Nacionalinis kibernetinio saugumo centras

Kibernetinio saugumo ir telekomunikacijų tarnyba prie Krašto apsaugos ministerijos
Šilo g. 5A, LT-10322 Vilnius, tel. + 370 5 210 3849, www.nksc.lt, el. p. info@nksc.lt

Ypač svarbios efektyviai kibernetinei gynybai saugumo kontrolės priemonės (angl. Critical Controls, CC)

	SAUGUMĄ DIDINANTI PRIEMONĖ	APRAŠYMAS
1.	**Tinklo įrenginių, kuriems leidžiama naudotis institucijos tinklo paslaugomis, identifikavimas (angl. Inventory of Authorized and Unauthorized Devices)**	Veiksmingai valdyti (inventorizuoti, stebėti ir šalinti) visus tinklo įrenginius, siekiant užtikrinti, kad tik tie įrenginiai, kuriems leidžiama tai daryti, galėtų pasinaudoti tinklo teikiamomis paslaugomis, o nežinomi ir nevaldomi įrenginiai būtų aptikti, jiems nebūtų leista dalyvauti tinklo veikloje.
2.	**Leistinos ir neleistinos naudoti programinės įrangos identifikavimas (angl. Inventory of Authorized and Unauthorized Software)**	Veiksmingai valdyti (inventorizuoti, stebėti ir šalinti) programinės įrangos naudojimą tinkle, siekiant užtikrinti, kad būtų įdiegta ir galėtų veikti tik leistina programinė įranga, o aptikta draudžiama naudoti programinė įranga būtų blokuojama.
3.	**Techninės ir programinės įrangos saugios konfigūracijos mobiliuosiuose įrenginiuose, darbo vietos ar tarnybinėse stotyse numatymas (angl. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers)**	Sukurti, pritaikyti ir veiksmingai valdyti (stebėti, tikslinti bei rengti ataskaitas) nešiojamųjų įrenginių, darbo vietos ar tarnybinių stočių techninės ir programinės įrangos saugumo konfigūraciją (saugumo nustatymo parametrus), siekiant užkirsti kelią pasinaudoti sistemų pažeidžiamumu. Konfigūracijų pokyčiai turi būti griežtai stebimi ir valdomi.
4.	**Nenutrūkstamas sistemų pažeidžiamumo vertinimas ir saugumo spragų taisymas (angl. Continuous Vulnerability Assessment and Remediation)**	Nuolat rinkti ir vertinti informaciją, susijusią su programinės įrangos pažeidžiamumu ir saugumo spragų ištaisymu. Neatidėliojant veikti pagal pateikiamas rekomendacijas, norint sumažinti galimybes piktavaliams pasinaudoti saugumo spragomis.
5.	**Naudojimosi administratoriaus teisėmis kontrolė (angl. Controlled Use of Administrative Privileges)**	Kurti procesus ir naudotis priemonėmis, skirtomis stebėti ir kontroliuoti, kaip naudojamasi administratoriaus teisėmis. Tokių teisių konfigūravimas ir suteikimas kompiuteriuose, tinkle ar programinėje įrangoje turi būti griežtai kontroliuojamas ir leidžiamas tik esant būtinybei.
6.	**Audito žurnalų įrašų stebėjimas, analizė ir saugojimas (angl. Maintenance, Monitoring and Analysis of Audit Logs)**	Audito įrašų, galinčių padėti aptikti ir suprasti vykstančias kibernetines atakas, atkurti sistemos veiklą įvykus saugumo incidentui, fiksavimas, valdymas ir analizė.
7.	**Elektroninio pašto ir naršyklių apsauga (angl. Email and Web Browser Protections)**	Mažinti galimybes piktavaliams manipuliuoti el. pašto ir interneto sistemų naudotojų elgsena.
8.	**Apsauga nuo kenkimo programų (angl. Malware Defenses)**	Kenkimo programų atsiradimo organizacijoje stebėjimas, jų plitimo ir veikimo organizacijos tinkle kontrolė. Apsaugos sistemų automatizavimas ir optimizavimas, norint sparčiai atnaujinti apsaugos priemones, efektyviai surinkti informaciją apie įvykius ir veiksmingai reaguoti į incidentus.
9.	**Tinklo prievadų, protokolų ir paslaugų naudojimo apribojimai (angl. Limitation and Control of Network Ports, Protocols and Services)**	Veiksmingai valdyti (stebėti, kontroliuoti ir riboti) tinklo prievadų, protokolų ir paslaugų tinklo įrenginiuose naudojimą, norint sumažinti galimybes piktavaliams rengti kibernetines atakas.
