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

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS
INFORMACINIŲ IŠTEKLIŲ ŽURNALINIŲ ĮRAŠŲ POLITIKA WINDOWS APLINKOJE

2020 m. gegužės 18 d.

Nacionalinis kibernetinio saugumo centras, vykdydamas kibernetinių incidentų tyrimus, pastebi tendenciją, kad vis dar nemažai organizacijų ir įmonių yra neįsidiegusios informacinių išteklių audito politikos. Įvykus kibernetiniam incidentui, tampa neįmanoma identifikuoti veiksmų ar naudotojų, vykdžiusių kenkimo veiką, vien dėl to, kad audito įrašai nėra kaupiami ar jų saugojimo terminas yra pernelyg trumpas.

„Windows“ šeimos operacinėse sistemose numatytas platus auditavimo, įvykių žurnalų registravimo funkcionalumas. Deja, tenka pripažinti, kad daugeliu atveju šis nemokamas funkcionalumas būna netinkamai sukonfigūruotas arba įvykių žurnalai nėra nuolatos peržiūrimi. Tinkamai sukonfigūruotas operacinėse sistemose vykstančių įvykių auditavimas leis laiku pastebėti žalingą veiklą, o, įvykus kibernetiniam incidentui, nustatyti jo priežastis ir pasekmes.

Pagal nutylėjimą ***„Windows“*** šeimos operacinėse sistemose įvykių žurnaluose audituojami (kaupiami) įvairūs įrašai: naudotojų prisijungimai, programinės įrangos diegimas, operacinių sistemų veikimo sutrikimai, kiti vykstantys procesai. Nemaža dalis auditavimo funkcionalumo nėra sukonfigūruota, pavyzdžiui naudotojo paskyrų sukūrimas ar veiksmai su naudotojų paskyromis nėra auditojami[1].

[1] Pagal nutylėjimą veiksmai su paskyromis nėra audituojami. Papildomą veiksmų su paskyromis auditavimą galima įjungti „Group Policy Management“ > „Computer Configuration“ > „Policies“ > „Windows Settings“ > „Security Settings“ > „Local Policies“ > „Audit Policy“

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

„Powershell“ – galingas ir plačiai naudojamas administravimo funkcionalumas, kuris išnaudojamas ne tik geriems tikslams, bet kartu naudojamas ir piktavalių. Operacinėje sistemoje įvykdžius ***„Powershell“*** programinį kodą, įvykių žurnaluose sugeneruojami tik šio proceso paleidimo ir sustabdymo įrašai. Norint gauti papildomos informacijos apie ***„Powershell“*** programinį kodą, kuris buvo įvykdytas, reikia įgalinti papildomą ***„Powershell“*** kodo blokų (angl. *Script Block*) auditavimą[2].

Viena iš galimybių aptikti žalingą programinį kodą yra stebėti operacinėse sistemose sukuriamus procesus. Proceso sukūrimas pagal nutylėjimą taip pat nėra pakankamai išsamiai ir aiškiai audituojamas. Labai svarbu ne tik stebėti sukuriamus procesus, bet ir matyti papildomą informaciją apie komandinę eilutę, kurios pagalba buvo sukurtas procesas[3].

Vertinant organizacijų ir įmonių informacinių išteklių auditavimo poreikius ir galimybes, rekomenduojame peržiūrėti jūsų informacinių išteklių audito politiką. Žemiau pateikta informacija apie specifinių įvykių auditavimą ir kaupimą yra rekomendacinio pobūdžio, todėl diegiant papildomą auditavimą reikėtų atsižvelgti į jūsų informacinės infrastruktūros galimybes bei siektinus tikslus. Pavyzdžiui failų ir katalogų prieigos kontrolės auditavimas yra „triukšmingas“ t. y. įvykių žurnaluose sugeneruojamas didelis įrašų skaičius. Papildomas auditavimo funkcionalumas pirmiausiai turėtų būti išbandytas testavimo aplinkoje, o tik to po perkeltas į produkcinę aplinką.

