Dino Esposito | Simone Massaro

Dietro le quinte della

CYBERSECURITY
Attacchi, danni e gestione del rischio

Uno scudo di conoscenza per arginare il marketing della paura ed evitare danni reali e d'immagine

Sono convinto che al mondo ci siano solo due tipi di aziende: quelle che hanno subito un attacco hacker e quelle che lo subiranno. E comunque tutte le aziende finiranno per convergere in un'unica categoria: quelle che hanno subito un attacco e che lo subiranno ancora.

Robert Mueller
Ex direttore FBI
RSA Cyber Security Conference, Marzo 2012

Dino Esposito | Simone Massaro

Dietro le quinte della

CYBERSECURITY

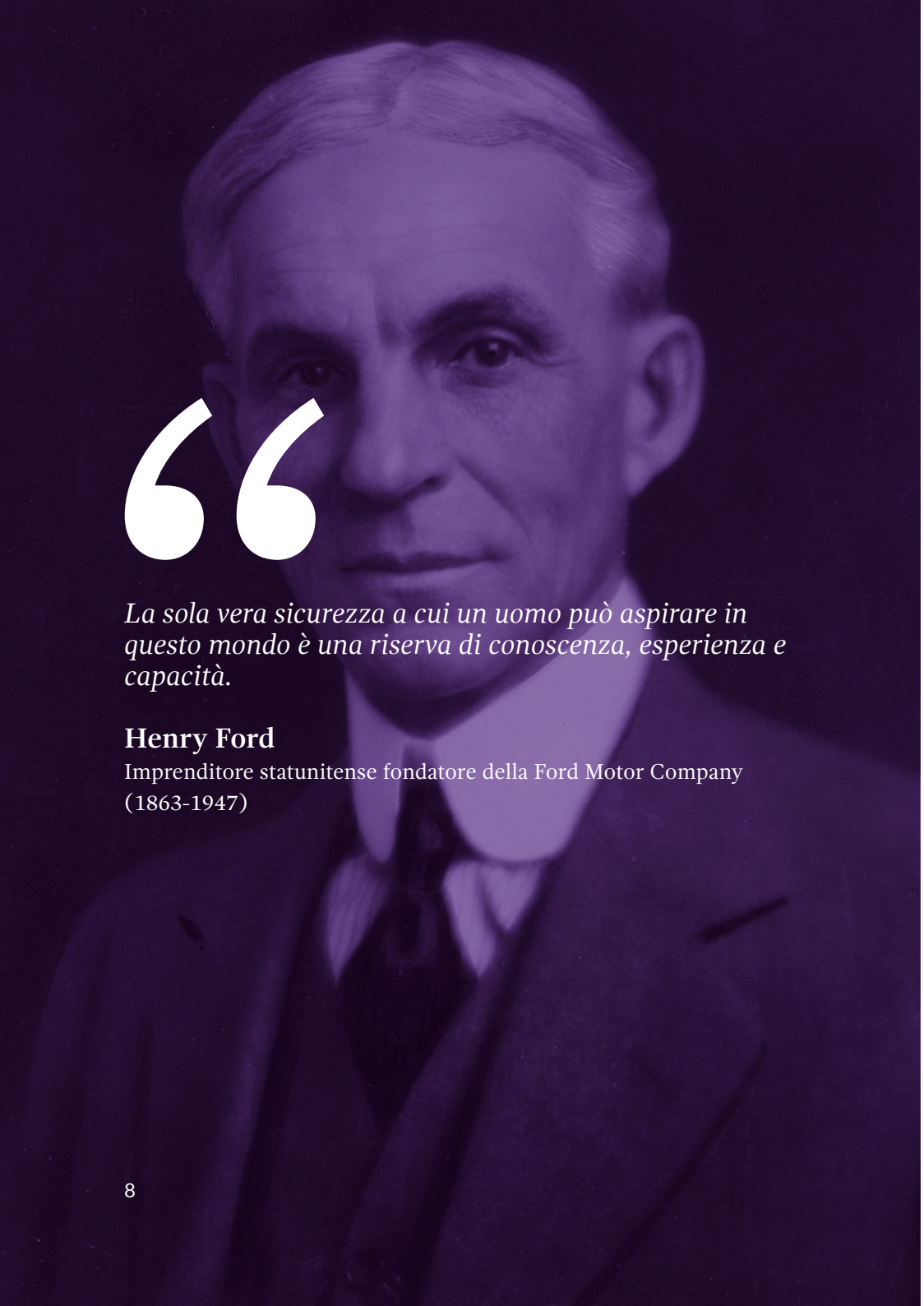
Attacchi, danni e gestione del rischio

Uno scudo di conoscenza per arginare il marketing della paura ed evitare danni reali e d'immagine

