NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

REKOMENDACIJOS ORGANIZACIJOS DEBESIJOS PASLAUGŲ SAUGUMUI UŽTIKRINTI

LAPKRITIS

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

ORGANIZACIJOS DEBESIJOS PASLAUGŲ SAUGUMO UŽTIKRINIMAS

Rekomendacijų tikslas

Debesijos aplinka yra dažnas taikinys dėl joje saugomų jautrių organizacijos duomenų, todėl tinkamai sukonfigūruotos saugumo kontrolės priemonės yra itin svarbios organizacijos tinklų ir informacinių sistemų (TIS) atsparumui. Šiame informaciniame leidinyje yra pateikiamos gairės, padėsiančios suprasti debesijos paslaugų grėsmes, gerinti jų saugumą bei mažinti kibernetinių incidentų tikimybę.

Auditorija

Šios rekomendacijos yra orientuotos į kibernetinio saugumo subjektus (toliau – organizacijos), naudojančius debesijos paslaugas.

Esama situacija

Debesijos paslaugos yra dažnai naudojamos daugelyje organizacijų. Remiantis European Union Agency for Cybersecurity (ENISA) 2024 metų grėsmių apžvalga, debesijos paslaugų naudojimas išlieka aukštas, ENISA apžvalgoje dalyvavę respondentai vidutiniškai naudojasi daugiau nei dviem debesijos paslaugų teikėjais, o daugiau kaip 47 % duomenų, laikomų debesijos aplinkoje, respondentų yra įvardijami kaip jautrūs ir nevieši.

Piktavaliai supranta šių paslaugų naudojimo mastą bei siekia jas išnaudoti savo tikslais. Dažnai piktavaliai ne tik vykdo atakas prieš debesijos aplinką, tačiau ir naudojasi debesijos paslaugomis ir patikimomis svetainėmis siekdami išvengti vykdomų atakų aptikimo – tai yra vadinama „naudojimusi patikimomis svetainėmis“ (angl. L*iving Off Trusted Sites,* LOTS). Pasitelkdami teisėtas debesijos paslaugas, piktavaliai siekia paslėpti savo veiklą ir naudodami specialiai paruoštas nuorodas tikisi apeiti organizacijų vykdomą tinklo srauto filtravimą.

Siekiant valdyti šias grėsmes rekomenduojame remtis Lietuvos Respublikos kibernetinio saugumo įstatymu (toliau – KSĮ), kuris perkelia Europos Tinklų ir Informacinių sistemų (toliau – TIS2) (angl. *Network and Information Security 2 Directive* arba NIS2) direktyvos nuostatas bei įpareigoja organizacijas užtikrinti ne tik tinkamą TIS kibernetinį saugumą, bet ir apsaugoti debesijos aplinką, vykdyti jai aktualią rizikų analizę, valdyti su debesijos aplinka susijusius incidentus bei užtikrinti tiekimo grandinės saugumą.

Debesijos paslaugų veikimo principai ir teikimo modeliai

Debesijos paslaugos suteikia galimybę organizacijos informacinius išteklius perkelti į nuotoliniu būdu pasiekiamą duomenų centrą („debesį“, angl. *cloud*), kurio fizinę priežiūrą užtikrina ir vykdo trečioji šalis (debesijos paslaugų teikėjas).

Organizacijos, pasitelkusios trečiąsias šalis (debesijos paslaugų teikėjus), gali naudotis darbo įrankiais, komunikacijos priemonėmis, duomenų talpyklomis ir serverių bei infrastruktūros aplinka, nepriklausomai nuo pačios organizacijos ar jos įrenginių fizinės vietos.

