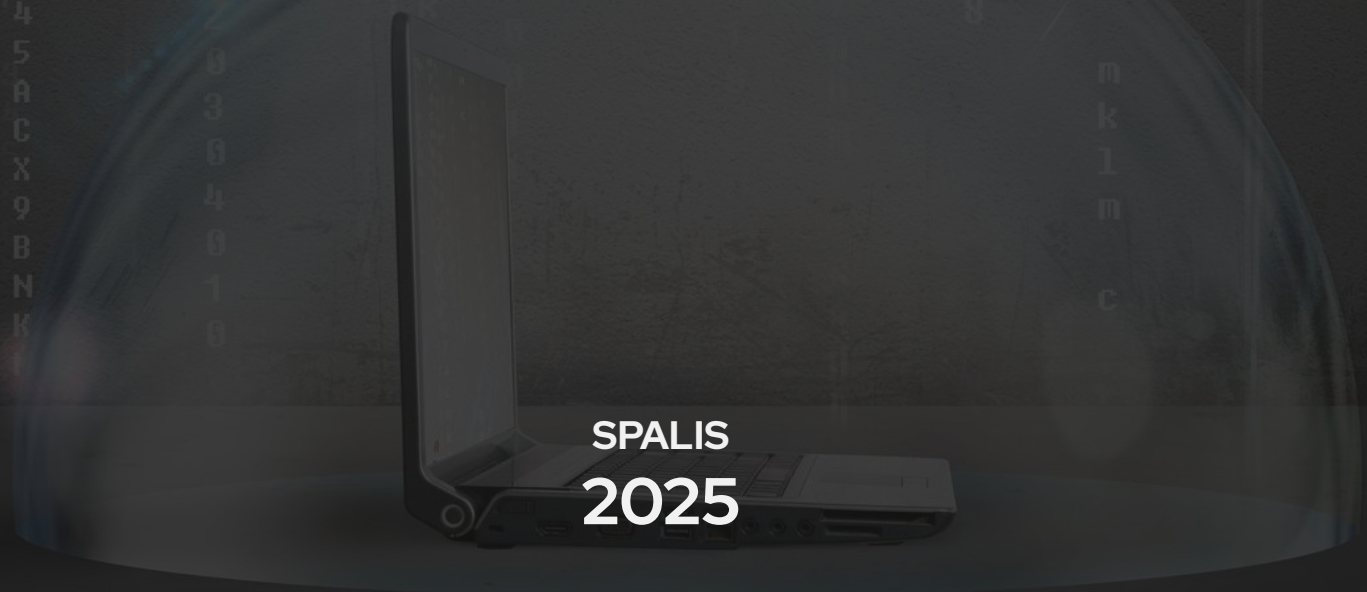
NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

REKOMENDACIJA ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS NAUDOJIMUI



SPALIS
2025

Bendrai finansuoja Europos Sąjunga

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.

Turinys

NKSC rekomendacija

ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS NAUDOJIMUI

Rekomendacijų tikslas

Šiame informaciniame leidinyje pateikiamos gairės, kokių veiksmų reikėtų imtis suveikus antivirusinei programinei įrangai (toliau – AV) bei kaip reikėtų elgtis su aptiktais kenkėjiškais failais. Šiuo leidiniu siekiame kibernetinio saugumo subjektams (toliau – organizacijoms, KSS) glaustai pateikti informaciją apie antivirusinės programinės įrangos svarbą, užtikrinant organizacijos tinklų ir informacinių sistemų (toliau – TIS) saugą, ir apie veiksmus, kuriuos būtina atlikti, esant AV įspėjimams. AV įspėjimas yra svarbus galimo kibernetinio incidento indikatorius, kurio negalima ignoruoti, todėl įvykus įspėjimui būtina imtis tolesnių veiksmų pranešant ir tiriant įvykį.

Auditorija

Šios rekomendacijos yra orientuotos į KSS ir jų darbuotojus, įskaitant ir tuos, kurie užtikrina kibernetinį saugumą ar valdo įdiegtą AV.

