OUCH! 2020. gada

SANS SECURITY AWARENESS

Ikmēneša informācijas drošības izdevums tev

Kā padarīt māju kiberdrošu

Pārskats

Pagātnē mājas tīkla izveide nebija nekas vairāk kā viena bezvadu maršrutētāja un pāris datoru uzstādīšana. Taču šodien daudzi no mums strādā, mācās vai izmanto internetu no mājām, tāpēc mums jāpievērš lielāka uzmanība mājas kiberdrošībai. Četri vienkārši padomi, kā to nodrošināt.

Jūsu bezvadu tīkls

Teju katras mājsaimniecības interneta tīkls sākas ar bezvadu interneta pieslēguma (Wi-Fi) risinājumu. Tieši šis risinājums ļauj jūsu iekārtām pieslēgties internetam. Pārsvarā mājas bezvadu tīklu kontrolē interneta maršrutētājs vai atsevišķs, īpašs bezvadu piekļuves punkts. Šīs abas iekārtas darbojas līdzīgi: pārraida bezvadu signālus, kas ļauj jūsu mājas ierīcēm pieslēgties internetam. Tas nozīmē, ka svarīgākā drošības atslēga, ir aizsargāt jūsu mājas bezvadu tīklu. Mēs iesakām sekojošus padomus, lai to aizsargātu.

- Nomainiet noklusējuma administratora paroli iekārtai, kura kontrolē jūsu bezvadu tīklu - interneta maršrutētājam vai bezvadu piekļuves punktam. Administratora konts ļauj konfigurēt bezvadu tīkla iestatījumus.
- Pārliecinieties, ka bezvadu tīklam var pieslēgties tikai tās ierīces, kurām uzticaties. Lai to panāktu, nodrošiniet augstu drošības līmeni. Tam nepieciešama parole, lai izveidotu savienojumu ar mājas tīklu un pēc tā izveides šifrētu tiešsaistes aktivitātes.
- Pārliecinieties, ka parole, kas tiek izmantota, lai pieslēgtos mājas tīklam, ir pietiekami sarežģīta un atšķiras no administratora paroles. Atcerieties, ka jūsu ierīces saglabā paroles, tāpēc tā ir jāievada tikai vienreiz katrai ierīcei.

Ja neesat pārliecināti, kā veikt šīs darbības, apmeklējiet sava interneta pakalpojumu sniedzēja tīmekļa vietni vai sava maršrutētāja vai bezvadu piekļuves punkta piegādātāja tīmekļa vietni.

Paroles

Izmantojiet stipru, unikālu paroli katrai savai ierīcei un tiešsaistes kontam. Atslēgas vārdi šeit ir *stipra* un *unikāla*. Jo garāka ir jūsu parole, jo tā ir drošāka. Mēģiniet izmantot vārdu sēriju, ko ir viegli atcerēties, piemēram, ***dzeltena-saule-debesīs***.

Unikāla parole nozīmē atšķirīgu paroli katrai ierīcei un tiešsaistes kontam. Lietojiet paroļu pārvaldnieku, lai tas atcerētos visas jūsu stiprās paroles. Paroļu pārvaldnieks ir drošības programma, un tā jūsu paroles glabā šifrētā virtuālā seifā.

Tāpat iesakām lietot divpakāpju autentifikāciju vienmēr, kad vien tā ir pieejama, it īpaši jūsu tiešsaistes kontiem. Tā izmanto jūsu paroli, taču tai pievieno arī otru autentifikācijas soli, piemēram, kodu, kas tiek nosūtīts uz viedtālruni, vai lietotni viedtālrunī, kas ģenerē jūsu kodu. Iespējams, šis ir pats svarīgākais solis, ko veikt, un tas ir daudz vieglāk, nekā jūs domājat.

Jūsu iekārtas

Nākamais solis ir noskaidrot, kādas ierīces ir pievienotas jūsu bezvadu mājas tīklam, un pārliecināties, vai visas šīs ierīces ir uzticamas un drošas. Tas ir pavisam vienkārši, ja mums ir tikai dators. Tomēr mūsdienās gandrīz jebko var pieslēgt mājas tīklam, ieskaitot viedtālruņus, televizorus, spēļu konsoles, bērnu monitorus, printerus, skaļruņus vai pat jaunāko modeļu automašīnas. Kad esat identificējuši visas mājas tīklam pieslēgtās ierīces, pārliecinieties, vai tās ir drošas. Labākais veids, kā to izdarīt, ir nomainīt noklusējuma paroles un, ja iespējams, aktivizēt iekārtu automātisko atjaunināšanu.

Rezerves kopijas

Dažkārt, lai arī cik rūpīgi jūs būtu, tomēr jūsu iekārtas var tikt uzlauztas. Ja tā ir noticis, tad parasti vienīgais veids, kā atgūt pazaudēto informāciju, ir atjaunot to no rezerves kopijām. Pārliecinieties, vai regulāri notiek jebkuras svarīgas informācijas dublēšana, un pārbaudiet, vai no šīm kopijām var veikt informācijas atjaunošanu. Lielākā daļa mobilo ierīču atbalsta automātisku datu dublēšanu mākonī. Savukārt, vairākumam datoru būs jāiegādājas kāda veida datu dublēšanas programmatūra vai pakalpojums. Tie parasti ir samērā lēti un vienkārši lietojami.

Viesredaktors

Randy Marchany ir Virginia Tech informācijas drošības speciālists. Viņš ir arī vecākais SANS instruktors un pasniedz SEC566, SEC440, un Kritisku drošības kontroles mehānismu ieviešanas un auditēšanas kursus. Sekojiet Randy @randymarchany.

Resursi

Kā padarīt paroles vieglāk iegaumējamas: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Paroļu pārvaldnieki: https://www.sans.org/security-awareness-training/resources/password-managers-0
Atjauninājumi: https://www.sans.org/security-awareness-training/resources/power-updating
Rezerves kopijas: https://www.sans.org/security-awareness-training/resources/got-backups
Iekārtas noklusējuma paroles: https://www.routerpasswords.com/

Tulkojums: CERT.LV