Debesijos paslaugų teikimo modeliai

IaaS. Tai paslaugų teikimo modelis, kuomet organizacija nuomojasi duomenų centro (debesijos) infrastruktūros išteklius – virtualius serverius (angl. *Virtual Private Server*, VPS), saugyklas, tinklo valdymą iš debesijos paslaugų teikėjų, tokių kaip: „*Microsoft Azure*“, „*Google Cloud Platform*“, „*Amazon Web Services* (AWS)“ ar kitų. Debesijos paslaugų teikėjas užtikrina tik fizinės įrangos ir tinklo infrastruktūrą, o klientas yra atsakingas už operacinių sistemų, aplikacijų, konfigūracijų ir duomenų saugumą. Šis modelis organizacijai suteikia daugiausiai lankstumo, tačiau didžiausia atsakomybės našta dėl saugumo užtikrinimo tenka pačiai organizacijai.

PaaS. Tai paslaugų teikimo modelis, kuomet organizacija nuomojasi aplikacijų kūrimui skirtą platformą iš debesijos paslaugų teikėjo, pavyzdžiui, *„Microsoft Azure App Service“, „Google App Engine“ ar „AWS Elastic Beanstalk“*. Debesijos paslaugų teikėjas užtikrina infrastruktūrą, operacinę sistemą, programinę įrangą ir duomenų bazes, o perkančioji organizacija dažnu atveju yra atsakinga tik už savo kuriamas aplikacijas, jų duomenis bei saugumą. Šis modelis leidžia organizacijai sutelkti dėmesį į aplikacijų kūrimą ir diegimą, sumažinant infrastruktūros priežiūros poreikį, tačiau už pačių aplikacijų saugumą atsakomybė tenka pačiai organizacijai.

SaaS. Tai paslaugų teikimo modelis, kuomet organizacija naudojasi trečiosios šalies teikiamomis programinės įrangos paslaugomis, kurios pasiekiamos per interneto naršyklę ar specialias aplikacijas, tokios programinės įrangos pavyzdžiai yra: *„Microsoft 365“, „Google Workspace“* ir *„Zoom“*. Programinė įranga šiuo atveju nėra perkama ar licencijuojama įprastiniu būdu – ji iš esmės yra nuomojama iš paslaugų teikėjo. Visi programinės įrangos diegimo, atnaujinimo ir infrastruktūros priežiūros klausimai yra debesijos paslaugų teikėjo atsakomybė, o organizacija rūpinasi tik prieigos valdymu, naudotojų teisių konfigūravimu ir duomenų apsauga SaaS platformoje.

Debesijos paslaugų teikėjai organizacijoms suteikia galimybę lanksčiai ir pagal poreikį keisti naudojamų IT išteklių apimtį, centralizuotai valdyti naudotojus, licencijas ir programinės įrangos aplinką. Taip pat suteikiamos automatizuotos atsarginių kopijų kūrimo galimybės, užtikrinamas aukštas paslaugų prieinamumas, patikimumas ir technologinis lankstumas. Tokios paslaugos yra rekomenduojamas mažoms organizacijoms, kurios neturi pakankamai žmogiškųjų išteklių nuosavos IT infrastruktūros priežiūrai ir valdymui, suteikiant joms galimybę naudotis moderniais sprendimais be didelių pradinių investicijų ir sudėtingos administravimo naštos.

Debesijos paslaugų sprendimų tipai

Rinkoje egzistuojančias pagrindines debesijos paslaugas galime suskirstyti į kelias pagrindines kategorijas: komunikacijos priemonės, duomenų saugojimo (talpyklų) sprendimai, infrastruktūros priegloba, duomenų analitikos įrankiai bei aplikacijų programavimo sąsajos (angl. *Application Programming Interface*, API). Kiekvienai kategorijai būtų galima rasti daug skirtingų paslaugų teikėjų ir sprendimų, tačiau toliau pateikiami dažniausiai naudojamų debesijos paslaugų teikėjų pavyzdžiai.

Darbo įrankiai.

Tai kasdien naudojami produktyvumo sprendimai, tokie kaip „*Microsoft Office 365*“, „*Google Docs*“ ar „*Open Office*“. Šios priemonės leidžia kurti, redaguoti ir dalintis dokumentais realiu laiku.

