CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

smile DIGITAL INNOVATION HUB

SISTEMI FORMATIVI CONFINDUSTRIA

LUISS

Cybersecurity per le imprese della Regione Emilia-Romagna
Contesto strategico e opportunità di sviluppo

Parma, Palazzo Soragna, Giovedì 15 giugno 2023, ore 9.30

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SISTEMI FORMATIVI CONFINDUSTRIA

LUISS

ROADSHOW CYBER 4.0

PROSSIME TAPPE

15 Giugno - Parma

26 Settembre Bari

3 Ottobre - Cagliari

17 Ottobre - Trento

15 Novembre - Udine

28 Novembre -Firenze

12 Dicembre - Venezia

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Roadshow Cyber 4.0

Cybersecurity per le imprese della Regione Marche

Contesto strategico e opportunità di sviluppo

Parma, 15 Giugno 2023

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Introduzione

Apertura dei lavori e saluti istituzionali

- **Annamaria Cucinotta,** *Presidente SMILE-DIH*
- **Matteo Lucchetti,** *Direttore Operativo, Cyber 4.0*

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Cybersecurity nel contesto della regione Emilia – Romagna

Il Centro di Competenza Bi-Rex

- **Gianmarco Moretti,** *IoT and Infrastructure Engineer Bi-Rex*

bi-rex

Big Data Innovation & Research Excellence

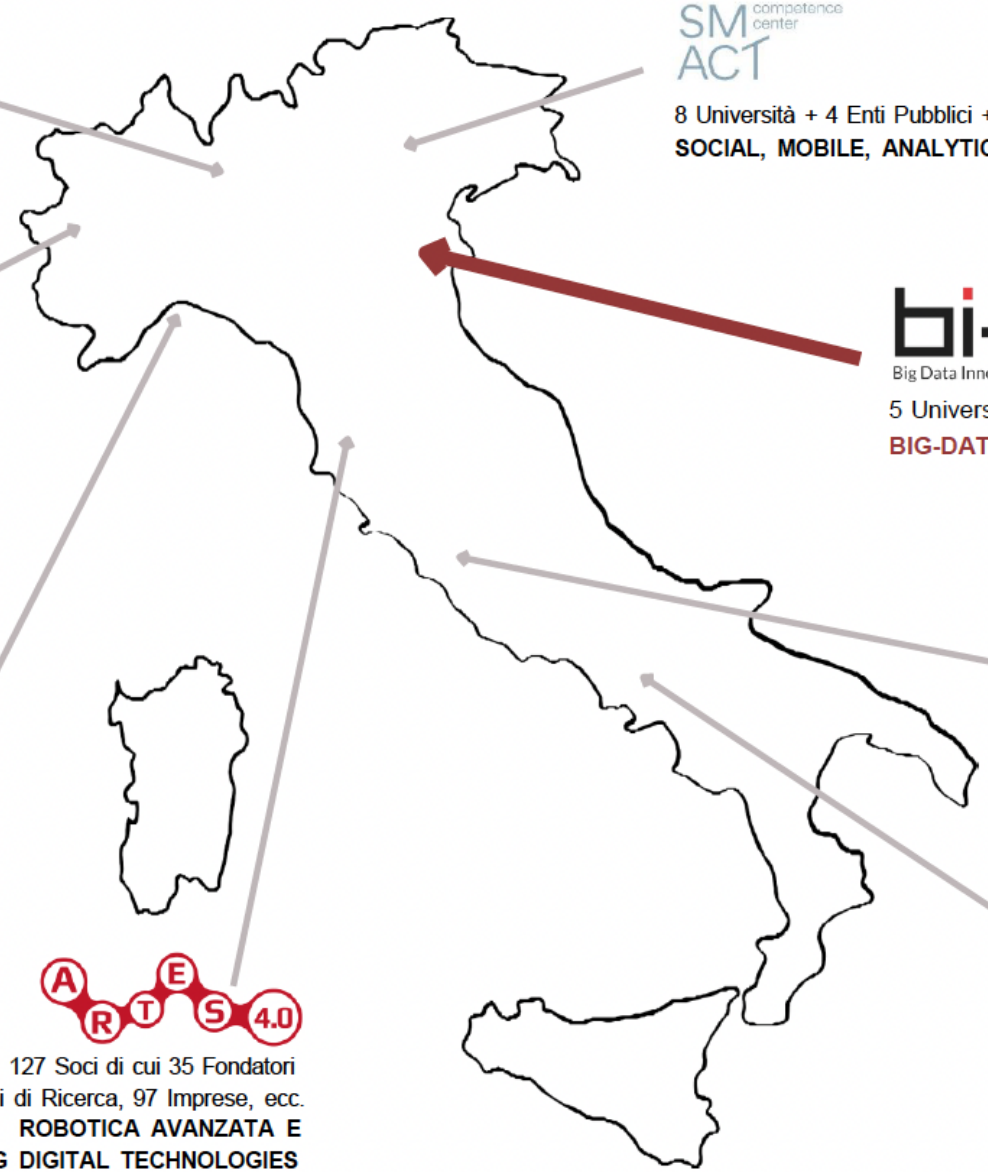
Gianmarco Moretti
IT Infrastructure Engineer
gianmarco.moretti@bi-rex.it

BI-REX è uno degli 8 **Competence Center** nazionali istituiti dal **Ministero dello Sviluppo Economico** nel quadro del piano governativo **Industria 4.0**.

Il nostro **Consorzio pubblico-privato**, nato nel 2018 e con sede a Bologna, riunisce in partenariato 60 player tra Università, Centri di Ricerca ed Imprese di eccellenza e ha un focus specializzato sul tema Big Data.

BI-REX è l'unico Competence Center a guida industriale.

GLI 8 COMPETENCE CENTER



MADE Competence Center 4.0

4 Università + 1 Ente Pubblico + 39 Imprese

ISOLE DIMOSTRATIVE SULLE TECNOLOGIE ABILITANTI

SM competence center ACT

8 Università + 4 Enti Pubblici + 30 Imprese

SOCIAL, MOBILE, ANALYTICS, CLOUD, IOT

bi-rex Big Data Innovation & Research Excellence

5 Università +7 Enti Pubblici + 48 Imprese

BIG-DATA e ADDITIVE MANUFACTURING

+CIM 4.0

2 Università +23 Imprese

MANUFACTURING 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

7 Università + 2 Enti Pubblici + 37 Imprese

CYBER-SECURITY

START4.0

4 Enti Pubblici + 33 Imprese

SICUREZZA E OTTIMIZZAZIONE INFRASTRUTTURE STRATEGICHE

ARTES 4.0

127 Soci di cui 35 Fondatori

13 Organismi di Ricerca, 97 Imprese, ecc.

ROBOTICA AVANZATA E ENABLING DIGITAL TECHNOLOGIES

MEDITECH COMPETENCE CENTER

8 Università + 131 Imprese (109 PMI)

TECNOLOGIE SOCIAL E BLOCKCHAIN

IL CONSORZIO 60 AZIENDE

12 ENTI

26 END USERS

22 TECHNOLOGY SERVICE PROVIDER

bi-rex

PMI italiane

Contesto nazionale e cybersecurity

- 4.4 Mln Imprese in Italia
  - 95.05% micro (<10 dipendenti)
  - 4.86% PMI (10-50 dipendenti) – 206.000 → 41% del fatturato totale, 33% impiegati totali
  - 0.09% grandi imprese (>50 impiegati)
- Dati recenti di una ricerca condotta su un campione significativo (10.000+)*:
  - 97% delle PMI ha adottato uno o più sistemi digitali, gestiti internamente
    - [e.g. email (90%), sito web (73%), BPM (61%), WiFi per esterni (35%), ecommerce (28%)]
  - **26% delle PMI italiane ha subito cyber attacchi nel 2022**
  - **52% of delle PMI ha allocato risorse nel 2023 per la protezione di dati e sistemi informativi, per una spesa media di 4.800 EUR, per un totale complessivo di più di 470Mln EUR** – Solo il 50% di loro ha già identificato anche il fornitore

* https://www.cybersecitalia.it/le-pmi-italiane-pronte-ad-investire-470-milioni-di-euro-sulla-sicurezza-informatica-nel-2023-i-dati-di-confesercenti/23204/

LA NOSTRA MISSION

Supportare le aziende nei loro processi di digitalizzazione e innovazione e nell'adozione delle tecnologie abilitanti in ottica Industria 4.0.

Facilitare lo scambio di "best practices" ed il Trasferimento Tecnologico.

- Infrastrutture uniche, capacità e opportunità di integrazione
- Open Call finanziata dal MIMIT per Imprese e Start-up
- Servizi integrati business-tecnologia-innovazione

I SERVIZI BI-REX

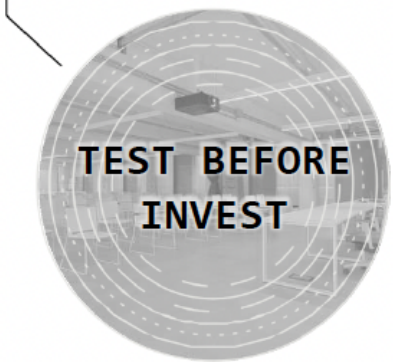
Tecnologica

Gestionale e Project Management

Access To Finance

Start-up

INNOVATION ONE STOP SHOP



I NUMERI DEI BANDI BI-REX

3 BANDI EMESSI
E ASSEGNATI

35 PROGETTI
>50 USE CASES

5,4 MILIONI DI
EURO STANZIATI

88 AZIENDE VINCITRICI
12 FILIERE COINVOLTE

+7 MILIONI DI EURO
INVESTIMENTI
AZIENDALI ATTIVATI

10 UNIVERSITÀ
6 ENTI DI RICERCA
>60 ASSEGNI

La Linea Pilota

ADDITIVE MANUFACTURING

SMART MANUFACTURING

Stampa 3D circuiti

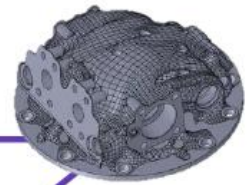
Selective Laser Melting

Deposizione Diretta

Materiali Plastici

Reverse engineering

Simulazione e progettazione



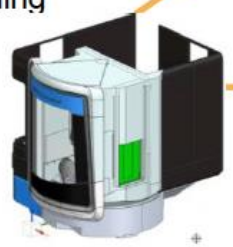
Centro di lavoro CNC

CONNETTIVITÀ 5G

Cloud e Edge computing

Robotica Mobile

Digital twin e virtual commissioning



Robotica Collaborativa

Data analytics

Realtà aumentata e virtuale

ROBOTICA E AUTOMAZIONE

BIG DATA E IoT

bi-rex

SS4SP: Safety and Security for Smart Production

Obiettivi

Migliorare sicurezza informatica, continuità operativa e safety di impianti dell'Industria 4.0

Use Case

- Standard IEC62443 **perimetro** in **Sacmi**
- Gateway IoT in **IMA/Bi-rex**

IMA SPA

Università degli Studi di Ferrara

SACMI

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

imola informatica

SIEMENS

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Alascom

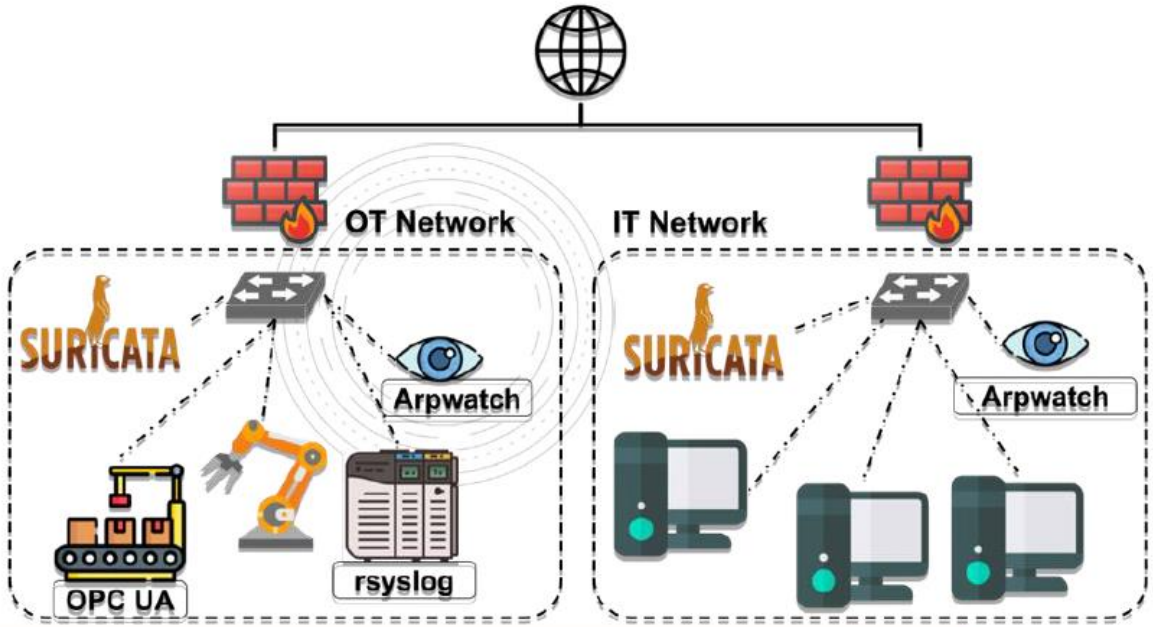
SAMP

bi-rex

SS4SP: Safety and Security for Smart Production

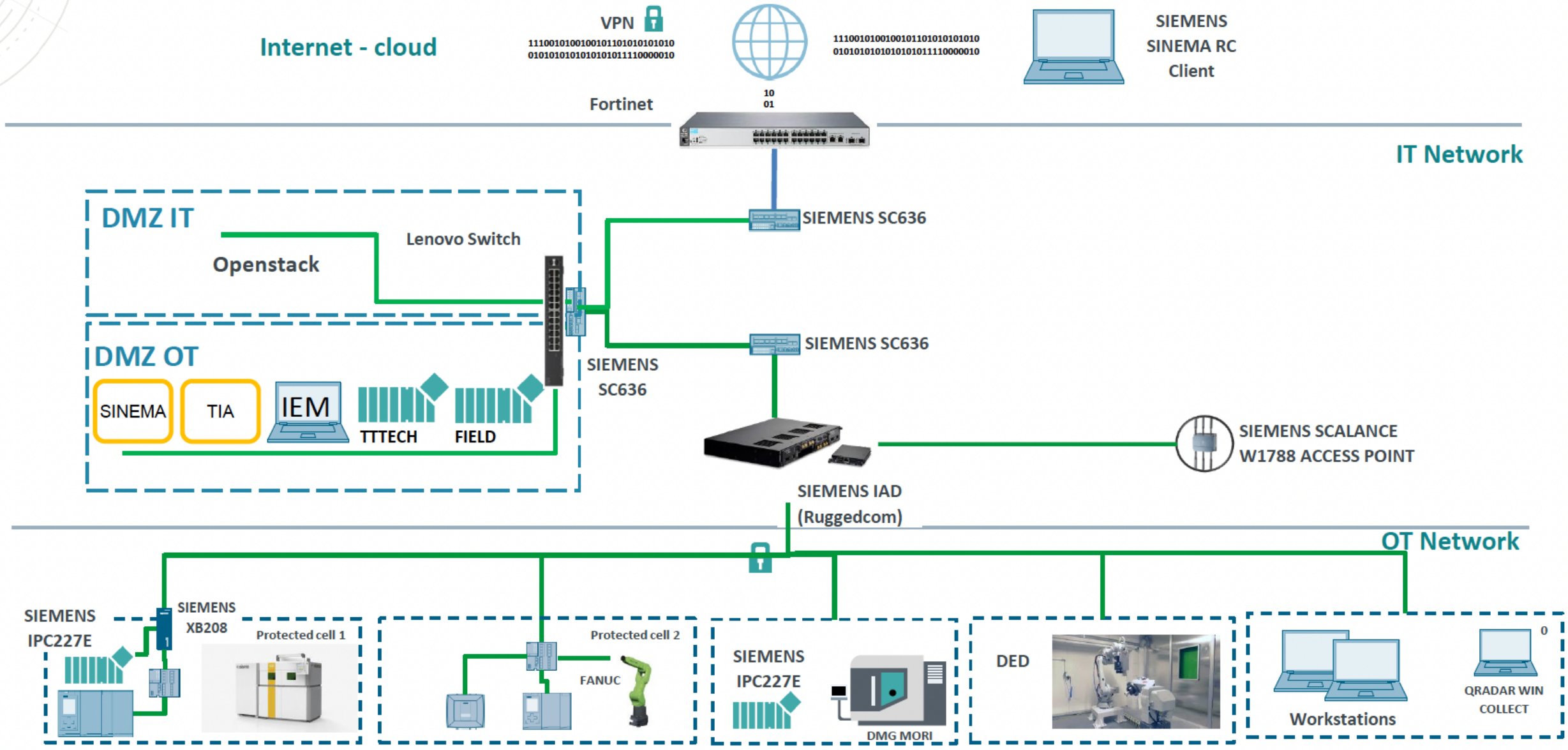
Output e Benefici

- **Riduzione dell'esposizione** al rischio cyber
- **Prevenzione** e **mitigazione** delle conseguenze su safety e continuità
- Adeguamento delle modalità operative



Metodologie e tecniche per la cyber security basate su approccio integrato IT/OT

Architettura di rete



Architettura di rete

Standard ISA 62443

- Separazione tra IT e OT
- Segregazione e Segmentazione
- Introduzione DMZ IT/OT con accesso in VPN
- Ispezione traffico OT e Intrusion-Anomaly Detenction (Nozomi)

Perché?

- Impedire flusso di dati diretto tra le macchine e l'esterno (in ambo le direzioni)
- Monitoraggio della rete
- Identificazione e prevenzione di attacchi
- Notifica verso il management e automazione di azioni di reazione agli attacchi (QRadar)

Architettura di rete

QRadar

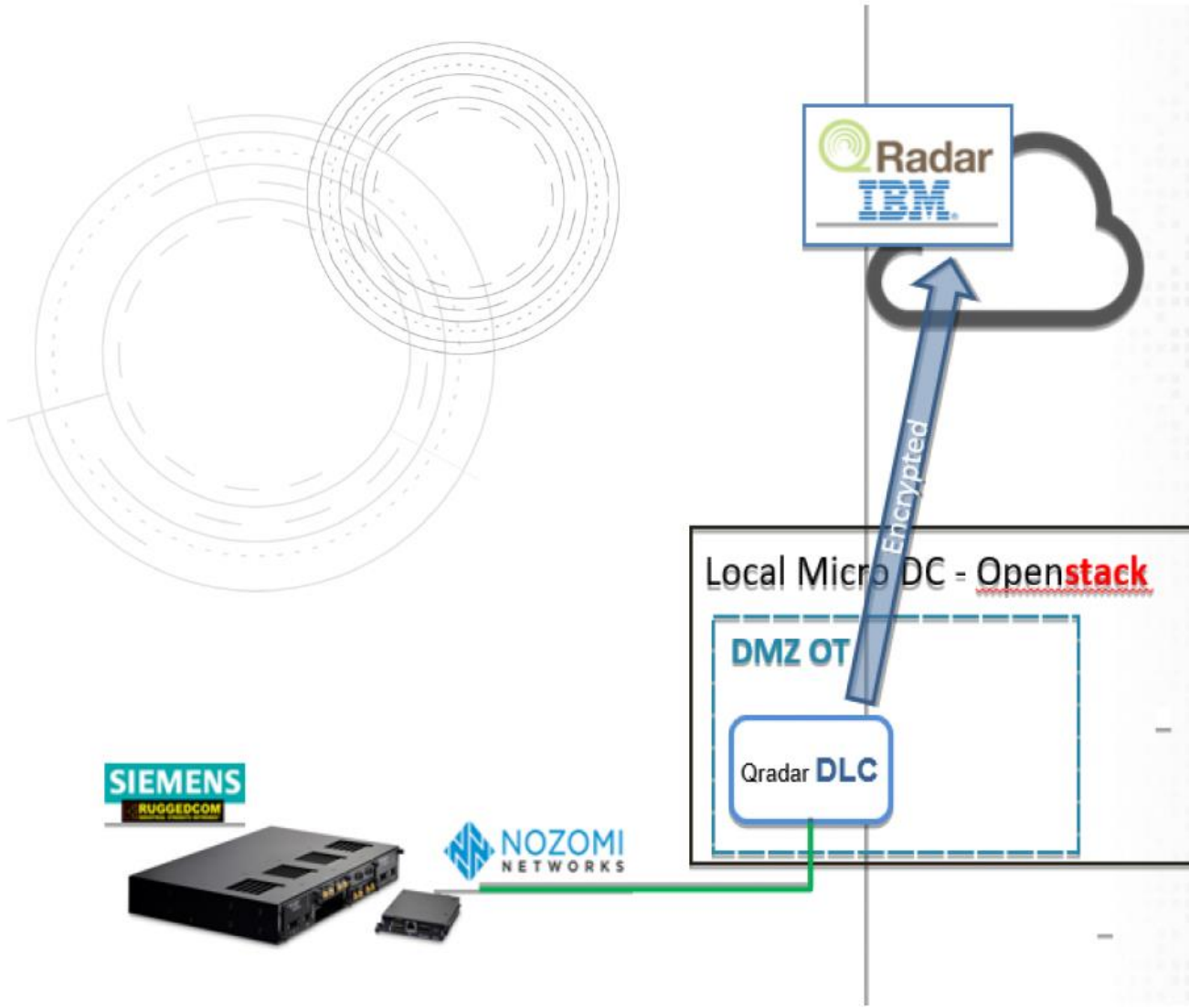
- Moduli Add-On per il parsing dei log (supporto terzi)
- Trigger per azioni dopo riconoscimento di determinati pattern

DLC

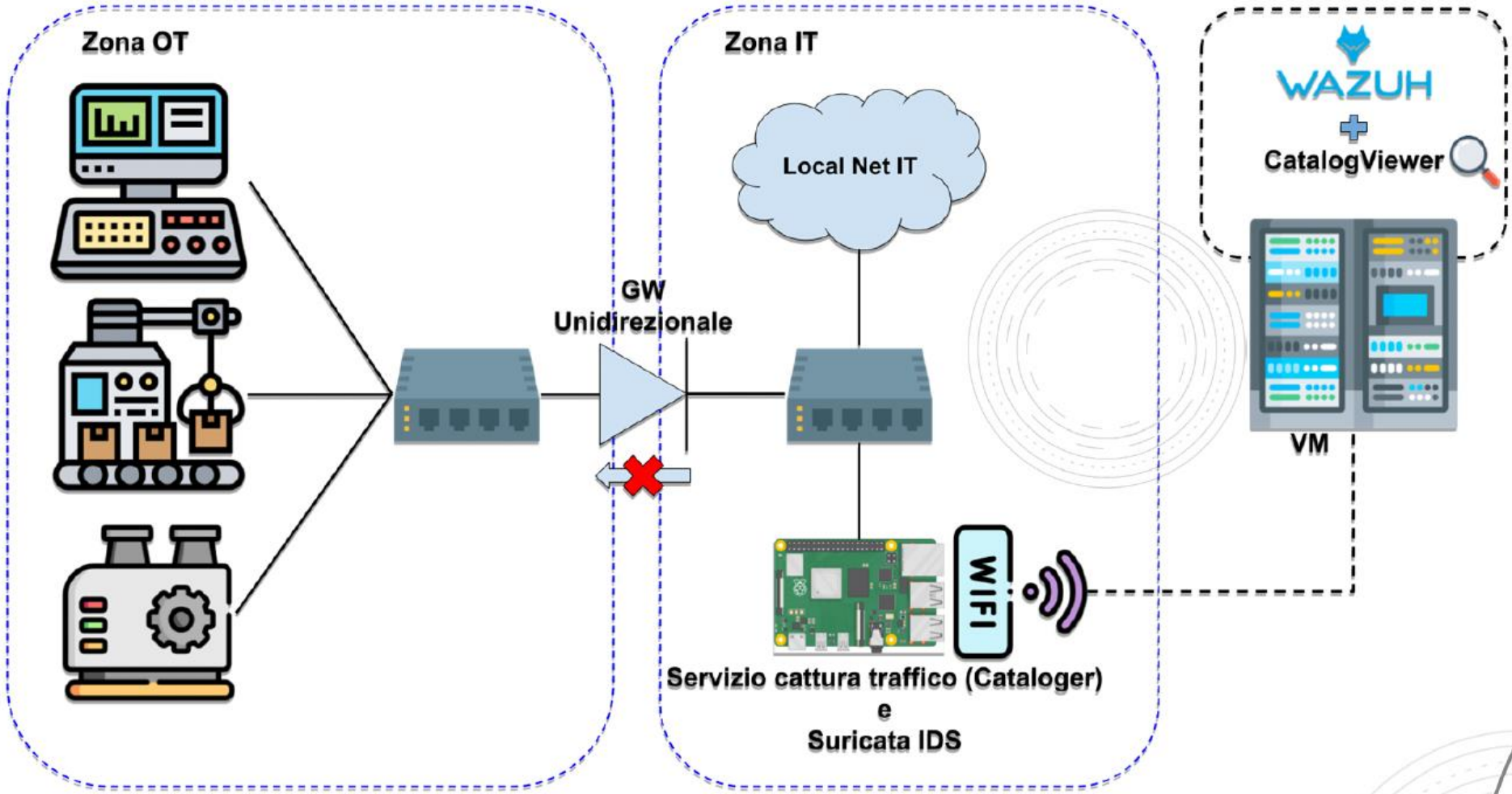
- Disconnected Log Collector
- Supporta differenti protocolli (syslog, API, JDBC) e eterogeneità dei device monitorati (HMI, Network device, Nozomi)

Nozomi

- Anomaly detection
- Log report



Use case BI-REX/IMA



CONTATTI

Via Paolo Nanni Costa 20, Bologna

+39.051.0923250

marketing@bi-rex.it

www.bi-rex.it

SEGUICI SU

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Il percorso dell'innovazione fra conformità e sicurezza: un esempio virtuoso.

Come operare durante un attacco cyber

- **Domenico Carnicella,** *Consigliere SMILE DIH*

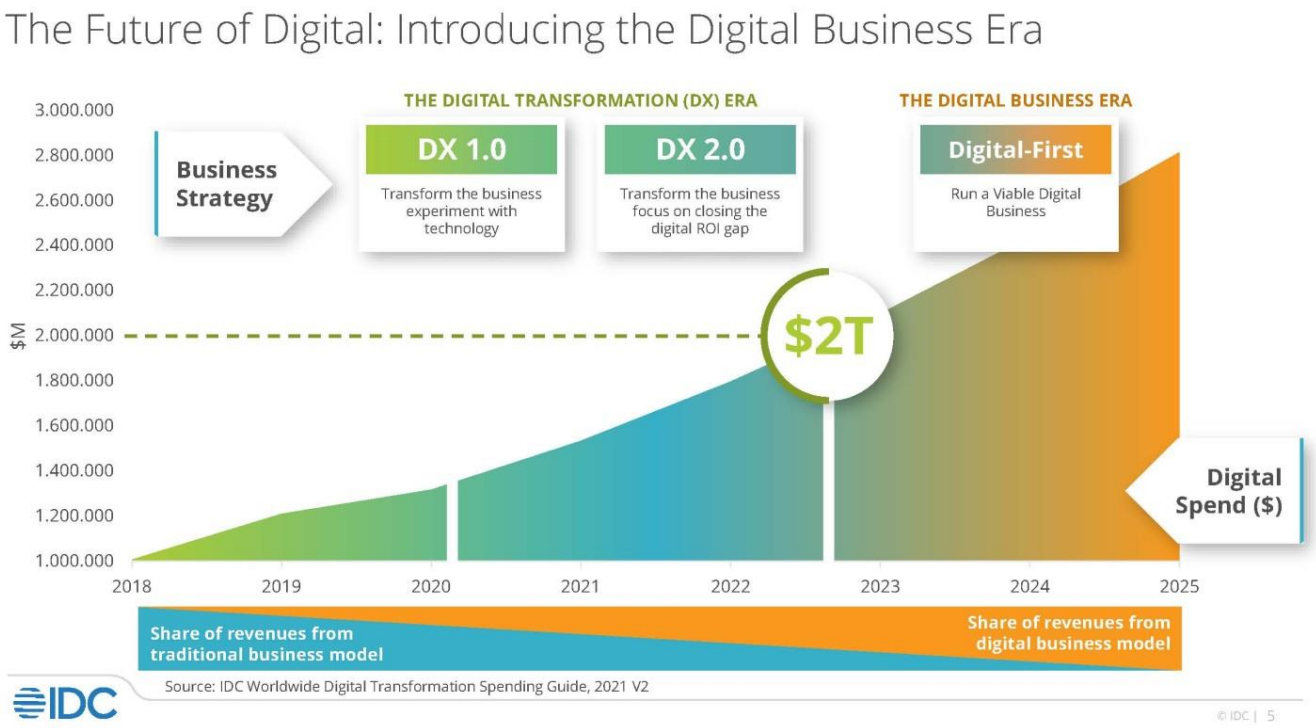
Come gestire il business col digitale

Resilienza, raccolta e monitoraggio dei dati, gestione dei processi, ecosistemi, piattaforme: **nuovi asset e nuovi perimetri da proteggere e difendere dagli attacchi informatici**

2023, l’anno delle aziende digital-first

- Solo le organizzazioni che hanno basato il proprio **business sull’analisi dei dati** e sull’adozione di **tecnologie abilitanti** hanno saputo adattarsi e **rimanere competitive** nonostante pandemia, problemi geopolitici e rincari dei costi energetici e delle materie prime
- La **digitalizzazione ha costituito l’ancora di salvezza** e permesso loro di scoprire la resilienza per contrastare in qualche modo tempeste sui mercati, interruzioni forzate, probabili recessioni, inflazione, mancanza di competenze, conflitti e restrizioni della catena di approvvigionamento

Le previsioni di spesa delle imprese nel digitale



- Le organizzazioni che hanno maturato una **cultura digitale** hanno già **valorizzato gli investimenti** e stanno addirittura aumentandoli in tal senso

VS

- Le organizzazioni **che non hanno ancora esplorato** i benefici del digitale dovrebbero cercare di recuperare il ritardo, perché….

