

Carrai spiega come aumentare la cybersicurezza per bloccare i cyberspioni

Al direttore - Nel 2017 bisogna chiedersi se non sia più potente ai fini di potenziali danni alla sicurezza dello stato ma anche all'insicurezza del privato cittadino un arsenale nucleare o un giovane hacker davanti al suo computer. La mia risposta è naturalmente la seconda perché per fortuna le armi non convenzionali tradizionali quali sono quelle nucleari sono alla portata di pochi e probabilmente ben controllate, mentre i giovani o meno giovani hacker sono in mezzo a noi e magari sono già dentro le nostre vite a nostra insaputa. La prima rivoluzione culturale nasce da questa parola: hacker. Molte volte la associamo a un significato cattivo e sporco ma farlo sarebbe come dire che tutti gli ingegneri nucleari o i fisici fossero degli sganciatori di armi nucleari. La cultura della difesa cibernetica nasce dallo studio degli attacchi. Chi sa come intrufolarsi dentro un sistema saprà anche come difenderti. *Si vis pacem para bellum* dicevamo i romani e mai come in questo caso il motto è adeguato. Entrare in una nuova dimensione quale è quella del mondo interconnesso comporta avere le giuste attrezzature. Sott'acqua andiamo con la maschera e il boccale per pochi secondi, con le bombole con qualche minuto. Nel mondo popolato di malware, trojan e virus, dark web e Cloud si deve andare con la dovuta attrezzatura e con le dovute cautele. Sapere che le nostre foto, le nostre mail, i nostri sistemi di messaggistica stanno nel cloud vuol dire che qualcuno vi potrebbe un giorno accedere in modo lecito o illecito.

Vale di più allora conservare tutto o lasciare che come un tempo la parola la portasse via il vento? Aprire file che ti arrivano da indirizzi email conosciuti con la

stessa facilità con cui si digita qualcosa su Google comporta che qualcuno potrebbe approfittare di te iniettandoti un virus e rendendoti un libro aperto sul mondo. A volte molte persone mi dicono con soddisfazione che loro non utilizzano mai il traffico dati ma alla mia domanda se si siano mai attaccati a una rete wifi le loro certezze crollano immediatamente. Altre volte sento persone che sono sicure perché loro utilizzano solo iOS e Mac e hanno letto della sicurezza di tali dispositivi la cui casa madre ha rifiutato persino al Fbi i codici di accesso. Quando però gli domando se nel tempo abbiano mai aperto magari in viaggio o magari all'università o in altro luogo pubblico la loro posta elettronica molti, quasi tutti, mi dicono di sì. Ecco basta quell'atto compiuto una volta su un terminale infetto per entrare in tutti i sistemi protetti del mondo.

Per non parlare delle grandi aziende, che magari hanno succursali sparse nel mondo. Basta una succursale un pò meno protetta per entrare anche nell'azienda presumibilmente più sicura del mondo. Che dire poi di chi salva i codici pin di accesso sul proprio smartphone perché lo considera come un block notes.

Tutto ciò che genera dati è insicuro perché i dati girano e una falla è sempre a portata di mano. La cybersicurezza è come la sicurezza fisica. Non ci sarà mai un sistema totalmente sicuro perché gli elementi in gioco sono la tecnologia e gli imprevedibili comportamenti umani; ciò che è possibile è fare come per gli allarmi, i vetri antisfondamento e le porte blindate: alzare il costo per entrare dentro un sistema e rendere l'atto di intrusione non più conveniente.

Marco Carrai

