ASMENS DUOMENŲ SAUGUMO UŽTIKRINIMO ASPEKTAI

ELEKTRONINĖS PREKYBOS SVETAINĖSE

2026 m. liepos 3 d.

1. Įžanga

Bendrasis duomenų apsaugos reglamentas (toliau – BDAR) reikalauja, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų tinkamas technines ir organizacines saugumo priemones siekiant **užtikrinti pavojų** tvarkomiems asmens duomenims **atitinkančio lygio saugumą**. Jie turėtų atsižvelgti į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios **tikimybės ir rimtumo pavojus** fizinių asmenų teisėms ir laisvėms (BDAR 32 straipsnis).

Elektroninės prekybos saugumo aplinka sparčiai keičiasi ir organizacijos turi būti pasiruošusios prisitaikyti prie naujų iššūkių. Norint geriau įvertinti rizikos veiksnius ir geriausią duomenų saugumo užtikrinimo praktiką, pirmiausia **reikia suprasti pavojingiausias grėsmes**, kylančias elektroninės prekybos svetainėms ir jose tvarkomiems asmens duomenims.

2. Elektroninės prekybos grėsmių tendencijos

2.1 Dirbtiniu intelektu paremtos atakos ir sukčiavimas sparčiai plinta

Dirbtinis intelektas (toliau – DI) ir jo pritaikymo galimybės keičia ir transformuoja elektroninę prekybą, tačiau kartu tai skatina ir naujų sukčiavimo metodų atsiradimą. Sukčiai ir piktavaliai naudoja DI įrankius ir mašininį mokymąsi, kad generuotų netikras, tačiau įtikinamai atrodančias tapatybes, kurias patikimai atpažinti darosi sunku tradicinei „Pažink savo klientą“ patikrai (angl. *KYC, Know Your Customer*). Kuriami sukčiavimo el. laiškai, kurie imituoja prekės ženklo stilistiką ir vizualinį turinį ar diegia DI robotus, kurie elgiasi kaip „tikri“ klientai. Šias grėsmes sunkiau aptikti ir prie jų greičiau prisitaikyti nei kovojant su rankiniu būdu vykdomomis sukčiavimo atakomis.

Siekiant su tuo kovoti, duomenų valdytojams rekomenduotina įvertinti poreikį investuoti į sukčiavimo prevencijos įrankius (pasitelkiant ir DI), naudojančius realaus laiko elgsenos analizę, šablonų atpažinimą ar pan., kad grėsmės būtų aptiktos prieš joms padarant žalą.

2.2 Daugiakanalės (angl. *Omnichannel*) prekybos plėtra plečia „atakos paviršių“

Elektroninė prekyba nebevyksta vien per internetines svetaines. Klientai dabar apsiperka naudodamiesi mobiliosiomis programėlėmis, socialinėmis platformomis, prekyvietėmis ir net DI įrankių pagalba. Kiekvienas iš šių elektroninės prekybos kanalų turi unikalių pažeidžiamumų ir piktavaliai tai pastebi. Dažniausios daugiakanalės prekybos rizikos kyla iš neapsaugotų API sąsajų (angl. *Application Programming Interface*), jungiančių vidines sistemas, netinkamai įdiegtų ar pasenusių saugumo protokolų skirtinguose prekybos kanaluose, sukčiavimo socialiniuose tinkluose ir suklastotų elektroninių parduotuvių. Įmonėms reikia suderintų ir visapusiškų apsaugos priemonių, kurios saugo kliento duomenis visuose sąlyčio taškuose (pavyzdžiui, net jei elektroninė parduotuvė yra gerai apsaugota, piktavaliai gali pasinaudoti silpniau apsaugota mobiliąja programėle ar API sąsaja ir taip pasiekti asmens duomenis).