Prima

Perché se prima valeva la regola:
«Pesce grosso mangia il Pesce piccolo»

adesso è cambiata in
«Pesce VELOCE mangia il Pesce LENTO»

(*anche se il pesce veloce è il più piccolo tra i due*)

Dopo

Le due immagini sono state generate con intelligenza artificiale (Bing, ChatGPT4 + DALL-E)

LE IMPRESE SONO CHIAMATE AD UN CAMBIAMENTO «OBBLIGATO»

COSTRUIRE UN'IMPRESA DIGITALE SIGNIFICA:

- Saperla gestire mitigando i rischi
- Individuare nuove metriche di leadership
- Adottare una cultura guidata dai dati e puntare al miglioramento continuo

IL PERCORSO PER DIVENTARE DIGITALI DEVE ESSERE STUDIATO AD-HOC

1) **Effettuare un'analisi preventiva prima di effettuare investimenti** per:

   - Sapere quanto si è pronti ad intraprendere un percorso di trasformazione digitale. Strumenti disponibili: **Digital Maturity Assessment** (DMA), **Test Industria 4.0**, **Cyber security Assessment**, ecc. che restituiscono **KPI sui processi operativi** e un possibile **piano d'azione** per efficientare i **processi** risultati maggiormente critici

2) **Scoprire le tecnologie abilitanti, testarle per poi scegliere quelle più adatte** perché:

   - Le soluzioni già adottate da altre imprese non sono mutuabili senza adattamenti, ma si possono valutare come casi d'uso o di successo
   - Le tecnologie innovative **si possono testare** (in laboratorio o sul campo) **prima di deciderne l'acquisto**

3) **Sapersi adattare velocemente al mutevole contesto attuale**

   - Istituire un percorso culturale di miglioramento continuo dei processi operativi che sfrutti i benefici dell'innovazione e del digitale

4) **Estendere l'azione sulla propria supply chain** che può **costituire un anello debole**, in quanto è dimostrato che:

   - Seppur piccoli interventi indotti per digitalizzare la catena di fornitura portano notevoli benefici: si ottimizzano i tempi di conferimento di materie prime o prelavorati, le scorte, la logistica, la distribuzione e si possono prevenire per tempo le variazioni di costo
   - Il 2023 è l'anno dell'**e-procurement** (diverse aziende strutturate premiano i fornitori più digitalizzati) e delle **piattaforme per la creazione di ecosistemi** dove possano esprimere il loro valore anche le **PMI** e **Startup innovative** e dove scoprire e valorizzare talenti

QUANDO UNA FABBRICA SI PUÒ DEFINIRE **INTELLIGENTE** ….E QUANDO UN'ORGANIZZAZIONE PUÒ DIRSI **INTERCONNESSA**

Fabbrica intelligente

Azioni endogene

Analisi (assessment)

Individuazione dei processi operativi eccellenti e critici

Individuazione delle tecnologie e test in laboratorio o sul campo

Adozione, integrazione IT/OT, gestione del cambiamento e continuo efficientamento dei processi operativi

Estensione del processo di digitalizzazione alla supply chain

Azioni esogene

Estensione del percorso di digitalizzazione alla catena di fornitura

Creazione di un ecosistema

Organizzazione interconnessa

NUOVI PERIMETRI DA SALVAGUARDARE E NUOVI DATI DA PROTEGGERE DA CONSIDERARE NELLA GESTIONE DEL RISCHIO

- La **convergenza** degli ambienti **IT**, **IoT** e **OT** ha aumentato la complessità e la vulnerabilità delle reti precedentemente isolate e dei sistemi cyber-fisici (CPS) di nuova concezione,
- introducendo la necessità di un **approccio olistico** alla scoperta delle risorse vulnerabili, alla valutazione dei rischi e ai possibili **rimedi per evitare tempi di inattività**.

GRAZIE

WWW.SMILE-DIH.EU

INFO@SMILE-DIH.EU

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Il percorso dell'innovazione fra conformità e sicurezza: un esempio virtuoso.

Come operare durante un attacco cyber

- **Juri Giordani,** *DataConSec*

DATACONSEC

DATA PROTECTION - CONSULTING - SECURITY

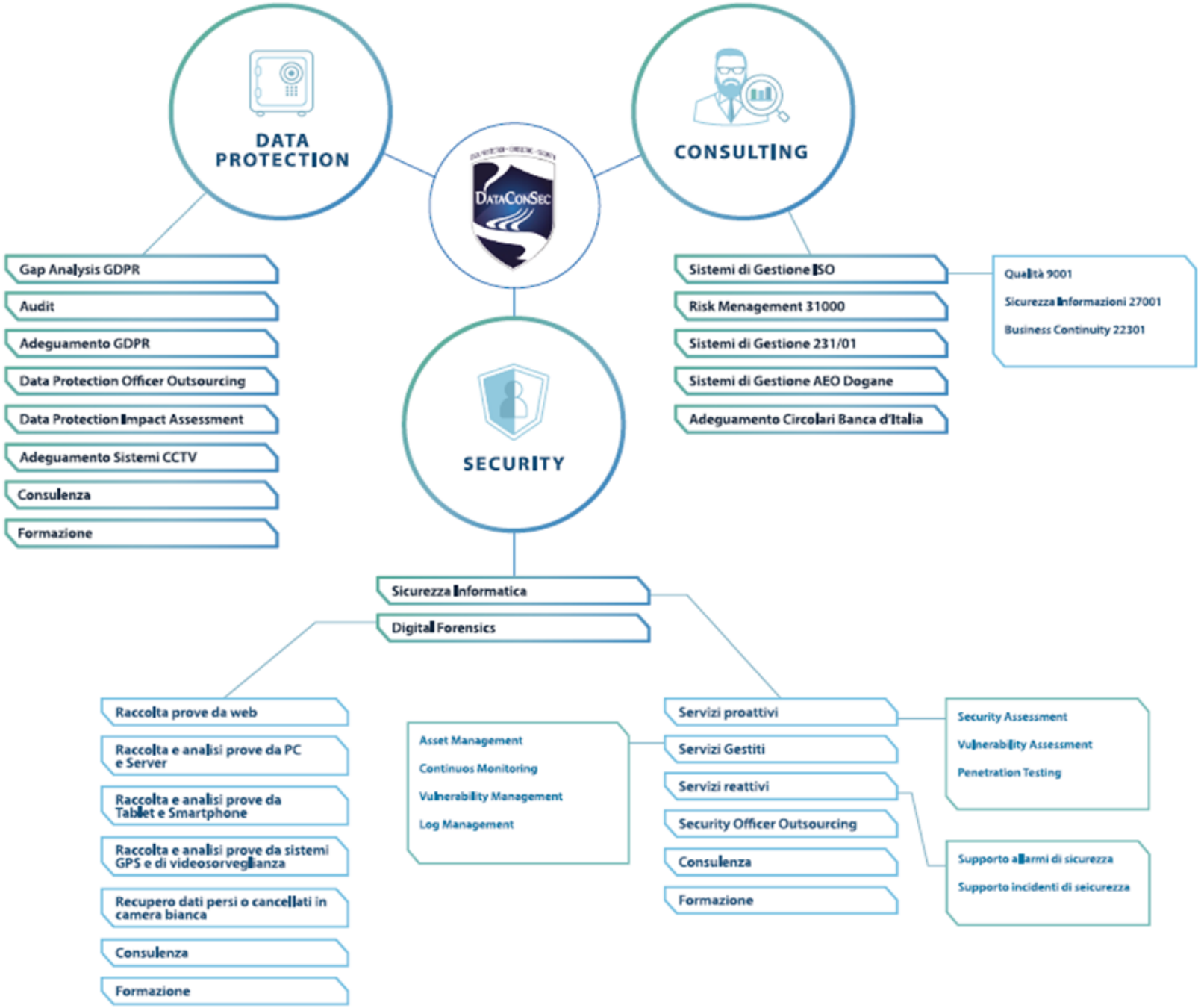
Il percorso dell'innovazione fra conformità e sicurezza: un esempio virtuoso

Domenico Carnicella, Consigliere SMILE-DIH
Jury Giordani DataConSec

Cybersecurity per le imprese della Regione Emilia-Romagna
Contesto strategico e opportunità di sviluppo

15 giugno 2023
Parma sede UPI,
Strada al Ponte Caprazucca 6/a

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER
smile DIGITAL INNOVATION HUB
SISTEMI FORMATIVI CONFINDUSTRIA
LUISS



Via Emilia

di **Andrea Violi**

Combustibili, la ricerca unisce Parma e Bologna

Scienziati al lavoro, in Emilia-Romagna, nel campo della ricerca applicata alla decarbonizzazione. Prosegue il progetto E-CO2, che persegue l'obiettivo di produrre, ad emissioni zero, combustibili innovativi usando l'anidride carbonica e l'idrogeno. Fra le possibili applicazioni: l'industria, l'edilizia, i trasporti. E-CO2 è finanziato dalla Regione e dal Fondo sviluppo e coesione ed è coordinato dal Laboratorio Enea Cross-Tec di Bologna in partnership con gli Atenei di Bologna e di Parma, il Laboratorio Energia Ambiente di Piacenza, Romagna Tech e diverse aziende: la multiutility Hera, Tper, Siram Veolia, Ecospray Technologies, Idro Meccanica e Buzzi Unicem. «Il metano sintetico prodotto da CO2 e idrogeno verde - ha detto nei giorni scorsi il coordinatore del progetto, ingegner Giuseppe Nigliaccio - potrebbe essere immesso nella rete gas naturale e trovare così impiego nei settori della mobilità, dell'industria e del residenziale. Proprio la possibilità di utilizzare la vasta rete gas presente nel nostro Paese, con funzione di accumulo energetico, costituisce il grande potenziale di impiego di questa tecnologia. Al contempo, si favorisce una maggiore penetrazione delle fonti rinnovabili elettriche, attraverso l'interazione della rete elettrica con quella del gas, il cosiddetto sector coupling». Il sito dedicato (https://e-co2.it) sottolinea: «Tra le strategie più vantaggiose per la transizione verso una low-carbon economy, la cattura della CO2 (CCU/CCS) gioca un ruolo primario». Fra i binari da seguire: eseguire una stima della potenziale

L'azienda Ha intuito in anticipo il valore delle informazioni per imprese e P.A.

DataConSec, pionieri della protezione dei dati

13 anni

L'avvio nel gennaio 2008
DataConSec è stata fondata a Parma dagli imprenditori Domenico Carnicella e Alessandro Rodolfi.

DataConSec è operativa dal 1° gennaio 2008. Sono stati Domenico Carnicella e Alessandro Rodolfi a fondare l'azienda, partendo da competenze ed esperienze acquisite e dando ascolto ad una comune intuizione: la normativa Privacy, in vigore dal 2004, stava generando l'esigenza, per imprese e pubblica amministrazione, di proteggere i dati e il loro valore in modo complessivo. Non si trattava solo di adeguarsi alla normativa ma serviva un approccio consulenziale orientato ad una visione globale che toccasse tutti gli aspetti del processo: documentale, tecnologico ed organizzativo. «Adesso cybersecurity e sicurezza dei dati personali sono argomenti "mainstream" ma noi siamo stati tra i primi a parlarne. Abbiamo avuto subito consapevolezza che occorreva affrontare a 360 gradi le tematiche di privacy, protezione dei dati e sicurezza delle informazioni», spiegano i due soci, che hanno focalizzato gli obiettivi anche nel nome dell'azienda, sintesi di data protection, consulenza e cybersecurity. «All'inizio abbiamo avuto molta diffidenza ad approcciare che non fosse solo formale e orientato a scongiurare sanzioni. Le informazioni e i dati sono tra i beni immateriali più importanti di un'azienda perché incidono sul valore del business e una loro errata o parziale protezione può esporre all'interruzione dell'attività o alla sua perdita d'efficacia. Per questo devono essere analizzati sotto il profilo legale, organizzativo e di processo, ponendo attenzione alla tecnologia attraverso cui sono gestiti dall'infrastruttura aziendale».

Un approccio articolato che richiede competenze specifiche e multidisciplinari, ma che ha trovato piena conferma con l'avvento del Gdpr europeo del 2016. «La nuova disciplina è perfettamente in linea con quanto noi già facevamo dal 2008 e ci ha aiutato ad innalzare il livello di consapevolezza sul tema. La sicurezza delle informazioni (ora cybersecurity) è diventata fondamentale, a protezione delle aziende ma anche come esigenza del mercato digitale europeo». Sull'onda della nuova normativa e della fiducia dei clienti, negli ultimi cinque anni scita arrivando ad una struttura di dodici dipendenti suddivisi su tre settori (amministrativo, giuridico e tecnico) e ad oltre trecento clienti tra PA, pmi e grandi aziende, anche multinazionali.

«Abbiamo investito sulle skills delle risorse umane, sulla loro formazione tecnica ma anche sulla capacità di cogliere l'evoluzione del mondo digitale. Il flusso dei dati e della tecnologia oggi è cambiato ed è esposto a molteplici minacce: solo analizzandolo se ne comprendono i fattori di rischio e si può costruire un sistema a protezione». Proprio l'evoluzione tecnologica delle aziende e la crescente digitalizzazione di alcuni processi, come quello produttivo e logistico nella filosofia Industria 4.0, aprono a complessità future. «Sarà fondamentale il valore delle competenze - concludono Carnicella e Rodolfi, che insegna anche Informatica giuridica all'Università di Milano -. In DataConSec ci stiamo rafforzando anche sotto questo profilo, attraverso la partecipazione a progetti di settore in collaborazione con alcuni atenei che innalzeranno la cultura informati-

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Contesto
economico/giuridico

Il Sole
24 ORE
del lunedì

€ 2 in Italia
Lunedì 27 Febbraio 2023
Anno 159°, Numero 57

L'esperto risponde
Il tema di oggi
Età e contributi: tutte le condizioni per accedere alle pensioni di vecchiaia

Possibile continuare con l'attività autonoma. Bonus temporale per gli invalidi
Aldo Forte
— nel fascicolo all'interno

Le sezioni digitali del Sole 24 Ore
L'area premium
Inchieste e approfondimenti nel sito del Sole 24 Ore
Norme & Tributi Plus
Quotidiani digitali su Fisco, Diritto, Enti Locali & Edilizia
Mercati Plus
Notizie, servizi e tutti i dati dai mercati finanziari
Lavoro
Contratti, sicurezza, formazione, controversie e welfare

Sicurezza IT
Pmi, è cyber allarme: sempre più nel mirino degli attacchi hacker

Nel 2022 crescono del 45% le denunce di assalti ai dati con richiesta di riscatto
Manifattura e servizi colpiti nel 53% dei casi

di Ivan Cimmarusti — a pagina 2

ANSA.it Hi-tech

Fai la ricerca

Cronaca | Politica | Economia | Regioni + | Mondo | Cultura | Tecnologia

PRIMOPIANO • HI-TECH • INTERNET & SOCIAL • TELECOMUNICAZIONI • SOFTWARE & APP • OSSERVATORI

ANSA.it › Tecnologia › Hi-tech › Garante Privacy, entro aprile OpenAI adotti misure per ChatGpt

Garante Privacy, entro aprile OpenAI adotti misure per ChatGpt

Informativa e verifica età, poi tornerà accessibile in Italia

Redazione ANSA
ROMA
12 aprile 2023
19:07
STORIA

Suggerisci
Facebook
Twitter
Altri
A+ A A-
Stampa
Scrivi alla redazione

Garante, entro il 30/4 OpenAI adotti misure per ChatGpt © ANSA/EPA

CLICCA PER INGRANDIRE

Contesto attacchi

Lo studio si basa sull'analisi di oltre 16.000 cyber attacchi noti, andati a buon fine e di particolare gravità, a partire dal 2011, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali, o che comunque prefigurano scenari particolarmente preoccupanti.

Nel periodo che prenderemo in esame, tra gennaio 2018 e dicembre 2022 si sono verificati un totale di 9.633 cyber attacchi, così suddivisi:

Fig. 1: *Andamento dei cyber attacchi nel periodo 2018 - 22*

Il nostro campione rappresenta il 58.4% del totale degli incidenti classificati in 12 anni, con una media complessiva di 161 attacchi al mese nell'intero periodo (erano 39 nel 2011, 130 nel 2018, e sono 207 nel 2022).

Rapporto Clusit 2023 sulla sicurezza ICT in Italia

SECURITY SUMMIT

L'anno scorso il sistema Italia ha registrato **un'intensificazione degli attacchi cyber verso le Pmi**, rivelatesi assai più vulnerabili rispetto alle grandi organizzazioni. **Ben l'80% degli attacchi ha riguardato imprese con un fatturato inferiore a 250 milioni di euro**, mentre il **51%** delle realtà colpite **ha meno di 100 dipendenti**.

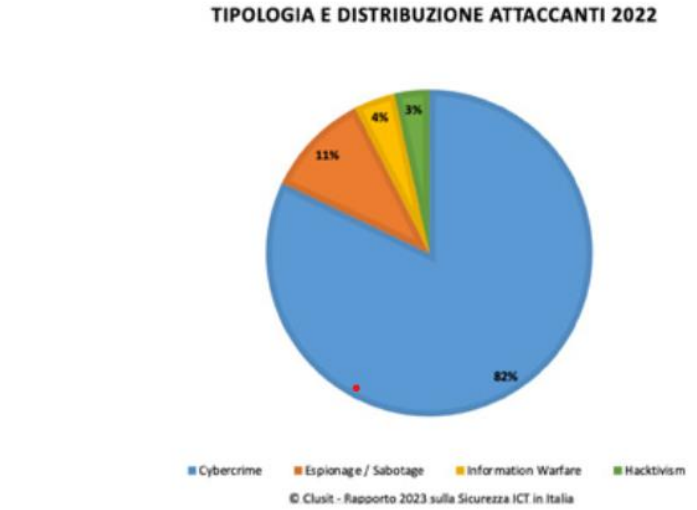


Fig. 7: *Andamento percentuale della tipologia di attaccanti nel 2022*

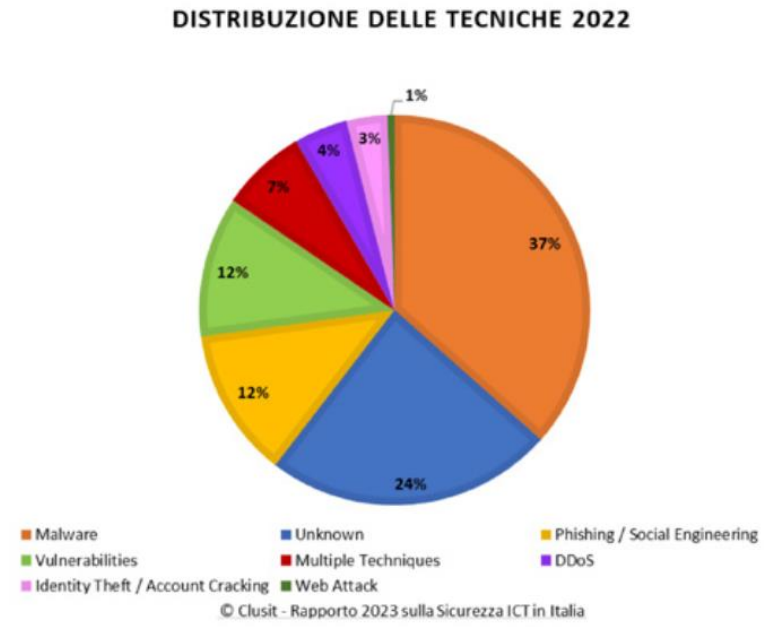
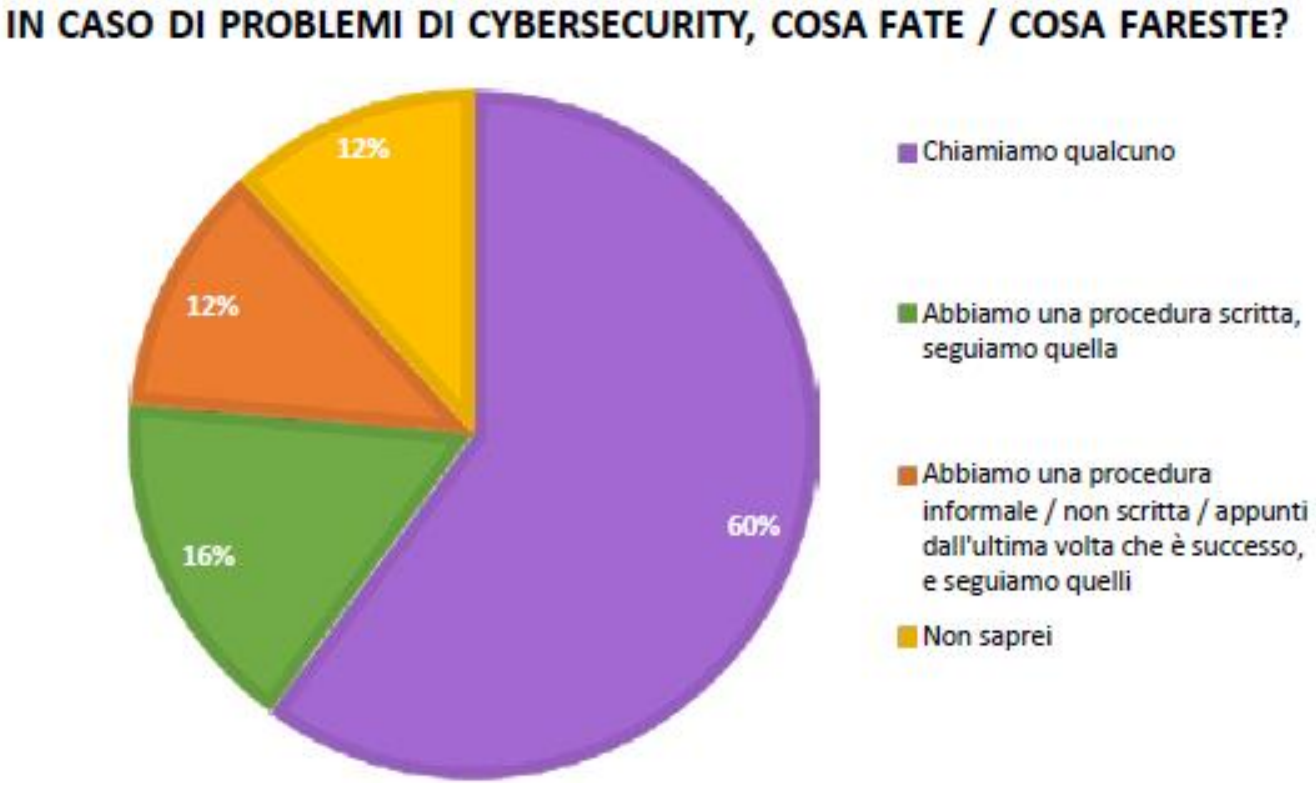
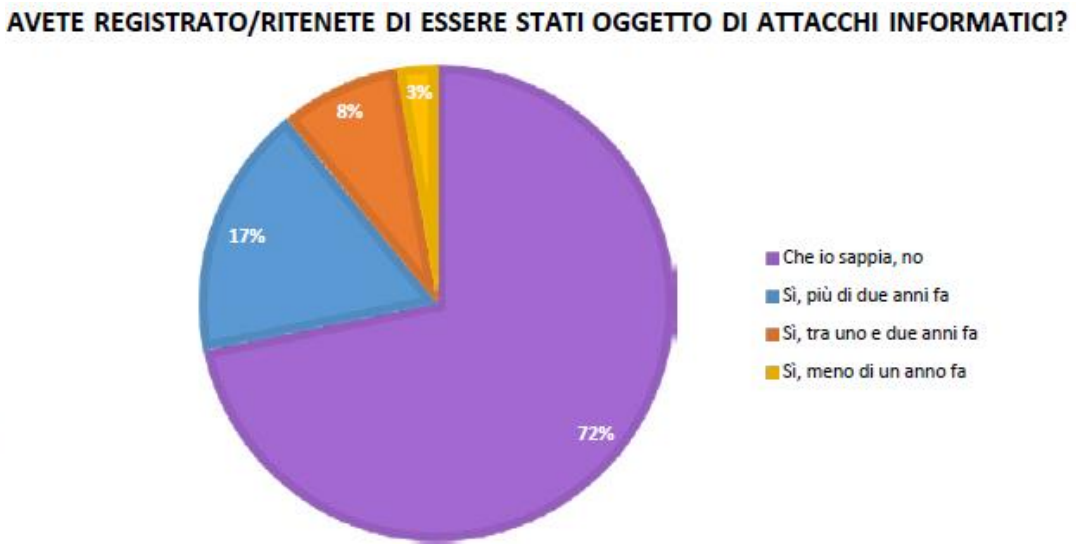


Fig. 13: *Distribuzione delle tecniche di attacco nel 2022*

Contesto PMI



In caso di **incidenti informatici** circa **due terzi** si affiderebbero a **fornitori esterni**, mentre **solo il 28% dispone di una procedura**, scritta (16%) o informale (12%). Preoccupante anche il **12% che non sembra avere ancora riflettuto sul tema**.



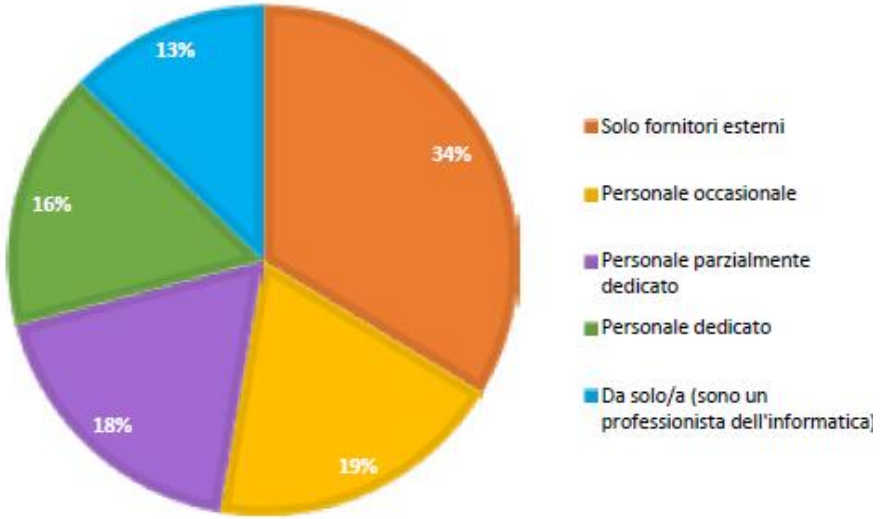
Quando si parla di **cyber attacchi**, il **72%** ritiene di **non esserne stato soggetto** (o **non ne è consapevole**). In totale **meno di un terzo ammette** di aver subito un attacco.

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

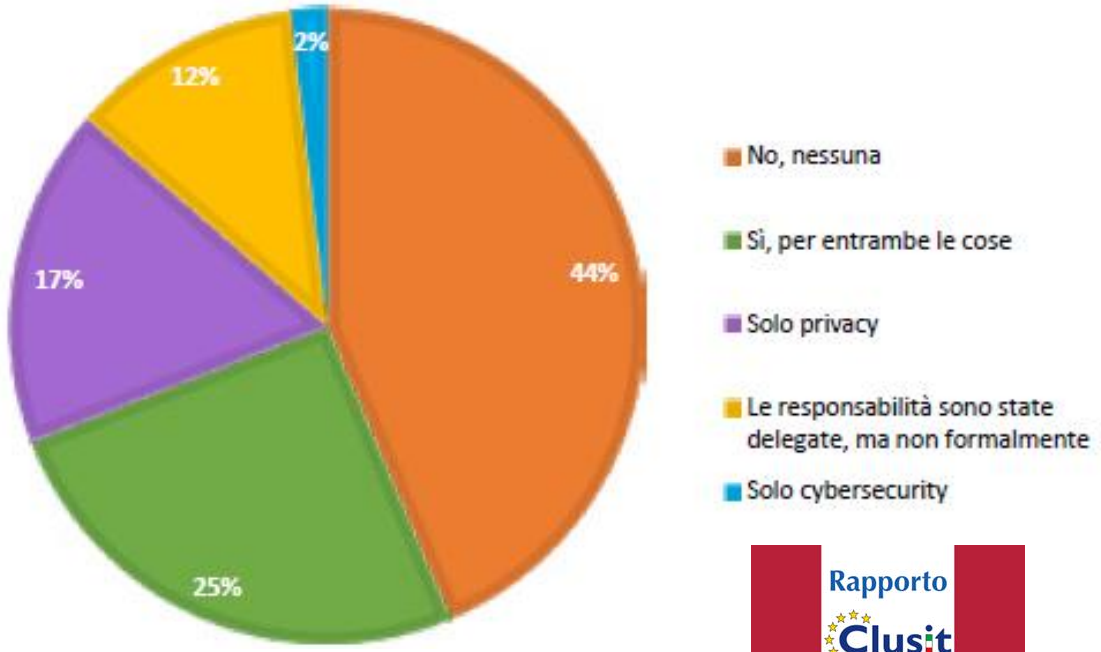
Contesto ruoli e responsabilità PMI

SURVEY - La Cybersecurity nelle micro e piccole imprese.
Una Survey di CNA Milano e dell'Unione Artigiani Milano

DA CHI È GESTITA L'INFORMATICA DELLA TUA ATTIVITÀ/AZIENDA?



C'È UN/UNA RESPONSABILE UFFICIALE DELLA CYBERSECURITY E/O DELLA PRIVACY?



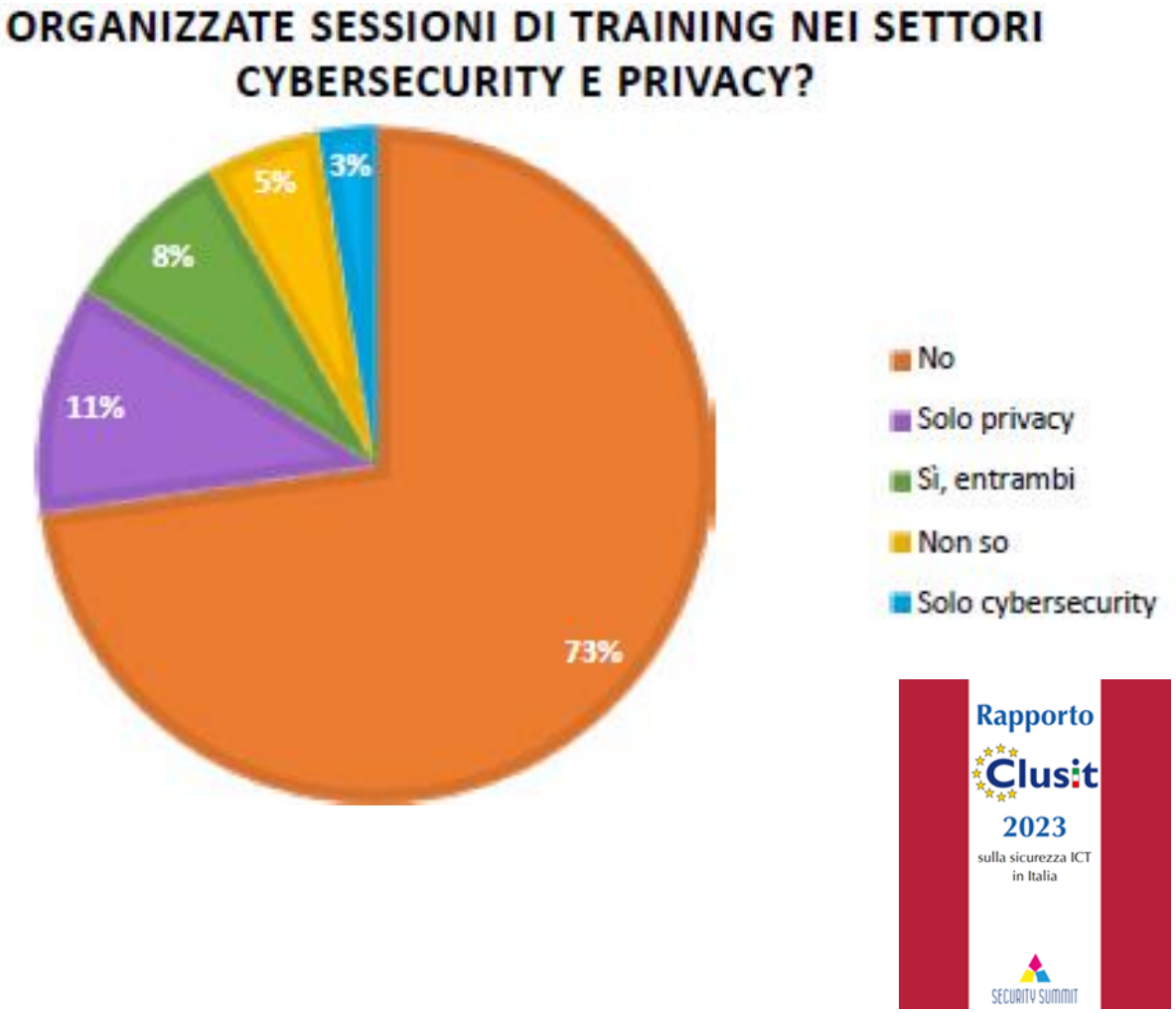
Nel **44%** dei casi non esiste **nessun responsabile** aziendale in materia di **Privacy e Cybersecurity**, un dato certamente preoccupante. Ma, se il 17% dispone almeno di un responsabile privacy, **solo il 2%** gestisce in autonomia le **responsabilità in materia di Cybersecurity**, informazione che mette in luce quanto ci sia ancora da fare in questo ambito. Sono solo **un quarto (25%)** le aziende virtuose che dispongono di **entrambi i responsabili**.

