Frumos și corect spus despre abundența atacurilor cibernetice și a amenințărilor este în [1], unde trasată este o paralelă cu bătăliile din razboaie. Niciuna nu este la fel, ceea ce este atât de adevărat în realitatea actuală. Acest lucru înseamnă că sunt folosite strategii și tactici similare, deoarece persoanele / hackerii au văzut că sunt eficiente și economisesc timp. Nimeni nu va re-inventarea roții decât dacă este absolut o necesitate. După cum se menționează în [1], vor fi utilizate tehnici comune care au fost utilizate cu o rată ridicată de succes, cum ar fi programele malware, phising și altele.

O altă sursă [2] recunoaște că criminalii sofisticați pot exploata cu ușurință erorile umane și vulnerabilitățile calculatorului. Din aceste atacuri, rezultatele pot diferi de la criminalii care accesează informațiile dvs. personale și financiare, si de a împiedica abilitatea dvs. de a utiliza dispozitivul și multe alte posibilități care vă lasă vulnerabili doar la posibilitatea de a vă pierde identitatea. În viguare exista deja legi împotriva crimelor cibernetice, dar doar atât poate face acum legea, deoarece este atât de greu să găsim persoana responsabilă care se ascunde în spatele tacticii și strategiilor folosite.

Atacurile pot fi oprite și evitate prin simpla folosire a uneia dintre multele măsuri de securitate găsite online, de la scanarea computerului la instalarea software-ului anti-malware la soluții complexe.

În ceea ce privește informațiile pe care tocmai le-am adunat din diferite surse, atacurile sunt împărțite în cel puțin două categorii, active și pasive. După cum se vede în [3], diferența majoră dintre aceste două tipuri este că în atacurile active conexiunea este interceptată și informațiile sunt modificate, iar în atacurile pasive informațiile sunt citite și analizate, dar nu modificate.

**Definiția atacurilor active** - sunt atacurile în care atacatorul încearcă să modifice informațiile sau creează un mesaj fals, pe care utilizatorul îl identifică drept real. Pentru a preveni aceste atacuri, utilizatorul are multe de făcut. Este dificil din cauza unei game largi de vulnerabilități potențiale în rețea și software. Pe primul loc este detectarea atacului și recuperarea datelor, pierdute din cauza întreruperilor sau întârzierilor. Aceste atacuri sunt de cele mai multe ori sub formă de întrerupere, modificare și fabricare.

**Definiția atacurilor pasive** – sunt atacurile în cazul în care interceptarea neautorizată, monitorizarea transmiterii sau colectarea de informații are loc. Nu există o alterare a informațiilor și a datelor, de aceea spre deosebire de atacul activ este mai greu de detectat. Ceea ce înseamnă că utilizatorul este neinformat de atacul care se întâmplă în sistemul său. Acest lucru poate fi evitat prin încriptarea fișierelor cu un sistem complex de chei sau cu certificate care nu permit altor părți să obțină conținutul fișierelor / datelor. Pentru acest tip, prevenirea este pe primul loc, nu detectarea ca în cazul atacurilor active.

Un atac pasiv poate fi de două tipuri: eliberarea conținutului mesajului și analiza traficului.

**Principalele diferențe** menționate de [3] sunt următoarele:

1. Atacul activ înseamnă că mesajele sunt modificate. Pe de altă parte, în atacurile pasive, atacatorul nu face schimbări.
2. Atacul activ provoacă daune sistemului, în timp ce atacul pasiv nu provoacă nici un rău.
3. Un atac pasiv este o amenințare la confidențialitatea datelor. În cazul în care un atac activ reprezintă o amenințare la adresa integrității datelor.
4. În atacurile active victima este conștientă de atac, iar în cazul atacurilor pasive victima este neinformată.

Ca o altă sursă [4], amenințările pot fi clasificate în patru categorii: directe, indirecte, voalate și condiționate.

**Amenințare directă** - descrie o țintă aleasă care este atacată cu un act specific. Atacul este clar și direct pentru victimă. Această categorie este folosită nu numai online, ci poate fi adresată direct victimei și în viața de zi cu zi.

**Amenințare indirectă** - descrie o amenințare vagă, neclară și ambiguă. Fiecare detaliu din plan, motivația, victimă și nu numai sunt mascate și nu sunt divulgate. Este posibil să apară, dar nu garantat.

**Amenințarea vehementă** - implică, dar nu amenință violent explicit. Este lăsată victimei să interpreteze și să dea o semnificație amenințările.

**Amenințarea condiționată** - este obișnuită pentru cazuri de extroziune. Un act violent se va întâmpla dacă anumite cerințe sau termeni nu sunt îndeplinite.

Toate atacurile și amenințările pot fi clasificate în diferite categorii. Este important să rețineți că diviziunea se bazează fie pe actori, fie pe victima. Când vorbiți despre aceste atacuri, rețineți că nu sunteți suficient de protejați, găsesc chiar cel mai mic decalaj de securitate și îl folosesc pentru avantajele lor. Deci, păstrați în datele în siguranță.