Introduzione

Da più parti si guarda al 2020, e al decennio che incomincia, come al tempo d'inizio di una presa di coscienza planetaria che tolga una volta per tutte la sicurezza informatica dalla lista delle priorità di facciata di ciascuna azienda per farne, invece, parte integrante della quotidianità. Ogni anno i report di svariati centri di ricerca, più o meno specializzati, ripetono come un mantra che la spesa nel mondo IT crescerà sfondando la soglia psicologica dell'ennesimo trilione di dollari. Al tempo stesso, ammoniscono che la parte destinata agli investimenti in cybersecurity rimarrà più o meno invariata e ben sotto il 30%.
È un dato di fatto, però, che il numero di attacchi riusciti, di qualsiasi tipo, aumenti ogni anno e con esso cresce per le aziende il costo di riparare il danno subito. Nonostante il dato allarmante, oltre la metà delle aziende, e non soltanto italiane, è convinta che la propria rete, e i propri dati, non costituiscano oggetto di interesse per la pirateria informatica e dunque non vi sia la necessità di prendere provvedimenti particolari. A microfoni spenti, però, i vertici delle stesse aziende ammettono di non conoscere con precisione né i rischi potenziali derivanti da eventuali attacchi informatici né le modalità di attuazione.
Il segnale più sinistro che testimonia la gravità della situazione viene dall'universo parallelo delle assicurazioni contro attacchi informatici. Secondo un'analisi di PricewaterhouseCoopers, nel 2020 si supererà la soglia dei dieci miliardi di dollari in polizze assicurative. Eppure negli ultimi due anni le compagnie assicuratrici hanno accettato di pagare i premi previsti solo in un numero esiguo di casi.

Perché?
Perché spesso i periti di parte hanno gioco facile a dimostrare che nelle aziende coinvolte erano assenti persino le misure più ordinarie di sicurezza informatica e, quand'anche vi siano state, è stata carente l'abilità di darne dimostrazione, vuoi per negligenza, per insufficienza di controlli o, più semplicemente, per errori ed omissioni.
Ben lungi dal rappresentare la pozione magica che tutto risolve, questo libro si propone l'obiettivo (oggettivamente ambizioso) di aumentare il livello di conoscenza dei meccanismi che guidano l'azione della pirateria informatica, mostrando le parti molli da rinforzare e i rischi potenziali.
E senza fare concessioni di sorta all'enfasi e al marketing della paura.



La sola vera sicurezza a cui un uomo può aspirare in questo mondo è una riserva di conoscenza, esperienza e capacità.

Henry Ford
Imprenditore statunitense fondatore della Ford Motor Company
(1863-1947)

1

UN GIORNO, ALL'IMPROVVISO

Fuori faceva molto caldo ed era pure normale visto che il calendario segnava il quattordici di agosto. E poi si era già capito da un po' che il 2003 sarebbe passato alla storia come l'anno delle temperature record. Nella sala di controllo della centrale di Eastlake, Ohio, c'era l'aria condizionata e all'esterno l'afa era pure mitigata dalla brezza che arrivava dalle sponde del lago Erie. Era un giovedì e l'operatore della FirstEnergy aveva appena iniziato il turno e sedeva distrattamente alla console con una tazza fumante in mano. La sua mente, inevitabilmente, guardava ben oltre i numeri che si susseguivano sullo schermo e arrivava fino alle prime luci del weekend in arrivo. Sapeva che il suo era un lavoro necessario; ma era anche un lavoro noioso visto che poi, alla fine, non succedeva mai niente.

Anche quello di Emily era un lavoro ripetitivo, in quell'ufficetto di mobili vecchi e moquette consunta al venticinquesimo piano di un anonimo grattacielo di Midtown Manhattan. Era sulla 72ma, non lontano dal museo di storia naturale e davvero a due passi da Central Park e dal celeberrimo mosaico in bianco e nero di Strawberry Fields. Emily lavorava per una compagnia di assicurazioni ed aveva davanti una lunga lista di polizze da verificare prima della fine della settimana.

