VALSTYBINĖ
DUOMENŲ
APSAUGOS
INSPEKCIJA

VDAI dėmesys taikytoms saugumo priemonėms prieš incidentą

Valstybinės duomenų apsaugos inspekcijos
Informacinių technologijų skyriaus
vyriausioji specialistė
Žana Grekienė

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Išskirtinis dėmesys taikytoms IT saugumo priemonėms prieš įvykstant incidentui

Pagrindas greitam reagavimui ir veiklos atkūrimui

Nepakankamas dėmesys lemia duomenų praradimą ar sistemų sutrikimus

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Kodėl svarbus išskirtinis dėmesys saugumo priemonėms prieš incidentą

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Dažniausios pasekmės

Tinkamai neįgyvendintos ar visai netaikytos priemonės dažnai tampa pagrindine incidentų priežastimi, sudarančia sąlygas pažeidžiamumams išnaudoti ir sistemoms sutrikti

- Informacinių sistemų užšifravimas (angl. *ransomware*)
- Duomenų nutekėjimas ar praradimas
- Paslaugų nepasiekiamumas
- Finansiniai ir reputaciniai nuostoliai

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Silpna prieigos kontrolė

Problema

- Prieigos kontrolės **mechanizmai dažnai nepakankamai griežti**.
- Darbuotojai **turi platesnes prieigos teises nei reikia jų funkcijoms atlikti**, **nėra** įgyvendinta kelių faktorių autentifikacija (angl. ***MFA***), o prieigų teisių suteikimo peržiūra neatliekama periodiškai.

Pasekmės

- Piktavaliai gali **pasinaudoti pavogtais prisijungimo duomenimis**.
- Lengviau įvykdomi vidiniai (angl. *insider threat*) incidentai.
- **Prarandamas duomenų vientisumas ir konfidencialumas**.

Prevencija

- Įdiegti **kelių faktorių autentifikaciją (angl. *MFA*)** visiems naudotojams.
- Naudoti **„žemiausių prieigos teisių“ (angl. *least privilege*) principą**.
- **Reguliariai peržiūrėti ir atnaujinti** naudotojų prieigų teisės.
- **Dokumentuoti visus prieigos teisių suteikimo ir panaikinimo procesus**.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Neatnaujinta programinė įranga

Problema

- Organizacijos dažnai **atidėlioja atnaujinimų diegimą**, ypač kai tai reikalauja sistemų stabdymo ar testavimo.
- Tačiau neįdiegti atnaujinimai (angl. *patchai*) palieka **atviras duris kibernetinėms atakoms**.

Pasekmės

- **Išnaudojami žinomi pažeidžiamumai**.
- Į sistemą **įdiegiama kenkėjiška programinė įranga**.
- **Prarandamas** infrastruktūros patikimumas.

Prevencija

- Nustatyti aiškią **programinės įrangos atnaujinimo politiką**.
- Jei įmanoma, **automatizuoti atnaujinimų diegimą**.
- **Testuoti atnaujinimus** bandymų aplinkoje prieš diegiant į gamybinę.
- **Sekti gamintojų rekomendacijas** dėl saugumo pataisymų.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Tinklo apsaugos trūkumas

Problema

- Tinklo saugumo priemonės dažnai būna **nepakankamos arba netinkamai sukonfigūruotos.**
- **Ugniasienės, įsibrovimų aptikimo sistemos** ar **VPN** (angl. Virtual Private Network) sprendimai ne visada tinkamai sukonfigūruoti.

Pasekmės

- Į tinklą patenka **kenksmingas srautas**.
- Įvyksta **duomenų nutekėjimas** per išorinius kanalus.
- Užmezgamas ryšys su vadinamaisiais „Command and Control (C2)“ serveriais (*tai **pagrindiniai valdymo serveriai**, kuriuos naudoja **kibernetiniai nusikaltėliai** tam, kad **nuotoliniu būdu valdytų užkrėstus įrenginius** (pvz., kompiuterius, telefonus ar serverius)*.

Prevencija

- Tinkamai konfigūruoti **ugniasienes** ir **VPN** ryšius.
- Naudoti **IP filtravimo (angl. *whitelist*)** principą, ribojant prisijungimus.
- Įdiegti **tinklo srauto stebėseną** bei įsibrovimų aptikimo sistemas.
- Periodiškai **tikrinti tinklo konfigūracijos saugumą**.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Darbuotojų ne informuotumas

Problema

- Net ir moderniausios technologinės priemonės nepadės, jei **darbuotojai neatsargiai elgiasi su informacija**.
- **Žmogiškasis faktorius yra viena dažniausių atakų priežasčių**.

Pasekmės

- Sėkmingos „**phishing“ atakos**.
- **Į sistemą įkeliami kenksmingi failai**.