2.3 Trečiųjų šalių ir tiekimo grandinės pažeidžiamumų daugėja

Šiuolaikinės elektroninės prekybos sistemos dažnai yra sukurtos trečiųjų šalių tiekėjų ekosistemos pagrindu – nuo mokėjimų apdorojimo ir vykdymo partnerių iki papildinių (įskiepių) ir debesijos infrastruktūros. Tačiau kiekvienas toks ryšys sukuria naują galimo poveikio tašką ir duomenų perdavimo grandinę, per kur gali kilti grėsmė, tokia kaip „Magecart“ atakos, kurios į atsiskaitymo puslapius įterpia kenkėjišką programinį kodą per trečiųjų šalių scenarijus. Išnaudojami tiekimo grandinės pažeidžiamumai, kurie sukompromituoja patikimomis laikytas integracijas. Grėsmės kyla ne tik iš įmonės vidaus, bet ir atsitiktinio informacijos nutekėjimas per tiekėjus. Trečiųjų šalių rizika yra vienas iš pagrindinių kibernetinių atakų vektorių elektroninėje prekyboje. Rizikos mažinimo strategijos turėtų apimti tiekėjų rizikos valdymą, saugumo (įsiskverbimo) testavimą ir nuolatinį išorinių jungčių stebėjimą.

3. Geriausia saugumo praktika kuriant elektroninės prekybos svetaines

Elektroninės prekybos procesų apsaugai reikalingas daugiasluoksnis požiūris, apimantis tiek prieigos kontrolę, tiek kitas duomenų saugumo priemones. Tinkama saugumo konfigūracija apsaugo nuo duomenų nutekėjimo ir kitų asmens duomenų saugumo pažeidimų bei užtikrina atitiktį BDAR.

„OWASP“ projekto svetainėje yra pateikiamas išsamesnis žiniatinklio programų, įskaitant ir elektroninės prekybos svetaines, 10 svarbiausių saugumo rizikų techninis aprašymas.

3.1 Daugiasluoksnė apsaugos strategija

Daugiasluoksnė apsauga veikia tvirtovės principu – jei puolėjai pralaužia vieną gynybos liniją, jų laukia kita. Tai sudėtingas labirintas, kur kiekvienas sluoksnis turi specifinę funkciją.

Perimetro saugumas. Žiniatinklio aplikacijų ugniasienė (WAF) veikia kaip išmanus sargas, kuris stebi kiekvieną duomenų paketą, ieškodamas žinomų atakų šablonų. Elektroninės prekybos

kontekste ji ypač svarbi, nes gali atpažinti ir blokuoti „SQL injekcijos“ atakas į produktų paieškos formas ar kenkėjiško kodo įterpimo į interneto svetainę (angl. *XSS, Cross-Site Scripting*) atakas mokėjimų apdorojimo puslapiuose.

DDoS apsaugos mechanizmai. Jie apsaugo nuo perkrovos atakų, kai piktavaliai bando sutrikdyti elektroninės prekybos svetainės veiklą dirbtiniu duomenų srautu, ypač per intensyvius pardavimų periodus, tokius kaip Juodasis penktadienis. Internetinių robotų (angl. *Bot*) valdymo sprendimai skirti atskirti realius klientus nuo automatinių programų, kurios gali bandyti išnaudoti elektroninės prekybos svetainės pažeidžiamumus ar sukurti netikras paskyras.

Aplikacijos lygmens saugumas. OWASP ASVS[1] gairės nurodo, kaip kurti programas, kad jos būtų atsparios įsilaužimams. Įvesties patvirtinimo (angl. *Input validation*) mechanizmai tikrina kiekvieną naudotojo įvestį – ar tai būtų el. pašto adresas, kreditinės kortelės numeris, ar prekės ar paslaugos komentaras – kad neleistų kenkėjiškam kodui patekti į sistemą.

Duomenų lygmens apsauga. Duomenų šifravimas visuose etapuose reiškia, kad net jei kas nors gautų prieigą prie duomenų, matytųsi tik nesuprantamas simbolių rinkinys. Prieigos teisių valdymas užtikrina, kad naudotojams būtų suteikiamos tik jų pareigoms vykdyti būtinos teisės ir prieiga prie informacijos.

3.2 Kovos su DI grįstomis grėsmėmis priemonės

Didžiausias šiuolaikinės elektroninės prekybos iššūkis – kova su DI pagalba vykdomais nusikaltimais. Tai lyg šachmatų partija, kur abi pusės naudoja vis išmanesnes technologijas.