Esama situacija

Pastebima, jog dažniausiai AV įspėjimas yra ignoruojamas, nors jis gali organizaciją įspėti apie kylančią grėsmę. Pastebėjus kenkėjišką failą, dažnai jis naudotojo yra tiesiog šalinamas ar į jį nekreipiamas dėmesys, nesureikšminant įvykio. Tokiu atveju nėra informuojama organizacijos kibernetinio saugumo komanda, o tai mažina organizacijos galimybes įvertinti esamą saugumo situaciją, valdyti grėsmes bei potencialiai gerinti turimas kontrolės priemones. Laiku nepranešus apie AV įspėjimą, gali lemti tai, kad organizacijoje įvyks kibernetinis incidentas ir jo poveikis plis nestabdomas, o tuo atveju, kai kenkėjiškas failas ištrinamas, gali būti sunaikinti įkalčiai ir apsunkintas kibernetinio incidento tyrimas.

Neišsiaiškinus, kaip ir kodėl kenkėjiška programa pateko į TIS galutinio naudotojo įrenginį bei nesurinkus reikiamos informacijos apie jos veikimą, išlieka didelė tikimybė, kad panašus įvykis gali pasikartoti. Atsižvelgiant į tai, kad šiuolaikinės kenkėjiškos programos tampa vis pažangesnės, o tipinis kenkėjiškas kodas geba slėptis tarp įprastų sistemos failų, būtina nuolat didinti ne tik techninio personalo, bet ir visų kitų organizacijos darbuotojų sąmoningumą ir kompetencijas. Antivirusinės programinės įrangos įspėjimai turi būti vertinami atsakingai, o į kiekvieną įvykį reikia reaguoti pagal nustatytas procedūras.

ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS VEIKIMAS

AV yra svarbi prevencinė įrenginių saugumo kontrolės priemonė, leidžianti didinti bendrą TIS saugumo lygį. Ji automatiškai arba pagal poreikį analizuoja įrenginyje esančius ir naujai atsisiųstus failus bei nuorodas el. pašte ar naršyklėje, tikrindama jų parašus ir elgseną. Aptikus kenkėjišką veiklą, nuorodos blokuojamos, o failai izoliuojami ir sustabdomi jų procesai. Jos veikimas grindžiamas keliais pagrindiniais metodais, kurie leidžia efektyviai vykdyti kenkėjiškų failų paiešką ir apsaugoti tiek asmeninius įrenginius, tokius kaip kompiuteriai ar telefonai, tiek organizacijų infrastruktūrą.

Pagrindiniai AV veikimo principai

Tikrinimas, kuris grindžiamas parašų palyginimu (angl. *Signature-based*).

Parašas – tai unikali duomenų seka arba maišos kodas, leidžiantis identifikuoti specifinę kenkėjišką programą. Šis metodas remiasi žinomų kenkėjiškų programų parašų palyginimu su įrenginyje esančiais failų parašais. Jei failo parašas sutampa su AV duomenų bazėje esančiu kenkėjiškos programos parašu, tuomet toks failas yra laikomas grėsme ir yra blokuojamas arba pašalinamas.

Tikrinimas, kuris grindžiamas elgsena (angl. *Behavior-based*).

Šis metodas stebi programų vykdomus procesus realiu laiku. Remiantis turima elgsenos duomenų baze, AV siekia identifikuoti įtartiną ar neįprastą elgseną, pavyzdžiui, netikėtą šifravimo algoritmo naudojimą ar ryšius su nežinomais serveriais.

Tikrinimas, kuris grindžiamas euristine analize (angl. *Heuristic analysis*).

Šis metodas naudoja taisyklių ir vertinimo modelių rinkinį, leidžiantį aptikti anksčiau nežinomą ar modifikuotą kenkėjišką kodą, pagrįstą įtartinais failų požymiais arba programos elgsena. Pavyzdžiui, elgsena grindžiama analizė nurodo, kokia veikla stebima, o euristinė – kaip ši veikla vertinama sprendimui priimti. Šis metodas yra dažnai naudojamas kovojant su nulinės dienos (angl. Zero-day) grėsmėmis, kadangi to negali padaryti parašais grindžiami metodai.