Rapporto Clusit 2023 sulla sicurezza ICT in Italia

SECURITY SUMMIT

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Contesto formazione e consapevolezza



Le risposte inerenti alla **formazione** in materia di **privacy e cybersecurity** sono un'ulteriore riprova di quanto si **investa ancora poco in questo ambito**: solo **l'11% delle aziende organizza sessioni di training** per il personale che comprendano anche tematiche di **Cybersecurity.** Un ulteriore **11% organizza formazione in materia di privacy**, mentre **il 73% non se ne occupa interamente.**

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Contesto PMI cyber

Le aziende italiane (Emilia Romagna) ***sono in prevalenza piccole e con un fatturato non elevato***

- *L'IT* ***non è in prevalenza gestito in azienda****.*

- *I* ***responsabili della Cybersecurity sono carenti*** *e la funzione stessa non è gestita in azienda: in caso di problemi* ***ci si rivolge all'esterno****.*

- *Si fa ancora* ***poco affidamento*** *sul* ***regolamento*** *sulla strumentazione informatica e sul* ***registro per il trattamento*** *dei dati personali.*

- ***Manca una procedura*** *ben definita per la gestione dei* ***data breach****.*

- ***Non si investe in formazione*** *in materia di privacy e Cybersecurity (soprattutto!)*

- ***Ai dispositivi personali è concessa la connessione alla rete aziendale*** *(e questo dovrebbe essere regolamentato).*

- *I* ***dispositivi mobili non*** *sono soggetti ad una* ***politica aziendale****.*

Contesto PMI cyber

DUE ELEMENTI DA CONSIDERARE PMI

•**Il primo riguarda** una differenza sostanziale in termini di **danno subito** tra gli incidenti in cui **lo *smart working* ha giocato un ruolo** e quelli in cui **non è stato** indicato come **elemento significativo**. Nella prima circostanza il costo ha raggiunto i 4,96 milioni di dollari, nella seconda, invece, scende a 3,89 milioni. Sembra dunque che le organizzazioni abbiano fatto molta fatica a adattare la propria gestione della ***cybersecurity* alle mutate condizioni lavorative**. Evidentemente, **nel momento in cui l'incidente è fuori dal perimetro fisico dell'azienda i tempi di reazioni sono più lenti** e la capacità di riconoscere tempestivamente l'attacco risulta compromessa.

•**Il secondo elemento** è l'ennesima conferma di come il **fattore umano sia ancora l'anello debole della catena**. Il **furto di credenziali-utente è ancora la causa più comune di incidenti** e allo stesso modo i **dati personali dei clienti** (come nome e cognome, e-mail e password) sono **coinvolti nel 44% dei casi.**

La **combinazione di questi due fattori finisce** per produrre un **circolo vizioso perché offre ai criminali i mezzi per ulteriori futuri attacchi**. Quest'ultimo dato conferma quanto riportato nel report Verizon dello scorso maggio dal quale emergeva che **nell'85% delle violazioni è coinvolto il fattore** umano sfruttato dai criminali attraverso diverse forme di **social engineering**, in particolare tramite phishing, presente nel 36% dei casi, oppure con la compromissione di email lavorative. **La difesa e la prevenzione, infatti, costano decisamente meno dei danni provocati dagli hacker e compagnia.**

Contesto cyber PMI ...conclusioni

.....peraltro, **non solo le responsabilità di cybersecurity**, ma addirittura **quelle IT** sono in prevalenza vissute come un **qualcosa di esterno all'azienda**, **da delegare** ad altri ogniqualvolta ciò sia percepito come possibile. Insomma, **l'informatica è un male necessario, e la cybersecurity a maggior ragione**.

Altre risposte, tuttavia, indicano come **questa delega sia operata con superficialità**, e senza realmente indagare se davvero sia efficace. **Si spera insomma di poter delegare ad altri il problema, quando si presentasse**, ma, come testimonia ad esempio la domanda relativa alla **gestione dei data breach**, **non c'è alcuna preparazione a monte**.

*Il modello è forse quello del **pompiere**. Come però ben sa chi ha subìto davvero un incendio, per l'azienda questo non basta: **i Vigili del Fuoco (quelli veri) sono i primi ad insistere sull'importanza della prevenzione**.*

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Le motivazioni che rallentano le organizzazioni nell'implementazione delle best practices per la sicurezza dei dati aziendali

Pensano di non essere vulnerabili.

Alcune organizzazioni ritengono di **essere di dimensioni così piccole da non rientrare nel novero dei target di un attacco informatico**. È una asserzione sbagliata e pericolosa. Infatti, la vulnerabilità dei dati rende le **piccole e medie imprese gli obiettivi ideali degli hacker**, soprattutto quando si tratta di **attacchi di tipo ransomware**. L'economia dei cyber criminali non mira all'azienda, ma al guadagno che può ottenere dai suoi dati. Per cui tutte le organizzazioni devono effettuare un **attento risk assessment dei propri asset e individuare le misure di sicurezza commisurate al proprio core business.**

Resistono al cambiamento.

Il verbo "trasformare" evoca un passaggio, una transizione, un **cambiamento del modus operandi** e, come si verifica ad ogni tentativo di rinnovamento, divide gli addetti ai lavori in due schiere opposte: quelli a favore, bendisposti alle innovazioni, e quelli contrari, che vorrebbero resistere al cambiamento. **Occorre avere il coraggio di abbandonare i vecchi schemi e approcciarsi al nuovo in maniera olistica: sposare le nuove tecnologie, le nuove metodologie e le nuove regole**.

Le motivazioni che rallentano le organizzazioni nell'implementazione delle best practices per la sicurezza dei dati aziendali

Sottostimano le conseguenze collaterali di un attacco cyber.

Quando si effettua la **stima dell'impatto** che potrebbe arrecare una minaccia nell'ambito della cybersecurity sono considerati **solo gli effetti principali** che può causare e non vengono presi in considerazione quelli secondari. Nel momento in cui si valuta un attacco informatico, troppo spesso, ci si concentra sui **costi diretti in relazione alla perdita o al furto delle informazioni di un'azienda** (ad esempio il database dei clienti).
Tuttavia, è l'infrastruttura nel suo complesso che viene invalidata dalla perdita o dal furto di tale componente e, pertanto, subire altri danni, **come la perdita di credibilità e di fiducia da parte dei clienti, calo di immagine, diminuzione dei ricavi**, ecc., con effetti devastanti che posso portare alla chiusura definitiva dell'attività.

Le motivazioni che rallentano le organizzazioni nell'implementazione delle best practices per la sicurezza dei dati aziendali

Monitorano le minacce utilizzando solo risorse interne.

Si tratta di un errore grave. È difficile, e in alcuni casi impossibile, **identificare le minacce utilizzando solo l'audit interno** perché, per un verso, **l'universo delle minacce è diventato molto complesso** e, dall'altro, si modifica continuamente. L'unica soluzione percorribile consiste nell'anticipare gli attacchi, piuttosto che difendere semplicemente l'organizzazione una volta che si verificano, perché -sempre più spesso – le conseguenze sono irrimediabili.

Per realizzare questa finalità occorre **attivare sistemi di monitoraggio e strumenti di scambio delle informazioni** che consentano di acquisire gli indicatori di compromissione (IoC) e gli indicatori di attacco (IoA) da fonti accreditate esterne all'organizzazione.

Innovazione & Cybersecurity
6 consigli pratici per evitare problemi

Perché la cybersecurity è un problema durante il processo di digitalizzazione

Da una parte, è vero che molti macchinari saranno acquistati per rinnovare le linee produttive e magari non immediatamente configurati per sfruttare queste caratteristiche di connettività.

Dall'altra, però, come per tutte le innovazioni tecnologiche, **la nuova complessità può portare le aziende *a prendere scorciatoie nei requisiti non funzionali* di progetto**. **Prima vittima, in questo, può essere la sicurezza, che rischia appunto di essere trascurata.**

- Il primo consiglio è di accertarsi che nella **redazione dei progetti** *«by design»* siano prese in **considerazione le esigenze di sicurezza** (il passaggio progettuale è obbligatorio, ma la sua qualità e approfondimento sono sostanzialmente una decisione dell'azienda).

- In secondo luogo, se l'azienda ha **personale IT interno**, o consulenti fidati, **dovrebbero essere coinvolti nella fase di progetto** (anche se normalmente non si occupano del processo produttivo).

Innovazione & Cybersecurity
6 consigli per evitare problemi

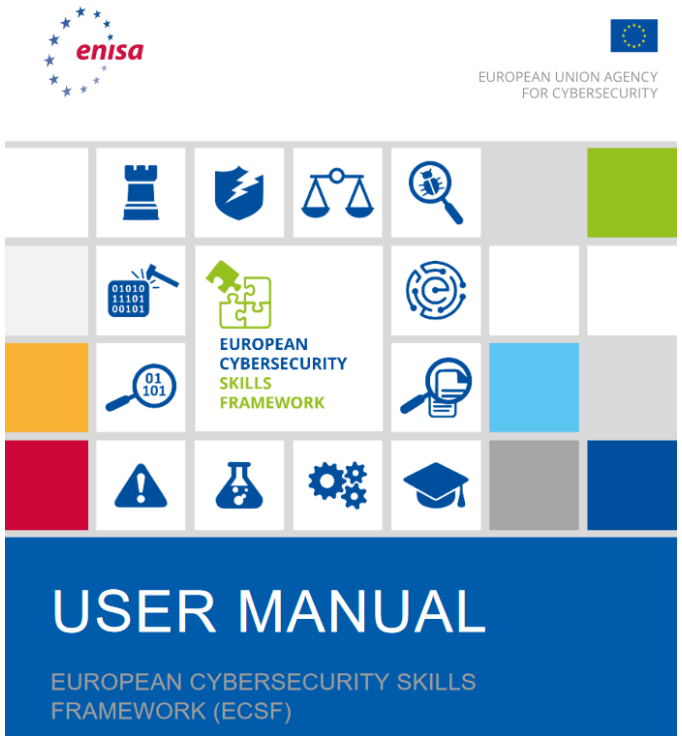
- E’ opportuno effettuare una **verifica della sicurezza dell’infrastruttura a termine** del progetto, **eseguendo un security assessment** con una società specializzata che abbia credenziali nel mondo dei sistemi industriali.

- E’ previsto, oltre una soglia di investimento, che ci sia un professionista esterno che attesti **la sicurezza «safety»** del macchinario industry 4.0. Allo stesso modo bisognerebbe che anche nel progetto **ci sia un punto dedicato alla sicurezza logica**. Così come ora per legge c’è una quota del progetto riservata **alla sicurezza dei lavoratori**, ce ne dovrebbe essere una per la **messa in sicurezza logica** delle macchine.

- Di converso, bisogna **prevedere tutti i requisiti legali (by design) e di compliance,** per non incorrere in sanzioni rilevanti in caso di violazioni dei dati.

- E’ importante che nella **selezione dei partner/ fornitori** vengano considerate le **competenze nel campo della cybersecurity** come fattore necessario e abilitante (best practice).

Competence: European Cybersecurity Skills Framework (ECSF)



«***Ha l'obiettivo di rafforzare la cultura della sicurezza informatica fornendo un comune linguaggio europeo tra i Paesi comunitari, facendo un passo essenziale in avanti verso il futuro digitale dell'Europa***.»

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

Profile Title	Chief Information Security Officer (CISO)
Alternative Title(s)	Cybersecurity Programme Director Information Security Officer (ISO) Information Security Manager Head of Information Security IT/ICT Security Officer
Summary statement	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.
Deliverable(s)	• Cybersecurity Strategy • Cybersecurity Policy
Main task(s)	• Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution • Supervise the application and improvement of the Information Security Management System (ISMS) • Educate senior management about cybersecurity risks, threats and their impact to the organisation • Ensure the senior management approves the cybersecurity risks of the organisation • Develop cybersecurity plans • Develop relationships with cybersecurity-related authorities and communities • Report cybersecurity incidents, risks, findings to the senior management • Monitor advancement in cybersecurity • Secure resources to implement the cybersecurity strategy • Negotiate the cybersecurity budget with the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources

Key skill(s)	• Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Analyse and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Anticipate required changes to the organisation's information security strategy and formulate new plans
	• Define and apply maturity models for cybersecurity management • Anticipate cybersecurity threats, needs and upcoming challenges • Motivate and encourage people
Key knowledge	• Cybersecurity policies • Cybersecurity standards, methodologies and frameworks • Cybersecurity recommendations and best practices • Cybersecurity related laws, regulations and legislations • Cybersecurity-related certifications • Ethical cybersecurity organisation requirements • Cybersecurity maturity models • Cybersecurity procedures • Resource management • Management practices • Risk management standards, methodologies and frameworks
e-Competences (from e-CF)	A.7. Technology Trend Monitoring — Level 4 D.1. Information Security Strategy Development — Level 5 E.3. Risk Management — Level 4 E.8. Information Security Management — Level 4 E.9. IS-Governance — Level 5

2.12 PENETRATION TESTER

Profile Title	Penetration Tester
Alternative Title(s)	Pentester Ethical Hacker Vulnerability Analyst Cybersecurity Tester Offensive Cybersecurity Expert Defensive Cybersecurity Expert Red Team Expert Red Teamer
Summary statement	Assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.
Mission	Plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. Identifies vulnerabilities or failures on technical and organisational controls that affect the confidentiality, integrity and availability of ICT products (e.g. systems, hardware, software and services).
Deliverable(s)	• Vulnerability Assessment Results Report • Penetration Testing Report
Main task(s)	• Identify, analyse and assess technical and organisational cybersecurity vulnerabilities • Identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity vulnerabilities • Test systems and operations compliance with regulatory standards • Select and develop appropriate penetration testing techniques • Organise test plans and procedures for penetration testing • Establish procedures for penetration testing result analysis and reporting • Document and report penetration testing results to stakeholders • Deploy penetration testing tools and test programs
Key skill(s)	• Develop codes, scripts and programmes • Perform social engineering • Identify and exploit vulnerabilities • Conduct ethical hacking • Think creatively and outside the box • Identify and solve cybersecurity-related issues • Communicate, present and report to relevant stakeholders • Use penetration testing tools effectively • Conduct technical analysis and reporting • Decompose and analyse systems to identify weaknesses and ineffective controls • Review codes assess their security
Key knowledge	• Cybersecurity attack procedures • Information technology (IT) and operational technology (OT) appliances • Offensive and defensive security procedures • Operating systems security • Computer networks security • Penetration testing procedures • Penetration testing standards, methodologies and frameworks • Penetration testing tools • Computer programming • Computer systems vulnerabilities • Cybersecurity recommendations and best practices • Cybersecurity-related certifications
e-Competences (from e-CF)	B.2. Component Integration B.3. Testing B.4. Solution Deployment B.5. Documentation Production	Level 4 Level 4 Level 2 Level 3

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Strumenti: UNI CEI EN ISO/IEC 27001:2017(22) contenuti

ISO 27001:2017 SGSI

- 1 - Scopo e campo di applicazione
- 2 - Riferimenti normativi
- 3 -Termini e definizioni
- 4 - Contesto dell'organizzazione
- 5 - Leadership
- 6 - Pianificazione
- 7 - Supporto
- 8 - Attività operative
- 9 - Valutazione delle prestazioni
- 10 -Miglioramento

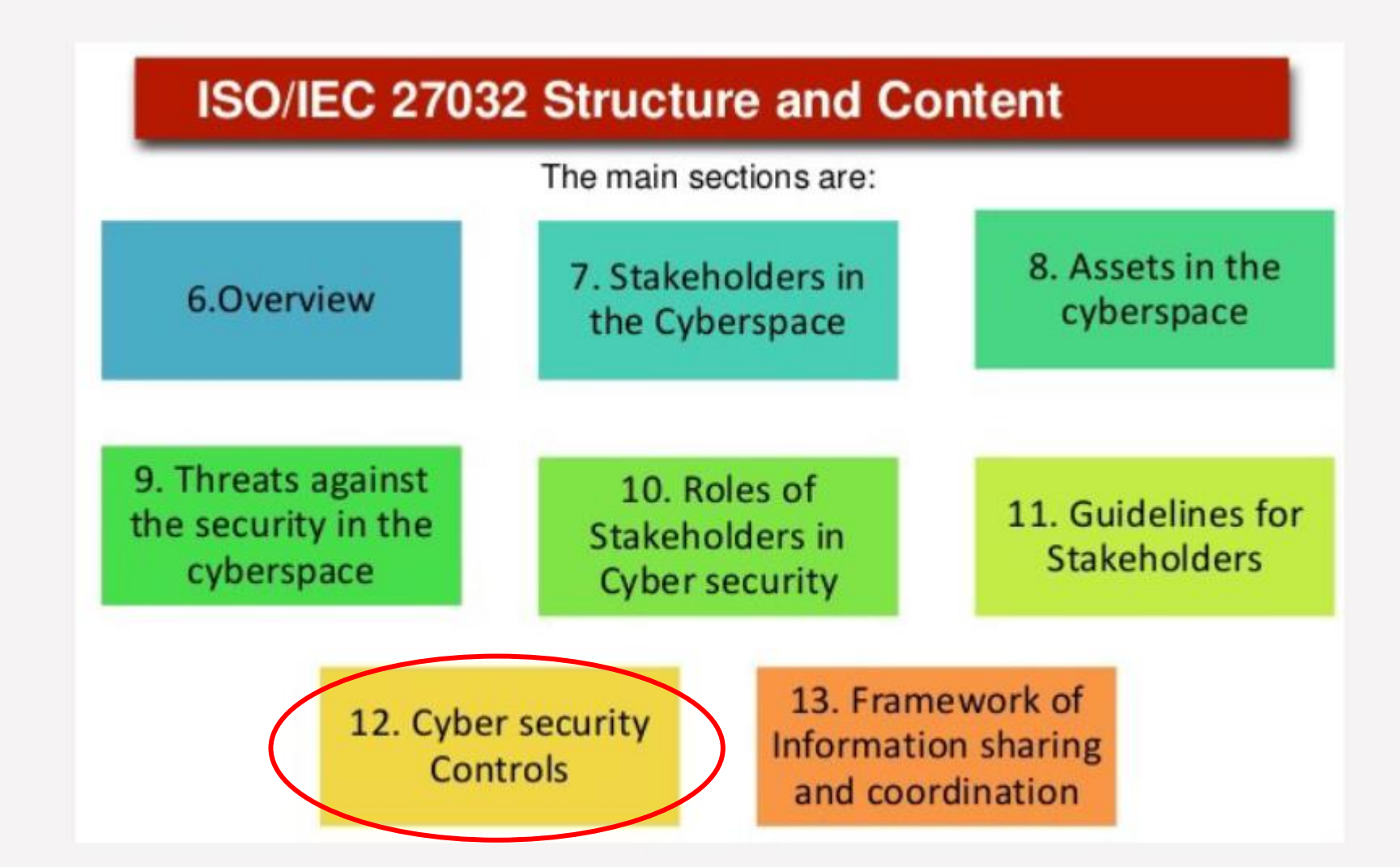
+

- A.5 Politiche per la sicurezza delle informazioni
- A.6 Organizzazione della sicurezza delle informazioni
- A.7 Sicurezza delle risorse umane
- A.8 Gestione degli asset
- A.9 Controllo degli accessi
- A.10 Crittografia
- A.11 Sicurezza fisica ed ambientale
- A.12 Sicurezza delle attività operative
- A.13 Sicurezza delle comunicazioni
- A.14 Acquisizione, sviluppo e manutenzione dei sistemi
- A.15 Relazioni con I fornitori
- A.16 Gestione degli incidenti relative alla sicurezza delle informazioni
- A.17 Sicurezza delle informazioni nella gestione della business continuity
- A.18 Compliance

ANNEX A 27001 CONTROLLI /CONTROMISURE
(Art. 32 GDPR MISURE DI SICUREZZA)

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

UNI CEI EN ISO/IEC 27032
Guidelines For Cyber Security



DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Strumenti: GDPR come strategia cyber

Cyberecurity, cosa cambia con il GDPR

Sino ad oggi molte aziende hanno ragionato **esclusivamente in ottica disaster recovery**, un approccio che alla luce **dell'entrata in vigore del GDPR non è più sufficiente**, perché la nuova normativa europea al suo interno possiede degli elementi che spingono maggiormente le aziende ad **attrezzarsi in un'ottica più complessiva di difesa e continuità per assicurare la conformità e i diritti degli interessati**. In effetti, anche se la continuità operativa non viene citata direttamente, **l'articolo 32 del GDPR** è abbastanza esplicito: **il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:**

a) la pseudonimizzazione e la cifratura dei dati personali;
b) ***la capacità di assicurare su base permanente*** *la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
c) la ***capacità di ripristinare*** *tempestivamente la disponibilità e l'accesso dei dati personali* ***in caso di incidente fisico o tecnico;***
d) **una procedura** per testare, verificare e **valutare regolarmente l'efficacia delle misure tecniche** e organizzative al fine di garantire la sicurezza del trattamento.

Questi punti presuppongono che **ogni organizzazione debba avere implementato una vera strategia di continuità operativa**, che sia periodicamente testata in modo da poterne dimostrare l'efficacia.

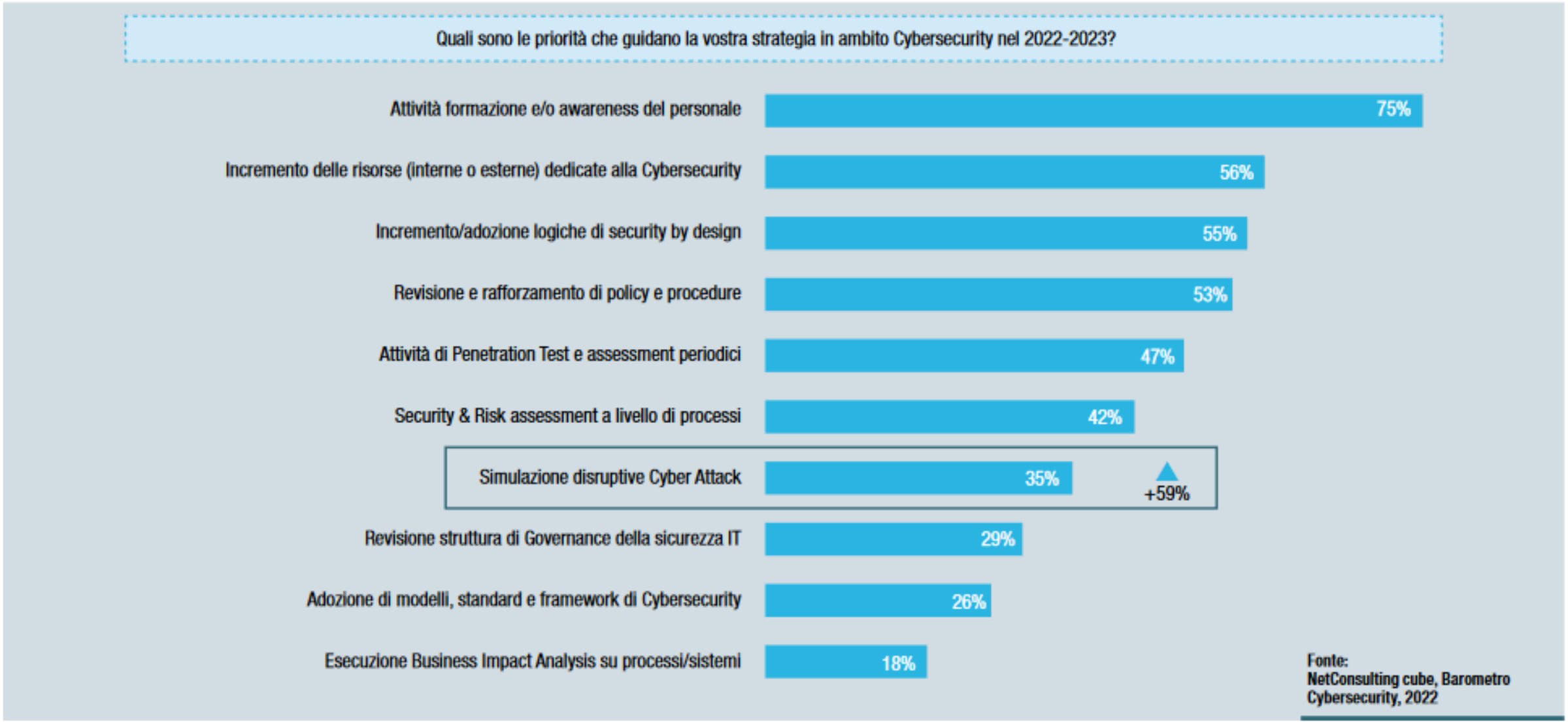
La sicurezza è una questione strategica

C’è un’attenzione significativa alla cyber security
Ma non è sufficiente.
La sicurezza informatica deve rappresentare un **obiettivo dal punto di vista professionale e aziendale**. Pertanto, la **strategia** da mettere in atto **deve essere condivisa** sia dal **singolo che dall’intera struttura aziendale**. Un’organizzazione che intende avviare un efficace e affidabile **percorso di Digital Transformation non deve più osservare la Cyber Security come un requisito dell’IT**, ma deve includere **le strategie di sicurezza tra gli obiettivi di business** per realizzare con successo la propria missione.

L’adozione di un approccio **“secure by design”** aiuta ad **anticipare i rischi** degli attacchi informatici. Ma occorre investire anche **in sistemi di gestione**: per esempio l’uso di una **soluzione di Data Management** può indicare in anticipo i rischi per la sicurezza informatica.

Per esempio….l’efficacia **di un progetto di digitalizzazione** può essere rafforzata con l’adozione **di un sistema di Identity Management** che assicuri una gestione semplificata e controllata degli accessi ai propri dati, oppure spostando i propri **asset in ambienti ISO27001 compliance** per proteggerli da possibili violazioni o manomissioni.

Cybersecurity e transizione digitale



Cosa può insegnarci un attacco cyber?

- Lo stato della cybersecurity al momento dell'attacco.
- L'attacco e le sue conseguenze.
- I punti deboli del sistema.
- Perché nessuno ha rilevato le vulnerabilità?
- Quali conseguenze?


