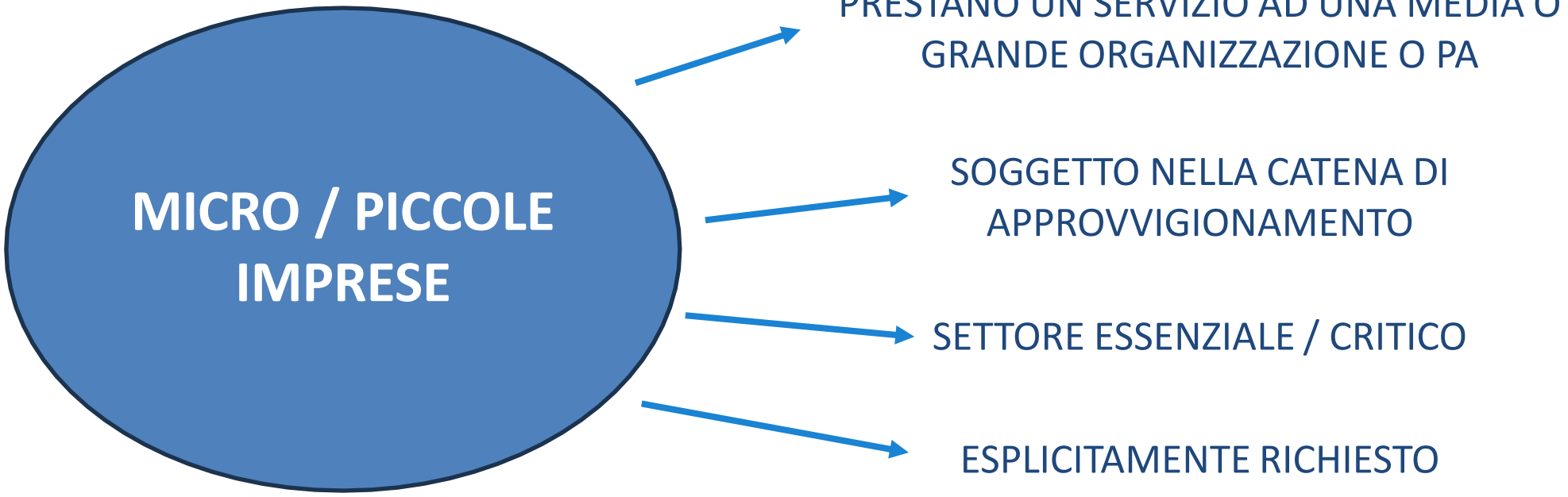
ORGANIZZAZIONI RITENUTE DI IMPORTANZA CRITICA

INTERA CATENA DI APPROVVIGIONAMENTO DELLA SINGOLA ORGANIZZAZIONE

ESCLUSIONE

ORGANIZZAZIONI CON MENO DI 50 DIPENDENTI O CON UN FATTURATO ANNUO INFERIORE A 10 MILIONI

NIS2: MICRO/PICCOLE IMPRESE



NIS2: MICRO/PICCOLE IMPRESE FORNITRICI DI BENI «FISICI»?

Un fornitore di beni fisici non tecnologici non ha accesso ai sistemi informatici della PA. Pertanto, tale attività non è considerata "critica" per la sicurezza nazionale o digitale.

Ma attenzione lo stesso al **coinvolgimento indiretto**!!

1) **Accesso ai portali della PA**: spesso si utilizzano piattaforme come il MePA o altri portali di e-procurement. La PA potrebbe chiedere di innalzare gli standard di sicurezza personali (es. obbligo di usare lo SPID o l'Autenticazione a due fattori - MFA) per garantire che nessuno rubi le credenziali e inserisca ordini falsi o modifichi i dati di pagamento.
2) **Questionari di qualificazione**: in fase di bando o di iscrizione all'albo fornitori, la PA potrebbe iniziare a inserire clausole standard sulla protezione dei dati e sulla cybersecurity. Potrebbe essere necessario dover dichiarare di avere misure minime di protezione sui propri computer (antivirus, backup).

CYBER RESILIENCE ACT - CRA

MENU CERCA LA STAMPA IL QUOTIDIANO ABBONATI

IL CASO

Usa, robot hackerati: aspirapolvere intelligente insulta i proprietari. Ecco come proteggersi

Essere insultati dai propri elettrodomestici è possibile. I robot sono vulnerabili, i dispositivi Ecovas sono pieni di falle, dai problemi con i Pin alle connessioni Bluetooth poco sicure

https://www.lastampa.it/esteri/2025/01/23/news/usa_elettrodomestici_hackerati_insulti_proprietari-14957154/

CYBER RESILIENCE ACT - CRA

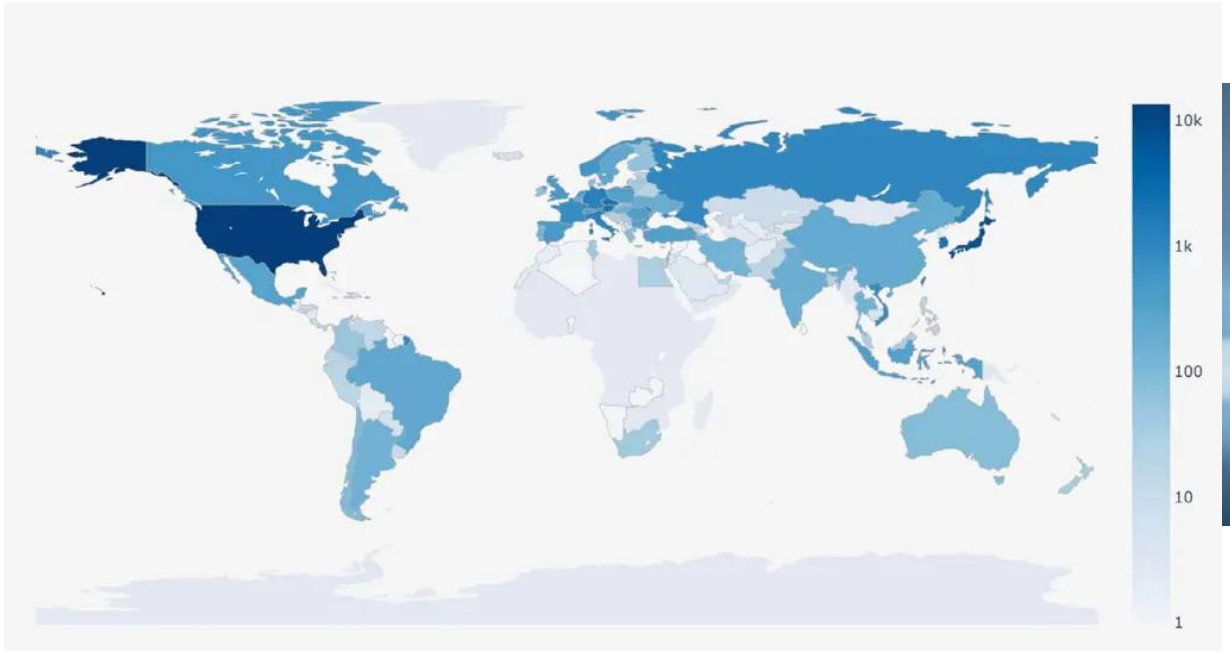
Videocamere private, migliaia di video trafugati e messi in vendita sul web (con tanto di tariffario)

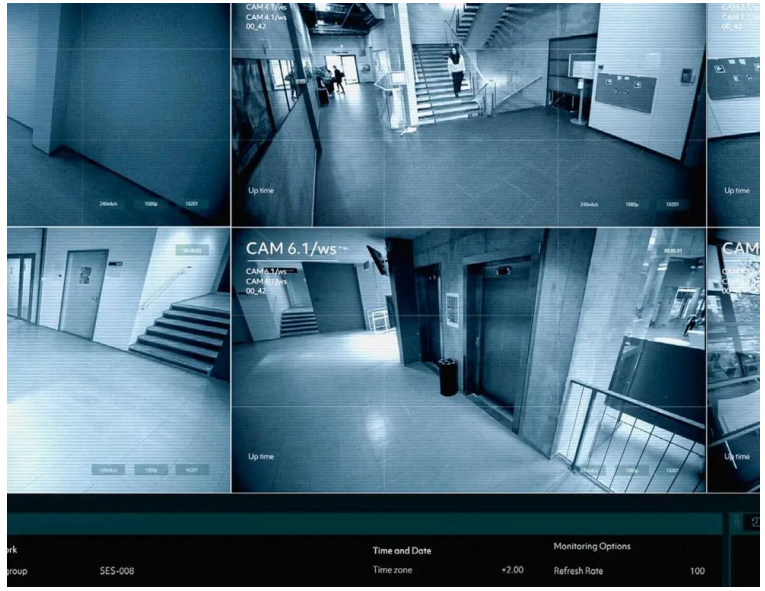
Individuato un portale con immagini da oltre 2mila abitazioni, centri estetici e studi medici. Prezzi da 20 a 575 dollari per ottenere persino il controllo dei dispositivi e visualizzare le immagini in diretta

Lo scorso 9 agosto un noto conduttore televisivo ha scoperto che in rete circolavano video sull'interno della propria abitazione che lo ritraevano insieme alla compagna. A metterlo al corrente sarebbe stato un messaggio inviato da un suo follower. I video erano riprese delle telecamere di videosorveglianza.
Il filmato, dopo essere stato caricato su un sito straniero poi oscurato, ha iniziato a circolare rapidamente sulle principali piattaforme di messaggistica e social, tra cui WhatsApp e Telegram, dove è stato condiviso a più riprese.

https://www.wired.it/article/de-martino-come-proteggere-videocamere-sorveglianza/

CYBER RESILIENCE ACT - CRA



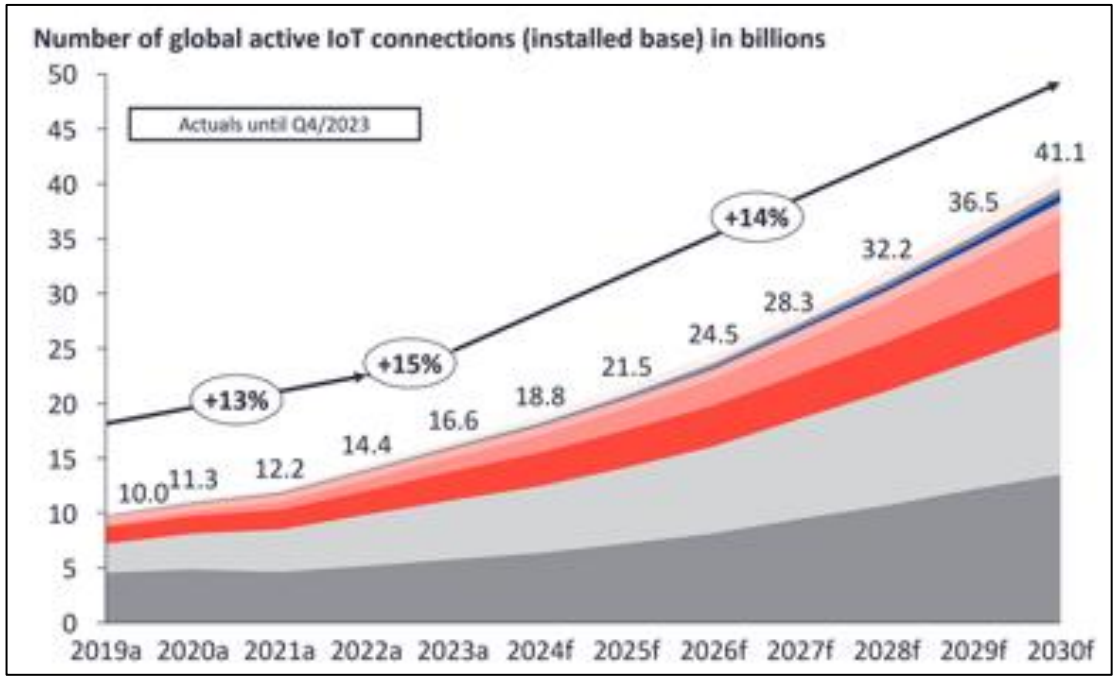


Lo scorso agosto, Bitsight ha pubblicato una nuova ricerca che lascia poco spazio ai dubbi: nel mondo esistono almeno 40.000 videocamere di sicurezza e telecamere di videosorveglianza accessibili liberamente da Internet, senza alcuna protezione, né password, né crittografia, né controlli di autenticazione.

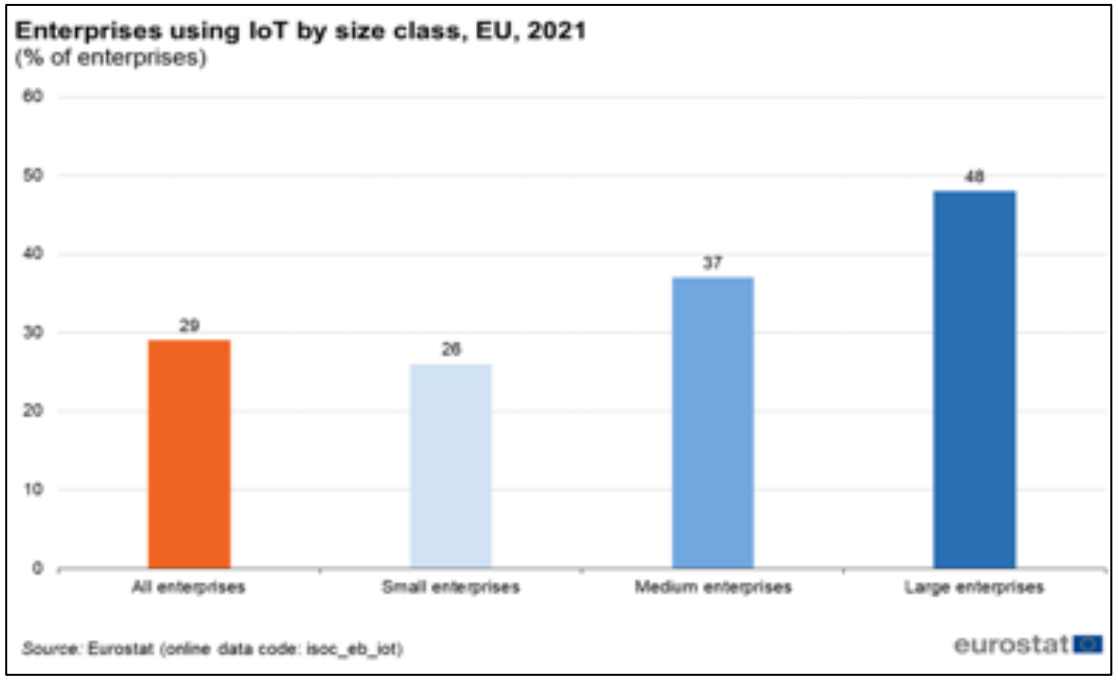
https://www.cybersecurity360.it/nuove-minacce/dalle-case-agli-uffici-come-40-000-videocamere-di-sicurezza-diventano-finestre-pubbliche/

CYBER RESILIENCE ACT - CRA

Il numero di dispositivi connessi aumenterà nei prossimi anni

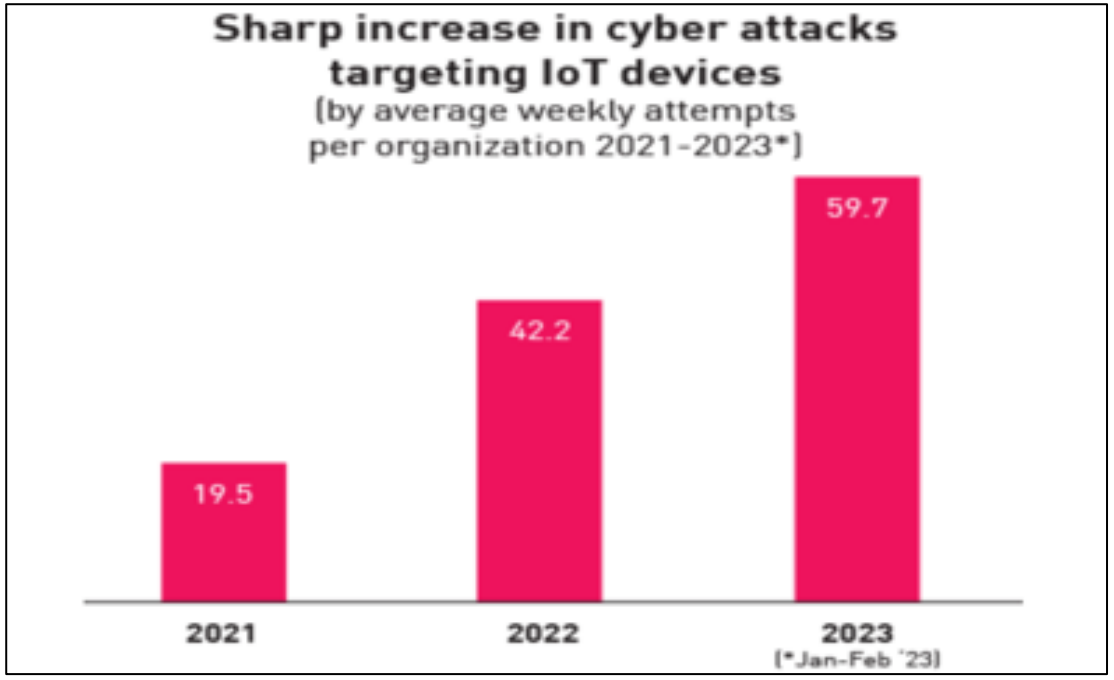


Il numero di connessioni è cresciuto indipendentemente dalla dimensione dell'azienda

