REKOMENDACIJA

ASMENS DUOMENŲ IR PRIVATUMO APSAUGA NAUDOJANTIS BELAIDŽIAIS TINKLAIS

ĮŽANGA

Skaitmeniniame pasaulyje mūsų privatumas ir asmens duomenų saugumas yra gana trapus, todėl svarbu tuo rūpintis ir skirti pakankamai dėmesio. Įrenginiai su prisijungimo prie įvairių belaidžių tinklų galimybe tapo mūsų kasdienybe. Nešiojamieji ir planšetiniai kompiuteriai, išmanieji telefonai, televizoriai ir kiti įrenginiai supa mus darbe, namuose ar kelionėse.

Belaidžiai tinklai pasižymi tuo, kad jų perduodami signalai sklinda ore, todėl yra didesnė tikimybė, kad jais perduodamą asmeninę informaciją ar duomenis gali bandyti perimti tretieji asmenys. Naudojantis specialiomis programomis galima nuskaityti perduodamų duomenų srauto turinį ir jame rasti vartotojo perduodamus asmens duomenis bei juos panaudoti piktavališkais tikslias.

Naudojimasis viešai prieinamais atvirais Wi-Fi technologija paremtais belaidžiais tinklais šiek tiek primena pokalbį viešoje vietoje, kur svetimi gali tave nugirsti. Jei nesiimsite atsargumo priemonių, prie atviro Wi-Fi tinklo prijungtas įrenginys jūsų duomenis ir informaciją ko gero 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.

Kita pasitaikanti potenciali grėsmė – netikras Wi-Fi prieigos taškas, vadinamoji „medaus puodynė“, kurio paskirtis – suvilioti jus prisijungti prie jo, kad galėtų perimti jūsų siunčiamą duomenų srautą. Tokie prieigos taškai dažniausia turi paprastus, viliojančius pavadinimus arba pavadinimus, skambančius panašiai kaip netoliese esančio tikro Wi-Fi prieigos taško.

Jei Wi-Fi belaidžiame tinkle jūsų neprašo įvesti slaptažodžio ar prisijungimo duomenų, tai toks tinklas yra neapsaugotas. Neapsaugotų Wi-Fi prieigos taškų (tinklų) galite rasti kavinėse, oro uostų salėse, prekybos centruose ir panašiose vietose, taip pat viešbučiuose ar įvairiose verslo įmonėse, kurios teikia savo klientams nemokamą interneto ryšį. 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.

1 pav. Simboliai, kurie parodo viešojo Wi-Fi tinklo prieigą

SAUGUS NAUDOJIMASIS VIEŠAISIAIS BELAIDŽIAIS TINKLAIS

Prieš prisijungdami prie viešo Wi-Fi tinklo, visada pabandykite patikrinti tinklo autentiškumą. Rinkitės tuos tinklus, kuriuos teikia jums žinomos įmonės ir tiksliai žinote tinklo pavadinimą bei prisijungimo duomenis.

Jei Wi-Fi tinklas, prie kurio norite prisijungti, jums nežinomas, pavyzdžiui, viešbutyje ar oro uoste, nebijokite paklausti tikslaus tinklo pavadinimo ir slaptažodžio. Jei abejojate, ar jums neaišku, prie kurio tinklo turėtumėte jungtis, geriau nesijunkite. Jūsų duomenų saugumas yra svarbus veiksnys, todėl venkite nereikalingos rizikos.

Jei Wi-Fi tinklas prisijungiant neprašo slaptažodžio, vadinasi jis yra neapsaugotas ir informacija juo perduodama nešifruota, atviru tekstu. Venkite naudotis tokiais tinklais, o jei naudojatės, tuo metu nesijunkite prie tinklalapių ar nesinaudokite e. paslaugomis, kur reikia įvesti jūsų paskyros duomenis. Taip pat venkite jungtis prie elektroninės bankininkystės paskyros ar atlikti finansines ir elektroninės prekybos operacijas, kai esate prisijungę prie neapsaugoto Wi-Fi tinklo.

