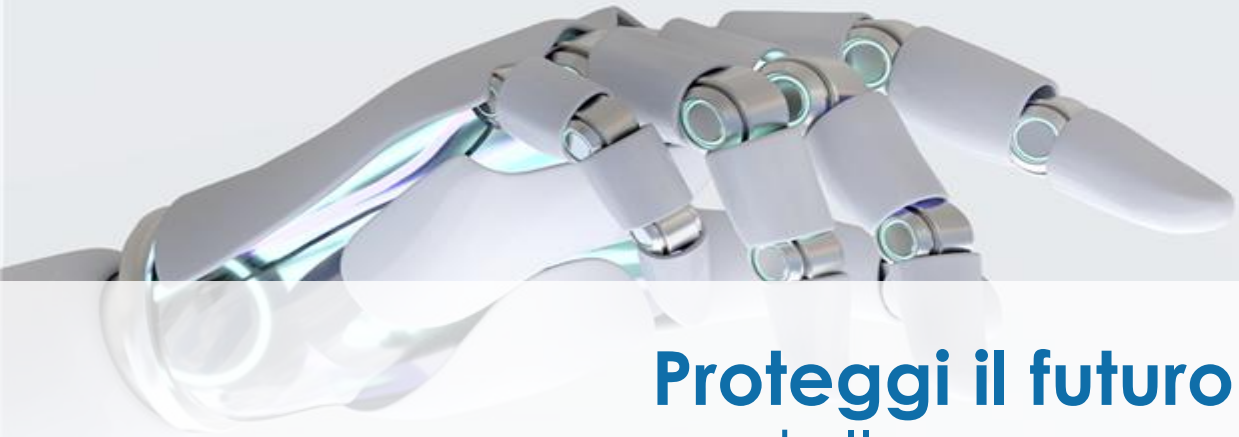


Proteggi il futuro della tua azienda:
dalle cause ai rimedi concreti
23/10/2025

Tommaso Bernardini

Project Manager

TECNOLOGIE PER L'INNOVAZIONE

Timeline TEC4I FVG

2000
Costituzione consorzio Friuli Innovazione

2004
Creazione del Parco Scientifico e Tecnologico Luigi Danieli

2005
Avvio incubatore TechnoSeed

2013
Ampliamento immobiliare PST (da 3.200 a 6.400 mq)

2018
Ingresso di RAFVG nella compagine societaria

2020
Riassetto societario

2022
Approvazione nuovo piano strategico

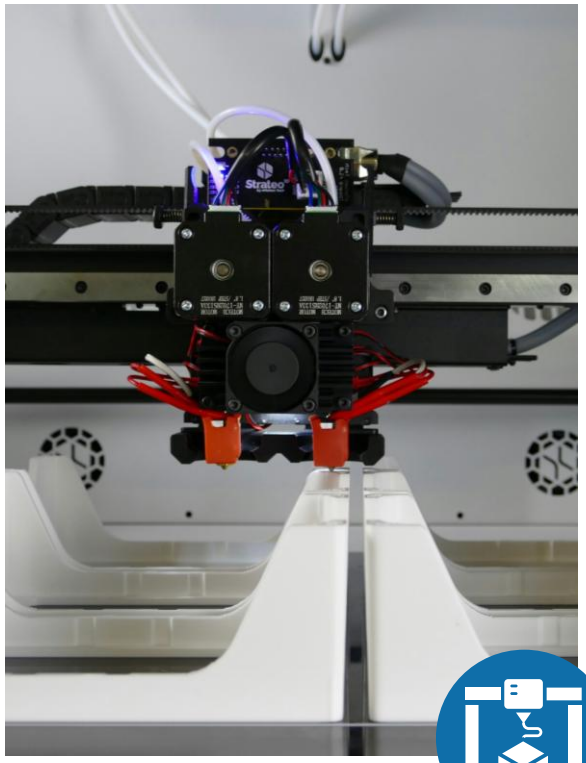
2023
Lancio nuovo brand
100 partecipanti

2024
Lancio cybersecurity

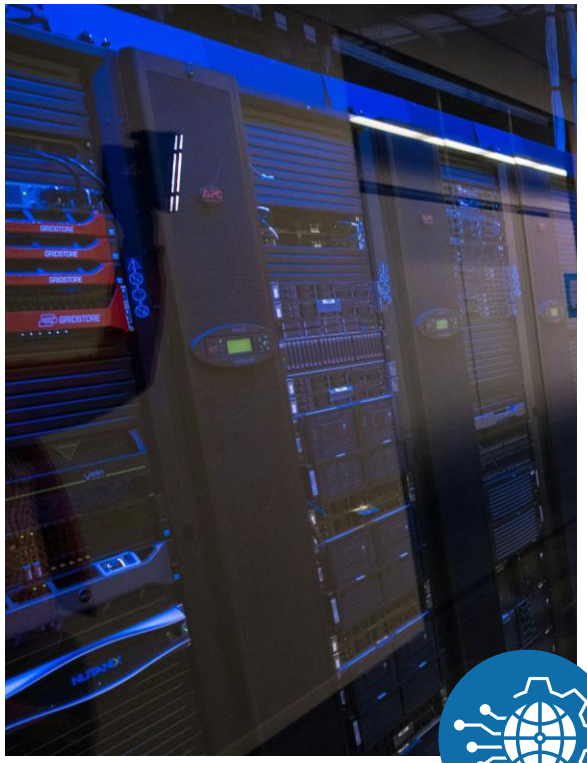
TEC4I FVG è il nuovo brand con cui **Friuli Innovazione** si presenta sul mercato, il marchio, facilmente riconoscibile, riflette il **rinnovamento organizzativo** e valorizza la **nuova strategia** e le nuove competenze per il territorio.

Oggi TEC4I FVG mette a disposizione infrastrutture e **competenze consolidate per lo sviluppo** concreto dell'impresa, sia essa una **PMI** sia una **startup**, in **4 principali ambiti**, due tecnologici e due metodologici.