Alle due del pomeriggio la temperatura raggiunse il picco e in tutto il Nordest degli Stati Uniti i condizionatori giravano al massimo. Per effetto del carico di energia e della temperatura esterna il materiale conduttore delle linee di alta tensione si espanse e i cavi si afflosciarono, come previsto, fino al limite inferiore della curva catenaria stimata

dai progettisti dell'elettrodotto.
Non si era mai verificato nulla del genere nelle precedenti estati, mai così calde, e alla FirstEnergy nessuno ritenne di preoccuparsi dell'altezza degli alberi sottostanti le linee, sebbene le direttive di sicurezza ne raccomandassero la regolare potatura che prevenisse il contatto con i cavi al loro limite inferiore.
Accidentalmente quel giorno la cima di un albero risultò troppo in alto così che il contatto con un cavo fu inevitabile.
Non fosse stato per il perverso bug di uno dei tanti sistemi software SCADA in uso nella centrale, i numeri sugli schermi si sarebbero immediatamente accesi di rosso generando un allarme e richiamando l'attenzione dell'operatore. Ciò non accadde e solo un'ora più tardi l'operatore della sala di controllo ebbe la sensazione che qualcosa non stesse andando per il verso giusto. Nel frattempo, però, altre linee di alta tensione erano cadute, vittime di un carico insostenibile. Dalla FirstEnergy non riuscirono a far nulla e due ore dopo si innescò un diabolico effetto domino che coinvolse il Sudest del vicino Canada e ben otto stati del Nordest, tra cui la città di New York.
Improvvisamente il computer di Emily si spense.
Lei si voltò istintivamente verso la postazione di fianco, ma sul volto della collega rivide la sua stessa faccia sorpresa. L'elettricità era saltata nell'intero l'edificio. Ancora pochi minuti e il caldo cominciò a farsi opprimente. Emily si affacciò alla finestra: era metà pomeriggio ma non si vedevano luci, nemmeno ai semafori e c'era sempre più gente raccolta in strada. Pian piano Emily unì le tessere del puzzle: niente corrente e dunque niente luce, computer, telefono, aria condizionata, ascensore, frigorifero. Peggio ancora: niente trasporti! Come sarebbe tornata a casa? Gli altri uffici? Gli ospedali? L'angoscia iniziò a serpeggiare.
Che stava succedendo?
Erano passati poco meno di due anni da quel 11 settembre e ancora la stragrande maggioranza dei newyorchesi era fortemente traumatizzata.

Cosa avrebbe dovuto fare?
A Eastlake intanto si provava a correr dietro alla catena di linee che cadevano come birilli, una dopo l'altra. Dall'iniziale afflosciamento di un singolo cavo di alta tensione alle due del pomeriggio del 14 agosto 2003 si arrivò nel giro di pochissime ore alla scomparsa di ben 60 Gigawatt di elettricità, con 50 milioni di persone che finirono immerse nel buio più totale.
Emily scese a piedi i 25 piani dell'ufficio in uno stato di panico latente, con solo una vaga idea di cosa potesse essere realmente accaduto. Una volta in strada, però, le fu tutto chiaro. Per fortuna, non si trattava di un'altra tragedia ma solamente di un gigantesco blackout.
Sollevata dall'angoscia di vivere un'altra terribile esperienza, la gente in strada fu presa da una crescente euforia ed un insolito spirito di squadra. Tutti aiutavano tutti e tutti erano amici di tutti. Col calare della sera, si vedevano perfetti sconosciuti parlarsi e incamminarsi per chilometri in un buio così totale da essere persino difficile da raccontare. La mancanza di corrente spinse Zabar's, celebre rivendita gourmet nel West Upper Side, a svendere prima, e a regalare poi, salmone, caviale e formaggi. E poi, per la gioia di tutti, i gelati.
Alla fine il blackout si tramutò in una specie di festa di strada anche se per molti tornare a casa fu un viaggio di ore, nel buio più nero e insieme a persone mai viste prima.
Per il pieno ritorno alla normalità ci vollero oltre due giorni.

La reazione a catena

Sebbene un po' romanzato, ciò che avete letto è il racconto dei fatti accaduti nel Nordest degli Stati Uniti a cavallo del ferragosto del 2003. In breve, si è trattato del blackout più rilevante della storia per numero di persone coinvolte. Ad esso è stato attribuito un costo economico complessivo di 8 miliardi di dollari, di cui una metà dovuta ai soli mancati guadagni di lavoratori ed investitori e l'altra agli sprechi di cibo e beni deperibili e alle spese extra necessarie per eliminare le conseguenze dell'evento.
La figura mostra due foto scattate da satelliti NASA alcune ore prima e alcune ore dopo il blackout. L'area cerchiata si riferisce alla zona di New York. In particolare al centro esatto del cerchio vi è la lingua di terra che corrisponde all'intera isola di Long Island.

