# Nell'era di Internet nessuno è alsicuro: cybersecurity e attacchi ciberneticiaa

## Dalla sicurezza informatica alla cybersecurity

La sicurezza informatica, che raggruppa in sé tuttiquegli strumenti adatti a proteggere riservatezza, integrità e disponibilità di qualsiasi sistemainformatico, è al giorno d’oggi uno dei principaliproblemi di multinazionali, aziende, organizzazioni,governi e privati cittadini.

Una particolare branca della sicurezza informaticariguarda la cybersecurity, vale a dire quella parte che controlla la resilienza, la robustezza el’affidabilità di una tecnologia di fronte ad eventualiattacchi che hanno lo scopo di compromette ilsistema e il suo funzionamento.

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

## Hacker e cracker

Quando si parla di sicurezza informatica la primaparola alla quale spesso si pensa è hacker, termine inglese derivato da to hack e che, tra i suoimolteplici significati, definisce un individuo abile edesperto dalle grandi competenze e conoscenzeinformatiche in grado di “aprirsi un varco” all’internodi un programma, in particolare, tra hardware esoftware. Da questa attività, volta a migliorare leprestazioni di un particolare sistema, proprio perchépermette di eliminare tutte le operazioni superflue bypassandole, deriva il temine hacking, ohackeraggio, attività perfettamente legale che,tramite l’utilizzo di test, mira a consolidare hardwaree software, proprio al fine di tutelarli dai possibiliattacchi dei crackers. Questi ultimi, conosciutimeglio come pirati informatici, sono individuiabilissimi ad intrufolarsi nei sistemi e a sfuggire aicontrolli, al fine di danneggiarli, rubare informazioni,commettere frodi e attività di spionaggio perinteressi 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 adistanza, che attraverso segnalatori meccanici situati in cima alle colline o alle torri, trasmettevanocodici per mezzo del movimento di tre regoli di legno. A seconda della posizione di queste braccia dilegno si