Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

Sfaturi esențiale de securitate a routerului

Îmbunătățiți securitatea rețelei dvs. cu câțiva pași de bază

By CTS Customized Training Solutions & CASE

Erasmus+

Urmând aceste sfaturi simple, puteți face rețeaua companiei dvs. mult mai sigură:

1. Uitați-vă la data de fabricare a routerului

Routerul dvs de încredere a fost alături de dvs de la începutul companiei tale? Îl tratezi ca pe un angajat de onoare? Înțelegem asta, chiar înțelegem! Dar atunci când securitatea afacerii dvs este în joc, nu mai este loc pentru a fi sentimental.

Nu există o modalitate ușoară de a determina dacă ar trebui să vă schimbați dispozitivul sau nu. Experții recomandă înlocuirea routerului la fiecare 2-3 ani, maximul absolut fiind de 5 ani. Ar trebui să vă schimbați imediat dispozitivul dacă acceptă doar un protocol de criptare despre care se știe că are vulnerabilități majore de securitate (mai multe informații despre acest subiect vor fi tratate mai târziu).

2. Actualizați firmware-ul

Cumpărați un router nou, configurați elementele de bază și apoi nu mai atingeți niciodată panoul de administrare? Cu toții am fost acolo! Dar există un motiv bun pentru a face check-in din când în când. Routerele, ca orice alt dispozitiv conectat la Internet, primesc actualizări constante de firmware. În timp ce unele dintre dispozitive se actualizează automat, altele necesită intervenția administratorului pentru a face acest lucru - dacă doar o lăsați așa, este posibil să pierdeți actualizări importante de securitate, care pot fi folosite de actori răi pentru a obține acces la rețeaua dvs.!

3. Dezactivați Wi-Fi Protected Setup (WPS)

În timp ce vizitați panoul de administrare, asigurați-vă că dezactivați WPS. Ce este WPS? Este o metodă de conectare a unui nou dispozitiv la rețea prin apăsarea unui buton fizic de pe router. Poate părea la îndemână (nu trebuie să memorați parola!), dar este foarte periculos să continuați. De ce?

WPS este cel mai comun mod printre hackeri de a obține acces neautorizat la rețeaua dvs. Multe instrumente de hacker se bazează exclusiv pe exploatarea WPS ca metodă de a încălca securitatea rețelei. Oprirea acestuia este unul dintre cei mai simpli și importanți pași pentru a vă menține rețeaua în siguranță!

4. Nu utilizați protocoale de criptare WEP sau WPA (dacă nu trebuie)

În timp ce vă configurați rețeaua Wi-Fi, sunteți întrebat dacă doriți să vă protejați prin parolă de rețea (trebuie făcut) și, dacă da, ce protocol de criptare doriți să utilizați. Acesta este locul în care cei mai mulți dintre noi începem să intrăm în panică, deoarece suntem bombardați de comenzi rapide enigmatice (WEP, WPA, WPA-PSK, WPA2-PSK și multe altele). De ce sunt atât de multe? Pe care să o aleg? Hai să răspundem la aceste întrebări!

Ca să fie simplu: protocoalele de criptare sunt o modalitate de a autoriza doar acele conexiuni care au cheia necesară (în cazul nostru, parola Wi-Fi) și de a le ține la distanță pe celelalte. WEP a fost primul ratificat

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Versiunea standard și începuturile sale merg până în 1999. A fost înlocuit de WPA (Wi-Fi Protected Access) în 2003, care a fost urmat de WPA2 în 2004. Din 2018, WPA3 a devenit disponibil pentru utilizare. Deci pe care ar trebui să-l folosiți? Răspunsul simplu este pe cel mai nou pe care îl acceptă routerul dvs. Dacă routerul dvs. permite doar utilizarea criptării WEP sau WPA, luați în considerare înlocuirea acestuia cât mai curând posibil. Ambele protocoale au vulnerabilități cunoscute care permit actorilor răi să vă acceseze rețeaua în doar câteva minute, folosind instrumente disponibile public. WPA2 este cel mai comun în acest moment, dar dacă intenționați să vă schimbați routerul în viitorul apropiat, obțineți un dispozitiv care acceptă Wi-Fi 6 și WPA3.

Deci, de ce sunt cei „periculoși” încă prin preajmă? Rețineți că dispozitivul care se conectează la router trebuie, de asemenea, să poată utiliza protocolul de criptare. Nu este neobișnuit ca o companie să folosească un anumit dispozitiv care poate funcționa numai pe un protocol mai vechi. Dacă acesta este cazul, luați în considerare crearea unei rețele suplimentare pentru ca dispozitivul respectiv să funcționeze pentru a evita compromiterea tuturor dispozitivelor dvs.

5. Creați o rețea separată pentru oaspeți

„Pot folosi Wi-Fi-ul dvs?” este o întrebare pe care o veți auzi mai devreme sau mai târziu în timp ce conduceți o afacere. Deși este o solicitare de înțeles (și total nevinovată) în 95% din timp, nu există niciodată suficientă prudență atunci când vine vorba de securitate, mai ales când majoritatea dispozitivelor moderne permit crearea unei rețele de invitați cu câteva apăsări de butoane. Amintiți-vă: deși oaspeții dvs. pot avea cele mai bune intenții, dispozitivele lor pot fi deja compromise fără știrea lor.

6. De fapt, utilizați o parolă pentru a vă proteja rețeaua ☺

Deși toate sfaturile de mai sus sunt importante, acesta este cel mai important. Toți acești pași nu vor funcționa dacă nu există o parolă, pentru început cu (puteți afla mai multe despre parolele sigure din setul nostru de instrumente Cele mai bune practici).

Mulțumim pentru atenție!

Erasmus+