AV SPRENDIMŲ TIPAI

Rinkoje egzistuoja keli pagrindiniai antivirusinės programinės įrangos tipai – tai atvirojo kodo (angl. *Open-source*), komerciniai, integruoti (angl. *Native*) bei naršyklėje prieinami sprendimai (angl. *Web-based*).

Kadangi kiekvienas iš jų turi skirtingas stipriąsias ir silpnąsias savybes, rekomenduojama neapsiriboti vienu sprendimu. Integruotus AV sprendimus galima papildyti atvirojo kodo arba komercinėmis priemonėmis, siekiant didesnio atsparumo kibernetinėms grėsmėms.

Atvirojo kodo antivirusinės programinės įrangos sprendimai
(angl. Open-source)

Tai atvirojo kodo antivirusinės programos, kurias gali atsisiųsti, naudoti ir pritaikyti pagal savo poreikius kiekvienas naudotojas. Jos dažniausiai veikia ir Windows, ir Linux operacinėse sistemose ir yra grindžiamos parašų principu. Vienas iš atvirojo kodo sprendimų yra Cisco gamintojo siūlomas „ClamAV“. Ši AV yra naudojama failų ir el. pašto duomenų srautų skenavimui. Nors jos funkcionalumas gali būti ribotas, lyginant su komerciniais produktais, tačiau šis sprendimas gali būti naudojamas kaip papildomas apsaugos sluoksnis, organizacijai turint ribotą biudžetą.

Integruoti antivirusinės programinės įrangos sprendimai
(angl. Native)

Tai operacinės sistemos gamintojo oficialiai palaikomi ir į pačią operacinę sistemą integruoti sprendimai:

Microsoft Windows

Microsoft Windows. WinOS rekomenduojama naudoti **Microsoft Defender**, numatytąjį apsaugos sprendimą, kuris veikia WinOS 10/11 sistemose. Jis veikia realiu laiku, aptinka jau įregistruotus grėsmių modelius, palaiko ir atlieka elgsenos analizę, apsaugo nuo spragų išnaudojimo (angl. Exploit) bei yra centralizuotai valdomas per Microsoft IT ūkio valdymo sprendimus. Renkantis papildomą AV sprendimą WinOS platformoje, naudotojai turėtų teikti pirmenybę toms AV, kurios palaiko **AMSI** (*Anti-Malware Scan Interface*), nes tokia antivirusinė programinė įranga užtikrina suderinamumą su Windows atnaujinimais ir saugumo funkcijomis.

Apple macOS

Apple kompiuteriuose kaip AV sprendimas yra integruota **XProtect** programinė įranga. Tai gamintojo palaikomas parašų palyginimu grįstas (angl. Signature-based) sprendimas, tikrinantis ir pašalinantis kenkėjiškus komponentus. XProtect veiksmingumas yra pakankamas individualiam naudotojui, tačiau, nors MacOS architektūroje yra gamintojo integruotos papildomos kontrolės priemonės, organizacijos lygmenyje papildomai rekomenduotume taikyti ir kitus AV sprendimus.

Linux operacinių sistemų šeima

Unix tipo operacinės sistemos, kaip: Ubuntu ar Debian, yra lanksčiai konfigūruojamos. Dėl itin didelio lankstumo ir minimalios techninės įrangos apkrovos, Linux distribucijos įprastai yra diegiamos aptarnaujančiuose kompiuteriuose, kur yra būtina maža techninių resursų apkrova ir lanksčiai valdoma konfigūracija. Dėl pakankamai lanksčios Linux OS platformos konfigūravimo ir dažnai kritinių išteklių palaikymo yra rekomenduojama įdiegti AV sprendimus.

Komerciniai antivirusinės programinės įrangos sprendimai

Komercinė AV gali būti ir įrenginyje veikianti programa (angl. Agent-based), ir naršyklėje veikianti paslauga (angl. Web-based). Įprastai komerciniai AV sprendimai pasiskirsto į kelis tipus ir siūlo platesnį funkcionalumų pasirinkimą negu integruoti ar atvirojo kodo sprendimai, pvz., ugniasienę, el. pašto apsaugą, duomenų nutekėjimo prevenciją (angl. Data Leak Prevention (DLP)), failų integralumo stebėjimą (angl. File Integrity Monitoring (FIM)) ar aktyvų reagavimą į grėsmes (angl. Endpoint Detection and Response (EDR)).