Ambiti di specializzazione

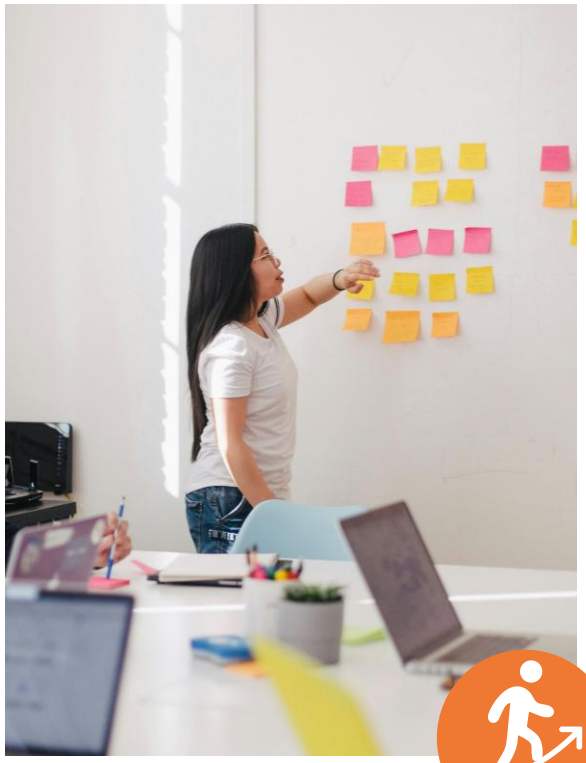


Design e stampa 3D



Tecnologie digitali

Finanza per l'innovazione



Nuove imprese

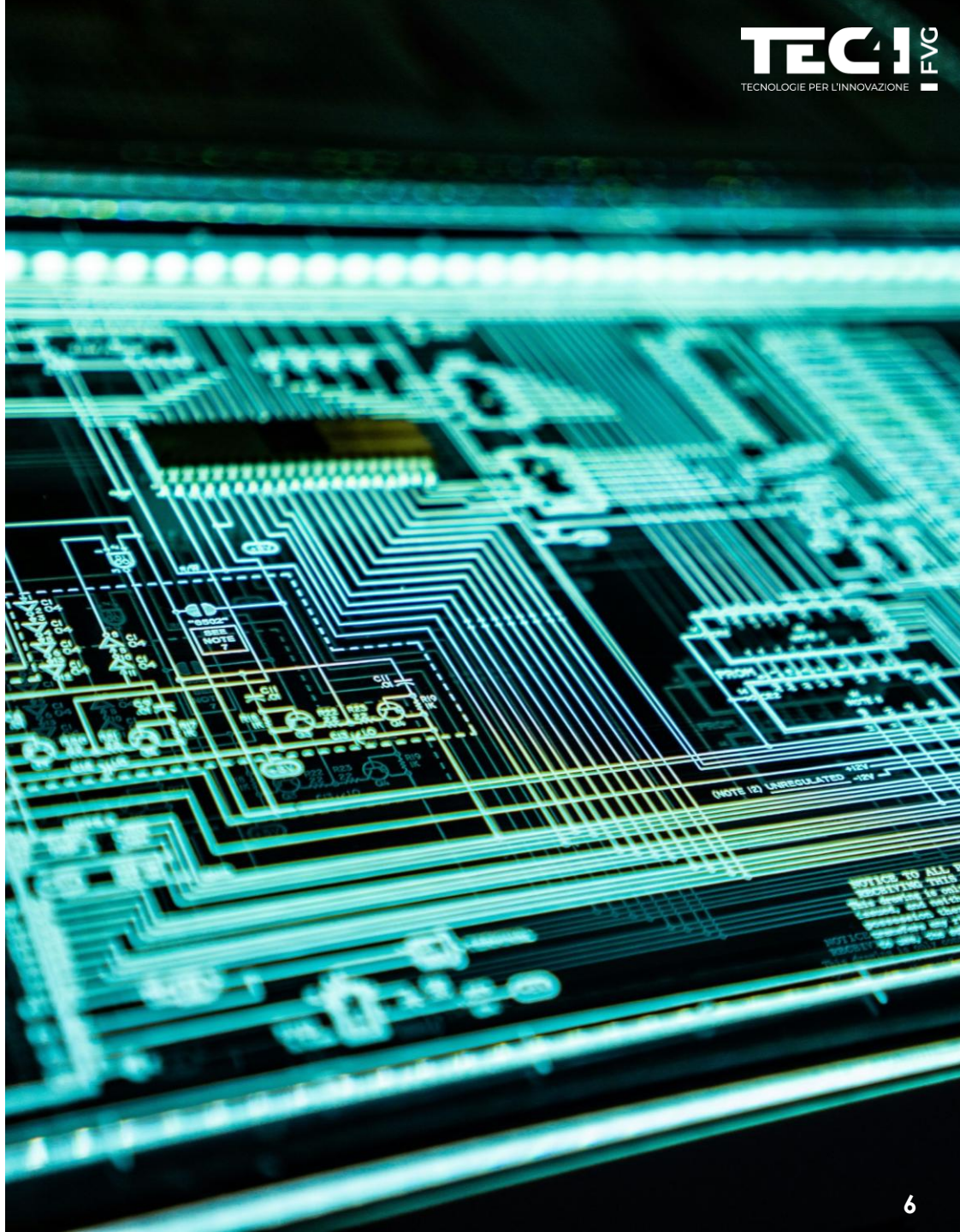
HUB D-ATA - Tecnologie digitali

L'hub **D-ATA** è un **laboratorio esperienziale** e centro di innovazione "data-driven".

Lo scopo è di agevolare l'**innovazione di processo** delle imprese avvicinandole a **metodologie e tecnologie** di data transmission, storage, analysis e security.

Tre **ambiti** di specializzazione:

- **Digitalizzazione**
- **Cybersecurity**
- **Edge Computing**



Loris Collina

Referente tecnico HUB Tecnologie Digitali

TECNOLOGIE PER L'INNOVAZIONE

Cybersecurity: i principali trend italiani

“Nel 2024 in Italia si sono registrati 357 attacchi informatici gravi, *tra quelli noti*. Il 10% degli attacchi globali, il numero più alto di sempre ”

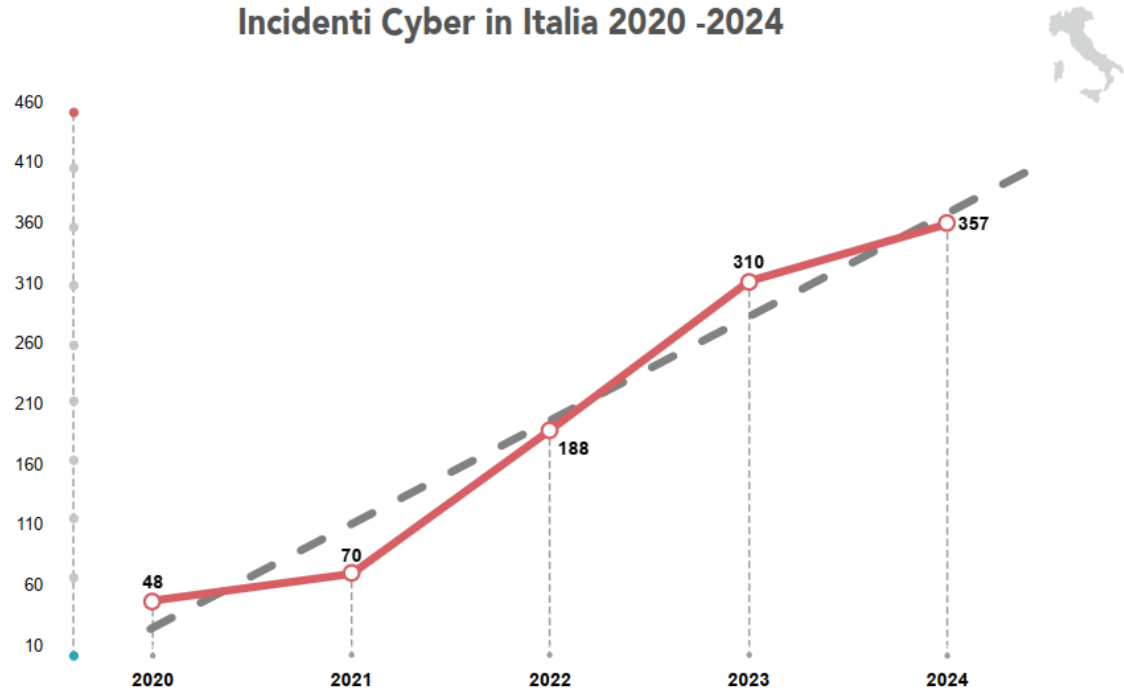
Clusit

“Non si tratta solo di quantità, ma anche della crescente sofisticazione degli attacchi, che nell'81% dei casi presentano una gravità alta o critica. Difendersi richiede come primo passo l'identificazione delle proprie
vulnerabilità per averne consapevolezza e poter prendere le opportune contromisure prima che malintenzionati le possano sfruttare a loro favore”

Cybersecurity: i principali trend italiani

2020-2024:

- **973** incidenti noti **di particolare gravità**
- **357** nel solo 2024 (+15% vs. 2023)
- **10%** degli incidenti **globali** (Francia 4%, Germania 3%, UK 3%)



Fonte rapporto @Clusit 2025 ICT Security in Italia

Cybersecurity: i principali trend italiani

2024:

AUMENTO DELLE VIOLAZIONI DEI DATI PERSONALI

I tentativi di attacco ai database aziendali sono cresciuti del 25% rispetto al 2023, con un focus particolare su settori come sanità, enti governativi e servizi finanziari. Ben 218 file di raccolte di credenziali appartenenti a cittadini italiani rilevati in vendita nel **Dark Web**

