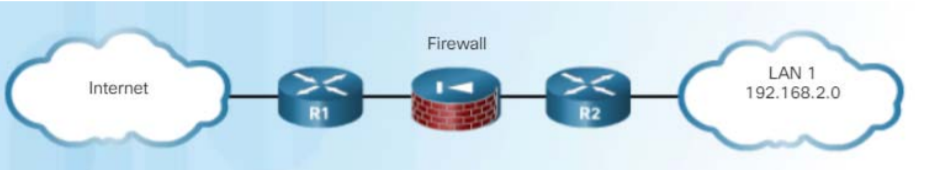
**Kuptimi I mbrojtjes**

Rreziku i sigurisë kibernetike përbëhet nga tre komponenta : **Asetet** – Janë vlerat e një organizate qofshin ato paisje të fundme, serverë, paisje tjera ose të dhëna. **Rreziku** – Paraqet dobësitë e një sistemi ose dizajni të cilat mund të shfrytëzohen nga kërcënimet. **Kërcënimet** – Janë cdo llojë rreziku potencial ndaj aseteve.

Assetet janë shumë të rëndësishme për kët edhe duhet mbrojtur, për të arritur mbrojetien e trye organizatat duhet të ken parasysh dy gjëra : 1.Invertarizmin e asteteve. 2.Zbatimin e politikave dhe procedurave për mbrojtien e tyre.

Për të zbatuar mbrojtien në thellësi të trafikun që hyn e del në një rrjetë duhet të përdorum një topologji të këtij lloji : Nevojitet një router edge i cili lidhet me internet dhe është i konfiguruar me një sër rregullash që i mundësojnë të zgjedhin se cilin trafik ta pranojnë e cilin jo. Pastaj vendoset një firewall i cili e filtron trafikun dhe në fund është routeri i brendshëm i cili bën edhe disa filtrime përfundimtare para se të arrij trafiku në destinacion. 

**Analogjia e qepës** : Është një qasje shumë shtresore e sigurisë ku akterët e kërcënimit duhet të kalojnë nëpër shumë shtresa deri të arrijnë tek e dhëna.

**Analogjia e artichokës** : Është një analogji më e mirë për rrjetat pa kufijë, mirpo i mundëson akterëve kërcënues që vetëm me hekien e disa shtresave të ken qasje në të dhëna.

Politikat janë themeli i sigurisë së rrjetit, ato përcatojnë se qfarë është e pranueshme.

Politikat e biznesit janë udhëzime të zhvilluara nga një organizat të qeverisë me veprimet e sajë dhe të punonjësve.

Politikat udhëzuese që duhet ndjekur një oranizatë janë : **Politikat e kompanisë** : Përcaktojnë sjelljen dhe përgjegjësitë e punëdhënësit dhe punonjësit. **Politikat e punonjësit** : Identifikojnë pagat, pushimet, orarin e punonjësve etj. **Politikat e sigurisë** : Janë sër objektivash të sigurisë që përcaktojnë se si duhet të sillen punonjësit, administratorët dhe kërkesat e sistemit.

**Politikat e përdorimit të pranueshëm** (AUP): Kto politika identifikojnë fuksionet që punojnjësit mund të kryejn dhe nuk lejohet ti kryejnë në komponentat e sistemit.

**BYOD** : Është një program i cili i pundëson punonjësve qasje në burimet e organizatës duke përdorur paisjet e veta personale.

BYOD ka disa politika në të cilat përfshihen : Specifikimi i qëllimeve të BYOD, identifikimi i personave që mund të sjellin paisjet me vete, identifikimi i pasijeve që përkrahen, identifkimi i rregullave që duhet respektuar dhe identifikimi i masave mbrojtëse që duhet marrë në rast se ndonjë paisje korruptohet.

Për të rritur sigurin e përdorimit të këtij programi, BYOD sygjeron disa praktika të cilat duhet ndjekur : Përdorimi i fjalkalimeve në gjdo paisje dhe llogari, ndalja e funksionit të auto connection me wifi, aktivizimi i find-my-device funksionit, paisja me antivirus, përditësimi i sistemit dhe backup i të dhënave.

Rregullat dhe standardet e pajtushmërisë përcaktojnë se cila organizat/a janë të detyruara të ofrojnë përgjegjësi nësë dështojnë.

Siguria e informacionit mirret me mbrojtien e informatave dhe sistemeve të informatave nga qasja, zbulimi, prishja, përdorimi i pa autorizuar.

**Kontrolli i qasjes**

**CIA Triangle** : Secila nga shkronja e ka kuptimin e vet **C** – Konfidencialitet : Në informata të ken qasje vetëm personat e autorizuar , **I** – Integritet : Personat e pa autorizuar mos të ken qasje në informata, **A** – Avalible(Disponushmëria) : Informata të jet e disponueshme për personat e autorizuar kurdo që ata e kërkojë.

Ekzistojnë disa modele të kontrollit të qasjes, ndër to përmendim : **Kontrolli i detyrueshëm i qasjes** (MAC) : Kontroll i rrept i qasjes, i mundëson akses përdoruesve duke u bazuar në pastrimin e sigurisë. **Kontrolli diskrecional i qasjes** (DAC) : Mundësonë përdoruesve të kontrollojnë qasjes në të dhënat e trye sikur të ishin pronar të tyre. **Kontrolli jo-diskrecional i qasjes** (RBAC) : Bazohet në rolet dhe përgjethsitë e përdoruesit. **Attribute-based-acces-control** (ABAC) : Qasja bazohet të atributet e burimit të qasur, përdoruesit që qasen dhe faktorët e mjedisit.

Model tjetër është modeli i parimit të privilegjit më të vogël : ku përdoruesve i ipet akses minimal vetëm për të kryen funksionet që i nevojiten për punë.

Kontrolli i qasjes i shkallëzuar **AAA** : Edhe këtu secila shkronjë e ka kuptimin e vetë **A** – Autetifikim, **A** – Autorizim, **A** – Kontabilitet.

**Autentfikimi** : Përdoruesit duhet të vërtetojnë se janë ata që pretendojnë.

**Autorizimi** : Përcakton burimet e qasëshme për përdoruesin dhe fuknsionet që mund ti kryej.

**Kontabiliteti** : Regjistronë gjdo gjë që përdoruesi bën dhe kur e bën.

Kemi dy metoda të AAA : **AAA autentifikimi lokal** – Përdoret për rrjeta të vogla, kur përdoret një router AAA dhe të dhënat për autentifikim ruhen në një databaz lokale. **AAA autentifikimi server** – Përdoret router AAA dhe një serverë AAA në të cilin ruhen të dhënat për autentifikim.

Serverat AAA përdorin **Accounting** (Kontabilitet) : për të regjistruar gjdo gjë që përdoruesit bëjn në të. Në këto Accounting ruhen informata si : Network Accounting, System Accounting, Command Accounting, Exec Accounting, Connection Accounting, Resource Accounting.