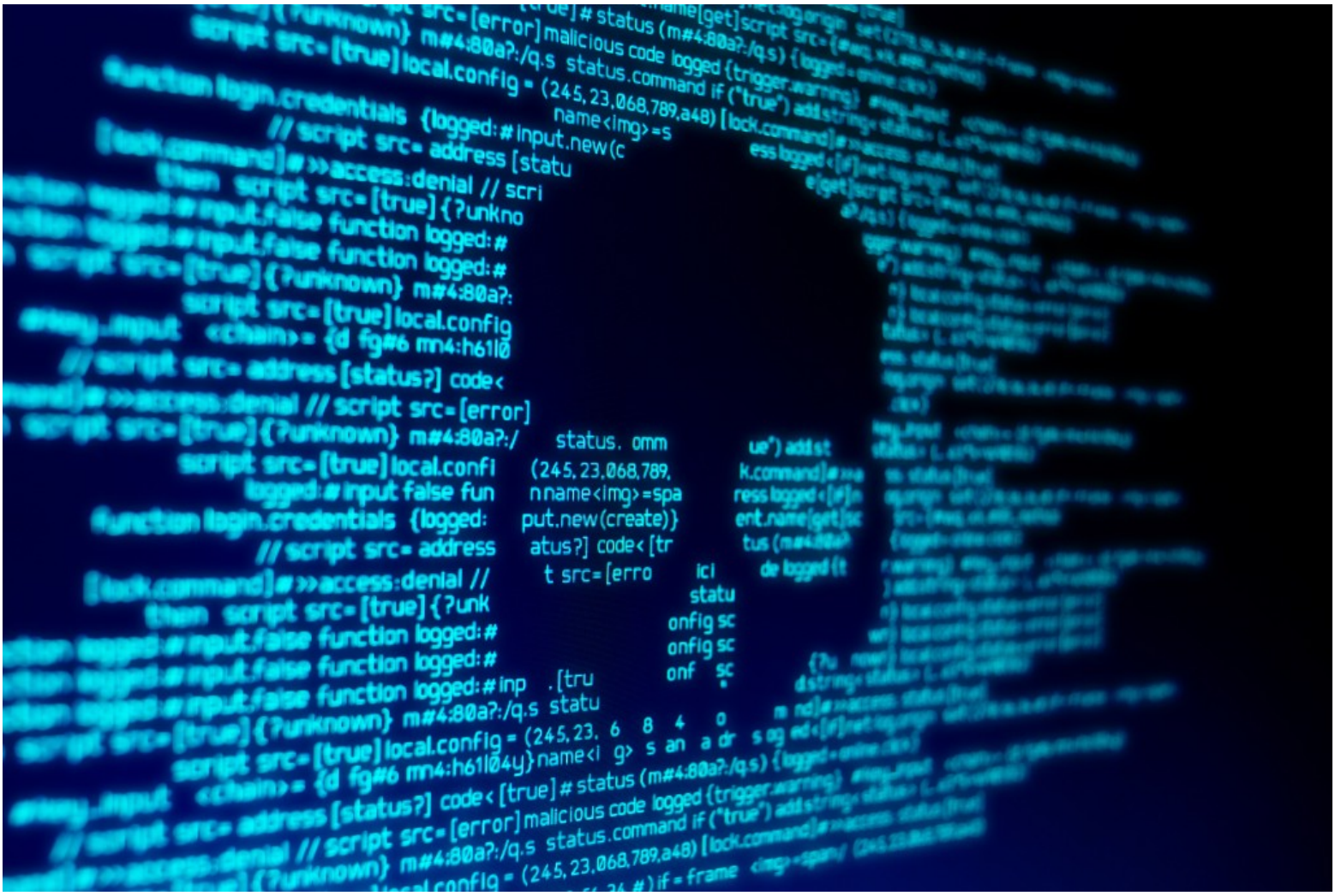


Nell'era di Internet nessuno è al sicuro: cybersecurity e attacchi cibernetici

Dalla sicurezza informatica alla cybersecurity

La sicurezza informatica, che raggruppa in sé tutti quegli strumenti adatti a proteggere riservatezza, integrità e disponibilità di qualsiasi sistema informatico, è al giorno d'oggi uno dei principali problemi di multinazionali, aziende, organizzazioni, governi e privati cittadini.