INCREMENTO DELLE CAMPAGNE RANSOMWARE

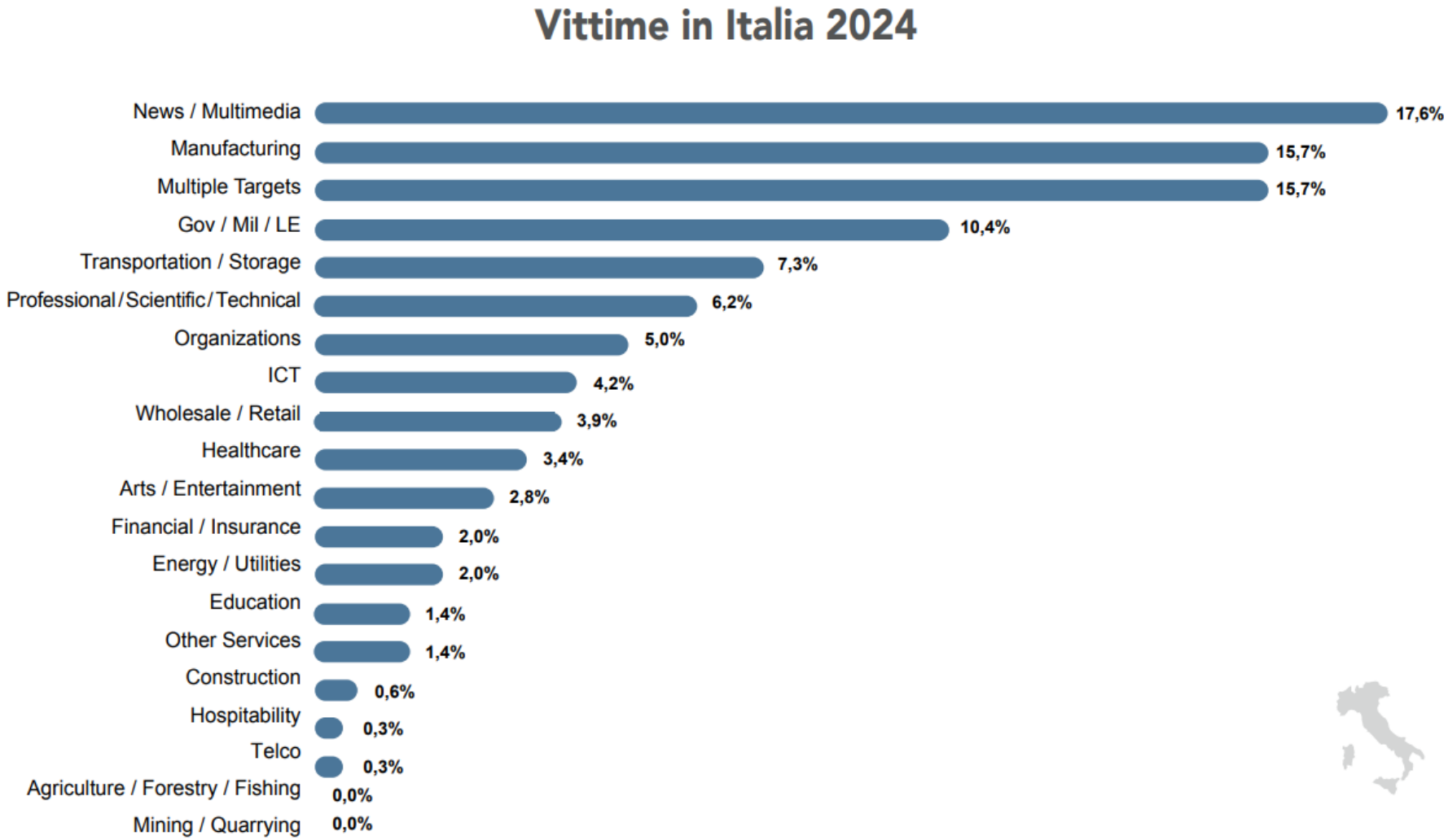
Si è osservato un incremento medio del 30% di attacchi informatici mirati aventi come obiettivo la richiesta di riscatto. Diverse PMI e istituzioni italiane sono state colpite da attacchi ransomware

UTILIZZO DELLA GEN-AI DA PARTE DEGLI ATTACCANTI

E' stato riscontrato un aumento dell'utilizzo dell'AI per creare **e-mail di phishing** più convincenti e bypassare le difese basate su algoritmi tradizionali. Una campagna di phishing condotta contro una nota banca ha sfruttato l'AI per simulare comunicazioni interne realistiche ingannando oltre 200 dipendenti.

Fonte rapporto @Clusit 2025 ICT Security in Italia

Settori maggiormente colpiti



Fonte rapporto @Clusit 2025 ICT Security in Italia

L’impatto di un attacco informatico

Gli **attacchi informatici** rappresentano una **minaccia costante** per le organizzazioni e portano a:

- Malfunzionamento dei propri sistemi IT
- Interruzioni operative e conseguente perdita di produttività
- Manipolazioni del sito web
- Perdita del know-how aziendale salvato nei dati potenzialmente cifrabili da un ransomware
- Pagamenti di corposi riscatti in valuta virtuale che non danno comunque garanzie sulla restituzione dei contenuti
- Divulgazione di documenti sensibili
- Versamenti bancari su conti correnti «trappola»
- Perdita di reputazione aziendale

  Multe e sanzioni
- Perdita di fatturato

Le aziende devono adottare misure preventive per proteggere i propri asset digitali e garantire l’ operatività.

Fonte rapporto CYBEROO Cyber Threat Report 2025

Casi recenti

Economia / PMI

Assalto hacker in Veneto, 30 pmi attaccate in 10 giorni

Rischi sventati, richiesti riscatti fino a 400 mila euro

Una trentina di aziende di dimensione medio piccola, con sede in Veneto, sono state fatte oggetto dal 21 febbraio scorso di altrettanti attacchi informatici arrecati ***sfruttando falle nei sistemi "firewall" e vulnerabilità di altra natura.***

Lo rende noto l'azienda specializzata nella sicurezza digitale Yarix (Var Group), di Treviso, la quale è stata comunque in grado di ripristinare la completa operatività dei propri clienti in 72 ore e di individuare gli autori delle aggressioni in un gruppo internazionale chiamato Threat Actor Akira.
I riscatti richiesti dai pirati informatici per "liberare" i sistemi delle aziende dai blocchi imposti dalla loro azione criminale sarebbero stati compresi tra i 100 mila ed i 400 mila euro ciascuna.

Fonte: ANSA, 04/03/25 (https://www.ansa.it/sito/notizie/economia/pmi/2025/03/04/assalto-hacker-in-veneto-30-pmi-attaccate-in-10-giorni_b89356fe-2181-4563-a24b-db17e1981f0f.html)

Casi recenti

Impresa	Settore	Prov.	Data	Tipologia di attacco	Conseguenze
Rothoblaas Srl	Costruzioni	BZ	26/09/24	Ransomware	Blocco produzione 3gg
Alf Group – Alf DaFrè	Legno-arredo	TV	10/02/25	Ransomware	Blocco produzione 2 sett., 350 dipendenti in CIG
Asolo Dolce Srl	Dolciario	TV	12/04/25	Ransomware	Blocco caselle email aziendali e esfiltrazione di dati industriali
Danieli & C. Officine Meccaniche	Siderurgia	UD	19/02/25	DDoS	Sito irraggiungibile per alcune ore

Fonti:

- Rothoblaas: https://www.rainews.it/tgr/bolzano/articoli/2024/09/azienda-altoatesina-paralizzata-da-attacco-hacker-037969d8-2153-4a98-9815-27b63687b30a.html
- Alf Group: https://www.cybersecitalia.it/alf-dafre-attacco-ransomware-allo-stabilimento-produzione-bloccata-e-350-dipendenti-in-cassa-integrazione/44073/
- Asolo Dolce: https://www.oggitreviso.it/asolo-dolce-finisce-nel-mirino-degli-hacker-dati-rubati-richiesta-di-riscatto-au23898-353435
- Danieli & C.: https://www.ansa.it/canale_tecnologia/notizie/cybersecurity/2025/02/19/terzo-giorno-di-attacchi-hacker-allitalia-giu-siti-banche_ad2c3a57-6922-47e0-9507-fd065fa338b6.html

Scenario normativo

Il **GDPR** (General Data Protection Regulation) è un regolamento europeo che disciplina la protezione dei dati personali. **Si applica a tutte le aziende e organizzazioni che trattano dati personali**.

