

Siguroni rrjetin pa tel (wireless)

Në botën e sotme, pothuajse të gjithë kanë të paktën një pajisje të lidhur me internetin. Me rritjen e numrit të këtyre pajisjeve të lidhura në internet, është e rëndësishme të zbatohet një strategji sigurie për të minimizuar potencialin e tyre për shfrytëzim nga hakerët. Pajisjet e lidhura me internetin mund të përdoren nga subjekte të liga për të mbledhur informacione personale, për të vjedhur identitete, për të kompromentuar të dhënat financiare dhe për të vëzhguar në heshtje përdoruesit. Marrja e disa masave paraprake në konfigurimin dhe përdorimin e pajisjeve ndihmon në parandalimin e sulmeve kibernetike.

Çfarë duhet të bëni për të minimizuar rreziqet për rrjetin tuaj pa tel?

1. *Ndryshoni fjalëkalimet e paracaktuara.*

Për të thjeshtuar konfigurimin, shumica e pajisjeve të rrjetit, duke përfshirë pikat e aksesit me valë, janë të para-konfiguruar me fjalëkalime të parazgjedhura të administratorit. Këto fjalëkalime të paracaktuara janë të disponueshme në internet. Ndryshimi i fjalëkalimeve të paracaktuara e bën më të vështirë përpjekjet e sulmuesit që të aksesojë pajisjen. Gjithashtu, përdorimi i fjalëkalimeve komplekse dhe ndryshimi periodik i tyre, është kryesore për mbrojtjen e pajisjes tuaj.

2. *Kufizoni aksesin.*

Lejoni të aksesojnë rrjetin tuaj vetëm përdoruesit e autorizuar. Përdorni llogarinë "guest", e cila është një veçori e përdorur gjerësisht në shumë ruterë me valë. Kjo veçori lejon t'u jepni miqve akses në valët e internetit në një kanal të veçantë me një fjalëkalim të veçantë, duke ruajtur privatësinë e kredencialeve tuaja kryesore.

3. *Enkriptoni të dhënat në rrjetin tuaj.*

Kriptimi i të dhënave tuaja me valë parandalon këdo që mund të jetë në gjendje të hyjë në rrjetin tuaj. Ekzistojnë disa protokolle enkriptimi për të siguruar këtë mbrojtje, si Wi-Fi Protected Access (WPA), WPA2 dhe WPA3, që kodojnë informacionin që transmetohet midis ruterave me valë dhe pajisjeve me valë. WPA3 është aktualisht kriptimi më i fortë. WPA dhe WPA2 janë ende të disponueshme, megjithatë këshillohet të përdorni pajisje që kanë si protokoll enkriptimi WPA3, pasi përdorimi i protokolleve të tjera mund ta lërë rrjetin tuaj të ekspozuar për sulme kibernetike.

4. *Mbroni identifikuesin e setit të shërbimit (SSID).*

Shmangni publikimin e SSID-së tuaj, për të parandaluar që të huajt të hyjnë lehtësisht në rrjetin tuaj. Të gjithë ruterat Wi-Fi lejojnë përdoruesit të mbrojnë SSID-në e pajisjes së tyre, gjë që e bën më të vështirë për sulmuesit gjetjen e një rrjeti. Ndryshoni SSID-në tuaj në diçka unike. Nëse lihet si në vlerën e paracaktuar nga prodhuesit, mund të lejojë një sulmues të identifikojë llojin e ruterit dhe ndoshta të shfrytëzojë çdo dobësi të njohur.

5. *Instaloni një mur zjarri (firewall).*

Duhet instaluar një muri zjarri në pajisjen tuaja me valë (një mur zjarri i bazuar në host), si dhe në rrjetin tuaj të shtëpisë (një mur zjarri i bazuar në router ose modem). Sulmuesit që përpiqen të sulmojnë drejtpërdrejt rrjetin tuaj pa tel mund të jenë në gjendje të anashkalojnë murin e

zjarrit të rrjetit tuaj - një mur zjarri i bazuar në host do të shtojë një shtresë mbrojtjeje për të dhënat në kompjuterin tuaj

6. *Mirëmbajtja e softuerit antivirus.*

Instaloni softuerin antivirus dhe mbajeni të përditësuar. Shumë programe antivirus kanë veçori shtesë që zbulojnë ose mbrojnë spyware dhe adware.

7. *Përdorni me kujdes shpërndarjen e skedarëve.*

Nëse nuk nevojitet, duhet të çaktivizohet shpërndarja e skedarëve ndërmjet pajisjeve. Gjithmonë duhet të lejoni shpërndarjen e skedarëve vetëm në rrjetet e shtëpisë ose të punës, asnjëherë në rrjetet publike.

8. *Mbajeni të përditësuar softuerin e pikës së aksesit tuaj.*

Prodhuesi i pikës suaj të aksesit me valë lëshon periodikisht përditësime dhe arnime (patch) për softuerin dhe firmware te pajisjes. Kontrolloni rregullisht faqen e internetit të prodhuesit që të bëni çdo përditësim ose arnim të pajisjes tuaj.

9. *Kontrolloni opsionet e sigurisë të ofruesit tuaj të internetit me valë dhe të prodhuesit të ruterit.*

Ofruesi i shërbimit të internetit dhe prodhuesi i ruterit ofrojnë informacione ose burime për të ndihmuar në sigurimin e rrjetit tuaj me valë. Kontrolloni suportin e klientit në faqet e tyre të internetit për sugjerime ose udhëzime specifike.

10. *Lidhu duke përdorur një Rrjet Virtual Privat (VPN).*

Shumë kompani dhe organizata kanë një VPN. VPN-të i lejojnë punonjësit të lidhen në mënyrë të sigurt me rrjetin e tyre kur janë larg zyrës. VPN-të kodojnë lidhjet në skajet dërguese dhe marrëse dhe mbajnë jashtë trafikun që nuk është i koduar siç duhet.