ULTRANET SHPK
NIPT: L76625005G
Adresa: Rr. Branko Kadia, Nr.6, Shkodër
E-mail: info@ultranet.al
Mob: +355 682019201

UDHEZUES PER PERDORUESIT

2019

ULTRANET SHPK
NIPT: L76625005G
Adresa: Rr. Branko Kadia, Nr.6, Shkodër
E-mail: info@ultranet.al
Mob: +355 682019201

Siguria luan një rol shumë kritik në pothuajse çdo fushë të një organizatë, një entitet qeveritar, madje edhe në shtëpinë tuaj. Kompjuterët, pajisjet celulare dhe Interneti po përballen cdo ditë me shumë sfida të sigurisë.

Kompjuterët/celularët tani janë përfshirë në listën e gjërave të domosdoshme për njeriun. Nga llogaritja më e thjeshtë matematikore deri tek ruajtja e të dhënave, ndërtimi i aplikacioneve, komunikimi me botën dhe kështu me radhë, ne të gjithë varemi tërësisht nga këto pajisje.

Përsa i përket rreziqeve të sigurisë për celularët/kompjuterët duhet të merren në konsideratë, sulmet e viruseve, vjedhja e të dhënave, fshirja e të dhënave dhe dëmtimi i pajisjeve.

Çfarë është siguria e rrjetit?

Siguria e rrjetit merret me aspekte të tilla si: parandalimi i aksesit të paautorizuar, mbrojtja kundër hakimit, keqpërdorimit, etj. Siguria mund të quhet si plotësuese e faktorëve si: konfidencialiteti, integriteti dhe disponueshmëria (CIA).

Llojet e ndryshme të Kërcënimeve të Rrjetit

Në vijim janë llojet e kërcënimeve nga të cilat mund të preket një rrjet:

1. **Aksesi i paautorizuar**

Ky është kërcënimi më i dëmshëm pasi çon në humbjen e informatave të rëndësishme dhe gjithashtu në sulme të mëtejshme, të cilat mund të jenë edhe më të dëmshme. Një sulmues pa dijeninë tuaj, fiton akses në seksionin tuaj të autorizuar dhe vjedh burimet e ndjeshme.

Në mënyrë që të mbroheni nga këto sulme duhet të ndiqni këto hapa:

- Zgjidhjet e Sigurisë (anti-virus, anti-malware, internet security, etj)

- Zbatimi i strategjive të forta të identifikimi.

- Mbajtja e përdoruesve dhe fjalëkalimeve të fshehta nga burimet jo të besueshme.

-Mos sigurimi i aksesit të panevojshëm për këdo.

- Vendosja e password-eve në mënyrë të personalizuar. Password-et sugjerohet të jenë të përbërë nga:

Shkronja (të vogla & kapitale)

Numra (0-9)

Karaktere special (psh. !@#$%)

2. Viruset dhe krimbat

Viruset dhe krimbat kompjuterikë janë programe shkatërruese të dizajnuara për të infektuar sistemet bazë, duke shkatërruar të dhënat thelbësore të sistemit dhe duke bërë rrjetet e paperdorueshme. Viruset janë bashkangjitur në një sistem ose fotografi të strehuesit dhe mund të gjenden në gjumë derisa të aktivizohen pa dashje nga një orë me zile apo ngjarje. Krimba janë më të përgjithshëm - duke infektuar dokumente, spreadsheets dhe skedarë të tjerë. Pasi të keni hyrë në sistemin tuaj, menjëherë do të fillojë të përsëritet, duke infektuar sistemet në rrjet dhe kompjuterët e pa mbrojtur. Viruset dhe krimbat formojnë blloqet e ndërtimit për shumë kërcënime kibernetike më të avancuara.

Instalimi i programeve anti-malware në të gjitha pajisjet dhe sistemet e rrjetëzuara mund të zvogëlojë ndjeshëm mundësinë e kontraktimit të këtyre viruseve ose t'u lejojë atyre të përhapen. Duke njohur kërcënimet në fillim dhe duke i përmbajtur ato, këto zgjidhje u mundësojnë administratorëve të zbulojnë programe të dëmshme dhe t'i largojnë ato para se të shkaktojnë ndonjë dëm.

3. Shkarkimi i kërcënimeve përmes shkarkimeve (Drive-by download attack)

Në të kaluarën, një mënyrë e thjeshtë për të siguruar që nuk po shkarkon një virus në kompjuter, ishte të mos shkarkoje dokumente nga burime të panjohura. Për fat të keq, sot nuk është kaq e lehtë.

Një drive-by download është një formë sulmi që lejon që kërcënimet të shkarkohen nga një faqe interneti përmes një browser-i, aplikacioni ose sistemi operativ të integruar pa ndonjë veprim nga ana e përdoruesit. Këto URL janë të dizajnuara për t'u dukur dhe vepruar si një faqe interneti e vërtetë, por në fakt, ata po mbjellin baza për disa lloje të ndryshme kode kërcënimesh me shpresën se njëri prej tyre do të kalojë përmes sigurisë së sistemit tuaj.

Mbajtja e browser-t tuaj të përditësuar është një nga mënyrat më të mira për të ndihmuar në identifikimin e këtyre faqeve me qëllime të këqija para se t'i vizitoni ato.

Gjithashtu mund të përdorësh një mjet për lundrim të sigurtë në internet, i projektuar për të filtruar kërcënimet e mundshme dhe për të siguruar që nuk mund të lundrosh tek ata.

4. Sulmet Phishing

Sulmet Phishing janë një formë e sulmeve të inxhinierisë sociale që është projektuar për të vjedhur të dhënat e përdoruesit, kredencialet e kartës së kreditit dhe lloje të tjera të informacionit financiar personal. Në shumicën e rasteve, këto sulme vijnë nga një burimi i perceptuar si i besuar, kur në të vërtetë ato janë të dizenjuara për të implikuar webfaqe me reputacion, institucione bankare dhe kontakte personale. Sapo t'i përgjigjeni këtyre mesazheve dhe të përdorni kredencialet tuaja ose të shkruani detajet tuaja financiare, informacioni do të dërgohet drejtpërdrejt tek burimin me qëllime të këqija.

ULTRANET SHPK
NIPT: L76625005G
Adresa: Rr. Branko Kadia, Nr.6, Shkodër
E-mail: info@ultranet.al
Mob: +355 682019201

Për të luftuar në mënyrë e duhur sulme phishing, vigjilenca është kritike. Për fat të keq, këto sulme të janë të vështira për t'u shmangur, por si rregull, ju duhet të jenë të kujdesshëm kur lexoni dhe hapni të gjitha emailet.

Të mos iu përgjigjeni email-ve mashtruese që ju bëjnë me dije se jeni fitues i një llotarie apo një çmimi të caktuar kur në të vërtetë ju nuk keni marrë pjesë në asnjë lojë apo shorte që të mundësojë një gjë të tillë. Zakonisht këto email-e kryhen në mënyrë automatike nga platforma kompjuterike të paidentifikuara jashtë vendit.

Para se të klikoni një lidhje të jashtme të postës elektronike, duhet të shikoni URL-në aktuale, pasi mund të jetë ndryshe nga teksti në email. Duhet të jeni 100% të sigurtë për burimin dhe fshini çdo email që ju duket mashtrues.