Data: 23.11.2017

GIORNALE del POPOLO
Quotidiano della Svizzera italiana

Giornale del Popolo
6903 Lugano
091/ 922 38 00
www.gdp.ch/

Genere di media: Stampa
Tipo di media: Quotidiani e settimanali
Tiratura: 10'658
Periodicità: 6x/settimana

Pagina: 4
Superficie: 39'535 mm²

Scuola universitaria professionale della Svizzera italiana
SUPSI

Ordine: 1083235
Tema n°: 375.034

Riferimento: 67543069
Clipping Pagina: 1/2

I risultati di un'indagine organizzata dalla Camera di commercio

Cyber-sicurezza in azienda «È ora di essere hacker»

di **MARTINA SALVINI**

La realtà ticinese può decisamente fare di più in materia, investendo non solo nei macchinari ma anche nel personale.

Serve un deciso cambio di marcia in materia di sicurezza cibernetica per imparare ad agire come un vero hacker. Eccessivo? Non proprio, se si pensa che nel nostro Cantone circa la metà delle aziende non è adeguatamente preparata di fronte a un attacco massiccio – e molto doloroso – come potrebbe essere quello che arriva dal web. La conferma arriva da un'inchiesta condotta dalla Camera di commercio, in collaborazione con la SUPSI, che ha visto protagoniste 30 realtà aziendali (del pubblico, multinazionali, fiduciarie, banche).

Un tema di grande attualità, come ha evidenziato il direttore della Camera di commercio **Luca Albertoni**, ancor più perché è in atto una revisione della Legge svizzera sul tema della protezione dei dati. Stando ai risultati presentati ieri, infatti, di fronte ai cyber attacchi, un quarto delle aziende intervistate non ha risorse dedicate e almeno un terzo non si rifà alle normative previste.

Ma c'è di più perché troppo spesso il tema della "cybersecurity" passa addirittura in secondo ordine ai piani alti delle aziende. Risultato? Il 20% ha già subito un danno, che non è solo economico – l'interruzione del servizio erogato o peggio a un furto di dati – ma pure di immagine. Con conseguenze che si dilatano nel tempo e che possono produrre pericolosi effetti "emotivi" sui collaboratori. Un senso di timore diffuso che finisce per rallentare l'intera catena produttiva della realtà aziendale, ha spiegato **Alessandro Trivilini**, responsabile del Servizio informatica forense del Dipartimento tecnologie innovative della SUPSI. Sì perché il problema degli attacchi informatici (ne abbiamo parlato il 17 novembre su queste pagine, ndr) è che possono restare silenti molto a lungo. L'azienda pensa di poter essere tranquilla, ma poi viene smentita. E oggi troppo pochi dipendenti sanno esattamente come intervenire e che comportamento adottare di fronte agli effetti potenzialmente catastrofici di un attacco informatico. Ecco perché – ha spiegato Trivilini – occorre una metamorfosi culturale. Un cambio di rotta quanto mai necessario visti i 700 attacchi al giorno nel mondo

Data: 23.11.2017

GIORNALE del POPOLO
Quotidiano della Svizzera italiana

Giornale del Popolo
6903 Lugano
091/ 922 38 00
www.gdp.ch/

Genere di media: Stampa
Tipo di media: Quotidiani e settimanali
Tiratura: 10'658
Periodicità: 6x/settimana

Pagina: 4
Superficie: 39'535 mm²

Scuola universitaria professionale della Svizzera italiana
SUPSI

Ordine: 1083235
Tema n°: 375.034

Riferimento: 67543069
Clipping Pagina: 2/2

(come quello avvenuto proprio ieri ai danni di Uber, costato il furto di dati di circa 57 milioni di utenti). Soluzione? Sarebbe bene «implementare delle misure tecniche e organizzative adeguate, in grado cioè di assicurare un livello di sicurezza appropriato al rischio», è stato evidenziato.

Alcune proposte in questa direzione sono state avanzate da **Paolo Lezzi,** CEO e fondatore di TheCyber SA, che ha collaborato all'indagine. Tra i suggerimenti snocciolati c'è quello di effettuare un vero test del reale livello di protezione da minacce avanzate e implementare il grado di monitoraggio della minaccia, prestando attenzione all'organizzazione interna. Il rischio cyber – ha spiegato Lezzi – «non viene rilevato e mappato nella sua interezza, e questo nonostante vi siano dei regolamenti che sempre più lo impongono». Ma un problema riguarda anche gli investimenti, che si concentrano sulle tecnologie trascurando invece l'organizzazione interna, la preparazione dei dipendenti. «È necessario investire sulla formazione», ha quindi chiosato Albertoni, spiegando pure il fine ultimo dell'inchiesta: approfondire il tema e imprimere una svolta al modello di business, affinché possa beneficiarne tutto il tessuto economico ticinese.