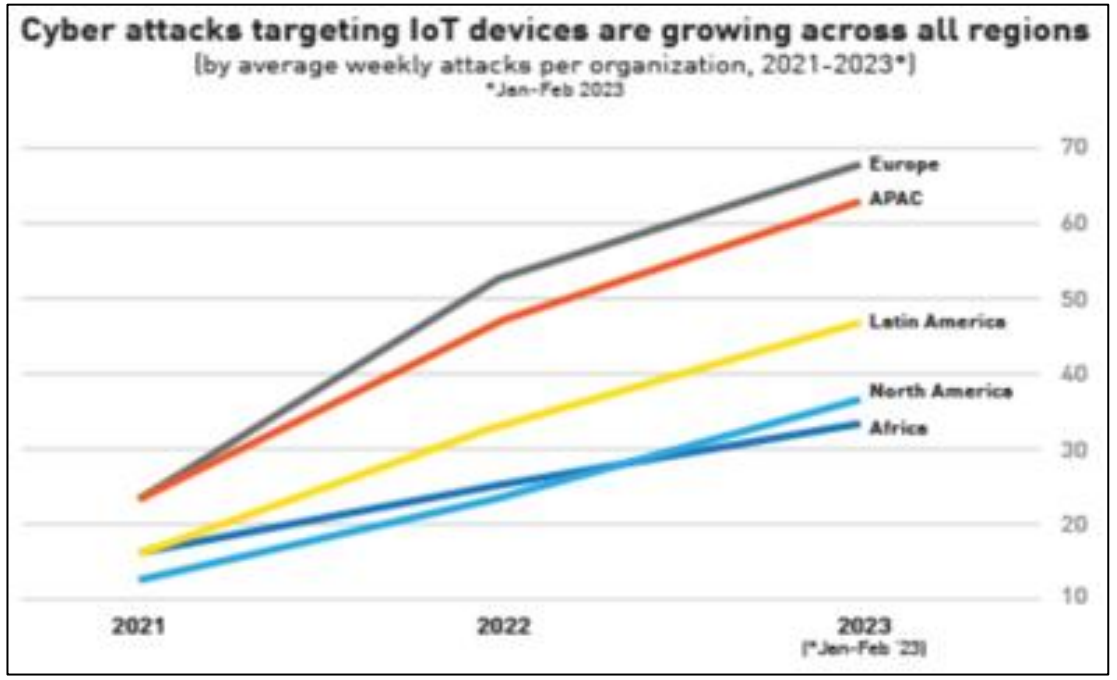


CYBER RESILIENCE ACT - CRA

Il numero di attacchi ai dispositivi connessi è in continuo aumento



L'Europa è caratterizzata da numeri maggiori di attacchi ai dispositivi connessi



CYBER RESILIENCE ACT - CRA

Per la prima volta, **la sicurezza informatica diventa un requisito legale obbligatorio** per la marcatura CE di quasi tutti i prodotti con componenti digitali (hardware e software) venduti in Europa

PRODUTTORI

Security by Design & Default: I prodotti devono essere progettati per essere sicuri "nativamente" (es. niente password predefinite come "admin/admin", crittografia dei dati attiva di default).
Gestione delle Vulnerabilità: Il produttore deve garantire aggiornamenti di sicurezza per tutta la durata prevista del prodotto (in genere almeno 5 o 10 anni).
Documentazione e SBOM: È obbligatorio creare una Software Bill of Materials (SBOM), ovvero una "lista degli ingredienti" software, per sapere esattamente quali librerie o componenti di terze parti sono presenti nel dispositivo e se sono vulnerabili.
Obbligo di Notifica: in caso di incidente grave o vulnerabilità sfruttata, i produttori dovranno informare l'ENISA (l'Agenzia UE per la cybersicurezza) entro 24 ore.

CYBER RESILIENCE ACT - CRA

Per la prima volta, **la sicurezza informatica diventa un requisito legale obbligatorio** per la marcatura CE di quasi tutti i prodotti con componenti digitali (hardware e software) venduti in Europa

IMPORTATORI

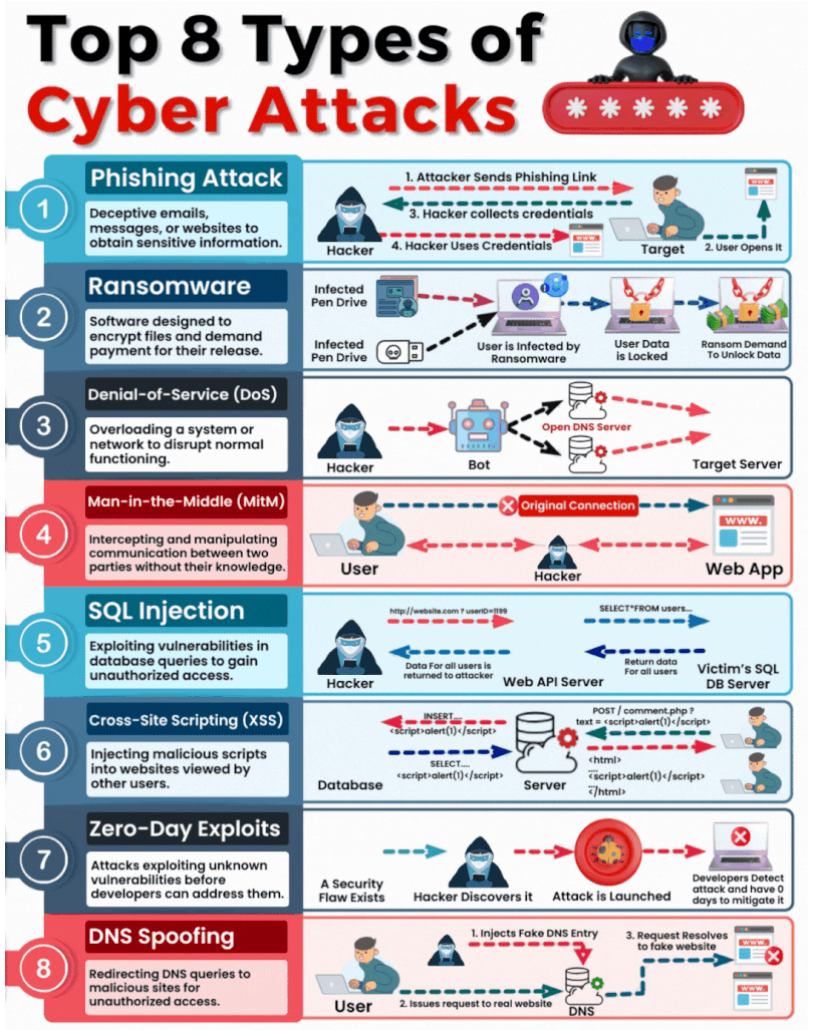
Dovere di Verifica: Prima di immettere il prodotto nel mercato UE, l'importatore deve verificare che il produttore extra-UE abbia eseguito le procedure di valutazione della conformità e che il prodotto porti la marcatura CE.
Blocco delle vendite: Se l'importatore ha motivo di credere che il prodotto non sia sicuro, non può immetterlo sul mercato e deve informare il produttore e le autorità di vigilanza.
Responsabilità Sussidiaria: Se il produttore non è stabilito nell'UE, l'importatore diventa il referente principale per le autorità di controllo.

AGENDA

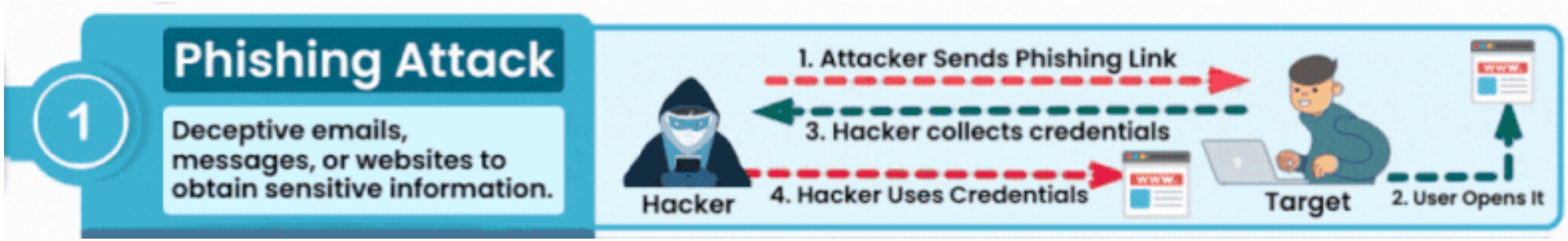
- INTRODUZIONE ALLA CYBERSECURITY
- UNO SGUARDO ALLE RECENTI DIRETTIVE, NORME E REGOLAMENTI
- **TIPOLOGIA DI ATTACCHI INFORMATICI: ESEMPI E RUOLO DEL IA**
- POSSIBILI CONTROMISURE

Cyber Security: alcune definizioni utili

- **VIRUS**: programma informatico che deve essere attivato dall'interazione della vittima con il file infetto
- **WORM**: programmi dannosi autonomi in grado di auto-replicarsi e propagarsi da sé non appena violano il sistema
- **MALWARE**: MALicious softWARE (Software malevolo) in grado di consentire a terzi di accedere in modo non autorizzato a informazioni sensibili o di interrompere il normale funzionamento di un'infrastruttura critica
- **RANSOMWARE**: tecnologie associate che i malintenzionati utilizzano per estorcere denaro agli utenti
- **PHISHING**: tecniche di social engineering per indurre gli utenti a rivelare informazioni di identificazione personale
  - SMISHING: SMS PHISHING (link malevolo inviato con SMS)
  - VISHING: Voice PHISHING (truffa attraverso voce telefonica)
  - QRishing: codice QR che indirizza ad un link malevolo



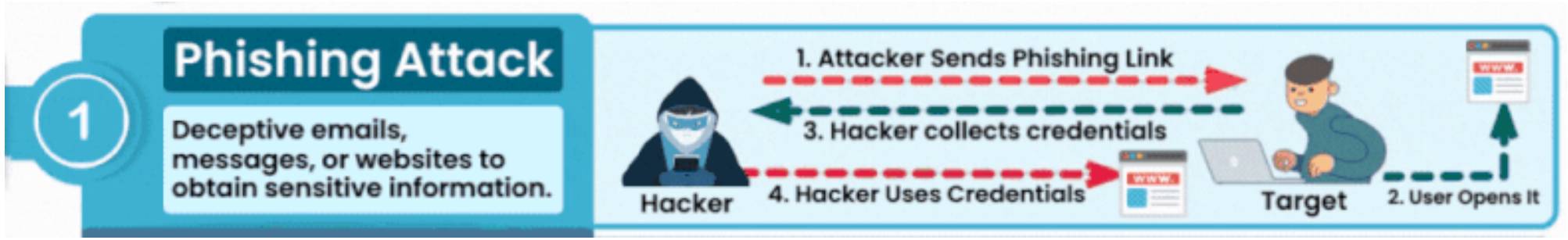
Phishing



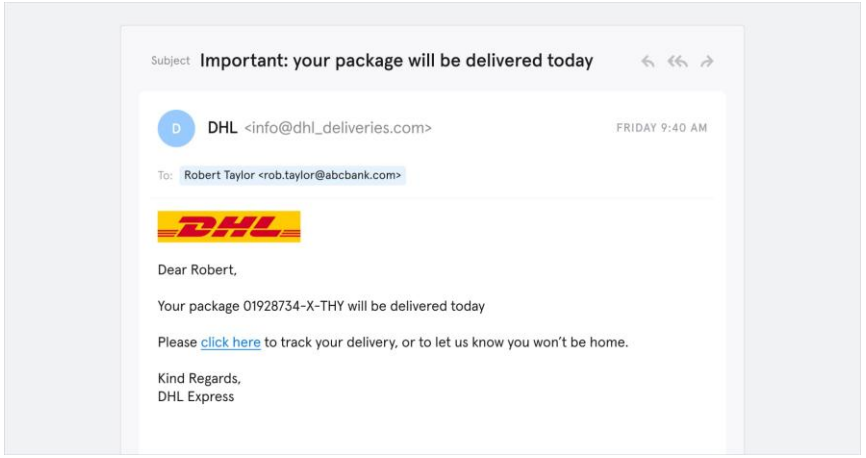
La vittima è manipolata (social engineering):

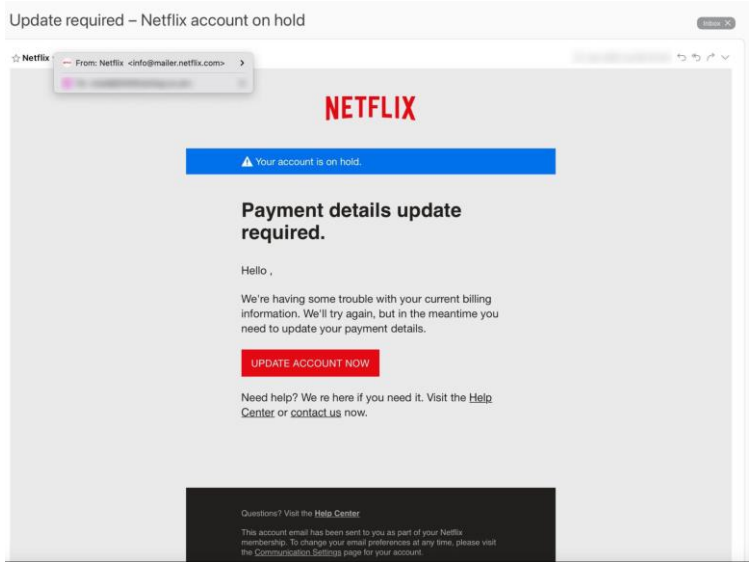
1) Avvicinata con informazioni realistiche o quasi credibili
2) Indotta a rispondere rapidamente
3) Invitata a fornire propri dati per risolvere la questione

Phishing

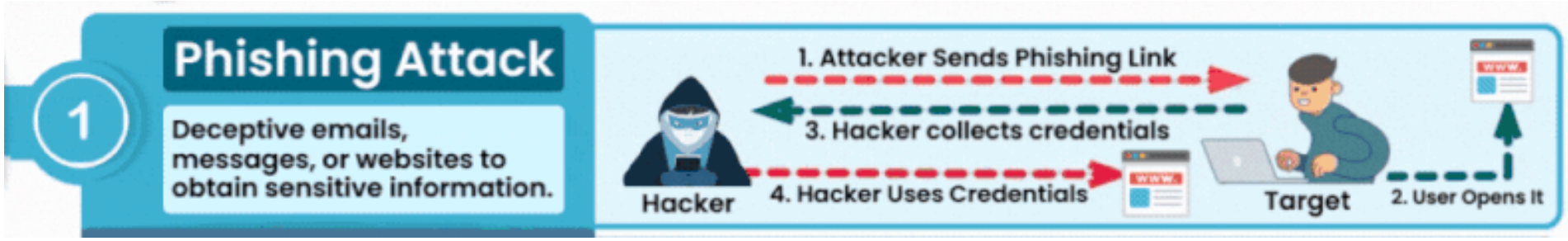


Uso di metodi di comunicazione quali email, messaggi, pop-up, siti web, al fine di ottenere dati sensibili di un utente o un'istituzione (username, password, coordinate bancarie, posizioni geografiche)





Phishing e IA



- **Superamento dei «segnali classici»**: le email di phishing non sono più facilmente riconoscibili attraverso errori grammaticali, design approssimativo o richieste inverosimili
- **Sofisticazione tramite IA**: L'intelligenza artificiale viene oggi utilizzata per creare campagne altamente personalizzate, credibili e difficili da distinguere dalle comunicazioni autentiche
- **Imitazione stilistica perfetta**: l'IA generativa permette di replicare fedelmente il tono e lo stile di messaggi legittimi
- **Abbattimento delle barriere linguistiche**: grazie all'IA, i cybercriminali possono scrivere correttamente anche in lingue che non conoscono
- **Targeting e Social Engineering**: Analizzando post sui social media, commenti e altri dati online, gli aggressori riescono a imitare lo stile comunicativo di persone specifiche, come colleghi o partner commerciali

- https://www.cybersecurity360.it/nuove-minacce/ai-e-deepfake-nuove-frontiere-del-phishing-come-difendersi/

Social Engineering con Deep Fake

Deep Fake

Deepfake indica contenuti fake (spesso video, ma non solo) **profondi** perché spesso prodotti mediante l'uso di **deep learning** (algoritmi basati su *Deep Neural Network*) per apprendere le caratteristiche verosimili da simulare e renderne difficili da individuarne la falsità, dunque anche nel significato di "falsi profondi"

I deepfake stanno diventando sempre più diffusi e convincenti. Un problema, quello della disinformazione, tanto rilevante da spingere autorità e istituzioni a normare il settore, oltre che informare il grande pubblico

- https://www.cybersecurity360.it/nuove-minacce/deep-fake-cosa-sono-e-come-riconoscerli-per-smascherare-la-disinformazione/

Social Engineering con Deep Fake

Deep Fake

Esistono tecnologie generative di IA che permettono di creare volti fotorealistici con nessuna attinenza a volti di persone reali (note e non)

FakeApp, altri software open source (ossia per cui è pubblicamente consultabile il codice sorgente) FaceSwap e DeepFaceLab e Reface sono stati realizzati per creare degli «Swap di volti»

Il **voice cloning**, o clonazione vocale, rappresenta oggi una delle minacce più concrete nel panorama della cyber security aziendale

- https://www.cybersecurity360.it/nuove-minacce/deep-fake-cosa-sono-e-come-riconoscerli-per-smascherare-la-disinformazione/

Social Engineering con Deep Fake

Deep Fake

Il 29 gennaio 2024, negli uffici di Hong Kong della multinazionale britannica Arup si è consumata una truffa che ha riscritto i parametri della criminalità informatica.