La **NIS2** (Network and Information Security) è la nuova direttiva europea che obbliga le aziende coinvolte ad **aumentare la propria cyber resilienza e a monitorare l'intera filiera IT delle aziende collaboratrici**.

Scenario normativo - GDPR

Il **GDPR** (Regolamento Generale sulla Protezione dei Dati) UE 2016/679 è entrato in vigore il 25 maggio 2018 Si applica a tutte le organizzazioni che trattano dati personali di cittadini UE, anche se l'azienda ha sede fuori dall'UE. **Qualsiasi informazione che può identificare una persona fisica** (nome, email, indirizzo IP, dati biometrici, preferenze religiose, dati medici ecc.).

Scenario normativo – GDPR (1/2)

Aspetti fondamentali di compliance:

1. Sicurezza dei dati (Art. 32 GDPR)

Implementare misure tecniche e organizzative adeguate per garantire:

- Riservatezza (accesso solo agli autorizzati)
- Integrità (dati non alterati)
- Disponibilità (dati sempre accessibili quando servono)
- ***Valutazione periodica dell'efficacia delle misure di sicurezza (VAPT è uno degli strumenti chiave)***

2. Crittografia e pseudonimizzazione

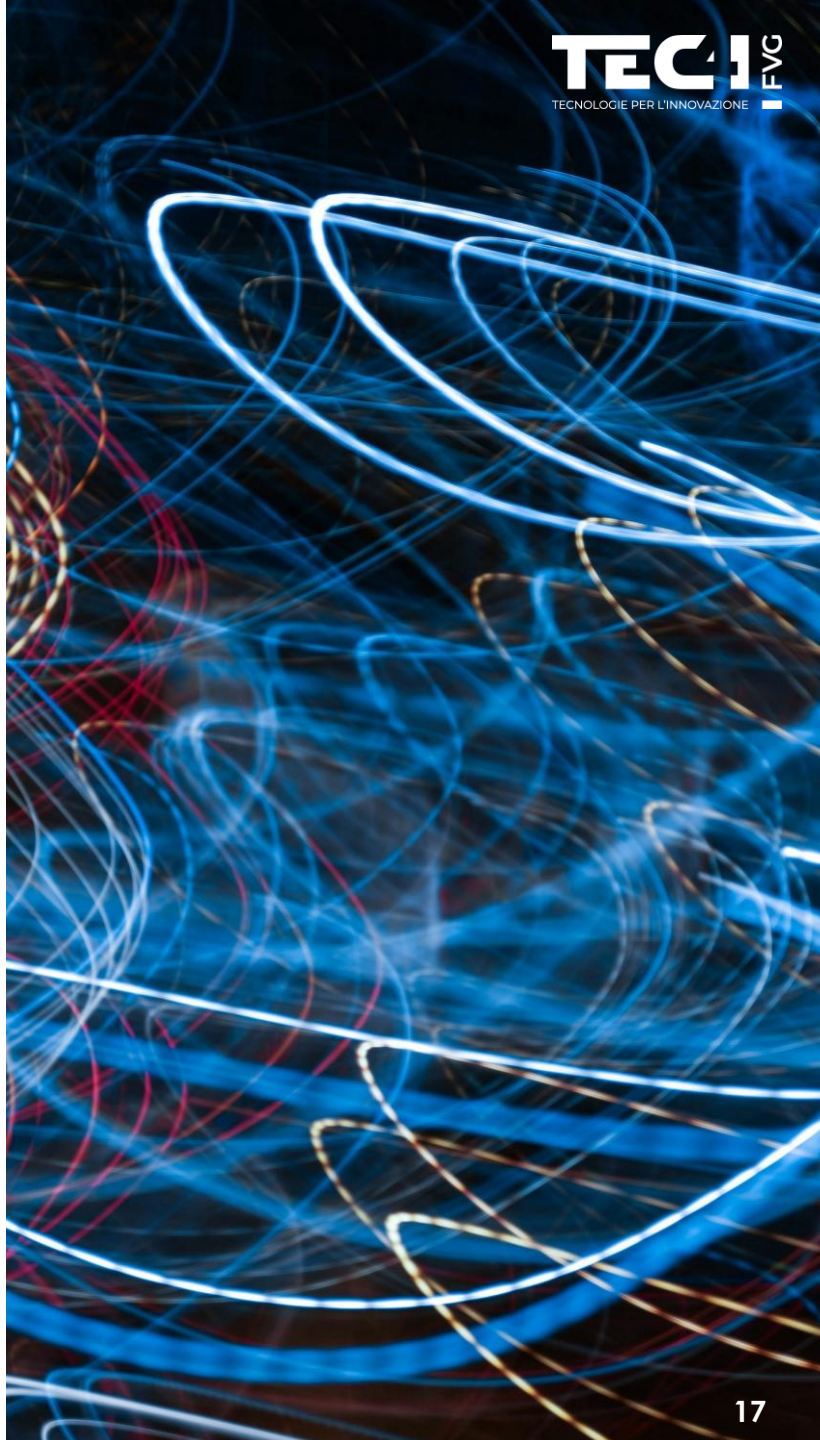
Cifratura dei dati per renderli illeggibili a chi non ha la chiave.
Pseudonimizzazione: sostituire dati identificativi nei documenti con alias o codici.

3. Data governance e gestione dei consensi

Sistemi che registrano e tracciano i consensi espliciti e la loro eventuale revoca.
Tracciabilità delle modifiche ai dati (audit trail)

4. Data minimization e gestione del ciclo di vita dei dati

Raccogliere solo i dati necessari per lo scopo dichiarato.
Automatizzare la cancellazione o l'anonimizzazione dopo la scadenza dei termini di conservazione.



Scenario normativo – GDPR (2/2)

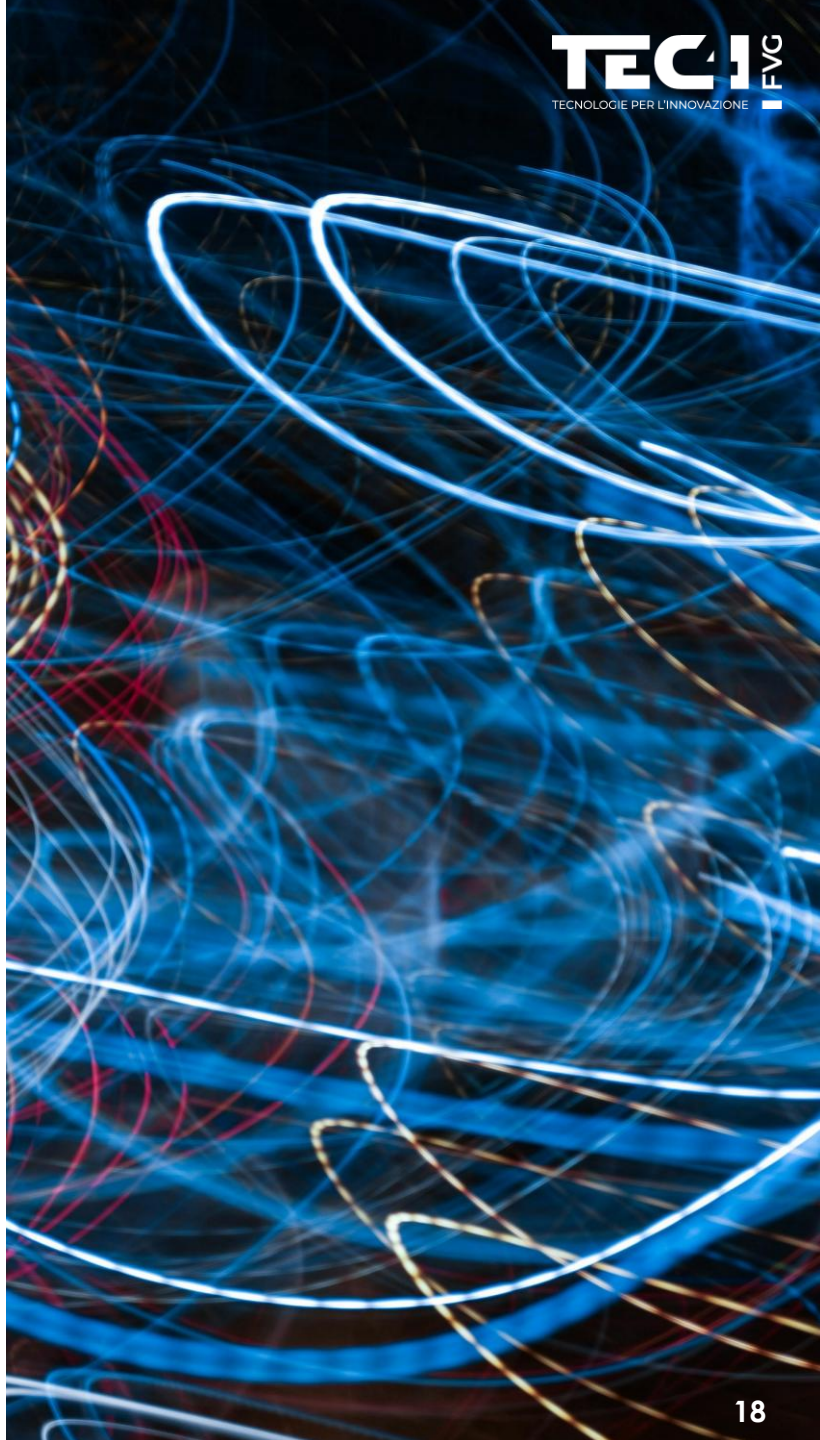
5. Controllo accessi e autenticazione
Implementare:
- Autenticazione a più fattori (MFA)
- Policy di password robuste
- Ruoli e privilegi di accesso ben definiti