Il Sole
24 ORE
del lunedì

L'esperto risponde
Il tema di oggi
Età e contributi: tutte le condizioni per accedere alle pensioni di vecchiaia

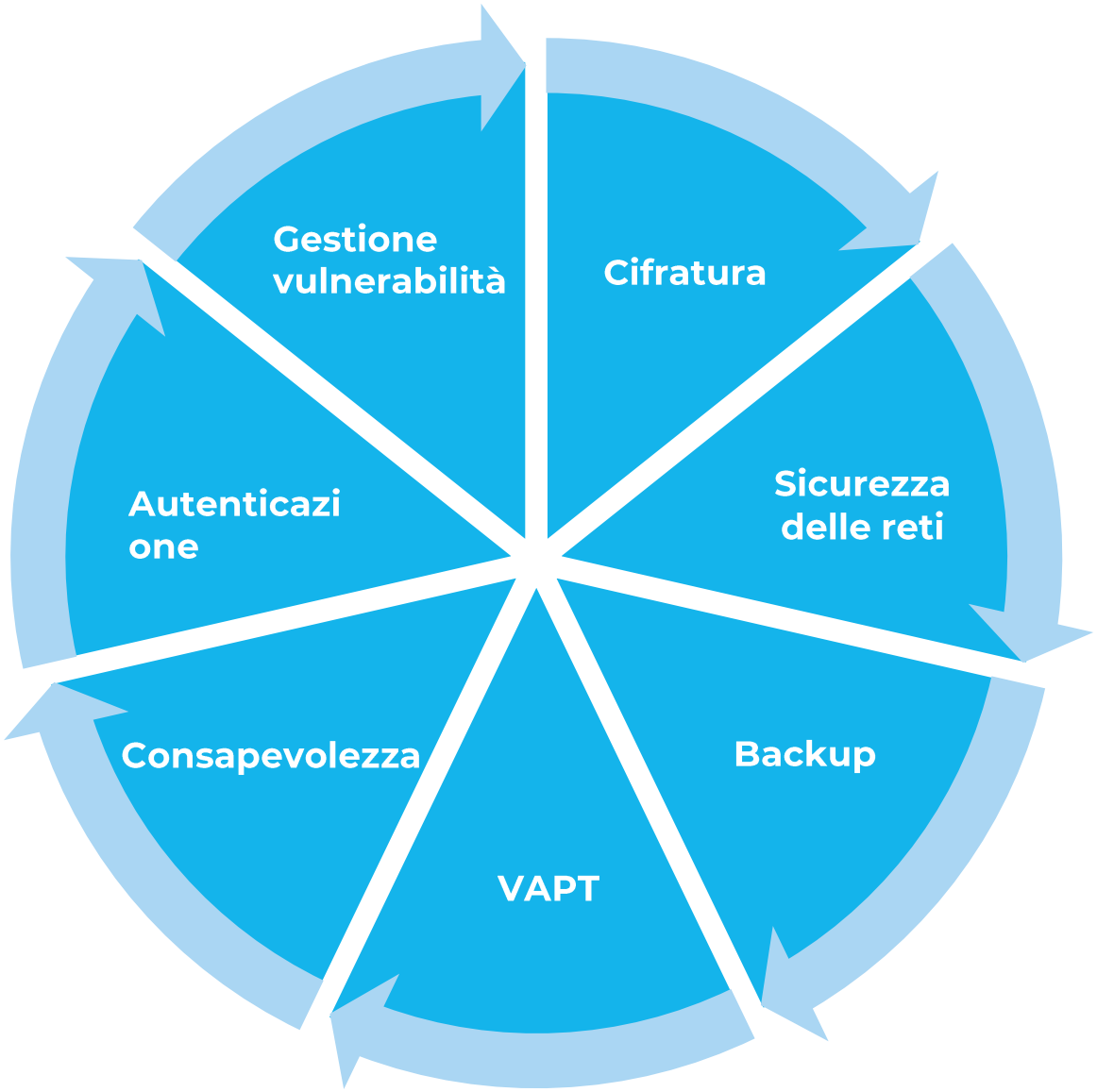
Lunedì 27 Febbraio 2023
Anno 159°, Numero 57

Sicurezza IT
Pmi, è cyber allarme: sempre più nel mirino degli attacchi hacker

Nel 2022 crescono del 45% le denunce di assalti ai dati con richiesta di riscatto
Manifattura e servizi colpiti nel 53% dei casi

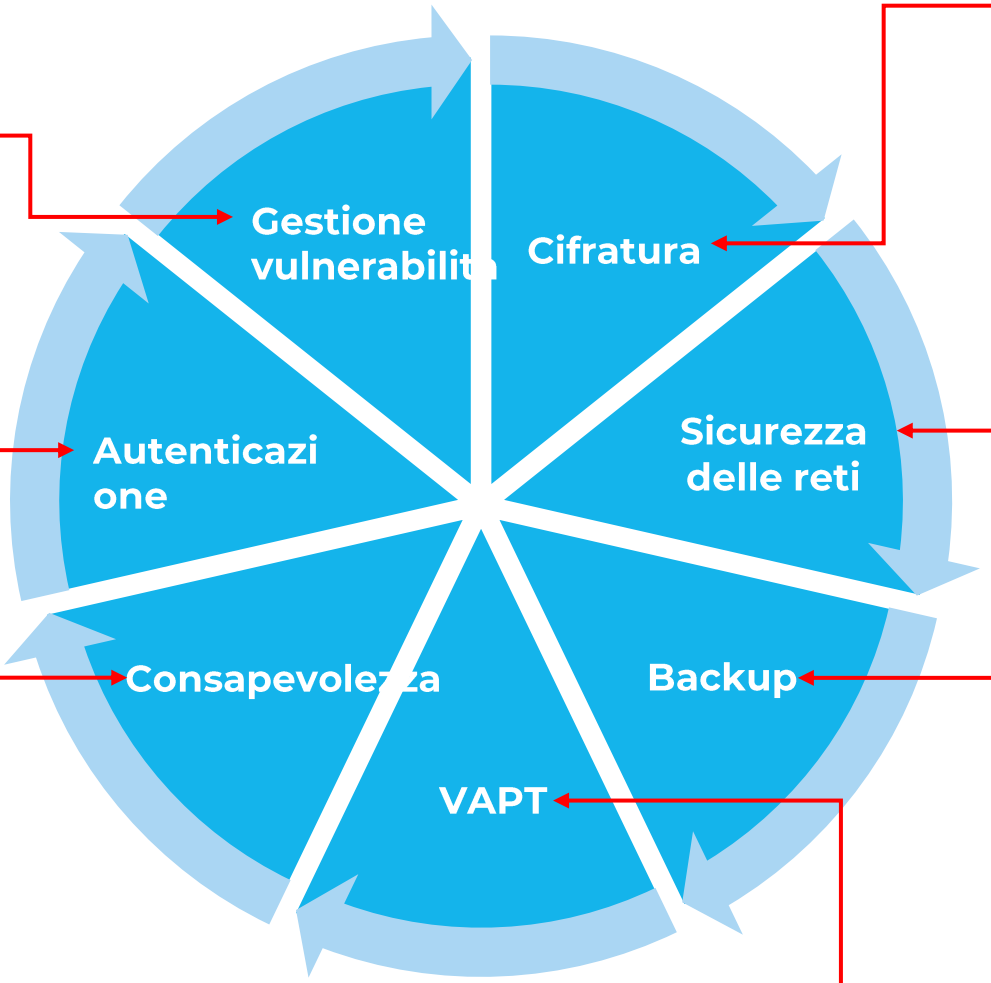
DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Lo stato della cybersecurity al momento dell'attacco



DataConSec
DATA PROTECTION - CONSULTING - SECURITY

I punti deboli del sistema



3) Mancata gestione delle vulnerabilità

4) Archivi non cifrati

5) NAS accessibili dall'esterno bypassando le

2) Debolezza dei sistemi e degli standard di

6) Mancato monitoraggio e test

1) Vettore di attacco: mail di phishing

7) VAPT svolto soltanto una volta, cinque anni prima dell'incidente

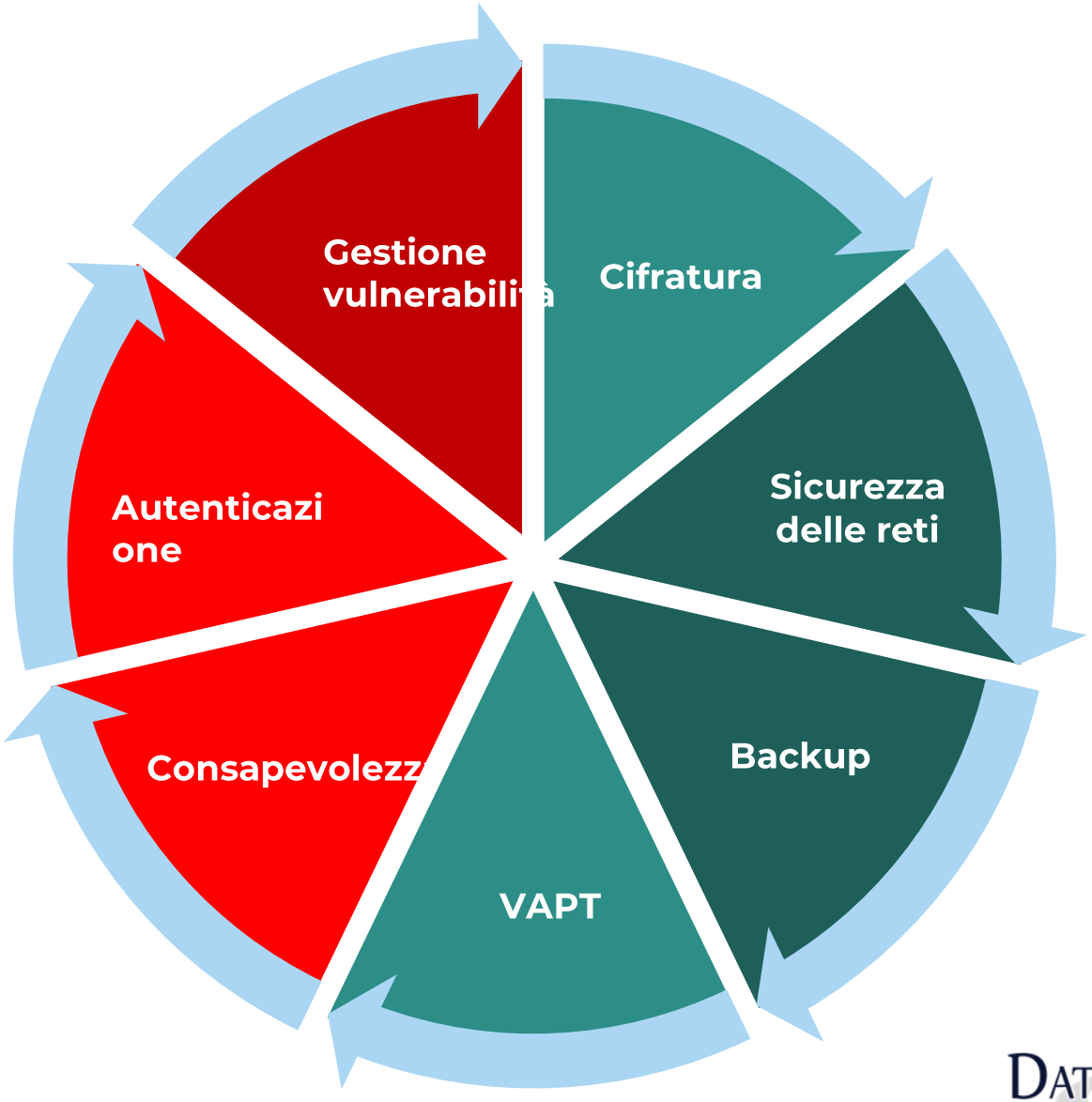
DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Come è avvenuto l'attacco?

- **Mail di phishing,** come veicolo dell'attacco: l'attaccante entra nella rete aziendale;
- **Tramite una vulnerabilità non gestita**, l'attaccante acquisisce lo *status di amministratore* del Domain Controller: massimo livello di accesso e di privilegi sulla rete aziendale;
- **Il codice malevolo** viene eseguito e diffuso nella rete aziendale, con modalità tali da evitare la rilevazione da parte dei sistemi di protezione: in questo modo sono **raggiunti i server e cifrati gli archivi**, senza dare modo di scollegarli dalla rete aziendale;
- Gli attaccanti **cancellano la quasi totalità dei log** che avrebbero consentito la ricostruzione degli eventi.

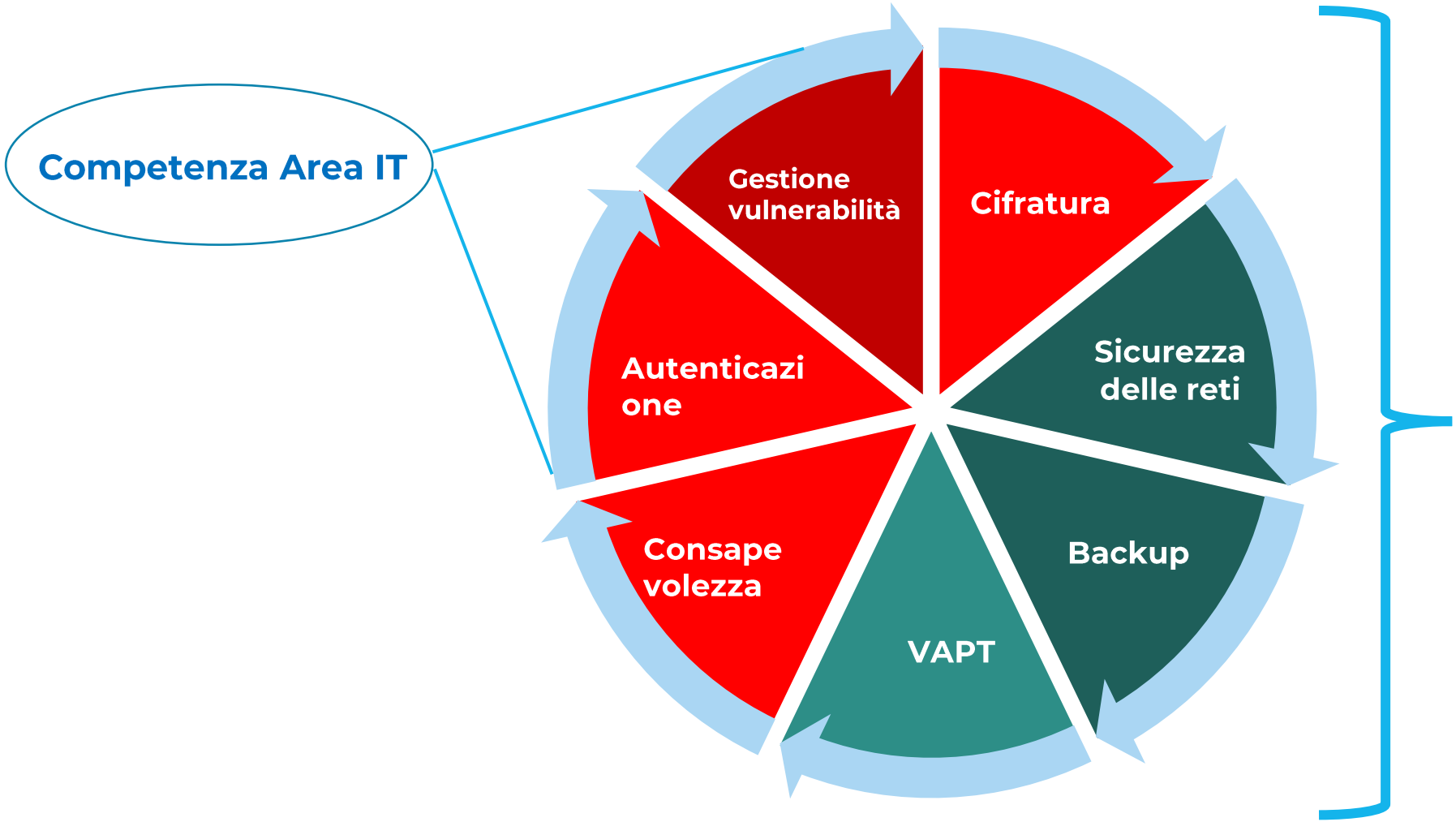
DataConSec
DATA PROTECTION - CONSULTING - SECURITY

L’effettivo stato della sicurezza



DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Perché nessuno ha rilevato le vulnerabilità?



Carenze del sistema di sicurezza:

- assenza di governance e management del rischio cyber;
- mancata valutazione del rischio cyber;
- vaghezza delle responsabilità interne;
- nessuna progettazione e visione d'insieme del sistema di sicurezza;
- Insufficiente consapevolezza degli utenti

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Quali conseguenze?

- Indisponibilità dei server: **sito internet irraggiungibile**;
- Indisponibilità dei backup: dati di produzione, del personale e amministrativi indisponibili; pertanto: **impossibilità di pubblicare i periodici, di elaborazione delle buste paga e della fatturazione**;
- **Notifica della violazione al Garante per la Protezione dei Dati Personali e agli interessati** (migliaia di persone tra clienti, dipendenti e fornitori);
- Denuncia alla Polizia Postale;
- Interessamento del **Computer Security Incident Response Team – Italia**;
- Gestione delle **comunicazioni con gli attaccanti**.

Che fare?

Gestione dell'attacco:

1. Individuazione del punto di attacco;
2. Ricostruzione dei profili di amministrazione;
3. Isolamento dei backup e interruzione delle comunicazioni da e verso internet;
4. Rilevazione dello stato di compromissione di tutte le macchine;
5. ***…senza la chiave di decifratura, i dati non potranno essere recuperati.***

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Conclusioni

- Il sistema **era solo formalmente protetto**: gli argomenti fondamentali della sicurezza prevedevano misure tecniche dedicate, ma:
  1. *Non selezionate e progettate sulla base all'esposizione al rischio cyber specifico di quell'organizzazione;*
  2. *Non implementate tenendo conto dell'infrastruttura informatica nel suo complesso;*
  3. *Non amministrate in modo da renderne effettiva l'efficacia;*
  4. *Non ne è stata misura l'efficacia con periodici interventi di test;*
- Non è stata valutata **la consapevolezza degli utenti** delle tecnologie in merito ai rischi cyber dell'organizzazione;
- Non sono stati previsti **sistemi di sicurezza gestita**, in grado di individuare tempestivamente gli attacchi verso i quali gli strumenti tradizionali non sono efficaci.

In definitiva, manca la governance del sistema di difesa dalle minacce cyber

DataConSec
DATA PROTECTION - CONSULTING - SECURITY

Link di approfondimento generali:

https://clusit.it/
https://www.garanteprivacy.it/
https://www.enisa.europa.eu/
https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6642
https://www.acn.gov.it/

Contatti:

Domenico Carnicella - d.carnicella@dataconsec.com
Juri Giordani – j.giordani@dataconsec.com
Alessandro Rodolfi - a.rodolfi@dataconsec.com

DATACONSEC
DATA PROTECTION · CONSULTING · SECURITY

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Il Centro di Competenza Cyber 4.0: attività e nuovi strumenti di finanziamento

- **Filippo Silvestri,** *Responsabile Business Development, Cyber 4.0*

Cyber 4.0

Centro di competenza nazionale ad alta specializzazione sulla cybersecurity, promosso e finanziato dal MIMIT, inizialmente nel piano Industria 4.0 e ora soggetto attuatore PNRR

- Avviato nel 2020, **Operativo da Aprile 2021, HQ al Tecnopolo Tiburtino – Roma**
- **8 Organismi di ricerca, 1 Istituzione pubblica, 35 Partner privati**
- **Supporto a imprese e PA**
- Possibilità di erogare **servizi commerciali**
- **Partecipazione a iniziative finanziate**

- **13+ Milioni di Euro per (co)finanziare la transizione digitale sicura (2023-2025)**

Compagine associativa

Università di Roma Tor Vergata

ROMA TRE UNIVERSITÀ DEGLI STUDI

UNIVERSITÀ DEGLI STUDI DELL'AQUILA

SAPIENZA UNIVERSITÀ DI ROMA

UNIVERSITÀ DEGLI STUDI DELLA TUSCIA

UNIVERSITÀ DEGLI STUDI DI CASSINO E DEL LAZIO MERIDIONALE

LUISS

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

sogei

Posteitaliane

FORMIT

INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO

Clusit
Associazione Italiana per la Sicurezza Informatica

TIM

Consiglio Nazionale delle Ricerche

AlmavivA

YOROI

LEONARDO

BV TECH
Securing the Future.

CY4GATE
ELETTRONICA GROUP

aizoon
TECHNOLOGY CONSULTING

NETGROUP

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

SISTEMI FORMATIVI CONFINDUSTRIA

FONDAZIONE E. AMALDI

POLO DI INNOVAZIONE AUTOMOTIVE

LAND

TECHNO CENTER

TELESPAZIO
a LEONARDO and THALES company

ThalesAlenia Space
a Thales / Leonardo company

DP

DI.GI. Academy

HMS IT

LAZIO CONNECT

INNOVERY
INNOVATION DISCOVERY

RADIO6ENSE

S&A
SISTEMI & AUTOMAZIONE

ARPEX
Environment Trentino

PRISMA
improve your business

mediavoice

TECNORAD
PERSONAL DOSIMETRY SERVICE

Formazione

Attività istituzionali | Servizi di mercato | Progetti finanziati | Networking

- **Corsi co-finanziati per PMI e PA**
- **Supporto nell'elaborazione strategie di formazione**
- **Webinar gratuiti, eventi informativi, workshop**
- **Attività di formazione extra accademica**
  - **CyberX Mind4Future**
  - **ITS**
- **Supporto a enti e istituzioni**
  - **Accademia Cybersicurezza Lazio** (start-up della scuola, definizione programmi, piani formativi, profili docenti e loro selezione e formazione, produzione materiali, controllo qualità, piano awareness nelle scuole)

Orientamento PMI

Attività istituzionali | Servizi di mercato | Progetti finanziati | Networking

Orientamento PMI

Vademecum PMI

- **12 azioni** per un business sicuro
- Basato su 12 Step ENISA

Ministero delle Imprese e del Made in Italy

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

UNINDUSTRIA UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE ROMA • FROSINONE • LATINA • RIETI • VITERBO

Postura cyber security PMI

- Basato su **Framework Nazionale Cybersecurity e Data Protection**
- **Analisi** aree di intervento prioritario, remediation roadmap, impatto economico e benefici
- **Estensione nazionale** – DIH, PID, Case Tecnologie Emergenti

Roadshow Cyber 4.0

- Coinvolgimento DIH e altre realtà attive in regione (Polizia Postale, CTE, etc.)
- Sessioni di info/ formazione e incontri con esperti, case studies e buone pratiche, quick Cyber Checkup
- Aggregazione di comunità locali per **information sharing**

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Orientamento imprese e PA

Attività istituzionali | Servizi di mercato | Progetti finanziati | Networking

Demo Lab e Test Before Invest – T4

1 SVILUPPARE UNA SOLIDA CULTURA DELLA CIBERSICUREZZA

2 FORNIRE UNA FORMAZIONE APPROPRIATA

3 GARANTIRE UN'EFFICACE GESTIONE DEI TERZI

4 SVILUPPARE UN PIANO DI RISPOSTA AGLI INCIDENTI

5 RENDERE SICURO L'ACCESSO AI SISTEMI

6 RENDERE SICURI I DISPOSITIVI

7 RENDERE SICURA LA PROPRIA RETE

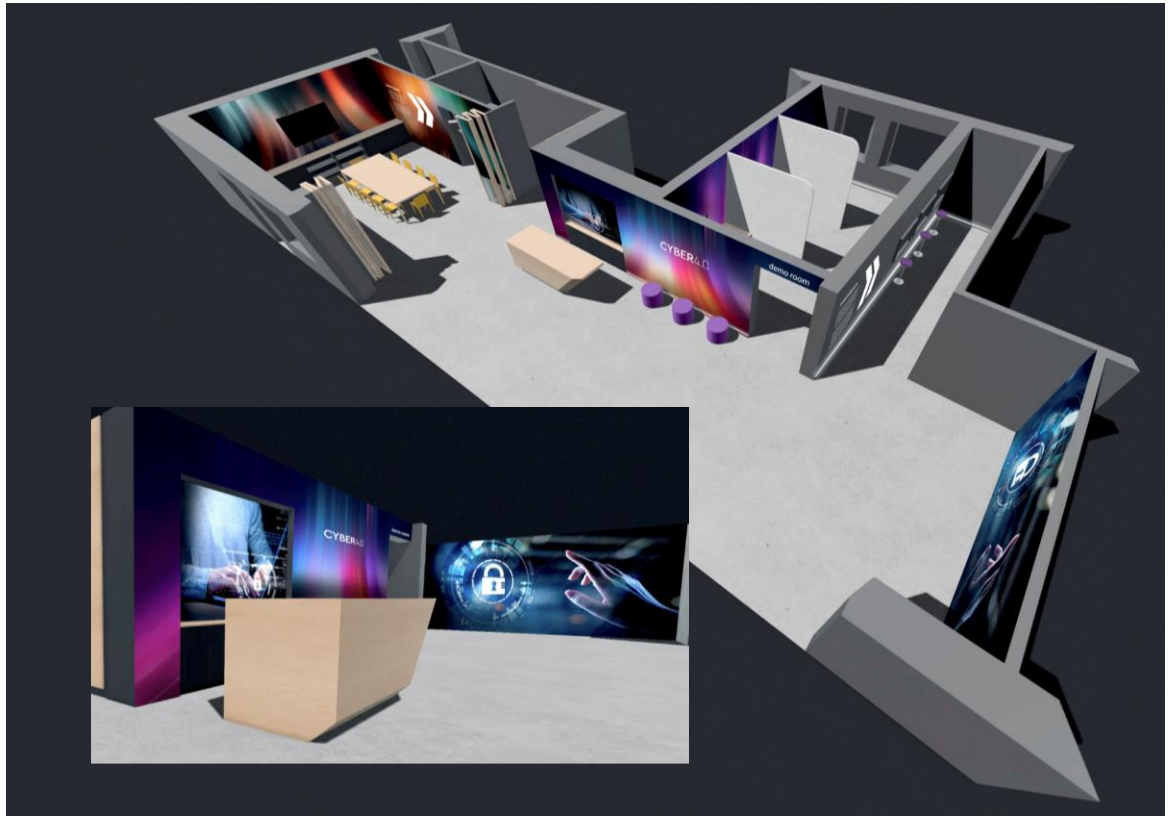
8 MIGLIORARE LA SICUREZZA FISICA

9 RENDERE SICURI I BACKUP

10 LAVORARE CON IL CLOUD

11 RENDERE SICURI I SITI ONLINE

12 CERCARE E CONDIVIDERE LE INFORMAZIONI



Orientamento imprese e PA

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Attività istituzionali | Servizi di mercato | Progetti finanziati | Networking

Strategic Advisory Istituzionale

- Position paper, benchmark, analisi, osservatori dedicati per advisory strategico alle istituzioni di riferimento
- Sviluppare azioni volte a rafforzare la collaborazione con Agenzia di Cybersicurezza Nazionale e MIMIT, anche alla luce della Strategia Nazionale di Cybersecurity

- **Analisi di mercato OT Security**
- **Strategia Industria Cyber Nazionale**
- **Osservatorio standard e normative cyber** (Ita e UE)
- **Osservatorio Cyber Security Framework e settori specifici** (es. sanità, finance, etc.)
- **Rischio terze parti**
- **Studio di fattibilità ISAC PMI**
- **Analisi nazionale della percezione del rischio di cybersecurity**
- **Supporto e partecipazione al policy making nazionale e EU**
- **Approfondimenti su tematiche verticali**
  - IoT
  - Metaverso
  - SCADA/ ICS

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Progetti di innovazione finanziati dal Centro

- Alto TRL, breve-media durata

CORE CYBER SECURITY

- **Cofinanziamento 2.2 M€**, budget totale progetti ca. 7 M€
- **15 progetti finanziati** (2021-2023), 29 aziende coinvolte – 80% PMI innovative e start-up

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

PNRR - Supporto all'innovazione

Attività istituzionali | Servizi di mercato | Progetti finanziati | Networking

Azioni co-finanziabili con intensità di aiuto correlata alla dimensione aziendale

- Audit tecnico, valutazione maturità tecnologica – **Assessment**
- Prova prima dell'investimento – **Test-before-invest**
- **Formazione**
- Consulenza su proprietà intellettuale
- Consulenza su **accesso ai finanziamenti**
- Consulenza su **innovazione tecnologica di processo e di prodotto, sensibilizzazione e networking**
- **Progettazione dell'intervento di innovazione**

Co-finanziamento

- Micro – 70-100%
- Piccole – 70-100%
- Medie – 60-90%
- Grandi – 40-50%

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Servizi di mercato a catalogo

Servizi che il Centro può erogare attraverso i propri soci

Identificazione e gestione dei rischi	• Cyber risk assessment and management • Risk monitoring • Vulnerability assessment e Penetration Testing • Threat Intelligence • Monitoraggio della supply chain
Protezione dei Dati	• Data Protection Office as as service • Data protection assessment • Privacy governance • Data protection impact assessment
Protezione dei Sistemi	• Identity and access management, Identity governance and administration • Network security • End Point security • Defence in depth • Patch management
Consulenza	• Consulenza tecnica, organizzativa, strategica in merito a: ICS, SCADA, IoT, CLOUD • Ricerca on demand, in collaborazione con il mondo accademico • Innovation Ecosystem
Monitoraggio e rilevamento minacce cyber	• Cyber threat intelligence e cyber threat modelling, SIEM, Threat detection, Proactive monitoring • Sistemi di early warning e rilevamento attacchi • Ransomware readiness
Risposta e gestione degli incidenti	• Orientamento e consulenza in merito a: SOC, CSIRT / CERT as a services • Supporto alla definizione di un modello (tecnico ed organizzativo) per la gestione degli incidenti informatici • Supporto alla gestione operativa di incidenti cyber
Certificazione	• Supporto per l'ottenimento di certificazioni in ambito information security e cybersecurity • Laboratorio di Valutazione di Sicurezza accreditato dall'organismo di certificazione OCSI
Formazione	• A catalogo • Custom • Piani di awareness

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

European Digital Innovation Hub

Attività istituzionali | Servizi di mercato | **Progetti finanziati** | Networking

Digital Europe – EDIH NEST

The **Network for European Security and Trust** is a one-stop shop for **cybersecurity solutions and capacity building initiatives**, targeting **SMEs and Public Administration of Central Italy**.

- Partners: **Cyber 4.0** (Coordinator), **DIH Lazio, DIH Umbria, DIH Abruzzo, Innova**
- Budget: **4.7 M€**
- Duration: **36 months** (2023-2025)
- Endorsements and collaborations: **National Cybersecurity Agency**, **Regione Lazio**, **Enterprise Europe Network, Italian Banking Association**

Cybersecurity tools and services

Facilities for test-before-invest

Capacity building initiatives

Assistance for access to finance and funding

Innovation ecosystems

EU regulatory framework, policies and strategies


SEAL OF EXCELLENCE

European Commission

European Commission

Digital Europe Programme

The project proposal

101120871 — NEST

"NEST - Network for European Security and Trust"

submitted under the Digital Europe Programme call

DIGITAL-2022-EDIH-03-INITIAL — Initial Network of European Digital Innovation Hubs

by

Associazione Cyber 4.0 and other participants

following evaluation by an international panel of independent experts

was recognised as a high-quality project proposal in a highly competitive evaluation process

Case delle Tecnologie Emergenti

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

MIMIT – Case delle Tecnologie Emergenti

CAGLIARI DIGITAL LAB

Valore totale progetto: € 12.550.000 – **Durata**: 24 mesi – **Decorrenza**: 02/02/2023

Allestimento:

- **piattaforma di quantum computing** per sperimentazione di soluzioni per le smart cities;
- **infrastruttura 5G indoor**
- **infrastruttura 5G outdoor e mobile edge computing**;
- **piattaforma in cloud con nodi adatti allo sviluppo di applicazioni di Intelligenza Artificiale e Deep Learning**;
- **piattaforma di open APIs** per l'integrazione dei servizio.

Attività Cyber 4.0: soluzioni di cybersecurity per tutti i sistemi e applicativi sviluppati, animazione, gestione comunicazione/divulgazione

PESARO CTE SQUARE

Valore totale progetto: € 10.977.000 – **Durata**: 24 mesi – **Decorrenza**: 02/02/2023

Allestimento:

- **Laboratorio Attivo** per ricerca, sviluppo, e sperimentazione in ambiente reale, trasferimento tecnologico di tecnologie innovative in ambiente urbano
- **Innovation Accelerator:** Startup building, Hackathon, Open Call, incubazione e accelerazione.
- **ICT Skill Transfer**: Coinvolgimento attivo end user

Attività Cyber 4.0: soluzioni di cybersecurity per tutti i sistemi e applicativi sviluppati, animazione, gestione comunicazione/divulgazione

La rete di collaborazioni istituzionali

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Attività istituzionali | Servizi di mercato | Progetti finanziati | **Networking**

- **MIMIT**
  - Network dei **Competence Center**
  - Network delle **CTE**
- **ACN**
- **Regione Lazio**
- **Accordi e partnership a livello nazionale**
  - Partnership con **rete dei DIH di Confindustria**
  - Collaborazione con **rete dei PID delle Camere di Commercio**
  - Europe Enterprise Network
  - Protocollo d'Intesa con **Società Italiana di Intelligence (SOCINT)**
  - MoU **Quantum for Space**
  - Protocollo d'Intesa con **Fondazione Amaldi**

- **Networking internazionale**
  - **EDIH** Network
  - **Ad Hoc Working Group su European Cybersecurity Skills Framework di ENISA**
  - Membri di **ECSO, European Cybersecurity Organization**
  - Protocollo di intesa con **Agenzia Catalana di Cybersecurity**
  - Membri di **Global Cyber Alliance**
  - Membri dello Stakeholder Group di **EU CyberNet**
  - Advisory Board **GFCE, Global Forum for Cyber Expertise**

Centri Competenza– Strategia MIMIT 2023

MINISTRO IMPRESE E MADE IN ITALY

Atto di indirizzo per la definizione delle priorità politiche per l'anno 2023 – 18/01/2023

PRIORITÀ III - AUTONOMIA STRATEGICA E TECNOLOGICA NELL'AEROSPAZIO, NELLA DIFESA, NEI SETTORI AD ALTA INNOVAZIONE E NELLE TELECOMUNICAZIONI

«Si dovrà poi promuovere l'autonomia strategica e tecnologica dei settori produttivi di punta coinvolti nel processo di transizione verde e digitale, dei settori ad alto potenziale innovativo, nelle aree dell'intelligenza artificiale e dell'efficienza energetica, utilizzando anche le risorse del PNRR, con uno sguardo attento alle tecnologie emergenti quali li 5G, li 6G, li Quantum Computing e li Cloud-Edge Computing.