Komunikacijos priemonės.

Tokios aplikacijos, kaip *„Google Chat“, „Microsoft Outlook“, „Zoom“, „Microsoft Teams“*, skirtos naudotojų komunikacijai raštu, garsu ar vaizdu. Svarbu pažymėti, kad šios priemonės dažnai tampa kibernetinių atakų taikiniais, nes per jas gali būti platinami sukčiavimo (angl. phishing) laiškai, kenkėjiški priedai ar kenksmingos nuorodos.

Duomenų saugyklos.

Debesijos saugyklos, tokios kaip *„Microsoft OneDrive“, „SharePoint“* ar „*Google Drive*“, suteikia galimybę centralizuotai kaupti ir dalintis organizacijos dokumentais. Vis dėlto, netinkamai sukonfigūravus prieigos teises, šiose saugyklose saugomi dokumentai gali būti užšifruoti ar nutekinti.

Infrastruktūros priegloba.

Šios paslaugos leidžia talpinti sistemas, aplikacijas ar duomenų bazes debesijos paslaugų teikėjo infrastruktūroje (pvz., virtualiuose privačiuose serveriuose – VPS). Dažniausiai naudojami paslaugų teikėjai – „*Amazon Web Services* (AWS)“, „*Microsoft Azure*“ ir kt. Atsakomybė už saugumą šiuo atveju yra pasidalijama: paslaugų teikėjas užtikrina fizinės ir tinklo infrastruktūros saugumą, o organizacija atsako už prieigos kontrolę, tinkamą sistemų konfigūraciją ir pažeidžiamumų valdymą.

Duomenų analitikos įrankiai.

Sprendimai, tokie kaip „*Microsoft Power BI*“ ar panašūs, leidžia kaupti, apdoroti ir vizualizuoti duomenis, tačiau naudojant šiuos įrankius kyla rizika dėl jautrios ir neviešos informacijos atskleidimo ar netyčinio paviešinimo.

Trečiųjų šalių integracijos (API).

Debesijos paslaugų ekosistemos dažnai plečiamos naudojant išorinius įskiepius ar API jungtis, tačiau svarbu paminėti, jog trečiųjų šalių aplikacijų integravimas didina tiekimo grandinės pažeidžiamumų riziką. Plačiau apie trečiųjų šalių rizikų valdymą galite skaityti NKSC interneto svetainėje.

Pagrindinės debesijos paslaugų grėsmės ir rizikos

Debesijos paslaugos suteikia organizacijoms lankstumo, efektyvumo ir geresnio paslaugų prieinamumo, tačiau tuo pačiu tampa vienu iš pagrindinių kibernetinių atakų taikiniu. Netinkamai sukonfigūruotos arba neprižiūrimos debesijos paslaugos gali lemti šias pagrindines grėsmes ir rizikas:

Neautorizuota prieiga.

Nepakankama prieigos kontrolė ir nenaudojama daugiafaktorinė autentifikacija (MFA) yra viena iš dažniausių debesijos paslaugų kompromitavimo priežasčių. Privaloma užtikrinti MFA visiems paslaugų naudotojams. Netinkamai valdoma autentifikacija sudaro galimybes neteisėtai prieigai prie debesijos paslaugų aplinkos ir joje saugomos jautrios ir neviešos informacijos.

Duomenų nutekėjimas.

Debesijos saugyklos, tokios kaip *„Google Drive“* ar *„SharePoint“*, suteikia patogią dokumentų dalijimosi aplinką, tačiau netinkamai sukonfigūruotos prieigos teisės gali leisti neautorizuotiems vidiniams ir išoriniams naudotojams pasiekti jautrią ir neviešą informaciją.

Išpirkos atakos (angl. *Ransomware*).