6. DPIA (Valutazione d'impatto)
Analisi dei rischi prima dell'avvio di trattamenti ad alto impatto (es. profilazione, sorveglianza).
Devono essere documentate.

7. Notifica delle violazioni (data breach)
Sistemi di monitoraggio e logging per rilevare accessi non autorizzati o fughe di dati.
Procedure automatizzate per segnalare il breach entro 72 ore.

8. Formazione e consapevolezza
Programmi di awareness per il personale IT e non IT su gestione sicura dei dati personali.

9. Trasferimento sicuro dei dati
Uso di protocolli sicuri (es. HTTPS, SFTP).



Scenario normativo – NIS 2

Oltre al Regolamento generale sulla protezione dei dati (GDPR), l'UE ha introdotto una **direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS)** per stabilire i requisiti di sicurezza informatica nelle reti. Nel 2023, la direttiva NIS è stata aggiornata e rinominata NIS 2. Questa direttiva è diventata **legge in Italia il 16 ottobre 2024**. **Le aziende Italiane dovranno uniformarsi alle misure tecniche previste dal decreto entro ottobre 2026.**

In sintesi l'obiettivo è quello di **rafforzare** e **stabilire un elevato livello comune di sicurezza informatica in tutta l'UE.**

Settori interessati dall'applicazione:

- **Energia** – inclusi energia elettrica, teleriscaldamento e teleraffrescamento, petrolio, gas e idrogeno.
- **Trasporti** – inclusi il trasporto aereo, ferroviario, per vie d'acqua e su strada.
- **Settore bancario** – inclusi gli enti creditizi.
- **Infrastrutture dei mercati finanziari**
- **Settore sanitario** – inclusi prestatori di assistenza sanitaria, laboratori di riferimento dell'UE, ricerca e sviluppo di medicinali, prodotti farmaceutici NACE C21 e dispositivi medici critici.
- **Acqua potabile** – inclusi fornitori e distributori di acqua.
- **Acque reflue** – inclusi la raccolta, lo smaltimento o il trattamento.
- **Infrastrutture digitali** – inclusi fornitori di: punti di interscambio internet ISP, DNS, registri TLD, servizi cloud, data center, CDN
- **Tecnologie dell'informazione e della comunicazione (TIC)** – inclusi fornitori di servizi gestiti e fornitori di servizi di sicurezza
- **Pubblica amministrazione** – inclusi enti di amministrazione centrale e di amministrazione regionale.
- **Spazio** – incluse le infrastrutture terrestri.

Scenario normativo – NIS 2

Mentre il GDPR parla di “misure adeguate” la NIS2 dettaglia in modo più chiaro cosa serve implementare.

Misure tecniche e organizzative obbligatorie (Art. 21 NIS2):

1. Gestione del rischio informatico
Incident response
Business continuity e disaster recovery
Sicurezza nella supply chain (fornitori inclusi)
Crittografia end-to-end e sicurezza dei sistemi di comunicazione
Controllo accessi e gestione delle identità
Gestione delle vulnerabilità note

2. Obbligo di misure proattive
Aggiornamenti e patching regolari
Segmentazione di rete
Backup cifrati
Sistemi di monitoraggio e rilevamento (SIEM, IDS/IPS)
***Test periodici quali VAPT*, test di intrusione**

3. Notifica incidenti di sicurezza
Incidenti devono essere notificati entro 24 ore (contro le 72h del GDPR)
Devono essere riportati anche gli incidenti potenzialmente gravi, non solo quelli effettivi
Occorre produrre un report completo entro 72h e uno finale entro un mese

4. Ruolo del management e governance interna
Il top management è personalmente responsabile in caso di violazione della direttiva
Obbligo di formazione continua per il personale e per i dirigenti

5. Supervisione, ispezioni e sanzioni
Le autorità nazionali come l' ACN (Autorità Nazionale per la Cybersicurezza in Italia) possono ispezionare e sanzionare
Sanzioni: fino a 10 milioni di euro o 2% del fatturato annuo mondiale

NIS 2 – Attività consigliate per tendere alla compliance

1 - Protezione perimetrale della rete aziendale, firewall con servizi di sicurezza attivi quali IDS, GAV, Botnet Detector, Filtro sulla navigazione web con categorizzazione dei siti, Geo IP Filter, Sandbox, DPI SSL Inspection, DNS Security

2 - Segmentazione della rete tramite adozione di VLAN

3 - Aggiornamento regolare sistemi operativi e software

4 - Endpoint protection sui dispositivi possibilmente in sinergia con il firewall

5 - Utilizzo di password complesse

6 - Protezione doppio fattore (2FA)

7 - Restrizione dei privilegi d'accesso ai dati, governance (Software specifici)

8 - Backup regolari, cifrati e immutabili

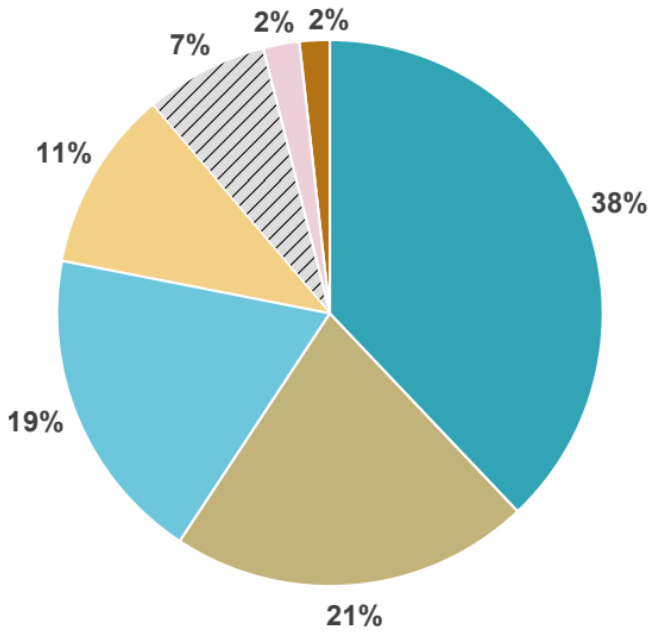
9 - Formazione e sensibilizzazione costante dei collaboratori

10 - Piano d'azione da applicare in caso d'attacco

11 - Monitoraggio costantemente dei sistemi informatici

12 - Audit di sicurezza e test di penetrazione regolari (VAPT)

Tipologie di attacchi più comuni rilevati in Italia nel 2024



Vulnerabilities: Lo sfruttamento di ***vulnerabilità*** comuni e zero-day su vari dispositivi IP. 1.473 CVE identificate sui devices di fornitori di cui 177 di livello critico e 456 di livello alto. Necessaria l'installazione di patch o aggiornamenti che spesso le aziende ignorano o non riescono a mettere in campo per tempo.

