SPECIALE

Cyber crime

RISCHIO CYBER, SERVIREBBE UNO SCUDO STELLARE

GLI INCIDENTI INFORMATICI SI SUSSEGUONO A RITMO ORMAI INCALZANTE: MA QUANTA RESPONSABILITÀ HA LA VITTIMA? LA SICUREZZA SUL WEB È SPESSO TRATTATA CON SUPERFICIALITÀ QUANDO, INVECE, DOVREBBE ESSERE PRESA DAVVERO SUL SERIO

di UMBERTO RAPETTO*

Inutile continuare a negarlo. Il vero rischio cibernetico siamo noi. Quella che potrebbe sembrare una simpatica frase ad effetto, degna del miglior incipit, è invece l'addolorata constatazione di chi da quasi quarant'anni abita in maniera nemmeno tanto passiva nella *digisfera* di questo pianeta.

L'apocalittico orizzonte lascia intravedere le conseguenze di sempre più frequenti incidenti informatici che azzoppano e a volte decapitano aziende e istituzioni che non avevano pensato di dover prendere in considerazione la minaccia hi-tech.
Incidenti di diversa caratura costellano virtualmente il cielo sopra le nostre teste, e soprattutto una pioggia di immaginarie meteoriti stanno piovendo senza che nessuno abbia un adeguato ombrello per trovare riparo. Si accatastano storie che se non fossero realmente accadute, avrebbero il sapore divertente di una lettura di svago.

TRECENTO GIOVANI E FORTI

Nel periodo natalizio, **The Heritage Company**, società di telemarketing con sede a Sherwood (mai nome fu così inopportuno) in Arkansas, ha scritto ai suoi oltre trecento dipendenti per invitarli a trovare un nuovo lavoro. Nessuna crudeltà nella dolente comunicazione, ma solo il drammatico resoconto del mancato ripristino dei sistemi informatici aziendali e quindi della perdita di tutti i dati a disposizione: il *ransomware*, che aveva crittografato archivi e cartelle di documenti, ha avuto la meglio su tecnici e esperti polverizzando l'operatività di una organizzazione che di informazioni viveva.
La signora **Sandra Franecke**, ceo della Heritage, impietrita dinanzi ai giornalisti che l'hanno presa d'assalto, ha raccontato dei due mesi di lotta laocoontica per liberarsi dalle spire del mostro che aveva cifrato e reso inutilizzabile il contenuto dei server. Nelle sue parole la disperazione di non aver mai preso in considerazione una simile evenienza o almeno di non aver mai affrontato con la dovuta sistematicità una insidia che sembrava lontana dal potersi manifestare e dal dare luogo a così catastrofici risultati.

**Generale (ris.) della Guardia di Finanza e comandante/fondatore del Gat-Nucleo Speciale Frodi Telematiche, è stato consigliere strategico di Franco Bernabè e group senior vice president di Telecom Italia. Tre lauree, docente universitario, giornalista e scrittore, ceo di Hkao-Human knowledge as opportunity e consigliere nel cda di Olidata SpA, è vice presidente della Autorità garante per la protezione dei dati personali della Repubblica di San Marino.*


© Yanawut - iStock

Chi legge dei trecento sventurati rimasti disoccupati magari si lascia scappare un infelice ricordo scolastico alla pari schiera capitanata da **Carlo Pisacane**, dimenticando che quei "giovani e forti" hanno segnato la storia e non considerando che di questi eserciti di lavoratori ne sono caduti, per colpa di un ransomware, molti altri in mille *spiagge* delle tante Sapri in giro per il mondo.

LA VITTIMA SE LO MERITA?

A essere macinati dai ransomware è toccato in sorte a interi sistemi municipali che hanno portato nel caos grandi città come Atlanta, Baltimora e New Orleans, a dimostrazione che anche i giganti possono avere piedi di argilla e finire al tappeto per un banalissimo inciampo. Non credo sia il caso di enumerare aziende di ogni calibro che (una infinità anche in Italia) si sono ritrovate KO, pagando il riscatto in bitcoin, non ottenendo le chiavi per decifrare, non disponendo di backup recenti.
La fattispecie delle infezioni virali di questa natura rappresenta il nord sulla bussola di chi dovrebbe occuparsi di certe problematiche. L'apparente banalità della minaccia cela la più completa struttura molecolare: gli atomi di questa combinazione sono la carenza di cautele, il deficit di cultura, l'inadeguatezza dell'ossatura tecnologica, il sostanziale disinteresse a certe tematiche, l'imperdonabile miopia manageriale.
Gli attacchi vanno a segno perché, tutto sommato, chi ne è vittima se lo merita. Tutto qui.
Non voglio essere cinicamente tranchant ma, non potendo esimermi dall'essere oggettivo e disincantato, mi vedo costretto a scorrere le dita sulla tastiera su cui scrivo spinto da quella concretezza che dovrebbe caratterizzare qualunque discussione su determinati argomenti.

