PATVIRTINTA
Valstybės įmonės Ignalinos atominės elektrinės generalinio direktoriaus
2022 m. gruodžio 30 d.
įsakymu Nr. ĮsTa-671

VALSTYBĖS ĮMONĖS IGNALINOS ATOMINĖS ELEKTRINĖS KIBERNETINIO SAUGUMO REIKALAVIMAI TIEKĖJAMS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės įmonės Ignalinos atominės elektrinės (toliau – IAE, įmonė) kibernetinio saugumo reikalavimai tiekėjams (toliau – Reikalavimai) reglamentuoja kibernetinio saugumo reikalavimus tiekėjams vykdant naujus projektus, modernizuojant esamas sistemas, tiekiant techninę ir programinę įrangą, kibernetinio saugumo valdymo paslaugas.

2. Reikalavimai parengti vadovaujantis:

2.1. Lietuvos Respublikos kibernetinio saugumo įstatymu;

2.2. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818;

2.3. TATENA techninėmis gairėmis „Branduolinės energetikos objektų kompiuterių saugumo metodai“ Nr. 17-T, 2021, Viena;

2.4. Lietuvos standartu LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“;

2.5. Teisės aktais tvirtinamų VĮ Ignalinos AE dokumentų rengimo tvarkos aprašu, DVSta-0208-4.

3. Atsižvelgiant į tai, kad IAE, kaip perkančioji organizacija veikia srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi ir valdo ypatingos svarbos informacinę infrastruktūrą, kelia reikalavimą, kad tiekėjų siūlomos prekės (įskaitant jų sudedamąsias dalis bei prekių ir jų dalių gamintojus), paslaugos ir darbai nekeltų grėsmės nacionaliniam saugumui, kai sandorio pagrindu susidarytų aplinkybės, nurodytos Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 13 straipsnio 4 dalies 1 punkte (Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 8 dalis).

4. Su šiais reikalavimais turi būti susipažinę ir jais vadovautis IAE padalinių vadovai, darbuotojai, dalyvaujantys pirkimų procesuose, specialistai, atsakingi už įmonės informacinės infrastruktūros kibernetinį saugumą, tiekėjai (subtiekėjai).

5. Dokumente vartojami sutrumpinimai:

FSSK – Fizinės saugos skyrius.

ITS – Informacinių technologijų skyrius.

PSS – Pirkimų ir sutarčių skyrius.

TVS – turinio valdymo sistema.

II SKYRIUS
REIKALAVIMAI PREKĖMS (TECHNINĖ IR PROGRAMINĖ ĮRANGA)

6. Reikalavimai prekėms (techninei ir programinei įrangai) aprašomi pirkimo dokumentuose (techninėse specifikacijose, pirkimo paraiškose ir kt.).

III SKYRIUS
REIKALAVIMAI PASLAUGOMS (SISTEMŲ PRIEŽIŪRA, KŪRIMAS IR MODERNIZAVIMAS)

7. Draudžiama naudoti nepatikimų gamintojų įrangą ir technologijas.

8. Operacinės sistemos, kita programinė įranga, taip pat naudojamos įrangos programinė dalis priėmimo eksploatuoti metu turi turėti naujausias versijas ir turėti gamintojo rekomenduojamus atnaujinimus.

9. Kompiuterio, kuriame veikia Windows OS, macOS ir kt., eksploatavimas be įdiegtos antivirusinės programos IAE informacinėje infrastruktūroje draudžiamas. Antivirusinės programos diegimas vykdomas kartu su ITS specialistais.

10. Informacija įrenginiuose turi būti šifruojama, rekomenduojama – kietojo disko lygmenyje (pvz., naudojant Microsoft Bitlocker funkcionalumą).

11. Viešaisiais elektroninių ryšių tinklais perduodamos informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (angl. Virtual private network, VPN).

12. Norėdami prisijungti prie IAE informacinių sistemų, tiekėjai turi naudoti IAE įdiegtą PAM (angl. Privileged Access Management) sistemą, dviejų faktorių autentifikavimą (2FA).

13. Jeigu atliekant sistemos derinimo darbus reikia laikinai prijungti tiekėjo kompiuterį tiesiai prie IAE įrengtos įrangos, tai šis kompiuteris turi būti pateiktas FSSK kibernetinio saugumo specialistams patikrinti.

14. Perkamos arba kuriamos sistemos turi turėti galimybę kurti atsargines konfigūracijų ir duomenų kopijas.

15. Priėmimo į eksploataciją metu tiekėjas jei įmanoma, turėtų pateikti atsarginę sistemos kopiją.

16. Sistemoms skirtuose serveriuose turi veikti tik būtini sistemos veikimui servisai.

17. Pramoninių procesų valdymo sistemų perimetras turi būti apsaugotas ugniasiene.

18. Serveriuose ir darbo stotyse turi būti įjungtos ugniasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus susijusį su įmonės informacinių išteklių funkcionalumu ir administravimu, duomenų srautą.

19. Turi būti uždrausti visi nebūtini valdymo protokolai.

20. Turi būti išjungti nenaudojami TCP (angl. Transmission Control Protocol) / UDP (angl. User Datagram Protocol) prievadai.