DDoS: Statisticamente in crescita in aumento del 53% rispetto al 2023. Altamente sfruttate e coinvolte botnet di dispositivi IoT, Videocamere IP, Router, centralini IP non aggiornati e altri dispositivi esposti su internet compromessi e ***vulnerabili.***

Malware: macrocategoria a cui appartengono gli attacchi ransomware. Diffusi principalmente grazie al phishing ma anche tramite lo sfruttamento di ***vulnerabilità*** o credenziali compromesse, sfrutta il dark web per estorcere denaro alle aziende

Phishing e Social Engineering: 29.191 Domini sospetti rilevati tra cui 900 particolarmente malevoli. La sofisticazione delle tecniche utilizzate tramite l'ausilio dell'intelligenza
artificiale e l'utilizzo sempre più presente di domini malevoli, piattaforme di videoconferenza o strumenti di condivisione file rendono questo vettore uno tra i più utilizzati.

Fonte rapporto @Clusit 2025 ICT Security in Italia

Vulnerabilità - Categorizzazione

Si tratta di falle di sicurezza nei dispositivi installati nelle nostre reti informatiche che quotidianamente vengono alla luce anche grazie al lavoro di ricerca di team di Cybersecurity. Quando una vulnerabilità viene trovata è solo questione di tempo perché la prova concettuale del bug venga implementata in tool specifici per l'attacco. Se la vulnerabilità non è stata nel frattempo risolta l'attacco ha successo permettendo nei peggiori dei casi l'esecuzione di codice RCE (Remote Code Execution) dall'interno del dispositivo.

I sistemi e i devices informatici tendono a invecchiare e con loro il firmware e il software che gli permette di funzionare. Il fw/sw viene costantemente aggiornato dai produttori per ottemperare ai problemi di sicurezza e bachi che col tempo vengono alla luce.
E' una rincorsa continua all'aggiornamento dei sistemi nell'intento di renderli più resilienti.
Purtroppo i produttori di dispositivi IT supportano solo per alcuni anni i propri prodotti rispettando quanto descritto in precedenza. Dopo alcuni anni i dispositivi entrano nella fase di EOL (End Of Life). Ad esempio i sistemi operativi Microsoft Windows Server 2003, 2008, 2012 R2 entrato in EOL a Ottobre del 2024 o vecchi switch di HP che non ricevono più software aggiornato per patchare la vulnerabilità OpenSSH descritta nella prossima slide. Non ricevono più l'adeguato supporto dei produttori, viene quindi richiesto il cambio del dispositivo con dispositivi più recenti, moderni e coperti dal supporto.

CVE *(Common Vulnerability and Exposures)*
Le vulnerabilità scoperte vengono raccolte in un database mantenuto dal Dipartimento della sicurezza interna degli Stati Uniti che ne tiene traccia assegnandogli un codice univoco preciso es. **CVE-2023-27997**

CVSS *(Common Vulnerability Scoring System)*
Standard Open-Source per categorizzare la gravità delle vulnerabilità. Da la possibilità alle aziende di gestire la priorità nella fase di remediation delle vulnerabilità incontrate che vengono categorizzate in una scala da 0 rischio minimo a 10 rischio massimo

Vulnerabilità più comuni rilevate nel 2024

CVE-2023-27997
Una gravissima vulnerabilità di tipo buffer overflow che ha interessato i diffusissimi firewal della **FORTINET.** Agli attaccanti ha consentito addirittura di eseguire codice da remoto.

CVE-2023-4966
Una vulnerabilità di tipo buffer overflow che ha interessato alcune versioni dei dispositivi Netscaler di **Citrix** usati per l'accesso remoto alle reti aziendali. Ha consentito agli attaccanti da remoto di accedere ad informazioni sensibili come i token di sessione.

CVE-2024-6387
Gravissima vulnerabilità che ha afflitto le librerie **OpenSSH** usate praticamente su ogni dispositivo IT per consentirne l'amministrazione. Essa ha permesso a un attaccante l'esecuzione di codice da remoto con privilegi da root.

CVE-2024-53704
Vulnerabilità di authentication bypass rilevata in alcune versioni non aggiornate di SonicOS utilizzate nei firewall **SonicWall.** Questa vulnerabilità affligge il portale di autenticazione SSL-VPN che normalmente è esposto su internet per permettere l'accesso alla rete aziendale da parte agli utenti da remoto.
Se correttamente sfruttata, l'attaccante riesce a bypassare la multi-factor authentication accedendo quindi a una sessione SSL-VPN valida.

Fonte rapporto CYBEROO Cyber Threat Report 2025

VAPT – Vulnerability Assessment e Penetration Test

Entrambi i servizi mirano a scovare le criticità dei sistemi informatici. Tuttavia l'approccio e il risultato sono diversi.

VA *(Vulnerability Assessment)*

- Individua e misura il **grado di gravita delle vulnerabilità analizzando ogni device IP** trovato in rete
- Comporta l'utilizzo di strumenti specifici come **Web-Vulnerability o Network-Security-Scanner**
- Si conclude con un **report** che elenca i possibili punti deboli di un sistema CVE in ordine di gravità e del livello di rischio associato e in alcuni casi fornisce indicazioni sui possibili rimedi o migrazioni verso dispositivi più recenti e aggiornati
- Non è invasivo, non cerca di prevaricare i sistemi del cliente

PT (Penetration Test)

- Si tratta di un **attacco vero** e proprio a **scopo dimostrativo** per verificare che una **vulnerabilità scovata sia effettivamente autentica** e quali **conseguenze** comporti per l'azienda che la subisce
- **Sfrutta le vulnerabilità** trovate per raggiungere la **compromissione dei sistemi**
- **Dimostra** come un attaccante malintenzionato potrebbe eludere le difese e sfruttare le vulnerabilità per accedere ai dati o prendere il controllo dei sistemi
- Viene svolta da **team di Etical Hacker** che utilizzano tool anche proprietari e tecniche aggressive
- Cerca di **limitare il più possibile i danni** ma comunque è **possibile una compromissione** dei sistemi per cui prima di lanciare un PT vengono presi accordi con il cliente e viene fatta firmare una manleva.

Vulnerability Assessment - Vantaggi

1. **Aumento della sicurezza informatica e conseguente calo del rischio legato al Cybercrime**

2. **Riduzione del rischio legale e reputazionale**

3. **Conformità normativa**. Favorisce il rispetto di normative e standard come **GDPR, ISO/IEC 27001, PCI-DSS, NIS2**. Fornisce report documentati utili in caso di audit o controlli di enti regolatori

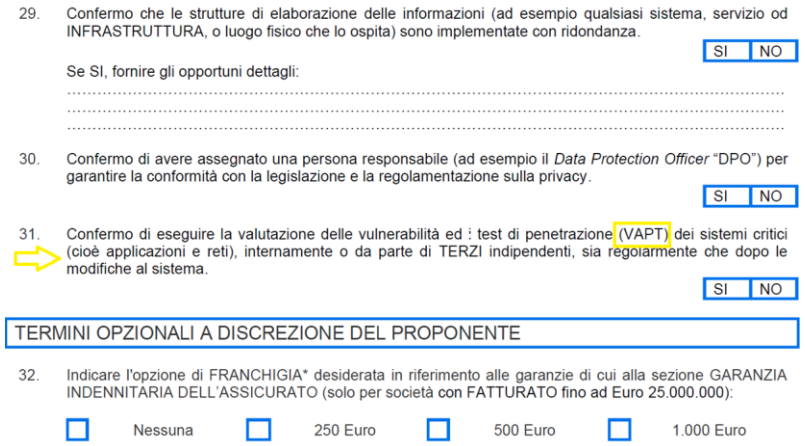
4. **Ottimizzazione dei costi** in quanto individuare vulnerabilità in anticipo è molto meno costoso che gestire un incidente.

