NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Liepa 2026

Rekomendacijos dėl kintančios kibernetinių grėsmių aplinkos

Turinys

Rekomendacijų tikslas

Kibernetinio saugumo srityje stebimas ryškus pokytis – naujai aptinkamų programinės įrangos pažeidžiamumų skaičius sparčiai auga, o piktavalių reakcijos laikas drastiškai trumpėja. Pastarųjų penkių metų pažeidžiamumų CVE (Common Vulnerabilities and Exposures) registracijos statistika rodo, jog kasmet užregistruojama apie 15 - 20% daugiau pažeidžiamumų nei ankstesniais metais, o laikas tarp paskelbimo apie pažeidžiamumą ir jo išnaudojimo faktiškai sunyko. Viena iš to priežasčių - spartus dirbtinio intelekto (toliau - DI) modelių tobulėjimas. Anksčiau pažeidžiamumų paieška reikalavo specifinių ekspertinių žinių ir daug valandų darbo. Šiandien DI modeliai leidžia šį procesą automatizuoti, todėl pažeidžiamumų paieška tapo greitesnė, efektyvesnė ir prieinamesnė. Ta pati technologinė pažanga pagreitino ne tik pažeidžiamumų aptikimo, bet ir kenkėjiško kodo kūrimo bei išnaudojimo procesus.

Šios tendencijos neišvengiamai reikalauja ir kibernetinio saugumo politikos pokyčių. Organizacijų kibernetinio saugumo procesai turi tapti greitesni, vykdomi nuosekliai ir, kur įmanoma, automatizuoti. Infrastruktūra turi būti tiksliai inventorizuota ir nuolat stebima, kad naujai atsiradę pažeidžiamumai būtų kuo greičiau nustatomi ir pašalinami.

NKSC teikia rekomendacijas, kaip organizacijos galėtų sustiprinti savo kibernetinį saugumą ir labiau pasiruošti su DI susijusioms grėsmėms. Nors dauguma jų nėra naujos, jų aktualumas šiandien stipriai išaugo, o ateityje augs tik dar labiau

Infrastruktūros inventorizacija ir atakos paviršiaus mažinimas

Siekiant tinkamai apsaugoti savo organizacijos infrastruktūrą, pirmiausiai reikia ją pažinti ir suprasti - kokios tarnybos ir komponentai ją sudaro. Turi būti sudarytas ir nuolat atnaujinamas valdomos bei naudojamos infrastruktūros sąrašas. Jame turėtų būti fiksuojama bent tokie valdomus išteklius aprašantys duomenys:

IP adresų rėžiai, aktyvios tinklo tarnybos, naudojamos operacinės sistemos, programinė įranga bei jos versijos, žiniatinklio aplikacijos, debesijos paslaugos.

Ypatingas dėmesys turėtų būti teikiamas infrastruktūrai, kuri yra pasiekiama už organizacijos tinklo vidaus, t.y. internetu.

Šis sąrašas turėtų būti reguliariai peržiūrimas ir vertinama, ar visi jame esantys komponentai vis dar yra reikalingi organizacijos veiklai. Nustačius, jog dalis turimos infrastruktūros nereikalinga – ši turi būti pašalinta. Kiekviena papildoma viešai pasiekiama sistema didina riziką tapti automatizuotų skenavimų ar atakų taikiniu.

Taip pat, įsivertinti kaip ir kokiems naudotojams yra pasiekiama likusi infrastruktūra, ypatingai jos valdymo paslaugos (tokios kaip SSH, RDP, valdymo sąsajos pasiekiamos HTTP protokolu ir pan.), bei apsvarstyti galimybes sumažinti jos pasiekiamumą. Pavyzdžiui, riboti prieigą pagal leistinų IP adresų sąrašą, perkelti infrastruktūrą į vidinį tinklą, leisti prisijungti tik naudojant VPN ar kitas priemones.