Il Ministero dovrà avere un ruolo propulsivo nella ***promozione degli investimenti in nuove applicazioni industriali di tecnologie innovative****, ad esempio nell'ambito del settore della microelettronica, realizzando specifiche infrastrutture dedicate alle attività di ricerca e sviluppo, passando attraverso la riconversione di siti industriali esistenti e l'insediamento di nuovi stabilimenti.* ***In generale, occorre valorizzare li ruolo dei Competence center, degli European Digital Innovation Hubs e delle Case delle Tecnologie Emergenti, rafforzando la capacità di incontro tra li mondo della ricerca e le imprese nell'applicazione di tecnologie all'avanguardia.»***

Nuovo Decreto finanziamenti 2023/2026

G.U. n.98 del 27/04/2023 – Serie Generale

Decreto Ministeriale 10/03/2023 - Attuativo del PNRR

M4: «Istruzione e ricerca»

C2: «Dalla Ricerca all'Impresa»

Investimento 2.3: «Potenziamento ed estensione tematica e territoriale dei centri di trasferimento tecnologico per segmenti di attività»

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

PNRR M4C2 – Investimento 2.3

Risorse

Investimenti totali: **€ 350.000.000**, dei quali:

- **€ 33.559.000 euro**, come quota italiana di cofinanziamento dei 13 Poli europei di innovazione digitale (EDIH) selezionati nella gara europea parte del programma Digital Europe;
- **€ 13.400.000**, per sostenere le spese relative al funzionamento dei **Competence Center**;
- **€ 100.000.000**, per i **Competence Center**, sia per la **gestione di progetti innovativi rivolti alle imprese**, in particolare PMI, che per **coprire i costi relativi all'erogazione di servizi** come da Tabella A;
- **€ 114.500.000**, per finanziare i **24 Poli europei di innovazione digitale che hanno ricevuto il "Seal of Excellence"** dalla Commissione Europea, ma che non sono finanziati dall'UE.

PNRR M4C2 – Investimento 2.3
Soggetti Attuatori

Gli otto centri di competenza, capaci di **programmi di trasformazione digitale delle imprese per processi, prodotti e modelli aziendali**

- CIM 4.0 - Competence Industry Manufacturing 4.0
- Made - Competence Center Industria 4.0
- BI-REX - Big data Innovation-Research EXcellence
- ARTES 4.0 – Industry 4.0 Competence Center on Advanced Robotics and enabling digital TEchnologies & Systems 4.0
- SMACT Competence Center
- MedITech Competence Center I 4.0
- START 4.0– Sicurezza e ottimizzazione delle Infrastrutture Strategiche Industria 4.0
- **CYBER 4.0 – Cybersecurity Competence Center**

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

PNRR M4C2 – Investimento 2.3
Soggetti Attuatori

EDIH «Seal Of Excellence»/01 – Tot. n. 24

1. **NEST** – Network for European Security and Trust – Capofila Centro di Competenza Cyber 4.0
2. **AI Magister** - progetto nazionale, capofila la società di consulenza Profima
3. **Edih** L - Lombardia con all'interno il Competence Center MADE
4. **HD-Motion** - progetto nazionale focalizzato sui Trasporti
5. **UDD** - Umbria
6. **Birex ++** - proposta nazionale sulla manifattura sostenibile, Capofila il Competence Center Bi-Rex
7. **Edih4DT** - per il settore pubblico del Sud Italia
8. **DMH** - Italia costiera e il settore marittimo
9. **DIS-HUB** - Alto Adige
10. **AI-Pact** - progetto nazionale dedicato al settore pubblico.
11. **SharD** - Hub - Sardegna
12. **Innova** - progetto nazionale per la PA

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

PNRR M4C2 – Investimento 2.3
Soggetti Attuatori

EDIH «Seal Of Excellence»/02

1. **Pics2** – Puglia, per diversi settori (Steel, Shipbuilding, Petrochemistry, Aerospace, Agrifood, Logistics)
2. **EDIHAMo** - Abruzzo e Molise
3. **ROME Digital Hub** - Lazio
4. **Dips** - Trento
5. **Ap-Edih** - Puglia
6. **Damas** – Capofila Leonardo - progetto nazionale per Automotive e Aerospace
7. **PAI** – Public Administration Intelligence
8. **NEURAL** – veNEto hUb foR Advanced digital technoLogies - Veneto
9. **InnovAction** – Network Italiano dei Centri per l'Innovazione Tecnologica
10. **IP4FVG** – Friuli Venezia Giulia
11. **CATCH atMIND** – advanCed digitAl TeChnology Hub for the Life Sciences at MIND
12. **Fondazione MAXXI – CURE** – Creativity for Urban Rebirth

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

PNRR M4C2 – Investimento 2.3
Soggetti Attuatori

EDIH già cofinanziati da Commissione EU – Tot. n. 13

1. **DIHcube** - ANCE
2. **Cetma DihSme** – Puglia e Basilicata
3. **ER2digit** - Emilia-Romagna
4. **MicroCyber** - Sicilia, Calabria, Campania, Basilicata, Sardegna, Puglia, Molise
5. **HSL (Heritage SmartLab)** - Basilicata
6. **Dante** - Cluster Tecnologico Nazionale “Smart Living Technologies” SMILE
7. **EDIH4Marche** - DIH Marche di Confindustria
8. **Chedih – Circular Health European Digital Innovation Hub** - Piemonte e Valle d’Aosta
9. **i-NEST** – CNIT – Consorzio Nazionale Interuniversitario per le Telecomunicazioni
10. **Toscana X.0** - capitanato da GATE4.0 Distretto Regionale Toscano al cui interno c’è il DIH di Confindustria
11. **P.R.I.D.E.** – Polo Regionale per l’Innovazione Digitale Evoluta - Campania Digital Innovation Hub
12. **Artes 5.0** - capitanato dal Competence Center Artes 4.0 con focus su Industria e PA
13. **Expand** - Competence Center CIM 4.0 - Piemonte e Valle d’Aosta

Target M4C2 – Target 13

- Costituzione di **42 nuovi centri** da raggiungere entro il quarto trimestre 2025, articolati in due tipologie (Centri di Competenza e EDIH);

I nuovi centri sono finanziati in funzione delle **esigenze emergenti di settori specifici o di ecosistemi locali.**

La **rete dei poli di innovazione** offre servizi quali: **sensibilizzazione, formazione, intermediazione tecnologica, accesso ai finanziamenti per l'innovazione tecnologica, audit tecnico e banchi di prova.**

Target M4C2 – Target 14

Prevede che i centri debbano fornire servizi di:

a) Test before invest;
b) Formazione;
c) Accesso ai finanziamenti;
d) Sostegno allo sviluppo di progetti innovativi (TRL – Technology Readness Level > 5);
e) Intermediazione tecnologica;
f) Sensibilizzazione a livello locale, per una **ricaduta attività complessive di € 600 milioni.**

Il target in oggetto deve essere raggiunto **entro il quarto trimestre 2025**

Target M4C2 – Target 15

Prevede il raggiungimento di almeno **4.500 piccole e medie imprese beneficiarie di un sostegno** mediante la fornitura di servizi tra cui:

a) Test before invest;
b) Formazione;
c) Accesso ai finanziamenti;
d) Sostegno allo sviluppo di progetti innovativi (TRL superiore a 5);
e) Intermediazione tecnologica;
f) Sensibilizzazione a livello locale

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

PNRR M4C2 – Investimento 2.3 – Linea B2
Intensità aiuti per servizio/dimensione imprese

SERVIZIO EROGATO		Micro imprese e piccole imprese	Medie imprese	Grandi imprese
Audit tecnico, valutazione maturità tecnologica (assessment)		100% (Art. 28 comma 4 GBER)	90% (Art. 28 comma 4 GBER)	40% (reg. "de minimis")
Prova prima dell'investimento		100% (Art. 28 comma 4 GBER)	80% (Art. 28 comma 4 GBER)	30% (reg. "de minimis")
Formazione	Fino a 24 ore	100% (Art. 28 comma 4 GBER)	80% (Art. 28 comma 4 GBER)	50% (Art. 31 GBER)
	Oltre 24 ore	70% (Art. 31 o Art. 28 comma 4 GBER)	60% (Art. 31 o Art. 28 comma 4 GBER)	40% (Art. 31 GBER)
Consulenza su protezione Proprietà Intellettuale		70% (Art. 28 comma 4 GBER)	60% (Art. 28 comma 4 GBER)	50% (reg. "de minimis")
Consulenza su accesso ai finanziamenti		70% (Art. 28 comma 4 GBER)	60% (Art. 28 comma 4 GBER)	50% (reg. "de minimis")
Consulenza su innovazione tecnologica di processo e di prodotto, networking e sensibilizzazione		80% (Art. 28 comma 4 GBER)	70% (Art. 28 comma 4 GBER)	50% (reg. "de minimis")
Progettazione dell'intervento di innovazione		50% (Art. 28 GBER)	40% (Art. 28 GBER)	30% (reg. "de minimis")

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

4C per le sfide di cybersecurity

Competenze

Capacità

Cooperazione

Concretezza

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Il Centro di Competenza Cyber 4.0: attività e nuovi strumenti di finanziamento

- **Martina Castiglioni,** *Responsabile formazione ed orientamento, Cyber 4.0*

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Attività istituzionali

Orientamento PMI e PA

Orientamento PMI

Vademecum PMI

- **12 azioni** per un business sicuro
- Basato su 12 Step ENISA

Ministero delle Imprese e del Made in Italy

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

Postura cyber security PMI

- Basato su **Framework Nazionale Cybersecurity e Data Protection**
- **Analisi** aree di intervento prioritario, remediation roadmap, impatto economico e benefici
- **Estensione nazionale** – DIH, PID, Case Tecnologie Emergenti

Roadshow Cyber 4.0

- Coinvolgimento DIH e altre realtà attive in regione (Polizia Postale, CTE, etc.)
- Sessioni di info/ formazione e incontri con esperti, case studies e buone pratiche, quick Cyber Checkup
- Aggregazione di comunità locali per **information sharing**

Il Vademecum per le PMI

1. *Sviluppare una solida cultura della cybersicurezza*
2. *Fornire una formazione appropiata*
3. *Garantire un'efficace gestione dei terzi*
4. *Sviluppare un piano di risposta agli incidenti*
5. *Rendere sicuro l'accesso ai sistemi*
6. *Rendere sicuri i dispositivi*
7. *Rendere sicura la propria rete*
8. *Migliorare la sicurezza fisica*
9. *Rendere sicuri i back up*
10. *Lavorare con il cloud*
11. *Rendere sicuri i siti online*
12. *Cercare e condividere conoscenze ed informazioni*

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Ministero delle Imprese e del Made in Italy

Il Vademecum per le PMI

Titolo

Azione

Integrazione

- ***Contesto e parole chiave (glossario)***
- ***Raccomandazioni***
- ***Riferimenti al contesto nazionale***
- ***Riferimenti metodologici***

Esempio

4. Sviluppare un piano di risposta degli incidenti

Testo originale di ENISA

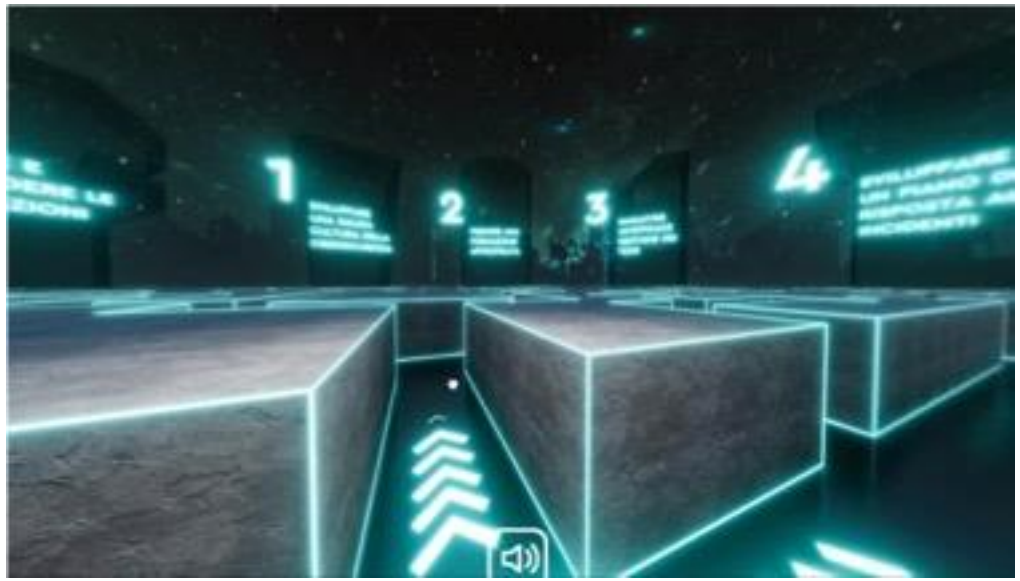
- **Parole chiave** – Incidente informatico, Data Breach, IoC, Polizia Postale, CSIRT Italia, High impact Incident.
- **Raccomandazioni** – Come creare un piano di risposta degli incidenti? Fasi: attività, ruoli, tempistiche – pianificazione e preparazione, identificazione e valutazione dell'evento, gestione, notifiche, miglioramento continuo)
- **Riferimenti nazionali** – Quando e come notificare un incidente informatico
- **Methodological references**
  - Riferimenti legislativi nazionali ed europei (NIS, NIS2,D.Lgs 65/2018, PSNC)
  - Riferimenti ai meccanismi di notifica nazionali
  - FNCS (Framework Nazionale per la Cybersecurity e la Data Protection)
  - Altri framework per la gestione degli incidenti

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Attività istituzionali

12 passi per un business sicuro

Demo Lab and Test Before Invest – T4



12 piazze virtuali per 12 azioni

- **INFO** – Raccomandazioni per le imprese
- **DEMO** – Accesso all'area demo
- **TOOLS** – Strumenti e soluzioni disponibili

Attività istituzionali

Orientamento PMI e PA

Demo Lab e Test Before Invest – Demo in fase di predisposizione

1. **Awareness e Formazione**
   - **Innovery**, Jumanji – Simulazioni immersive
   - **Netgroup**, Simulazione campagna di phishing
   - **Poste Italiane**, Portale di cybersecurity awareness
2. **OSINT**
   - **Digital Platforms**, Skywalker OSINT – Verifica delle fonti con Intelligenza Artificiale
   - **Netgroup**, Information gathering su visitatore (OSINT)
   - **Prisma**, Dominio Intelligence Platform
3. **CERT & Security Operations**
   - **Poste Italiane**, CERT Rating
   - **Università Tor Vergata**, Monitoraggio e protezione impianti critici ospedalieri
4. **Malware analysis**
   - **Prisma**, Dynamic Blue – Malware Analysis
5. **Information Sharing**
   - **Università Tor Vergata**, Cyber Threat Information Sharing per la Sanità (MISP + Open Data)
6. **Supply Chain Security**
   - **Poste Italiane**, SCAI – Supply Chain Automation Tool
   - **Digital Platforms**, GRC per Supply Chain Security
   - **Prisma**, Dominio Cyber & Privacy Governance e Supply Chain Security
   - **Innovery**, RiskOut
7. **Big Data**
   - **Università Tor Vergata**, Big Data security – Applicazione a dati biomedicali (cervello)
8. **Cloud**
   - **Netgroup**, Virtual desktop
9. **IoT**
   - **Digital Platforms**, IoT e verifica firmware con Intelligenza Artificiale
   - **Radio6ense**, IoT cybersecurity
10. **Tecnologie di sicurezza**
    - **Università Tor Vergata**, Write-once File System
11. **Online Fraud**
    - **BV Tech**, Fraudsealer (AI & ML)
12. **Progetti di ricerca e innovazione Cyber 4.0** – Video illustrativi
    - **AIA Guard**
13. **Luiss**, Project work MSc Cybersecurity

Cybersecurity assessment per le PMI

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Il *Test Cybersecurity e Infrastrutture IT - OT fornisce una valutazione del* ***livello di sicurezza cibernetica delle infrastrutture e soluzioni IT presenti in azienda.***

Tutti i risultati sono poi elaborati in maniera personalizzata, sulla base di quanto raccolto dagli specialisti del DIH e con il supporto specialistico di Cyber 4.0; all'interno di uno specifico report sono illustrate le evidenze specifiche e le possibili linee di intervento.

Cybersecurity assessment per le PMI

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Remediation proposte per far fronte alle vulnerabilità emerse. Per ciascuna proposta sono descritti:

- ***i tempi di attuazione***
- ***impatto economico stimato***
- ***possibili soluzioni tecnologiche a supporto***
- ***priorità di implementazione (alta, a medio e lungo termine)***

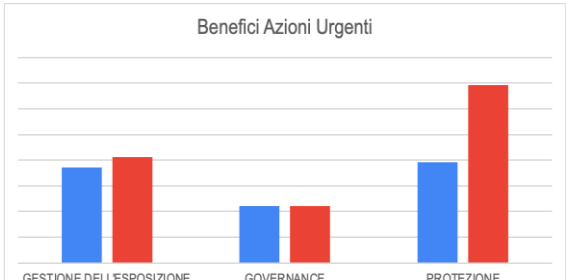
La priorità di implementazione è stata stabilita in accordo con le indicazioni di ENISA presenti nel documento «Cybersecurity for SMES».

Summary remediation Cyber azioni PRIORITARIE

CICERO DIH LAZIO

VALUTAZIONE BENEFICI

Come si vede dal grafico, i primi miglioramenti prodotti dalle remediation prioritarie si riflettono in un aumento significativamente la protezione (quasi del doppio), lasciando invariata la governance. Il livello di gestione dell'esposizione aumenta leggermente.



VALUTAZIONE IMPATTO

L'impatto relativo allo sviluppo delle remediation PRIORITARIE è stimato rispetto ai seguenti range:

1. Effort risorse umane intere: dalle 2 alle 4 giornate
2. Costi servizi professionali: tra i 1.000 e i 1.200 euro
3. Costi HW-SW: nessun costo

Costi Servizi Professionali

Gestione Esposizione	Protezione	Governance	Infrastruttura
0	1.000/1.200€	0	0

Costi HW-SW

Gestione Esposizione	Protezione	Governance	Infrastruttu
0	0	0	0

Esemplificativo

Cybersecurity assessment per le PMI

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Sezione Questionario Infrastrutture IT – OT

Esempio compilato dal Mentor (questionario base)

Quali soluzioni software sono adottate in azienda?

	Soluzioni				Dipendenza dei processi		
	1	2	3	4	Totale	Parziale	Nulla
Progettazione ed Ingegneria	CAD	CAM	VC/PDM	EXCEL	FALSO	FALSO	FALSO
Produzione	MES	APS	ERP	Altro (specificare)	FALSO	FALSO	FALSO
Qualità	DMS	AMS	IMS	Altro (specificare)	FALSO	FALSO	FALSO
Manutenzione	CMMS	EAM		Altro (specificare)	FALSO	FALSO	FALSO
Logistica	WMS	TMS		INVOICEX per magazzino e DDT	FALSO	VERO	FALSO
Supply Chain	MRP	EDI		Altro (specificare)	FALSO	FALSO	FALSO
Risorse Umane	Amministrazione	Gestione personale	WFM	Altro (specificare)			
Marketing, Customer Care e Vendita	CRM	Chatbot	E Commerce	su sit vendi			

L'azienda utilizza applicazioni e servizi sul cloud? INFRASTRUTTURA IT
Si, tutte le applicazioni utilizzate sono su cloud (es. webmail, servizi di cloud data store come Dropbox, etc.).
Sì, utilizziamo applicazioni basate su cloud, insieme ad applicazioni installate sulla nostra infrastruttura IT locale.
No, utilizziamo solo applicazioni installate sui server della nostra infrastruttura IT locale.
No, utilizziamo solo applicazioni installate sui personal computer desktop presenti in azienda.

Il censimento degli asset per processo permette di:

1) ***Acquisire consapevolezza da parte della PMI in merito agli strumenti utilizzati, per ciascun processo;***
2) *Concretizzare gli output dei risultati cybersecurity, inserendo riferimenti* ***in merito ad asset e processi supportati;***
3) ***Customizzare l'identificazione delle raccomandazioni*** *che compongono la roadmap cybersecurity consigliata;*
4) ***Formalizzare*** *, tramite l'aiuto del Mentor ed in maniera efficace,* ***un primo censimento del perimetro tecnologico della PMI,*** *e dunque della superficie a rischio informatico.*

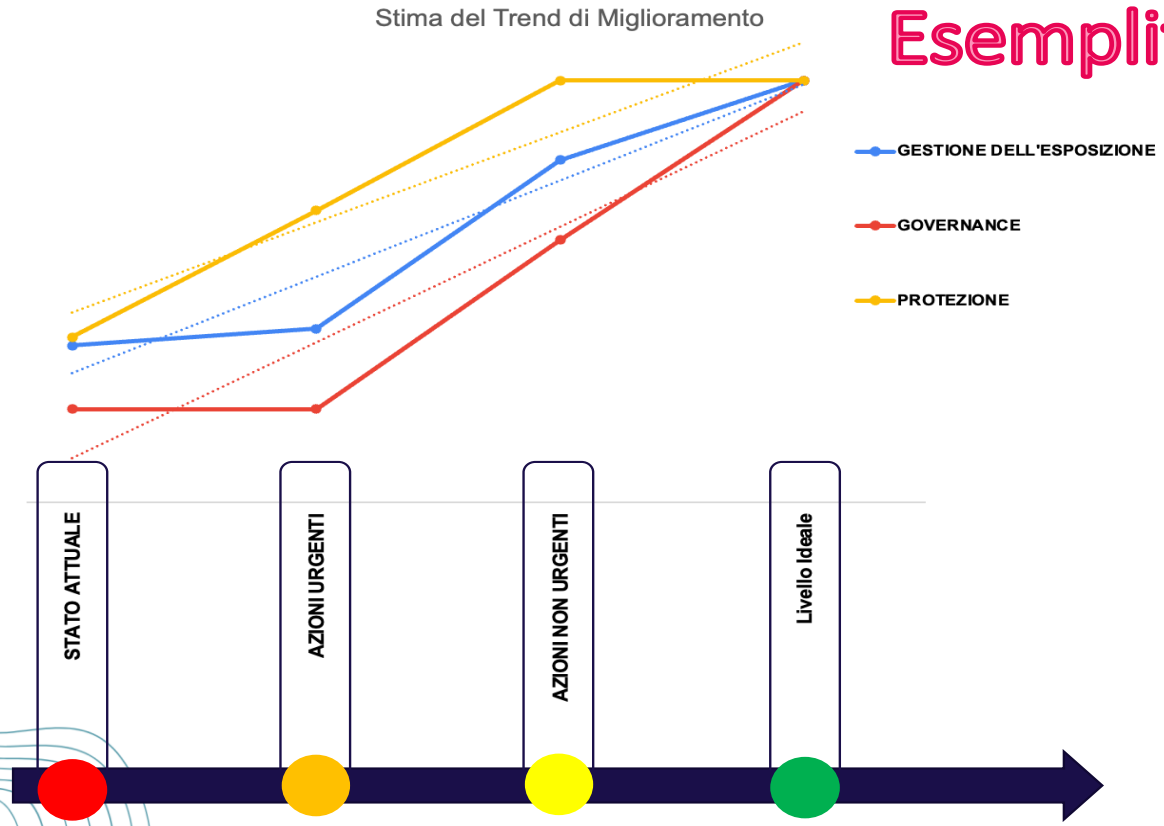
Cybersecurity assessment per le PMI

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CICERO DIH LAZIO

Risultati Attesi - Cybersecurity

Nel presente grafico viene illustrata una stima di miglioramento per quanto riguarda gli ambiti di Esposizione, Governance e Protezione.
N.B. La presente stima costituisce una simulazione indicativa dei miglioramenti apportati grazie all'applicazione delle remediation.



Esemplificativo

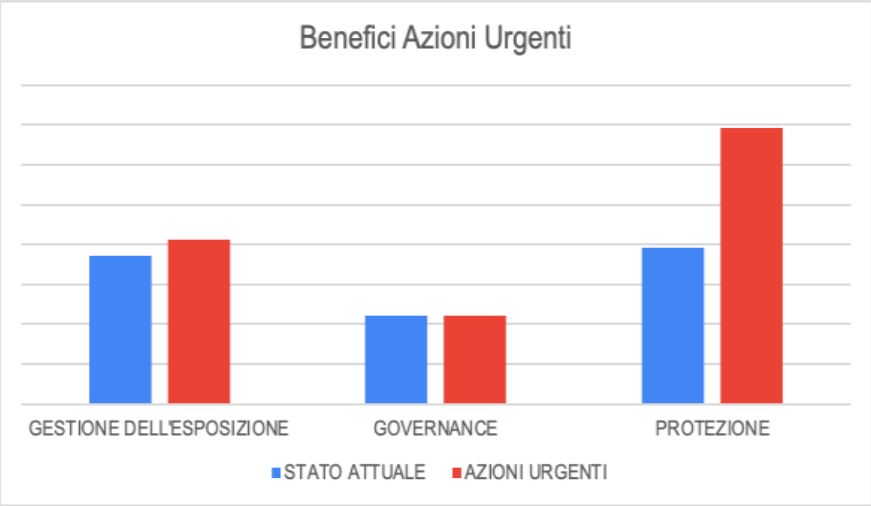
Come si vede dal grafico, partendo dallo stato attuale dopo l'implementazione delle azioni urgenti, il livello di protezione aumenta significativamente. Allo stesso tempo, si può notare un leggero incremento nel livello di gestione dell'esposizione. Con l'applicazione delle azioni non urgenti, si nota come la protezione continui a crescere proporzionalmente allo stadio precedente. In questo caso, si verificano aumenti significativi sia nei livelli di gestione dell'esposizione che in quelli di governance.

Cybersecurity assessment per le PMI

Summary remediation Cyber azioni PRIORITARIE

VALUTAZIONE BENEFICI

Come si vede dal grafico, i primi miglioramenti prodotti dalle remediation **prioritarie** si riflettono in un aumento significativamente la **protezione** (quasi del doppio), lasciando invariata la **governance**. Il livello di **gestione dell'esposizione** aumenta leggermente.



VALUTAZIONE IMPATTO

L'impatto relativo allo sviluppo delle remediation PRIORITARIE è stimato rispetto ai seguenti range:

1. Effort risorse umane intere: dalle 2 alle 4 giornate
2. Costi servizi professionali: tra i 1.000 e i 1.200 euro
3. Costi HW-SW: nessun costo

Costi Servizi Professionali

Gestione Esposizione	Protezione	Governance	Infrastruttura
0	1.000/1.200€	0	0

Costi HW-SW

Gestione Esposizione	Protezione	Governance	Infrastruttura
0	0	0	0

Esemplificativo

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Gestione del rischio cyber: un paradigma culturale da adottare e una metodologia da applicare. Simulazioni di attacchi cyber e modalità di difesa

- **Daniele Incerti,** *Consulente Cybersecurity, Sistemi Formativi Confindustria*

Cyber Security 4.0

DanieleRiccardo Incerti - IT Analyst & Dott. Ing. Vincenzo Vitiello

Sicurezza nazionale

Clusit: Italia nel mirino degli hacker; +169% gli attacchi nel 2022 rispetto al 2021. A livello mondiale la crescita è del 21%

DI REDAZIONE PUBBLICATO IL 7 MARZO 2023 NESSUN COMMENTO

MILANO. Con 2.489 incidenti gravi a livello globale, il 2022 si caratterizza per l'ennesima volta come l'anno peggiore da sempre per la cyber security: sono stati 440 gli attacchi in più rispetto al 2021, che segnano una crescita annua del 21%; la media mensile degli incidenti è stata 207, contro i 171 dell'anno precedente. Il picco massimo dell'anno – e di sempre – si è registrato nel mese di marzo, con 238 attacchi.

Nel contesto delle crescenti tensioni internazionali tra superpotenze e di un conflitto ad alta intensità combattuto ai confini dell'Europa anche l'Italia appare ormai in maniera evidente nel mirino: nel 2022 nel nostro Paese è andato a segno il 7,6% degli attacchi globali (contro il 3,4% del 2021). In numero assoluto sono stati 188 gli attacchi verso il nostro Paese, dato che segna un incremento del 169% rispetto all'anno precedente. A completare il quadro italiano, la gravità elevata o critica nell'83% dei casi.

14/03/2023 15:08 / Cronaca

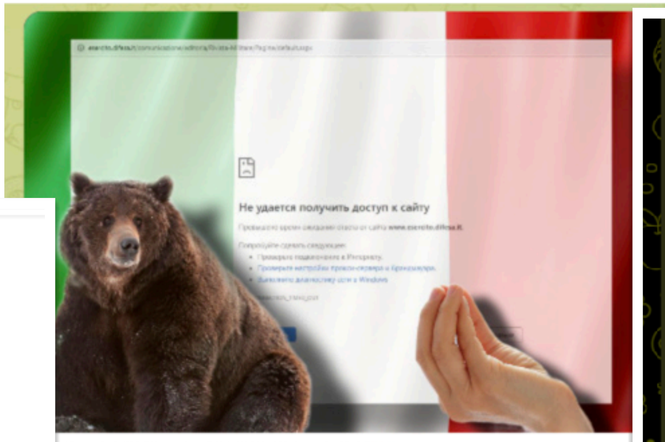
Attacco hacker, i siti della Difesa italiana nel mirino dei filorussi

I siti della Difesa sotto finiti di nuovo sotto attacco hacker. L'azione è stata rivendicata dal collettivo filorusso "NoName057".

Un nuovo **attacco hacker**, che ha colpito in particolare i **portali del Ministero della Difesa** e dell'**Arma dei Carabinieri**, è stato rivendicato, oggi, dal collettivo filorusso *NoName057*.

I SITI DELLA DIFESA SOTTO FINITI DI NUOVO SOTTO ATTACCO HACKER. L'AZIONE È STATA RIVENDICATA DAL COLLETTIVO FILORUSSO "NONAME057"

I siti sotto attacco hacker sono rimasti a lungo irraggiungibili. Come era già accaduto il 22 febbraio scorso, quando nel mirino dello stesso collettivo filorusso erano i siti di Esteri, Interno,



/e continue our Italian journey🇮🇹

anged the portal of the Italian army:

https://check-host.net/check-report/ebd79f0k8df

After breakfast with French croissants🥐 we went to eat Italian pizza🍕🇮🇹

We shut down the website of the Italian Ministry of Defense:

https://check-host.net/check-report/ebcdd05kf5d

👉Subscribe to [redacted]
🐻Join our [redacted]
⚠️Subscribe to [redacted]

🇷🇺Victory will be ours!

