Humans for Cybersecurity

NETGROUP

La Cybersecurity e le PMI

28 Giugno 2022

Campania DIH
Digital Innovation Hub
RETE CONFINDUSTRIA

meditech
COMPETENCE CENTER

Humans for Cybersecurity

Le problematiche Cyber

Il viaggio verso la Cybersecurity non ha come destinazione la tecnologia: quello è soltanto il punto di partenza.

Una importante vulnerabilità è rappresentata dal fattore umano che è sempre più l'oggetto degli attacchi cyber.

Il Capitale Umano

La strategia vincente è basata sulla **centralità dell'uomo**: alla meta si giunge con l'allineamento fra strategia d'impresa e strategia per la sicurezza IT, basata sulle reali competenze delle risorse umane.

Humans for Cybersecurity significa costruire conoscenza, consapevolezza e competenze nelle persone per prevenire, riconoscere e combattere le minacce cyber.

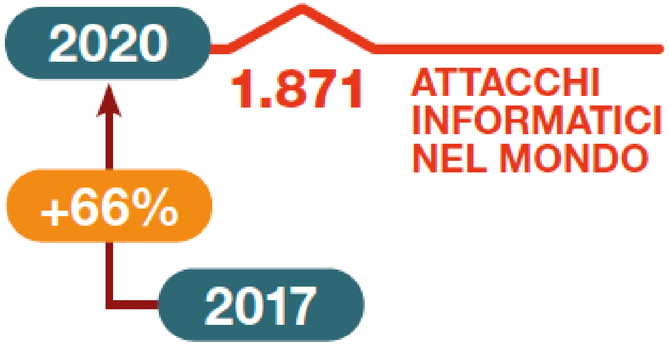
Trasformazione digitale e strategia per la sicurezza

Innovazione tecnologica per la competitività e la resilienza

Le misure previste dal PNRR traghetteranno il sistema Paese e le nostre PMI verso quella digitalizzazione essenziale ad affrontare le sfide del futuro.

Esposizione delle PMI al Cyber Crime

Diffusione di **Smart Working**, **Cloud**, **IoT**, estendono la superficie d'attacco ed aumentano sia il rischio legato alle infrastrutture tecnologiche che agli strumenti e servizi connessi, utilizzati da gran parte dei dipendenti delle aziende.



