tel. 1843
el. p. info@nksc.lt
https://www.nksc.lt/

INFORMACINIS BIULETENIS

REKOMENDACIJOS YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS

2022 m. liepos 27 d.
Vilnius

Siekdamas stiprinti organizacijų kibernetinio saugumo brandą ir atsižvelgdamas į padidėjusias kibernetines grėsmes bei kasmet augantį kibernetinių incidentų skaičių, Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) parengė informacinį biuletenį[1], kuriame aprašytos prioritetinės kibernetinio saugumo stiprinimo priemonės.

NKSC ragina organizacijas, ypač ypatingos svarbos informacinės infrastruktūros valdytojas, imtis papildomų apsaugos priemonių ir išvengti kibernetinių incidentų, vadovautis toliau pateiktomis rekomendacijomis, kaip apsaugoti informacinę infrastruktūrą.

Eil. Nr.	Priemonė	Nuo ko apsaugo priemonė?	Priemonės nauda	Priemonės įgyvendinimo rekomendacijos	Prioritetas	Atvirų šaltinių įrankiai[2]
1	Darbuotojų ir trečiųjų šalių nuotolinių prieigų prie ryšių ir informacinių sistemų kontrolė	Nesankcionuoti prisijungimai prie infrastruktūros ir informacinių išteklių	Leidžia kontroliuoti ir stebėti prisijungimus, suteikia galimybę prevenciškai užkardyti incidentus	Trečiųjų šalių prieigos kontrolė pagal poreikį (angl. *on-demand*) gali būti užtikrinama naudojant kelių faktorių autentifikavimo sprendimus (angl. *Multi-factor authentication*), bendrojo autentifikavimo (angl. *Single-Sign On*) priemones, nustatant prisijungimų galiojimo laiką (ne ilgesnį kaip 8 val.). Prieigos prie debesijos išteklių gali būti valdomos naudojant debesijos išteklių pasiekiamumo priemones (angl. *Cloud access security broker*)	Labai aukštas	-
2	DNS filtravimas bei audito įrašų registravimas	Programinė kenkimo įranga, duomenų vagystės	DNS filtravimas suteikia galimybę, prieš apsilankant svetainėje, patikrinti jos adresą. Jeigu svetainės adresas yra įtrauktas į kenkimo svetainių sąrašą, naudotojas jos pasiekti negalės. Sukurti DNS	Pakeisti esamus DNS įrašus į paslaugos teikėjo DNS, tai užtikrina kenkimo domenų blokavimą. Sukurti DNS filtravimo taisykles. Registruoti DNS užklausas, kad būtų galima	Labai aukštas	„pfBlockerNG“, „Pi-hole“, ELK, „AlienVault OSSIM“