DIFFIDARE DAI SEDICENTI ESPERTI

Parlare di cyber ha preso il posto del discorrere al bar del campionato di calcio vissuto dalla poltrona di casa oppure del narrare epopee sentimental-sessuali che provano solo una sconfinata fantasia erotica e nulla più. A disquisire della più sofisticata dimensione della sicurezza si accalcano orde barbariche di incompetenti che si improvvisano in ruoli di estrema criticità

Umberto Rapetto

senza avere la minima consapevolezza dei danni che andranno ad arrecare a chi (privo della benché minima capacità di committenza) li arruola.
Sedicenti esperti hanno tramutato la realtà nel set del cult movie *L'invasione degli ultracorpi*, aggirandosi per l'Italia ("isole comprese" come diceva un noto imprenditore dell'arredamento) parlando di cose che non conoscono e dispensando ferali consigli a sprovveduti convinti di trovarsi dinanzi a una entità soprannaturale. Il decadimento che deriva si riverbera a 360 gradi e viene messo in conto a soggetti apparentemente lontani dal luogo delle tante deflagrazioni.
Le schegge vanno a trafiggere chi fruisce dei servizi o utilizza i prodotti della ditta bersagliata dagli hacker e gli esempi non mancano. L'utente non riesce a collegarsi al fornitore, che comunque non può nemmeno dare risposte o che replica in maniera errata. Il prodotto si rivela inaffidabile per un bug piazzato ad arte da un programmatore precario assunto a progetto, sfruttato e carico di veleno per le ovvie amarezze per il mancato riconoscimento di professionalità e impegno.

LE ASSICURAZIONI CONTRO IL LUPO

Pur barricate dietro possenti fortificazioni, le compagnie assicuratrici confidano nel baluardo di severe analisi del rischio, di parametri rigorosi, di valutazioni intransigenti. È questo lo sbarramento più idoneo?
Saltano in ballo i tre porcellini dell'omonima fiaba e delle tre casette fatte di canne, di legno e di mattoni. Sicuramente assicuratori e riassicuratori (gioioso questo tintinnare delle medesime sillabe) avranno optato per la costruzione più robusta, così da contrastare il potente soffio del lupo, ma mi auguro che abbiano considerato che l'animale (nel nostro caso il malintenzionato, l'hacker, l'organizzazione criminale o addirittura terroristica, le squadre d'assalto State-controlled cinesi e russe…) conosce altrettanto bene quella favola e sa come giocare una eventuale simile partita.
Le check-list e le procedure di verifica che il contraente di una polizia sia effettivamente *hackerproof* si basano sul riscontro delle misure di sicurezza adottate. Le aggressioni anche.
Queste ultime, però, non guardano al pregresso ma

GLI ANTICORPI CONTRO IL CYBER CRIME

POPOLAZIONE AZIENDALE ADEGUATAMENTE FORMATA

"EVANGELIZZAZIONE" A FIANCO DI SOFTWARE E HARDWARE

SOCIAL ENGINEERING

METTERE ALLA PROVA LE RISORSE UMANE

fanno riferimento alla condizione corrente in quel preciso istante e fanno perno sulle vulnerabilità *zero-day*, ovvero i punti deboli conosciuti da zero giorni e quindi mai presi in considerazione da nessuno. Se una simile dinamica vanifica qualunque sforzo svolto a radiografare il sistema da assicurare, non è il caso di disperare.

IL DANNATO CLIC

La *cyber security*, al netto delle banalizzazioni che furoreggiano nei convegni, è fortunatamente un organismo complesso in cui non sono soltanto le tecnologie a determinare la salute delle aziende e delle istituzioni. Gli anticorpi più efficaci sono garantiti soprattutto dalla popolazione aziendale e dalla rispettiva preparazione a servirsi delle risorse informatiche a disposizione. Un adeguato livello di formazione (teorica, online, in aula…) costituisce la più efficace vaccinazione e innesca condotte virtuose che sono il principale ostacolo a chi ha preso di mira un possibile bersaglio.
Se è vero che i ransomware più evoluti dribblano, manco fossero Maradona ai tempi d'oro, antivirus e firewall arrivando a destinazione con estrema facilità, è altrettanto certo che senza il dannato *clic* del mouse dell'utente certe istruzioni maligne non verrebbero mai eseguite.
Il dipendente sensibilizzato e preparato, quindi, è il miglior soldato di questa guerra. Ma quanto peso ha la *truppa* nelle considerazioni su cui poggia la stipula di una polizza cyber?


© Chainarong Prasertthai / iStock

UNA QUESTIONE DAVVERO SERIA

Le realtà assicurative più attive sul mercato hanno pensato bene di erogare direttamente servizi di messa in sicurezza e di vincolare l'assicurazione del cliente alla implementazione di sistemi ritenuti affidabili e alla messa in opera da parte di una squadra *in-house* di comprovata attendibilità. Qualche grande compagnia ha piuttosto preso in considerazione un piano di *evangelizzazione* da affiancare al processo d'installazione di hardware e software?
Al di là degli ormai vintage *penetration test* (su cui sarebbe il caso di fare una pacata riflessione, magari in una prossima occasione), qualcuno ha mai provato a immaginare check basati sul social engineering e quindi incernierati su tecniche di persuasione dei lavoratori la cui ipnosi sovente non richiede sforzi eccessivi?
La diagnostica solitamente viene riservata a macchine e programmi, e solo qualche volta si estende agli apparati di rete che (specie con le ombre cinesi che disegnano spettrali figure) possono celare trappole micidiali. Raramente sono messe alla prova le risorse umane, partendo da quelle nel settore Ict per arrivare all'ultimo impiegato che incarna **Kevin Costner** nel *Balla coi lupi* dell'impresa o dell'ente.
Forse, finita la lettura di questi ragionamenti ad alta voce, varrà la pena di rivedere le metriche su cui si fondano i principi cardine della valutazione del rischio e della quotazione delle coperture. L'auspicio, in realtà, è semplicemente che la questione venga, una volta per tutte, presa sul serio. Ma davvero sul serio.
Ci stiamo giocando il futuro, non dimentichiamocelo.