Una particolare branca della sicurezza informatica riguarda la cybersecurity, vale a dire quella parte che controlla la resilienza, la robustezza e l'affidabilità di una tecnologia di fronte ad eventuali attacchi che hanno lo scopo di compromette il sistema e il suo funzionamento.

È facile dunque comprendere come nell'era di Internet nessuno può dirsi al sicuro da eventuali minacce che corrono lungo la rete, da qui la necessità di ampliare sempre di più gli strumenti a protezione dei sistemi informatici che contengono dati sensili e informazioni di ogni sorta al servizio della collettività.

Hacker e cracker

Quando si parla di sicurezza informatica la prima parola alla quale spesso si pensa è hacker, termine inglese derivato da to hack e che, tra i suoi molteplici significati, definisce un individuo abile ed esperto dalle grandi competenze e conoscenze informatiche in grado di "aprirsi un varco" all'interno di un

programma, in particolare, tra hardware e software. Da questa attività, volta a migliorare le prestazioni di un particolare sistema, proprio perché permette di eliminare tutte le operazioni superflue bypassandole, deriva il temine hacking, o hackeraggio, attività perfettamente legale che, tramite l'utilizzo di test, mira a consolidare hardware e software, proprio al fine di tutelarli dai possibili attacchi dei crackers. Questi ultimi, conosciuti meglio come pirati informatici, sono individui abilissimi ad intrufolarsi nei sistemi e a sfuggire ai controlli, al fine di danneggiarli, rubare informazioni, commettere frodi e attività di spionaggio per interessi economici, politici e militari.

Se l'attività degli hackers ha un fondamento culturale ed etico basato sull'idea di un accesso alle informazioni quanto più aperto possibile e sull'utilizzo di softwares liberi, i crackers perseguono obiettivi meno nobili e sfruttano le loro competenze a proprio vantaggio o per fini poco leciti.

Gli attacchi cyber nella storia

Fulcro attorno al quale ruotano hackers e crackers sono dunque programmi, dati e informazioni che possono essere copiati, distrutti o sequestrati allo scopo di ottenere qualsiasi beneficio per il proprio tornaconto. Così dallo spionaggio industriale a quello militare, economico e politico, nessuno può dirsi al sicuro da eventuali attacchi, soprattutto nell'epoca in cui l'utilizzo di strumenti e infrastrutture informatiche avvolge ogni sfera dell'agire umano. Dai semplici smartphones di ignari utenti, alle informazioni segrete della National Security Agency, ogni sistema può "essere bucato" nel suo punto di vulnerabilità e messo a nudo.

La Storia è piena di tentativi di accesso più o meno legali a sistemi informatici, alcuni noti per via dell'enorme danno arrecato, altri meno conosciuti.

Il primo curioso attacco hacker può essere considerato quello messo in atto da due fratelli francesi, nel 1834. Già dai primi anni del 1790 in Francia si utilizzavano dei sistemi di comunicazione a distanza, che attraverso segnalatori meccanici situati in cima alle colline o alle torri, trasmettevano codici per mezzo del movimento di tre regoli di legno. A seconda della posizione di queste braccia di legno si comunicava un messaggio criptato che era osservato e ritrasmesso per mezzo di un telescopio. Era la tecnologia del telegrafo ottico, inventato da Claude Chappe e utilizzato dal governo francese, che permetteva la diffusione di informazioni in pochissime ore rispetto ai tempi lunghissimi della posta ufficiale. I due fratelli, speculatori finanziari, riuscirono ad inserire un codice privato nel messaggio criptato che sarebbe servito per ricevere informazioni riguardo fluttuazioni dei titoli di Stato sulla Borsa di Parigi in modo tale da investire nella Borsa di Boerdeaux.

Nel 1971, fu Bob Thomas a creare il primo worm in grado di autoreplicarsi. Il malware denominato Creeper portò alla creazione di Reaper, il primo antivirus della Storia.
Uno dei primi attacchi hacker nel senso moderno del termine può essere considerato quello messo in atto da uno studente, Robert Tappan Morris, nel 1988. Con l'obiettivo di dimostrare la scarsa sicurezza della rete, Morris creò un virus che, replicandosi, si diffuse rapidamente infettando circa 6000 macchine quasi tutte delle istituzioni pubbliche, procurando così ingenti danni.

