Phishing
AI POWERED PROTECTION

THREAT AWARENESS

Human Firewall: trasformare ogni dipendente in una linea di difesa

Come costruire una cultura della sicurezza che riduce i rischi di attacco

A cura del team CENANT di GPI Cyberdefence

20 dicembre 2025 www.gpiphishing.com

THREAT AWARENESS

Come costruire una cultura della sicurezza che riduce i rischi di attacco

01 Il paradosso del fattore umano

Quando le aziende pensano alla cybersecurity, la riflessione cade quasi sempre sulla tecnologia: firewall di nuova generazione, sistemi di crittografia avanzata, piattaforme di endpoint detection. Eppure, secondo il Proofpoint Human Factor Report, il 95% degli attacchi informatici sfrutta errori umani. La tecnologia da sola non basta.[1]

L'essere umano è contemporaneamente l'anello più debole e la risorsa più preziosa nella catena della sicurezza. Una persona distratta che clicca su un link malevolo può vanificare anni di investimenti tecnologici. Lo stesso dipendente, se adeguatamente formato, può bloccare sul nascere attacchi che nessun software avrebbe intercettato.

02 Cos'è l'Human Firewall

Il termine *Human Firewall* descrive l'insieme di comportamenti, competenze e procedure che trasformano ogni persona dell'organizzazione in un presidio attivo di sicurezza. Non si tratta di un corso obbligatorio da seguire una volta all'anno: è un approccio culturale e organizzativo che richiede formazione continua, consapevolezza costante e procedure chiare.

Immaginate un'azienda con mille dipendenti, ognuno collegato alla rete interna. Se anche solo uno di loro, per disattenzione, aprisse un'e-mail malevola, potrebbe innescare un attacco ransomware capace di bloccare l'intera infrastruttura per settimane, come è accaduto, tra gli altri, alla Regione Lazio nel 2021.

RIFERIMENTI

1 Proofpoint Human Factor Report (2022).
2 IBM Cyber Resilient Organization Report (2023).
3 Proofpoint, Voice of the CISO — Report annuale (2024).
4 GPI Cyberdefence, analisi multicaso (2025).
5 FBI Internet Crime Report (2023).
6 Google Security Blog.

03 I quattro pilastri su cui costruire

Formazione continua e simulazioni pratiche. Non basta spiegare cosa sia il phishing: occorre mostrarlo. Le aziende che combinano corsi periodici con simulazioni di attacco reale (e-mail-trappola, test di risposta) riducono il tasso di click su e-mail di phishing dal 20-30% iniziale fino al 4-5% dopo dodici mesi.[4]

Regole chiare e semplici. Le policy di sicurezza devono essere comprensibili a tutti i livelli aziendali. Una regola incompresa non viene seguita. Linee guida su gestione delle password, segnalazione di anomalie e verifica delle richieste finanziarie devono essere pratiche e accessibili.

Cultura della segnalazione. Ogni persona deve sentirsi responsabilizzata, e non giudicata, quando segnala un'e-mail sospetta o un comportamento anomalo. La tempestività di una segnalazione può impedire che un attacco si propaghi.

Coinvolgimento del vertice. NIS2 e DORA richiedono esplicitamente il coinvolgimento del CDA e del top management. La sicurezza non può essere delegata solo all'IT: deve essere una priorità condivisa ai massimi livelli.

> *Le aziende con dipendenti ben formati impiegano il 27% di tempo in meno per identificare e rispondere a una violazione di sicurezza rispetto a quelle prive di un programma strutturato (IBM Cyber Resilient Organization Report).*

RIFERIMENTI

1 Proofpoint Human Factor Report (2022).
2 IBM Cyber Resilient Organization Report (2023).
3 Proofpoint, Voice of the CISO — Report annuale (2024).
4 GPI Cyberdefence, analisi multicaso (2025).
5 FBI Internet Crime Report (2023).
6 Google Security Blog.

04 Da dove iniziare

Investire sull'Human Firewall non è un costo: è la difesa con il miglior rapporto costo-efficacia disponibile oggi.

Il primo passo è una valutazione onesta dello stato attuale: quanti dipendenti sanno riconoscere un'e-mail di spear phishing? Quanti conoscono la procedura aziendale in caso di incidente? Una baseline chiara consente di misurare i progressi nel tempo e di dimostrare il valore degli investimenti in formazione, un argomento sempre più rilevante anche per i board aziendali.

RIFERIMENTI

1 Proofpoint Human Factor Report (2022).
2 IBM Cyber Resilient Organization Report (2023).
3 Proofpoint, Voice of the CISO — Report annuale (2024).
4 GPI Cyberdefence, analisi multicaso (2025).
5 FBI Internet Crime Report (2023).
6 Google Security Blog.

GPI PHISHING — CYBERSECURITY PLATFORM

Trasforma ogni dipendente in una linea di difesa attiva

Simulazioni reali, formazione continua e misurazione del rischio per costruire il tuo Human Firewall.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com

© 2026 GPI Cyberdefence S.r.l. — Tutti i diritti riservati.