Daugiau informacijos apie auditavimo įrašų kaupimo galimybės pateikiama čia: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings

Įvykių žurnalų tipai

Pagrindiniai ***„Windows“*** šeimos operacinių sistemų įvykių žurnalai yra:

- ***„Security“*** – saugoma prieigos kontrolės ir saugumo nustatymų informacija. Įvykiai įrašomi atsižvelgiant į lokalios ar globalios grupinės politikos auditavimo kriterijus.
- ***„System“*** – saugoma operacinėje sistemoje veikiančių servisų, sistemos komponentų, tvarkyklių, resursų ir kita informacija. Įvykiai įrašomi atsižvelgiant į operacinę sistemą ar jos komponentus.

[2] Pagal nutylėjimą „PowerShell“ kodo blokai nėra audituojami. Papildomą kodo blokų auditavimą galima įgalinti „Group Policy Management“ > „Computer Configuration“ > „Administrative Templates“ > „Policies“ > „Windows Components“ > „Windows PowerShell“ > „Turn on PowerShell Script Block Logging“.

[3] Pagal nutylėjimą proceso sukūrimas ir jo komandinė eilutė nėra auditojami. Papildomą proceso ir komandinės eilutės auditavimą galima įgalinti „Group Policy Management“> „Computer Configuration“ > „Policies“ > „Windows Settings“ > „Security Settings“ > „Advanced Audit Configuration“ > „Detailed Tracking“ > „Audit Process Creation“ ir „Group Policy Management“ > „Computer Configuration“ > „Policies“ > „Administrative Templates“ > „System“ > „Audit Process Creation“ > „Include command line in process creation events“

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

- ***„Application“*** – saugoma programinės įrangos (aplikacijų) ir su operacinės sistemos veikimu nesusijusi informacija.
- ***„Setup“*** – saugoma diegimo ir atnaujinimų informacija.
- ***„Applications and Services“*** – apima apie 150 įvairių įvykių žurnalų (***„Task Scheduler“, „Windows Firewall“***, ***„Powershell“*** ir kitus).

Įvykių žurnalų saugojimas

„Windows“ šeimos operacinių sistemų įvykių žurnalai, pradedant ***„Vista“ / „Server 2008“*** operacine sistema, saugomi *.evtx formatu. Įvykių žurnalai saugomi kataloge ***„C:\Windows\System32\winevt\Logs“***. Dažniausiai pasitaikanti įvykių žurnalų saugojimo konfigūravimo klaida, kad paliekama gamintojo nustatyta 20 MB įvykio žurnalo (failo) dydžio reikšmė. Operacinėse sistemose, ypač tarnybinėse stotyse, generuojamas didelis įvykių skaičius, todėl įvykių žurnalų įrašai išsaugomi tik už kelias dienas ar net kelias valandas. Žemiau pateikta informacija apie gamintojo rekomenduojamas įvykių žurnalų saugojimo nustatymų reikšmes:

Operacinė sistema	Rekomenduojamas maksimalus įvykio žurnalo dydis (kilobaitais)	Rekomenduojamas maksimalus visų įvykių žurnalų dydis (kilobaitais)	Apytikslis maksimalus įvykių žurnalų įrašymo greitis (įvykių per sekundę)	Rekomenduojamas maksimalus įvykio žurnalo dydis peržiūrai (kilobaitais)
„Windows Server 2008“, 32-bit	4,194,240	16,776,960	2,000	4,194,240
„Windows Server 2008“ ir naujesnė, 64-bit	4,194,240	16,776,960	5,000	4,194,240
„Windows Vista“ ir naujesnė, 32-bit	4,194,240	16,776,960	2,000	4,194,240
„Windows Vista“ ir naujesnė, 64-bit	4,194,240	16,776,960	5,000	4,194,240

Įvykių žurnalų dydis gali būti keičiamas skirtingai būdais:

- Naudojant ***„Powershell“***. Daugiau informacijos: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/limit-eventlog?view=powershell-5.1;
- Naudojant grupinę politiką. Daugiau informacijos: https://docs.microsoft.com/en-au/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff182311(v=ws.10)