tel. 1843
el. p. info@nksc.lt
https://www.nksc.lt/

			filtravimo taisyklių rinkiniai apsaugo nuo žinomų dažniausiai pasitaikančių grėsmių, o audito įrašų registravimas leidžia įvykus incidentui atlikti detalų jo tyrimą	atlikti kibernetinių incidentų tyrimą		
3	Programinės įrangos atnaujinimai	Pasinaudojimas žinomomis programinės įrangos spragomis, sistemų perėmimas, sutrikdymas, duomenų vagystės	Reguliarus operacinių sistemų, programinės įrangos ir jos komponentų atnaujinimas padeda išvengti incidentų dėl pasinaudojimo žinomomis spragomis	Automatinis ir rankinis reguliarus programinės įrangos atnaujinimas pagal formalizuotą procedūrą	Labai aukštas	„OpenCVE.io“/ „Cve.org Cisa.gov“
4	Slaptažodžių vartojimo tvarka	Įsilaužimas, paskyrų perėmimas, duomenų vagystės	Tinkama slaptažodžių vartojimo tvarka padeda užtikrinti paskyrų ir sistemų saugą	Slaptažodžiai turi būti kompleksiniai, sudaryti iš kelių skirtingų simbolių klasių, ne trumpesni nei 12 simbolių. Rekomenduojama slaptažodžius sudaryti naudojant prasmės neturinčias frazes – taip sudaromi ilgesni slaptažodžiai, kuriuos nesunku įsiminti. Taip pat rekomenduojama naudoti žinomus ir patikimus slaptažodžių saugojimo sprendimus, taip užtikrinant efektyvų kompleksinių ir ilgų slaptažodžių valdymą	Labai aukštas	„KeePass“
5	DNS infrastruktūros apsauga	Paskirstytos paslaugos trikdymo atakos (toliau – DDoS), DNS serverio gedimas/apkro-vimas	Svetainių pasiekiamumas labai priklauso nuo DNS serverio apkrovimo. Jeigu DNS serveriai yra atakuojami piktavalių, jų veikla gali sulėtėti arba visiškai sutrikti ir svetainės tapti nebepasiekiamos	Pasirinkti tokį DNS paslaugos teikėją, kuris įgyvendintų Lietuvoje galiojančius kibernetinio saugumo reikalavimus bei užtikrintų apsaugą nuo DDoS	Aukštas	-
6	Viešai pasiekiamų išteklių apsauga	DDoS atakos, programų spragos ir architektūriniai pažeidžiamumai, paskyrų perėmimas	Interneto svetainių ugniasienės (angl. *Web Application Firewall*) ir apsaugos nuo DDoS sprendimai padės užtikrinti, kad interneto svetainės lankytojai visada pasieks Jūsų interneto svetainę	Sukurti ir tinkamai aprašyti taisykles, skirtas žiniatinklio atakoms prieš interneto svetaines filtruoti	Aukštas	„Libmodsecurity“

tel. 1843
el. p. info@nksc.lt
https://www.nksc.lt/

7	Vieno prisijungimo sprendimo (toliau – SSO) naudojimas visose programose ir tinklo įrenginiuose	Slaptažodžio pakartotinis vartojimas, internetu pasiekiami decentralizuoti ištekliai	SSO sprendimai centralizuotai valdo naudotojų autentifikavimą ir autorizavimą, leidžia greitai atšaukti sukompromituotą slaptažodį	Sukurti aiškią prisijungimo prie programų ir naudotojų teisių tvarką ir parengti šios tvarkos aprašą. Pagal šią tvarką riboti sesijų trukmę ir prisijungimų skaičių, taip pat sukonfigūruoti SSO su visomis naudojamomis programomis	Aukštas	„Key-cloak“
8	Kelių veiksnių autentifikacijos (toliau – MFA) taikymas visose programose ir tinklo įrenginiuose	Įsilaužimas, duomenų vagystės, paskyros perėmimas	MFA funkcija reikalinga, kad prisijungiant būtų naudojamas daugiau negu vienas skirtingas autentifikavimo būdas (papildomai gali būti naudojamas trumpąja žinute gautas kodas, fizinis raktas, patvirtinimas programėlėje) ir taip užtikrinama dviejų ar daugiau lygių paskyros apsauga	Pasirinkti Jūsų organizacijai tinkamiausią MFA sprendimą	Aukštas	„privacyIDEA“, „FreeIPA“, „FreeOTP“
9	Išorinės infrastruktūros prievadų ir paslaugų skenavimas	Prieigos prie resursų apsauga	Periodinis TCP/UDP prievadų skenavimas leidžia identifikuoti atvirus prievadus ir paslaugas, kurių egzistavimas gali būti perteklinis, taip suteikiant papildomas galimybes piktavaliams identifikuoti saugumo spragas bei jomis pasinaudoti, vykdyti kibernetines atakas	Prievadų skenavimas vykdomas automatiniais įrankiais. Pertekliniai ir atviri prievadai turi būti atjungti nuo viešos prieigos, o būtini – apriboti, suteikiant prieigą tik tam tikriems IP adresams, patenkantiems į leistiną sąrašą	Aukštas	„Nmap“, „Open-VAS“
10	Ryšių ir informacinių sistemų segmentacija	Prieigos prie svarbiausių resursų apsauga	Tinklo skirstymas į patikimumo zonas ir tarpzoninių duomenų filtravimas leidžia apsaugoti itin jautrių sistemų prieigą nuo įsilaužėlių	Suskirstyti sistemas pagal patikimumą ir apsaugos lygį į tinklo segmentus (zonas) ir riboti tarpzoninius duomenų mainus ugniasienės taisyklėmis	Aukštas	„pfSense“
11	Duomenų srauto stebėsena ir analizė aptinkant kibernetinius incidentus	Programinė kenkimo įranga, išpirkos reikalaujančios programos	Saugus žiniatinklio maršrutizatorius (toliau – SWG). Saugos sprendimas, neleidžiantis nepatikrintam interneto srautui patekti į vidinį tinklą. SWG, esantis tarp naudotojo ir interneto, užtikrina tinklo apsaugą,	Nustatyti griežtą duomenų apsaugos tvarką, kuri leistų stebėti duomenų srautą. Iš tarpinio serverio išeinantis srautas nukreipiamas per SWG	Aukštas	„Snort“, „Suricata“, „Zeek“, ELK