9 10:51

di-530-milioni-di-euro-per-lufficio-di-baldoni/

Red Hot Cyber

NoName057(16) continua a burlarsi dell'Italia. "stanziato un budget di 530 milioni di euro" per l'ufficio di Baldoni

NoName riporta oggi sul suo canale Telegram nel quale continua a burlarsi dell'Italia e della nostra Agenzia di Cybersicurezza Nazionale

Gratteri: "Dobbiamo assumere ingegneri informatici e hacker". Il crimine è più forte dello Stato se non corriamo ai ripari

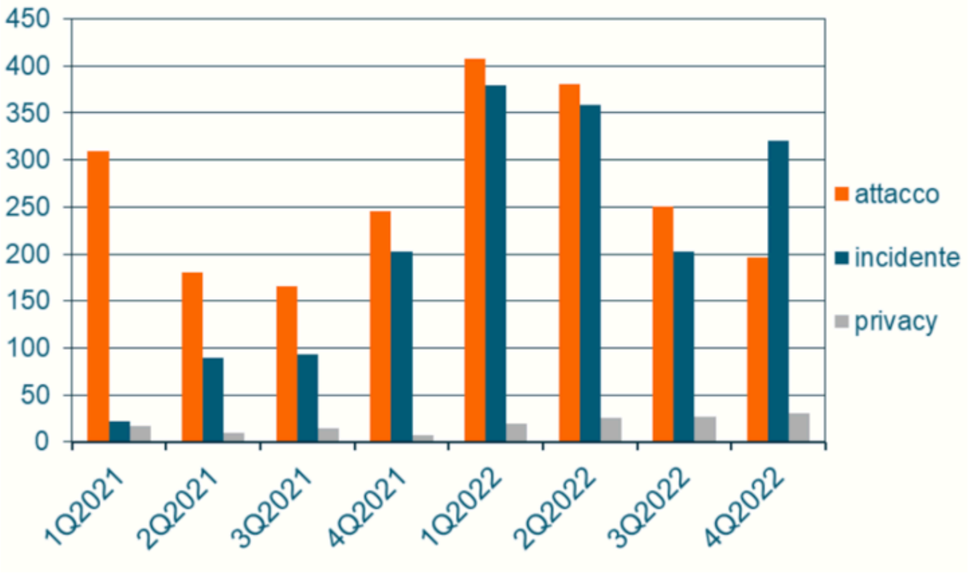


Figura 5 - Numero di attacchi, incidenti e violazioni privacy nel 2021, 2022 in Italia

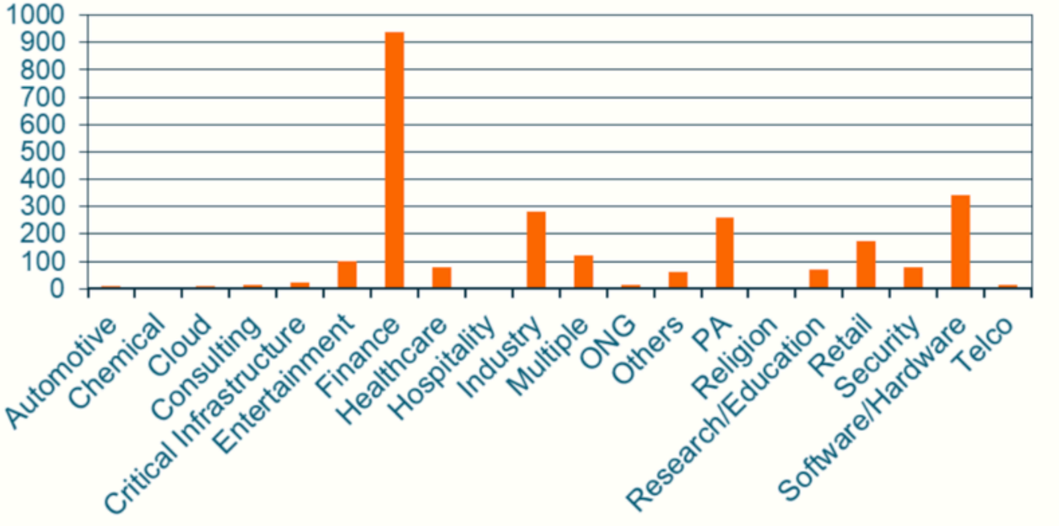


Figura 9 - Tipologia vittime di attacchi, incidenti e violazioni privacy nel 2022 in Italia

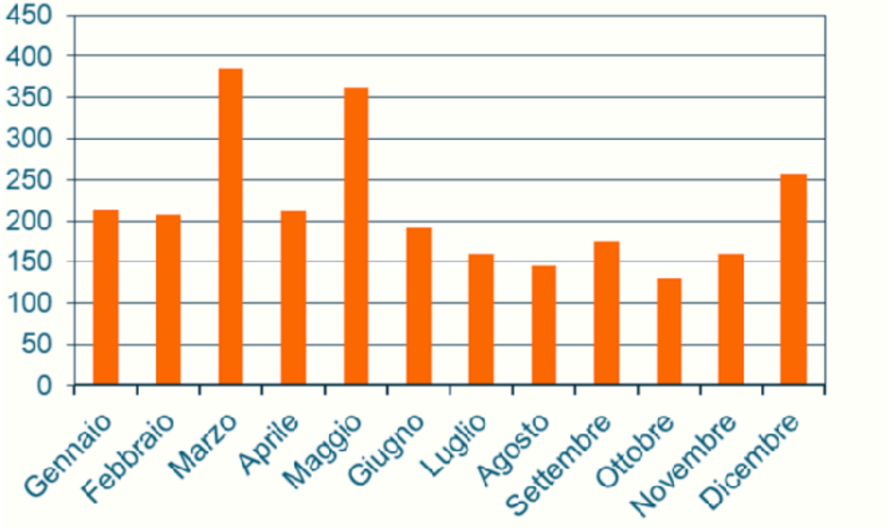
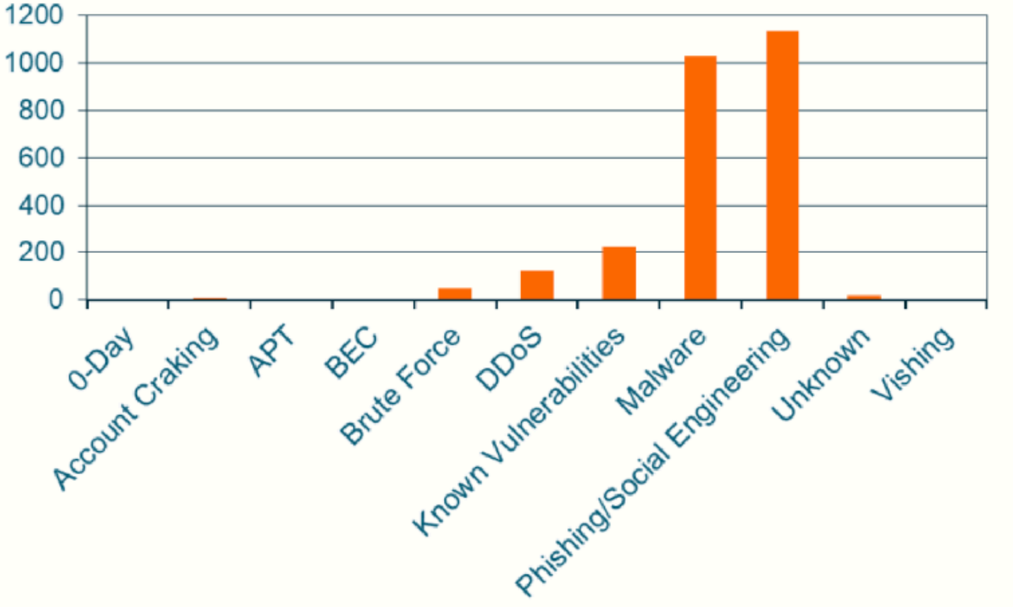


Figura 2 - Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi in Italia nel 2022



CRONACA | 06 Dic 2009

Attaccato da hacker sito web della Gazzetta di Parma

E' entrato nel sistema del sito internet della Gazzetta di Parma, ha inserito l'immagine di un teschio verde corredato dalla sua 'firma' e l'ha pubblicata in homepage.

E' entrato nel sistema del sito internet della Gazzetta di Parma, ha inserito l'immagine di un teschio verde corredato dalla sua 'firma' e l'ha pubblicata in homepage.

Un hacker che si fa chiamare 'Mauzzz' è l'autore di un attacco informatico avvenuto questa mattina ai danni di gazzettadiparma.it, il sito web del quotidiano emiliano. "Siamo riusciti a cancellare l'inserzione, ma purtroppo abbiamo subito alcuni danni che influiscono sulla gestione delle notizie¯, si leggeva successivamente sul sito. Secondo alcuni addetti ai lavori, il 'pirata' è conosciuto per avere messo il proprio segno su varie home page. (ANSA).

@fnsisocial

CRONACA
11 Nov 2021

Resti umani in una grotta dell'Etna, la Procura di Catania disporrà un esame per verificare se sono di Mauro De Mauro

Redazione
01 luglio 2021 11:28

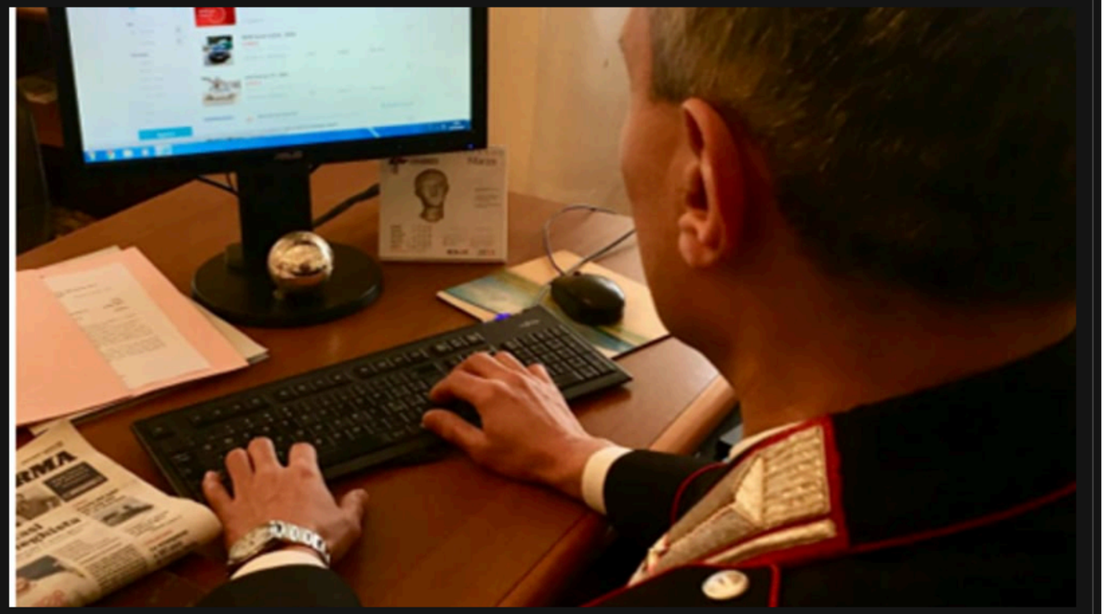
Si parla di

truffa

CRONACA

Due hacker entrano nei conti di un'azienda di Parma e rubano oltre 50 mila euro: denunciati

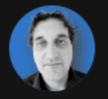
I carabinieri sono riusciti ad identificarli: segnalati alla Procura per frode informatica



Si sono introdotti all'interno dei conti correnti bancari online di un'azienda parmigiana e sono riusciti a sottrarre **oltre 50 mila euro. Due hacker**, che hanno agito online dopo essere entrati in possesso - grazie ad una truffa informatica- dei codici di accesso ai depositi bancari, sono stati identificati e **denunciati dai carabinieri di Parma.**

Secondo le prime informazioni, infatti, i due - utilizzando alcuni sistemi informatici - sono riusciti ad entrare all'interno del sistema e, nel corso di alcuni giorni, sono riusciti ad effettuare dei bonifici a proprio favore per una cifra considerevole. Il valore totale delle transizioni effettuate ammonta infatti ad oltre 50 mila euro. I militari, che hanno avviato le

parmatoday.it/cronaca/attacco-hacker-russo-azienda-ospedaliero-universitaria.html



Christian Donelli
Giornalista ParmaToday
28 febbraio 2023 12:25

CRONACA

Hacker attaccano il sistema informatico dell'azienda Ospedaliero-Universitaria di Parma: mistero sul furto di dati sensibili

L'accesso abusivo, di probabile origine russa, sarebbe partito dal server di posta elettronica per poi propagarsi al server del sistema Pacs, all'interno del quale sono archiviate le immagini dei referti clinici

Immagine di repertorio

Ascolta questo articolo ora...

Nella giornata di domenica 12 febbraio 2023 un attacco hacker, di probabile origine russa, avrebbe 'bucato' la rete informatica interna dell'Azienda Ospedaliero-Universitaria di Parma, che comprende l'Ospedale Maggiore e la Facoltà di medicina e chirurgia dell'Università di Parma. In conseguenza dell'accesso abusivo al sistema informatico alcuni dati sensibili degli utenti sarebbero stati trafugati.

Attacco informatico all'Ospedale Universitario di Parma. A rischio dati sensibili degli utenti

Attacco informatico all'Ospedale di Parma

L'attacco sarebbe partito dall'intrusione nel server di posta elettronica interno (dai server di Microsoft Exchange) e si sarebbe propagato al server del sistema di ***Picture Archiving and Communication System (Pacs),*** dove sono archiviate le immagini dei referti clinici dei pazienti.

Questo è stato possibile in quanto i criminali informatici hanno effettuato dei movimenti laterali sulla rete, per poi raggiungere il sistema Pacs.

Il ***Pacs (Picture Archiving and Communication System)*** è una tecnologia di imaging medico utilizzata per archiviare, gestire e presentare in modo sicuro immagini elettroniche e referti clinicamente rilevanti.

CYBER CRIMINALITÀ

L'hacker cambia l'Iban in fattura e la truffa è «perfetta»

di **Chiara Cacciani** - 10 Giugno 2023, 09:55

CRONACA DI PARMA

GUARDIA DI FINANZA

**'Ndrangheta: fatture f
sequestro da 2,5 milio
Operazione in corso, a
anche a Parma**

POLIZIA DI STATO

**Negozi etnici, controll
tappeto in via Trento e
Leonardo. Denunciato
straniero per ubriache
resistenza a pubblico u
espulso**

Cybersecurity, a Parma solo il 39% delle PMI si protegge

14 Febbraio 2023

L'attacco hacker dei giorni scorsi, in un contesto di crescente digitalizzazione dell'economia, ripone in primo piano il tema della sicurezza informatica di enti e imprese.

Secondo la rilevazione tematica di Eurobarometro della Commissione europea in Italia la quota di micro, piccole e medie imprese che nell'ultimo anno ha fronteggiato almeno un attacco informatico è del 37%, superiore di 9 punti percentuali rispetto al 28% della media Ue.

Come evidenziato nel focus territoriale del 23° report Confartigianato, nell'ultimo anno i reati informatici in Emilia-Romagna sono cresciuti del 12,8%, dinamica a doppia cifra che risulta però inferiore a quella nazionale del +18,4%. Tra le province i reati informatici registrano una crescita

Hacker famosi

Hack: “Risolvere in maniera brillante un problema nel modo in cui nessuno aveva pensato.”

- L'hacking è l'attività di esplorare, manipolare o violare sistemi informatici o reti, con lo scopo di ottenere informazioni o causare danni.
- Esistono tre tipi di hacker: white hat, gray hat e black hat, oltre ai cracker.
- I white hat sono hacker etici che lavorano per identificare e risolvere le vulnerabilità dei sistemi informatici e delle reti, proteggendo gli utenti.
- I gray hat sono hacker che possono violare i sistemi informatici o le reti senza autorizzazione, ma lo fanno per dimostrare le vulnerabilità del sistema e spingere i proprietari a migliorare la sicurezza.
- I black hat sono hacker malintenzionati che violano i sistemi informatici e le reti per ottenere benefici illegali, come rubare informazioni o danneggiare i sistemi.
- I cracker sono coloro che utilizzano le stesse tecniche degli hacker per violare sistemi informatici o reti, ma con intenti criminali.

Kevin Mitnick

- è un hacker informatico che si è poi trasformato in consulente per la sicurezza informatica e autore.
- È diventato famoso negli anni '80 e '90 per i suoi attacchi informatici ad aziende e agenzie governative di alto profilo.
- Le sue abilità di hacking erano così avanzate che è stato inserito nella lista dei ricercati dall'FBI per i crimini informatici.
- Dopo aver scontato cinque anni di prigione, Mitnick ha cambiato vita e diventato un esperto rispettato di sicurezza informatica, aiutando le aziende a proteggersi dagli hacker.
- Ha scritto anche diversi libri sulla sicurezza informatica, tra cui "L'arte dell'inganno" e "Ghost in the Wires".
- La storia di Mitnick serve come esempio dei pericoli dell'hacking informatico e dell'importanza di adottare solide misure di sicurezza informatica

Kevin David Mitnick, detto Condor, è un programmatore, cracker e imprenditore statunitense, che si è distinto per avere introdotto la tecnica dell'IP spoofing e per le sue notevoli capacità nell'ingegneria sociale, avendo eseguito alcune tra le più ardite incursioni nei computer del governo degli Stati Uniti. Wikipedia

Nascita: 6 agosto 1963 (età 59 anni), Van Nuys, Los Angeles, California, Stati Uniti

Coniuge: Bonnie Vitello (s. 1987–1990)

Istruzione: University of Southern California, Pierce College, James Monroe High School

Genitori: Alan Mitnic, Rochell Kramer

Takedown

Da Wikipedia, l'enciclopedia libera.

Questa voce sugli argomenti film d'azione e film thriller è solo un abbozzo.
Contribuisci a migliorarla secondo le convenzioni di Wikipedia. Segui i suggerimenti dei progetti di riferimento 1, 2.

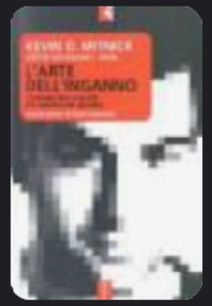
Takedown, anche noto come ***Hackers 2***, è un film del 2000 diretto da Joe Chappelle.

Il film è tratto dalla storia vera narrata nell'omonimo libro di Tsutomu Shimomura e John Markoff, che racconta le indagini e il successivo arresto del noto *hacker* Kevin Mitnick ad opera dell'FBI.

Tsutomu Shimomura

Born	October 23, 1964 (age 58) Nagoya, Japan
Citizenship	American
Education	California Institute of Technology
Occupation(s)	Computer programmer, physicist
Known for	Catching Kevin Mitnick

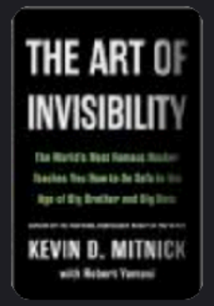
Libri



L'arte dell'inganno
2001

Il fantasma nella rete
2011

L'arte dell'intrusi…
2005



The Art of Invisibility: The Worl...
2017

Raven Adler

Si tratta di un hacker dotato ed intelligente, ***diplomata al liceo a soli 14 anni e ha conseguito la laurea a 18 anni.*** Ha spesso preso parte a conferenze di hacking, ed **è stata anche la prima donna ad effettuare uno speech alla DefCon di Las Vegas,** uno dei raduni di hacker più prestigiosi al mondo.

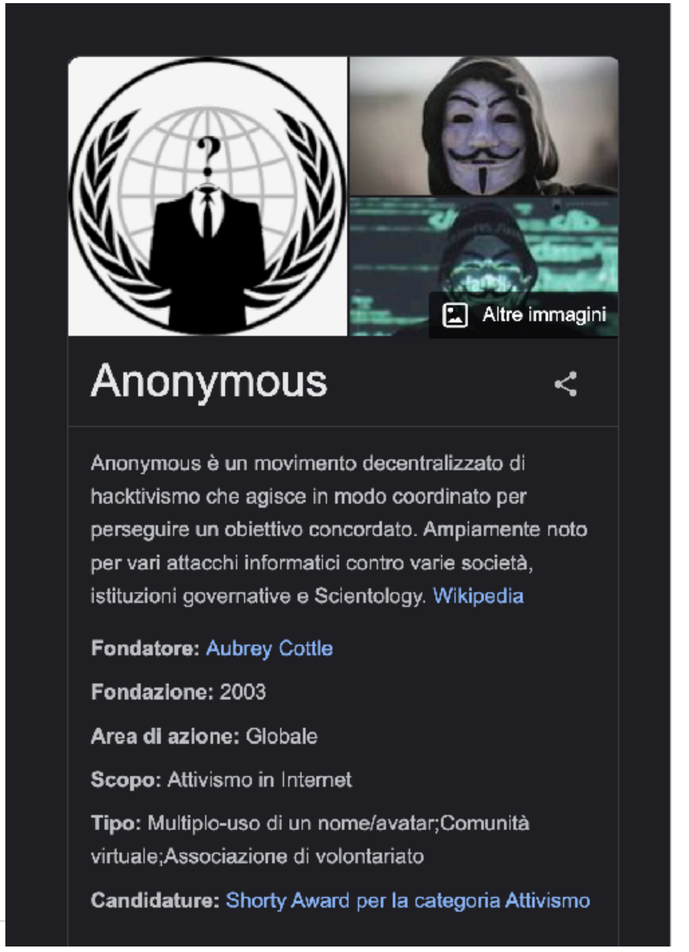
Alle domande sul suo aspetto, spesso risponde che le piacerebbe essere conosciuta per il suo lavoro, non per essere una donna. Attualmente, la Adler è **specializzata nella protezione dei dati end-to-end,** questo l'ha resa famosa all'interno delle grandi organizzazioni per proteggere al meglio le informazioni sensibili.

Lavora come consulente senior per la sicurezza di numerose aziende e continua a tenere conferenze e a pubblicare regolarmente i suoi lavori su riviste del settore.

Anonymous: tutto ciò che è solido sarà hackerato

Anonymous è stato molte cose, senza mai avere un volto identificabile, ma solo una maschera. A un certo momento sembrava davvero in grado di hackerare ogni cosa. Questa ultima puntata di *Rivoluzionari in codice* racconta la storia del collettivo hacker più incredibile della storia e del suo lascito

Il video di Anonymous contro Putin ANONYMOUS/TWITTER



Hacktivism

Hacktivism

GIOVANNI ZICCARDI · IL RICORDO · 11.01.2023

Internet bene comune: a 10 anni dalla morte, la battaglia di Aaron Swartz è più importante che mai

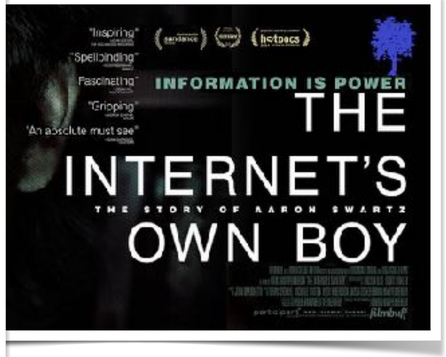
L'11 gennaio 2013 l'hacktivista si suicidava, dopo aver combattuto per orientare la potenza della trasformazione tecnologica a sostegno dei diritti e delle libertà di tutti. Giovanni

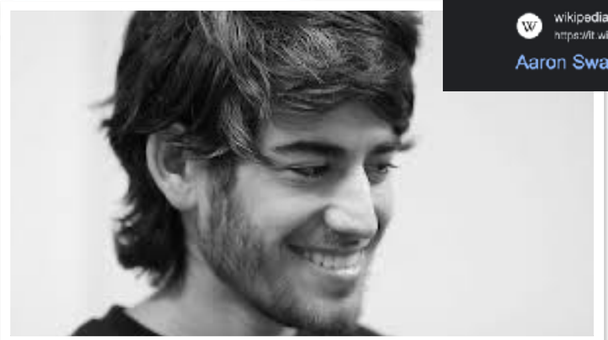
L'importanza della curiosità

Il giovane hacker ribadiva costantemente l'importanza centrale della curiosità in capo alle persone e al cittadino, della **necessità di mettere tutto in discussione**, di valutare con cura tutti gli aspetti di un qualsiasi fenomeno sociale, di una legge o dell'operato di un'istituzione. Uno scrutinio costante e inflessibile sull'operato del pubblico e del privato.

Tutta la sua attività fu mossa, sempre, da una inarrestabile curiosità che si lega direttamente alle **origini dell'informatica e all'aspetto più nobile della tradizione dell'hacking**. Una curiosità innata, senza freni, che porta a superare limiti, a violare confini, a cercare di far cadere il velo di segretezza che il potere è così propenso a mantenere per tutelare la sua posizione di vantaggio nei confronti del cittadino.

Per Aaron, del resto, al centro di tutto vi era la convinzione che **l'informazione** e, di conseguenza, uno Stato con cittadini correttamente informati fossero il bene più importante e più prezioso. Un bene del quale nessuno, in nessuna parte del mondo, doveva essere privato.





Informazioni

Aaron Hillel Swartz è stato un programmatore, scrittore e attivista statunitense. Coautore della prima specifica dell'RSS e delle licenze Creative Commons, é il cofondatore di Reddit e il gruppo di ... Wikipedia

Nascita: 8 novembre 1986, Highland Park, Illinois, Stati Uniti

Morte: 11 gennaio 2013, Brooklyn, New York, Stati Uniti

Organizzazione fondata: reddit Inc.

Genitori: Susan Swartz, Robert Swartz

Sepoltura: 15 gennaio 2013, Shalom Memorial Park Jewish Funeral Home, Illinois, Stati Uniti

Feedback

Circa 207.000 risultati (0,38 secondi)

Il 19 luglio 2011, Swartz fu accusato dal procuratore del Massachusetts di aver violato la legge per ottenere informazioni da un computer protetto e di averlo incautamente danneggiato, con riferimento al download di circa 5 milioni di articoli accademici da JSTOR.

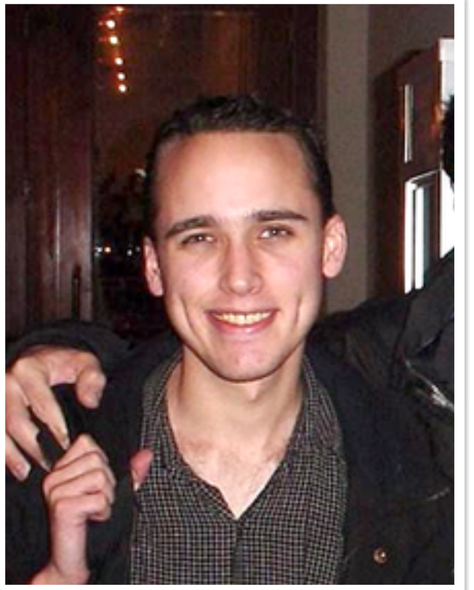
wikipedia.org
https://it.wikipedia.org › wiki › Aaron_Swartz

Aaron Swartz - Wikipedia

3/ Adrian Lamo

Nel 2001, il ventenne Adrian Lamo usò in Yahoo uno strumento di gestione di contenuti non protetti per modificare un articolo del Reuters e aggiungere una citazione falsa attribuita all'ex procuratore generale John Ashcroft. Spesso Lamo attaccava i sistemi e successivamente informava sia la stampa che le sue vittime. In alcuni casi aiutava persino a porre rimedio al problema, per migliorare la sicurezza. Tuttavia, come sostiene Wired, Lamo si spinse ben oltre nel 2002, quando violò l'intranet del New York Times, si aggiunse alla lista degli esperti e iniziò a fare ricerche su personaggi pubblici di spicco. Poiché preferiva vagare per le strade con poco più di uno zaino e spesso non aveva un indirizzo stabile, si guadagnò il soprannome di "the homeless hacker" (l'hacker senzatetto).

Nel 2010, a 29 anni, Lamo scoprì di essere affetto dalla sindrome di Asperger, una lieve forma di autismo spesso chiamata "sindrome dei nerd" perché chi ne è affetto ha difficoltà ad avere semplici interazioni sociali e manifesta un comportamento strano e sempre concentrato. Molti esperti credono che questo spieghi l'ingresso di Lamo nel mondo dell'hacking: la sindrome di Asperger, a quanto emerge, è prevalente nella comunità degli hacker.



Krisina Svechinskaya rimane uno dei nomi più noti nell'hacking. Hacker russo è stata studentessa di alto livello della New York University, ma la maggior parte la riconoscerà per una serie di lavori di hacking high-end che hanno potenzialmente portato alla perdita di milioni di dollari.

Specializzata nell'uso dei cavalli di Troia Zeus, Svechinskaya attaccò migliaia di conti bancari, la maggior parte negli Stati Uniti, creando molteplici fake account sia attraverso Bank of America che Wachovia. Ha poi utilizzato altre nove persone per creare passaporti falsi. E' stata catturata ed indagata con più accuse. Nel complesso, alcune autorità stimano che abbia rubato $ 3 milioni in pochi mesi.

Kristina è stata arrestata nel 2011 ma rilasciata dopo aver pagato $ 25.000 come cauzione. Se fosse stata condannata, avrebbe potuto essere incarcerata per più di 40 anni.

Gli attacchi hacker più famosi della storia

1. Attacco a Equifax (2017): Nel 2017, Equifax, una delle tre maggiori agenzie di credito degli Stati Uniti, ha subito un attacco informatico che ha compromesso i dati personali di oltre 143 milioni di persone, tra cui nomi, numeri di previdenza sociale, date di nascita e altre informazioni sensibili.

2. Attacco a Yahoo (2013-2014): Tra il 2013 e il 2014, Yahoo ha subito due attacchi informatici che hanno compromesso i dati personali di tutti i suoi utenti, ovvero circa 3 miliardi di account. Tra le informazioni rubate c'erano nomi, email, numeri di telefono, date di nascita e password. Uno degli attacchi hacker più famosi per la quantità dei dati violati.

3. Attacco a Target (2013): Nel 2013, Target, una grande catena di negozi al dettaglio, ha subito un attacco informatico che ha compromesso i dati di circa 40 milioni di clienti, tra cui nomi, indirizzi email, numeri di carta di credito e altre informazioni sensibili.

4. Attacco a Sony Pictures Entertainment (2014): Nel 2014, Sony Pictures Entertainment è stata vittima di un attacco informatico massiccio, che ha compromesso i dati personali di migliaia di dipendenti, tra cui nomi, indirizzi email, numeri di previdenza sociale e altre informazioni sensibili. Tra gli attacchi hacker più famosi della storia perché ha colpito uno dei brand più prestigiosi al mondo.

5. Attacco a Marriott International (2018): Nel 2018, Marriott International ha subito un attacco informatico che ha compromesso i dati di circa 500 milioni di clienti, tra cui nomi, date di nascita, numeri di telefono, indirizzi email e numeri di carta di credito. Certamente uno degli attacchi hacker più famosi che ha riempito le prime pagine dei giornali.
Questi sono solo alcuni degli attacchi hacker più famosi nella storia recente. Gli hacker sono sempre più sofisticati e le aziende, così come i privati cittadini, devono fare di tutto per proteggere i propri dati e quelli dei loro clienti. Una buona pratica è quella di utilizzare software di sicurezza aggiornati, di proteggere le password e di educare i dipendenti sull'importanza della sicurezza informatica. In questo modo, si può ridurre il rischio di subire un attacco hacker e proteggere i dati sensibili dei propri utenti.