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

Įvykių žurnalų kaupimas / stebėjimas

Įvykių kategorija	Paskirtis	Įvykio ID	Įvykių žurnalas, kuriame saugomi įvykiai
Paskyrų naudojimas	Kontroliuoti naudotojų paskyras bei jų elgseną kompiuterių tinkle. Aptikti slaptažodžių parinkimo atakas (*angl. Brute-Force*). Kontroliuoti paskyras, turinčias išplėstinių (administratoriaus) teisių.	**4624** – sėkmingas prisijungimas **4625** – nesėkmingas prisijungimas **4634 / 4647** – sėkmingas atsijungimas **4648** – *„RunAS“* prisijungimas **4672** – prisijungimas turint išplėstines teises (administratoriaus) **4720** – sėkmingas paskyros sukūrimas **4722** – paskyra buvo įjungta **4724** – buvo atliktas bandymas atstatyti paskyros slaptažodį **4728** – naudotojo paskyra buvo įtraukta į globalią saugumo grupę (*angl. security-enabled global group*) **4732** - naudotojo paskyra buvo įtraukta į lokalią saugumo grupę (*angl. security-enabled local group*) **4735** – lokali saugumo grupė (*angl. security-enabled local group*) buvo pakeista **4738** – naudotojo paskyra buvo pakeista **4740** – naudotojo paskyra buvo užrakinta (locked) **4756** - naudotojo paskyra buvo įtraukta į universalią saugumo grupę (*angl. security-enabled universal group*)	***„Security“***
Nuotolinės prieigos ***„Remote Desktop Connection“*** programinė įranga	Kontroliuoti ***„Remote Desktop Connection“*** programinės įrangos naudojimą kompiuterių tinkle.	**4778** – prisijungimo sesijos atnaujinimas **4779** – prisijungimo sesijos atjungimas	***„Security“***
		1024 – prisijungimo sesijos seka (paskirties kompiuterio / tarnybinės stoties vardas) **1102** – prisijungimo sesijos seka (paskirties IP adresas)	***„Microsoft-Windows-TerminalServices-RDPClient/Operational“***
		1149 – sėkmingas prisijungimas (nurodoma iš kur prisijungta / naudotojo vardas)	***„Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational“***
		21 – sėkminga prisijungimo sesija **22** – sėkminga prisijungimo sesijos pradžia **25** – sėkmingas prisijungimo sesijos atnaujinimas	***„Microsoft-Windows-TerminalServices-LocalSessionManager / Operational“***

		131 – bandymas prisijungti **98** – sėkmingas prisijungimas	***„Microsoft-Windows-RemoteDesktopServices-RdpCoreTS / Operational“***
Paskyrų prisijungimai (*angl. Account Logon*)	Kontroliuoti naudotojų paskyras bei jų elgseną kompiuterių tinkle.	***„NTLM“*** protokolas: **4776** – sėkminga / nesėkminga paskyros autentifikacija ***„Kerberos“*** protokolas: **4768** – leidimo išdavimas, leidimas buvo išduotas (Ticket Granting) (sėkmingas prisijungimas) **4769** – paslaugos leidimas (Service Ticket) užklaustas (prieiga prie tarnybinės stoties resursų) **4771** – nesėkminga prieš-autentifikacija (nesėkmingas prisijungimas)	***„Security“***
Bendro naudojimo tinklas (*angl. Network shares*)	Bendro naudojimo katalogų ir failų prieigos, kūrimo, modifikavimo ar trynimo kontrolė. Rekomenduojama įgalinti tik sistemose, kuriose saugomi jautrūs duomenys, kadangi auditavimo mechanizmas sugeneruoja didelį įvykių skaičių	**5140** – gauta prieiga prie bendro naudojimo tinklo **5145** – gauta prieiga prie bendro objekto / failo (sugeneruojamas didelis įvykių skaičius) **5142-5144** – audituoja bendrinimo katalogų/failų kūrimą, modifikavimą ir trynimą	***„Security“***
Sisteminiai uždaviniai (*angl. Scheduled tasks*)	Sisteminių uždavinių kontrolė. Neretai žalingas programinis kodas paleidžiamas sisteminių uždavinių pagalba.	**4698** – sisteminis uždavinys sukurtas **4699** – sisteminis uždavinys ištrintas **4700** – sisteminis uždavinys įgalintas **4701** – sisteminis uždavinys išjungtas **4702** – sisteminis uždavinys atnaujintas	***„Security“***
		106 – sisteminis uždavinys sukurtas **140** – sisteminis uždavinys atnaujintas **141** – sisteminis uždavinys ištrintas **200** – sisteminis uždavinys įvykdytas **201** – sisteminis uždavinys užbaigtas	***„Microsoft-Windows-TaskScheduler/Operational“***
Servisai	Operacinėse sistemose veikiančių servisų kontrolė	**7034 –** serviso veikimas buvo nutrauktas netikėtai **7035** – servisas siuntė ***„Start“*** / ***„Stop“*** kontrolę **7036** – servisas buvo paleistas arba sustabdytas **7040** – paleidimo tipas buvo pakeistas („*Boot*“ | „*On Request*“ | „*Disabled*“) **7045** – naujas servisas buvo įdiegtas	***„System“***
		4697 – naujas servisas buvo įdiegtas	***„Security“***
Įvykių žurnalų trynimas	Įvykių žurnalų kontrolė. Įvykių žurnalai gali būti trinami tik naudotojo, turinčio administratoriaus	**1102** – įvykių žurnalai buvo ištrinti	***„Security“***
		104 - įvykių žurnalai buvo ištrinti	***„System“***

