UKMERGĖS RAJONO SAVIVALDYBĖS
ADMINISTRACIJA
DUOMENŲ APSAUGOS PAREIGŪNAS

Biudžetinė įstaiga, Kęstučio a. 3, 20114 Ukmergė, tel. (8 340) 60302, faks. (8 340) 63370,
el. p. savivaldybe@ukmerge.lt; http:// www.ukmerge.lt
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188752174

Pagal adresatų sąrašą 2021-01-14 Nr. (6.23)18-165

REKOMENDACIJA DĖL ASMENS DUOMENŲ SAUGUMO UŽTIKRINIMO, NAUDOJANTIS BELAIDŽIAIS TINKLAIS

Nešiojamieji ir planšetiniai kompiuteriai, išmanieji telefonai ir kiti įrenginiai supa mus tiek darbe, tiek namuose. Įrenginiai su prisijungimo prie įvairių belaidžių tinklų galimybe tapo mūsų kasdienybe. Naudojimasis viešai prieinamais atvirais Wi-Fi technologija paremtais belaidžiais tinklais primena pokalbį viešoje vietoje, kur svetimi gali tave nugirsti. Jei nesiimsite atsargumo priemonių, prie atviro Wi-Fi tinklo prijungtas įrenginys jūsų duomenis ir informaciją siųs atviru tekstu, ir bet kas, turintis ir mokantis naudotis gana įprasta programine įranga, galės nesunkiai nuskaityti jūsų perduodamą konfidencialią informaciją, įskaitant ir jūsų slaptažodžius bei kitus prisijungimo prie paskyrų duomenis. O jei dar jūs tą patį slaptažodį naudojate kelioms paskyroms interneto svetainėse, tai gali tapti rimta problema, nes piktavalis, sužinojęs vienos jūsų paskyros duomenis, gali bandyti atspėti ir perimti jūsų kitų paskyrų duomenis.

Namų vartotojų Wi-Fi prieigos taškai taip pat gali būti nesaugūs, jei savininkas neįjungia savo įrenginyje šifravimo ir palieka tinklą atvirą. Net jei Wi-Fi tinklas turi slaptažodį, vis tiek tai negarantuoja saugumo, nes jūs bendrai naudojatės (dalijatės) šiuo tinklu su daugeliu žmonių, todėl jūsų duomenys gali būti nesaugūs. Nors dauguma maršruto parinktuvų (angl. router) turi integruotas ugniasienes, kurios apsaugo nuo grėsmių iš interneto, bet tai nereiškia, kad jos saugo nuo vartotojų, kurie yra tame pačiame tinkle, kaip ir jūs. Taigi, piktavalis, perėmęs jūsų duomenų srautą, gali sužinoti jūsų kompiuterio adresą (IP), vietą, vartotojo vardus ir slaptažodžius, kokias interneto svetaines lankote ir ką rašote el. paštu.

Remdamasi Valstybinės duomenų apsaugos inspekcijos pateiktomis rekomendacijomis bei išaiškinimais, pateikiu keletą patarimų, kuriuos įgyvendinę, apsaugosite savo naudojamus įrenginius ir juose esančius asmens duomenis bei kitą konfidencialią informaciją.

SAUGUMO PATARIMAI NAUDOJANTIS BELAIDŽIAIS TINKLAIS:

- Pati geriausia apsauga nuo nepatikimo tinklo nesinaudoti juo. Todėl jei tik galite, geriau naudokitės mobiliuoju 3G/4G internetu, o ne Wi-Fi tinklu. Su mobiliuoju 3G/4G internetu būsite saugesni. Savo telefone taip pat galite aktyvinti mobilaus prieigos taško (angl. Wi-Fi hotspot) arba pririšimo per USB (angl. tethering) funkcijas, jei, pavyzdžiui, prie interneto jungiatės su nešiojamuoju kompiuteriu (kuriame neturite interneto), o išmaniajame telefone turite galimybę naudotis mobiliuoju internetu.

