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

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS
BAZINĖS KIBERNETINIO SAUGUMO REKOMENDACIJOS NUOTOLINIAM DARBUI

2020 m. kovo 16 d.

ORGANIZACIJŲ VADOVAMS IR IT SPECIALISTAMS

1. Organizuoti darbą nuotoliniu būdu pagal principą „būtina žinoti“. Darbas nuotoliniu būdu kelia informacijos konfidencialumo pažeidimo rizikas. Dėl šios priežasties nuotoliniu būdu dirbantiems asmenims turėtų būti suteikiama tik tokia prieiga prie informacijos ir (ar) informacinių sistemų, kiek ji yra reikalinga darbuotojų funkcijoms atlikti. Rekomenduojama organizacijų vadovams ar atsakingiems asmenims dokumentuoti prie kokios informacijos prieigą turi nuotoliniu būdu dirbantys asmenys.

2. Komunikacijų šifravimas. Organizacijos įrenginiai prie informacinių išteklių turėtų jungtis tik saugiu būdu. Ši tikslą galima pasiekti užtikrinant, kad darbuotojai iš namų jungtųsi tik iš žinomų įrenginių, naudojant adekvačias kriptografines priemones:

- organizacijos vidiniams ištekliams ir informacinėms sistemoms pasiekti – VPN,
- autentifikavimas naršyklėje pasiekiamose informacinėse sistemose vykdomas *https* būdu TLS protokolu (ne senesniu kaip 1.2 versijos),
- elektroninio pašto prieiga pasiekiama tik iš žinomų IP adresų, autentifikuojantis keliais būdais (pvz., pirminė prieiga su išduotu sertifikatu, o kitame etape – prisijungimo vardas ir unikalus slaptažodis).

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

3. **Organizacijos įrenginių nuotolinę prieigą organizuoti pagal principą „kas neleidžiama, tas draudžiama“.** Esant galimybei rekomenduojama leisti prisijungti tik žinomiems įrenginiams ir (arba) iš žinomų IP adresų. VPN prieigoje blokuoti visus kreipinius, kurių nėra leistinų IP adresų sąraše. Jungiantis per WEB aplikacijas naudoti unikalius, organizacijos suformuotus *User Agent* identifikatorius.

4. **Informacijos šifravimas.** Informacija įrenginiuose turi būti šifruojama, rekomenduojama — kietojo disko lygmenyje (pvz. naudojant *Microsoft Bitlocker* funkcionalumą).

5. **Darbo stočių administratoriaus teisių ribojimas.** Tarnybiniuose įrenginiuose rekomenduojama naudotojams nesuteikti administratoriaus prieigos teisių.

6. **Kelių faktorių autentifikavimas, saugūs slaptažodžiai.** Prieiga prie darbo stoties turi būti apribota naudojant unikalius prisijungimo duomenis. Jungiantis prie organizacijos informacinės sistemos rekomenduojama naudoti kelių faktorių autentifikavimą.

7. **Apriboti išorinį prisijungimą.** Apriboti išorinio prisijungimo galimybes atvirais RDP ir SSH protokolais.

8. **Nuotoliniu būdu dirbantiems asmenims skirti organizacijos paruoštus kompiuterius.**

NUOTOLINIU BŪDU DIRBANTIEMS ASMENIMS

1. **Belaidžio tinklo prieigos kontrolė.** Pasikeiskite belaidžio tinklo prieigos slaptažodžius į saugius. Nenaudokite numatytojo (angl. *default*) prieigos prie maršrutizatoriaus slaptažodžio (prisijungimo duomenys prie maršrutizatoriaus pateikiamos įrenginio instrukcijoje). Dažnu atveju numatytasis prisijungimo vardas ir slaptažodis sutampa ir yra *admin*. Taip pat patikrinkite ar yra aktyvuotas belaidžio tinklo šifravimas (naudokite WPA3 šifravimą, o jeigu įrenginys tokio nepalaiko, tuomet naudokite WPA2). Patikrinkite, ar pakeistas pradinis tinklo pavadinimas (SSID), jeigu ne – pasikeiskite.