Kenkėjiška programinė įranga gali užšifruoti naudotojo ar visos organizacijos duomenis debesijoje ir reikalauti išpirkos už jų atkūrimą. Debesijos paslaugos nėra atsparios šioms atakoms – užšifruoti galima tiek sinchronizuotus failus „*OneDrive*“, tiek failus, bendrinamus „*Google Drive*“ aplankuose. Net jei paslaugų teikėjas užtikrina atsargines kopijas, laiku neaptikus incidento gali būti prarasti svarbūs duomenys.

Socialinės inžinerijos atakos ir sukčiavimas (angl. *Social Engineering, Phishing*).

Apgaule, apsimetant kitu asmeniu ar įmone, siekiama išgauti neviešą informaciją arba prieigą prie informacinių resursų. Dažniausiai platinami el. laiškai ar žinutės, kuriuose prašoma atidaryti kenkėjiškas nuorodas arba atsisiųsti priedus. El. paštas, *„MS Teams“*, *„Zoom“*, *„Slack“* ar *„Google Chat“* yra pagrindiniai kanalai sukčiavimui ir kenkėjiškoms nuorodoms platinti.

Konfigūracijos klaidos.

Didelė dalis incidentų debesijos aplinkoje kyla dėl neteisingų nustatymų, neautorizuotų trečiųjų šalių integracijų ar klaidingai nustatytos paslaugų politikos (pvz., suteiktos perteklinės prieigos teisės).

Tiekimo grandinės pažeidžiamumai.

Debesijos paslaugų aplinkoje neretai suteikiama prieiga trečiųjų šalių integracijoms per API. Jei integruotos trečios šalys nėra tinkamai kontroliuojamos, jos gali tapti atakos taikiniu. ENISA pabrėžia, kad tiekimo grandinės išpuoliai debesijoje (pvz., kenkėjiški įskiepiai ar integracijos) tampa vis dažnesni ir gali paveikti daugelį organizacijų vienu metu. Daugiau apie trečiųjų šalių rizikų valdymą skaitykite NKSC rekomendacijose.

Atsižvelgiant į aukščiau išvardintas grėsmes ir rizikas, organizacijos, pasitelkusios debesijos siūlomus sprendimus, privalo užtikrinti tinkamą šių sprendimų konfigūravimą, priežiūrą bei valdymą.

Kontrolės priemonės

Siekiant užtikrinti tinkamą debesijos paslaugų saugumą, yra būtina taikyti griežtą prieigos kontrolę pagal organizacijoje nustatytas roles ir jų prieigos teises; taip pat, ne mažiau svarbu ir aktyviai nuolat prižiūrėti duomenų apsaugos, el. pašto saugumo, nuolatinės stebėsenos bei incidentų valdymo ir paslaugų tęstinumo sprendimus. Organizacijai, pasitelkiančiai debesijos paslaugų teikėjus, **rekomenduojame** papildomai taikyti žemiau išvardintas saugumo kontrolės priemones.

Prieigos valdymas ir autentifikacija.

Darbuotojams būtina taikyti žemiausių teisių principą – suteikiama tik minimali, laike ribota ir tik darbo funkcijoms vykdyti reikalinga prieiga. Rekomenduojama įgyvendinti „*Zero Trust*“ modelį, kuomet kiekviena prieiga prie TIS išteklių yra autentifikuojama, autorizuojama ir registruojama, o kartu su ja nustatykite ir sąlyginę prieigos politiką (angl. *Context-Based Access Control,* CBAC), kai vartotojo prieiga papildomai ribojama pagal papildomus atributus (įrenginį, vietą ir kt.).

Visoms paskyroms yra privaloma taikyti sudėtingus slaptažodžius ir daugiafaktorinę autentifikaciją (MFA). Rekomenduojama uždrausti anoniminius prisijungimus prie *„Teams“, „Zoom“* ar kitų nuotolinių susitikimų platformų. Esant techninėms galimybėms debesijos aplinkoje įjunkite ir sukonfigūruokite „*Attack Surface Reduction*“ (ASR) taisykles.