Agentu paremti sprendimai (angl. Agent-based).

Tai antivirusinės programos, kurios veikia kaip įrenginyje įdiegti agentai (klientai). Šie agentai nuolat veikia fone, stebi sisteminius įvykius, tikrina failus, procesus bei tinklo veiklą realiuoju laiku. Toks veikimo principas būdingas ir kai kuriems atvirojo kodo sprendimams.

Įrankiai, prieinami interneto naršyklėje *(angl. Web-based)*.

Taip pat negalime pamiršti ir įrankių, veikiančių interneto naršyklėse. Naršyklėje prieinami įrankiai leidžia analizuoti įkeliamus failus ir adresų nuorodas. Svarbu pažymėti, kad šie įrankiai gali būti naudojami tik kaip papildoma apsauga prie esamo AV sprendimo, bet ne ją pakeisti. Dažnai jie veikia tik po failo patekimo į sistemą ir neturi aktyvios stebėsenos funkcijos. Taip pat į šiuos įrankius neturėtų būti keliami nevieši organizacijos failai, nes įkeltas failas tampa prieinamas trečiosioms šalims. Išimtis yra taikoma tada, kai pats failas nėra keliamas, bet yra įkeliamas tik failo maišos kodas (angl. hash).

AV sprendimų integracija su kitais saugumo sprendimais

AV gali veikti kaip savarankiški sprendimai arba būti integruotos į platesnio funkcionalumo saugumo sprendimus, tokius kaip:

EDR (angl. *Endpoint Detection and Response*).

Skirta aptikti, tirti, skanuoti ir reaguoti į grėsmes galiniuose įrenginiuose, tokiuose kaip kompiuteriai ar telefonai.

XDR (angl. *Extended Detection and Response*).

Išplečia EDR galimybes, apimdama kelias TIS paslaugas, įskaitant tinklo, debesų ir el. pašto apsaugą.

NDR (angl. *Network Detection and Response*).

Orientuotas į grėsmių analizę ir identifikavimą tinklo lygmenyje. NDR sprendimai taiko elgsenos analizę ir mašininio mokymosi metodus apdorodami pirminius tinklo duomenų paketus (angl. Raw network packets) bei metaduomenis, susijusius su vidiniu ir išoriniu tinklo srautu. Tokiu būdu identifikuojami net ir pažangiai užmaskuoti atakų modeliai ar ryšių anomalijos, kurie gali likti nepastebėti įprastomis, galinių taškų saugumo priemonėmis.

MDR (angl. *Managed Detection and Response*).

Tai trečiųjų šalių teikiama saugumo paslauga, kuri ne tik analizuoja ir aptinka grėsmes, bet ir aktyviai reaguoja į incidentus 24/7 režimu. MDR sprendimai dažnai apima EDR, NDR ir XDR sprendimų funkcijas ir suteikia galimybes turėti daugialypę TIS apsaugą mažoms bei vidutinėms įmonėms, neturinčioms vidinio saugumo operacijų centro (SOC).

Pastaruoju metu pastebima, kad kenkėjiškos programos naudoja daugiaformį (angl. *Polymorphic code*) ar užšifruotą kodą (angl. *Encrypted code*), todėl kenkėjišką programinę įrangą tampa vis sunkiau aptikti, naudojant tik parašais grįstus metodus. Dėl šios priežasties, daugelis AV sprendimų naudoja elgsena grindžiamą analizę, siekdami identifikuoti kenkėjišką veiklą realiu laiku.

AV yra būtina TIS saugumo kontrolės priemonė, tiek individualiuose įrenginiuose, tiek organizacijos infrastruktūroje. Rekomenduojama naudoti kelis AV tipus ir neapsiriboti tik vienu, tokiu būdu būtų galima užtikrinti didesnę saugumo kontrolę galiniuose įrenginiuose.