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

2. **Nesaugūs įrenginiai.** Įsitikinkite ar prie jūsų belaidžio tinklo nėra prijungtų nesaugių įrenginių, pvz. daiktų interneto įrenginių, tokių kaip IP kameros, televizoriai ir pan. Jeigu nesate įsitikinęs, kad toks įrenginys atitinka ES šalyse keliamus saugumo reikalavimus – atjunkite jį nuo namų tinklo.

3. **Failų bendrinimas.** Dirbant nuotoliniu būdu iš asmeninio kompiuterio – išjunkite failų bendrinimą (jeigu tokį esate įgalinęs).

4. **Saugi programinė įranga.** Nuotoliniu būdu prie organizacijos informacinių išteklių junkitės naudodamiesi tik legalią operacinę sistemą ir kitą programinę įrangą. Išdiekite P2P programinę įrangą, leidžiančią atsiųsti failus ar vykdyti vaizdinio turinio transliacijas (*Torrent, BiTorrent, Ace Stream, Soda player* ir pan.).

5. **Saugumo priemonių naudojimas.** Naudokite legalią antivirusinę programinę įrangą, rekomenduojama su papildomu funkcionalumu – ugniasiene, elektroninio pašto apsauga ir pan. Periodiškai atlikite kompiuterio skenavimus dėl kenkėjiškos programinės įrangos.

6. **Administratoriaus prieiga.** Nuotoliniu būdu rekomenduojama dirbti naudojant naudotojo paskyrą, kuriai nebūtų suteiktos administratoriaus prieigos teisės, leidžiančios įdiegti papildomą programinę įrangą.

7. **Duomenų šifravimas.** Šifruokite duomenis kietojo disko lygmenyje, pvz. jeigu jūsų operacinė sistema palaiko *Microsoft Bitlocker* funkcionalumą, pasinaudokite juo.

8. **Socialinė inžinerija.** Nesilankykite su darbu nesusijusiose interneto svetainėse, atidžiai vertinkite nuorodas elektroniniuose laiškuose. Nuolat tikrinkite siunčiamos informacijos patikimumą, nepriiminėkite skubotų sprendimų.

9. **Pasitikrinkite savo IP adresą.** Įsitikinkite ar jūsų įrenginys nebuvo užfiksuotas dalyvaujant kenkėjiškoje veikloje. Tą padaryti galite NKSC svetainėje – https://www.nksc.lt/tikrinti.html

10. **Programinės įrangos atnaujinimas.** Įsitikinkite, ar jūsų kompiuteryje ir į tinklą prijungtuose įrenginiuose naudojama programinė įranga yra naujausios versijos, ar įdiegti programinės įrangos atnaujinimai (jeigu ne – atsisiųskite ir įdiekite).

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

11. Kelių faktorių autentifikavimas, saugūs slaptažodžiai. Jungiantis prie organizacijos informacinės sistemos rekomenduojama naudoti kelių faktorių autentifikavimą bei papildomai naudoti kompiuterio slaptažodį (saugų slaptažodį turėtų sudaryti ne mažiau 8 simbolių, naudojant didžiąsias ir mažąsias raides, skaičius ir specialiuosius simbolius).

12. Perduodamą informaciją apsaugoti saugiais slaptažodžiais. Rekomenduojama perduodamą ar į trečiųjų šalių resursus keliamą jautrią informaciją (pvz. naudojantis debesijos paslaugomis) apsaugoti slaptažodžiais, kurie būtų perduodami kitais būdais, pvz. SMS žinutėmis.

NKSC atkreipia dėmesį, kad darbui nuotoliniu būdu galioja tokios pat saugumo taisyklės kaip ir įprastine tvarka. Esminis skirtumas – **atsakomybė už informacijos saugumą didžiąja dalimi atitenka nuotoliniu būdu dirbančiam asmeniui**.