Duomenų dalijimasis ir duomenų nutekėjimo prevencija (angl. Data Leak Prevention, DLP).

Organizacijos nevieša informacija privalo būti pasiekiama tik iš vidinio tinklo arba naudojantis virtualiu privačiu tinklu (angl. VPN). Privaloma vykdyti dokumentų klasifikavimą ir žymėjimą (angl. labelling), kad jautrūs dokumentai nebūtų prieinami išorinėms organizacijoms ar kitoms trečiosioms šalims. Rekomenduojama riboti viešos prieigos nuorodų dalinimosi galimybes bei nustatyti aiškią duomenų dalinimosi politiką. Siūlome naudoti failų skanavimą (AV) tiek el. laiškams, tiek debesijoje saugomiems dokumentams.

Pašto sistemų saugos priemonės.

Debesijos el. pašto sistemose būtina aktyvuoti SPF, DKIM ir DMARC politiką, kad būtų užkirstas kelias el. laiško siuntėjo domeno imitavimui. Ypač svarbu diegti *anti-phishing, anti-malware, „Safe Links“* ir *„Safe Attachments“* funkcionalumus bei suteikti naudotojams galimybę pranešti apie įtartinus laiškus (*„Report Message“*). Rekomenduojama reguliariai vykdyti darbuotojų mokymus apie socialinės inžinerijos atakas bei simuliuoti realių atakų scenarijus. Plačiau apie el. pašto saugumo priemones skaitykite NKSC išleistose rekomendacijose.

Audito žurnalai ir stebėsena.

Saugumo įvykiams stebėti rekomenduojama debesijos paslaugų žurnalus (*logs*) integruoti su SIEM sprendimais (pvz., ELK *Stack, Wazuh, Azure Sentinel, Splunk* ar kitais). Naudokite debesijos paslaugų saugios prieigos brokerį (CASB), pvz., *„Defender for Cloud Apps“*, kuris leidžia stebėti, klasifikuoti naudojamas programas ir aptikti neleistinas veiklas. Užtikrinkite, kad būtų sukonfigūruota saugumo pranešimų (alerts) sistema – AV įspėjimai. Bet kokie įtartini pranešimai apie prisijungimus, masinius duomenų pasiekimus turi būti nedelsiant siunčiami į SOC (angl. *Security Operations Centre*) ar kitai organizacijoje atsakingai IT saugumo komandai.

Mobiliųjų įrenginių apsauga.

Valdykite mobiliuosius įrenginius per MDM (angl. *Mobile Device Management*) ar EMM (angl. *Enterprise Mobility Management*) (pvz., *„Microsoft Intune“*, *„Google Endpoint Management“*) sprendimus, taikykite PIN ar biometrijos autentifikaciją, šifravimą bei kitas informacijos saugos politikas. Užtikrinkite, kad tik atitinkantys saugumo reikalavimus įrenginiai galėtų naudotis debesijos paslaugomis.

Atsarginės kopijos.

Patariama kurti papildomas, versijų pagrindu paremtas, atsargines kritinių duomenų kopijas, kurios būtų saugomos atskirai nuo pagrindinės infrastruktūros („*offsite*“ arba „immutable backup“). Rekomenduojama remtis tos pačios debesijos ekosistemos sprendimais, pavyzdžiui, naudojant *Microsoft - „Azure Backup“, Google Cloud Provider - „Google Cloud Backup and DR“, AWS - „AWS Backup“ ar panašiais.*

Atsakomybių ribos.

Siūloma taikyti debesijos paslaugų teikėjo rekomenduojamus minimalius ir būtinus saugumo nustatymus ir aiškiai dokumentuoti debesijos paslaugų teikėjo bei perkančiosios organizacijos atsakomybės ribas (angl. *shared responsibility model*), jas nustatyti SLA (angl. *Service Level Agreement*) ir DPA (angl. *Data Processing Agreement*) sutartyse bei periodiškai, atsižvelgiant į valdomų duomenų kritiškumą, atsakomybės ribas peržiūrėti.