Toliau pateikiama keletas patarimų, kaip naudotis belaidžiais tinklais, kad jūsų asmens duomenys būtų saugesni.

Naudokite savo Wi-Fi tinklą ar mobilų 3G/4G internetą

Pati geriausia apsauga nuo nepatikimo tinklo – nesinaudoti juo. Jei tik galite, geriau naudokitės mobiliuoju 3G/4G internetu, o ne Wi-Fi tinklu. Su mobiliuoju 3G/4G internetu būsite saugesni. Žinoma, neretai mobilusis internetas turi greičio ir duomenų srauto apribojimų, tačiau jei turite galimybę, teikite prioritetą ryšio paslaugoms, kurioms teikti naudojami mobiliojo ryšio tinklai. 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 e. 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.

HTTPS protokolą automatiškai naudoti jums padės „HTTPS Everywhere“ naršyklių plėtinys. Ji galite parsisiųsti iš čia: https://www.eff.org/https-everywhere.

Apsvarstykite galimybę naudotis VPN paslaugomis

Deja, ne visos interneto svetainės naudoja HTTPS protokolą ir SSL/TLS šifravimą. Jei jums reikia papildomos apsaugos ir privatumo ar jūs dažnai perduodate konfidencialius duomenis, pagalvokite apie galimybę naudotis VPN (angl. *virtual private network*) paslaugomis.

Naudojantis VPN paslauga, visas jūsų duomenų srautas, prieš patekdamas į internetą, bus nukreipiamas per atskirą, saugų ir privatų tinklą. Tai suteiks jums tokį saugumą, tarsi veiktumėte vidiniame privačiame tinkle, nors iš tikro jūs naudositės viešuoju tinklu.

Teikiamos VPN paslaugos būna įvairios. Rekomenduojame rinktis tuos paslaugos tiekėjus, kurie užtikrina, kad nesaugo vartotojų aktyvumo ir naudojimosi žurnalų (angl. *no logs policy*) ir teikia automatinio išjungimo funkciją, jei netikėtai yra pertraukiamas jūsų ryšys (angl. *kill switch*).

Išjunkite failų dalijimąsi tinkle ir įjunkite ugniasienę

Kai esame namie ir dirbame kompiuteriu, bendrai naudotis (angl. *sharing*) įvairiais failais ar spausdintuvu yra patogu ir įprasta, tačiau, kai naudojamės viešais Wi-Fi tinklais, tai gali būti nesaugu. Rekomenduojame išjungti ir tinklo įrenginių aptikimo funkciją (angl. *network discovery*). Šie nustatymai padės jūsų įrenginiui būti mažiau matomam tinkle.

Dažnai įrenginiuose yra integruotos bent jau bazines funkcijas turinčios ugniasienės (angl. *firewall*). Įsitikinkite, kad jos įjungtos. Tai taip pat šiek tiek padidins jūsų saugumą tinkle.

Naudokite dviejų faktorių (2FA) autentifikaciją

Dviejų ar daugiau faktorių autentifikacija yra papildomas saugos veiksmas, kurį turite atlikti, norėdami prisijungti prie savo paskyros. Paprastai šis saugos veiksmas reikalauja įvesti saugos kodą, kurį gavote telefonu prieš prisijungdami.

Papildomas autentifikavimo būdas sumažins grėsmę, kad jūsų svarbių paskyrų prisijungimo duomenys bus atskleisti. Esant aktyvintai dviejų faktorių autentifikacijai, įsibrovėlis negalės gauti prieigos prie jūsų paskyros net ir sužinojęs jūsų prisijungimo vardą bei slaptažodį.

Atsižvelgiant į tai, kokias paslaugas naudojate, galite aktyvinti papildomą autentifikaciją SMS, naudojantis programėle ar net specialia USB atmintine. Rekomenduojame naudoti šį saugos būdą visoms svarbioms paskyroms, su kuriomis galite prisijungti prie jums svarbių paslaugų ar pasiekti savo jautrius asmens ar finansinius duomenis.

Interneto svetainėje https://twofactorauth.org/ galite pamatyti, kokios interneto paslaugos, kokius autentifikavimo metodus palaiko.

