Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS
WI-FI TINKLO APSAUGOS PATARIMAI ORGANIZACIJOMS

2019 m. gruodžio 13 d.

Nuo 2018 metų birželio ne pelno siekianti organizacija „Wi-Fi Alliance“ pradėjo sertifikuoti įrenginius, palaikančius „Wi-Fi Protected Access 3“ saugumo protokolą (toliau – WPA3). NKSC vertinimu, siekiant užtikrinti organizacijos tinklo kibernetinį saugumą, yra tikslinga naudotis naujausiomis kibernetinio saugumo technologijomis, juolab WPA3 palaikantys įrenginiai rinkoje yra lengvai prieinami.

Kas yra organizacijos tinklo apsauga?

Organizacijos kompiuterinio tinklo (toliau - tinklas) apsauga apima tinklo, apjungiančio sistemas, tarnybinių stočių, kompiuterizuotų darbo vietų ir tokių įrenginių, kaip išmanūs telefonai ir planšetiniai kompiuteriai, apsaugą. Atsižvelgiant į tai, kad tinklai nuolat kinta, dėmesys jų apsaugai išlieka vienu pagrindinių tinklo kibernetinio saugumo prioritetu.

Su kokiomis saugumo grėsmėmis susiduria organizacijų bevieliai tinklai?

Laidiniai tinklai dažniausiai turi pakankamas apsaugos priemones: ugniasienes, įsilaužimo aptikimo sistemas, antivirusines programines įrangas, „Proxy“ tarnybines stotis ir kitas apsaugos priemones. Belaidei tinklo prieigai (toliau – Wi-Fi) dažniausiai skiriamas nepakankamas dėmesys kibernetinio saugumo atžvilgiu, todėl ji gali būti lengvai pažeidžiama ir panaudota įsilaužimui į vidinį organizacijos tinklą. Kibernetiniai programišiai, nusikaltėliai,

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

pasinaudoję Wi-Fi tinklo prieigos tašku, gali patekti į vidinį organizacijos tinklą ir vykdyti įvairią kenkėjišką veiklą, pvz.: paketų šniukštinėjimą (angl. „packet sniffing“), netikrų prieigos taškų sukūrimą, slaptažodžių vagystes, intelektualinės nuosavybės, komercinės paslapties vagystes ir pan. Šios atakos gali sutrikdyti tinklo veiklą, lėtinti procesus, vykstančius tinkle, ar net visiškai paralyžiuoti tinklą.

Kaip galima sumažinti Wi-Fi tinklo kibernetinio saugumo rizikas?

Bevielio tinklo saugumo protokolai yra nuolatos tobulinami. Šiuo metų populiariausias Wi-Fi apsaugos protokolas yra „Wi-Fi Protected Access 2“ (toliau – WPA2). 2018 m. birželio mėnesį pasirodęs WPA3 turi pakeisti WPA2. Organizacijos, naudodamos „WPA3-Enterprise“ protokolą, gali užtikrinti didesnį saugumą. „WPA3-Enterprise“ remiasi WPA2 ir užtikrina nuoseklų saugos protokolų taikymą tinkle.

Wi-Fi apsaugos rekomendacijos:

- kiekviename tinkle įdiegti bevielio tinklo įsilaužimo aptikimo (angl. „Wireless intrusion detection system“) (toliau - WIDS) ir belaidžio tinklo įsilaužimo prevencijos (angl. „Wireless intrusion prevention system“) (toliau - WIPS) sistemas;
- įsitikinti, kad naudojama techninė ir programinė įranga neturi žinomų pažeidžiamumų, esant poreikiui – nedelsiant atnaujinti;
- naudoti tik tą techninę ir programinę įrangą, kuri turi galimybes ją saugiai konfigūruoti;
- naudoti šifravimą ten, kur tai įmanoma;
- įgalinti kelių faktorių autentifikavimą prieigai prie tinklo. Jeigu to padaryti neįmanoma, apsvarstykite kitas saugaus autentifikavimo priemones, nesusijusias su vienu bendruoju slaptažodžiu, pvz. „Active Directory“ slaptažodžiu;
- naudoti EAP-TLS (angl. „Extensible Authentication Protocol-Transport Layer Security“) sertifikato pagrindu (arba geresnio) veikiančias priemones ir metodus viso autentifikavimo proceso apsaugai;
- naudoti CCMP (angl. „Counter Mode Cipher Block Chaining Message Authentication Code Protocol,“) ar modernesnę šifravimo technologiją;
- sukurti svečiams skirtą Wi-Fi tinklą ir atskirti jį nuo pagrindinio organizacijos tinklo;
- įrenginiai, kurie turi galimybę naudotis Wi-Fi tinklu, tačiau tam nėra poreikio, turėtų būti atjungti;
- atjungti P2P (angl. Peer-to-peer) tinklo modelį, kuriame keitimasis resursais vyksta tiesiogiai tarp Wi-Fi tinklo naudotojų;
- naudoti WPA3-Enterprise;

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Kas dar gali būti padaryta apsaugant Jūsų tinklą?

Įdiegus WIDS ir WIPS sistemas tinklo administratoriai galės realiu laiku stebėti ir aptikti iškilusias grėsmes, taip mažinant saugumo riziką. Šios sistemos turi galimybę aptikti ir automatiniu būdu atjungti neautorizuotus įrenginius. WIDS suteikia galimybę automatiškai stebėti ir aptikti neleistinus ar netikrus prieigos taškus, tuo tarpu WIPS imasi atsakomųjų veiksmų prieš nustatytas grėsmes. WIPS taip pat sumažina šias įprastas grėsmes: netikrų prieigos taškų sukūrimą, neteisingas prieigos taškų konfigūracijas, neteisėto ryšio užmezgimą, MITM (man-in-the-middle attacks) atakų tikimybę, „ad-hoc“ tinklų atsiradimą, MAC (Media Access Control) klastojimą ir DOS (denial-of-service attacks) atakų tikimybę.

Žemiau pateikiamas WIDS/WIPS konfigūravimo rekomendacijų sąrašas. Rekomenduojame tinklo administratoriams pritaikyti šias rekomendacijas atsižvelgiant į organizacijos vidinę politiką.

- naudokite žalingų procesų aptikimo galimybes;
- nustatykite WIDS/WIPS sistemas aptikti 802.11a/b/g/n/ac standarto įrenginius prijungtus prie laidinio ar belaidžio tinklo;
- įgalinkite „no Wi-Fi“ politiką tinklo potinklyje arba potinkliuose;
- nustatykite automatinį ataskaitų ir pranešimų generavimą;
- įgalinkite įvykių žurnalų saugojimo ir stebėjimo realiu laiku politiką;
- numatykite mažiausiai keturių skirtingų lygių teises / roles, leidžiančias administratoriams deleguoti konkrečias teises.