10.	**Duomenų atkūrimo pajėgumas (angl. Data Recovery Capability)**	Taikyti procesus ir priemones, skirtas itin svarbių duomenų atsarginėms kopijoms daryti. Metodika turi būti išbandyta ir užtikrinti patikimą duomenų atkūrimą reikiamu laiku.
11.	**Saugios tinklo įrenginių, tokių kaip saugasienės, maršruto parinktuvai, komutatoriai, konfigūracijos numatymas (angl. Secure Configurations for Network Devices such as Firewalls, Routers and Switches)**	Nustatyti, taikyti ir veiksmingai valdyti (stebėti, tikslinti bei rengti ataskaitas) tinklo įrenginių saugumo konfigūraciją, laikantis griežtai apibrėžtos konfigūracijos valdymo ir pokyčių kontrolės proceso tvarkos, siekiant užkirsti kelią piktavaliams pasinaudoti paslaugų ir įrenginių nustatymo parametrų pažeidžiamumu.
12.	**Tinklo perimetro apsauga (angl. Boundary Defense)**	Aptikti, stabdyti bei valyti potencialiai pavojingą duomenų srautą, keliaujantį tarp skirtingo patikimumo lygio tinklo segmentų.
13.	**Duomenų apsauga (angl. Data Protection)**	Taikyti procesus ir priemones, skirtas apsisaugoti nuo tikslinio duomenų rinkimo ir informacijos nutekinimo (eksfiltravimo), užtikrinti neskelbtinos informacijos vientisumą ir konfidencialumą.
14.	**Prieigos kontrolė, paremta principu „būtina žinoti“ (angl. Controlled Access Based on the Need to Know)**	Taikyti procesus ir priemones, skirtas stebėti ir kontroliuoti, kad prieiga prie itin svarbių išteklių (informacijos, sistemų ir pan.) būtų suteikiama tik esant motyvuotam poreikiui. Suteikiant prieigą, remtis iš anksto numatyta politika, kuriems kompiuteriams, programoms ar darbuotojams tai yra reikalinga.
15.	**Belaidės prieigos kontrolė (angl. Wireless Access Control)**	Taikyti procesus ir priemones, skirtas belaidžių tinklų, prieigos taškų ir belaidžių sistemų saugumui užtikrinti bei kontroliuoti, kad belaide prieiga naudotųsi tik teises tai daryti turintys naudotojai (neviršydami jiems suteiktų teisių).
16.	**Naudotojų paskyrų stebėjimas ir kontrolė (angl. Account Monitoring and Control)**	Aktyviai kontroliuoti sistemų ir taikomųjų programų naudotojų paskyras visą jų gyvavimo (kūrimo, naudojimo, laikino stabdymo, naikinimo) ciklą, siekiant sumažinti piktavalių galimybes išnaudoti sistemos saugumo spragas.
17.	**Saugumo srities gebėjimų vertinimas ir reikiamų mokymų numatymas (angl. Security Skills Assessment and Appropriate Training to Fill Gaps)**	Identifikuoti specifinių įgūdžių ir žinių, būtinų norint užtikrinti organizacijos informacinių sistemų apsaugą, poreikį (prioritetai teikiami ypač svarbiems veiklos procesams ir jų saugumui užtikrinti). Įvertinus poreikį didinti kibernetinį sąmoningumą, taikant veiklos planavimo priemones ir remiantis saugumo politika, sukurti ir pritaikyti darbuotojų gebėjimų tobulinimo planą.
18.	**Taikomųjų programų saugumas (angl. Application Software Security)**	Valdyti visos sukurtos ar įgytos programinės įrangos saugumo gyvavimo ciklo elementus. Siekti užkirsti kelią piktavalių planams pasinaudoti galimomis saugumo spragomis; stengtis jas aptikti ir ištaisyti.
19.	**Reagavimas į incidentus ir jų valdymas (angl. Incident Response and Management)**	Organizacijos informacijos ir reputacijos apsaugos užtikrinimas, diegiant reagavimo į incidentus infrastruktūrą (veiklos planai, vaidmenų paskirstymas, mokymai, komunikacija, valdymas) tam, kad būtų greitai aptinkamos vykstančios atakos, efektyviai suvaldoma žala, aptinkami įsilaužėliai ir panaikinami jų veiklos padariniai, atkuriamas tinklo ir sistemų vientisumas.
20.	**Bandymai įsilaužti ir „raudonųjų komandų“ pratybos (angl. Penetration Tests and Red Team Exercises)**	Visapusiškai išbandyti organizacijos gynybos galimybes (technologijas, procesus, personalą), imituojant piktavalio veiksmus ir tikslus.