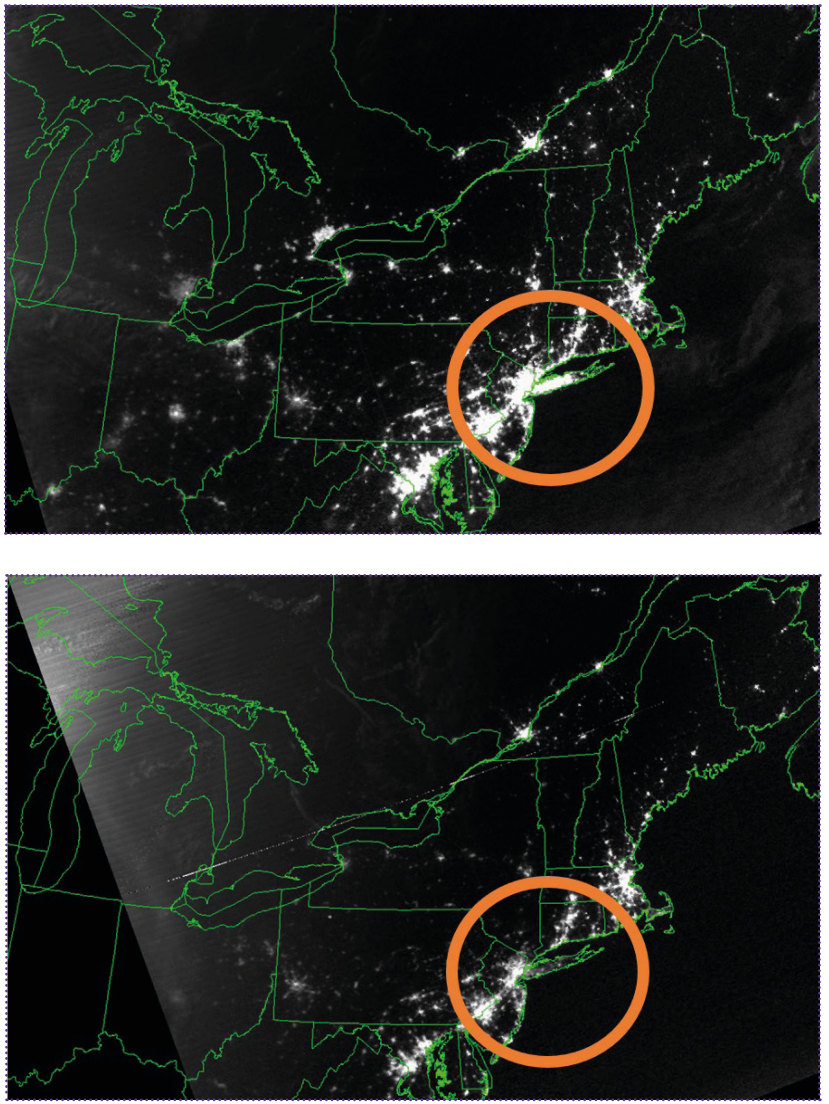


FIGURA 1-1

Area di New York prima e dopo il blackout dell'agosto 2003

Foto di https://earthobservatory.nasa.gov

Oltre al conto economico, il blackout del 2003 ha presentato anche un conto piuttosto salato in termini di vite umane. All'epoca il Centro Nazionale per le Informazioni Biotecnologiche (NCBI) stimò in circa un centinaio il numero di persone che persero la vita per cause ricollegabili in modo diretto al blackout: incidenti stradali per l'assenza di semafori e la scarsissima illuminazione, avvelenamento da monossido, improvvisa carenza di farmaci salvavita e peggioramento di condizioni di salute già precarie.
La commissione chiamata ad investigare sul blackout identificò la causa scatenante nell'effetto drammaticamente combinato di tre elementi:

~ Il bug di un software SCADA impiegato nel monitoraggio della centrale elettrica FirstEnergy dove tutto incominciò

~ La scarsa formazione e la limitata esperienza del personale di servizio nella sala di controllo

~ Gli alberi vicini ai cavi dell'alta tensione non adeguatamente potati

Dopo il blackout l'intera rete elettrica americana fu profondamente ristrutturata prendendo spunto da una serie di osservazioni critiche fatte alcuni anni addietro da organismi di controllo e bellamente ignorate fino al disastro. Inoltre, a partire dal 2003 le reti elettriche nazionali e regionali sono diventate sempre più digitali. Ciò ha razionalizzato sia la distribuzione che i consumi e inoltre ha reso complessivamente più efficiente la rete. Il termine smart-grid si riferisce proprio a questo tipo di intelligenza informatica.
Dall'altro lato, però, la digitalizzazione ha reso l'infrastruttura energetica più vulnerabile di prima rendendola potenzialmente vittima non solo di attacchi fisici ma anche di attacchi informatici.