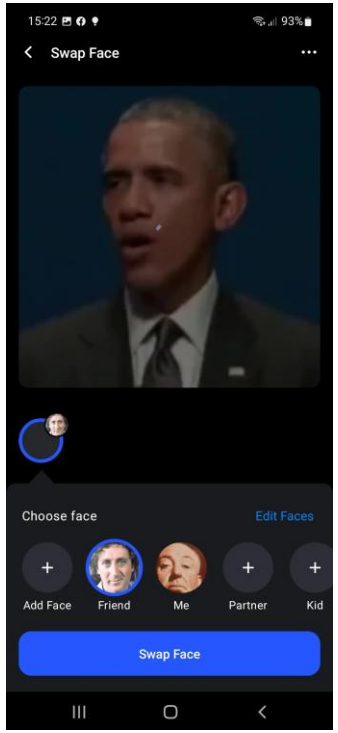
Un dirigente del settore finanziario, **dopo aver ricevuto una videochiamata** dal presunto direttore finanziario dell'azienda e da altri colleghi di alto livello**, ha autorizzato il trasferimento di 25,6 milioni di dollari statunitensi** distribuiti in quindici operazioni verso cinque conti bancari.

Tutti i partecipanti alla videoconferenza, ad eccezione della vittima, erano deepfake generati dall'intelligenza artificiale.

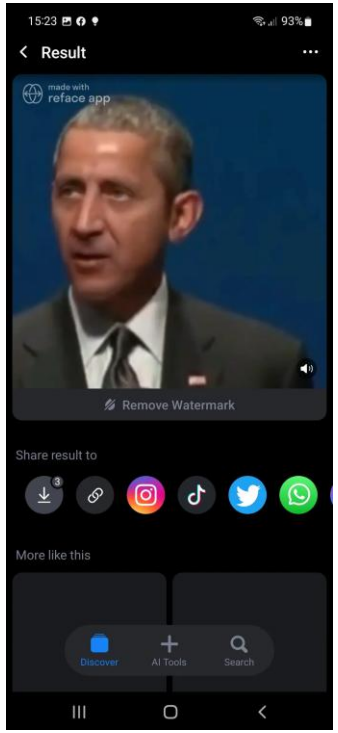
- https://www.ictsecuritymagazine.com/notizie/email-di-phishing/

Social Engineering con Deep Fake: un esempio di video fake

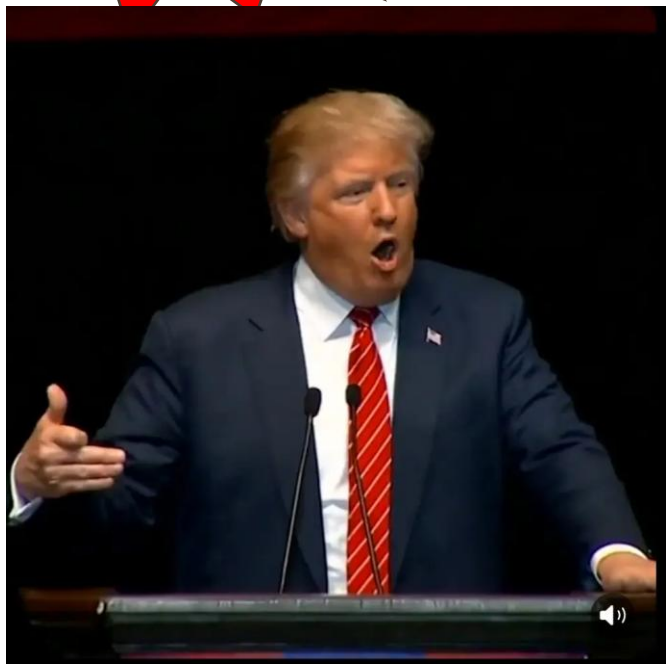
Deep Fake



Barack Obama



Gene Wilder



Donald Trump

Harrison Ford

https://www.cybersecurity360.it/nuove-minacce/deep-fake-cosa-sono-e-come-riconoscerli-per-smascherare-la-disinformazione/

Social Engineering con IA e Deep Fake: un esempio di voce fake

Deep Fake

Truffa del falso Crosetto, recuperati i soldi di Massimo Moratti: erano su un conto olandese

di Rosario Di Raimondo

L'ex presidente dell'Inter aveva consegnato quasi 980mila euro. Il ministro: "Ottimo lavoro dei magistrati e delle forze di polizia". L'imprenditore: "Carabinieri di una bravura incredibile"

- https://milano.repubblica.it/cronaca/2025/02/12/news/truffa_falso_crosetto_recuperati_soldi_moratti-423998861/

Cyberbullsimo: Minaccia all'incolumità

OPEN

ATTUALITÀ BOLOGNA · BULLISMO · EMILIA-ROMAGNA · GIOVANI · INCHIESTE · PEDOFILIA · SOCIAL MEDIA · SUICIDI

Il suicidio di Inquisitor Ghost in diretta su TikTok: «Mio figlio Vincent Plicchi accusato di adescamento e pedofilia»

14 OTTOBRE 2023 - 05:51 di Redazione

Due informative dei carabinieri sulla vicenda. Il padre Matteo denuncia un piano ordito da una minorenne e dal fidanzato

CORRIERE DELLA SERA — CORRIERE TORINO — ABBONATI — Accedi

IN EVIDENZA Ferragnez, la rottura: domenica l'ultima lite . E lei aveva già consultato un celebre divorzista

Il papà di Carolina Picchio: mia figlia, simbolo della lotta al cyberbullismo, ci insegna a saper ascoltare

di Paolo Picchio

Carolina Picchio morì suicida, a 14 anni, nel gennaio del 2013 dopo la diffusione sul web di un video a sfondo sessuale

Biella, consigliera assente per allattare: la polemica in aula in un video diffuso dal Pd

Solidarietà alla consigliera Marta Bruschi da parte del gruppo Pd alla Camera

- https://www.open.online/2023/10/14/bologna-suicidio-vincent-picchi-inquisitor-ghost-accuse-padre/
- https://torino.corriere.it/notizie/cronaca/23_marzo_13/il-papa-di-carolina-picchio-mia-figlia-simbolo-della-lotta-al-cyberbullismo-ci-insegna-a-saper-ascoltare-1cb1b2a3-2aee-4bbb-adbd-d45cf3639xlk.shtml

Cyber Security: recenti trend di Phishing

Finti colloqui di lavoro, la nuova frontiera delle frodi: come difendersi

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

Un fenomeno crescente che sfrutta diversi aspetti della catena di ricerca di lavoro. Annunci di offerte false, fraudolente ricerche di personale, tutto per carpire dati essenziali dalle vittime e, in alcuni casi, anche installare un ransomware

Pubblicato il 30 lug 2025

Dario Fadda
Research Infosec, fondatore Insicurezzadigitale.com

Sfruttamento della ricerca di lavoro: i criminali approfittano di chi cerca opportunità professionali online per diffondere strumenti di monitoraggio e gestione remota (RMM)

Conseguenze degli attacchi: queste tecniche aprono la strada a furti di dati, frodi finanziarie e installazione di malware o ransomware

Finti inviti a colloqui: vengono inviate e-mail fraudolente camuffate da inviti per piattaforme come Zoom o Microsoft Teams

Uso di software RMM legittimi: invece di un vero incontro, la vittima viene indotta a installare software RMM reali (come SimpleHelp, ScreenConnect o Atera) per permettere all'attaccante il controllo del sistema

- https://www.cybersecurity360.it/news/finti-colloqui-di-lavoro-la-nuova-frontiera-delle-frodi-come-difendersi/

Cyber Security: recenti trend di Phishing

Phishing su WooCommerce: come proteggersi dal malware travestito da patch di sicurezza

È stata identificata un'astuta campagna di phishing che sta prendendo di mira gli utenti di WooCommerce, il popolare plugin di e-commerce per WordPress. L'esca si presenta come un avviso ufficiale di sicurezza, ma nasconde una backdoor che può compromettere completamente un sito web. Come difendersi

Tutto parte da un'e-mail camuffata da comunicazione ufficiale, inviata **da indirizzi ingannevoli** afferenti a woocommerce"help @ security-woocommerce[.]com

Il messaggio avvisa l'utente di una **presunta vulnerabilità critica** denominata "Unauthenticated Administrative Access", invitandolo a installare urgentemente un aggiornamento di sicurezza

- https://www.cybersecurity360.it/news/finti-colloqui-di-lavoro-la-nuova-frontiera-delle-frodi-come-difendersi/

Cyber Security: recenti trend di Phishing

Blob URI: la nuova frontiera del phishing per aggirare i controlli di sicurezza

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

È stata identificata una nuova tecnica di phishing che usa i Blob URI, ossia URL per il browser validi solo all'interno della sessione dell'utente. Trattandosi di contenuti locali, tali link non possono essere analizzati dai tradizionali strumenti di sicurezza. Ecco i dettagli e i consigli per difendersi

Pubblicato il 12 mag 2025

Salvatore Lombardo
Funzionario informatico, Esperto ICT, Socio Clusit e autore

I cyber criminali hanno iniziato a sfruttare i Blob URI (indirizzi generati dal browser che puntano a dati temporanei memorizzati localmente nella memoria del browser stesso) per veicolare **pagine di phishing direttamente nel browser dell'utente**

Queste pagine appaiono legittime e funzionano come normali pagine web, ma in realtà sono **progettate per rubare credenziali o indurre l'utente a scaricare malware**

- https://www.cybersecurity360.it/news/finti-colloqui-di-lavoro-la-nuova-frontiera-delle-frodi-come-difendersi/

Cyber Security: recenti trend di Phishing

Darcula: ecco come hanno rubato 884.000 carte di credito tramite SMS

Home › Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

Le tipologie di truffe e i metodi usati dai cyber criminali sono in continua evoluzione per adattare le tecniche di attacco e proseguire nelle loro attività. Darcula, piattaforma di phishing as a service (PhaaS), è l'ultimo esempio di sfruttamento malevolo di tecnologie innovative. Ecco come funziona

Pubblicato il 8 mag 2025

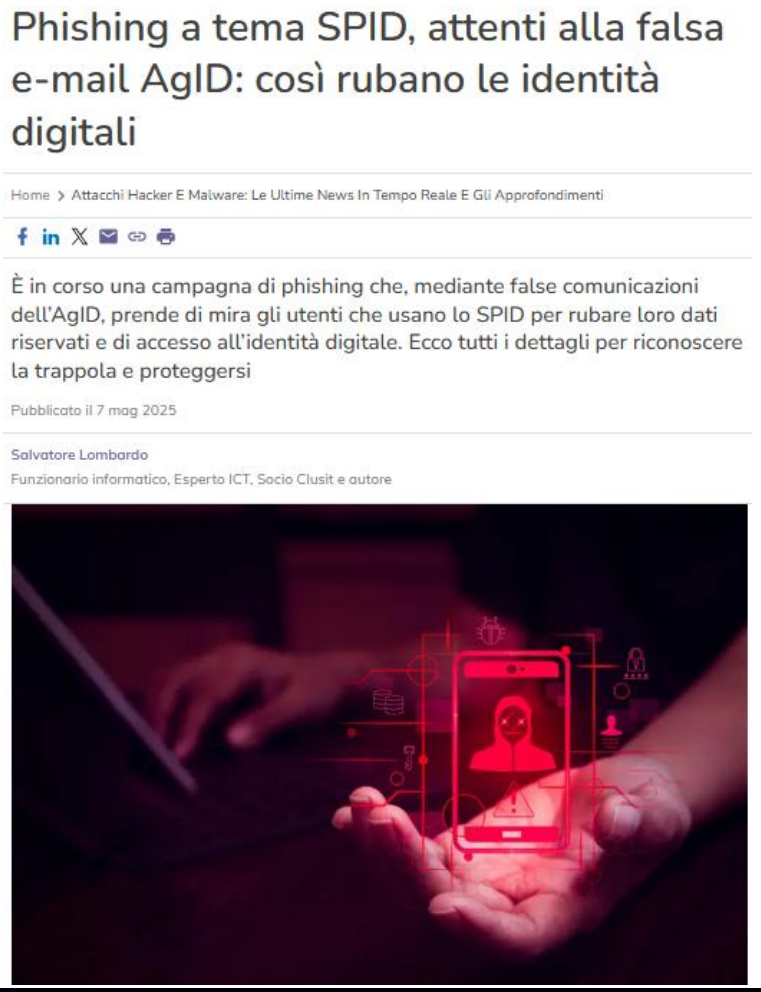
Dario Fadda

Research Infosec, fondatore Insicurezzadigitale.com

- **Rete di domini ingannevoli**: utilizza circa 20.000 domini fasulli che imitano brand famosi per trarre in inganno le vittime.
- **Canali di attacco**: sfrutta principalmente SMS e sistemi di messaggistica avanzata per veicolare i tentativi di phishing.
- **Tematiche comuni**: i messaggi simulano situazioni quotidiane, come la notifica di multe stradali o problemi con la spedizione di pacchi.
- **Automazione e gestione**: include un pannello di controllo semplificato che genera automaticamente kit di phishing per vari brand.
- **Monetizzazione rapida**: offre funzionalità per convertire i dati delle carte di credito rubate in carte virtuali, velocizzando il profitto illecito.
- **Utilizzo dell'IA Generativa**: integra modelli linguistici (LLM) per creare truffe personalizzate in qualsiasi lingua e su diversi argomenti, aumentandone l'efficacia

- https://www.cybersecurity360.it/news/finti-colloqui-di-lavoro-la-nuova-frontiera-delle-frodi-come-difendersi/

Cyber Security: recenti trend di Phishing



Phishing a tema SPID, attenti alla falsa e-mail AgID: così rubano le identità digitali

Home › Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

È in corso una campagna di phishing che, mediante false comunicazioni dell'AgID, prende di mira gli utenti che usano lo SPID per rubare loro dati riservati e di accesso all'identità digitale. Ecco tutti i dettagli per riconoscere la trappola e proteggersi

Pubblicato il 7 mag 2025

Salvatore Lombardo

Funzionario informatico, Esperto ICT, Socio Clusit e autore

Il sito malevolo mira a **sottrarre informazioni sensibili** tra cui **credenziali di accesso SPID**, **copie di documenti d'identità**, **video di riconoscimento**.

"L'obiettivo della campagna è sottrarre le credenziali SPID delle vittime, insieme a copie di documenti di identità e a video registrati secondo istruzioni specifiche per la procedura di riconoscimento, come: "Guarda verso la telecamera. Rimani serio, poi sorridi", spiegano nel rapporto gli analisti del CERT-AgID.

- https://www.cybersecurity360.it/news/finti-colloqui-di-lavoro-la-nuova-frontiera-delle-frodi-come-difendersi/

Cyber Security: recenti trend di Phishing

Attenzione all'e-mail truffa della multa non pagata

Matteo Polimeni
EDITOR E VIDEOMAKER

Negli ultimi mesi sempre più persone hanno ricevuto un'e-mail che parlava di una **"multa non pagata"**. Il messaggio sembra provenire da un ente ufficiale, usa loghi credibili e un tono formale, tanto da sembrare autentico a un primo sguardo. Ma dietro quelle parole si nasconde una trappola studiata nei minimi dettagli. Si tratta di una delle truffe online più diffuse del momento, capace di colpire anche gli utenti più attenti.

Come funziona la truffa della multa non pagata

La tecnica alla base è sempre molto semplice, e super efficace: fare leva sulla paura e sull'urgenza. Il messaggio, apparentemente inviato dal "**Sistema Nazionale delle Infrazioni Stradali"**, comunica che il destinatario non avrebbe ancora pagato una sanzione per una presunta sosta non autorizzata. L'e-mail riporta anche un importo preciso — solitamente 120 euro — e una minaccia: se il pagamento non avviene entro 48 ore, la cifra può triplicare.

Il mittente sembra affidabile: la mail mostra loghi ufficiali come PagoPA, un linguaggio amministrativo impeccabile e un'interfaccia grafica curata. Tutti elementi pensati per disorientare chi legge e spingerlo a cliccare sul link contenuto nel messaggio per **finalizzare il pagamento e risolvere la pratica amministrativa**. Ed è proprio lì che scatta la trappola: quel link non porta al portale della Pubblica Amministrazione, ma a un sito fraudolento, creato per rubare i dati bancari e svuotare i conti delle vittime.