Gavus autorių sutikimą, parengta naudojantis *SANS* instituto ir Kibernetinio saugumo tarybos (angl. *Council on Cyber Security*) informacija.

Kodėl svarbu skubiai atnaujinti organizacijos naudojamas programas?
Kibernetiniai nusikaltėliai, sužinoję apie išleistus programų naujinius, juos ištiria ir stengiasi pasinaudoti delsiančiųjų atnaujinti programas aplaidumu – esamų programų spragomis, siųsdami į jų kompiuterius kenksmingą programinį kodą.

Kokią programinę įrangą atnaujinti yra ypač svarbu?
Operacines sistemas (įsilaužėliai gali mėginti pasinaudoti neužtaisytomis spragomis), naršykles (didelė dalis kenksmingo programinio kodo plinta per nesaugius tinklalapius), taikomųjų biuro programų paketus, PDF formato dokumentų peržiūros programas (užkrėstus dokumentus elektroniniu paštu siunčia kibernetiniai nusikaltėliai), *Java* ir *Flash* grotuvus (nesaugūs tinklalapiai užkrečia lankytojų, kurie naudojasi neatnaujinta programine įranga, įrenginius).

Kodėl svarbu apie kibernetinius pavojus informuoti organizacijos darbuotojus?
Dažnai prevencija tampa geriausia gynyba. Jei naudotojai bus apdairūs, neatidarinės užkrėstų elektroninių laiškų, atsakingai elgsis internete, tai leis sutaupyti daug kompiuterių tinklo saugumo ir administravimo specialistų darbo laiko, taip pat organizacijos lėšų.

Nuo ko pradėti, jei organizacija nedidelė ar tik pradeda rūpintis savo kibernetiniu saugumu?
Svarbiausių veiksmų sąrašas (rekomendacijos itin tinka mažoms organizacijoms, kurių techninė infrastruktūra ir finansinės galimybės yra nedidelės):
1. Sudaryti leistinos naudoti programinės įrangos sąrašus (angl. *application whitelisting – CC 2*).
2. Naudoti standartizuotos, saugios konfigūracijos sistemas (angl. *use of standard, secure system configuration – CC 3*).
3. Skubiai (ne vėliau kaip per 48 val. nuo naujinių išleidimo) diegti naudojamos programinės įrangos naujinius (angl. *patch application software within 48 hours – CC 4*).
4. Skubiai (ne vėliau kaip per 48 val. nuo naujinių išleidimo) diegti naudojamos operacinės sistemos naujinius (angl. *patch system software within 48 hours – CC 4*).
5. Griežtai riboti naudotojų, turinčių administratoriaus teises, skaičių (angl. *reduce the number of users with administrative privileges – CC 3 ir CC 5*).

Rengiant šią santrauką, remtasi *SANS* instituto ir Kibernetinio saugumo tarybos (angl. *Council on Cyber Security*) gerąja praktika.
Kibernetinio saugumo taryba (angl. *Council on Cyber Security*) – tai nepriklausoma, pelno nesiekianti organizacija, kurios uždavinys – kurti ir plėtoti gerus kibernetinio saugumo sprendimų pavyzdžius (tarp jų ir 20 šiame plakate įvardytų ypač svarbių kontrolės priemonių). Tarybos tinklalapyje **http://www.counciloncybersecurity.org** galite rasti naujausią Kontrolės priemonių aprašo versiją, daug pagalbinių darbo priemonių, pateikčių ir kitos medžiagos, susijusios su ypatingos saugumo kontrolės būdais.

Itin detalius plakate išvardytų ypač svarbių saugumo kontrolės priemonių aprašymus galite rasti tinklalapyje **http://www.sans.org/critical-security-controls** (jis priklauso kibernetinio saugumo mokymų ir atestavimo institutui *SANS*).

SANS instituto svetainėje (**http://www.sans.org/critical-security-controls/vendor-solutions**) taip pat aprašomos tikros organizacijų, kurios sėkmingai pritaikė šias kontrolės priemones, istorijos ir pateikiama gautos naudos analizė. Realių pavyzdžių („kas veikia“ tipo) ataskaitos suteikia naudingos informacijos – į ją vertėtų atsižvelgti prieš pasirenkant ir įsigyjant organizacijos poreikius geriausiai atitinkančius sprendimus.

Maketavo KAMBRD Leidybos skyrius, Totorių g. 25, LT-01121 Vilnius; 2015. Spausdino LK KKC, Muitinės g. 4, Domeikava, LT-54359 Kauno r.; www.kam.lt