N° casi ad impatto sull'Industria: dal 7% nel 2020 al 18% nel 2021

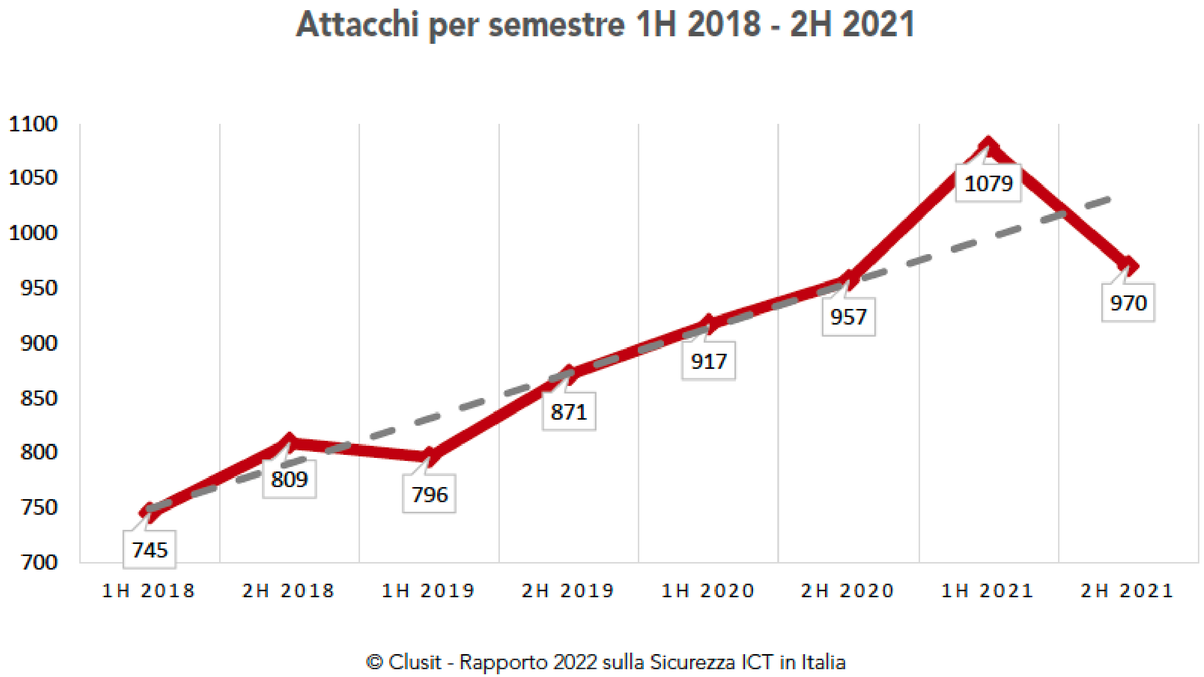
Security by Design

Non possiamo esimerci da una strategia per la progettazione di infrastrutture tecnologiche e servizi che tenga in debita considerazione i nuovi perimetri operativi e il rischio derivante dal fattore umano.

Contesto generale di riferimento

Rapporto Clusit

Dal rapporto ClusIT del 2022 sulla sicurezza dell'ICT in Italia, si rileva che **il 2021 è stato l'anno peggiore di sempre** evidenziando un **trend persistente di crescita degli attacchi**, della loro gravità e dei danni conseguenti.



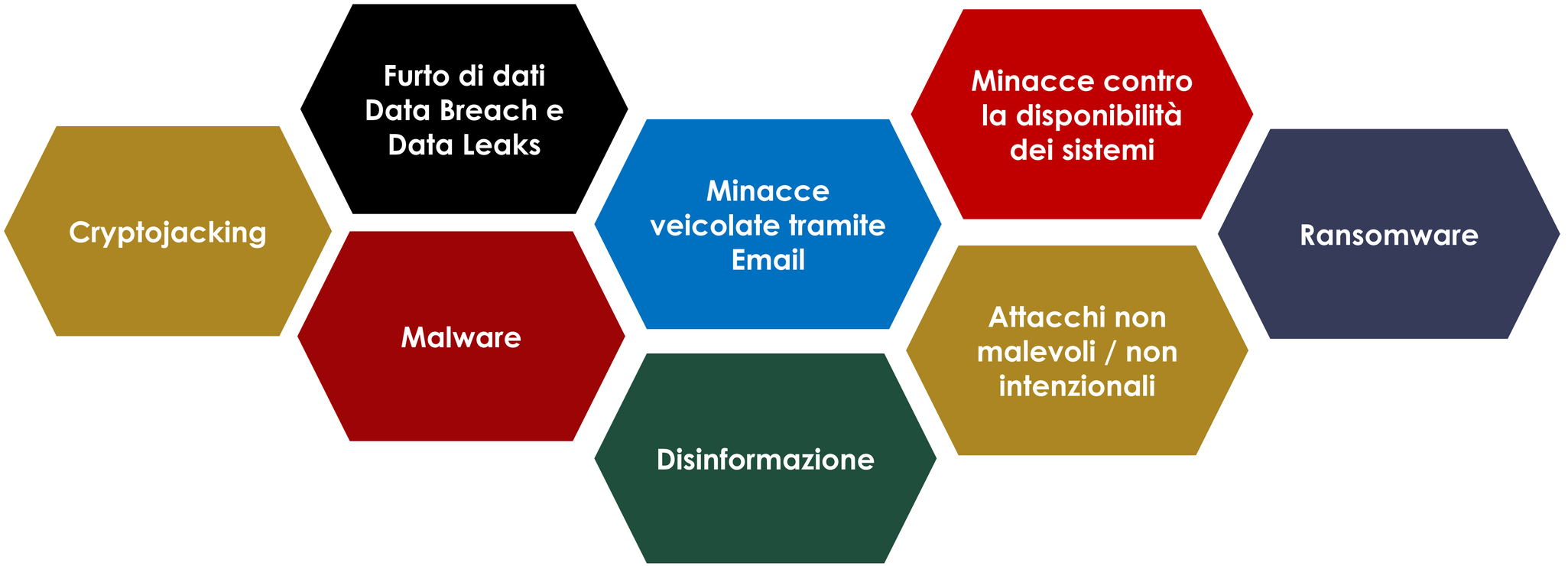
Attacchi gravi - 2021 vs 2020

- "Transportation / Storage" **+93,3%**,
- "Other Services" **+66,7%**,
- "News / Multimedia" **+60,5%**,
- "Wholesale / Retail" **+51,9%**,
- "Gov / Mil / LE" **+36,4%**,
- "Hospitability" **+36,4%**,
- "Professional / Scientific / Technical" **+26,2%,**
- "Healthcare" **+24,8%**.

