Data: 23.11.2017

laRegione Ticino

La Regione Ticino
6500 Bellinzona
091/ 821 11 21
www.laregione.ch

Genere di media: Stampa
Tipo di media: Quotidiani e settimanali
Tiratura: 32'386
Periodicità: 6x/settimana

Pagina: 6
Superficie: 44'001 mm²

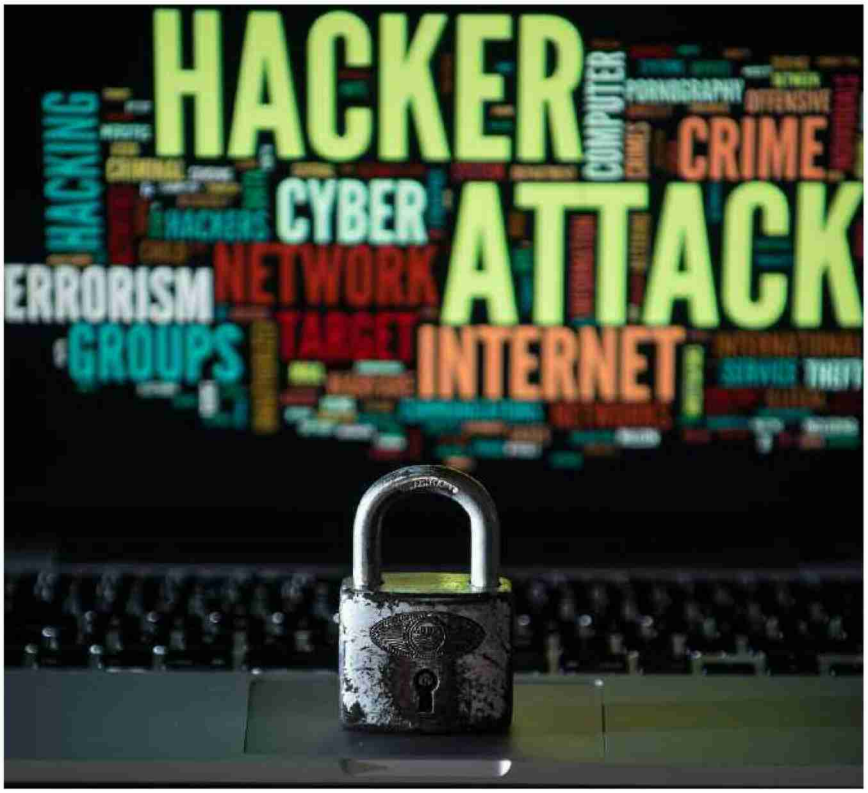
Scuola universitaria professionale della Svizzera italiana
SUPSI

Ordine: 1083235
Tema n°: 375.034

Riferimento: 67541900
Clipping Pagina: 1/2

Spesso le aziende ticinesi non hanno consapevolezza dei pericoli informatici

Quei rischi sottovalutati



La sicurezza dovrebbe venire prima di tutto TI-PRESS

di Generoso Chiaradonna

Un'analisi della Camera di commercio mette in evidenza la vulnerabilità dei sistemi cibernetici. Ma la chiave è sempre il fattore umano.

È l'inconsapevolezza il vero nemico di cittadini e aziende. Quando si parla di Cyber risk, per esempio, non si conoscono o si sottovalutano i rischi e quindi si è inevitabilmente vulnerabili. Nelle imprese ticinesi, stando a un'analisi effettuata dalla società InTheCyber e Supsi per conto della Camera di commercio, non sempre questi rischi sono tenuti in considerazione. Una scarsa diffusione dell'analisi di questi rischi e una limitata capacità di analisi dei danni economici che ne possono derivare sono di fatto delle alleate dei 'criminali informatici'.

Eppure negli ultimi anni è cresciuta l'attenzione verso i rischi informatici, anche perché la tecnologia è sempre più protagonista di ogni attività lavorativa, esponendo di fatto le aziende a maggiori pericoli, primo fra tutti l'interruzione del servizio, ma anche la perdita di dati sensibili o il rischio reputazionale. E gli attacchi informatici sono ormai all'ordine del giorno, fra malware, phishing e sfruttamenti della vulnerabilità della rete.

«C'è bisogno di un cambio di mentalità sia da parte degli imprenditori e dirigenti, sia da parte di chi si trova al fronte», spiega Alessandro Trivilini, responsabile del Servizio di informatica forense del Dipartimento tecnologie innovative della Supsi. «Dobbiamo pensare come un hacker per cercare di capire quali sono le vulnerabilità del nostro sistema», continua Trivilini.

Spesso, infatti, è un errore umano e non una falla di sistema la chiave d'entrata

Data: 23.11.2017

laRegione Ticino
IL GIORNALE DELLA SVIZZERA ITALIANA

La Regione Ticino
6500 Bellinzona
091/ 821 11 21
www.laregione.ch

Genere di media: Stampa
Tipo di media: Quotidiani e settimanali
Tiratura: 32'386
Periodicità: 6x/settimana


Vitol minaccia di lasciare Ginevra
Quei rischi sottovalutati

Pagina: 6
Superficie: 44'001 mm²

Scuola universitaria professionale della Svizzera italiana
SUPSI

Ordine: 1083235
Tema n°: 375.034

Riferimento: 67541900
Clipping Pagina: 2/2

utilizzata dai Cyber criminali. Scaricare un allegato di posta elettronica oppure dare inconsapevolmente delle informazioni sensibili a quella persona che si cela – via social o e-mail – dietro un nome amico e familiare. «Il fattore umano è determinante per un incidente informatico perché è altamente prevedibile», continua l'esperto della Supsi. Eppure delle 36 aziende intervistate rappresentative di banche, fiduciarie, multinazionali e istituzioni pubbliche o parapubbliche, ben il 71% ha subito un tentativo di phishing (furto di dati) e il 53% di ransomware (ricatti informatici) negli ultimi 24 mesi. «Ma quello che più colpisce è che la metà degli intervistati tende a privilegiare il proprio business rispetto alla sicurezza», spiega invece Paolo Lezzi, Ceo e fondatore di InTheCyber. Quindi, nonostante l'enfasi che quasi quotidianamente viene posta sui vari malware (WannaCry, eccetera) che colpiscono aziende molto note, c'è una sorta di fatalismo da parte delle imprese ticinesi. Eppure – continua Lezzi – basterebbero pochi accorgimenti tecnici e una buona informazione presso i propri collaboratori per evitare tanti episodi spiacevoli che costano tempo e denaro.

Sorprende il caso di Uber

I dati di 57 milioni di clienti di Uber sono stati piratati, ma la multinazionale per il trasporto privato lo ha tenuto nascosto per un anno preferendo pagare un riscatto, ben 100mila dollari, agli hacker che avevano piratato nomi, e-mail, numeri di telefono di 50 milioni di clienti e 7 milioni di autisti. I dati sono stati poi distrutti. Se anche i colossi tecnologici sono vulnerabili, figuriamoci una Pmi. «Non è questione di dimensione – spiega Trivilini – ma di cultura della prevenzione che è sempre di natura umana».