UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO
Sezione:ECONOMIA ITALIANA ED INTERNA...

SOLE 24 ORE
Dir. Resp.:Fabio Tamburini
Tiratura: 173.364 Diffusione: 131.844 Lettori: 744.000

Edizione del:31/01/19
Estratto da pag.:1,10
Foglio:1/2

Imprese digitali
Aziende sotto scacco e truffe È allarme cyberspionaggio

Allarme cyberspionaggio. È la nuova emergenza che imprese e pa devono fronteggiare e gestire insieme a manipolazione dell'opinione pubblica e truffe.

—a pagina 10

Aziende sotto scacco e truffe È allarme cyberspionaggio

ECONOMIA DIGITALE
In crescita esponenziale il numero degli attacchi: nel mirino i dati sensibili

Investimenti per 1,2 miliardi ma solo una Pmi su due spende per la propria difesa

Enrico Netti

Allarme cyberspionaggio. È questa la nuova emergenza che imprese e amministrazioni pubbliche e private si trovano a dovere fronteggiare e gestire insieme a truffe, manipolazione dell'opinione pubblica perché le elezioni europee sono ormai prossime, per finire con il blocco e il "sequestro" di impianti e linee produttive smart e quant'altro rientra nell'internet delle cose. Queste le nuove minacce per il prossimo triennio secondo l'ultima edizione dell'Osservatorio «Information security & privacy» della School of management del Politecnico di Milano che verrà presentato il prossimo 5 febbraio durante il convegno «Winter is coming: adapt to react!» e Il Sole 24 Ore è in grado di anticipare.

Un primo elemento è l'aumento esponenziale dei cyberattacchi a cui le aziende italiane faticano a rispondere considerando la rapida evoluzione delle offensive online. Cresce il valore del mercato italiano delle soluzioni di information security e privacy che lo scorso anno ha raggiunto i 1,2 miliardi (+9% sul 2017). In realtà i big spender sono soprattutto le grandi aziende responsabili dei tre quarti degli investimenti mentre lo scorso anno il volano degli investimenti è stato l'adeguamento al Gdpr.

«L'aumento dell'attività di spionaggio rende evidente come sia sempre più frequente il rischio di imbattersi in cyber criminali che mirano a impossessarsi di elementi di proprietà intellettuale e industriale, fattori di vantaggio competitivo - spiega Gabriele Faggioli, responsabile scientifico dell'Osservatorio -. Le informazioni rubate si possono rivendere sui mercati, usare in quelli azionari, per avere ritorni economici». Quasi sempre gli hacker trovano poi un insospettabile alleato nel comportamento dei dipendenti e nei sistemi ict obsoleti o non aggioranti. Così la serie di reati compiuti spazia dalle truffe, 83% dei casi, alle estorsioni (78%), gli attacchi a fine di spionaggio (46%), le interruzioni di servizio (36%). È solo questione di tempo e aumenterà il livello di sofisticazione degli attacchi: i bersagli saranno i dispositivi mobili, dagli smartphone all'ecosistema dell'internet delle cose oltre alle grandi infrastrutture critiche di luce, acqua, gas e tlc, gli edifici smart e i veicoli connessi.

Sulle scelte delle aziende continua inoltre a pesare il percorso di adeguamento al Gdpr che continua ad assorbire buona parte dei budget. È altro fronte caldo perché le informazioni chiave dei clienti rappresentano un ricco bottino: secondo le stime della Polizia postale questi dati del signor Rossi sul mercato illegale valgono da 2 a 18 euro. «Il ritorno economico di queste azioni è di tale portata che i cybercriminali hanno tutto l'interesse a perseguirli - aggiunge Alessandro Piva, direttore dell'Osservatorio -. Le aziende devono adeguare i sistemi di sicurezza e quando si tratta di proprietà industriale, intellettuale o informazioni sensibili devono concentrare gli investimenti». In ambito indu-


Aziende sotto scacco e truffe È allarme cyberspionaggio
10 NOMINATION AI PREMI OSCAR
LA FAVORITA

Peso:1-1%,10-23%

striale tra le criticità c'è la mancanza di consapevolezza verso questi rischi mentre tra un campione di Pmi solo una su due agisce sul fronte della cybersicurezza. Insomma non hanno difese sul fronte cyberspionaggio. «L'80% delle realtà europee è potenzialmente vulnerabile a questa minaccia ed il 70% non dispone di una capacità continuativa di detection & response avanzata in grado di rilevare "presenze" ostili - avverte Paolo Lezzi, Ceo di Inthecyber, organizzazione leader nella cyber defense e nell'intelligence -. Inoltre è necessario trovare un canale legale e istituzionale per perseguire e neutralizzare queste minacce».

enrico.netti@ilsole24ore.com

Offensiva. La proprietà intellettuale e le informazioni sensibili delle aziende sono il nuovo bottino degli hacker