tel. 1843
el. p. info@nksc.lt
https://www.nksc.lt/

			tikrindamas žiniatinklio užklausas			
12	Vartotojų rolių peržiūra	Sistemos užvaldymas administratoriaus teisėmis	Perteklinių rolių nebuvimas apsunkina piktavalio galimybes užvaldyti sistemą administratoriaus teisėmis ir taip gauti prieigą prie svarbių duomenų ir (ar) procesų	Reguliari vartotojų rolių peržiūra taikant būtinumo principą. Naudotojams neturi būti suteikiamos administratoriaus teisės, turi būti kaip galima labiau apribotos naudotojų ir privilegijuotų procesų vykdymo, rašymo, skaitymo rolės. Administratorių rolės turėtų būti suskirstytos pagal informacinių išteklių prieigas	Aukštas	-
13	SSO ir MFA naudojimas kartu visose programose ir tinklo įrenginiuose	Tikslinė duomenų vagystės ataka, laipsniška tinklo įsibrovimo ataka	MFA yra saugumo mechanizmas, užtikrinantis, kad būtų naudojamas daugiau nei vienas faktorius prisijungiant prie programų ar tinklo įrenginių, o SSO leidžia naudotojui pasiekti visus resursus naudojant vieną slaptažodį. Kartu naudojant SSO ir MFA pagerinama naudotojo patirtis ir saugumas, taip pat lengviau stebėti tinklo veiklą	Aiškiai apibrėžti, kas gali pasiekti tam tikrus resursus. Integruoti tapatybės paslaugas	Vidutinis	-
14	Papildoma IT infrastruktūros apsauga	Tinklo lygio DDoS atakos	Dažnai interneto svetainės yra geriau apsaugotos nei išoriniai tinklo elementai. Todėl būtina užtikrinti ir šių elementų apsaugą nuo DDoS atakų	Apsaugoti visus išorinius IP adresus nuo DDoS atakų. Tinklus jungti naudojant GRE (angl. *Generic Routing Encapsulation*) ir IPsec (angl. *Internet protocol security*) tunelius arba fizinį tinklų sujungimą. Leisti įeinantį srautą tik iš apsaugą nuo DDoS teikiančio paslaugų teikėjo IP adresų	Vidutinis	-
15	El. laiškų tikrinimas	Duomenų vagystės, išpirkos reikalaujančios programos	El. pašto apsaugos sprendimai leidžia patikrinti el. laiškus prieš jiems patenkant į galutinio naudotojo pašto dėžutę	Naudoti programinę ir (ar) aparatinę įrangą el. laiškams tikrinti. Turėti patvirtintą el. pašto naudojimo ir tvarkymo tvarkos aprašą	Vidutinis	„Apache SpamAssassin“

