**Atacuri de securitate în internet**

**Securitatea rețelelor de calculatoare** este în acest moment parte integrantă a domeniului rețelelor de calculatoare și ea implică protocoale, tehnologii, sisteme, instrumente și tehnici pentru a securiza și opri atacurile rău intenționate. Atacurile cibernetice au crescut considerabil în ultimii ani, iar conform unor rapoarte Europol, infracțiunile comise în spațiul cibernetic provoacă pagube anual de peste 1 trilion de dolari. Fiind un domeniu complex, au fost create domenii de diviziune pentru a putea face administrarea mai facilă. Acesta împărțire permite profesionistilor o abordare mai precisă în privința instruirii, cercetării și diviziuni muncii în acest domeniu. Sunt 12 domenii ale securității rețelelor specificate de International Organization for Standardization (ISO)/International Electrotechnical Commission(IEC):

1. [**Evaluarea Riscului**](https://ro.wikipedia.org/wiki/Evaluarea_Riscului) e primul pas în administrarea riscului și determină valoarea cantitativă și calitativă a riscului legat de o situație specifică sau o amnințare cunoscută;
2. **Politica de Securitate** este un document care tratează măsurile coercitive și comportamentul membrilor unei organizații și specifică cum vor fi accesate datele, ce date sunt accesibile și cui;
3. **Organizarea Securității Informației** e un model de guvernare elaborat de o organizatie pentru securitatea informației
4. **Administrarea Bunurilor** reprezintă un inventar potrivit unei scheme clasificate pentru bunurile informaționale
5. **Securitatea Resurselor Umane** defineste procedurile de securitate privind angajarea, detașarea și părăsirea de către un angajat a organizației din care va face, face sau a făcut parte
6. **Securitatea Fizica și a Mediului** descrie măsurile de protectie pentru centrele de date din cadrul unei organizații
7. **Administrarea Comunicațiilor și Operațiunilor** descrie controalele de securitate pentru rețele și sisteme
8. **Controlul Accesului** priveste restricțiile aplicate accesului direct la rețea, sisteme, aplicații și date
9. **Achiziția, Dezvoltarea și Păstrarea Sistemelor Informatice** definește aplicarea măsurilor de securitate în aplicații
10. **Administrarea Incidentelor de Securitate a Informației** tratează cum anticipează și răspunde sistemul la breșele de securitate
11. **Administrarea Continuității Afacerii** descrie mîsurile de protecție, întreținere și recuperare a proceselor critice pentru afacere și sisteme
12. **Conformitatea** descrie procesul de asigurare a conformității cu politicile de securitate a informației, standarde și reguli

Aceste 12 domenii au fost create pentru a servi ca bază comună pentru dezvoltarea de standarde și practici de securitate eficiente și pentru a da încredere activităților desfășurate între organizații.

Tot pe criterii de eficiență în abordare și usurință în învațare, atacurile de securitate la adresa rețelelor sunt împartite cu carater general în: recunoaștere, acces și de imposibilitate onorări cererii (DoS).

**Atacuri interne**

Multe atacuri privind securitatea rețelei provin din interiorul ei. Atacurile interne se referă la furt de parole (care pot fi utlizate sau vândute), spionaj industrial, angajați nemulțumiți care tind de a cauza daune angajatorului, sau simpla utilizare necorespunzătoare. Majoritatea acestor încălcări pot fi soluționate cu ajutorul ofițerului de securitate a companiei, care monitorizează activitatea utilizatorilor rețelei.

### Puncte de acces nesecurizate

Aceste puncte de acces nesecurizate fără fir sunt foarte slabe împotriva atacurilor din exterior. Ele des sunt prezentate pe comunitățile locale ale hakerilor. Punctul slab este că orice persoană poate conecta un ruter fără fir ceea ce ar putea da acces neautorizat la o rețea protejată.

### Back Doors

Comenzi rapide administrative, erori de configurare, parole ușor descifrabile pot fi utilizate de către hackeri pentru a avea acces. Cu ajutorul căutătorilor computerizați (bots), hackerii pot găsi punctul slab al rețelei.

### Denial of Service (DoS și DDoS)

Un atac cibernetic de tip DoS (*Denial of Service*) sau DDoS (*Distributed Denial of service*) este o încercare de a face ca resursele unui calculator să devină indisponibile utilizatorilor. Deși mijloacele și obiectivele de a efectua acest atac sunt variabile, în general el constă în eforturile concentrate ale unei, sau ale mai multor persoane de a împiedica un site sau serviciu Internet să funcționeze eficient, temporar sau nelimitat. Inițiatorii acestor atacuri țintesc de obicei la site-uri sau servicii găzduite pe servere de nivel înalt, cum ar fi băncile, *gateway*-uri pentru plăți prin carduri de credite, și chiar servere întregi.