Elgsenos analizės sistemos (angl. *Behavioral Analysis System*). Jos išmoksta atpažinti, kaip paprastai elgiasi tikri klientai – kaip greitai jie perkelia pelės žymeklį, kokiais intervalais spaudžia klavišus, kiek laiko praleidžia skaitydami prekių aprašymus. Sistema sureaguoja, pakelia grėsmės lygį, kai pastebi, kad kažkas elgiasi netipiškai (pvz., per greitai pildo formas ar perkelia pelę idealiai tiesiai).

Mašininio mokymosi algoritmai. Jie analizuoja tūkstančius elgesio bruožų vienu metu ir gali pastebėti subtilias anomalijas, kurių žmogus nepastebėtų. Pavyzdžiui, jei kažkas naudoja tikrą kreditinės kortelės numerį, bet jo naršymo stilius primena robotą, sistema tai vertins kaip įtartiną elgesį.

Įrenginio atspaudų atpažinimo (angl. *Device Fingerprinting*) technologija. Ji sukuria unikalų kiekvieno įrenginio „pirštų atspaudą“ – nustatydama ekrano rezoliuciją, naršyklės versiją, įdiegtus šriftus ir šimtus kitų charakteristikų. Įrenginio atspaudų atpažinimas turi būti naudojamas tik saugumo užtikrinimo tikslu (pvz.: sukčiavimo prevencijai, prieigos anomalijoms aptikti ar kaip kelių pakopų autentifikacijos (MFA) dalis).

Adaptyvūs saugumo mechanizmai. Budrumas keičiasi pagal situaciją, pvz., jei kažkas bando prisijungti naktį iš kito miesto su įrenginiu, kuriuo iki tol nebuvo jungtasi, sistema gali pareikalauti papildomų tapatybės patvirtinimo žingsnių. O jei tas pats asmuo prisijungia darbo dieną iš įprasto kompiuterio, procesas bus kaip įprastas.

[1] Adresas internete: https://owasp.org/www-project-application-security-verification-standard/

3.3 API ir mikroservisų saugumas

Šiuolaikinės elektroninės prekybos sistemos yra tarsi skaitmeniniai miestai su sudėtingais komunikacijų tinklais. API sąsajos yra lyg keliai, kuriais keliauja informacija tarp skirtingų sistemos dalių.

API vartų (angl. *Gateway*) sprendimai. Čia vyksta autentifikacija (kas jūs esate) ir autorizacija (ką jums leidžiama daryti). Užklausų dažnio ribojimo (angl. *Rate limiting*) funkcija apsaugo sistemą nuo pernelyg dažno užklausų siuntimo.

Mikroservisų saugumas susiduria su iššūkiu, kad šiuolaikinės sistemos susideda ne iš vienos didelės sistemos, o iš daugybės mažų specializuotų paslaugų. Kiekviena tokia paslauga – ar tai būtų pirkinių krepšelio valdymas, mokėjimo apdorojimas ar atsargų sekimas – turi saugiai bendrauti su kitomis paslaugomis. Duomenų perdavimas tarp paslaugų turi būti šifruotas ir autentifikuotas, net jei jie vyksta to paties duomenų centro viduje.

Nulinio pasitikėjimo architektūros (angl. *Zero Trust Networking*) modelis remiasi principu „niekuo nepasitikėk, viską tikrink“. Net jei komunikacija vyksta tarp to paties serverio dalių, kiekvienas prisijungimas turi būti patvirtintas.

3.4 Asmens duomenų saugumo pažeidimų valdymas

Asmens duomenų saugumo pažeidimų valdymas nėra tik techninis klausimas – tai kompleksinis organizacijos proceso elementas, reikalaujantis tiek technologinių sprendimų, tiek aiškių procedūrų ir gerai pasiruošusios komandos. Asmens duomenų saugumo pažeidimų valdymas prasideda nuo efektyvios prevencijos ir pasiruošimo.

Elektroninės prekybos svetainėse būtina kelių sluoksnių apsauga, kur pirmas sluoksnis – tai tinklo lygmens apsauga (žiniatinklio aplikacijų ugniasienės, DDoS apsauga), antras sluoksnis – aplikacijos lygmens apsauga (įvesties patikrinimas, autentifikacija), trečias sluoksnis – duomenų lygmens apsauga (duomenų šifravimas, prieigos kontrolė) ir ketvirtas sluoksnis – stebėjimas ir reakcija (žurnalinių įrašų analizė, anomalijų aptikimas).