5. **Miglioramento continuo**: offre una visione aggiornata e periodica della postura di sicurezza dell'azienda.

6. **Supporto alle decisioni**: fornisce dati oggettivi che supportano la direzione IT e la dirigenza nel prendere decisioni strategiche aiutando a definire le priorità di intervento sulla base della gravità e dell'impatto delle vulnerabilità.

7. **Maggiore fiducia di clienti e partner**. Dimostra un impegno attivo nella sicurezza, migliorando la reputazione e la fiducia da parte di stakeholder, clienti e partner commerciali.

8. **Condizioni più vantaggiose su polizze assicurative contro il Cybercrime**



29. Confermo che le strutture di elaborazione delle informazioni (ad esempio qualsiasi sistema, servizio od INFRASTRUTTURA, o luogo fisico che lo ospita) sono implementate con ridondanza.

SI | NO

Se SI, fornire gli opportuni dettagli:

.....

.....

.....

30. Confermo di avere assegnato una persona responsabile (ad esempio il *Data Protection Officer* "DPO") per garantire la conformità con la legislazione e la regolamentazione sulla privacy.

SI | NO

31. Confermo di eseguire la valutazione delle vulnerabilità ed i test di penetrazione (VAPT) dei sistemi critici (cioè applicazioni e reti), internamente o da parte di TERZI indipendenti, sia regolarmente che dopo le modifiche al sistema.

SI | NO

TERMINI OPZIONALI A DISCREZIONE DEL PROPONENTE

32. Indicare l'opzione di FRANCHIGIA* desiderata in riferimento alle garanzie di cui alla sezione GARANZIA INDENNITARIA DELL'ASSICURATO (solo per società con FATTURATO fino ad Euro 25.000.000):

☐ Nessuna ☐ 250 Euro ☐ 500 Euro ☐ 1.000 Euro

Esempio di polizza contro il Cybercrime

TEC4I FVG
TECNOLOGIE PER L'INNOVAZIONE

TEC4I Cybersecurity Checkup

Scopri quanto è davvero sicura la tua azienda:
vulnerabilità, esposizioni e azioni concrete in un'unica analisi.

TEC4I Cybersecurity Checkup

TEC4I **Cybersecurity Checkup** è un checkup completo per valutare la vulnerabilità dei sistemi informatici aziendali.

1. Extended Vulnerability assessment (EVA)

Assessment tecnico che permette di identificare le **vulnerabilità** presenti nelle reti e nei dispositivi aziendali.

2. Cyber Risk Investigation

Indagine nel web e dark web (CRI) per rilevare eventuali dati aziendali già compromessi. Il tutto è completato dal **supporto** specialistico **dei tecnici TEC4I**, che aiutano nell'interpretazione dei risultati e nella definizione delle **azioni correttive.**

Vantaggi

- **Visione completa** della situazione di **sicurezza** del sistema
- **Report** pratici e dettagliati
- **Validazione** da esperti CEH (**Certified Ethical Hacker**)

È sufficiente un'unica analisi per identificare le vulnerabilità, i servizi esposti e le azioni specifiche da intraprendere per correggere il problema.

TEC4I EVA "Extended Vulnerability Assessment"

VAPT: EVA (*Extended Vulnerability Assessment)*

Un servizio di Vulnerability Assessment esteso in quanto include anche alcune caratteristiche tipiche dei Penetration Test.
Si compone di tre moduli:

EVA INTERNAL:
Viene svolto dal nostro personale tecnico dopo un allineamento con il supporto IT del cliente.
Viene preparato l'elenco dei dispositivi da analizzare, viene instaurata una VPN per permettere l'accesso in rete al software di analisi e viene lanciata la scansione sui dispositivi interni alla rete presenti anche su diverse VLAN se presenti.
Durante il test i dispositivi devono rimanere accesi e collegati alla rete. Tempo medio di esecuzione otto, nove ore ma dipende dal numero di IP da analizzare. Non pregiudica il lavoro dei dipendenti che durante il test possono continuare a lavorare.

EVA PUBLIC:
La scansione viene lanciata verso gli IP del cliente pubblicati in internet come ad esempio Firewall, sistemi di accesso VPN, servizi di condivisione files, server esposti, router ecc..

EVA URL:
Viene analizzato il sito web dell'azienda o altri siti di proprietà aziendale alla ricerca di codice malformato o librerie obsolete che possono portare alla compromissione del sito. I risultati possono essere inviati al manutentore del sito web per le opportune correzioni

TEC4I EVA
Extended Vulnerability Assessment

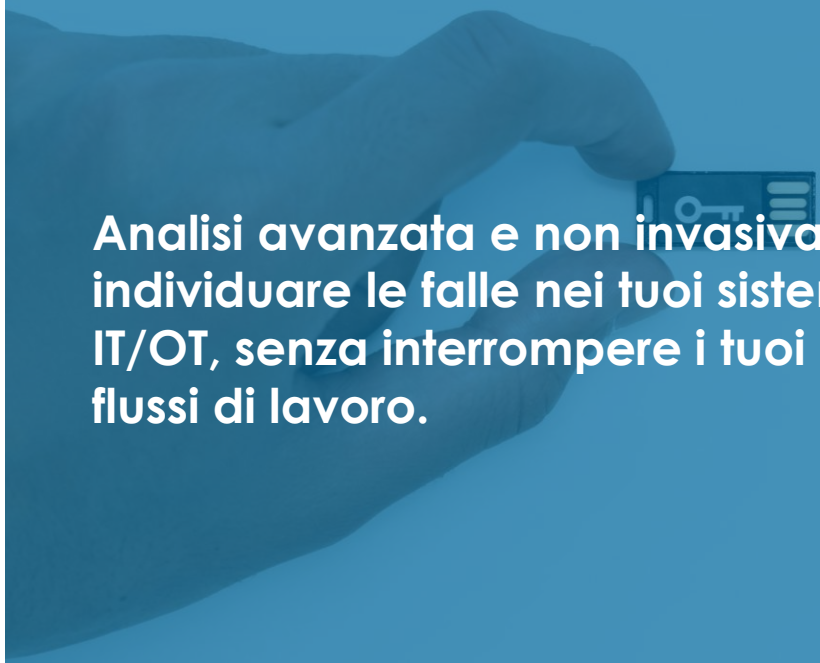
TEC4I EVA è un'analisi automatica delle **vulnerabilità di reti e dispositivi**: un test avanzato per identificare punti deboli nei sistemi IT/OT aziendali.

Come funziona
- **Test adattivo** e non invasivo, con scansione interna/esterna
- **Tecnologia IA** basata su framework OWASP, OSSTMM, CVE/CWE/CVSS
- **Nessuna interruzione dei servizi**

Output
- Elenco **vulnerabilità rilevate**
- **Dettagli tecnici** e suggerimenti di **remediation**

Vantaggi
- **Visione chiara** delle criticità
- **Report** conforme a **ISO 27001/2, NIS2** e **GDPR** (Art. 32)
- Validazione CEH (**Certified Ethical Hacker**)

Processo
1. Brief tecnico
2. Test on-site 24-48h
3. Consegna e discussione report



Analisi avanzata e non invasiva per individuare le falle nei tuoi sistemi IT/OT, senza interrompere i tuoi flussi di lavoro.

TEC4I Cyber Risk Investigation

Raccolta, analisi e interpretazione dati da fonti aperte e chiuse per individuare potenziali informazioni informatiche diffuse online a riguardo il dominio aziendale per proteggere le aziende in modo efficace.