Incidentų valdymas ir paslaugų tęstinumas.

Incidentams aptikti ir reaguoti naudokite „*Defender Threat Explorer*“, „*Compliance Center Alerts*“ ar kitus debesijos paslaugų teikėjo siūlomus analizės įrankius. Visa incidentų valdymo ir paslaugų tęstinumo eiga turi būti testuojama ir periodiškai tobulinama.

Sistemų saugumo rodikliai.

Stebėkite pagrindinius sistemų saugumo rodiklius, naudodami debesų tiekėjų įrankius, pavyzdžiui, „*Microsoft Secure Score*“ (*Defender* portalas), „*AWS GuardDuty*“, „*Google Security Command Center*“ ar kitus.

Tinkamai įdiegus šias rekomenduojamas kontrolės priemones, organizacija reikšmingai padidintų debesijos paslaugų saugumą bei sumažintų potencialių incidentų poveikį verslo tęstinumui, net ir susidūrus su pažangiomis kibernetinėmis grėsmėmis.

Duomenų lokalizacija ir privatumas

Debesijos aplinkoje laikomų duomenų geografinė vieta (angl. *Data residency* arba *Data localization*) yra labai svarbi dėl teisinių, privatumo ir saugumo aspektų. Europos Sąjungoje taikomi teisės aktai, pavyzdžiui, BDAR (Bendrasis duomenų apsaugos reglamentas), nustato asmens duomenų perdavimą EEE (Europos ekonominės erdvės) ribose. Duomenų tvarkymas už EEE ribų gali lemti papildomus reguliacinius reikalavimus bei iš organizacijos reikalauti papildomų saugumo priemonių ir standartų taikymo duomenų saugumui užtikrinti.

Duomenų lokalizacijos svarba EEE:

Teisinis atitikimas. Valstybės institucijos ir organizacijos, tvarkančios jautrius asmens duomenis už EEE ribų, turėtų užtikrinti, kad duomenų perdavimas ir prieiga kitose jurisdikcijose atitiktų BDAR ir TIS2 keliamus reikalavimus.

Privatumas ir prieigos rizikos. Duomenys, kurie yra fiziškai saugomi ar prieinami duomenų centruose už EEE ribų, gali būti paveikti užsienio teisės aktų (pvz., prieigos reikalavimai trečiosioms šalims). Šios rizikos turi būti vertinamos, atliekant debesijos paslaugų teikėjo pirminę analizę.

Operacijų kontrolė ir veiksmų atsekamumas. Lokalizacija EEE ribose ir Europos Sąjungoje taikomi teisės aktai palengvina žurnalų (angl. *logs*) rinkimą, teisinę prieigą prie įrodymų bei greitesnį reagavimą incidento atveju.

Renkantis debesijos paslaugų teikėjus, patariama atsižvelgti į šias rekomendacijas:

Sutartyse reikalaukite aiškios duomenų lokalizacijos. DPA ar SLA turi nurodyti, kur (kokiose šalyse / regionuose) laikomi, apdorojami ir saugomi perkančiosios organizacijos duomenų rinkiniai. Rekomenduojame reikalauti, kad perkančiosios organizacijos duomenų rinkiniai būtų laikomi tik EEE. Taip pat turi būti aiškiai nurodytos ir suteiktos pakankamos audito teisės duomenų rinkinių savininkui.

Pasitelkite paslaugų teikėjus, turinčius „data residency“ funkcijas. Sprendimai, turintys duomenų laikymo regiono pasirinkimo (angl. *Advanced Data Residency / Sovereignty*) galimybes, suteikia perkančiosioms organizacijoms laisvę nurodyti, kuriame regione bus laikomi organizacijos duomenys.