Gli attacchi hacker più diffusi

Tutti questi attacchi portati a segno sono stati anche il più grande corso di formazione mondiale sulla security. Insomma la sicurezza è diventata un aspetto quotidiano, normale, usuale per miliardi di persone.
Sono questi i "doni del male": i continui successi degli Cracker (la versione malvagia degli hacker) hanno portato a nuovi livelli di security nei servizi digitali più diffusi e questo ha generato una nuova consapevolezza, un nuovo atteggiamento nei confronti delle modalità di proteggere la propria vita e il proprio lavoro. Ma qualisono gli attacchi ancora oggi più diffusi?
In particolare sembra che gli hacker si siano concentrati su queste tipologie di crimini:
• **phishing** via mail, che resta, per il 94% dei casi, la via più utilizzata per far sì che gli utenti installino dei malware sui propri dispositivi. Gli hacker sembrano essersi ingegnati anche per quanto riguarda i metodi per aggirare i controlli sul phishing. È per tale motivo che hanno iniziato a utilizzare anche programmi quali Teams, Slack oppure sms per inviare i loro messaggi malevoli;
• il **ransomware** resta invece la minaccia più insidiosa soprattutto per il settore pubblico, la sanità oppure altre aziende che operano in settori particolari, ma anche per i provati cittadini.
• le **criptovalute** sembrano infine essere il nuovo terreno di caccia degli hacker. Tali strumenti sembrano essere oggetto di attacco soprattutto per quanto riguarda il furto di informazioni e l'utilizzo di malware che scambiano gli indirizzi dei portafogli digitali, sono tra i più in crescita e presto potrebbero entrare nella lista degli attacchi hacker più famosi

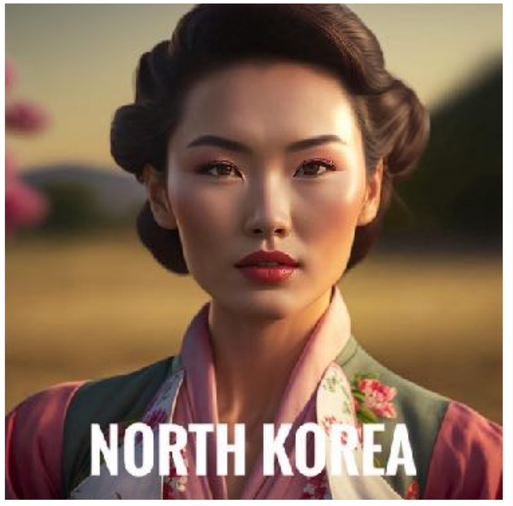
CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

AI

I asked Wonder app to paint
"Pope running from the police"


CANADA


AUSTRALIA


NORTH KOREA

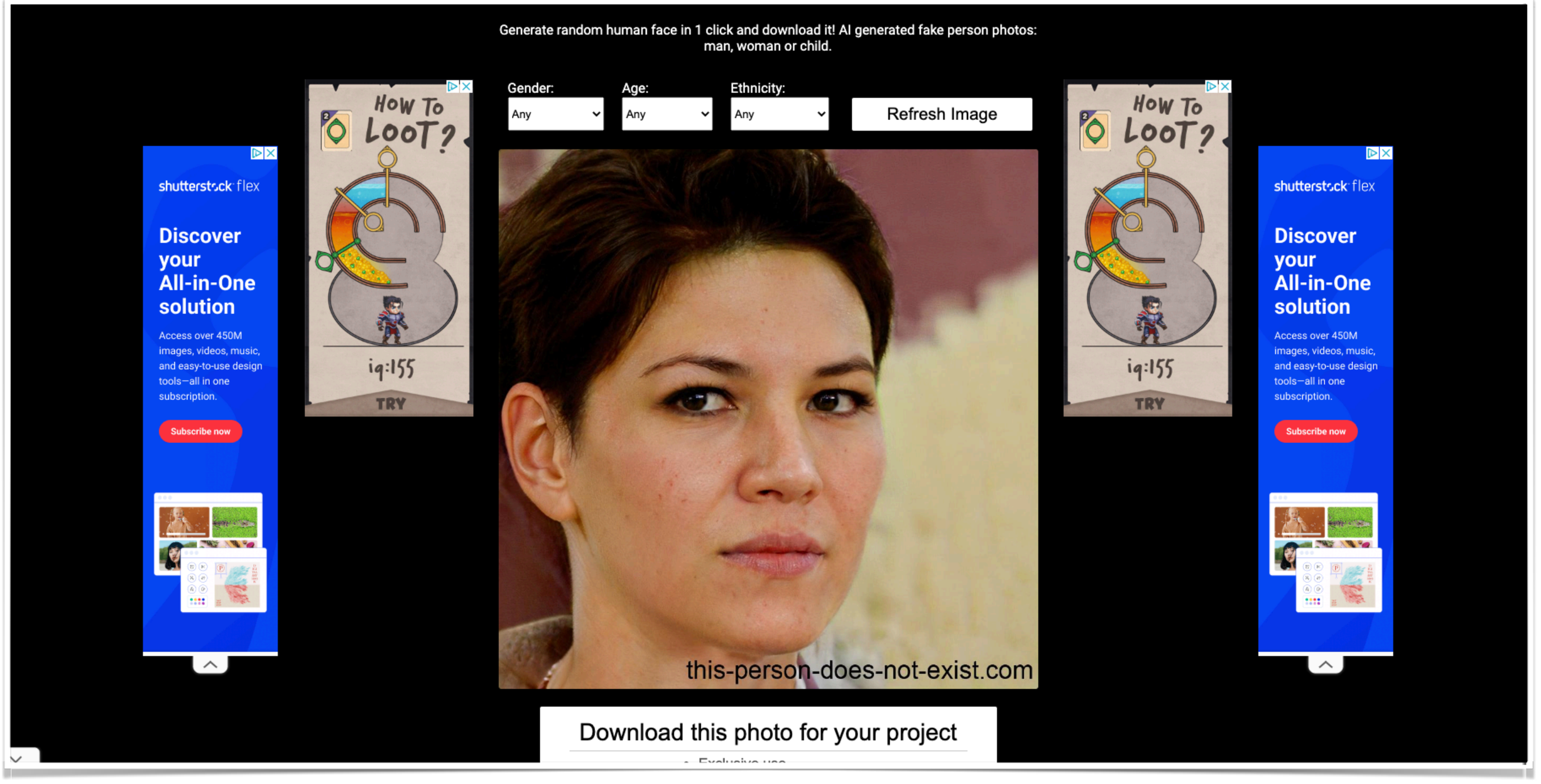

EGYPT


IRAN


IRELAND


BRAZIL


INDIA



https://this-person-does-not-exist.com/en

Ultimate Alternatives of ChatGPT

By @hasantoxr

For Writing
1. ChatSonic
2. ChatABC
3. JasperAI
4. Quillbot

For Coding
1. CoPilot
2. Tabnine
3. MutableAI
4. Safurai
5. 10Web

For Research
1. PaperPal
2. Perplexity
3. YouChat
4. Elicit

For Twitter
1. Tweetmonk
2. TribeScaler
3. Postwise
4. Tweetlify

Productivity
1. Synthesia
2. Otter
3. Bardeen
4. Copy AI

Content Creation
1. Writesonic
2. Tome
3. Copysmith
4. TextBlaze

For Images
1. StockImg
2. Midjourney
3. NightCafe
4. Photosinic

For Videos
1. Steve AI
2. Pictory
3. DeepBrain
4. Lumen5

For AI Audio
1. Murf AI
2. Speechify
3. Lovo AI
4. Media AI

For Music
1. Boomy AI
2. Soundraw
3. Beatoven
4. Soundful

Presentations
1. Beautiful AI
2. Simplified
3. Slidesgo
4. Sendsteps

Resume Builder
1. KickResume
2. Rezi AI
3. Resume AI
4. Enhance CV

Here is a chart of 20 jobs that GPT-4 can potentially replace, along with the human traits being replaced:

Number	Job	Human Trait Replaced
1	Data Entry Clerk	Speed and Accuracy
2	Customer Service Representative	Communication and Empathy
3	Proofreader	Attention to Detail
4	Paralegal	Research and Organization
5	Bookkeeper	Mathematical Skills
6	Translator	Language Proficiency
7	Copywriter	Creativity and Writing
8	Market Research Analyst	Analytical Skills
9	Social Media Manager	Content Creation and Curation
10	Appointment Scheduler	Time Management
11	Telemarketer	Persuasion and Communication
12	Virtual Assistant	Multitasking and Organization
13	Transcriptionist	Listening and Typing Skills
14	News Reporter	Fact-checking and Writing
15	Travel Agent	Planning and Coordination
16	Tutor	Knowledge and Teaching
17	Technical Support Analyst	Troubleshooting and Problem-solving
18	Email Marketer	Writing and Targeting
19	Content Moderator	Critical Thinking and Judgment
20	Recruiter	Interviewing and Assessment

AI News and Highlights, March 2023:

1. OpenAI released ChatGPT and Whisper APIs
2. Ford launched Latitude AI
3. UBC's new AI model predicts cancer patient survival
4. Hubspot introduced Chatspot
5. Discord launches AI features.
6. New Bing crossed 100M Daily Active Users
7. GM released a new ChatGPT-like assistant
8. GPT-4 officially launched
9. Google brought AI to Google Workspace
10. Google released PaLM API
11. Microsoft launched 365 Copilot
12. First, open source text to video 1.7 billion parameter model released
13. Apple tested AI in Siri, Operation Bobcat
14. Runway released Gen-2
15. Bing launched Bing image Crestor
16. Adobe launched Firefly
17. ChatGPT bug exposed some user chat history
18. GitHub launched Copilot X
19. Opera released in-browser tools
20. ChatGPT released plugins
21. Canva launched AI tools
22. Character AI raised $150 million
23. AI-generated Pope broke the internet
24. Apple acquired an AI startup
25. Zoom released Zoom IQ
26. Replit teamed up with Google
27. Perplexity released a new iPhone app
28. A group of AI leaders called for a pause on AI
29. Goldman Sachs suggested AI impacts 300M jobs
30. UNESCO called for AI ethics implementation

AI Frontier
By Steve Nouri

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Devices

FLIPPER

Home Shop Docs Blog Forum IT

Flipper Zero

$169.00 SOLD OUT

Shipping calculated at checkout.

Quantity: 1

SOLD OUT

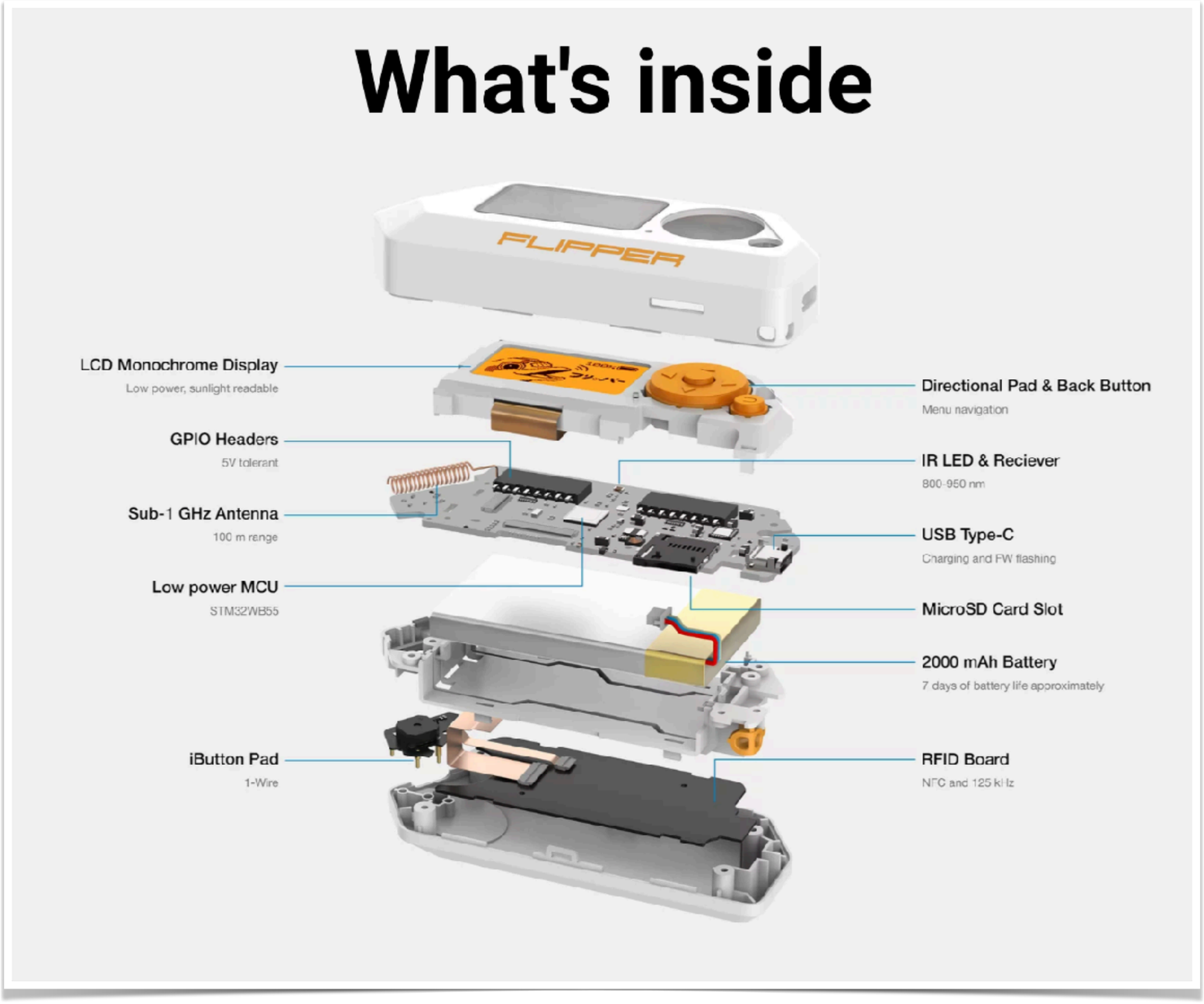
Flipper Zero is a portable multi-tool for pen-testers and geeks in a toy-like body. It loves researching digital stuff like radio protocols, access control systems, hardware, and more. It's fully open-source and customizable, so you can extend it in whatever way you like. More about Flipper Zero

One order can contain up to:

- 2 Flippers
- 3 Silicone Cases
- 3 Wifi Devboards
- 5 Screen Protectors
- 5 Prototyping Boards

If your order violates these limits, it will be canceled. These limits might change in the future.

Flipper Zero is a portable multi-tool for pentesters and geeks in a toy-like body. It loves hacking digital stuff, such as radio protocols, access control ...



- Modulo per intercettare ed emulare onde sotto 1GHz
- Antenna 433MHz con copertura di 50 metri
- Lettore ed emulatore di RFID a 125kHz
- Lettore ed emulatore di NFC
- Modulo Bluetooth
- Modulo infrarossi
- Modulo Touch Memory (i-Button)
- GPIO
- Porta USB (per attacchi Bad Usb)
- Lettore MicroSD
- Batteria integrata da 2000 mAh
- Buzzer
- Motore di vibrazioni
-

Cosa può fare Flipper Zero

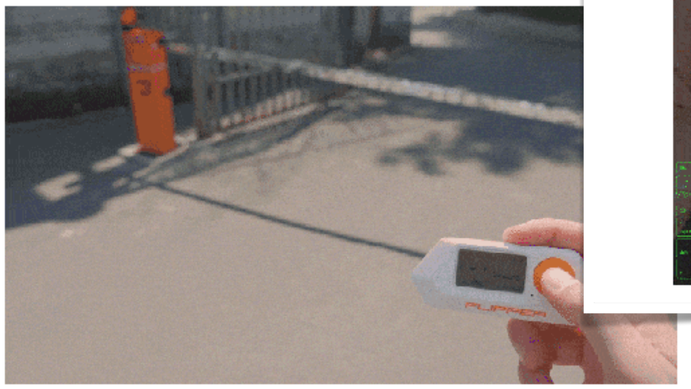
Andando più nel concreto, cerchiamo di capire per cosa può essere utile nella pratica un Flipper Zero. Sappiate che, grazie a questo giocattolino, riuscirete a **sentirvi un po' come il protagonista del gioco "Watch Dogs"**, dopo averci preso un po' la mano. E se le ve lo state chiedendo: sì, **sarete in grado di aprire porte e cancelli in pochi istanti**, nonchè di hackerare qualsiasi computer in pochi secondi. Ma andiamo con calma 😀

In linea di principio, Flipper Zero è in grado, come già detto, di comunicare con tutti
utilizzino un protocollo supportato da questo congegno.
Alcuni esempi:

- **Tessere NFC** degli hotel
- **Telecomandi** per aprire porte e cancelli, la maggior parte basati sulla frequenza
- Chiavette di accesso "i-Button", utilizzate anche da molti distributori automatici,
- **Chiavi/tessere RFID**, anch'esse utilizzate per aprire porte, cancelli, disattivare sis
- **Sistemi infrarossi**: pensiamo ai telecomandi di televisori e via discorrendo

Capite bene che quindi, grazie al Flipper, potremmo, più o meno facilmente:

- Aprire cancelli e porte, intercettando il segnale "lanciato" dal trasmettitore origin
- Aprire le portiere di un'auto
- Clonare una tessera per aprire le stanze di un Hotel, emulandone poi il conteru
  Flipper in una vera e propria tessera di accesso
- Aprire una Tesla (tra poco vedremo come)



Le possibilità sono praticamente infinite. Essendo il firmware Open Source, la community che ru
interno al Flipper Zero lavora quotidianamente per ampliarne le funzioni, **rilasciando anche dei firmwa
non ufficiali** in grado di sbloccare alcuni parametri di "default" limitati (come, ad esempio, le freque
che è possibile utilizzare).
Per qualsiasi richiesta di supporto o aiuto, è presente il server Discord ufficiale (in lingua inglese), opp
il **canale Telegram non ufficiale in lingua Italiana.**

Bad USB

Flipper Zero è dotato di una porta USB Type-C, utile sicuramente per poter ricaricare la batteria, **ma anche per prendere il controllo di qualsiasi computer (o smartphone) al quale viene collegato**.
Flipper è infatti, una volta collegato mediante porta USB, in grado di trasformarsi in una tastiera e mouse che, precedentemente programmato, **eseguono automaticamente determinati comandi, nell'arco di pochissimi istanti.** Così facendo, ad esempio, sarà possibile istruire il Flipper a scaricare un file malevolo all'interno del computer al quale viene collegato, per poi avviarlo. Oppure ancora: potremmo istruire Flipper affinché effettui una copia di specifici file all'interno della sua MicroSD, il tutto in modo automatizzato.
Sarà quindi sufficiente avvicinarci al computer "vittima", collegare il Flipper ed attendere pochi istanti. Ed ecco che il gioco è fatto.

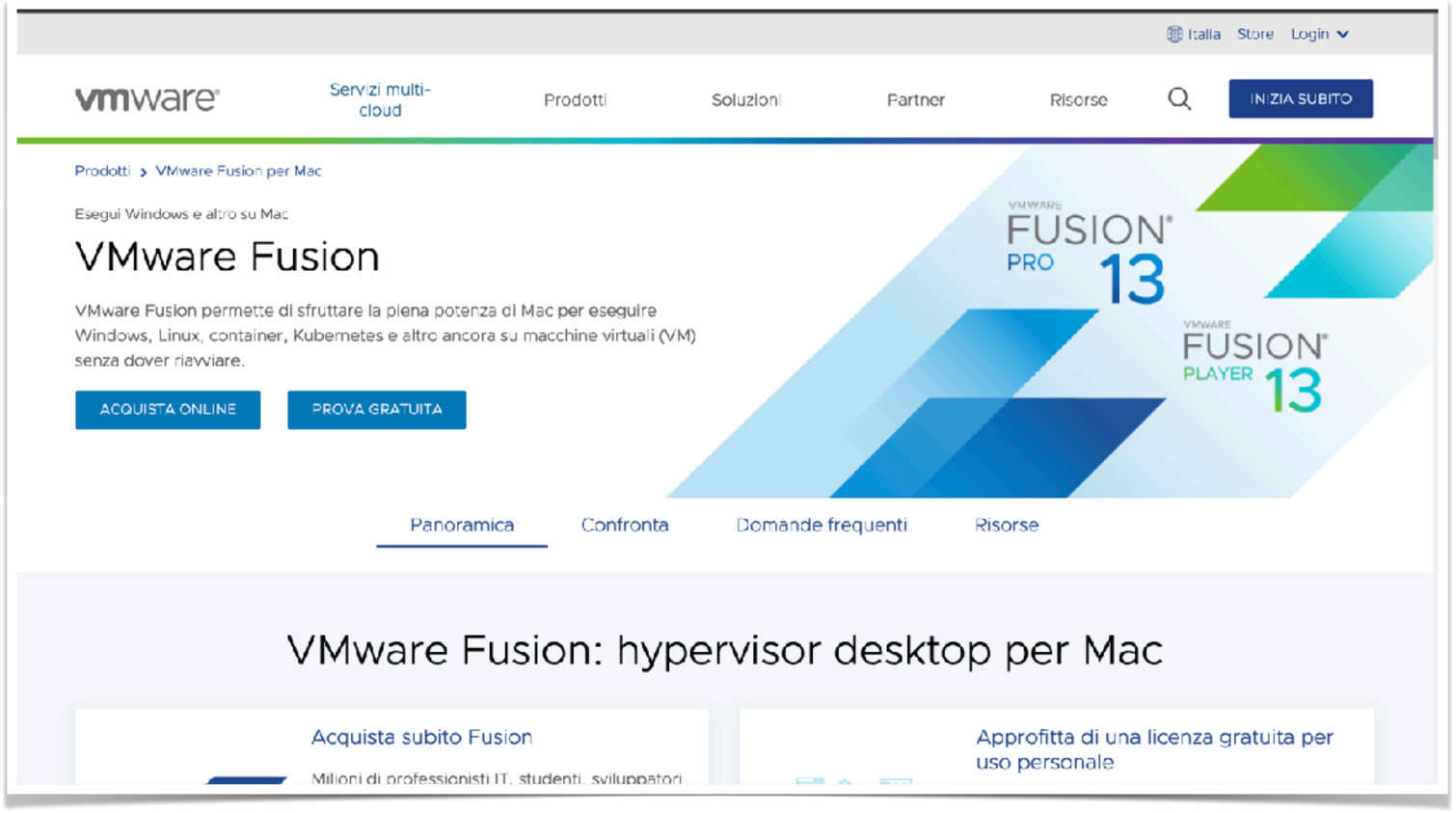
Aprire una Tesla

Quando una Tesla si avvicina ad una colonnina di ricarica, l'auto apre automaticamente lo sportello che permette di collegare il connettore elettrico. Questo avviene in quanto la colonnina di ricarica emette un segnale a 315 MHz, che, guarda caso, può essere intercettato ed emulato da parte del Flipper Zero.
I firmware non ufficiali di cui sopra vi ho parlato **sono in grado di emulare tale segnale a 315 MHz**. Questo significa che, grazie al Flipper, **sarete in grado di aprire qualsiasi sportello di ricarica di una Tesla**, quando sarete nelle vicinanze. Su YouTube sono presenti diversi video in cui viene mostrato questo funzionamento. Qui sotto ve ne propongo uno.

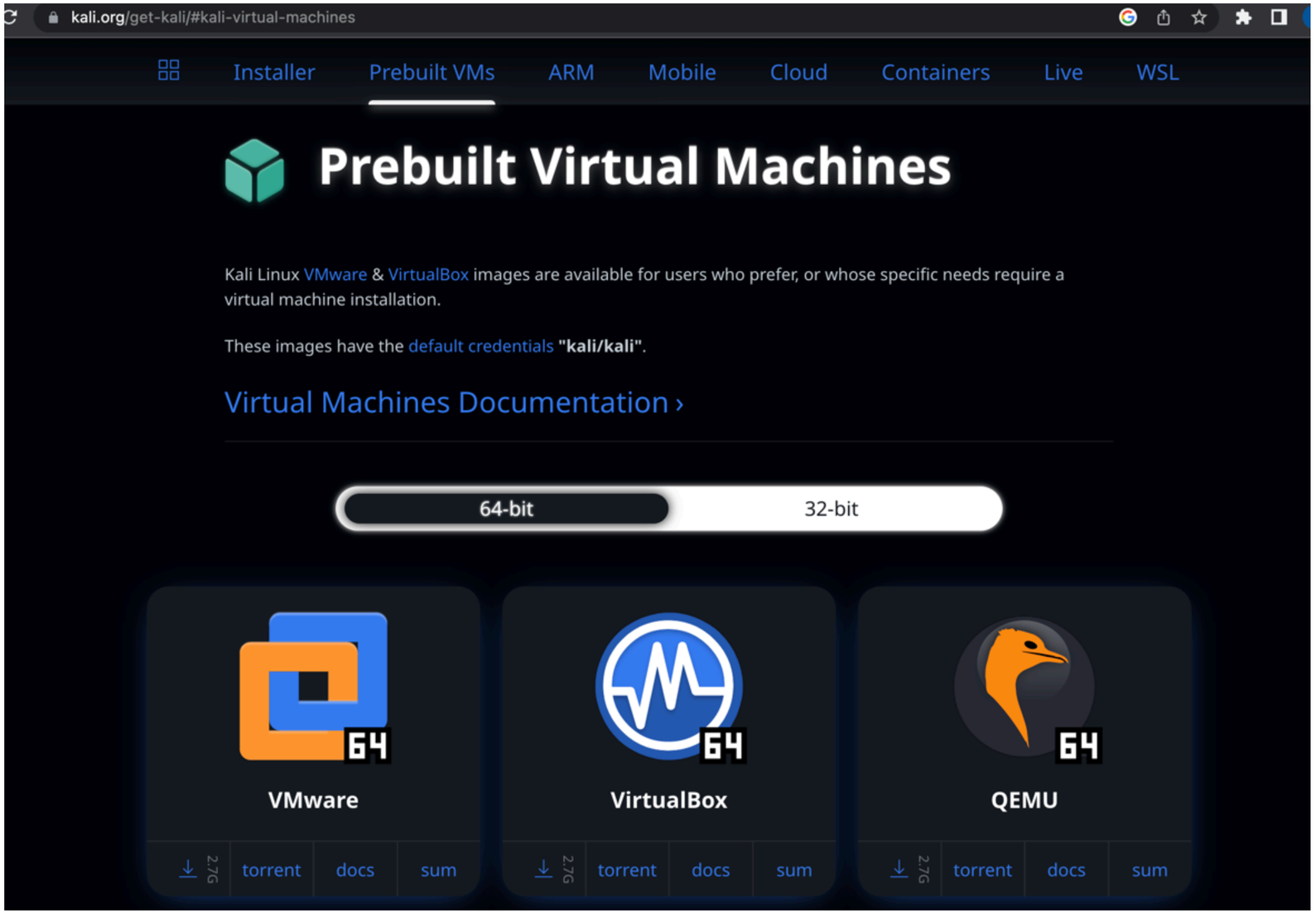
https://www.kickstarter.com/projects/flipper-devices/flipper-zero-tamagochi-for-hackers/

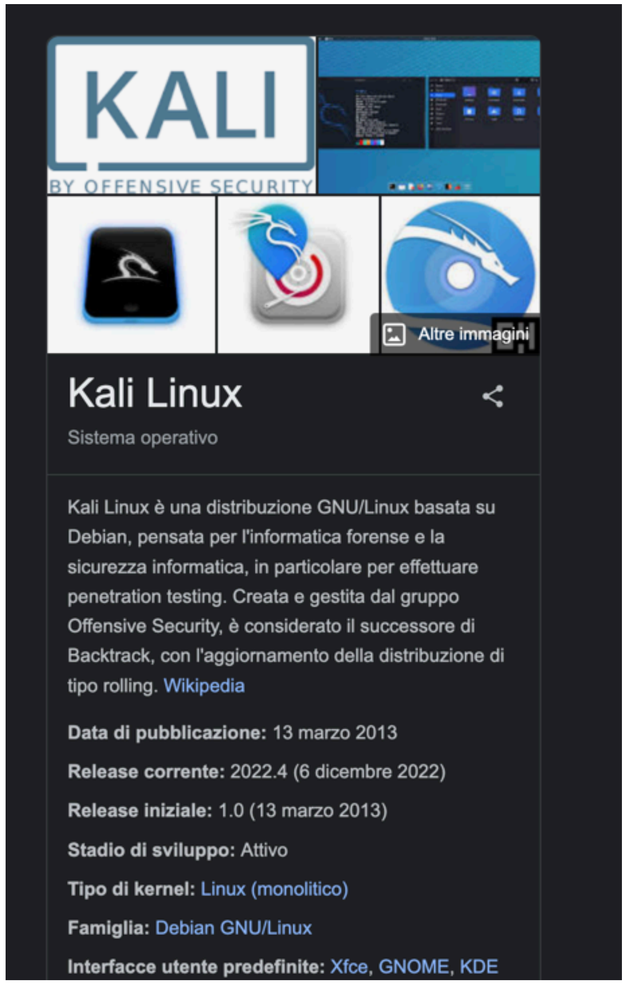
CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Tools


Italia Store Login
vmware
Servizi multi-cloud
Prodotti
Soluzioni
Partner
Risorse
INIZIA SUBITO
Prodotti › VMware Fusion per Mac
Esegui Windows e altro su Mac
VMware Fusion
VMware Fusion permette di sfruttare la piena potenza di Mac per eseguire Windows, Linux, container, Kubernetes e altro ancora su macchine virtuali (VM) senza dover riavviare.
ACQUISTA ONLINE
PROVA GRATUITA
VMWARE FUSION PRO 13
VMWARE FUSION PLAYER 13
Panoramica
Confronta
Domande frequenti
Risorse
VMware Fusion: hypervisor desktop per Mac
Acquista subito Fusion
Approfitta di una licenza gratuita per uso personale


VMware Inc.
Società
vmware
VMware Inc. è una società per azioni sussidiaria di Dell Technologies con quartier generale a Palo Alto e centri di sviluppo a Palo Alto, San Francisco, Cambridge e a Bangalore, nello Stato del Karnataka. Wikipedia
Assistenza clienti: 00 1 650-475-5345
Fatturato: 12,85 miliardi USD (2022)
Date di acquisizione: 15 dicembre 2003, 7 settembre 2016
Sede centrale: Palo Alto, California, Stati Uniti
Fondatori: Diane Greene, Mendel Rosenblum, Edouard Bugnion, Scott Devine, Edward Wang
Fondazione: 1998, Palo Alto, California, Stati Uniti
CEO: Rangarajan Raghuram (1 giu 2021–)
Valore azionario: VMW (NYSE)
117,94 USD -0,63 (-0,53%)
15 mar, 12:39 GMT-4 - Limitazione di responsabilità


kali.org/get-kali/#kali-virtual-machines
Installer
Prebuilt VMs
ARM
Mobile
Cloud
Containers
Live
WSL
Prebuilt Virtual Machines
Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require a virtual machine installation.
These images have the default credentials "kali/kali".
Virtual Machines Documentation ›
64-bit
32-bit
VMware
VirtualBox
QEMU
2.7G
torrent
docs
sum
2.7G
torrent
docs
sum
2.7G
torrent
docs
sum


KALI
BY OFFENSIVE SECURITY
Altre immagini
Kali Linux
Sistema operativo
Kali Linux è una distribuzione GNU/Linux basata su Debian, pensata per l'informatica forense e la sicurezza informatica, in particolare per effettuare penetration testing. Creata e gestita dal gruppo Offensive Security, è considerato il successore di Backtrack, con l'aggiornamento della distribuzione di tipo rolling. Wikipedia
Data di pubblicazione: 13 marzo 2013
Release corrente: 2022.4 (6 dicembre 2022)
Release iniziale: 1.0 (13 marzo 2013)
Stadio di sviluppo: Attivo
Tipo di kernel: Linux (monolitico)
Famiglia: Debian GNU/Linux
Interfacce utente predefinite: Xfce, GNOME, KDE

nmap.org

Npcap.com Seclists.org Sectools.org Insecure.org

NMAP.ORG

Site Search

Download | Reference Guide | Book | Docs | Zenmap GUI | In the Movies

Get Nmap 7.93 here

News

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on Npcap.com, Seclists.org, Insecure.org, and Sectools.org.
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [Release Announcement | Download page]
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [Release Announcement | Download page]
- Nmap 7.80 was released for DEFCON 27! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement/Details], [Download Site]
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes | download]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for security tools. Are you familiar with all of the 49 new tools in this edition?
- Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [Download page | Release notes]
- Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam--all in 38 minutes!