Fornendo il nome del dominio aziendale come ad esempio **@aziendatest.it** parte la ricerca online

Le aziende sono sempre più vulnerabili ai cyber attacchi a causa delle informazioni disponibili e condivise online
Conoscere ciò che circola nel web a riguardo il proprio dominio aziendale aiuta a proteggersi
Viene compresa l' esposizione aziendale
Fornisce dati su attacchi passati

L'analisi restituisce indicazioni su queste tipologie di dato rinvenute online:

Dal Dark-Web:
Cookies
Credentials
DB Records
JSON Files

Da fonti OSINT (Open Source Intelligence, ovvero "Intelligence da fonti aperte")
URLs
IPs
Domains
Typo domains
E-mails

TEC4I Cyber Risk Investigation

Scopri se i tuoi dati sono già nelle mani sbagliate tramite la **TEC4I CRI (Cybersecurity Risk Investigation).**

Come funziona
È un'**indagine** automatizzata **su web e dark web** per rilevare dati aziendali compromessi:

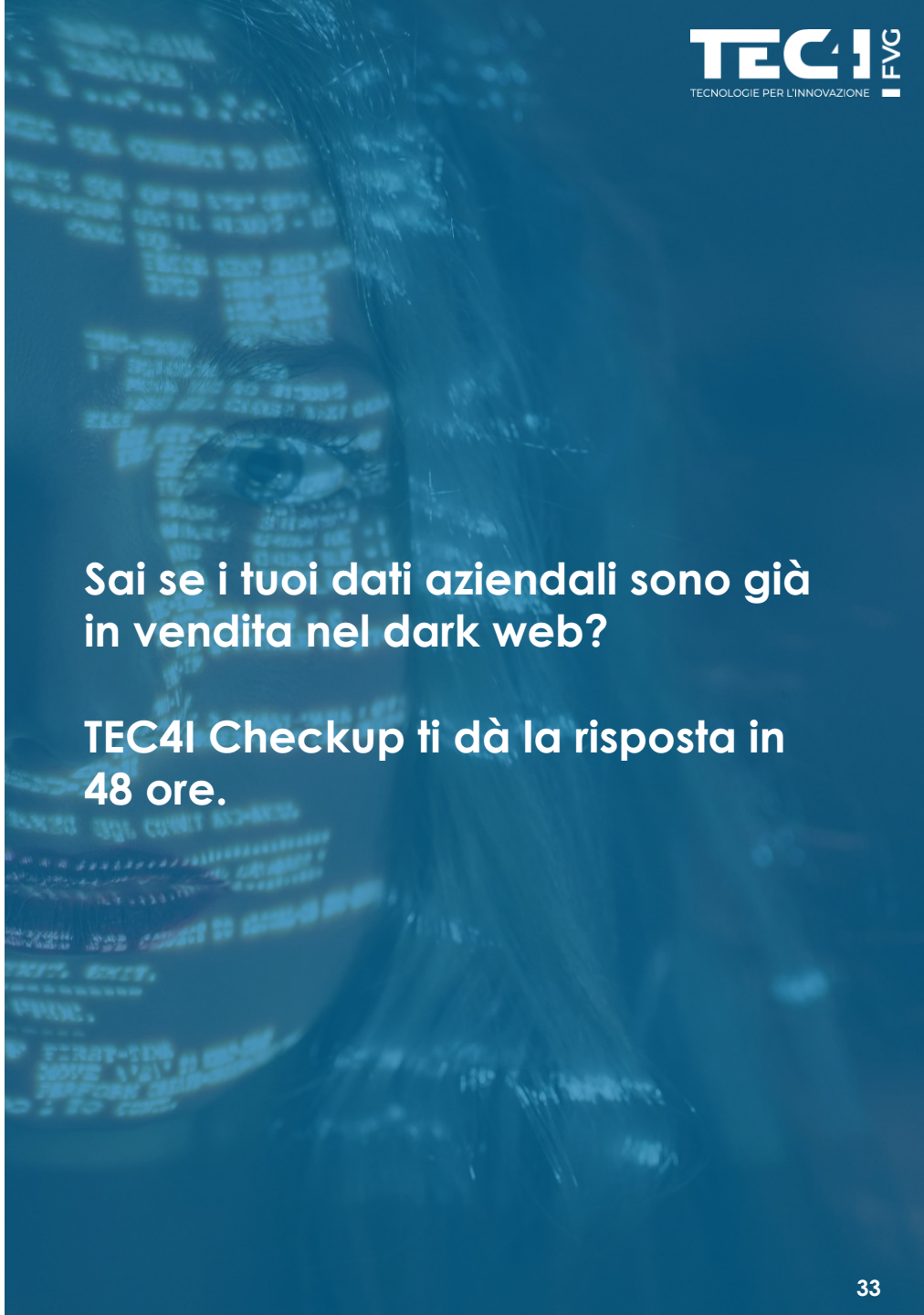
- Credenziali email/password rubate
- Vulnerabilità di siti e infrastrutture IT
- Informazioni esposte e punti di attacco

Output

- **Elenco** dei **dati compromessi** (email, IP, credenziali) e data di pubblicazione
- **Cybersecurity Risk Score** sintetico
- **Dettagli tecnici** e suggerimenti di **remediation**

Vantaggi

- **Mappatura chiara** delle informazioni esposte
- **Nessuna interruzione dei sistemi** durante l'analisi



Sai se i tuoi dati aziendali sono già in vendita nel dark web?

TEC4I Checkup ti dà la risposta in 48 ore.

Il progetto IP4FVG - EDIH

Progetto IP4FVG - EDIH (Industry Platform for Friuli Venezia Giulia EDIH), **finanziato** dall'Unione Europea - **Fondo NEXT Generation EU, M4C2 I2.3 PNRR**.

Finanziamento PNRR: oltre **4,4 milioni di euro**

Il progetto mira a **offrire nuovi servizi ad alto valore aggiunto alle imprese**, in particolare **PMI**, con **scontistiche fino al 100% del prezzo del servizio**.

Gli **obiettivi** principali sono:

- Migliorare le **competenze** digitali
- Accelerare l'**utilizzo** delle nuove tecnologie
- Incentivare l'adozione di **soluzioni** di Intelligenza Artificiale (AI), High Performance Computing (HPC) e **Cybersecurity** (CS)

IP4 FVG EDIH

Finanziato dall'Unione europea NextGenerationEU

Ministero delle Imprese e del Made in Italy

TEC4I Cybersecurity Checkup

Checkup completo sulla **vulnerabilità dei sistemi informatici** della tua azienda, composto da:

- Digital Maturity Assessment
- Extended Vulnerability Assessment
- Cyber Risk Investigation
- Remediation counseling

Prezzo del pacchetto: 6.830€

Condizioni agevolate grazie al **progetto IP4FVG-EDIH** - **scontistiche applicate sul prezzo** del servizio in base alla **dimensione aziendale:**

Micro-Piccola impresa Sconto: 100%	**Media impresa** Sconto: 86%	**Grande impresa** Sconto: 36%
0€	**933€**	**3.898€**

Finanziato dall'Unione europea NextGenerationEU
Ministero delle Imprese e del Made in Italy

Formazione

Digital skills - one day courses: brevi corsi di formazione (12 ore) definiti sulla base delle specifiche esigenze delle imprese riguardanti la trasformazione digitale aziendale - in collaborazione con il Consorzio Friuli Formazione, anche su tematiche inerenti la ***Cyberecurity Awareness***

Prezzo del servizio: 2.500€

Condizioni agevolate grazie al **progetto IP4FVG-EDIH** - **scontistiche applicate sul prezzo** del servizio in base alla **dimensione aziendale:**

Micro-Piccola impresa Sconto: 100%	**Media impresa** Sconto: 80%	**Grande impresa** Sconto: 50%
0€	**500€**	**1.250€**

Finanziato dall'Unione europea
NextGenerationEU

Ministero delle Imprese e del Made in Italy

D-ATA
Hub tecnologie digitali

Per maggiori informazioni potete contattare:

Tommaso Bernardini

tommaso.bernardini@tec4ifvg.it

T +39 0432 629 922

M +39 346 8843402

Loris Collina

loris.collina@tec4ifvg.it

T +39 0432 629 929

M +39 344 059 5293

data@tec4ifvg.it