Un hackeraggio durato quasi 30 anni è quello messo in atto da Greg Chung ai danni di Boeing, alla quale sono stati sottratti documenti aereospaziali e militari per un valore di circa due miliardi di dollari. Rivendute alla Cina, queste informazioni esponevano al rischio non solo la multinazionale ma anche gli Stati Uniti. Anche Snowden, ex dipendente della CIA, nel 2013 sottrasse e diffuse informazioni riservare alla NSA riguardo un programma segreto di sorveglianza di massa ideato da USA e Regno Unito.

Nel 2014 Sony Pictures fu presa di mira da un gruppo di hacker chiamati "Guardians of Peace" che cancellarono e pubblicarono documenti e informazioni riservate, bloccando l'accesso in rete ai dipendenti del colosso cinematografico. Il motivo che sembra aver scatenato il cyber attacco fu il tentativo di impedire

la diffusione di un lungometraggio titolato The Interview in cui un giornalista, insieme al sui direttore, tentavano di assassinare il leader Kim Jong–un durante un intervista.

Nel 2015 Tv5Monde, un'emittente francese, fu presa di mira da CyberCaliphate, un squadra di hacker che riscrisse il palinsesto televisivo per oltre tre ore, bloccando di fatto il servizio. Il gruppo aveva contatti con organizzazioni terroristiche e utilizzò anche i canili social della Tv per diffondere dati e informazioni di militari francesi coinvolti nella guerra contro l'organizzazione terroristica.

Petya nel 2016, NotPetya e WannaCry nel 2017 sono alcuni degli hackeraggi più famosi. Si stima che i costi causati da NotPetya si aggirino intorno ai 10 miliardi di dollari, mentre i sistemi informatici infettati da WannaCry sono oltre 230.000 diffusi in 150 Paesi.

A novembre del 2020, un attacco ai sistemi informatici dell'Università di Düsseldorf ha causato la morte di una donna, la cui vita dipendeva dalle macchine collegate al sistema dell'Università, nel Düsseldorf University Hospital. È la prima vittima ufficiale dei cyber attacchi.

Poche settimane fa dall'Olanda giungevano notizie poco rassicuranti riguardo la sicurezza informatica. Tre società olandesi che si occupano di protezione informatica richiedevano un intervento urgente del governo per far fronte ai numerosi attacchi hacker che si diffondono a macchia d'olio nel Paese.

A luglio di quest'anno è tornato alla ribalta Pegasus, uno spyware creato dalla società israeliana NSO utilizzato inizialmente per controllare traffici di terroristi e criminali, impiegato poi per spiare capi di Stato, giornalisti e attivisti. Già nel passato questa applicazione spia era stata ritenuta responsabile di aver sfruttato delle vulnerabilità di WhatsApp per spiare gli utenti. A tal proposito la piattaforma social aveva avviato una causa nei confronti della NSO, mentre Amnesty International aveva fatto ricorso contro il colosso della messaggeria istantanea, denunciando i numerosi attacchi a giornalisti, attivisti e politici. Tra questi Associated Press, Reuters, Cnn, il Wall Street Journal, Le Monde, il Financial Times, Al Jazeera, oltre 189 giornalisti, 600 politici, e molti uomini d'affari e attivisti dei diritti umani, tutti spiati da Pegasus, che di fatto è definito un programma militare inserito a pieno titolo in una nuova dimensione di scontro: la cyberguerra.

La vicenda di Pegasus, oltre che far riflettere sulla nuova dimensione assunta dallo spionaggio, mette al centro della discussione un'ulteriore questione: la legittimità dei trojan di Stato e il loro utilizzo.

Nell'era dell'Internet of Things, l'internet delle cose, ogni oggetto è connesso in rete e può diventare una potenziale arma, un mezzo per controllare e spiare chiunque, ampliando lo spettro delle possibilità di azione degli hacker e dei cracker. Non solo attacchi informatici che hanno come obiettivo dati e informazioni da distruggere o rivendere, ma anche il controllo da remoto di qualsiasi macchina connessa. A maggio di quest'anno un attacco cibernetico nei confronti del Colonial Pipeline, uno dei più grandi gasdotti americani ha costretto alla chiusura quasi 8.000 chilometri di gasdotto causando grandi disservizi.

In un Mondo sempre più interconnesso, che viaggia spedito verso la digitalizzazione della società, la difesa cibernetica richiede investimenti e strategie mirate, piani d'azione e politiche volte a intercettare i pericoli e a contenere i danni causati dal momento che un eventuale attacco informatico può raggiungere livelli di distruzione paragonabili ad un attacco armato.

Read More