MalpensaNews

Cyber risk, basta un errore umano per fermare un’azienda

Michele Mancino · Tuesday, February 10th, 2026

Un piccolo dispositivo, grande quanto una chiavetta Usb. Un cavo apparentemente innocuo. Durante la presentazione del **Cyber Index PMI Lombardia**, organizzata da **Confindustria Varese** con **Generali**, un esperto del team Cyber security specialist Generali global corporate & commercial, mostra al pubblico un piccolo congegno chiamato **Flipper Zero**. Collegato a un PC tramite porta Usb, viene riconosciuto come una **tastiera fidata e può digitare automaticamente script velocissimi** per rubare password, installare malware o creare backdoor per accessi remoti futuri. In pochi secondi il danno (simulato) è fatto. «Non c’è nulla come un esempio pratico per far percepire la vulnerabilità di un sistema. Oggi questo dispositivo è contenuto in un semplice cavetto» spiega **Giovanni Peduto**.

IL FATTORE UMANO È DETERMINANTE

L’esperimento rende immediato uno dei messaggi centrali emersi dal confronto. È vero che le tecnologie di difesa evolvono, ma l’ingresso degli attacchi passa ancora molto spesso dai **comportamenti delle persone**. Password deboli, clic impulsivi, uso improprio degli strumenti digitali continuano a rappresentare la prima vulnerabilità, anche nelle aziende più strutturate.

LA CYBERSICUREZZA È UN RISCHIO DI IMPRESA

È in questo contesto che si collocano i dati del **Rapporto cyber index PMI Lombardia**. Il campione Nord-Ovest analizzato comprende **251 imprese** tra Lombardia, Piemonte, Liguria e Valle d’Aosta. Le aziende lombarde mostrano livelli di **maturità superiori alla media dell’area,** ma anche una maggiore esposizione agli attacchi. Il **36% dichiara di averne subiti negli ultimi tre anni**, contro il 29% del Nord-Ovest, un dato in crescita rispetto alle precedenti rilevazioni. Una dinamica che riflette la struttura del tessuto produttivo, come sottolinea Silvia Pagani, direttore di Confindustria Varese: «La crescente interconnessione di imprese, macchinari e dati lungo la filiera aumenta produttività e competitività, ma amplia anche la superficie di attacco. Per questo la **cybersicurezza** non è più solo un tema tecnico, **è un vero rischio d’impresa**».

LA SUFFICIENZA

L’indice sintetico complessivo si attesta a **61/100**, una sufficienza che nasconde forti differenze interne. L’approccio strategico è il pilastro più maturo, segno di una maggiore attenzione del management. **Più critiche invece le aree di identificazione e attuazione**: se il 78% delle imprese mappa i propri asset informatici e il 54% svolge audit di sicurezza, **solo il 44% dispone di un piano di ripristino**. Quasi la metà delle aziende lombarde resta sotto il livello 60 di maturità.

Sul piano strategico interviene **Barbara Lucini**, responsabile country sustainability & social responsibility di Generali Italia, sottolinra che: «Il Cyber Index PMI mostra segnali incoraggianti in Lombardia, ma conferma la **necessità di continuare a investire in consapevolezza e prevenzione**. La cyber sicurezza è una responsabilità condivisa e una leva strategica per la competitività e la resilienza del Paese».

TRA IL DIRE E IL FARE C'È DI MEZZO L'HACKER

Il quadro è rafforzato dal sondaggio istantaneo svolto in sala e commentato da **Alessandro Piva**, direttore dell'**Osservatorio Cybersecurity & Data Protection del Politecnico di Milano**. Dalle risposte emerge un divario ancora marcato tra **consapevolezza strategica e capacità di attuazione concreta** delle misure di sicurezza, con difficoltà legate soprattutto alla complessità della materia e alla carenza di risorse dedicate. Dal punto di vista istituzionale, **Emilio Tucci**, vice capo della Divisione Programmazione, investimenti e coordinamento dell'A**genzia per la Cybersicurezza Nazionale**, richiama il tema della consapevolezza: «È ancora uno dei principali fattori di debolezza», nonostante bandi, strumenti e infrastrutture siano disponibili. A questo si affianca l'intervento di **Valentina Lo Voi**, che ribadisce come «**il fattore umano resti la prima vulnerabilità**» e come la formazione non sia un costo, ma un investimento necessario.

IL RISCHIO CYBER È UN TEMA DI BUSINESS

Accanto alle istituzioni, emerge la voce del territorio. **Giuseppe Zanolini,** presidente del Gruppo Terziario Avanzato di **Confindustria Varese,** osserva: «Per anni la sicurezza informatica è stata considerata un tema tecnico, delegato all'IT. **Oggi è un tema** di **business** che riguarda il management e tutta l'organizzazione». In imprese sempre più aperte e interconnesse, aggiunge, «basta il comportamento sbagliato di una sola persona per esporre l'intera azienda».

LA SICUREZZA È PARTE DELLA SOSTENIBILITÀ

Sul piano operativo, **Pierluigi Petrali**, direttore del **Digital innovation hub Lombardia,** richiama l'importanza degli **assessment**: «La prima leva concreta è trasformare la consapevolezza implicita in **consapevolezza esplicita**. Mettere nero su bianco la **postura di sicurezza dell'azienda è il punto di partenza**».
Un passaggio che riguarda anche la sostenibilità: «Un'impresa che non governa **il rischio cyber mette a rischio la propria continuità nel tempo**. La sicurezza oggi è parte integrante della sostenibilità aziendale».
A completare il quadro è il punto di vista assicurativo. **Daniele Melchiori**, cyber & it insurance hub di Generali Italia, porta casi reali in cui «è bastata una password mai cambiata per anni» per bloccare intere aziende. Episodi che confermano come, al di là delle tecnologie, il fattore umano resti l'elemento decisivo nella maggior parte degli attacchi.

This entry was posted on Tuesday, February 10th, 2026 at 4:19 am and is filed under Economia, Scienza e Tecnologia
You can follow any responses to this entry through the Comments (RSS) feed. You can skip to the end and leave a response. Pinging is currently not allowed.