- https://www.virgilio.it/video/email-truffa-multa-222838

Cyber Security: recenti trend di Phishing

BUONO A SAPERSI 10 DICEMBRE 2025 Condividi

Mancato pagamento pedaggio: la truffa segnalata da Autostrade

- **Modalità di contatto**: le vittime vengono approcciate tramite e-mail, SMS o messaggi su WhatsApp riguardo a un presunto pedaggio non pagato
- **Tono del messaggio**: la comunicazione è spesso perentoria, sollecitando un saldo immediato per evitare sanzioni o costi aggiuntivi
- **Sito web contraffatto**: il messaggio include un link a una pagina web che imita l'aspetto grafico e i loghi ufficiali per apparire legittima
- **Utilizzo dei dati rubati**: una volta inserite le informazioni, i criminali possono effettuare transazioni dirette o rivendere i dati a terzi
- **Rischi per l'utente**: le conseguenze includono perdite economiche e la compromissione della propria identità digitale

- https://www.virgilio.it/video/mancato-pagamento-pedaggio-truffa-phishing-autostrade-224916

Cyber Security: recenti trend di Phishing

- **Tecnica di installazione:** i truffatori applicano dispositivi falsi, chiamati skimmer, sopra i lettori di carte originali dei distributori automatici
- **Funzionamento dei dispositivi:** gli skimmer consentono di copiare i dati sensibili presenti sulle carte degli utenti
- **Strumenti aggiuntivi:** per completare il furto, vengono spesso utilizzate microcamere o tastierini contraffatti per registrare la digitazione del codice PIN
- **Utilizzo dei dati rubati:** le informazioni carpite vengono impiegate per effettuare pagamenti online o prelievi non autorizzati

- https://www.virgilio.it/video/truffa-distributore-benzina-199068

Cyber Security: recenti trend di Phishing

Truffa con PAYPAL

- **Sfruttamento di funzioni ufficiali**: la truffa utilizza una funzione legittima di PayPal relativa alla gestione degli abbonamenti ricorrenti
- **Notifiche automatiche**: il sistema viene attivato dalla piattaforma stessa, che invia un'e-mail automatica quando un pagamento ricorrente risulta sospeso
- **Manipolazione dei campi**: i truffatori creano finti abbonamenti e modificano i campi informativi inserendo la descrizione di un acquisto inesistente
- **Induzione al contatto**: il messaggio include un link e un numero di telefono che la vittima viene invitata a contattare per annullare l'operazione

- https://www.virgilio.it/video/truffa-paypal-phishing-225310

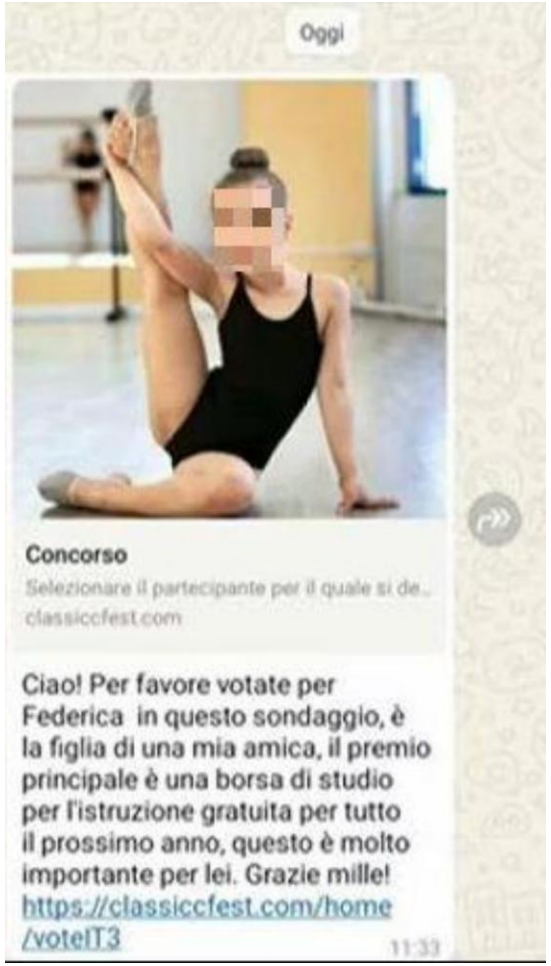
Cyber Security: recenti trend di Phishing

Truffa su WhatsApp

- **Piattaforme di origine**: i truffatori utilizzano i social network (Facebook, Instagram, ecc.) per pubblicare annunci sponsorizzati ingannevoli
- **Esche utilizzate**: i messaggi promettono vincite a concorsi, estrazioni a premi, regali tecnologici o buoni acquisto
- **Richiesta del numero**: per partecipare, viene richiesto all'utente di inserire il proprio numero di telefono collegato a un account WhatsApp attivo
- **Invio del codice di verifica**: l'utente riceve un codice alfanumerico di 8 cifre, generato automaticamente dall'app per registrare l'account su un nuovo dispositivo o attivare WhatsApp Web
- **Presa di controllo dell'account**: i criminali utilizzano il codice fornito per attivare una sessione WhatsApp Web

- https://www.virgilio.it/video/truffa-whatsapp-codice-8-cifre-225335

Cyber Security: recenti trend di Phishing



Truffa della «ballerina» su WhatsApp

- **Il pretesto dell'amicizia:** il messaggio cita una ragazza, spesso chiamata "Federica", presentata come la figlia di un'amica per creare un legame affettivo
- **Richiesta di supporto:** viene chiesto alla vittima di esprimere un semplice voto online per aiutarla
- **Falsa rassicurazione:** nel testo si specifica esplicitamente che non è richiesto alcun pagamento, aumentando la credibilità della richiesta
- **Meccanismo di Smishing:** la truffa sfrutta i servizi di messaggistica per indirizzare l'utente verso una pagina che imita un sito ufficiale
- **Sottrazione delle credenziali:** per "votare", alla vittima viene chiesto di inserire le proprie credenziali o un codice ricevuto via SMS
- **Fiducia nella rubrica:** l'efficacia è elevata perché i messaggi arrivano da numeri già presenti in rubrica (già compromessi), risultando affidabili agli occhi della vittima
- **Accesso e propagazione:** i truffatori ottengono il controllo dell'account WhatsApp della vittima per diffondere lo scam e inviare richieste di denaro ai suoi contatti

- https://tg24.sky.it/tecnologia/2026/01/12/truffa-della-ballerina-whatsapp
- https://adiconsum.it/truffa-della-ballerina-come-funziona-e-come-difendersi/

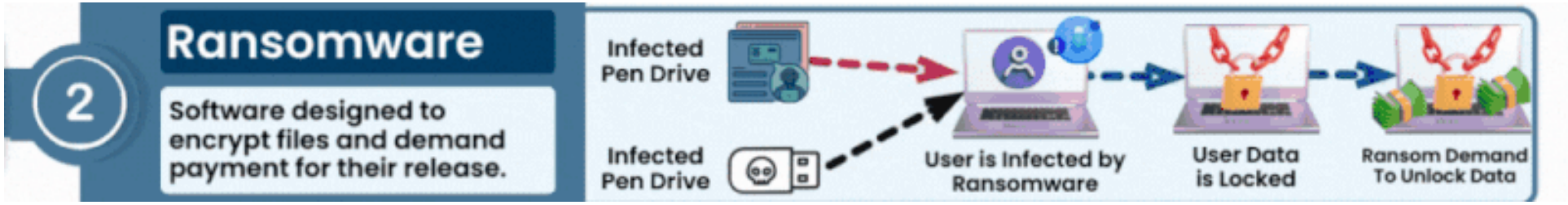
Cyber Security: recenti trend di Phishing

Truffa della tessera sanitaria

- **Oggetto dell'inganno**: la vittima riceve un'e-mail che segnala l'imminente scadenza della propria tessera sanitaria
- **Leva psicologica**: il messaggio fa leva sulla necessità di garantire la continuità delle prestazioni mediche e dei benefici sanitari per spingere l'utente ad agire subito
- **Azione richiesta**: viene suggerito di cliccare su un link allegato all'e-mail per richiedere tempestivamente il rinnovo
- **Sottrazione di dati personali**: il link rimanda a un modulo in cui inserire informazioni sensibili dell'intestatario.
- **Informazioni mirate**: i dati richiesti includono nome e cognome, data di nascita, indirizzo completo, numero di telefono e indirizzo e-mail

- https://www.virgilio.it/video/truffa-tessera-sanitaria-225755

Ransomware: minaccia agli enti



Rappresenta una tipologia di Malware (Malicious Software) che infettando il dispositivo colpito (PC, Smartphone, Database) limita l'accesso ai dati mediante criptazione del dato a scopo di riscatto

la Repubblica

L'attacco alla Regione Lazio è partito dal pc di un dipendente in smartworking

di Arturo Di Corinto, Bruno Ruffilli

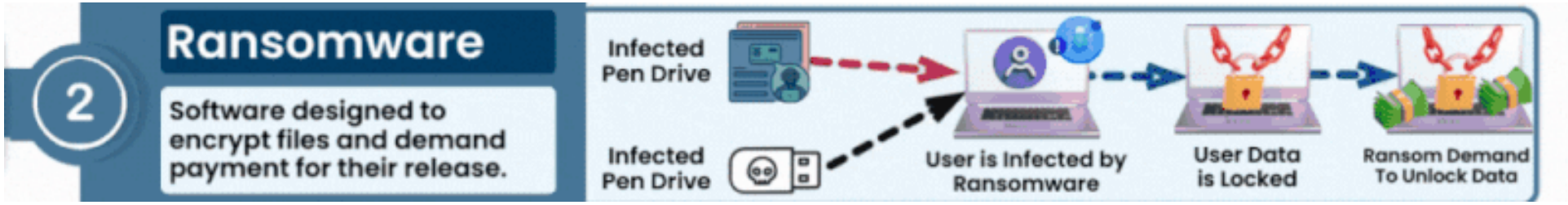
L'assessore alla Sanità Alessio D'Amato a Italian Tech: "Criptato e reso inutilizzabile anche il backup dei dati, ma il sistema delle prenotazioni per i vaccini tornerà a funzionare in tre giorni". Il ransomware utilizzato potrebbe essere RansomEXX, e non Lockbit 2.0 come si è detto finora

03 AGOSTO 2021 AGGIORNATO ALLE 21:13 — 3 MINUTI DI LETTURA

Vettore dell'attacco: l'intrusione è stata causata dalla violazione delle credenziali di un dipendente che lavorava in modalità smart working.
Fattore umano e attenzione: l'attacco ha sfruttato un momento di vulnerabilità legato al lavoro agile
Compromissione dei backup: l'aspetto più critico dell'evento è stata la cifratura dei backup dei dati, che ha impedito il ripristino immediato dei sistemi.
Natura del danno: i dati non sono stati trafugati, ma "immobilizzati" attraverso tecniche di crittografia (tipiche dei ransomware).

- https://www.repubblica.it/tecnologia/2021/08/03/news/l_attacco_alla_regione_lazio_e_partito_dal_pc_di_un_dipendente_in_smartworking-312819783/

Ransomware: minaccia alla sanità



Rappresenta una tipologia di Malware (Malicious Software) che infettando il dispositivo colpito (PC, Smartphone, Database) limita l'accesso ai dati mediante criptazione del dato a scopo di riscatto


MILANOTODAY

MT

Redazione

25 aprile 2023 22:05

ATTUALITÀ

Secondo attacco hacker in 4 giorni: pronto soccorso e ospedali di nuovo in tilt

Il nuovo attacco al gruppo MultiMedica, che comprende il San Giuseppe di Milano e l'ospedale di Sesto

Si parla di

hacker

sanità

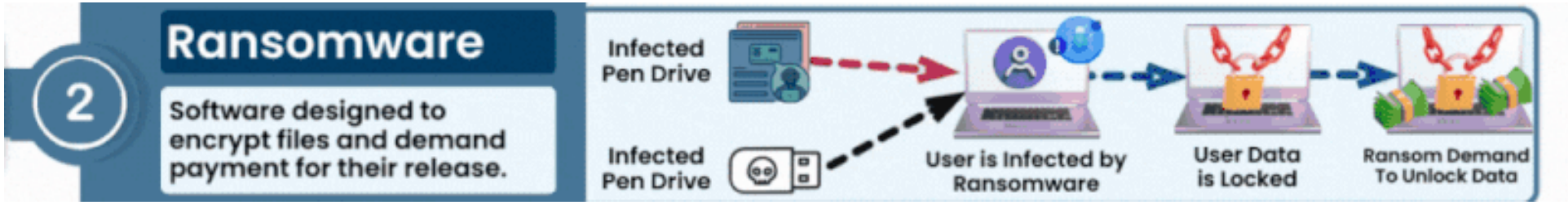
Un ambulatorio dell'ospedale San Giuseppe - Foto LaPresse

Sequenza degli eventi: la struttura ha subito due attacchi hacker in pochi giorni

Servizi sospesi: a causa del blocco dei sistemi, sono state sospese tutte le attività ambulatoriali, il ritiro dei referti e l'accettazione di nuove ambulanze nei Pronto Soccorso

- https://www.milanotoday.it/attualita/hacker-ospedali-multimedica.html

Ransomware: minaccia ai trasporti



Rappresenta una tipologia di Malware (Malicious Software) che infettando il dispositivo colpito (PC, Smartphone, Database) limita l'accesso ai dati mediante criptazione del dato a scopo di riscatto

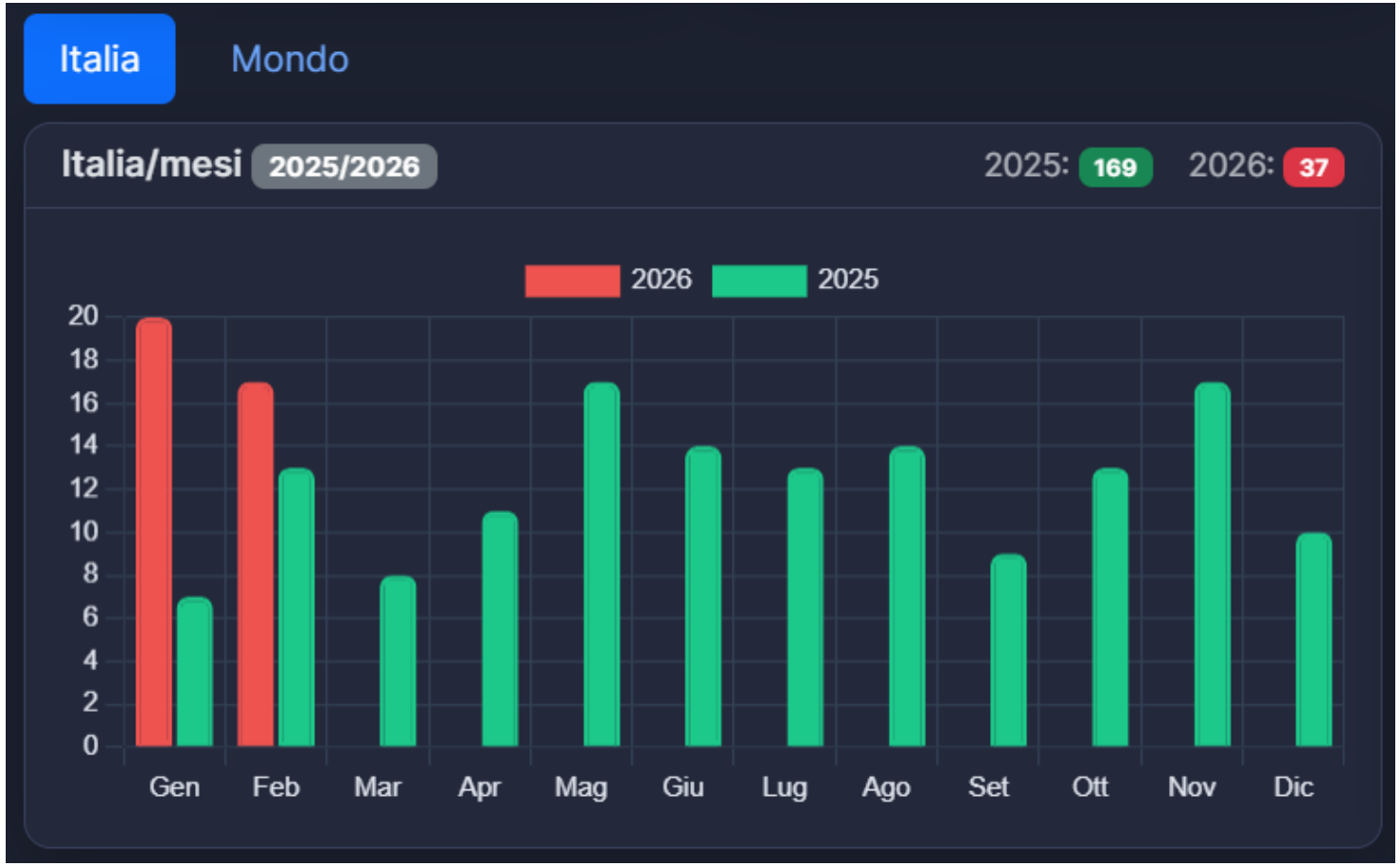
Tipologia di attacco: i sistemi informatici sono stati colpiti da un ransomware
Servizi compromessi: l'attacco ha causato il blocco delle biglietterie fisiche nelle stazioni e dei terminali self-service in tutta Italia
Responsabilità e riscatto: gli hacker hanno richiesto un riscatto in criptovalute (milioni di dollari) per fornire la chiave di decrittazione
Vettore dell'intrusione: il virus sarebbe stato introdotto compromettendo l'account di un amministratore di sistema o di un gestore dei servizi informatici