Naudokite ištisinį užšifravimą

Ištisinio užšifravimo (angl. *end to end encryption*) ryšio technologija sukurta taip, kad niekas negalėtų perskaityti siunčiamo pranešimo, išskyrus siuntėją ir gavėją. Pranešimas yra apsaugotos užraktu ir tik gavėjas bei siuntėjas turi specialų šifravimo raktą, reikalingą pranešimui atrakinti ir jį perskaityti. Kiekvienas išsiųstas pranešimas turi unikalų užraktą ir raktą.

Ši technologija yra labai svarbi, siekiant užtikrinti savo pokalbių privatumą, naudojantis žinučių siuntimo programėlėmis internete. Naudokite tik tas žinučių siuntimo programėles, kuriose jau yra aktyvintas arba galima aktyvinti ištisinį užšifravimą.

Išjunkite Wi-Fi ryšį, kai jo nereikia

Rekomenduojame nebūti prisijungus prie Wi-Fi tinklo, kai nesinaudojate internetu. Jei jums ryšys nebereikalingas, tiesiog atsijunkite nuo jo. Kuo ilgiau jūs esate tinkle, tuo labiau esate matomas ir labiau dominate tuos, kurie naudoja kenkėjišką programinę įrangą.

Atsijungę nuo Wi-Fi ar visiškai išjungę belaidžio tinklo funkciją, jūs pailginsite savo įrenginio akumuliatoriaus veikimo laiką.

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.

NAMŲ BELAIDŽIO TINKLO SAUGUMO UŽTIKRINIMAS

Kruopščiai sukonfigūruoti namų tinklo įrenginius užima daugiau laiko, negu daugelis norėtume, tad dažniausiai mes skubame ir neskiriame tam daug dėmesio ir laiko. Kodėl svarbu sukonfigūruoti visus skirtingus parametrus ir kas blogo gali nutikti, jei mes tiesiog paliksime įrenginiuose numatytuosius nustatymus?

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 (angl. *malware*) 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)*);

Kartais klaidingai manoma, kad visi belaidžiai tinklai ir maršruto parinktuvai iš principo yra nesaugūs arba bent jau mažiau saugūs, negu alternatyvūs tinklai. Tai yra tiesa tuo atveju, jei jūs naudojate įrangą, kurioje palikti visi standartiniai gamintojo (angl. *default*) parametrai.

Patikrinkite ir susikonfigūruokite tinklo įrenginių saugos parametrus, taip jūsų namų tinklas taps saugesnis. Svarbu įsitikinti, kad jūsų naudojamas maršruto parinktuvas palaiko šias funkcijas:

- ***WPA2 saugos šifravimas*:** WPA2 šifravimo metodas būtų puikus pasirinkimas, siekiant apsisaugoti nuo įsilaužimų. Rinkitės maršruto parinktuvą, palaikantį WPA2 šifravimo metodą. Šis pasirinkimas bus saugesnis už WPA, o ypač už WEP metodą, kuris pripažįstamas kaip visiškai nebesaugus ir jo primygtinai rekomenduojama niekur nenaudoti.
- ***Tinklo adresų keitimas*** (angl. *network address translation (NAT)*): tinklo adresų keitimas (vertimas) padeda atskirti jūsų vidinį kompiuterių tinklą nuo interneto (išorinio tinklo). Tai padeda apsaugoti jūsų kompiuterius ir kitus prijungtus įrenginius vidiniame kompiuterių tinkle nuo atakų, kai įsibrovėliui reikia tiesioginės komunikavimo sąsajos su įrenginiu. Įdiegus NAT, ataka toliausiai galės nukeliauti tik iki jūsų maršruto parinktuvo ir neturės galimybės tiesiogiai susisiekti su įrenginiu vidiniame tinkle.
- ***Integruota apsauga nuo grėsmių*:** tai vienas iš geriausių būdų saugotis nuo kenkimo programinės įrangos dar prieš jai patenkant į jūsų vidinį tinklą. Tai sustiprins jūsų apsaugą nuo šnipinėjimo programinės įrangos, virusų ir kitų grėsmių.
- ***Įdiegta ugniasienė*:** įdiegta ugniasienė apsaugos jus nuo įvairių grėsmių, atskirdama (blokuodama) nepageidaujamą duomenų srautą, einantį per jūsų įvadinį įrenginį, nuo tinkamo srauto. Bet koks įeinantis bandymas prisijungti, kuris nėra tinkamai autorizuotas, bus atmestas.