### *Hackers, Crackers, Script Kiddies*

**Hackerii** Cuvântul hacker în sine are mai multe interpretări. Pentru mulți, ei reprezintă programatori și utilizatori cu cunoștinte avansate de calculator care încearcă prin diferite mijloace să obțină controlul sistemelor din internet, fie ele simple PC-uri sau servere. Se referă de asemeni la persoanele care ruleaza diferite programe pentru a bloca sau încetini accesul unui mare număr de utilizatori, distrug sau șterg datele de pe servere. Termenul "Hacker" are și o interpretare pozitivă, descriind profesionistul in rețele de calculatoare care-și utilizează aptitudinile în programarea calculatoarelor pentru a descoperi rețele vulnerabile la atacuri de securitate. Actiunea in sine, aceea de hacking e privită ca cea care impulsionează cercetarea în acest domeniu.

**Crackerii** sunt niște persoane care au un hobby de a sparge parole și de a dezvolta programe și virusuri de tip cal troian (**en**: Trojan Horse), numite Warez. De obicei ei folosesc programele pentru uz propriu sau pentru a le relizeaza pentru profit.

**Script kiddies** sunt persoane care nu au cunoștințe sau aptitudini despre penetrarea unui sistem ei doar descarcă programe de tip Warez pe care apoi le lansează cu scopul de a produce pagube imense. Aceste persoane sunt angajați nemulțumiți, teroriști, cooperativele politice.

### Viruși și viermi

Virușii și viermii reprezintă programe care au proprietatea de a se automultiplica, sau fragmente de cod care se atașează de alte programe (viruși) sau calculatoare (viermii). Virușii de obicei stau în calculatoarele gazdă, pe când viermii tind să se multiplice și să se extindă prin intermediul rețelei.

Santy, primul "webworm" cunoscut in Internet. Se baza pe o vulnerabilitate din cadrul phpBB (open source bulletin board software) si folosea Google pentru a gasi noi sisteme vulnerabile si a se raspandi in Internet. In trei ore de la lansare s-a raspandit pe tot globul, in 24 de ore a afectat intre 30.000 si 40.000 de sisteme. Google a filtrat, intr-un final, search query-ul folosit de vierme pentru a localiza noi sisteme vulnerabile.

### Cal troian

Calul Troian (Trojan Horse) se atașează de alte programe. Când se descarcă un fișier care este infectat cu acest virus, el va urma sa infecteze sistemul, unde oferă hackerilor acces de la distanță si puterea de a manipula sistemul.

### Botnets

Îndată ce un calculator (sau probabil mai multe calculatoare) au fost compromise de un Troian, hackerul are acces la aceste calculatoare infectate, unde de aici el poate lansa atacuri cum ar fi [DDoS](https://ro.wikipedia.org/w/index.php?title=DDoS&action=edit&redlink=1) (Distribuited Denial of Service).

Grupa de calculatoare care sunt sub controlul hakerului se numesc botnets. Cuvântul botnet provine de la robot, aceasta însemnând că calculatoarele îndeplinesc comenzile proprietarului lor și rețea însemnând mai multe calculatoare coordonate.

### Sniffing/Spoofing

Sniffing se referă la actul de interceptare a pachetelor TCP (Transmission Control Protocol). Spoofing se referă la actul de trimitere nelegitimă a unui packet de așteptare ACK.

### Atacuri remote si atacuri locale

Atacurile remote presupun exploatarea unei vulnerabilitati in cadrul unui serviciu/proces daemon care asteapta cereri pe un anumit port. In urma exploatari cu succes a unei vulnerabilitati remote, atacatorul ajuge sa ruleze pe sistem cod cu privilegiile utilizatorului care ruleaza procesul daemon / serviciul.

Atacurile locale presupun ca atacatorul poate rula cod cu privilegiile unui anumit utilizator pe sistem (spre exemplu studentii pot initia un atac local). Exploatate cu succes duc la escaladarea de privilegii, obtinerea unor privilegii mai ridicate (root, administrator) pentru un control total al sistemului. In unele cazuri atacul local nu mai este necesar, spre exemplu in contextul atacului unui server sau aplicatii Web (atacatorul este interesat in alterarea continutului web nu al intregului sistem de fisiere).