

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 compromettere 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 sensibili 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 termine 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 cracker. 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 software liberi, i cracker 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 cracker 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