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

	teises. Kiekvieną kartą ištrynus įvykių žurnalus, susikuria **1102** įvykis. ***„Security“*** įvykių žurnalo trynimo atveju – **104**.		
Programinės įrangos / aplikacijų diegimas	Programinės įrangos / aplikacijų diegimo kontrolė	**1033** – diegimas baigtas (sėkmingai | nesėkmingai) **1034** – programinė įranga / aplikacija buvo pašalinta (sėkmingai | nesėkmingai) **11707** – diegimas baigtas sėkmingai **11708** – diegimas nutruko **11724** – programinė įranga / aplikacija buvo pašalinta sėkmingai	***„Application“***
„Windows Management Instrumentation “ (WMI)	***„WMI“*** – bazinė technologija, skirta centralizuotam valdymui ir stebėjimui, neretai išnaudojama žalingo kodo įvykdymui.	**5857-5861** – audituojama filtrų/naudotojų veikla	***„Microsoft-Windows-WMI-Activity/Operational “***
„PowerShell“	***„Powershell“*** – galingas ir plačiai naudojamas administravimo funkcionalumas, tačiau ***„Powershell“*** funkcionalumas išnaudojamas ne tik geriems tikslams, bet naudojamas ir piktavalių.	**8193–8194** – sesija sukurta **8197** – prisijungimo sesija uždaryta **4103–4104** – įrašomi skriptų blokai (*angl. script blocks*)	***„Microsoft-Windows-PowerShell/Operational“***
		400/403 – „ServerRemoteHost“ nuotolinės prisijungimo sesijos pradžia/pabaiga	***„Windows PowerShell“***
Klaidų pranešimai	Operacinės sistemos, servisų ir procesų klaidų pranešimų stebėjimas. Operacinėje sistemoje bandant paleisti arba veikiant žalingam programiniam kodui, sutrinka įprastas operacinės sistemos ar jos komponentų veikimas, generuojami klaidų pranešimai (įvykiai)	**1001** – ***„Windows“*** klaidų pranešimai (WER)	***„System“***
		1000-1002 – programinės įrangos/aplikacijų klaidos ir sutrikimai	***„Application“***
		7022 – servisas nestartavo **7023** – serviso veikimas nutrauktas, klaida: **7024** - serviso veikimas nutrauktas, specifinė serviso klaida: **7025** – bent vieną servisą ar tvarkyklę nepavyko paleisti, paleidžiant sistemą **7026** – nepavyko įkelti *„boot-start“* ar *„system-start“* tvarkyklių	***„System“***
Procesai	Operacinėje sistemoje vykstančių procesų stebėjimas. Ypatingas dėmesys turi būti skirtas komandinei eilutei, kurios pagalba paleidžiamas procesas	**4688** – naujas procesas sukurtas **4689** – proceso pabaiga	***„Security“***
Ugniasienė	Operacinės sistemos ugniasienėje vykstančių įvykių kontrolė	**5154** – ***„Windows Filtering Platform“*** leido programinei įrangai ar servisui klausytis įvesties tinklo prievado **5156** – ***„Windows Filtering***	***„Security“***