Il blackout del 2003, così come la maggioranza di quelli che sono avvenuti negli anni successivi, sono stati il risultato ultimo di errori umani a fronte di eventi casuali più o meno prevedibili.

Nessuno di essi, per quanto è dato di sapere, è mai stato causato da un cyber-attacco. Ma ciò non vuol dire che il cyber-attacco ad una centrale elettrica non sia, di fatto, possibile.

Ove avesse mai luogo, un attacco informatico ad un segmento di infrastruttura energetica, di trasporti o telecomunicazioni potrebbe facilmente produrre danni su scala ben maggiore del blackout del 2003 a New York. Senza tema di smentita, un hacker che assumesse il controllo di una centrale elettrica di qualsiasi tipo potrebbe causare danni fisici alla strumentazione, incendi, esplosioni e naturalmente dare il là ad una catena interminabile di disservizi che colpirebbero le persone e causerebbero migliaia di vittime in modo diretto e indiretto.

Ho iniziato questo capitolo raccontando una storia vera—il blackout nel Nordest degli Stati Uniti dell'estate 2003—ma l'argomento del libro resta la cybersecurity.

Qual è, dunque, il nesso logico tra il blackout e la pirateria informatica?

Il senso ultimo della cosa

Di per sé, la pirateria informatica non è dissimile dalla pirateria che ha infestato i mari dei Caraibi nei secoli scorsi dando persino origine a saghe letterarie e cinematografiche. E non è dissimile da quella che in tempi molto più recenti ha preso forma in medio-oriente, in particolare nello stretto di Hormuz. La pirateria è alimentata principalmente da avidità e più in generale da scopi economici e strategici.

Ogni forma di pirateria, armata o tecnologica che sia, può funzionare solo in quanto capace di sfruttare falle e intrinseche debolezze della vittima. Per gli U-Boot nazisti durante la seconda guerra mondiale, e per qualsiasi corsaro dei setti mari, è stato fin troppo facile affondare (o depredare) i convogli, pressoché disarmati, che trasportavano persone e merci.

È di fatto una legge della natura: se la vittima è debole e indifesa, e al tempo stesso porta con sé del valore intrinseco, è giocoforza che sia attaccata. Ed è inevitabile che soccomba. Soprattutto se non è in grado di difendersi o se nel farlo commette errori marchiani.

Nell'ambito informatico le vittime designate sono gli individui ma ancor di più le aziende. Il movente è sempre l'avidità intesa sempre più spesso come controllo e monitoraggio volto all'acquisizione di un vantaggio strategico.

Torniamo brevemente al blackout del 2003. Come appurato dalla commissione investigativa, le cause erano riconducibili a tre fattori fondamentali:

~ Difetti del software di controllo

~ Scarsa preparazione tecnica

~ Negligenza operativa

Sono gli stessi fattori che rendono possibile un cyber-attacco. Possiamo generalizzare ed aggregare i tre fattori in due:

~ Falle nell'infrastruttura sia hardware che software in essere

~ Falle nella percezione del ruolo della sicurezza informatica

Nel primo ambito rientrano a pieno titolo tutti i bug sia relativi al software applicativo che al software di più basso livello che sostiene il sistema di rete. Nel secondo ambito, invece, rientrano i comportamenti umani e tra essi la superficialità e la faciloneria con cui troppo spesso ci si avvicina a messaggi di posta elettronica, aggiornamenti di pacchetti software, configurazione di apparati di rete, scambio di dati e si definiscono processi di business.
Un blackout, inteso come semplice mancanza di elettricità, può non essere percepito come un evento catastrofico e i suoi stessi effetti secondari, inclusi

i cento morti indiretti di New York, possono essere inconsciamente archiviati come eventi tragicamente casuali senza coglierne il legame con l'evento scatenante.
Analogamente, un attacco informatico, inteso come semplice interruzione di un servizio digitale, può non essere percepito come evento catastrofico e anche i suoi effetti secondari, quali che siano, possono essere inconsciamente archiviati come mere conseguenze senza coglierne gli effetti più remoti e profondi.

