Kevin: il pericolo per Internet arriva da terrorismo e dal fattore umano

(Corriere Economia, marzo 2004)

Quando sale sul palco della "Security conference" organizzata a Milano da Icd, appare un po' ingrassato. Elegante, in giacca e cravatta, con la faccia tipica del bravo ragazzo da college americano. Se non fosse per il nome "Kevin Mitnich" annunciato dallo speaker, nessuno capirebbe che a parlare è l'hacker più temuto del mondo. Adesso dopo cinque anni di carcere e tre di libertà vigilata, con l'obbligo di non avvicinarsi ad alcun apparecchio elettronico in grado di collegarsi ad Internet, è passato dall'altra parte della barricata. Come ex hacker pentito, è diventato consulente della Commissione per la Sicurezza Nazionale, mettendo così a disposizione la grande esperienza in reti informatiche e sistemi di comunicazione. La sentenza dei giudici gli impone un'ultima restrizione: per altri sette anni la sua storia non potrà essere usata per sceneggiature cinematografiche perchè: «sarebbe un esempio negativo per i giovani». Corriere Economia lo ha incontro per chiedergli che cosa ne pensa del cyberterrorismo e della vulnerabilità delle reti aziendali.

Kevin, dopo gli attentati dell'11 settembre, dobbiamo aspettarci che i terroristi attacchino Internet, mettendo il web fuori uso?

«Direi proprio di no. Teniamo presente che Internet è nato negli anni '60 in ambito militare, con l'intento di resistere ad attacchi nucleari. La sua struttura intrinseca consente di trasmettere informazioni da un computer all'altro anche con un elevato numero di nodi fuori uso. Come è possibile distruggere migliaia di punti di accesso primari? E poi i terroristi non possono eliminare quello che gli serve».

Ci spieghi meglio

«Non hanno interesse a mettere fuori gioco il web. Perché per loro Internet risulta un potente mezzo di comunicazione. In rete trovano informazioni sugli obiettivi e le persone da colpire. Ma dipendono dal web anche per contattare con messaggi in codice chi li spalleggia e li finanzia».

Però i Governi, Stati Uniti in testa, hanno paura che dalla rete arrivino cyberattacchi alle Istituzioni.

«Certo. Per i terroristi Internet diventa un'efficiente arma per colpire i centri nevralgici dove risiedono informazioni riservate. Alle organizzazioni criminali non manca certo il denaro per assoldare hacker, con il compito di "bucare" i sistemi governativi dell'occidente. Ecco perché non bisogna mai abbassare la guardia».

Ma in concreto che cosa fare per difendersi?

«Partiamo dal presupposto fondamentale che non esiste sistema informativo sicuro al 100%. Ogni tecnologia presenta zone oscure di vulnerabilità. Allora bisogna agire secondo quella che definisco strategia circolare».

Cioè?

«Installare firewall, antivirus, procedure antiintrusione controllo degli accessi. Poi testare i punti di vulnerabilità. Individuato il primo "buco", trovare subito il rimedio e ripartire con i controlli. E così via. Senza mai smettere».

E i controlli chi li esegue?

«Team di specialisti in security. Spesso coadiuvati da ex hacker come me».

In ambito aziendale, troviamo gli stessi problemi di sicurezza?

«Direi di si. Con in più l'aggravante che spiego nel mio libro "L'arte dell'inganno": cioè il fattore umano. Infatti la violazione di un sistema informativo non avviene sfruttando solo strumenti tecnologici, bensì attaccando l'uomo, l'anello debole della catena».

Ci spieghi in concreto di che cosa si tratta?

«In questo caso l'hacker si impossessa di password, procedure e listati catturandoli con un inganno, messo a segno verso un dipendente che lascia in giro o butta nel cestino biglietti con i

propri numeri di codice. Ma li comunica anche via telefono (io l'ho messo in atto parecchie volte con successo) a chi si spaccia per supervisore del sistema o tecnico che deve inserire con urgenza una nuova versione del software. E poi ci sono migliaia di file con dati sensibili disponibili negli archivi elettronici delle aziende di servizi, negli uffici postali, banche e assicurazioni».

Insomma, ci sta dicendo che ognuno di noi ha disseminato centinaia di tracce della propria identità.

«Esatto. Per un hacker di medie capacità rubare l'identità di altri con strumenti digitali è solo una questione di tempo e pazienza. E una volta assunta la nuova "faccia" sarà semplice commettere un cybercrimine».

E come può difendersi il comune cittadino?

«Deve rilasciare i propri dati in rete solo quando è necessario, non scrivere codici e password su biglietti che poi tiene sulla scrivania e nel portafoglio, prestare attenzione alle telefonate di sconosciuti che chiedono informazioni troppo personali. Insomma proteggere la propria identità nel mondo reale e virtuale».

Che cosa farà adesso?

«A 40 anni, come hacker "in pensione" metto a disposizione le mie competenze per la security in ambito pubblico e privato. Poi tengo conferenze e sto scrivendo un nuovo libro per far conoscere al pubblico questo incredibile mondo parallelo».

Kevin, si ritiene ancora il più bravo?

«Il fatto di avere combattuto sui due lati della barricata mi dà dei vantaggi. Faccio del mio meglio per sfruttarli».

Chi è Kevin Mitnich

Kevin David Mitnich ha 40 anni. L'hacker più famoso del pianeta è noto semplicemente col nome di "Kevin". Inizia a 13 anni come radioamatore e scopre subito la sua passione per ogni oggetto elettronico che gli consente di comunicare con il mondo esterno. Solitario e autodidatta, a metà degli anni '80 colleziona i primi arresti a scuola perché manomette i laboratori di informatica. Da allora un'escalation di azioni illegali compiute contro compagnie telefoniche, aziende high tech del calibro di Motorola, Nokia, Sun, Novell, università e centri di ricerca. Viene arrestato nel 1995 in North Carolina dall'Fbi, dopo una lunga caccia all'uomo durata 14 anni. Condannato, ha scontato prima 4 anni e 11 mesi in un carcere di massima sicurezza, isolato da ogni apparecchio elettronico; poi altri 3 anni di libertà vigilata. Nel 2000 ha fondato a Los Angeles "Defensive thinking", un'azienda specializzata in sicurezza informatica. Pentito e riabilitato adesso lavora come consulente sulla security. Da poco è uscito in Italia il suo libro "L'arte dell'inganno" (edito da Feltrinelli).