tel. 1843
el. p. info@nksc.lt
https://www.nksc.lt/

16	Scenarijų (angl. *script*) ir bibliotekų tikrinimas, ieškant kenkimo kodo	Jautrios informacijos filtravimas, įskaitant naudotojų prisijungimo duomenis	Trečiųjų šalių „JavaScript“ ir kitų bibliotekų naudojimas gali būti rizikingas dėl saugumo spragų, atsirandančių tokiose bibliotekose	Pateikti žiniatinklio srautą iš už atvirkštinio tarpinio serverio. Įdėti CSP (angl. *Content Security Policy*) atsakymų antraštes, siekiant gauti scenarijų skaitymo ir paleidimo procesą. Naudoti SRI (angl. *Subresource Integrity*) priemones trečiųjų šalių bibliotekų integralumui tikrinti. Naudoti automatinį įrankį, renkantį ir stebintį pakitimus, jei atsirastų kenkimo kodas	Vidutinis	„NPM Audit“, „Retire.js“, „OWASP Dependency-Check“, „Open-VAS“
17	Netinkamų konfigūracijų paieška saugumo nustatymuose	Silpnas autentifikavimas, nesaugus šifravimas ir netinkama DNS konfigūracija	Dėl netinkamos komponento ar sistemos konfigūracijos gali atsirasti pažeidžiamumai, kuriais galima pasinaudoti	Naudoti automatizuotą įrankį, kuris gali aptikti blogas konfigūracijas bei pateikti rekomendacijas, kaip jas ištaisyti	Vidutinis	„Open-VAS“
18	Patikima tarnybinių stočių ir kompiuterizuotų darbo vietų konfigūracija	Sistemų užvaldymas, jautrių duomenų perėmimas, privilegijų eskalacija	Netinkama tarnybinių stočių ir kompiuterizuotų darbo vietų konfigūracija dažnai atveria galimybes piktavaliams nesudėtingai eskaluoti privilegijas, nuskaityti jautrius duomenis	Užtikrinti tinkamą tarnybinių stočių ir kompiuterizuotų darbo vietų konfigūraciją remiantis geriausiomis saugos praktikomis (NIST, CIS rekomendacijos)	Vidutinis	„Open-VAS“
19	Atsarginės duomenų kopijos ir duomenų atkūrimo planas	Visiškas duomenų praradimas po saugos incidento	Kibernetinio incidento atveju netekus duomenų, šių duomenų atsarginės kopijos leidžia užtikrinti veiklos tęstinumą su minimaliais nuostoliais	Duomenų atsarginės kopijos turi būti daromos reguliariai ir laikomos logiškai atskirtame tinkle arba pas atskirą paslaugos teikėją. Rekomenduojama turėti duomenų atkūrimo po incidento planą ir reguliariai vykdyti pratybas, išbandant duomenų atkūrimo iš atsarginių kopijų procesą	Vidutinis	-
20	Organizacijos domeno apsauga	Domeno praradimas	Domeno praradimas gali sukelti didelių finansinių ir reputacinių nuostolių	Naudoti MFA prisijungiant prie domeno administravimo paskyros. Žinoti domeno galiojimo laiką, nepamiršti jo pratęsti	Žemas	-

[1] Biuletenyje pateikta informacija aktuali 2022-07-27. Biuletenis parengtas remiantis šiais šaltiniais:
https://www.cisecurity.org/controls/cis-controls-list
https://criticalinfrastructuredefense.org/
https://www.ncsc.gov.uk
https://www.nist.gov/cyberframework
https://owasp.org/www-project-top-ten/

[2] Nurodyti atvirų šaltinių įrankiai yra rekomendacinio / pavyzdinio pobūdžio ir universalūs. Jų naudojimas negarantuoja saugumo. Siekiant tinkamai naudoti įrankius, reikalingas kvalifikuotas personalas.