- https://www.corriere.it/tecnologia/22_marzo_23/trenitalia-bloccata-hacker-biglietterie-self-service-non-funzionano-fe4d6004-aaa2-11ec-89dc-0e9cfd23fb65.shtml

Ransomware: osservatorio costante

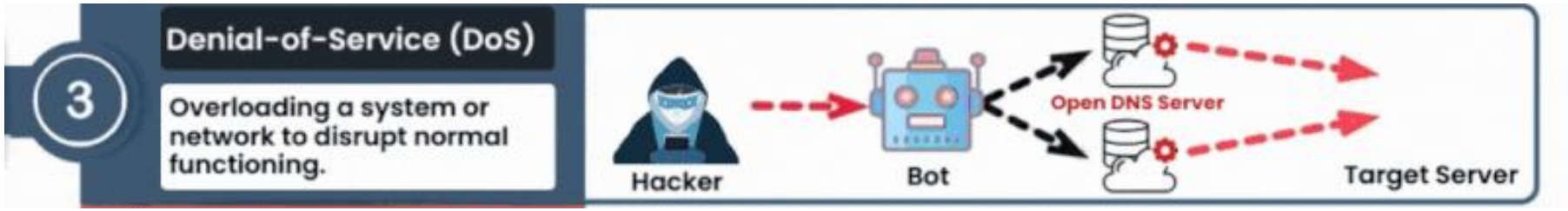
- https://ransomfeed.it/

Ransomware: osservatorio costante



- https://ransomfeed.it/

DDoS: Distributed Denial of Service



Rappresenta il tentativo di bloccare o interrompere il corretto funzionamento di un servizio (Server, Pc, Database, dispositivi di rete) mediante l'invio di traffico dati anomalo


CORRIERE DELLA SERA

LOGIN:

ABBONATI Accedi

IN:EVIDENZA Domande & Guide Quiz & Meme La Scelta Giusta CampBus Colazioni Digitali Chi Siamo

Attacco hacker ai siti italiani, cosa sappiamo: cos'è lo Slow Http Attack

diPaolo Ottolina

Nuova offensiva di un collettivo (filo)russo, NoName057. Non sono stati violati i perimetri dei siti, ma affossati i server con un attacco di tipo DDoS (

CORRIERE TV

I primi video generati da Sora, la nuova intelligenza artificiale di Open AI


SOSTIENICI

il Fatto Quotidiano

Fondazione FQ

CRONACA

Attacco hacker a tre aeroporti italiani: "Rivendicati da un gruppo sedicente filo-palestinese"

di F. Q. | 25 OTTOBRE 2023

Un **attacco hacker** ha colpito **tre aeroporti italiani**: quelli di **Valle d'Aosta**, **Calabria** e **Puglia**. Gli attacchi sono di **tipo Ddos** (Distributed denial of service) ed hanno determinato rallentamenti nei siti degli scali. A rivendicare l'azione è stato il gruppo **Mysterious team Bangladesh**, già noto in passato per attacchi nei Paesi


Attacco hacker russo all'Italia: colpiti siti di banche, porti e aziende

Gli hacker filorussi NoName057(16) hanno colpito l'Italia martellando i siti di banche, porti e aziende. Questa volta hanno agito insieme ai filopalestinesi di Alixsec

Mauro Di Gregorio
GIORNALISTA POLITICO-ECONOMICO

Pubblicato: 12 Gennaio 2025 13:00

CONDIVIDI

Attacchi alle infrastrutture critiche

- **Contesto**: Centrale di Natanz, Iran (2010)
- **Target**: PLC Siemens S7-300 e convertitori di frequenza
- **Vettore**: Chiavetta USB (Air-gap bypass)
- **Danno fisico**: Distruzione meccanica di 1.000 centrifughe per l'uranio
- **Key Takeaway**: Il software può distruggere l'hardware fisico

Langner R., "Stuxnet: Dissecting a Cyberwarfare Weapon"Rivista: IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51. Anno 2011

Attacchi alle infrastrutture critiche

- **Contesto**: Ivano-Frankivsk, Ucraina (2015-2016)
- **Target**: Sistemi SCADA e interruttori di circuito
- **Vettore**: Spear-phishing e malware BlackEnergy/Industroyer
- **Impatto**: 230.000 persone senza energia elettrica per ore
- **Key Takeaway**: Primo caso di blackout nazionale causato da cyber-attacco

Liang G., Weller S. R., Zhao, J., Luo, F., Dong, Z. Y, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks", IEEE Transactions on Power Systems. Anno 2016

Attacchi alle infrastrutture critiche

- **Contesto**: Impianto petrolchimico, Arabia Saudita (2017)
- **Target**: Schneider Electric Triconex Safety Instrumented System (SIS)
- **Obiettivo**: Disattivare i sistemi di emergenza (safety layers)
- **Pericolo**: Rischio di esplosione o rilascio di gas tossici
- **Key Takeaway**: Malware progettato per colpire la sicurezza umana (Life Safety)

Di Pinto A., Dragoni Y., Carcano, "TRITON: The First Malware to Attack Industrial Safety Systems", Conferenza Black Hat USA, Anno 2018.

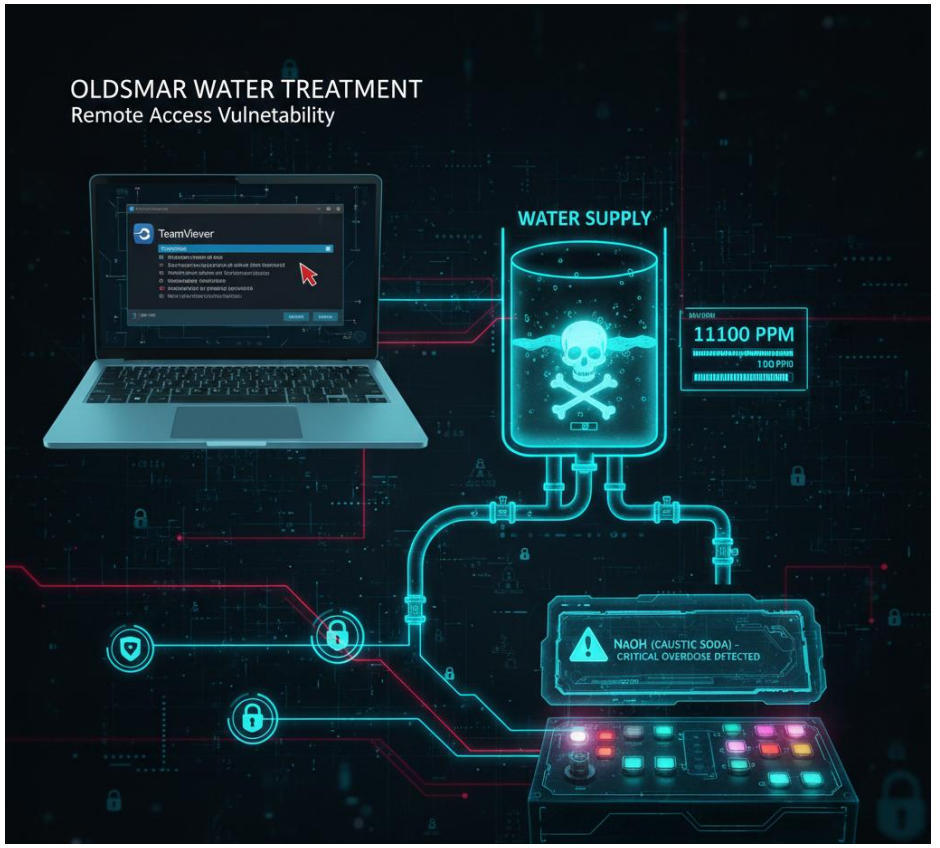
Attacchi alle infrastrutture critiche

- **Contesto**: Costa Orientale, USA (2021)
- **Target**: Rete aziendale IT (Billing e Management)
- **Vettore**: Password compromessa su VPN senza MFA
- **Conseguenza**: Chiusura precauzionale di 5.500 miglia di oleodotto
- **Key Takeaway**: L'interdipendenza IT-OT rende critica anche la rete gestionale

Di Mase D., et al, "Supply Chain Cybersecurity: Lessons from the Colonial Pipeline Attack", CISA - Cybersecurity and Infrastructure Security Agency. Anno 2021

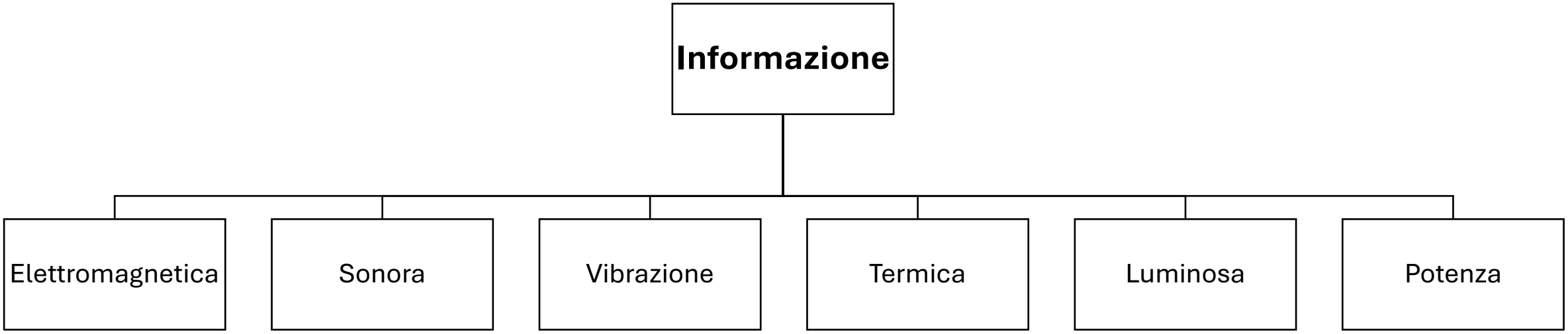
Attacchi alle infrastrutture critiche

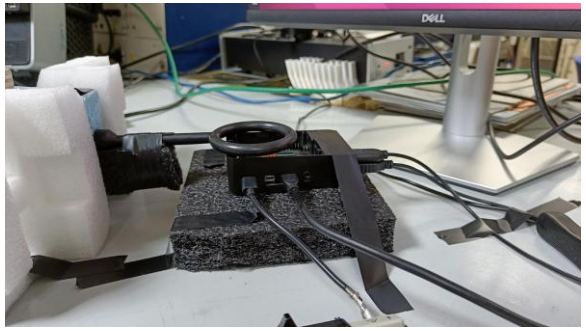
- **Contesto**: Florida, USA (2021)
- **Target**: Sistema di controllo chimico dell'acqua potabile
- **Vettore**: Abuso di software desktop remoto (TeamViewer)
- **Azione**: Tentativo di aumentare la soda caustica da 100 a 11.100 ppm
- **Key Takeaway**: Vulnerabilità degli accessi remoti nelle utility municipali

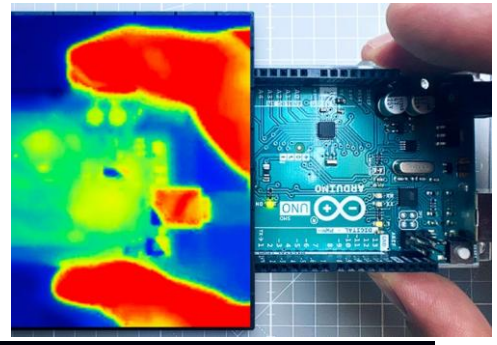


Barker I., "The Oldsmar hack: A wake-up call for water security", Security Journal, Anno 2021.

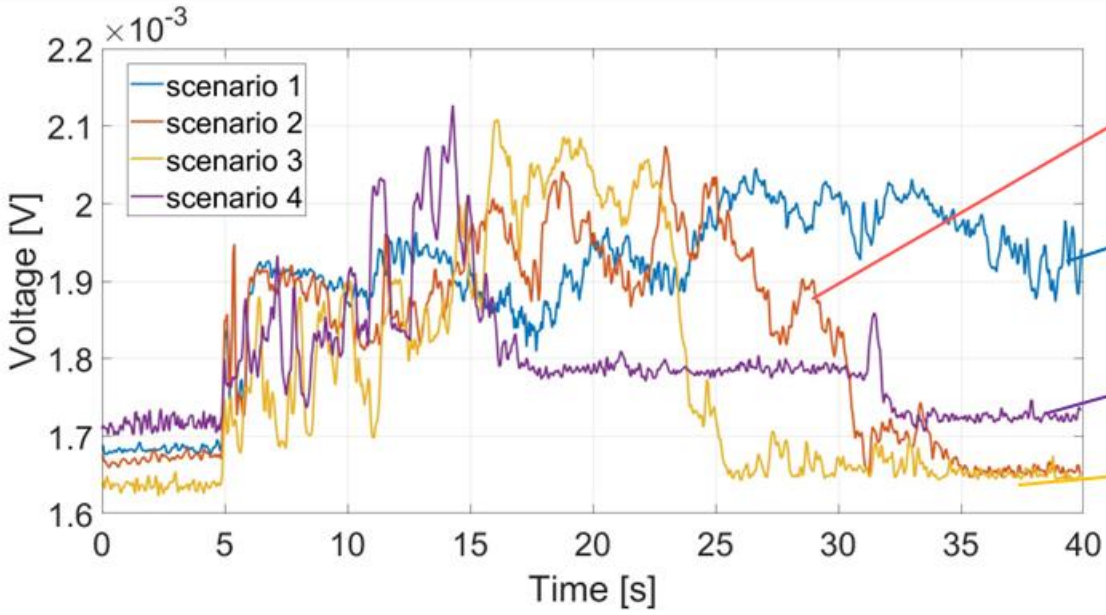
Non solo attacchi a software e network ma anche ai dispositivi…: Side-Channel Attack

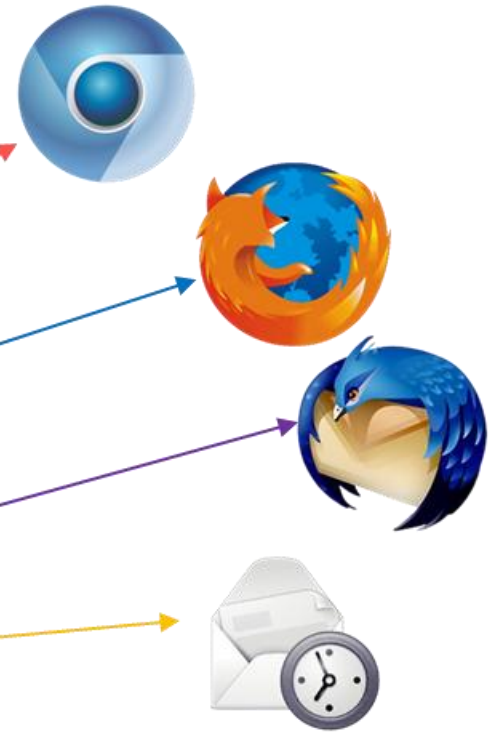






Non solo attacchi software e network ma anche ai dispositivi…: Side-Channel Attack



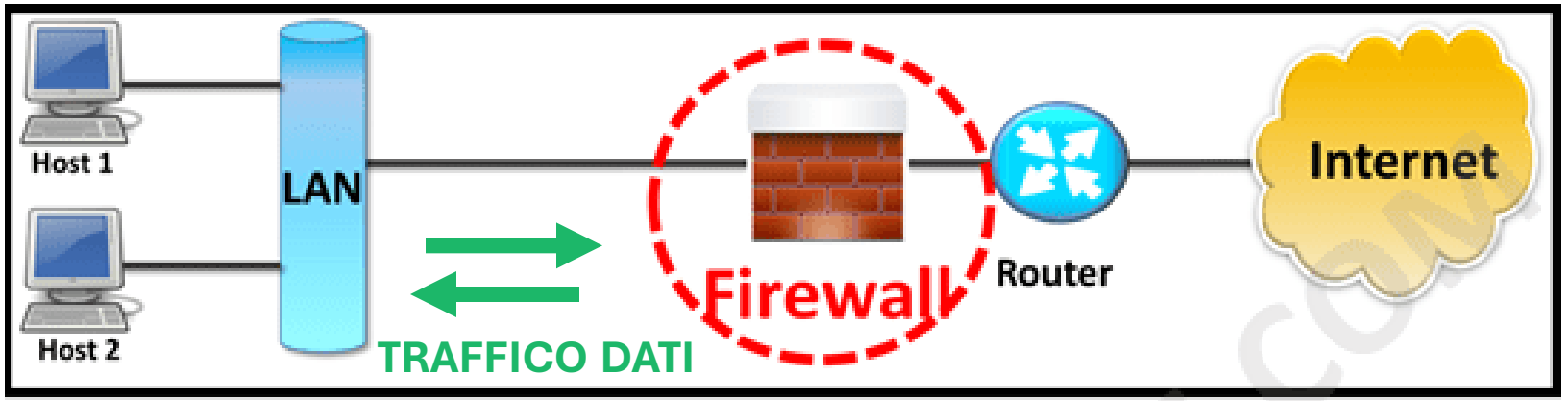


V. Rega, D. Capriglione, F. Marignetti, M. Molinara and A. Amodei, "Profiling Running Applications in Connected Devices Through Side-Channel and Machine Learning Techniques," in IEEE Access, vol. 12, pp. 170923-170935, 2024, doi: 10.1109/ACCESS.2024.3491916.