		Platform“ leido tinklo sujungimą **5157** – ***„Windows Filtering Platform“*** blokavo tinklo sujungimą **5158** – ***„Windows Filtering Platform“*** leido prisijungti prie lokalaus tinklo prievado **4946** – pakeistas ***„Windows“*** ugniasienės išimčių sąrašas. Taisyklė buvo pridėta **4947** – pakeistas ***„Windows“*** ugniasienės išimčių sąrašas. Taisyklė buvo modifikuota **4948** – pakeistas ***„Windows“*** ugniasienės išimčių sąrašas. Taisyklė buvo pašalinta **4950** – ***„Windows“*** ugniasienės nustatymai buvo pakeisti **4957** – ***„Windows“*** ugniasienė netaikė šios taisyklės:	
„AppLocker“	***„AppLocker“*** funkcionalumas gali veikti dviem režimais: auditavimo ir priverstiniu (*angl. audit and enforce mode*). ***„AppLocker“*** funkcionalumas gali būtų įdiegtas tik ***„enterprise-level“*** operacinėse sistemose	**8003** – <failas .*exe/.*dll> buvo paleistas, bet bandymas paleisti būtų užblokuotas jeigu ***„AppLocker“*** funkcionalumas būtų įgalintas (auditavimo režimas) **8006** – <failas .*msi> arba <skriptas> buvo paleistas, bet bandymas paleisti būtų užblokuotas jeigu ***„AppLocker“*** funkcionalumas būtų įgalintas (auditavimo režimas) **8002** – <failą .*exe/.*dll> buvo leista įvykdyti **8004** – <failą .*exe/.*dll> buvo neleista įvykdyti **8005** – <failą .*msi> arba <skriptą> buvo leista įvykdyti **8007** – <failą .*msi> arba <skriptą> buvo neleista įvykdyti	***„AppLocker“***
Audito politika	Pokyčių, atliekamų audito politikoje, kontrolė	**4719** - sistemos audito politika buvo pakeista	***„Security“***
		6005 – įvykių žurnalų servisas startavo	***„System“***
USB įrenginiai	USB įrenginių kontrolė. Pagal nutylėjimas įvykių žurnalas yra išjungtas.	**2003** – įkeliamos tvarkyklės, kad būtų galima valdyti naują įrenginį **2010** – įkeliamos tvarkyklės, kad būtų galima valdyti naują įrenginį. **2101** – ***„Pnp“*** ar ***„Power Management“*** operacija tam tikram įrenginiui	***„Microsoft-Windows-DriverFrameworks-UserMode/Operational“***
Failų ir katalogų prieiga	Failų ir katalogų prieigos kontrolė, laibai triukšminga – sugeneruojamas didelis	**4656** – prieiga prie objekto buvo paprašyta **4660** – objektas buvo pašalintas **4663** – bandoma nuskaityti | įrašyti |	***„Security“***

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

	įvykių skaičius. Reikalingi atskiri prieigos kontroles sąrašai (*angl. ACL*), kuriuose būtų nurodyti audituojami objektai (failai | katalogai)	ištrinti objektą	
Bevielio tinklo prieiga	Prieigos prie bevielio tinklo kontrolė	**11000** – bevielio tinklo asociacija pradėta **8001** – sėkmingas prisijungimas prie bevielio tinklo **8002** – nesėkmingas prisijungimas prie bevielio tinklo	***„Microsoft-Windows-WLAN-AutoConfig/Operational“***