OUCH! 2025. gada janvāris

OUCH!

SANS SECURITY AWARENESS

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Viedās mājas ierīces: Bloķējiet tās, pirms to dara kibernoziedznieki

Digitālais murgs: Kibernoziedznieki jūsu mājās

Sāra un viņas ģimene bija sajūsmā par savām jaunajām viedajām mājas ierīcēm, priecājoties par iespēju viegli kontrolēt apgaismojumu un slēdzenes, izmantojot tikai dažus pieskārienus vai balss komandas. Tomēr kādu vakaru viņu sajūsma pārvērtās satraukumā – Sāra pamanīja, ka viņas viedais termostats negaidīti pats sevi noregulē. Sākotnēji viņa uztvēra to kā kļūmi, taču patiess nemiers pārņēma tad, kad sāka mirgot gaismas un noslēpumaini atvērās ieejas durvis. Situācija saasinājās, kad bērnu uzraudzības monitorā atskanēja sveša cilvēka balss, sīki aprakstot viņas bērna istabu. Tajā brīdī Sāra saprata, ka viņu mājoklis ir uzlauzts. Kibernoziedznieki bija pārņēmuši kontroli pār viņu viedajām ierīcēm, apdraudot viņu privātumu un drošību. Doma, ka svešinieki vēro viņas mazuļa miegu, lika Sārai justies neaizsargātai un apdraudētai. Satraucošā pieredze pastiprināja Sāras vajadzību aizsargāt gan viedās mājas ierīces, gan visas ģimenes drošību un mieru.

Kas ir viedās mājas ierīces?

Viedās mājas ierīces ir ar internetu savienotas ierīces un iekārtas, piemēram, termostati, drošības kameras, viedās slēdzenes, gaismas un, iespējams, pat veļas mazgājamā mašīna, kas padara mūsu mājas efektīvākas, ērtākas un dažkārt pat drošākas. Šīs ierīces tiek kontrolētas ar lietotņu, balss komandu vai automatizētu sistēmu palīdzību, piedāvājot vēl nebijušu komfortu.

Tomēr ērtības, ko tās sniedz, ir saistītas arī ar riskiem. Tā kā šīs ierīces ir savienotas ar internetu, tās ir ievainojamas, ja nav pienācīgi aizsargātas. Ja tās ir uzlauztas, iebrucēji var piekļūt jūsu personiskajai informācijai, izspiegot ikdienas darbības un pat kontrolēt fiziskās ierīces jūsu mājās.

Kāpēc ir tik svarīgi aizsargāt viedās mājas ierīces?

Viedo mājas ierīču drošība nav saistīta tikai ar pašu ierīču aizsardzību, bet gan ar visas jūsu mājsaimniecības aizsargāšanu. Kiberuzbrucēji bieži meklē mazāk aizsargātās ierīces un sāk ar tām. Kad ierīce ir kompromitēta, kiberuzbrucējs var izmantot uzlauzto ierīci, lai piekļūtu citām ierīcēm jūsu mājas tīklā, nozagtu sensitīvus datus vai pat atbloķētu jūsu durvis. Savstarpēji saistītajā pasaulē viedo ierīču aizsardzībai ir izšķiroša nozīme, lai saglabātu jūsu personīgo drošību, privātumu un sirdsmieru.

Piecas lietas, ko varat darīt, lai aizsargātu savas viedās mājas ierīces

1. **Nekavējoties mainiet noklusējuma paroles**: Daudzas viedās ierīces ir aprīkotas ar noklusējuma, rūpnīcas iestatītām parolēm, kas ir labi zināmas vai kuras viegli uzminēt kibernoziedzniekiem. Uzreiz nomainiet tās uz spēcīgām, unikālām parolēm un izmantojiet paroļu pārvaldnieku, lai tās saglabātu.

2. **Izveidojiet daudzfaktoru autentifikāciju (MFA), jo ar vienu vairs nepietiek**: Dažas viedās mājas ierīces pieprasa izveidot tiešsaistes kontu, lai piekļūtu ierīcei un to pārvaldītu. Aizsargājiet šos kontus ar MFA, kas nodrošina papildu drošības līmeni, pieprasot gan paroli, gan unikālu vienreizēju kodu, kas tiek nosūtīts uz tālruni. Kibernoziedznieki ienīst MFA, jo tas ievērojami apgrūtina viņu darbu.

3. **Nodrošiniet savām viedajām ierīcēm savu Wi-Fi tīklu**: Izveidojiet viedajām ierīcēm īpašu tīklu, kas būtu atdalīts no personīgajām vai darba ierīcēm. Daudzos Wi-Fi piekļuves punktos vai maršrutētājos to bieži sauc par viesu tīklu. Tas palīdz izolēt ierīces un ierobežo kaitējumu, ja kāda no tām tiek kompromitēta.

4. **Veiciet atjauninājumus, kad vien tie ir pieejami**: Ražotāji regulāri izlaiž atjauninājumus, lai novērstu drošības nepilnības. Pārliecinieties, ka jūsu ierīcēs ir jaunākās programmaparatūras un programmatūras atjauninājumi, lai saglabātu aizsardzību pret jauniem apdraudējumiem. Visvienkāršākais veids, kā to izdarīt, ir iespējot ierīcēs automātisku atjaunināšanu. Noteikti apsveriet iespēju nomainīt jebkuru ierīci, kas vairs netiek atbalstīta vai nesaņem drošības atjauninājumus no tās ražotāja.

5. **Izslēdziet neizmantotās funkcijas**: Viedajām ierīcēm bieži vien ir dažādas funkcijas, no kurām daudzas jūs, iespējams, nekad neizmantosiet. Jo vairāk funkciju jums ir aktīvas, jo vairāk kibernoziedzniekiem ir iespēju kā iekļūtu ierīcē. Izslēdziet visus nevajadzīgos pakalpojumus, piemēram, attālināto piekļuvi vai balss komandas, lai samazinātu ieejas punktus, kurus varētu izmantot kibernoziedznieki.

Jūsu viedajai mājai nav jākļūst par kibernoziedznieku rotaļu laukumu. Veicot tikai dažus soļus, jūs varat izbaudīt visu, ko piedāvā tehnoloģijas, un vienlaikus gulēt mierīgāk, zinot, ka kontrolējat situāciju.

Viesredaktore

Saja Sujita Venkatesana (Sai Sujitha Venkatesan) ir vecākā drošības inženiere Dell produktu drošības incidentu reaģēšanas komandā un WiCyS (Women in CyberSecurity) Silīcija ielejas organizācijas valdes locekle. Viņa aizrautīgi interesējas par visu, kas saistīts ar drošību, tostarp par darbaspēka daudzveidību. Linkedin: https://www.linkedin.com/in/saisujitha/

Resursi

Atjauninājumu spēks: https://www.sans.org/newsletters/ouch/power-updating/
Frāzveida paroļu spēks: https://www.sans.org/newsletters/ouch/power-passphrase/
Paroļu pārvaldnieku spēks: https://www.sans.org/newsletters/ouch/power-password-managers/

Tulkojums: CERT.LV