CORRIERE DELLA SERA

Data 19-03-2017
Pagina
Foglio 1 / 2

PROFESSIONE HACKER: I PIRATI ORA SONO ASSUNTI DALLE AZIENDE

Sempre più richiesti dal mercato per la difesa dagli attacchi informatici, riferiscono direttamente ai vertici Tra le professioni in crisi non c'è quella degli hacker: oggi sono diventati forse un po' più «borghesi» come Raoul Chiesa, il più famoso ex pirata informatico italiano che fa il consulente insieme ad altri hacker come Carlo De Micheli con la società Security Brokers. Qualcuno mette anche la cravatta in azienda e compare negli organigrammi aziendali alla voce di Responsabile security o Chief information officer. Quelli della nuova generazione come Gianluca Varisco, appena assunto nel team digitale di Palazzo Chigi da Diego Piacentini, non amano poi la parola hacker come «tag» della propria professione. Ma il curriculum parla abbastanza chiaro: come racconta lo stesso Varisco si è occupato di «soluzioni di cifratura per telefonia fissa e mobile», prima di andare a vivere a Berlino dove era specializzato in «sicurezza e infrastruttura per conto di Rocket Internet», grande gruppo tedesco quotato (lo stesso che controlla società come Foodora). D'altra parte la presa di distanza dal termine «hacker» è anche una strategia nei colloqui di lavoro perché alcune società, come Vodafone, non li assumono per politica aziendale. Avrebbero il vizio di portarsi via i segreti aziendali dopo un po'. Una professione in crescita Se il termine non va sempre di moda la sostanza non cambia: servono. E con la diffusione dell'Internet delle cose, delle auto a guida assistita, degli oggetti casalinghi che sono dei Piccoli fratelli la dipendenza non potrà che aumentare. In rete esistono anche delle piattaforme specializzate per assumerli come www.hireandhack.com anche se non è mai chiaro per chi lavorino in definitiva. «È vero che in altri Paesi sono partiti prima di noi — sintetizza Stefano Grassi, capo della Security di Tim — Germania e Gran Bretagna si sono attrezzati con brigate di migliaia di hacker già da un lustro se non di più, ma ora ci siamo anche noi». In Gran Bretagna la sicurezza informatica è un'industria super specializzata da 58 mila posti di lavoro. E l'offerta di lavoro cresce tanto che da settembre alcune scuole selezionate introdurranno 4 ore settimanali di hacking per 5.700 ragazzi di 14 anni. Si tratta di un test che durerà 5 anni finalizzato proprio a difendere il Paese. Anche in Italia questa offerta non potrà che crescere: lo dicono i numeri degli attacchi. Negli ambienti delle cyber intrusioni gira una battuta: «Se qualcuno vi parla di sicurezza informatica allora vuole dire che non si è nemmeno accorto che gli sono entrati in casa». Migliaia di attacchi Solo la rete Telecom subisce migliaia di attacchi ogni anno. I più pericolosi, i cosiddetti Ddos, sono cresciuti del 19% e l'infrastruttura principale di accesso a Internet in Italia è chiaramente un buon parametro di cosa accade anche fuori. «Noi subiamo decine se non centinaia di intrusioni al giorno anche se quello che conta è quanti di questi arrivino poi ad avere un'efficacia. Nel 2016 ce n'è stato solo uno veramente importante» racconta Massimiliano Gerli, chief information officer di Amplifon. Cosa c'entra Amplifon? «Cercano i dati sensibili dei nostri clienti e dei nostri dipendenti». D'altra parte affittare uno di questi software costa 5 dollari. Provare per credere su quantumbooter.net. C'è anche una prova gratuita per 24 ore. Se Amplifon ne subisce così tanti possiamo immaginare cosa accade alle altre società. «Quello che le aziende non capiscono è che i criminali informatici possono attaccare chiunque — spiega Chiesa — perché la porta di accesso è la vulnerabilità del provider». Come faceva il famoso software spione di Hacking Team. I board delle società ogni tre mesi ricevono un documento secretato sugli attacchi subiti. Certo, sono numeri che non escono quasi mai, se non quando qualche caso filtra nelle maglie della cronaca. Nel 2016 Deutsche Bank ha bloccato una truffa informatica da un miliardo, ma solo perché un dipendente solerte ha notato degli errori di grammatica in alcune richieste che arrivavano dal sistema creditizio del Bangladesh. D'altra parte se fosse tutto a posto non si capirebbe come mai ogni volta i report sul Paese siano preoccupanti: «Mai come nel 2016 sono emersi in maniera così

chiara i rischi ai quali le aziende sono esposte» ha scritto da poche settimane Fastweb. Per le banche gli attacchi sono aumentati del 64%. Gli anelli deboli possono essere anche gli individui: provate a fare una ricerca con un ".it" nella lista dei clienti del sito di incontri extraconiugali Ashley Madison messa in rete dagli hacker. Usciranno dipendenti di diverse società tra cui primarie banche italiane. Considerando che molti utenti tendono ad usare la stessa password gli hacker che hanno i database di Ashley Madison potrebbero avere le credenziali di accesso alle aziende. Trasparenza e nuove regole Gli istituti hanno l'obbligo di comunicare gli attacchi critici a Bankitalia, le altre società strategiche come le telecomunicazioni devono farlo al Garante della Privacy, Antonello Soro. Anche questi dati rimangono segreti. Ma le cose dovranno cambiare velocemente e anche questo potrebbe essere un a buona notizia per la professione hacker. «Per ora — spiega l'avvocato Gianluigi Marino dello studio Dla Piper — esistono degli obblighi solo per le telecomunicazioni, per chi gestisce il fascicolo sanitario elettronico e per chi raccoglie dati biometrici per l'ingresso dei propri dipendenti. Ma dal 25 maggio 2018 diventerà applicabile il nuovo regolamento Ue: tutti dovranno notificare gli attacchi subiti entro 72 ore e se hai un fornitore esterno dovrai accertarti che siano in grado di reagire. Per chi non lo farà ci saranno sanzioni fino a 10 milioni o pari al 2% del fatturato globale». I codici rubati alla Hacking Team Le competenze a giudicare da alcuni casi ci sono: il caso di hacking Team negli ambienti dell'intelligence italiana, a distanza di quasi due anni, è ancora considerato il caso più negativo di intrusione informatica per i suoi effetti. I media analizzarono le fatture tra i 400 gigabyte di dati. Gli hacker si presero i codici: pezzi interi del software spione sono riemersi di recente negli attacchi portati da Apt28 e Apt29, due gruppi di spioni russi riconducibili, secondo gli esperti, ad ambienti filo governativi russi. «Il caso è stato gestito male: la società era stata lasciata troppo libera, avremmo dovuto farla rientrare nel perimetro di Selex» giudica un alto esponente che preferisce l'anonimato del Cnaipic, il centro per la protezione informatica delle infrastrutture critiche della Polizia Postale. D'altra parte il furto dei codici dimostra che il software era valido. Il tema non è solo un esercizio storico: le istituzioni stanno ragionando su come favorire la rinascita di un software italiano ora che appare ormai chiaro come la rete esterna del ministero degli Esteri, ambasciate e consolati, era stata bucata per anni sempre dai russi. E chi era il fornitore esterno della piattaforma di sicurezza della Farnesina? Kaspersky. Società russa che in un primo momento aveva indicato i cinesi come i colpevoli.