• Naudokite HTTPS protokolą, kur tik galite. Naršydami interneto svetainėse ar naudodamiesi elektroninėmis paslaugomis, visur, kur reikia prisijungti, įvedant kokius nors paskyros ar kitus konfidencialius duomenis, naudokitės tik tomis svetainėmis, kurios užtikrina saugų šifruotą prisijungimą. Tokias svetaines atpažinsite iš adreso pradžioje esančios santrumpos https naršyklės URL adreso juostoje arba iš toje juostoje rodomo žalios spynelės ženklo. Tai reiškia, kad ši svetainė ar bent jau šis konkretus puslapis turi galiojantį skaitmeninį sertifikatą ir duomenų SSL/TLS šifravimą, todėl duomenų perdavimas tarp serverio ir naršyklės yra šifruojamas, o tai užtikrina, kad piktavaliui įsiterpti ir pakeisti ar perimti jūsų duomenis tampa žymiai sudėtingiau. Tuo atveju, jei adreso juostos priekyje žalios spynelės ar https nematote atsijunkite nuo naudojamų paskyrų arba visai prie jų nesijunkite, nes nėra užtikrinamas jūsų įvedamų duomenų perdavimo saugumas.

• Rūpinkitės turimos programinės įrangos atnaujinimu. Nepamirškite įsidiegti programinės įrangos atnaujinimų savo įrenginiuose, jei jie yra prieinami. Paprastai atnaujinimus siunčia programinės įrangos kūrėjai, kad ištaisytų programų pažeidžiamumus, kurie kelia grėsmę saugumui. Dažniausiai programinės įrangos atnaujinimą atlikti nėra sunku ir tai stipriai prisideda prie kibernetinio saugumo užtikrinimo.

• Palikti savo namų tinklo įrenginius nesaugius ar atvirus, tai tas pats, kaip palikti atrakintas ir atviras savo buto duris. Visi, kurie nori patekti į vidų (gauti prieigą), gali lengvai tai padaryti. Tuo metu be jūsų žinios jie turi ne tik prieigą prie jūsų namų tinklo išteklių (įrenginių), bet ir naudojasi jūsų interneto ryšiu. Be kita ko, jūs patys galite nukentėti, nes:

✓ Įsibrovėliai gali pavogti ir panaudoti piktiems tikslams jautrią asmeninę informaciją apie jus ir kitus žmones;

✓ Naudoti jūsų interneto ryšio pralaidumą jums nežinant ar pasinaudoti jūsų interneto ryšiu neteisėtiems veiksmams atlikti;

✓ Užkrėsti jūsų tinklą ar įrenginius virusais ar kitokia kenkimo programine įranga.

✓ Jūs galite tapti atsakingas dėl, pasinaudojus jūsų įranga, atliktų kibernetinių nusikaltimų;

✓ Jūsų namų tinklas gali tapti netinkamas naudoti dėl atsisakymo aptarnauti atakos (angl. denial of service (DoS)).

• Pakeiskite visus numatytus slaptažodžius ir vartotojų vardus. Šiais laikais visi maršruto parinktuvai ar belaidžio tinklo prieigos taškai turi įdiegtą prieigą per naršyklę prie jų valdymo aplinkos ir nustatymų įrankių. Jūs įvedate įrenginio adresą tinkle į naršyklę, suvedate lange paskyros prisijungimo duomenis ir gaunate prieigą prie įrenginio.

• Niekada nepalikite įrenginiuose įrangos gamintojo tipinių numatytų slaptažodžių ir vartotojų vardų. Įsibrovėliai gana lengvai internete gali susirasti tipinius gamintojo naudojamus prisijungimo duomenis ir jais pasinaudodami, perimti jūsų įrenginio kontrolę ir pasinaudoti juo, kad jums pakenktų ar kitaip sutrikdytų jūsų įrangos darbą.

• Rinkitės stiprų slaptažodį, kurį būtų sunku ar net neįmanoma atspėti. Keiskite ji nors kas 90 dienų arba tada, kai kyla įtarimų, kad slaptažodį kas nors sužinojo. Venkite pakartotinai naudoti jau buvusius slaptažodžius.

• Aktyvinkite tinklo šifravimo sistemą. Nors skirtingos įrangos nuostatos gali skirtis, tačiau pastaruoju metu visi Wi-Fi galintys teikti įrenginiai komplektuojami su kokios nors formos šifravimo technologijomis. Šifravimo technologijos veikia taip, kad įslaptintų visą jūsų tinklu siunčiamą informaciją, kad įsibrovėliams ar atsitiktiniams žmonėms ji taptų kuo sunkiau perskaitoma.