21. Leidžiama naudoti belaidžio tinklo įrenginius, atitinkančius šiuos kibernetinio saugumo reikalavimus:

21.1. Belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje.

21.2. Turi būti uždrausta belaidėje sąsajoje naudoti SNMP (angl. Simple Network Management Protocol) protokolą.

21.3. Turi būti uždraustas lygiarangis (angl. peer-to-peer) funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšį tarpusavyje.

21.4. Prisijungimas prie belaidžio tinklo turi būti užmegztas naudojant WPA2/WPA3 protokolą autentifikavimui ir šifravimui. Rekomenduojamas WPA3 protokolas, nes jis užtikrina geriausią saugumo lygį. Belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu.

21.5. Prieš pradedant šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelėje standartiniai gamintojo raktai.

22. Kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungtas lygiarangis (angl. peer-to-peer) funkcionalumas, belaidė periferinė prieiga.

23. Kiekvienas sistemų naudotojas turi būti unikaliai atpažįstamas.

24. Kasdienių užduočių vykdymas neturi vykti iš sistemos administratoriaus paskyros. Paprasti vartotojai, kurie nuolat dirba sistemoje, turėtų turėti tik minimalias būtinas teises darbui.

25. Įeinant į paskyrą turi būti naudojamas slaptažodis ar kitas unikalaus vartotojo identifikavimo (autentifikavimo) būdas.

26. Jeigu sistema yra svarbi IAE informacinės infrastruktūros funkcionavimo ar saugumo požiūriu arba yra prieinama interneto ryšį turintiems vartotojams, rekomenduojama naudoti 2FA.

27. Prisijungimo prie sistemų slaptažodžių reikalavimai:

27.1. slaptažodis turi būti sudarytas iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių. Vartotojo slaptažodį turi sudaryti ne mažiau kaip aštuoni simboliai, Administratoriaus slaptažodį turi sudaryti ne mažiau kaip dvylika simbolių;

27.2. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pvz., gimimo data, šeimos narių vardai ir panašiai);

27.3. draudžiama slaptažodžius atskleisti kitiems asmenims, užsirašytus slaptažodžius palikti matomoje vietoje;

27.4. slaptažodis turi būti keičiamas kas 90 dienų;

27.5. turi būti nustatytas didžiausias leistinas sistemų naudotojo mėginimų įvesti teisingą slaptažodį skaičius. Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, sistemų naudotojo paskyra turi užsirakinti;

27.6. draudžiama techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į atitinkančius reikalavimus.

28. Siekiant kontroliuoti tinklo išteklių vartotojų ir administratorių atliekamus veiksmus, turi būti fiksuojama ši informacija:

28.1. sistemų naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti) / atsijungimas;

28.2. sistemų naudotojų / administratorių teisių naudotis sistemos / tinklo ištekliais pakeitimai;

28.3. konfigūracijos pakeitimai;

28.4. įvykstančios klaidos.

IV SKYRIUS
REIKALAVIMAI KURIANT WEB APLIKACIJAS

29. Web aplikacijos administratorius turi turėti galimybę keisti reikalavimus naudotojų slaptažodžiams (nustatyti, koks bus reikalaujamas slaptažodžio ilgis, kokie turi būti specialūs simboliai, didžiosios/mažosios raidės, skaičiai ir pan.).

30. Draudžiama slaptažodžius saugoti programiniame kode.

31. Web aplikacijos, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius.

32. Web aplikacijos administratorius turi turėti galimybę gauti informaciją iš kokio IP adreso jungėsi naudotojas ir kokius veiksmus atliko.

33. Turi būti fiksuojami ir administratoriui pateikiami nepavykę bandymai prisijungti prie TVS ir web aplikacijos vartotojų profilių.

34. Web aplikacija turi užtikrinti galimybę informaciją pasiekti naudojantis saugiu HTTPS (angl. Hypertext Transfer Protocol Secure) ryšiu.

35. Turi būti numatyta apsauga nuo kenkėjiško kodo įkėlimo į web aplikaciją (pvz., apribota galimybė įkelti bylas su plėtiniais .exe, .bat ir pan.).

36. Web aplikacijos negali turėti Open Web Application Security Project (OWASP) Top 10 periodiškai skelbiamame aktualiame dokumente ir ankstesnėse šio dokumento versijose nurodytų pažeidžiamumų. Rekomenduojama atlikti web aplikacijos saugumo testavimą naudojant SAST (angl. Static Application Security Testing) ir DAST (angl. Dynamic Application Security Testing) įrankius.

V SKYRIUS
ATSAKOMYBĖ

37. Tiekėjai už šių reikalavimų laikymąsi atsako teisės aktų nustatyta tvarka.

38. FSSK, ITS, PSS vadovai atsako už šių reikalavimų vykdymo kontrolę.

39. IAE padalinių vadovai, darbuotojai dalyvaujantys pirkimų procesuose atsako už rengiamų pirkimo dokumentų atitiktį šiems reikalavimams.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

40. Šis dokumentas peržiūrimas esant būtinybei.

41. Šie reikalavimai keičiami, pripažįstami netekusiu galios įmonės generalinio direktoriaus įsakymu.