PATARIMAI BELAIDŽIO NAMŲ TINKLO SAUGUMUI PADIDINTI

Gal prireikė sukonfigūruoti naujai įsigytą maršruto parinktuvą ar belaidžio tinklo prieigos tašką, o gal tiesiog norite pagerinti jau turimos įrangos saugumą, toliau pateikiami žingsniai, kuriuos privalu atlikti.

Kuo daugiau pateiktų patarimų įgyvendinsite, tuo stipresnis ir saugesnis bus jūsų tinklas. Net ir panaudoję tik kelis iš jų – žymiai sustiprinsite tinklo saugą.

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. Tai padaryti gali net ir neprofesionalus įsilaužėlis – jūsų įrangos darbą gali sutrikdyti tiek jūsų nemėgstantis kaimynas, tiek smalsaujantis vaikas.

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. Geriau naudokite slaptažodžių šabloną, kad galėtumėte lengviau atsiminti, ar slaptažodį frazę, tačiau stenkitės, kad tai taip pat nebūtų lengvai atspėjama sistema.

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 (populiarūs jau pirmiau paminėti WPA2 ir WPA pavyzdžiai). Šifravimo technologijos veikia taip, kad įslaptintų visą jūsų tinklu siunčiamą informaciją, kad įsibrovėliams ar atsitiktiniams žmonėms ji taptų kuo sunkiau perskaitoma.

Pasirinkite stipriausią šifravimo metodą, prieinamą jūsų tinkle (tinklo įrangoje). Kuo stipresnį šifravimą pasirinksite, tuo sunkiau bus net ir su profesionaliomis įsilaužimo programomis gauti jūsų šifravimo raktus, tad jūsų tinklas bus saugesnis.

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. Patariama jį kuriant nenaudoti adreso, įstaigos pavadinimo ar kitos su jumis susijusios informacijos, kad būtų sunkiau atspėti jūsų tinklo pavadinimą.

Paliktas gamintojo numatytasis tinklo pavadinimas įsibrovėliams tarsi signalizuoja apie tai, kad galbūt jūs nepakeitėte ir kitų numatytųjų nustatymų, kaip antai, prisijungimo paskyros duomenų ar panašiai, todėl galimai esate „lengvas taikinys“.

Įprastomis aplinkybėmis maršruto parinktuvas reguliariais intervalais transliuoja su juo susijusio tinklo pavadinimą (angl. *SSID broadcasting*). Tai leidžia matyti ir bandyti pasiekti netoliese esančius tinklus, kai ieškome aplink Wi-Fi signalo. Ši funkcija praverčia įstaigoms, viešbučiams ir panašiai, bet tikrai nebūtina namų tinkle. Įprastai šią funkciją įrenginiuose galima įjungti arba išjungti. Tikrai pakanka tik jums žinoti savo tinklo pavadinimą, o svečių įrenginius galėsite prijungti pats. Taigi, išjungus jūsų tinklo pavadinimo rodymo funkciją, jūsų tinklas bus saugesnis, nes apie ji žinos ir jį matys mažiau žmonių.

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.

Nustatykite, ar jūsų prieigos taškas yra geroje vietoje

Normalu ar net pageidautina, kad jūsų namų Wi-Fi signalas apimtų namų vidų ir net šiek tiek išeitų į išorę, tačiau patartina kuo mažiau signalo teikti už norimos teritorijos ribų, kad jūsų signalas nebūtų lengvai aptinkamas ir juo būtų sunku pasinaudoti pašaliniams be jūsų leidimo.

Verta pagalvoti, kur jūsų namuose būtų gera vieta maršruto parinktuvui (prieigos taškui). Tinkamiausia vieta buto ar namo viduryje, o ne prie lango ar sienos. Kuo sunkiau bus pašaliniams pasiekiamas Wi-Fi signalas, tuo mažiau bus pagundos jiems bandyti įsibrauti.