AGENDA

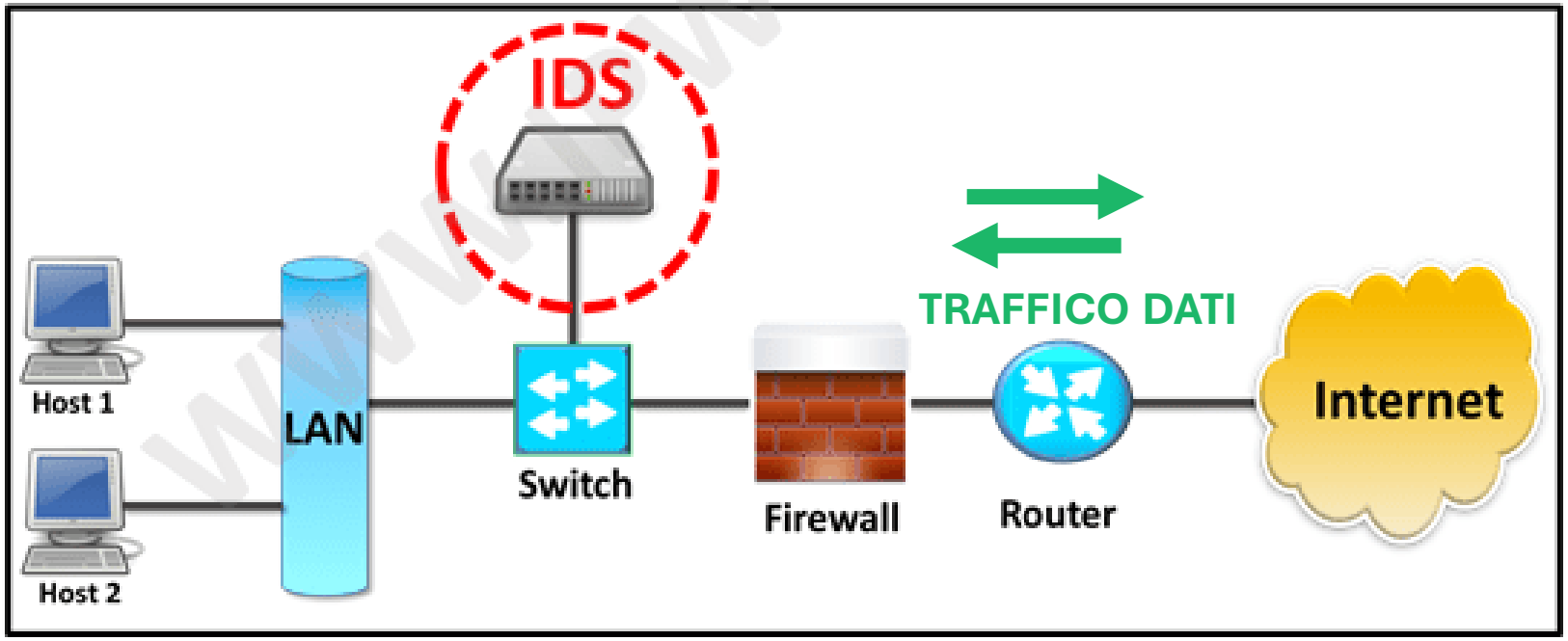
- INTRODUZIONE ALLA CYBERSECURITY
- UNO SGUARDO ALLE RECENTI DIRETTIVE, NORME E REGOLAMENTI
- TIPOLOGIA DI ATTACCHI INFORMATICI: ESEMPI E RUOLO DEL IA
- **POSSIBILI CONTROMISURE**

Cyber Security: Contromisure tecniche



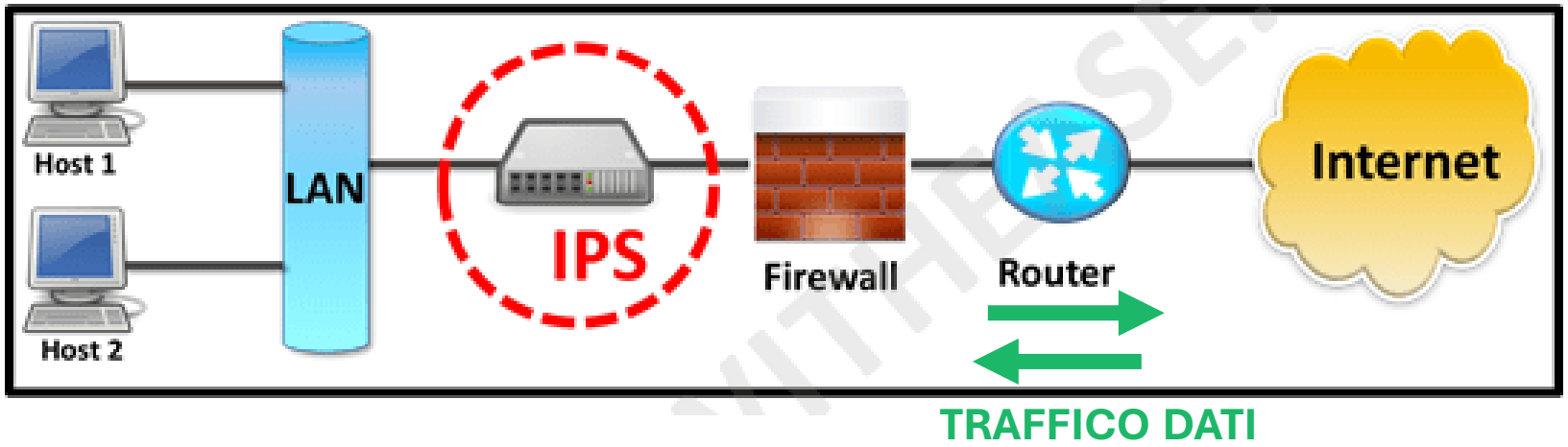
- ✓ Utilizza regole di controllo
- ✓ Blocca il traffico

Cyber Security: Contromisure tecniche



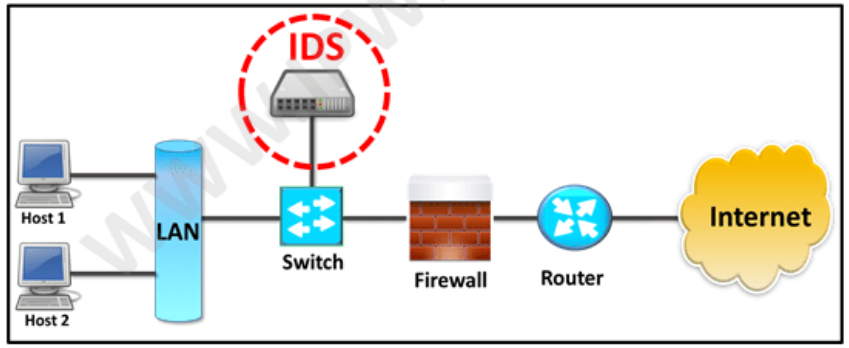
- ✓ Monitora il traffico in ingresso e in uscita
- ✓ Passivo (Posizionato dopo il firewall)
- ✓ Invia alert

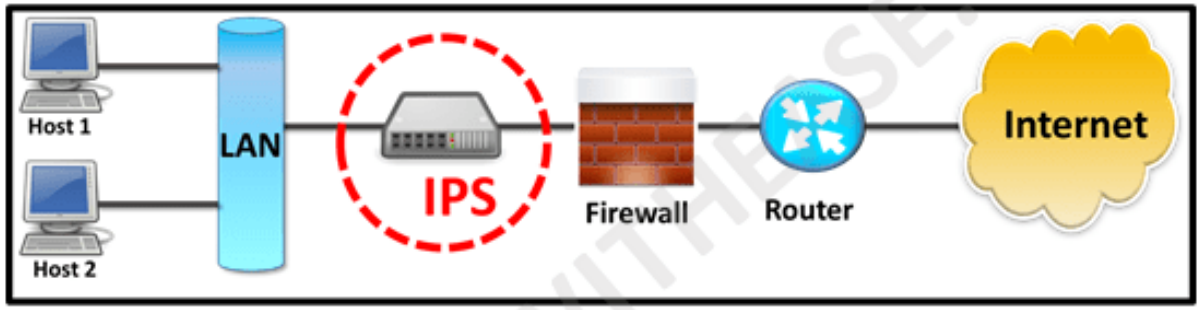
Cyber Security: Contromisure tecniche



- ✓ Ispeziona il traffico in ingresso e in uscita
- ✓ Attivo («In linea» dopo il firewall)
- ✓ Blocca tramite regole e policy di controllo

Cyber Security: Contromisure tecniche





L'AI PER MIGLIORARE LA CAPACITÀ DI RILIEVO DELLE INTRUSIONI

- ✓ I sistemi basati su AI e ML hanno la capacità significativa di rilevare minacce precedentemente sconosciute (attacchi zero-day) attraverso anomaly detection e pattern recognition
- ✓ L'anomaly detection è fondamentale nell'analisi del traffico di rete per identificare attacchi DDoS, tentativi di intrusione di rete e altri pattern sospetti che indicano accessi non autorizzati

ALCUNE REGOLE FONDAMENTALI

- Password Forti e Autenticazione Multi-Fattore (MFA): Creare password uniche, complesse e attivare l'MFA ovunque possibile
- Diffidare di Email e Link Sospetti: Non aprire allegati sconosciuti, non cliccare su link sospetti e verificare sempre il mittente
- Aggiornamenti Costanti: Mantenere sempre aggiornati sistemi operativi, browser e tutte le applicazioni
- Backup Regolari: Eseguire copie di sicurezza dei dati importanti per proteggerli in caso di perdita o attacco
- Attenzione alle Reti Wi-Fi Pubbliche: Evitare di usare reti pubbliche per operazioni sensibili
- Software e Download Sicuri: Installare programmi solo da fonti ufficiali e affidabili, evitare fonti sconosciute

ALCUNE REGOLE FONDAMENTALI

- Gestione Dati e Privacy: Non condividere password e non utilizzare la stessa password su diversi servizi, fare attenzione a cosa si pubblica sui social e usare in modo attento i servizi cloud
- Riconoscere e Segnalare Anomalie
- Intelligenza Artificiale (IA) e Chatbot: Usare con cautela per attività generiche, mai per dati sensibili o critici
- Non fidarsi di richieste di trasferimenti di denaro
- Fare sempre logout se ci si allontana dal proprio computer
- Attenzione a orecchie e occhi indiscreti
- Formazione Continua

Cyber Security – TRIADE CIA

Come assicurare i tre principi chiave della sicurezza informatica ?

CONFIDENZIALITA’

- Garantibile da algoritmi di crittografia:
  - AES (Advanced Encryption Standard)
  - DES (Data Encryption Standard)
  - 3DES (Triple Data Encryption Standard)

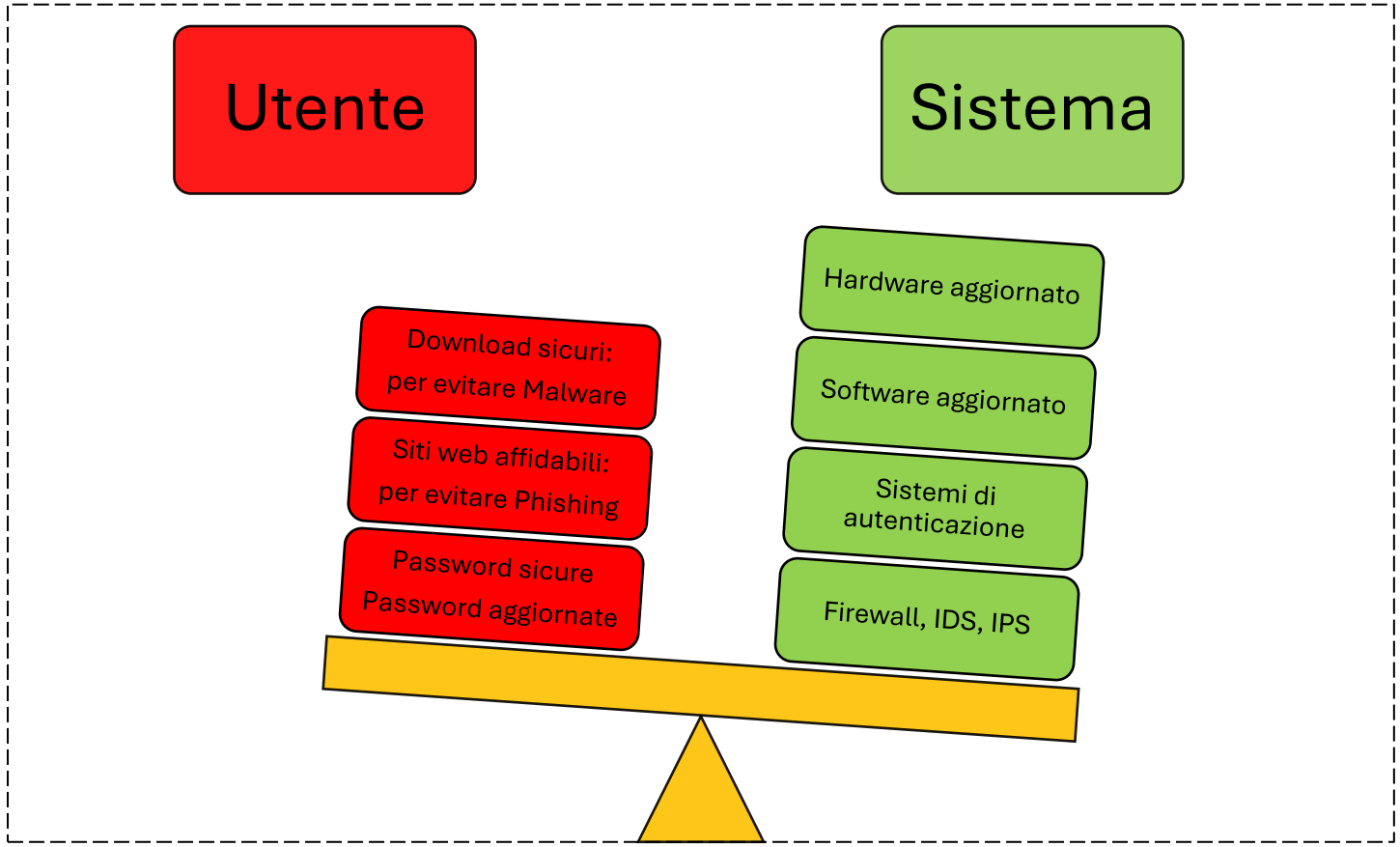
INTEGRITA’

- Garantibile con:
  - Restrizioni accessi
  - Intrusion Detection Systems

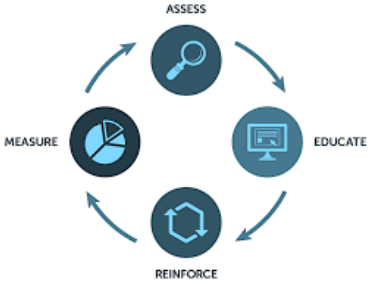
DISPONIBILITA’

- Garantita con:
  - Hardware e software aggiornati
  - Ridondanza

Cyber Security: Contromisure tecniche e personali



FORMAZIONE



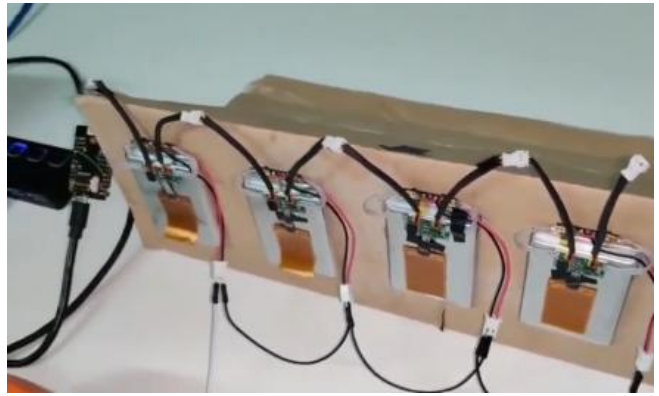
Alcuni esempi di attività di ricerca e progetti sulla Cyber Security: *ethical hacking-vulnerability analysis*

