Grandi aziende italiane nel mirino degli hacker

Enrico Netti


IMPRESA&TERRITORI

Gli investimenti verso l'Africa fanno scalo negli Emirati Arabi

Grandi aziende italiane nel mirino degli hacker

Nel 2017 speso poco più di un miliardo per la difesa

I furbi delle fake news mirano a spot e traffico

La frode corre sul cambio di Iban

LEONARDO DA VINCI

L'ANTICIPO

Hacker all' attacco con ransomware, massive phishing e spear phising. Sono queste le più comuni tipologie di tentativi che hanno colpito le grandi società italiane nel 2016. Offensive che negli ultimi tempi hanno avuto una recrudescenza: quasi i due terzi delle società tra il 2015 e il 2017 hanno registrato un aumento dell' attività di intrusione. Tra aziende ed enti pubblici l' 81% dichiara di avere subito attacchi nel corso dell' ultimo anno ma solo un terzo ritiene di disporre di competenze e capacità tecniche in grado di rilevare le intrusioni. Infatti gli hacker più abili una volta penetrati nei computer preferiscono mantenere una presenza occulta, intrufolandosi negli archivi alla ricerca del colpo grosso. E ci sono aziende, come si è visto con il caso Uber esploso in tutta la sua rilevanza la scorsa settimana, che nascondono per mesi ad autorità e clienti le violazioni. I dati sensibili di oltre 57 milioni di persone tra autisti e clienti Uber sono stati rubati nell' ottobre 2016 e solo la scorsa settimana la società Usa ha ammesso il fatto con l' aggravante di avere pagato 100mila dollari agli autori per tenere nascosto il furto. Indiretta conferma di come nemmeno le multinazionali digitali adottino difese efficaci. È quanto rivela il «Barometro cyber security 2017» realizzato da Inthecyber, l' European center for advanced cyber security (Eucacs) e Netconsulting 3 con il patrocinio, tra gli altri, della Presidenza del Consiglio dei ministri, che sarà presentato domani a Milano. Ne emerge un quadro sconfortante, a conferma di come la sicurezza non sia affrontata in modo adeguato dalle grandi aziende quotate che compongono il panel del Barometro. Sempre più spesso le porte d' ingresso usate dagli hacker sono i social e gli smartphone, che si aggiungono alle mail. «Il 90% delle aziende italiane può subire una violazione dei dati e lo spionaggio industriale continuativo - commenta Paolo Lezzi, executive vice president Eucacs e chairman della conferenza -. È migliorata la protezione dei pc ma non la capacità complessiva di identificazione degli attacchi soprattutto di tipo targettizato e sofisticato». Ecco un deficit in quello che dovrebbe essere un

processo strutturato di verifiche ed esercitazioni che attestino costantemente il livello di tenuta dei sistemi Ict. I danni causati dai "soliti ignoti" riguardano il furto di brevetti e dati sensibili e strategici, quelli reputazionali, la caduta dei ricavi. Se il rischio di attacchi e furti di dati cresce, lo stesso non si può dire per i budget a difesa dei sistemi business critical. Gabriele Faggioli, responsabile scientifico dell' Osservatorio information security & privacy del Politecnico di Milano, parla di sotto-investimenti alla luce dei 972 milioni spesi nel 2016 che, secondo una stima, quest' anno diventeranno 1,05 miliardi (+5%). Non molto: e così Lezzi suggerisce al governo di privilegiare, anche in un' ottica di Industria 4.0, gli sgravi per le aziende che investono in servizi continuativi di auditing, simulazione di attacco, monitoraggio, intelligence e formazione. Per ora quasi un' azienda su due segue uno standard internazionale di riferimento come l' Iso 27001 e poco più di un terzo partecipa a programmi e progetti per condividere le informazioni sulle minacce informatiche subite. C' è poi un altro tipo di deficit: quello degli esperti in cyber sicurezza. «Dobbiamo investire pesantemente e costantemente per la formazione del personale a tutti i livelli» aggiunge Umberto Gori, direttore scientifico della conferenza. Le grandi imprese inoltre trascurano di assicurarsi su questi rischi. «L' Italia è un mercato ancora giovane per la copertura da rischi cyber e meno del 5% delle aziende medio-grandi ha già acquistato una polizza per questi rischi, e tra le quotate italiane siamo a circa il 15% -spiega Andrea Bono, General Manager di Marsh Italia -. Il volume dei premi intermediati per questa copertura oggi è di circa 15-20 milioni ma prevediamo che nel 2020 si supereranno i cento ». enrico.netti@ilsole24ore.com