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.

Techninės įrangos gamintojai periodiškai išleidžia programinės įrangos atnaujinimus. Atnaujinimai ne tik papildo įrenginio funkcionalumą, bet ir ištaiso žinomus pažeidžiamumus, kuriais, jei atnaujinimai būtų neįdiegti, galėtų pasinaudoti įsilaužėliai.

Išjunkite belaidį tinklą, jei visai ar ilgesnį laiką jo nenaudojate

Daugelis namuose belaidį tinklą laiko įjungtą visą laiką. Priežastis paprasta – mes tiesiog norime arba mums reikia visą laiką būti pasiekiamiems internetu (angl. *online*), tačiau nebūtina palikti įjungto belaidžio ryšio, jei jūsų nėra namuose ilgą laiką, pavyzdžiui, jei išvykstate ilgesniam laikui atostogų ar į komandiruotę.

Įsilaužėlis negalės pasinaudoti belaidžiu ryšiu, jei jis bus neaktyvus, taigi, negalės įsilaužti ir į jūsų įrenginius, ir jums nereikės jaudintis, kad ko nors nenutiktų, kol būsite išvykęs. Išjungtas belaidis ryšys gali jums padėti sutaupyti pinigų, jei jūs mokate už interneto duomenų kiekį, nes, jums nesant namuose, niekas negalės pasinaudoti jūsų interneto ryšiu. Išvykdami ilgesniam laikui išjungę belaidį ryšį apsaugosite savo įrangą nuo panaudojimo neteisėtiems tikslams ar sugadinimo.

SAUGUMAS NAUDOJANTIS „BLUETOOTH“ RYŠIU

„Bluetooth“ belaidė technologija suteikia galimybę sujungti mobiliuosius įrenginius, tokius kaip nešiojamieji kompiuteriai ar įvairūs išmanieji įrenginiai, kaip antai, telefonai, televizoriai, laikrodžiai, ausinės ir kiti įrenginiai, nedideliu apie 100 metrų atstumu.

2 pav. Simbolis, kuris parodo „Bluetooth“ ryšio technologiją

Išjunkite „Bluetooth“ ryšio funkciją, jei jos nenaudojate

Jeigu nesinaudojate „Bluetooth“ technologija, tačiau jūsų turimas įrenginys šią funkciją palaiko, reiktų įsitikinti, kad „Bluetooth“ yra išjungtas. Įsijunkite šią funkciją tik tada, kai reikia, o baigę naudotis – vėl išjunkite. Išjungta nenaudojama „Bluetooth“ funkcija padės taupyti įrenginio akumuliatoriaus veikimo laiką iki kito įkrovimo.

Įjunkite „Bluetooth“ neaptikimo režimą

„Bluetooth“ apsaugos mechanizmas leidžia vartotojui pasirinkti, ar įrenginys gali būti aptiktas iš šalies. 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 įrenginių „poravimą“ atlikite įsitikinę, kad to jums tikrai reikia. Jei gaunate įtartiną „Bluetooth“ pranešimą ar prašymą susiporuoti, nors to pats neinicijavote, tiesiog ignoruokite ar visai išjunkite „Bluetooth“ ryšio funkciją.

Žinoma, niekas negali garantuoti 100 proc. apsaugos nuo įsilaužėlių, tačiau tinkamų priemonių ir pakankamo jų kiekio panaudojimas yra gera pradžia.

Kuo sunkiau įsibrovėliams gauti prieigą prie jūsų kompiuterinės įrangos, tuo mažiau tikėtina, kad jie norės vargti mėgindami prisijungti prie jūsų įrenginių. Geriau apsaugoti įrenginiai padės geriau apsaugoti ir jūsų asmens duomenis bei privačią informaciją.

Parengė Valstybinės duomenų apsaugos inspekcijos
Informacijos ir technologijų skyriaus vyriausiasis specialistas Valdas Šulinskas
Inspekcijos adresas internete *https://www.ada.lt*