EMC²LAB

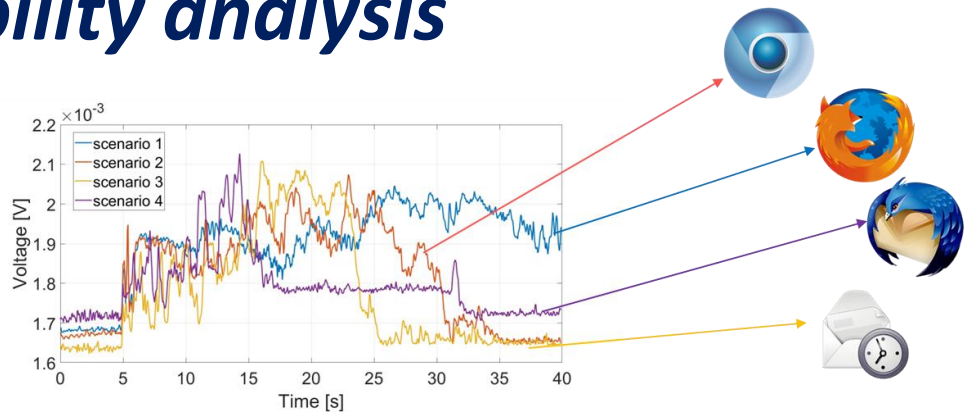
Electromagnetic Compatibility & Cyber Intelligence Laboratory

AIDA

Artificial Intelligence Laboratory



Alcuni esempi di attività di ricerca e progetti sulla Cyber Security: *ethical hacking-vulnerability analysis*



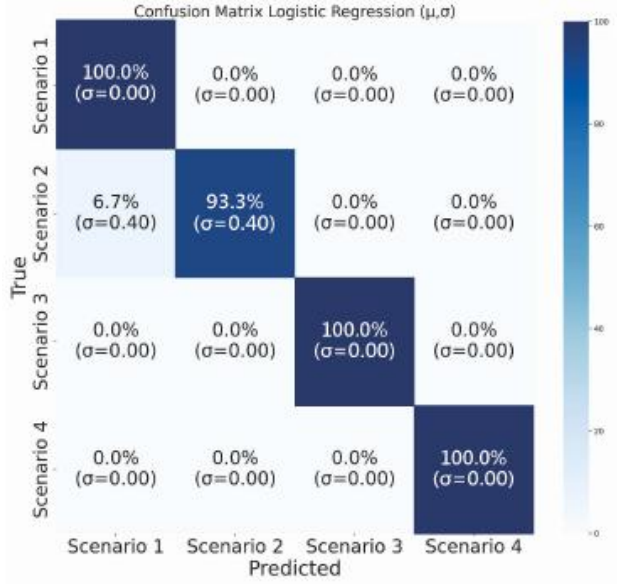
Tecniche di Intelligenza Artificiale

DUT
Raspberry Pi 4
Model B

Probe
ETS Lindgren 7406-901
[1 kHz ÷ 3 GHz]

Oscilloscope
TiePie HS6
[0 Hz ÷ 250 MHz]

PC Desktop



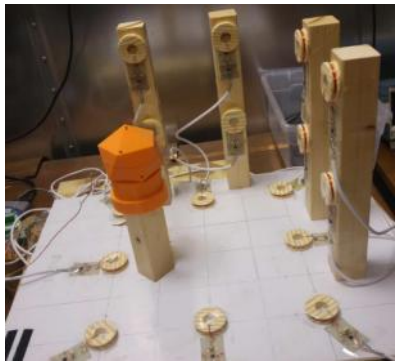
Alcuni esempi di attività di ricerca e progetti sulla Cyber Security: *Il progetto CyberGuardEV (Sistema Integrato per la Sicurezza Informatica nelle Stazioni di Ricarica per Veicoli Elettrici)*

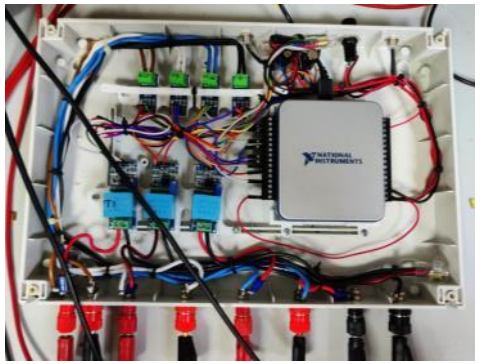
EMC²LAB

Electromagnetic Compatibility & Cyber Intelligence Laboratory (https://www.unicas.it/emclab/)

LAMI

Laboratorio di Misure Industriali (https://www.unicas.it/lami/)





Alcuni esempi di attività di ricerca e progetti sulla Cyber Security: *Il progetto CyberGuardEV (Sistema Integrato per la Sicurezza Informatica nelle Stazioni di Ricarica per Veicoli Elettrici)*

TME SRL (CAPOFILA)

ALFAGREEN SOLUTIONS SRL ← Spin-off UNICAS

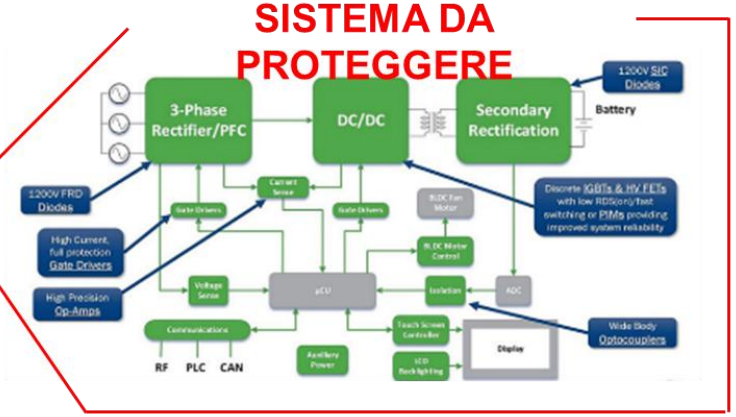
UNICAS

UNIPD

Alcuni esempi di attività di ricerca e progetti sulla Cyber Security: *Il progetto CyberGuardEV (Sistema Integrato per la Sicurezza Informatica nelle Stazioni di Ricarica per Veicoli Elettrici)*

COLONNINA DI RICARICA FAST CHARGE (DC)

SISTEMA DA PROTEGGERE



ADD-ON DA REALIZZARE

COMMUNICATION LAYER

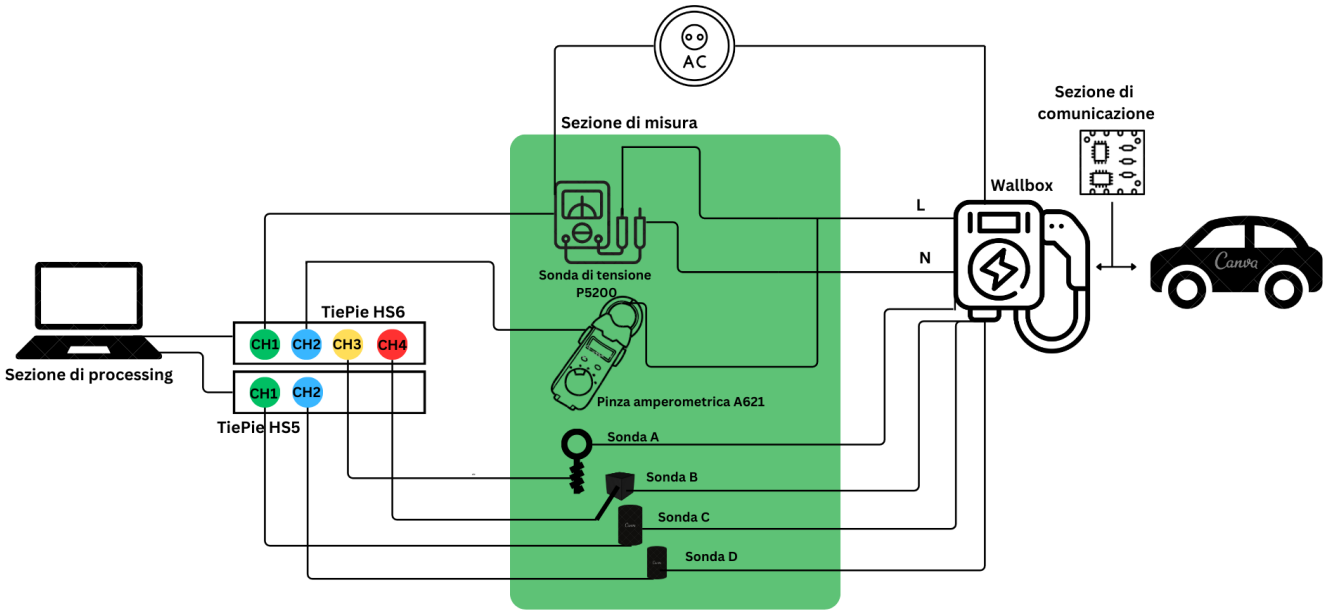
DATA ACQUISITION AND PROCESSING LAYER

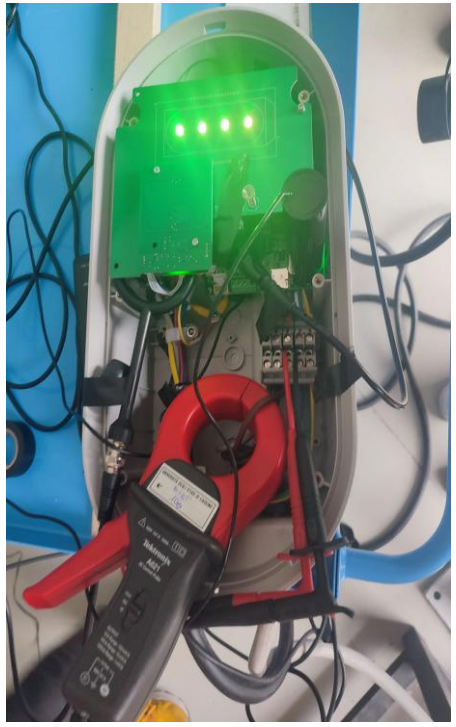
SENSOR LAYER

H-field probe

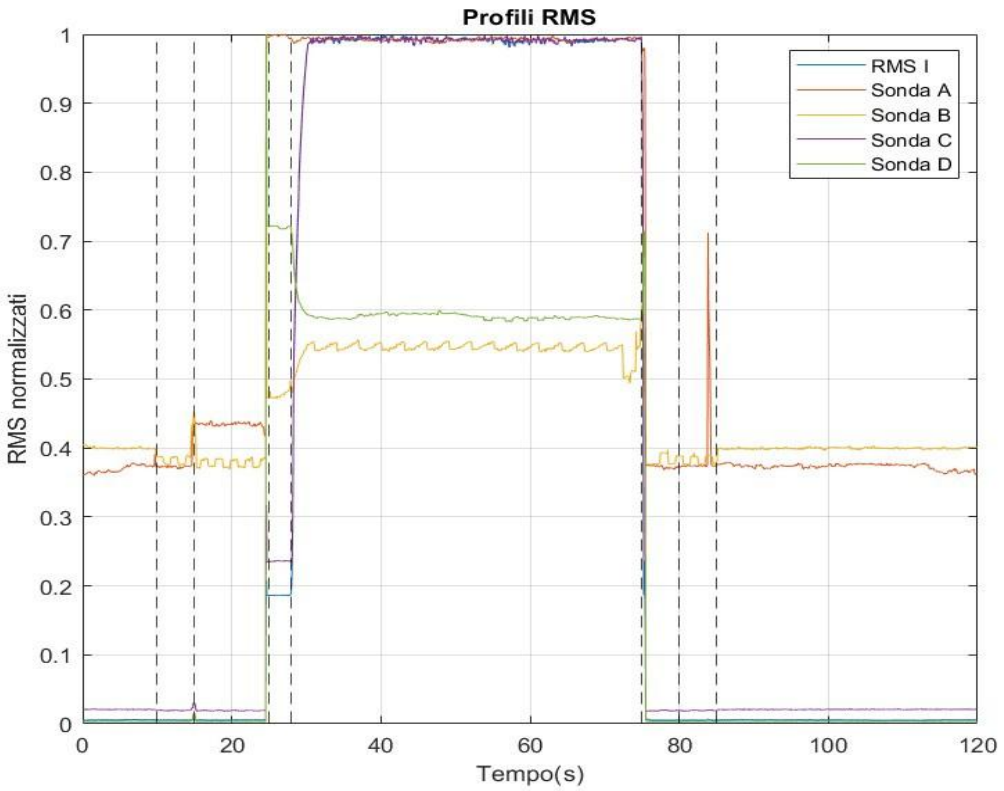
Current probe

Alcuni esempi di attività di ricerca e progetti sulla Cyber Security: *Il progetto CyberGuardEV (Sistema Integrato per la Sicurezza Informatica nelle Stazioni di Ricarica per Veicoli Elettrici)*



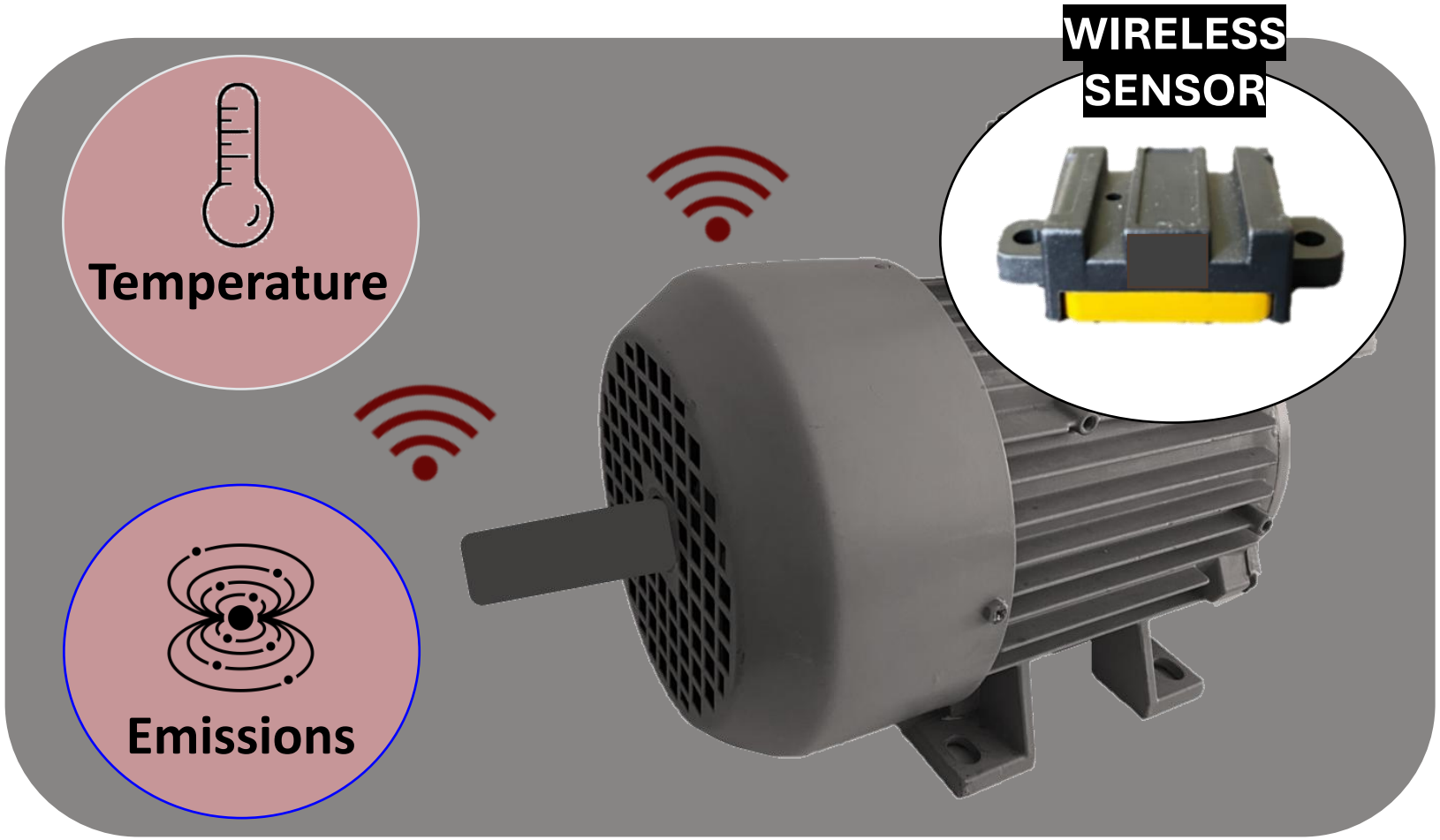


Alcuni esempi di attività di ricerca e progetti sulla Cyber Security: *Il progetto CyberGuardEV (Sistema Integrato per la Sicurezza Informatica nelle Stazioni di Ricarica per Veicoli Elettrici)*