Vertinkite duomenų perkėlimo riziką ir užsitikrinkite garantijas. Jei duomenys gali būti perkelti už EEE ribų, iš anksto nustatykite tam tinkamas perkėlimo priemones. Joms nustatyti galite vadovautis Europos duomenų apsaugos valdybos gairėmis.

Reikalaukite audito ir ataskaitų galimybių. Paslaugų teikėjas turi suteikti prieigą prie žurnalų ir audito rezultatų arba leidimą vykdyti nepriklausomą auditą (jei to prireiktų).

Aiškiai apibrėžtos duomenų lokalizacijos sąlygos padeda užtikrinti organizacijos teisinę atitiktį, sumažina privatumo bei prieigos rizikas ir stiprina organizacijos atsparumą kylantiems kibernetiniams ir duomenų apsaugos iššūkiams.

Nuolatinė priežiūra, konfigūracijos valdymas, saugumo higiena ir darbuotojų mokymai

Kaip ir bet kuris kitas IT sprendimas, taip ir efektyvus debesijos paslaugų saugumas reikalauja nuolatinės priežiūros, įskaitant periodinę patikrą ir konfigūracijos atnaujinimą. Pateiktos organizacinės ir techninės veiklos yra rekomenduojamos, siekiant užtikrinti patikimą debesijos aplinkos apsaugą, sumažinti pažeidžiamumų riziką ir užtikrinti organizacijos veiklos tęstinumą.

Konfigūracijų valdymo praktika. Debesijos paslaugų teikėjo aplinkoje naudokite centralizuotą konfigūracijų valdymą (angl. *Policy as Code*, PaC), versijavimą ir testavimo kanalus *(staged rollout)* prieš diegiant pakeitimus į gamybinę aplinką. Įjunkite automatinius saugumo atnaujinimus, o visas kitas naujas sistemines konfigūracijas ištestuokite prieš diegiant į gamybinę aplinką. Konfigūracijai valdyti ir centralizuotiems konfigūracijos saugumo rodikliams stebėti siūlome naudoti debesijos paslaugų teikėjo įrankius, pavyzdžiui, *Microsoft Defender portal / Microsoft Entra / Azure Security Center, Google Cloud Security Command Center, AWS Security Hub* ar kitus.

Prieigos peržiūra ir privilegijų valdymas. Vykdykite reguliarius (rekomenduojama kas 30 d.) prieigos ir privilegijų peržiūros ciklus. Kritinėms ir privilegijuotoms rolėms naudokite *„Privileged Identity Management“* (PIM) sprendimą, kuris leidžia laikinai suteikti privilegijuotas teises tik esant poreikiui ir užtikrinti jų automatinę galiojimo pabaigą.

Periodinė įvykių peržiūra. Užtikrinkite, kad svarbiausių debesijos paslaugų komponentų žurnalai (pvz., *Microsoft Exchange/SharePoint/OneDrive, Google Cloud Provider audit logging, AWS CloudTrail*) būtų renkami ir periodiškai peržiūrimi (pvz., SIEM ir SOAR priemonėmis). Taip pat reguliariai tikrinkite, ar saugumo pranešimai (alerts) veikia tinkamai ir apie įtartinus įvykius yra informuojama SOC ar kita atsakinga IT saugumo komanda.

Informacijos saugumo higiena ir darbuotojų mokymai. Vykdykite reguliarius darbuotojų mokymus, kibernetinių atakų simuliacijas, specializuotus administratorių mokymus. Puoselėkite informacijos saugumo kultūrą, įtraukite informacijos saugumo higienos principus į kasdienes operacijas: šalinkite nebenaudojamas paskyras, neaktyvius kriptografinius raktus, peržiūrėkite suteiktas prieigas išorės naudotojams.