Prevencija

- Reguliarūs **kibernetinio saugumo mokymai** visiems darbuotojams.
- **Praktiniai testai** (pvz. imituoti „phishing“ laiškai).
- Vidinė **komunikacija** apie naujausias grėsmes.
- **Saugumo kultūros stiprinimas** organizacijos viduje.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Nėra atsarginių kopijų

Problema

- Kai duomenų atsarginės kopijos neatnaujinamos arba laikomos toje pačioje sistemoje, kuri užpuolama, jų atkūrimas tampa neįmanomas.

Pasekmės

- **Duomenų praradimas** po IS užšifravimo (angl. ***ransomware***) atakos.
- Ilgas sistemos atkūrimo laikas.
- Finansiniai ir reputaciniai nuostoliai.

Prevencija

- Daryti **reguliarias atsargines kopijas**.
- Naudoti **3-2-1 taisyklę**: 3 kopijos, 2 skirtingos laikmenos, 1 – atskirtoje vietoje.
- Reguliariai testuoti duomenų atkūrimo galimybes.
- Užtikrinti, kad kopijos būtų **užšifruotos** ir neprieinamos per pagrindinę sistemą.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Trūksta žurnalinių įrašų valdymo

Problema

- **Nėra sukonfigūruotos veiklos stebėsenos ar žurnalinių įrašų analizės**.
- Dėl to **incidentai** gali būti **nepastebėti ilgesnį laiką**.

Pasekmės

- **Nepavyksta nustatyti įsilaužimo priežasties**.
- **Sudėtinga atsekti** pažeidimo mastą.
- **Trūksta įrodymų tyrimui / vertinimui**.

Prevencija

- Įdiegti **centralizuotą žurnalų valdymo sistemą (SIEM)**.
- **Stebėti įtartiną veiklą realiu laiku**.
- Nustatyti žurnalų **saugojimo trukmę ir prieigos kontrolę**.
- Periodiškai **analizuoti** žurnalinių įrašų duomenis.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Nėra rizikų vertinimo ir testavimo

Problema

- **Be reguliaraus rizikų vertinimo** organizacija nežino, kokios grėsmės jai realiai gresia.
- **Nėra nustatoma, kur silpniausios vietos** ar kokių priemonių reikia tobulinimui.

Pasekmės

- Nepastebėti **pažeidžiamumai išlieka ilgą laiką**.
- Nėra prioritetų saugumo investicijoms.
- Incidentų valdymas tampa reaguojantis, o ne prevencinis.

Prevencija

- Atlikti **reguliarius rizikos vertinimus** (bent kartą per metus).
- Dokumentuoti rezultatus ir veiksmų planus.
- Įtraukti rizikų analizę į strateginį valdymą.
- **Testuoti saugumo priemones** po bet kokių Informacinių sistemų pokyčių.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Pažeidžiamumų skenavimas

Problema

- **Neskenuojant informacinių sistemų pažeidžiamumų**, nežinomos silpnos vietos lieka atviros ilgą laiką.
- Tai **leidžia** kibernetiniams nusikaltėliams **pasinaudoti** senais ar naujai atsiradusiais **trūkumais**.

Pasekmės

- **Įsilaužimai per viešai žinomus pažeidžiamumus (CVE)** (angl. *Common Vulnerabilities and Exposures - unikalus identifikatorius viešai žinomam saugumo pažeidžiamumui*).
- Duomenų nutekėjimai ar serverių kompromitavimas.
- Rizika, kad incidentas bus pastebėtas tik po ilgalaikio veikimo.

Prevencija

- Atlikti reguliariai **automatinį pažeidžiamumų skenavimą** (pvz. kartą per mėnesį).
- Naudoti specializuotus įrankius (pvz. *Nessus, OpenVAS, Qualys)*.
- Vykdyti **įsiskverbimo testus** (angl. *penetration testing*), ypač po sistemų atnaujinimo.
- Dokumentuoti aptiktus pažeidžiamumus ir jų šalinimo eigą.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Išvada

Dauguma kibernetinių incidentų įvyksta ne dėl „sudėtingų atakų“, o dėl **neįgyvendintų bazinių saugumo priemonių**.

Efektyvi saugumo sistema remiasi trimis principais:

Techninės priemonės

ugniasienės, antivirusinės programos, žurnaliniai įrašai, IS pažeidžiamumų skenavimas.

Žmonės

mokymai, atsakomybės, saugumo kultūra.

Procesai

prieigos valdymas, atnaujinimai, atsarginės kopijos, IS testavimai.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Rekomendacija

Rekomenduojama

Periodiškai vertinti taikytų saugumo priemonių veiksmingumą, atlikti jų testavimą (*pvz., pažeidžiamumų analizę, saugumo auditą*).

Atnaujinti jas pagal kintančias technologines grėsmes.

Tokiu būdu užtikrinamas nuolatinis pasirengimas incidentų prevencijai ir jų efektyviam reagavimui.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Ačiū

Prevencija visada kainuoja mažiau nei incidento padarinių likvidavimas.