• Pakeiskite tinklo pavadinimą ir išjunkite SSID transliavimą. Kartu su prisijungimo informacija, kaip antai, vartotojo vardas ir slaptažodis, kiekvienas Wi-Fi įrenginys saugo dar ir numatytąjį tinklo pavadinimą, vadinamąjį SSID (angl. service set identifier). Neturėdamas jūsų tinklo pavadinimo įsibrovėlis sunkiau į jį pateks, todėl numatytąjį tinklo pavadinimą privalu pasikeisti.

• Apsvarstykite galimybę įjungti MAC adresų filtrą. Kiekvienas Wi-Fi ryšio paslaugomis besinaudojantis įrenginys yra susietas su savo unikaliu identifikatoriumi fiziniu adresu, kuris vadinamas MAC (angl. media access control) adresu. Vienas iš maršruto parinktuvo darbų valdyti

įrenginių (nešiojamojo kompiuterio, išmaniojo telefono ir t. t.), kurie naudojasi belaidžiu ryšiu, kad prisijungtų prie interneto, MAC adresus. Kai MAC adresų filtravimas yra įjungtas, maršruto parinktuvas, turėdamas patvirtintų įrenginių sąrašą, patikrina kiekvieną naujai aptiktą įrenginį. Įrenginys, nesantis sąraše, negauna prieigos.

• Apsvarstykite galimybę įrenginiams priskirti statinius kompiuterio adresus (IP) Kalbant apie IP adresų priskyrimą įrenginiams, kurie pasiekiami jūsų namų tinkle, yra du pasirinkimai galima automatiškai kiekvienam įrenginiui priskirti IP adresą, naudojantis DHCP (angl. dynamic host configuration protocol), arba IP adresą galima priskirti rankiniu būdu. Dažnai pasirenkama DHCP, nes taip paprasčiau ir lengviau, tačiau svarbu suprasti, kad įsibrovėliai jūsų tinkle taip pat gali pasinaudoti DHCP, kad gautų galiojantį IP adresą. Verta apsvarstyti galimybę naudoti rankiniu būdu suteikiamą statinį IP adresą kiekvienam įrenginiui, suteikiant juos iš fiksuoto ribotos apimties adresų intervalo.

• Apribokite maršruto parinktuvo konfigūravimo galimybes ir atnaujinkite įrenginio programinę įrangą Siekiant sumažinti grėsmes, rekomenduotina, jei įrenginyje įdiegta tokia galimybė, uždrausti prisijungti prie maršruto parinktuvo valdymo (konfigūravimo) aplinkos iš interneto ar to paties belaidžio tinklo. Pakanka palikti galimybę konfigūruoti įrenginį naudojantis tik laidinių kompiuterių tinklu.

SAUGUMO PATARIMAI NAUDOJANTIS BLUETOOTH RYŠIU:

• Išjunkite Bluetooth ryšio funkciją, jei jos nenaudojate. Jeigu nesinaudojate Bluetooth technologija, tačiau jūsų turimas įrenginys šią funkciją palaiko, reiktų įsitikinti, kad Bluetooth yra išjungtas. Išjungta nenaudojama Bluetooth funkcija padės taupyti įrenginio akumuliatoriaus veikimo laiką iki kito įkrovimo. Tuo atveju, kai Bluetooth įrenginio aptikimas yra įjungtas, jį gali matyti ir bandyti pasiekti aplinkui esantys įrenginiai. Perjungus Bluetooth įrenginį į neaptikimo režimą, sumažėja bandymų neteisėtai prisijungti.

• Atidžiai atlikite įrenginių suporavimą. Bluetooth technologija yra pagrįsta poravimo principu, t. y. su norimu valdyti įrenginiu reikia sudaryti porą naudojant tą patį įvestą PIN kodą. Piktavaliai gali bandyti pasinaudoti socialine inžinerija, norėdami perimti jūsų įrenginio kontrolę. Būkite atidūs ir jei gaunate įtartiną Bluetooth pranešimą ar prašymą susiporuoti, nors to pats neinicijavote, tiesiog ignoruokite ar visai išjunkite Bluetooth ryšio funkciją.

Kuo daugiau pateiktų patarimų įgyvendinsite, tuo stipresnis ir saugesnis bus jūsų tinklas. Net ir panaudoję tik kelis iš jų žymiai sustiprinsite tinklo saugą. Geriau apsaugoti įrenginiai padės geriau apsaugoti jūsų asmens duomenis bei konfidencialią informaciją.

Duomenų apsaugos pareigūnė Kristina Karpovienė

Kristina Karpovienė, (8 340) 68392, kristina.karpoviene@ukmerge.lt