Dažnėjančios tiekimo grandinės (angl. *supply chain*) atakos taip pat didina ir vidinėje infrastruktūroje naudojamos programinės įrangos, ypač atvirojo kodo (angl. *open-source)* komponentų inventorizacijos reikšmę

Programinės įrangos atnaujinimas

Dėl reikšmingai sutrumpėjusio laiko tarp pažeidžiamumo atskleidimo ir jo išnaudojimo, itin svarbu yra užtikrinti greitą pažeidžiamumų šalinimo procesą. Jeigu įmanoma, saugumo atnaujinimai turėtų būti diegiami automatizuotai ir kuo greičiau po jų išleidimo. Taip pat būtina iš anksto planuoti programinės įrangos gyvavimo ciklo pabaigą ir užtikrinti, kad nebūtų naudojama gamintojo nebepalaikoma programinė įranga.

Kita vertus, dėl išaugusio tiekimo grandinės atakų skaičiaus, rekomenduojama įsivertinti galimybę diegti **ne saugumo** atnaujinimus ne anksčiau kaip po keleto dienų ar ilgiau nuo jų išleidimo. Tai suteikia laiko atitinkamai reaguoti į tokios programinės įrangos kompromitavimo atvejus. Be to, tokius atnaujinimus rekomenduojama diegti etapais, o ne vienu metu visuose organizacijos įrenginiuose, kad kilus nenumatytoms problemoms, jų poveikis būtų kuo mažesnis. Tačiau kadangi dalis gamintojų saugumo pataisymus ir kitus programinės įrangos pakeitimus pateikia viename atnaujinimų pakete, organizacijos pačios turėtų įvertinti, ar tikslinga atidėti tokių atnaujinimų diegimą. Priimant sprendimą rekomenduojama atsižvelgti į ištaisomų saugumo spragų kritiškumą, jų išnaudojimo tikimybę, ar egzistuoja tinkamos sąlygos joms išnaudoti, ar pažeidžiama sistema yra pasiekiama iš interneto, bei galimas sėkmingo išnaudojimo pasekmes.

Jei įmanoma, organizacijos turėtų sudaryti naudojamos programinės įrangos sudėtinių dalių sąrašus (angl. *Software Bill of Materials*, SBOM), kurie padeda identifikuoti programinės įrangos komponentus ir jų tarpusavio priklausomybes, todėl leidžia greičiau įvertinti naujai atskleistų pažeidžiamumų poveikį organizacijos sistemoms.

Autentifikacijos saugumas

Nemaža dalis kibernetinių incidentų įvyksta dėl nutekintų prisijungimo duomenų arba slaptažodžių spėliojimo atakų. Siekiant sumažinti tokių incidentų tikimybę, rekomenduojama:

- Naudoti tik unikalius ir sudėtingus slaptažodžius. Minimalus slaptažodžio ilgis turėtų būti ne trumpesnis kaip 15 simbolių. Slaptažodį turėtų sudaryti mažosios ir didžiosios raidės, skaičiai bei specialieji simboliai. Rekomenduojama naudoti atsitiktinai sugeneruotus slaptažodžius ir juos saugoti slaptažodžių tvarkyklėse.

- Jei paslauga palaiko, vietoje slaptažodžių rekomenduojama naudoti prieigos raktus (angl. *passkeys*), kurie yra atsparesni fišingo atakoms ir nereikalauja slaptažodžių naudojimo.

- Visoms paskyroms, kuriose tai įmanoma, įjungti daugiaveiksnę autentifikaciją (angl. MFA). Papildomam autentifikacijos veiksniui rinktis saugias autentifikavimo programėles ar aparatinius autentifikavimo raktus.

- Jei įmanoma, įgalinti papildomas prieigos saugumo priemones, pavyzdžiui: leisti prisijungti tik iš patvirtintų IP adresų, naudoti klientų sertifikatus (*mTLS*), taikyti geografinį prieigos ribojimą ir kita.

- Riboti galimybes naudoti automatizuotus įrankius prisijungimo bandymams, taikant tokias priemones kaip CAPTCHA, užklausų dažnio ribojimas (angl. *rate limiting*), progresyvus delsimas po nesėkmingų prisijungimo bandymų ar laikinas paskyros arba IP adreso blokavimas. Žiniatinklio aplikacijas rekomenduojama apsaugoti žiniatinklio aplikacijų ugniasienėmis (angl. *Web Application Firewall*, WAF).

- API raktus ir kitus autentifikavimo duomenis saugoti saugiose paslapčių valdymo sistemose. Jų negalima saugoti programiniame kode ar viešose saugyklose. Šie raktai turėtų būti reguliariai rotuojami, suteikiant jiems tik būtinas prieigos teises ir, jei įmanoma, nustatant jų galiojimo laiką.