GRĖSMĖS, KURIŲ PASIREIŠKIMĄ AR POVEIKĮ AV LEIDŽIA SUMAŽINTI

AV yra kibernetinio saugumo priemonė, skirta aptikti, izoliuoti ir pašalinti įvairias kenkėjiškas programas (angl. Malware), kurios gali padaryti žalą TIS, pavogti duomenis ar sutrikdyti organizacijos veiklą. AV padeda apsisaugoti nuo šių pagrindinių grėsmių:

Kenkėjiška programinė įranga (angl. *Malicious code / software / activity*). AV aptinka, pašalina ir izoliuoja kenkėjišką programinę įrangą, tokią kaip: virusai, Trojos arkliai, šnipinėjimo programos ar kitos.

Išpirkos atakos (angl. *Ransomware*). Šios atakos metu kenkėjiška programinė įranga užšifruoja naudotojo duomenis ir reikalauja išpirkos. AV padeda laiku identifikuoti ir užkirsti kelią šioms atakoms.

Socialinės inžinerinės atakos, sukčiavimas (angl. *Social engineering, phishing*). AV taip pat gali aptikti ir blokuoti kenkėjiškus priedus ar nuorodas, siunčiamus per el. paštą, kuriomis yra siekiama išvilioti neviešus organizacijos ar prisijungimo duomenis.

Jei antivirusinė sistema aptinka kenkėjišką kodą, itin svarbus greitas reakcijos laikas. Per šį laiką kenkėjiškas kodas gali spėti surinkti ir išsiųsti piktavaliui naudotojo slaptažodžius, kompiuteryje esančią informaciją, įdiegti papildomų programų ar plėtinių, pakeisti registrus ir pan., todėl svarbu nedelsiant imtis tolesnių veiksmų ir apsaugos priemonių.

VEIKSMAI, KURIŲ REIKĖTŲ IMTIS GAVUS AV ĮSPĖJIMĄ

Pirmi organizacijos darbuotojų veiksmai, kai aptinkamas kenkėjiškas failas

AV aptikti kenkėjiški failai yra svarbi medžiaga kibernetinio incidento tyrimui. AV įspėjimus apie identifikuotą įtartiną ar kenkėjišką failą, pirmiausia, reikėtų nedelsiant perduoti organizacijos SOC, kibernetinio saugumo skyriui ar atitinkamiems IT saugumo specialistams, tam, kad organizacija galėtų įvertinti situaciją, ar nebuvo padaryta žala TIS. Šis pranešimas leistų pradėti pirminę įvykio analizę, įvertinti situaciją ir užtikrinti tolesnį tyrimo procesą, kai įvykis priskiriamas kibernetinio incidento kategorijai.

Neatlikus išsamaus incidento tyrimo ir neišsiaiškinus atsiradimo priežasčių bei pasekmių, išlieka didelė tikimybė, kad incidentas pasikartos ir nebus nustatytas poveikio mastas ar įgyvendintos riziką mažinančios priemonės.

Tolesni kibernetinio saugumo specialistų atliekami veiksmai

Pirmiausia, kibernetinis incidentas lokalizuojamas, kai atliekami šie veiksmai:

- Paveikto galinio įrenginio izoliacija nuo tinklo – siekiant užkirsti kelią grėsmei toliau plisti organizacijos TIS.
- Kenkėjiškų failų, procesų ar domenų blokavimas organizacijos saugumo sistemose, siekiant užkirsti kelią papildomoms atakoms.
- Naudotojo ir kitų suinteresuotų šalių informavimas apie darbo vietos ar įrangos izoliavimą, laikantis nustatytų organizacijos procesų.

Lokalizavus kibernetinį incidentą, atliekama tolesnė AV sistemos suveikimo grėsmės analizė ir įvertinama, kaip plačiai grėsmė galėjo išplisti. Nustatoma, ar failas buvo paleistas galiniuose įrenginiuose, kokius procesus sukūrė, ar bandė užmegzti ryšį su išoriniais IP adresais, ar atliko sistemos modifikacijas (pvz., keitė registro įrašus, diegė kenkėjišką kodą). Analizės metu yra svarbu įvertinti:

Failo kilmę:

kaip failas atsirado TIS, ar buvo gautas el. paštu, atsisiųstas, ar sukurtas vidinėje sistemoje.