Consapevolezza dei rischi

Gli attacchi in ambito tecnico, economico, etico

L'allargamento del perimetro digitale comporta l'aumento dei rischi cyber, sia quantitativi che qualitativi.



ENISA Threat Landscape 2021 – Le 8 macro-categorie di attacchi più frequenti

Unire intelligenza umana ed innovazione tecnologica

La Cybersecurity come sfida culturale

L'incremento dei livelli di cybersecurity passa dall'acquisizione della **consapevolezza del rischio**.

Occorre mettere in campo competenze specifiche, per garantire una costante sicurezza dei sistemi e dei dati.

Ogni innovazione digitale nasce dalle persone ed è rivolta alle persone

I nuovi mestieri

È necessario un numero importante di specialisti, che vanno creati per portare avanti il settore della cybersecurity, in continua espansione.

E vanno creati anche sfruttando modelli di apprendimento, di trasferimento tecnologico, tipici dei vecchi mestieri, affiancando **Senior Specialist** a giovani, ma anche non giovani, a **persone con talento** e con la volontà, la determinazione di voler imparare un nuovo mestiere.

L'approccio Humans for Cybersecurity

La strategia **Humans for Cybersecurity** è disegnata per accompagnare le PMI, fin dai primi passi, lungo il percorso della consapevolezza e della protezione cyber.

I punti di attenzione riguardano:

Esposizione dei Sistemi

Presenza di vulnerabilità sui sistemi del Cliente

Esposizione del Personale

Presenza di dati sfruttabili per attacchi di social engineering

Esposizione dei Dati

Presenza di dati aziendali utilizzabili per fini fraudolenti

L'analisi e la mitigazione avvengono mediante:

- servizi di **Weakness and Vulnerability Assessment**, per l'identificazione di eventuali debolezze architetturali e di possibili vulnerabilità di sicurezza;
- servizi di **Penetration Testing**, volti a verificare l'effettiva sfruttabilità delle vulnerabilità rilevate o per identificare debolezze e vulnerabilità specifiche dell'ambiente esaminato;
- attività di **Fixing**, **Re-check** e **Mitigazione** delle vulnerabilità riscontrate.

Monitoraggio costante e protezione dei dati

Humans for Cybersecurity

Una strategia di **cybersecurity efficace è un processo continuo** di controllo e riduzione del rischio, per tale motivo occorre attivare servizi di monitoring del rischio derivante dal fattore tecnologico e umano, mediante attività di:

- ***Preemptive Threat Intelligence*** – Raccolta informazioni sui possibili agenti di minaccia, nuove TTP e vulnerabilità 0-days;
- ***Data Breach Protection*** – monitoraggio costante del surface, deep e dark web alla ricerca di indicatori di data breach;
- ***Fraud Prevention*** – monitoraggio continuo del deep e dark web, per attuare reazioni rapide a schemi di frode;
- ***Brand Protection*** – identificazione dei casi di uso lesivo o non autorizzato del marchio, vendita merci contraffatte;
- ***Executive Protection*** – protezione della reputazione delle figure chiave al fine di intercettare contenuto lesivo.

Centrale nella strategia è anche la componente di **Security Awareness** per sensibilizzare le PMI su svariati aspetti della sicurezza delle informazioni, incrementando il livello di consapevolezza dei dipendenti, innalzando il livello di sicurezza dell'organizzazione e l'efficacia in termini di protezione dei dati aziendali critici e dei dati personali.

La certificazione delle professionalità

Humans for Cybersecurity

Humans for Cybersecurity è **creare un trust tra chi protegge e chi è protetto**, puntando fortemente sulla certificazione sia della competenza tecnica che dell'affidabilità della persona, nonché sul valore aggiunto per il sistema Paese dell'impiego di aziende, tecnologie e professionalità **made in Italy**.

ASFÁLEIA

Unire le forze – nessuno si salva da solo

se il nemico è subdolo, insidioso, potente, tanto maggiore deve essere il vigore dell'unione necessaria a fronteggiarlo.

Humans for...key takeaways

A fronte del notevole incremento delle minacce Cyber ed alla poca attenzione sui rischi che ne derivano per le PMI, nasce **Humans for Cybersecurity**.

Humans for Cybersecurity

- Sviluppo della cultura sulla cybersecurity
- Supporto nella protezione e nella creazione di nuove professionalità
- Modello trusted e centralizzato su fiducia ed italianità