Pažeidžiamumų paieška

Organizacijos turėtų nuolat vykdyti savo informacinių sistemų ir infrastruktūros pažeidžiamumų paiešką, taikydamos tiek automatizuotas, tiek rankines vertinimo priemones. Rekomenduojama automatizuotą pažeidžiamumų skenavimą atlikti ne rečiau kaip kartą per ketvirtį, o papildomai – po reikšmingų infrastruktūros pakeitimų ar naujų sistemų diegimo. Siekiant įvertinti realų sistemų atsparumą ir nustatyti pažeidžiamumus, kurių automatizuoti įrankiai gali neaptikti, ne rečiau kaip kartą per metus rekomenduojama atlikti įsilaužimų testavimą (angl. *penetration testing*).

Taip pat organizacijos turėtų nuolat stebėti viešai skelbiamą informaciją apie naujai nustatytus pažeidžiamumus ir aktyviai išnaudojamas grėsmes, remdamosi Nacionalinio kibernetinio saugumo centro skelbiamais pranešimais, žinomų išnaudojamų pažeidžiamumų (angl. *Known Exploited Vulnerabilities*, KEV) katalogais bei programinės ir techninės įrangos gamintojų saugumo pranešimais. Nuolatinė stebėsena leidžia laiku identifikuoti organizacijai aktualias rizikas, tinkamai nustatyti jų prioritetus ir imtis pažeidžiamumų šalinimo veiksmų.

Kitos bendrinės rekomendacijos

Toliau pateikiame keletą papildomų bendrinių, tačiau ne mažiau svarbių rekomendacijų:

- **Tinklo ir išteklių segmentacija**. Tinklo ir informacinių išteklių segmentacija padeda apriboti galimo kibernetinio incidento plitimą, neleisdama užpuolikui laisvai judėti tarp skirtingų sistemų ir tinklo segmentų. Tinklas ir ištekliai turėtų būti suskirstyti pagal jų paskirtį ir jautrumo lygį, o ryšys tarp segmentų (ar tarp sistemų tame pačiame segmente, jei sistema atlieka kritines funkcijas) turėtų būti leidžiamas tik tada, kai jis yra būtinas veiklai.

- **Atsarginės kopijos**. Rekomenduojama reguliariai kurti svarbiausių duomenų, sistemų ir konfigūracijų atsargines kopijas, užtikrinant, kad jos būtų apsaugotos nuo neteisėto pakeitimo ar ištrynimo, o bent viena kopija būtų saugoma atskirai nuo pagrindinės infrastruktūros. Taip pat būtina reguliariai testuoti atsarginių kopijų atkūrimą, siekiant įsitikinti, kad po incidento organizacija galėtų efektyviai ir per priimtiną laiką atkurti savo veiklą.

- **Centralizuotas žurnalų kaupimas ir stebėsena**. Rekomenduojama užtikrinti centralizuotą sisteminių, programų ir kitų svarbių informacinių sistemų žurnalų (angl. logs) kaupimą bei jų nuolatinę stebėseną, naudojant SIEM ar panašius sprendimus. Tai leidžia laiku nustatyti saugumui reikšmingus įvykius, aptikti įtartiną veiklą ir operatyviai reaguoti į galimus kibernetinius incidentus.

- **Darbuotojų kibernetinio saugumo mokymai**. Organizacijos turėtų reguliariai vykdyti darbuotojų kibernetinio saugumo mokymus, siekdamos, kad darbuotojai gebėtų atpažinti dažniausiai pasitaikančias kibernetines grėsmes. Mokymų metu rekomenduojama supažindinti su fišingo (angl. *phishing*), kitų socialinės inžinerijos metodų bei dirbtinio intelekto pagalba kuriamų suklastotų garso ir vaizdo įrašų (angl. *deepfakes*) požymiais. Taip pat rekomenduojama periodiškai organizuoti praktines fišingo simuliacijas ir kitas pratybas, kurios padeda įvertinti darbuotojų pasirengimą, ugdyti saugaus elgesio įpročius ir mažinti žmogiškosios klaidos riziką.