Komunikaciją su kitomis sistemomis:

Išorinės sistemos: jei failas inicijuoja užkoduotą ar įtartiną ryšį su išoriniais IP adresais, tai gali būti įsilaužėlio komunikacijos serveris (angl. Command and Control) serverio indikatorius.

Vidinės sistemos: jei aptinkami prievadų ar pažeidžiamumų skenavimai, tinklo identifikavimo bandymai ar naudotojų teisių eskalavimo veiksmai, tai gali rodyti kenksmingą veiklą.

Lokalizavus kibernetinį incidentą ir atlikus grėsmės analizę, remiantis Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (NKSC) parengtu kibernetinio incidento tyrimui būtinos informacijos surinkimo ir išsaugojimo informaciniu biuleteniu, su galimai kenkėjiškais, antivirusinės programos aptiktais failais rekomenduojama toliau elgtis, laikantis šio veiksmų eiliškumo:

1. **Išsaugokite AV suveikimo informacinį pranešimą.** Neišjunkite antivirusinės pranešimo ir išsaugokite pateikiamą informaciją, pavyzdžiui, kur buvo aptiktas kenkėjiškas failas, kas buvo bandoma inicijuoti ir pan.
2. **Nesunaikinkite aptikto failo.** Jei tai leidžia situacija, venkite automatinio, skuboto ar neapgalvoto failo ištrynimo.
3. **Sukurkite operatyviosios atminties ir „kietojo“ disko atvaizdus.** Jei įtariama, kad kenkėjiška programa galėjo veikti atmintyje ar buvo paleista sistemoje, pirmiausia rekomenduojama padaryti „kietojo“ disko ir operatyviosios atminties (RAM) atvaizdus (angl. Image).
4. **Surinkite pirminę informaciją.** Naudodamiesi įrankiais bei komandomis (pvz., „Sysinternals Suite“, „Powershell“, „ps aux“ ar kitais), užfiksuokite esamą veikiančios sistemos (angl. Live) informaciją.
5. **Išsaugokite įvykių žurnalus.** Įsitikinkite, kad visi įvykiai iš specifinių žurnalų, pvz., `C:\Windows\System32\winevt\Logs`, `/var/log/` ar kitų, yra eksportuoti ir apsaugoti nuo tolesnių pakeitimų.
6. **Surinktą informaciją apsaugokite.** Surinktus tyrimo duomenis saugokite, užtikrinkite jų autentiškumą ir integralumą. Efektyviausias būdas tai atlikti yra laikyti surinktą informaciją kontroliuojamoje aplinkoje bei apskaičiuoti failo kontrolinę sumą.
7. **Dokumentuokite visus veiksmus.** Surašykite atliktų tyrimo veiksmų eigą, naudotus įrankius, komandas, grėsmių indikatorius (angl. Indicators of Compromise (IoC)) ir kitą surinktą informaciją.

Detalesnę informaciją apie įkalčių surinkimą, išsaugojimą ir perdavimą galite rasti šiuo adresu:

https://www.nksc.lt/doc/biuleteniai/2024_01_29_irodymu%20issaugojimas.pdf

PRANEŠIMO APIE AV SUVEIKIMĄ SVARBA

AV suveikimas – tai potencialus kibernetinio incidento indikatorius, kurio ignoravimas gali sukelti rimtas pasekmes organizacijos viduje. Vadovaujantis Kibernetinio saugumo reikalavimų aprašu (toliau – KSRA) ir Nacionaliniu kibernetinių incidentų valdymo planu, KSS privalo fiksuoti, analizuoti ir, priklausomai nuo situacijos rimtumo, apie tokius incidentus pranešti NKSC.