Verslo tęstinumo atkūrimo vertinimas. Nustatykite atsarginių kopijų kūrimo ir valdymo politiką, atlikite periodinius atkūrimo testus (angl. *disaster recovery and restore tests*), nustatykite RTO (*Recovery Time Objective*) ir RPO (*Recovery Point Objective*) tikslus. Neapsiribokite tik debesijos paslaugų teikėjo siūlomu duomenų versijavimu – užtikrinkite nepriklausomą, logiškai atskirtą atsarginių kopijų kūrimą.

Nuosekli ir periodinė debesijos paslaugų priežiūra leidžia laiku nustatyti ir pašalinti konfigūracijos spragas, efektyviai valdyti prieigos teises bei užtikrinti saugomų duomenų konfidencialumą, integralumą bei prieinamumą. Tai sudaro prielaidas ne tik sumažinti kibernetinių incidentų tikimybę, bet ir užtikrinti organizacijos veiklos tęstinumą net ir susidūrus su kibernetinėmis grėsmėmis.

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

DEBESIJOS PASLAUGŲ SAUGUMO UŽTIKRINIMAS

Debesijos aplinka yra dažnas taikinys dėl joje saugomų jautrių organizacijos duomenų, todėl tinkamai sukonfigūruotos saugumo kontrolės priemonės yra itin svarbios organizacijos tinklų ir informacinių sistemų (TIS) atsparumui.

Esama situacija

Debesijos paslaugos plačiai naudojamos organizacijose - pagal ENISA 2024 m. grėsmių apžvalgą, respondentai vidutiniškai naudoja daugiau nei du debesijos paslaugų teikėjus, **o daugiau kaip 47 %** debesijoje laikomų duomenų laikomi jautriais ir neviešais.

Debesijos paslaugų veikimas ir modeliai

Debesijos paslaugos leidžia organizacijoms perkelti savo informacinius išteklius į nuotolinį duomenų centrą, kurį prižiūri paslaugų teikėjas, ir naudotis įvairiais įrankiais bei infrastruktūra nepriklausomai nuo vietos.

- **On-Premise.** Infrastruktūra laikoma organizacijos patalpose.
- **PaaS.** Platforma teikiama kaip paslauga.
- **IaaS.** Infrastruktūra teikiama kaip paslauga.
- **SaaS.** Programinė įranga teikiama kaip paslauga.

Debesijos paslaugų grėsmės ir rizikos

- Neautorizuota prieiga
- Duomenų nutekėjimas
- Išpirkos atakos
- Socialinės inžinerijos atakos ir sukčiavimas
- Konfigūracijos klaidos
- Tiekimo grandinės pažeidžiamumai

Kontrolės priemonės

- Prieigos valdymas ir autentifikacija
- Incidentų valdymas ir paslaugų tęstinumas
- Pašto sistemų saugos priemonės
- Audito žurnalai ir stebėsena
- Mobiliųjų įrenginių apsauga
- Atsarginės kopijos
- Atsakomybių ribos
- Sistemų saugumo rodikliai
- Duomenų dalijimasis ir duomenų nutekėjimo prevencija

Duomenų lokalizacija ir privatumas

Debesijos duomenų geografinė vieta lemia teisinį atitikimą, privatumo užtikrinimą ir operacijų kontrolę. Pagal BDAR ir TIS2 reikalavimus, duomenų laikymas EEE ribose padeda išvengti papildomų reguliacinių rizikų ir palengvina reagavimą į incidentus.

Renkantis paslaugų teikėją atsižvelkite į:

Audito galimybes.
Teikėjas turi suteikti prieigą prie žurnalų ir ataskaitų arba leisti atlikti nepriklausomą auditą.

Perkėlimo riziką.
Jei duomenys gali būti perkelti už EEE ribų - numatykite saugias perkėlimo priemones pagal EDAV gaires.

„Data residency“ funkcijas.
Rinkitės teikėjus, leidžiančius pasirinkti duomenų saugojimo regioną.

Aiški duomenų lokalizacija.
Nurodykite, kad duomenys būtų laikomi tik EEE teritorijoje;

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.