Nmap

Software

Nmap è un software libero distribuito con licenza GNU GPL da Insecure.org creato per effettuare port scanning, cioè mirato all'individuazione di porte aperte su un computer bersaglio o anche su range di indirizzi IP, in modo da determinare quali servizi di rete siano disponibili. Wikipedia

Autore originale: Gordon Lyon

Data di pubblicazione: settembre 1997

Licenza: (licenza libera)

Linguaggio: Python; Java; Lua; C; C++

Linguaggi di programmazione: Python, C, C++, Lua

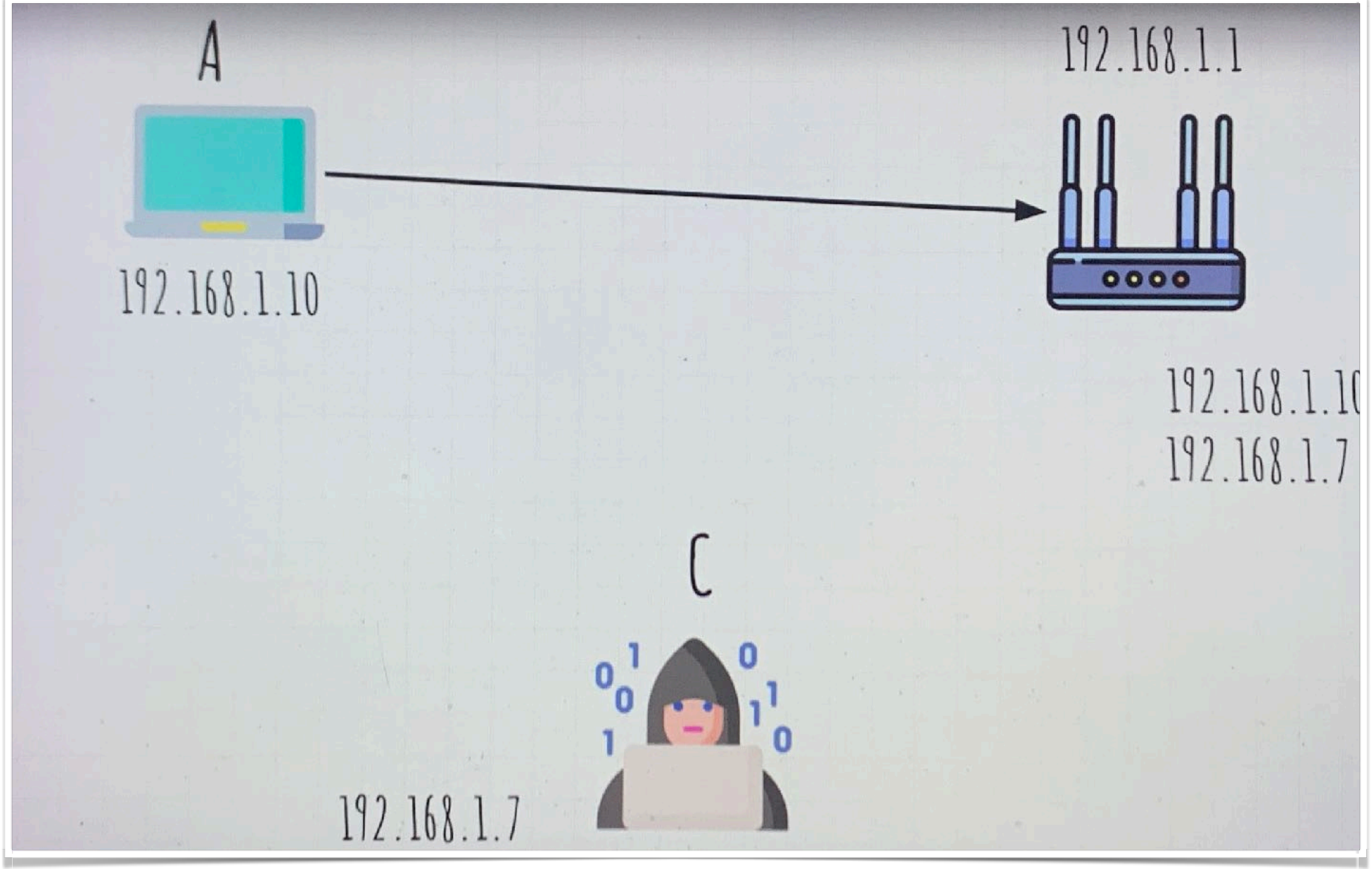
Action...

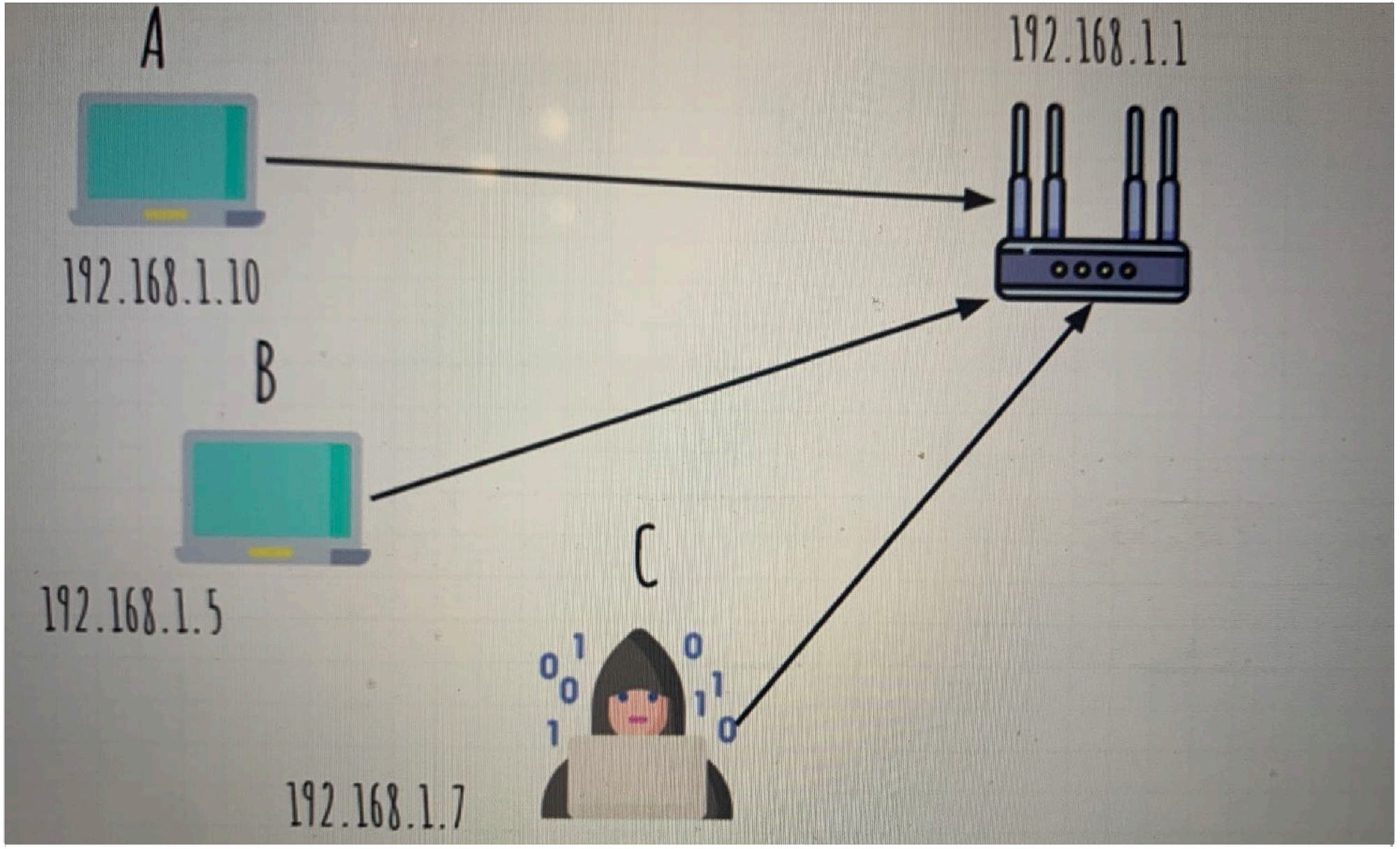
Cosa fare per difendersi?

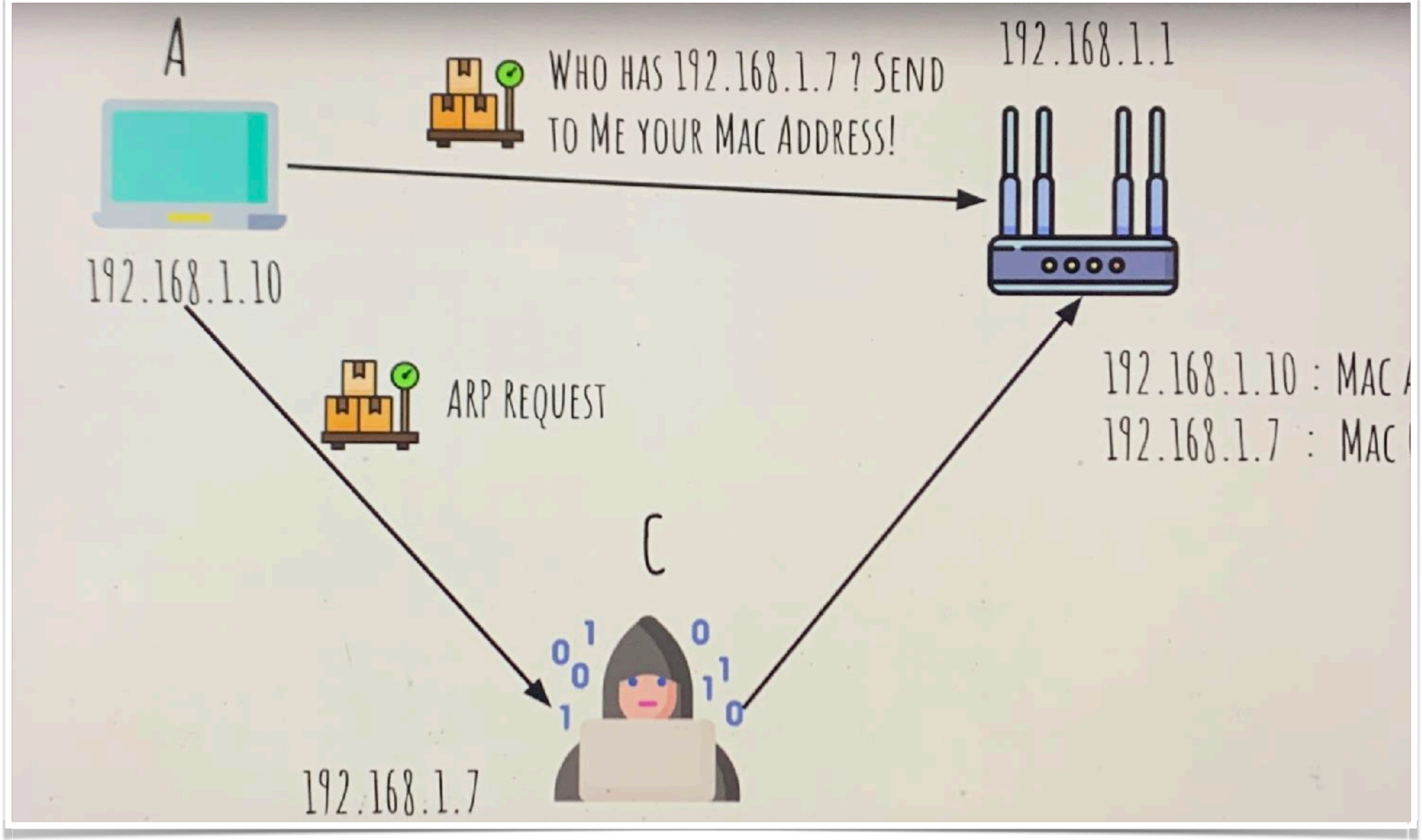
1. Utilizzare protocolli di sicurezza come HTTPS o SSL per cifrare il traffico di rete.
2. Configurare la tabella ARP in modo statico, impedendo ai dispositivi di aggiornare automaticamente la tabella ARP.
3. Configurare la rete in modo che i dispositivi eseguano la risoluzione ARP solo per i dispositivi di rete autorizzati.
4. Utilizzare software di rilevamento dell'ARP poisoning per monitorare la rete e identificare eventuali attacchi.
5. Utilizzare strumenti di autenticazione e controllo degli accessi per limitare l'accesso alla rete solo ai dispositivi e agli utenti autorizzati.

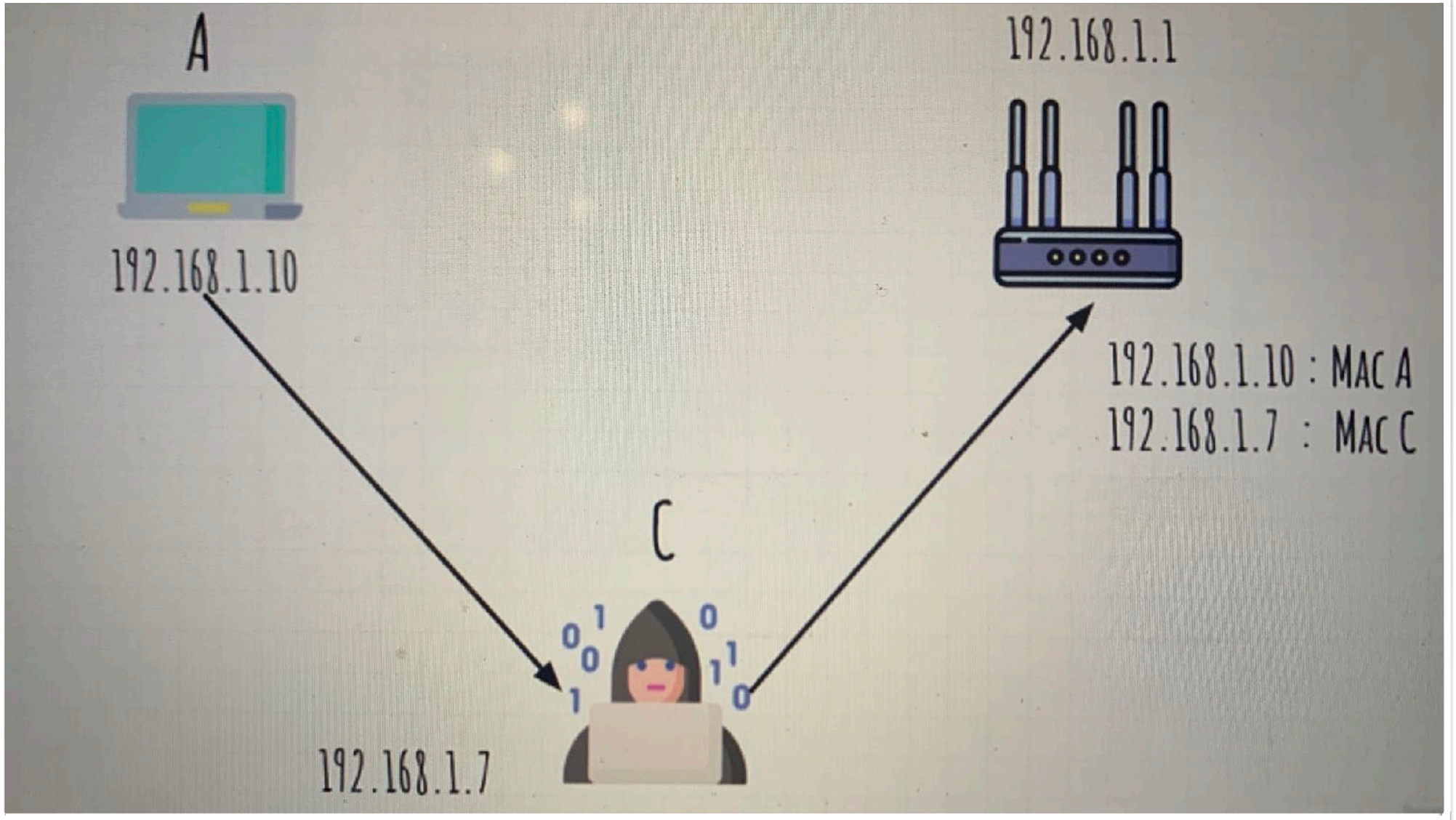
Man in the Middle


MAN IN THE MIDDLE


A
192.168.1.10
192.168.1.1
192.168.1.10
192.168.1.7
C
192.168.1.7


A
192.168.1.1
192.168.1.10
B
192.168.1.5
C
192.168.1.7


A
WHO HAS 192.168.1.7 ? SEND TO ME YOUR MAC ADDRESS!
192.168.1.1
192.168.1.10
ARP REQUEST
192.168.1.10 : MAC A
192.168.1.7 : MAC
C
192.168.1.7


A
192.168.1.10
192.168.1.1
192.168.1.10 : MAC A
192.168.1.7 : MAC C
C
192.168.1.7

Email spoofing

email spoofing

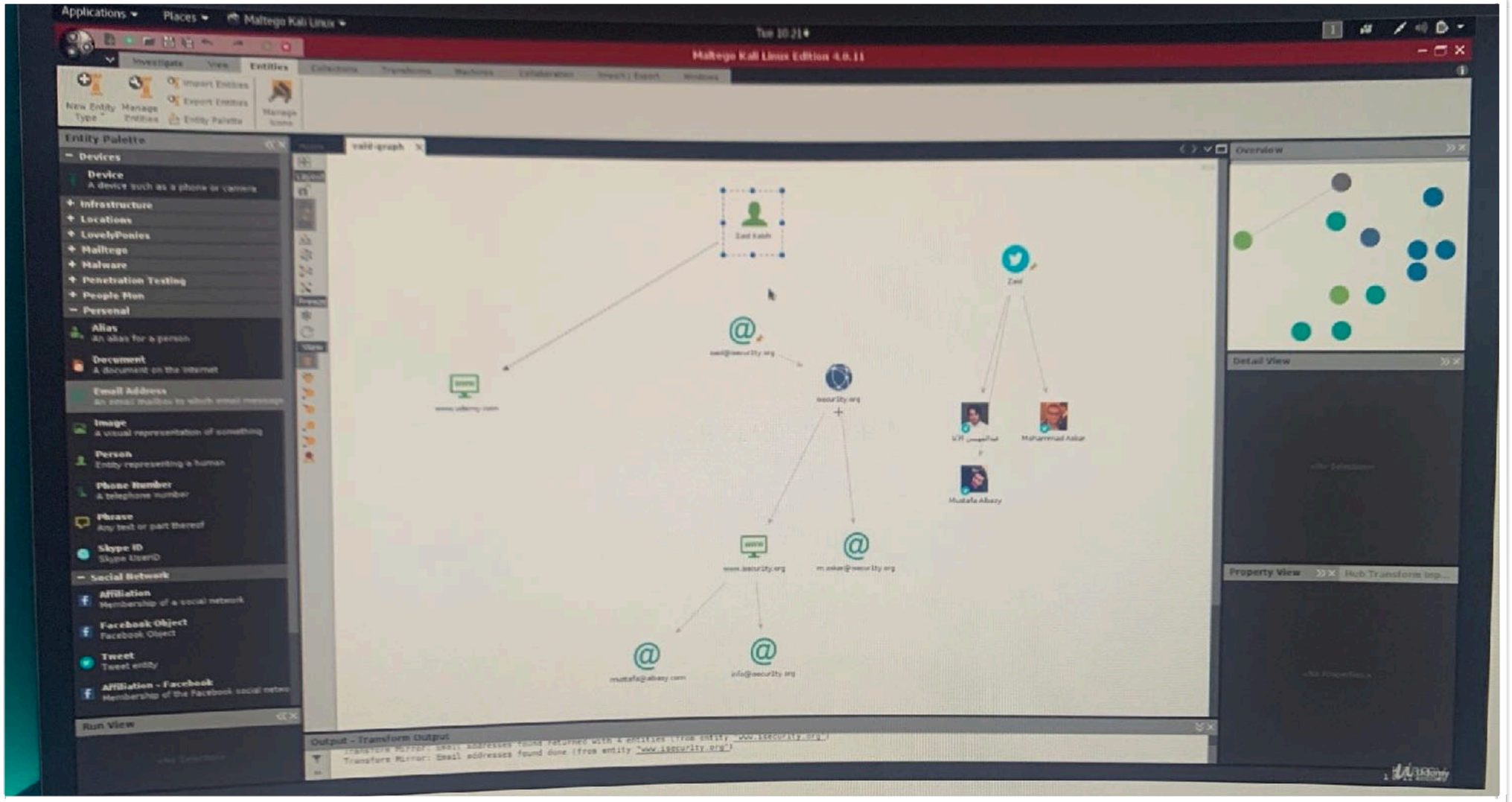
L'email spoofing è una tattica comune utilizzata nei tentativi di phishing e spam, in cui l'indirizzo email di un mittente viene falsificato per apparire come se provenga da un'altra fonte.

è una pratica in cui l'indirizzo email del mittente viene falsificato, cioè viene modificato per apparire come se l'email fosse stata inviata da un'altra persona o organizzazione.

Questo è spesso utilizzato in phishing e altre email fraudolente per ingannare il destinatario a rivelare informazioni personali o finanziarie.

1 Information Gathering

- Gather information about target (company/website/person).
- Discover associated websites, links, companies.
- Associated people, names, emails, phone numbers, social networks, friends.
- Associated social networking accounts.
- Display all info on a graph and build attack strategies.


Applications
Places
Maltego Kali Linux
Maltego Kali Linux Edition 4.0.11
Entity Palette
Devices
Device
A device such as a phone or camera
Infrastructure
Locations
LovelyPonies
Mailtego
Malware
Penetration Testing
People Mon
Personal
Alias
An alias for a person
Document
A document on the internet
Email Address
Image
A visual representation of something
Person
Entity representing a human
Phone Number
A telephone number
Phrase
Any text or part thereof
Skype ID
Skype UserID
Social Network
Affiliation
Membership of a social network
Facebook Object
Facebook Object
Tweet
Tweet entity
Affiliation - Facebook
Membership of the Facebook social netwo
Run View
Overview
Detail View
Property View
Output - Transform Output
Transform Mirror: Email addresses found done (from entity "www.isecurity.org")

Fake Emails

- Send fake emails.
- Looks like it's sent from any address !
- Pretend t o be a friend, company, boss ...etc.
- Friend → Ask to open a file (image, pdf ..etc).
- Support member → ask to login to control panel using fake login page.
- Support member → ask to run a command on server.
- Ask to visit a normal web page.
- .....etc

LEARN TO HACK

WITH

ANTOINE MATTHEWS

SPOOF EMAILS USING EMKEI.CZ

Da: servizioclienti@t1m.it

A: destinatario@email.com

Oggetto: Importante: aggiorna le tue impostazioni di fatturazione

Gentile Cliente,

Abbiamo riscontrato un problema con le tue informazioni di fatturazione.

Per continuare a usufruire dei nostri servizi senza interruzioni, ti preghiamo di aggiornare le tue informazioni di fatturazione il più presto possibile.

Clicca sul link sottostante per aggiornare le tue informazioni:

Aggiorna le tue informazioni di fatturazione

Se non aggiorni le tue informazioni di fatturazione entro 48 ore, potremmo dover sospendere temporaneamente i tuoi servizi.

Ti ringraziamo per la tua attenzione a questa importante questione.

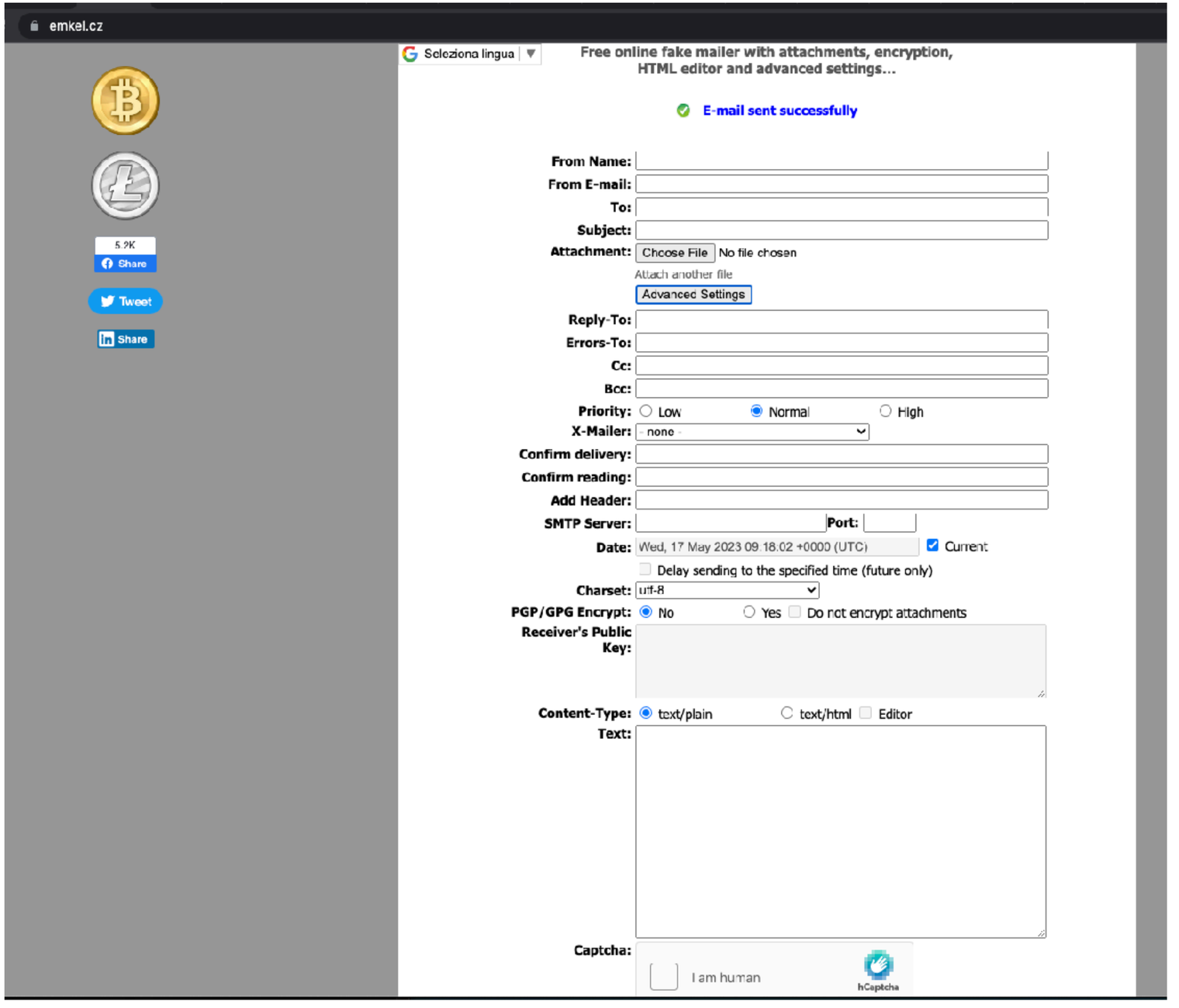
Cordiali saluti,

Il tuo team di servizio clienti TIM

Nell'email di sopra, ci sono alcuni segnali di allarme che possono indicare che si tratta di uno spoofing:

Indirizzo email del mittente: Nonostante il mittente sembri essere "servizioclienti@tim.it", un esame più attento rivela che l'indirizzo email è in realtà "servizioclienti@t1m.it". Questo è un classico esempio di come gli aggressori possono utilizzare caratteri simili per ingannare i destinatari.
Link sospetti: Il link per "aggiornare le tue informazioni di fatturazione" non conduce al sito ufficiale di TIM, ma a un dominio diverso. Questo è un segnale di allarme comune nelle email di phishing e di spoofing.
Richiesta di azione urgente: L'email mette pressione sul destinatario per agire rapidamente, dicendo che i servizi saranno sospesi se non vengono aggiornate le informazioni di fatturazione. Questa è una tattica comune usata dagli aggressori per spingere i destinatari a cliccare su link o aprire allegati senza pensarci due volte.
Ricorda, se ricevi un'email sospetta, non dovresti mai cliccare su link o aprire allegati. Se non sei sicuro, contatta direttamente l'organizzazione o l'individuo da cui l'email sembra provenire, utilizzando un numero di telefono o un indirizzo email che sai essere legittimo.

Bisogna inoltre creare un account su mailup sendinblue per avere smtp server, con gmail etc non funziona.



https://emkei.cz/

Ecco un breve tutorial su come riconoscere un tentativo di email spoofing:

1. **Esamina l'indirizzo email del mittente**:

Non fidarti solo del nome visualizzato. Spesso, gli spoofers utilizzeranno un nome familiare o affidabile, ma l'indirizzo email associato sarà off. Posiziona il mouse sopra il nome per visualizzare l'indirizzo email completo.

2. **Controlla errori di ortografia e grammatica**:

Molti tentativi di phishing sono pieni di errori di ortografia e di grammatica. Se un'email contiene molti errori, potrebbe essere un segno che qualcosa non va.

3. **Fai attenzione alle richieste urgenti o minacciose**:

Le email che creano un senso di urgenza o che minacciano conseguenze negative se non si agisce immediatamente sono spesso un segno di phishing.

4. **Non fare clic su link sospetti**:

Se non sei sicuro della legittimità di un link in un'email, non fare clic su di esso. Invece, vai direttamente al sito web digitando l'indirizzo nella barra degli indirizzi del browser.

5. **Utilizza una soluzione di sicurezza email:**

Ci sono molte soluzioni di sicurezza email disponibili che possono aiutare a proteggere la tua posta elettronica da tentativi di phishing e spoofing.

Ricorda, la consapevolezza è la chiave per prevenire lo spoofing delle email. Assicurati che il tuo team sappia cosa cercare e come agire quando sospettano di un tentativo di phishing.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Grazie

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Per rimanere aggiornati sulle attività di Cyber 4.0 …

Profilo LinkedIn

CYBER 4.0 - Cybersecurity Competence Center

Sito web

www.cyber40.it

Newsletter bisettimanale

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Grazie per l'attenzione

Chiusura lavori e light lunch