Visi pranešimai apie kibernetinį incidentą padeda NKSC atlikti valstybinio lygmens grėsmių stebėseną ir analizę, o surinkta informacija naudojama:

- **Identifikuoti pasikartojančius atakų modelius;**
- **Identifikuoti potencialias plataus masto grėsmes;**
- **Rengti įspėjimus kitoms organizacijoms;**
- **Stiprinti nacionalinius kibernetinio saugumo pajėgumus.**

Organizacijose identifikuojami ir registruojami antivirusinių įspėjimų įvykiai leidžia objektyviai įsivertinti, ar turimos kibernetinio saugumo priemonės yra pakankamos. Tokie pranešimai rodo, kad AV suveikė tinkamai, tačiau kenkėjiška programa galėjo patekti į sistemą neaptikta kitų apsaugos priemonių, tokių kaip: el. pašto filtravimas, ugniasienė ar tinklo srauto tikrinimas. Kuo ankščiau grėsmė identifikuojama, tuo yra mažesnis galimas kibernetinės grėsmės poveikis organizacijai.

Informacijos perdavimas NKSC

Kibernetinio incidento atveju yra būtina vadovautis organizacijoje patvirtintu kibernetinių incidentų valdymo planu, nustatančiu atsakomybės paskirstymą, informacijos perdavimą ir pranešimo apie incidentą tvarką.

Prieš pranešant apie incidentą NKSC yra atliekamas esamos situacijos vertinimas:

- įvertinamos sutrikusios paslaugos ir jų apimtis;
- nustatomi (galimi) finansiniai nuostoliai;
- vertinama, ar incidentas paveikė trečiuosius asmenis, kokia žala jiems padaryta;
- įvertinamas incidento suvaldymo lygis;
- surenkami techniniai įrodymai.

Sukaupus reikiamą informaciją apie incidentą pranešama NKSC, vadovaujantis Kibernetinio saugumo įstatymo 18 straipsnio nuostatomis ir KSRA III skyriaus 14-18 punktų reikalavimais. **Apie kibernetinį incidentą galima pranešti vienu iš šių būdų:**

- elektroninio pašto adresu cert@nksc.lt, informaciją teikiant šifruotu pranešimu (naudojant NKSC viešąjį raktą 0x3956D9B5);
- telefonu 1843;
- interneto svetainės adresu https://www.nksc.lt/pranesti.html ;
- per Nacionalinę kibernetinių incidentų valdymo platformą Kibernetinio saugumo informacinė sistema (KSIS), https://www.nksc.lt/ksis.

Jei incidentas tęsiasi ilgiau negu mėnesį, informacija turėtų būti toliau reguliariai bent kartą per mėnesį atnaujinama. NKSC gali prašyti teikti ir tarpines ataskaitas ar papildyti duomenis.

ANTIVIRUSINĖS PROGRAMOS PASIRINKIMO KRITERIJAI

Tinkamo antivirusinio sprendimo pasirinkimas priklauso nuo daugelio veiksnių, tačiau efektyviausia apsauga pasiekiama tada, kai yra derinami keli, skirtingi AV tipai, pvz., integruotas ir komercinis ar atvirasis kodas. Renkantis antivirusinę programinę įrangą, rekomenduojama atsižvelgti į:

Organizacijos rizikos apetitą. Įvertinti, kokios grėsmės yra labiausiai tikėtinos konkrečiai organizacijai, atsižvelgiant į organizacijos vykdomą veiklą.

Turimą IT infrastruktūros apimtį. Įvertinti, kokios operacinės sistemos ir įrenginiai naudojami, ar yra reikalinga apsauga mobiliesiems įrenginiams, serveriams ir pan. Efektyviausias būtų AV sprendimas, galintis reikalingais funkcionalumais padengti visus įrenginius.

Esamų saugumo sprendimų suderinamumą. Įvertinti, ar siekiamas AV sprendimas būtų suderinamas su jau naudojamomis saugumo priemonėmis.

Biudžetą ir palaikymo galimybes. Įvertinti, ar organizacijoje numatytas biudžetas padengtų mokamus sprendimus, ar būtų įmanomas hibridinis riboto mokamų ir atvirojo kodo AV sprendimų diegimas.

ANTIVIRUSINĖS PROGRAMOS PALAIKYMAS IR HIGIENA

Dažnai šiuolaikiniai AV sprendimai turi įjungtą automatinį programinės įrangos atnaujinimą tam, kad naudotojas būtų apsaugotas nuo aktualiausių kenkėjiškų sprendimų. Norint užtikrinti maksimalų AV sprendimo efektyvumą, yra būtina laikytis šių esminių principų:

Reguliariai atnaujinkite operacinę sistemą ir AV. Jei įmanoma, įjunkite automatinius atnaujinimus, kad būtų įdiegti naujausi saugumo pataisymai.