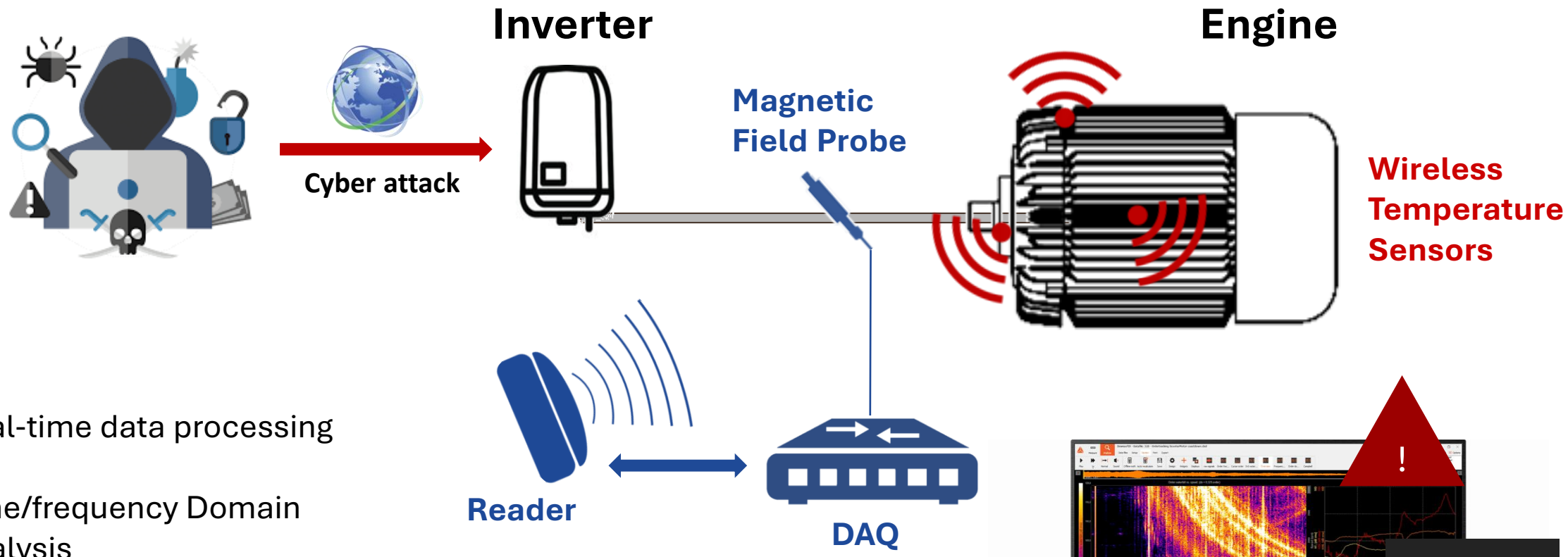
STATO	Tempo (s)	Evento
Stato 0	Da t=0 a t=10 Da t=85 a t=120	Stato di riposo Fine ricarica
Stato 1	Da t=10 a t=15 Da t=75 a t=80	Plug-in Dopo deautenticazione
Stato 2	Da t=15 a t=25	Autenticazione
Stato 3	Da t=25 a t=28	Pre-carica
Stato 4	Da t=28 a t=75	Ricarica attiva
Stato 5	Da t=80 a t=85	Car-out; Plug-out

DEMO 1: Intrusion Detection System per applicazioni industriali



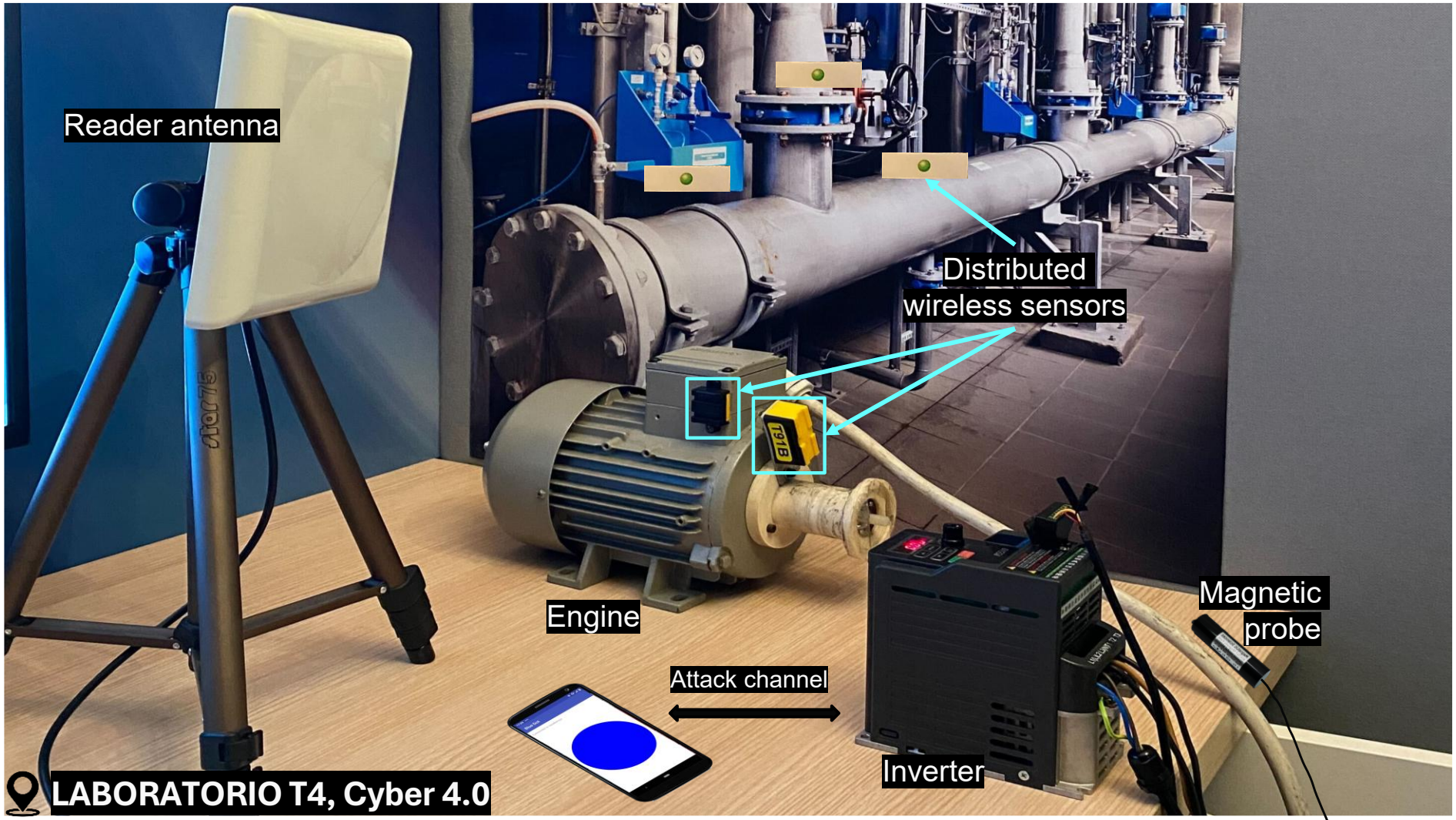
- Zero/Low power batteryless wireless sensors
- Low enviromental impact
- Great capillarity
- Monitoring of the inacessible

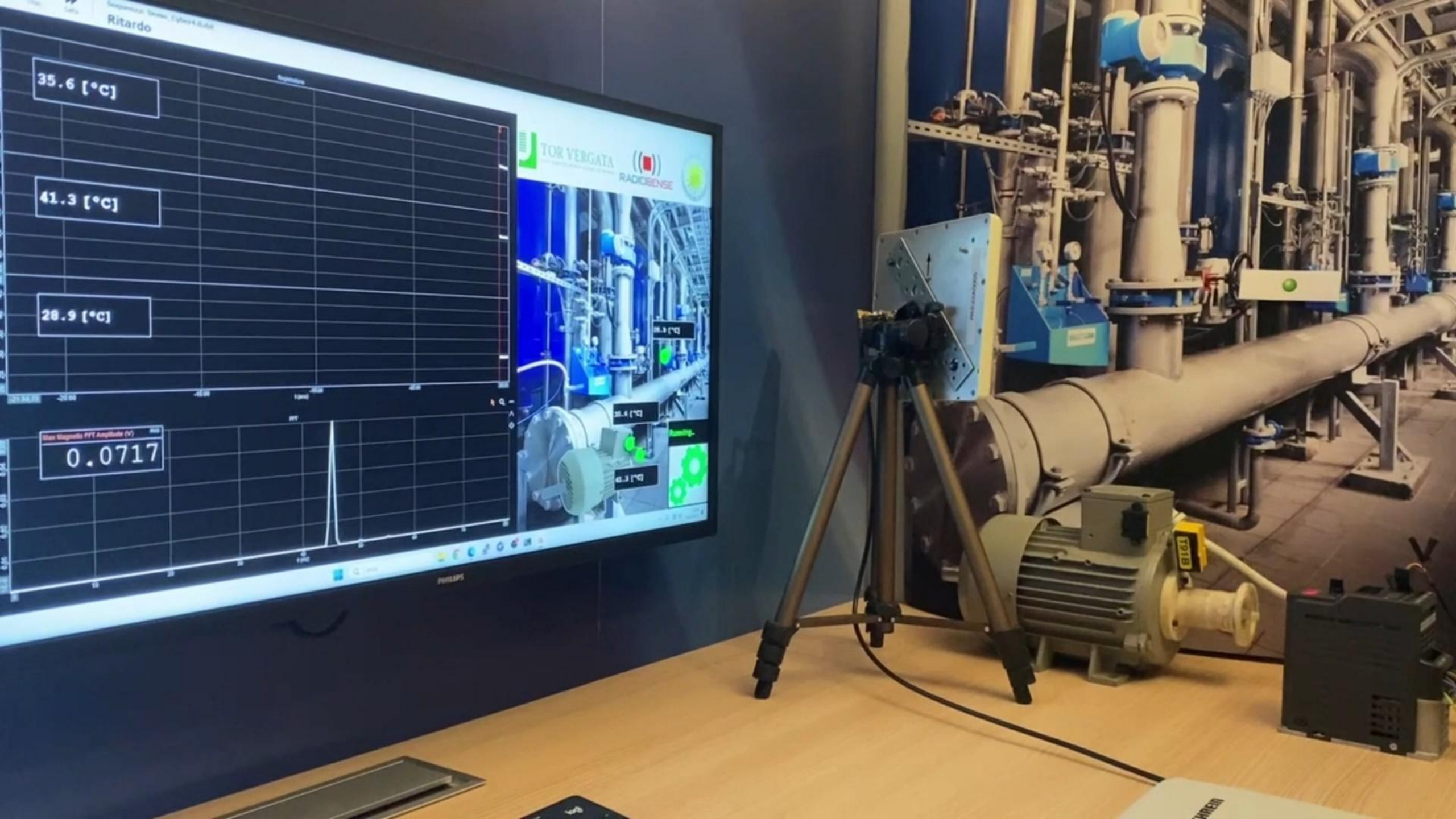
DEMO 1: Intrusion Detection System per applicazioni industriali



- Real-time data processing
- Time/frequency Domain Analysis
- EM/Thermal fingerprinting

DEMO 1: Intrusion Detection System per applicazioni industriali

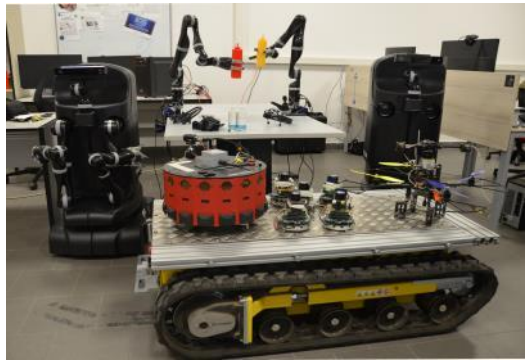



Ritardo
35.6 [°C]
41.3 [°C]
28.9 [°C]
0.0717
TOR VERGATA
RADIOBENSE
PHILIPS

Alcuni esempi di attività di ricerca e progetti sulla Cyber Security: *penetration testing*

LAI

Robotics Laboratory
(https://www.unicas.it/lai/)



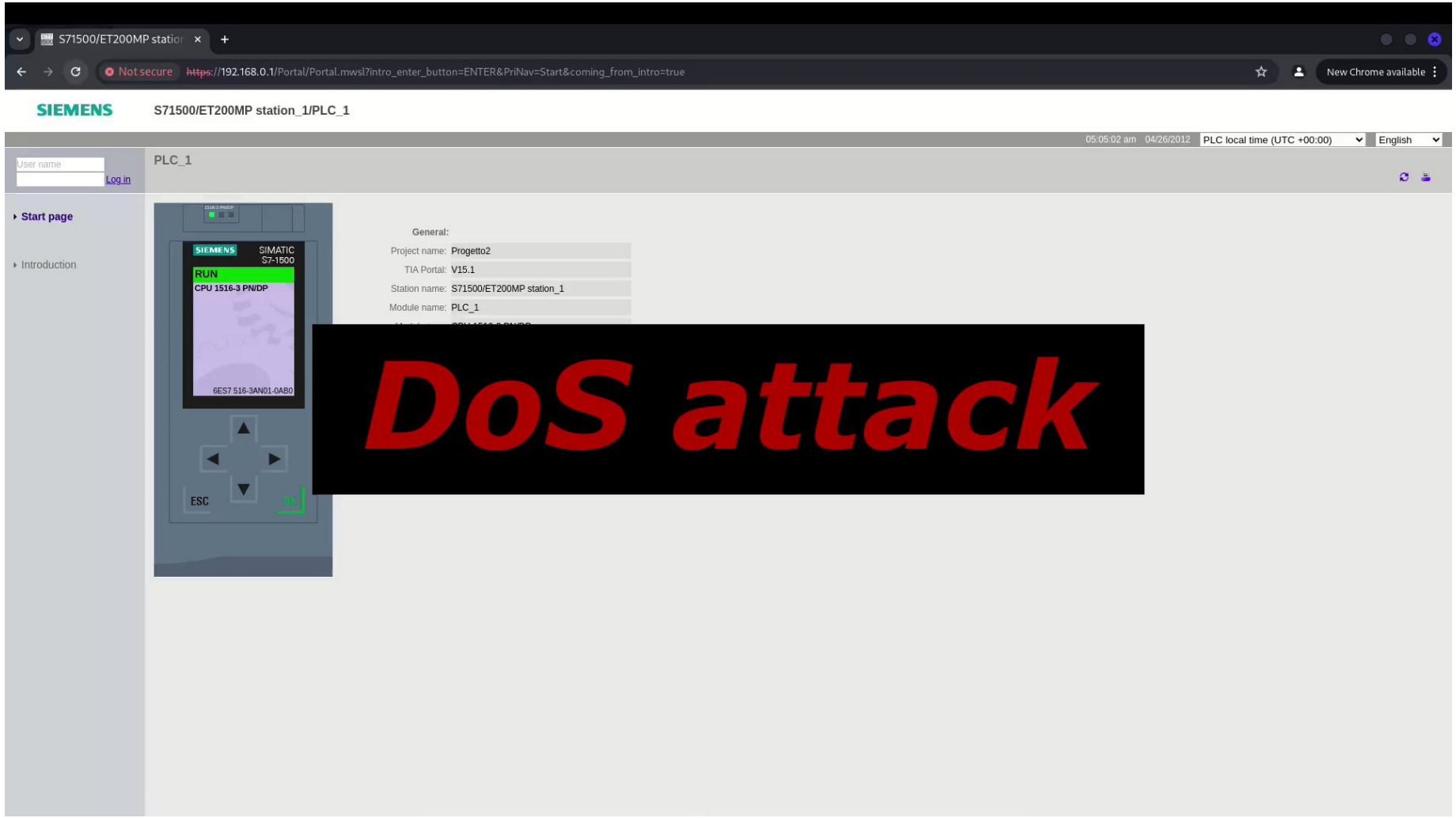
Spin-off (Unicas)

EVERYBOTICS
TECHNOLOGY IS CHANGING FAST, BE READY

DEMO 2: Vulnerability analysis di un Programmable Logic Controller

Identificazione delle vulnerabilità e penetration test a bordo di un PLC Siemens SIMATICS7-1500

DEMO 2: Penetration testing di un Programmable Logic Controller



Cyber Security: Rimanere aggiornati…

CLUSIT: Associazione Italiana per la Sicurezza Informatica (https://clusit.it/)

CYBERSECURITY360: testata del gruppo Digital360 per la cyber security (sicurezza informatica (https://www.cybersecurity360.it/)

ACN: L'Agenzia per la cybersicurezza nazionale (ACN) è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza (https://www.acn.gov.it/)

CYBER 4.0: Centro di competenza ad alta specializzazione sulla Cyber Security (https://www.cyber40.it/)

Riferimenti
Domenico Capriglione
Professore Ordinario di Misure Elettriche ed Elettroniche
Presidente del Consiglio di Corso di Studi in Ingegneria Elettrica
Responsabile scientifico del EMC2Lab (Electromagnetic Compatibility & Cyber Intelligence Laboratory)
Presidente del comitato Internazionale IEEE IMS TC-37 Measurements & Networking (https://ieee-ims.org/technical-committee/tc-37)
www.unicas.it
email: domenico.capriglione@unicas.it
Phone: +3907762994361-3398