



NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS
KAIP UŽTIKRINTI DAIKTŲ INTERNETO ĮRENGINIŲ SAUGUMĄ

2020 m. spalio 28 d.

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos ragina piliečius tinkamai pasirūpinti naujai įsigytų įrenginių saugumu. Šiais laikais didelė dalis elektroninių prietaisų priklauso daiktų interneto (angl. *Internet of Things*, – *IoT*) grupei: išmanieji televizoriai, laikrodžiai, žaislai, telefonai ir planšetiniai kompiuteriai. Visa tai be abejo palengvina gyvenimą, prideda komforto, tačiau reikalauja dar didesnės informacijos sklaidos. Dalinamės keliais svarbiais patarimais, kuriais turėtų vadovautis kiekvienas, norintis padidinti savo daiktų interneto įrenginių saugumą.

NAUDOKITE SUDĖTINGĄ SLAPTAŽODĮ

Slaptažodžiai yra labiausiai paplitusi autentifikavimo forma ir dažnai tai vienintelė duomenų apsaugos priemonė. Kai kurie nauji prietaisai yra sukonfigūruoti su numatytais pagal nutylėjimą (angl. *default*) slaptažodžiais, kad palengvinti vartotojui jų įdiegimą. Šie slaptažodžiai pagal nutylėjimą yra lengvai randami internete, tad jie nesuteikia jokios apsaugos. Rinkitės stiprų ir sudėtingą slaptažodį norėdami apsaugoti savo įrenginį. Rekomenduojame paskaityti kitą mūsų informacinių biuletenį apie slaptažodžių svarbą bei kaip pasirinkti stiprų ir saugų slaptažodį: https://www.nksc.lt/doc/biuleteniai/NKSC_Slaptazodziu_saugumo_biuletenis.pdf

ĮVERTINKITE ĮRENGINIO NUSTATYMUS

Dauguma įrenginių siūlo įvairių funkcijų, kurias galite pritaikyti savo kasdienybėje. Įgalindami tam tikras funkcijas galimai sumažinate saugumą. Išjunkite funkcijas, kurių nenaudojate ar jums jos yra nereikalingos/perteklinės. Svarbu išnagrinėti įrenginio nustatymus, ypačingai



saugumo, ir išsirinkti tokias parinktis, kurios yra tinkamos jums ir nedidina grėsmių tikimybės. Jeigu įdiegiate kodą programai ištaisyti (angl. *patch*) ar naują programinę įrangą, arba sužinote kažką, kas gali turėti įtakos jūsų įrenginio saugai, iš naujo įvertinkite apsaugos nustatymus ir įsitikinkite, kad jie yra tinkami. Esant galimybei įgalinkite prieigą tik iš jūsų naudojamų IP adresų (angl. *allow list*).

ĮSITIKINKITE, KAD ĮDIEGTA NAUJAUSIA PROGRAMINĖ ĮRANGA

Įsitikinkite, kad jūsų įrenginiuose yra įdiegtos naujausios programinės įrangos versijos. Kartais programinėje įrangoje gali būti pažeidžiamumų. Kai gamintojai sužino apie jų produktų pažeidžiamumą, dažniausiai jie išleidžia atnaujinimą programai ištaisyti, kurį įsidiegti ištaisote tam tikras programinės įrangos spragas.

ĮRENGINĮ PRIE INTERNETO JUNKITE ĮVERTINĘ GALIMAS GRĖSMES

Įvertinkite galimas grėsmes jungdamiesi prie interneto: duomenų praradimą, įrenginio dalyvavimą kenkėjiškoje veikloje ir t.t. Piktavaliai gali pasinaudoti tuo, kad jūsų įrenginys yra prijungtas prie interneto ir išnaudoti galimai esamas įrenginio spragas tam, kad perimtų jautrią informaciją ar naudotųsi jūsų turimais prietaisais.

PAPILDOMI PATARIMAI

Dar keli patarimai, kurie padės jums apsaugoti savo daiktų interneto įrenginius:

- Pakeiskite maršrutizatoriaus gamyklinius nustatymus (tinklo pavadinimą, slaptažodžius). Daugiau informacijos rasite čia: https://www.nksc.lt/naujienos/nksc_rekomenduoja_pasikeisti_marsrutizatoriu_gamyk.html;
- Maršrutizatoriuose naudokite WPA3 arba WPA2 bevielio tinklo protokolus;
- Jeigu įmanoma, naudokite 2 žingsnių autentifikavimą. Daugiau informacijos apie šį būdą rasite jau minėtame biuletenyje: https://www.nksc.lt/doc/biuleteniai/NKSC_Slaptazodziu_saugumo_biuletenis.pdf