Reguliariai vykdykite įrenginio failų skenavimą. Skenavimas reikalingas, kad aptiktumėte ir pašalintumėte ankščiau nepastebėtas grėsmes. Net jei antivirusinė veikia realiu laiku, periodiniai patikrinimai leidžia aptikti anksčiau neidentifikuotas, paslėptas ar su uždelstu veikimu aktyvuojamas grėsmes.

Reguliariai tikrinkite, ar AV tikrai veikia. Dalis kenkėjiškų sprendimų siekia išjungti antivirusinę apsaugą ar pakeisti jos nustatymus, todėl svarbu periodiškai patikrinti, ar antivirusinė programinė įranga įjungta ir aktyvi, ar ji veikia be trikdžių.

Neišjunkite AV net trumpam. Oficialius, integruotus antivirusinės programinės įrangos sprendimus visada rekomenduojama laikyti įjungtus . Jei būtina sustabdyti tam tikrą funkciją (pvz., failų izoliavimą), tai turėtų būti daroma tik išimtiniais atvejais, kontroliuojant aplinką ir esant kibernetinio saugumo įgaliotinio patvirtinimui.

Rinkitės AV iš patikimo tiekėjo. Rekomenduojama naudoti teigiamą reputaciją turinčių, viešai audituojamų ir draugiškų valstybių gamintojų AV. Naudojant nežinomą ar nepatikimą sprendimą kyla rizika, kad produktas gali būti neefektyvus, pasenęs ar net kenkėjiškas.

Patikima ir nuolat veikianti antivirusinė sistema yra viena iš svarbiausių pirmosios gynybos linijos priemonių, tačiau tik tuo atveju, kai ji nuosekliai prižiūrima ir nuolatos veikia.

ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS NAUDOJIMAS

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

AV yra svarbi prevencinė įrenginių saugumo kontrolės priemonė, leidžianti didinti bendrą TIS saugumo lygį.

Grėsmės, kurias AV padeda suvaldyti

- Kenkėjiška programinė įranga
- Išpirkos atakos
- Socialinės inžinerinės atakos, sukčiavimas

Pagrindiniai AV veikimo principai

- Tikrinimas, kuris grindžiamas **parašų palyginimu.**
- Tikrinimas, kuris grindžiamas **elgsena.**
- Tikrinimas, kuris grindžiamas **euristine analize.**

Veiksmai, kurių reikėtų imtis gavus AV įspėjimą

Pirmiausia praneškite organizacijos SOC ar IT saugumo specialistams, kad būtų įvertinta situacija ir galima žala TIS.

Tolesni kibernetinio saugumo specialistų atliekami veiksmai:

- Paveikto galinio įrenginio izoliacija nuo tinklo
- Kenkėjiškų failų, procesų ar domenų blokavimas
- Naudotojo ir kitų suinteresuotų šalių informavimas

Pranešimai apie kibernetinius incidentus padeda NKSC stebėti ir analizuoti grėsmes, identifikuoti atakų modelius, įspėti organizacijas bei stiprinti nacionalinį kibernetinį saugumą.

Detalesni specialistų veiksmai pateikti rekomendacijose →

Antivirusinės programos palaikymas ir higiena

- Reguliariai atnaujinkite operacinę sistemą ir AV
- Reguliariai vykdykite įrenginio failų skenavimą.
- Reguliariai tikrinkite, ar AV tikrai veikia.
- Neišjunkite AV net trumpam.
- Rinkitės AV iš patikimo tiekėjo.

Informacijos perdavimas NKSC

Kibernetinio incidento atveju vadovaukitės organizacijos incidentų valdymo planu, kuriame nustatyta atsakomybė ir pranešimo tvarka. Pranešti galima šiais būdais:

cert@nksc.lt *šifruokite naudodami raktą 0x3956D9B5*	1843	https://www.nksc.lt/pranesti.html	nksc.lt/ksis *per KSIS platformą*

Bendrai finansuoja Europos Sąjunga

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.