Le falle di sicurezza

Ogni software (e hardware) diventa vulnerabile nel momento in cui è costretto ad interagire con un operatore umano. La ragione è quasi sempre la necessità di acquisire dati in modo interattivo il che costringe i progettisti a lasciare aperte porte. Per quanto si possano predisporre barriere difensive, filtri e checkpoint rimarrà sempre uno spazio aperto per il libero arbitrio dell'essere umano che, se troppo libero. diventa un assist fenomenale per ogni pirata informatico che si rispetti.
Poi viene la componente dell'errore umano insito nella scrittura del software o nella realizzazione dell'hardware. In questo caso, però, c'è una buona notizia: le falle di sicurezza scoperte sono sempre chiuse a strettissimo giro dalle aziende produttrici e gli aggiornamenti rilasciati prontamente. Solo che poi l'installazione della nuova versione spetta alle aziende clienti e al personale IT, interno o esterno che sia. Spesso, invece, accade che versioni insicure di applicazioni software rimangano installate per anni continuando ad essere un formidabile veicolo per la diffusione di attacchi informatici.
In generale, vale la regola che se è il problema di sicurezza ha a che fare con un bug software allora è un problema ragionevolmente risolvibile e che verrà risolto ragionevolmente in brevissimo tempo. Tutto ciò, però, da solo non è sufficiente a ripristinare l'inviolabilità perduta e non azzera i costi di recupero dagli eventuali danni subiti.

Le falle culturali

Seppure con svariate eccezioni che saltano fuori periodicamente, l'hardware e il software si possono considerare relativamente sicuri. Quantomeno la superficie di attacco si riduce sempre di più nel tempo per effetto dei bug fix, anche se essa non potrà mai arrivare a zero.
L'esercito americano, manco a dirlo, vanta una lunghissima esperienza nel campo della sicurezza militare ed informatica. Gran parte di essa deriva dalla visione trasmessa dal padre della propulsione navale nucleare, l'ammiraglio Hyman G. Rickover. Per anni responsabile della costruzione di impianti di cruciale importanza per la sicurezza nazionale, l'ammiraglio divenne famoso per la cultura della sicurezza che trasmise ai gruppi di lavoro: dalla più elementare sicurezza sul lavoro alla protezione di luoghi, ai permessi di accesso fino all'intelligence.
Il fattore umano, diceva Rickover, conta molto di più di qualsiasi aspetto tecnico. È certamente di fondamentale importanza riuscire a proteggere e mettere in sicurezza l'infrastruttura hardware e software ma al tempo stesso va tenuto in debita considerazione che un errore umano può, in un attimo, vanificare anni di sforzi abbattendo con una sola e sconsiderata azione anche il più moderno e sofisticato sistema di difesa.
La lezione più rilevante che viene dall'esperienza dell'ammiraglio Rickover è che è necessario inculcare la cultura della sicurezza all'interno di ciascuna organizzazione in modo che ogni singolo processo e ogni operazione sia concepita, insegnata e infine compiuta in modo da minimizzare rischi di ogni sorta - per la persona, per l'organizzazione, per il lavoro stesso e per i dati che esso genera o trasmette.

Una falla culturale è ben più invasiva di una qualsiasi altra falla strettamente tecnologica. La falla culturale, infatti, impatta sui processi interni delle organizzazioni, sul modo di raccogliere e gestire i dati personali ed operativi e su come tali informazioni viaggino poi da un nodo all'altro dell'organizzazione. Chiudere una falla culturale, che sia relativa alla sicurezza sul lavoro, alla protezione dei dati o alla più generale sicurezza informatica richiede un grosso impegno e una volontà politico-gestionale forte.

La vera sfida è qui

Senza scendere in facili retoriche, ogni euro speso investendo in cybersecurity, è un euro risparmiato dal conto con cui si riparano i danni di eventuali attacchi subiti.

Una barriera difensiva veramente efficace è fatta sia di strumenti tecnologici (hardware e software) che di processi ad hoc ed è un deterrente che agisce a due livelli. Potrebbe forse non scoraggiare del tutto l'esecuzione di cyber-attacchi, ma saprebbe respingerli o quantomeno ostacolarli a sufficienza. Inoltre, la presenza di una barriera difensiva efficace sicuramente non invoglia l'hacker a ritentare. Agli hacker piace vincere. Ma soprattutto agli hacker piace vincere facile.