Vien techninių saugumo priemonių nepakanka, nes kiekvienas apsaugos sluoksnis turi būti ne tik techninis, svarbios ir organizacinės priemonės. Galite turėti tobulą technologinę infrastruktūrą, bet jei nors vienas darbuotojas visur naudoja tą patį nesaugų slaptažodį ar nuolat persisiunčia konfidencialius duomenis į asmeninius įrenginius, visa sistema tampa pažeidžiama.

Svarbus asmens duomenų saugumo pažeidimo valdymo aspektas yra krizių komunikacijos valdymas. Efektyvūs krizių valdymo planai nustato aiškią komandos struktūrą – kas vadovauja veiklos atkūrimui, kas bendrauja su žiniasklaida, kas yra techninis koordinatorius ir pan. Svarbu nepamiršti dokumentuoti priimtus sprendimus, atliktus tyrimus ir ataskaitas. Krizės metu reikia priimti daug ir greitų sprendimų, o vėliau gali būti sunku atsekti, kodėl buvo pasirinktas būtent toks, o ne kitoks problemos sprendimas. Tai svarbu ne tik organizacijos vidinei duomenų saugumo pažeidimo analizei, bet ir teikiant pranešimą VDAI apie asmens duomenų saugumo pažeidimą.

Pasitaiko, kad duomenų saugumo pažeidimai prasideda nuo žmogiškosios klaidos, tačiau svarbu suprasti, kad žmogiškoji klaida ne visada atsitiktinė – ji gali būti sisteminių problemų pasekmė. Po

realių incidentų organizacijos imasi ne tik techninių sprendimų, bet ir darbo kultūros pokyčių. Darbuotojai turi jaustis saugūs pranešdami apie įtartinas, keistas situacijas.

Nors darbuotojų apmokymas (pvz., atpažinti kenkėjiškas nuorodas) yra efektyvi prevencijos priemonė, tačiau to nepakanka, būtina taikyti kelių sluoksnių gynybą nuo kenkėjiškos veiklos, taikyti pažangias technines saugumo priemones, pritaikant jas ankstyvam ir efektyviam kenkėjiškos veiklos požymių aptikimui, analizei ir stabdymui. Po įvykusio ir jau suvaldyto asmens duomenų saugumo pažeidimo svarbu objektyviai įvertinti „pamokas“ ir tapti atsparesniems. Siekiant didinti atsparumą, reikia nustatyti sistemines problemas ir ieškoti joms sprendimų.

3.5 Technologijų integravimo strategija

Technologijų diegimas turi būti atliekamas sistemiškai, užtikrinant, kad nauji sprendimai nepablogintų esamų sistemų saugumo ir stabilumo. Kiekvienos technologijos įdiegimas turi būti pagrįstas aiškiais argumentais, rizikų bei naudos analize.

1. „API-pirmiausia“ architektūros plėtojimas:

Šiuolaikinės elektroninės prekybos sistemos turi būti kuriamos remiantis „API-pirmiausia“ (angl. *API-first*) principu, tai leidžia lanksčiai integruoti naujus saugumo ir privatumo funkcionalumus. Mikroservisų architektūra (kai didelė sistema suskaidoma į daug mažų, savarankiškai veikiančių paslaugų (mikroservisų) ypač tinkama tokiems sprendimams, nes leidžia nepriklausomai vystyti ir atnaujinti atskirus komponentus nepaveikiant visos sistemos.

> Veiksmingos saugumo priemonės turėtų ne tik apsaugoti asmens duomenis, bet ir išlikti kuo mažiau pastebimos bei netrukdyti naudotojams atlikti įprastų veiksmų.

Pavyzdžiui, kelių veiksnių autentifikavimą (MFA) rekomenduotina diegti palaipsniui, pradedant nuo rizikingesnių operacijų (tokių kaip administratorių prisijungimai, mokėjimų tvirtinimas ar prieiga prie klientų duomenų) ir palaipsniui išplečiant į visus naudotojo prieigos taškus (interneto svetainę, mobiliąją programėlę ar savitarnos portalą).

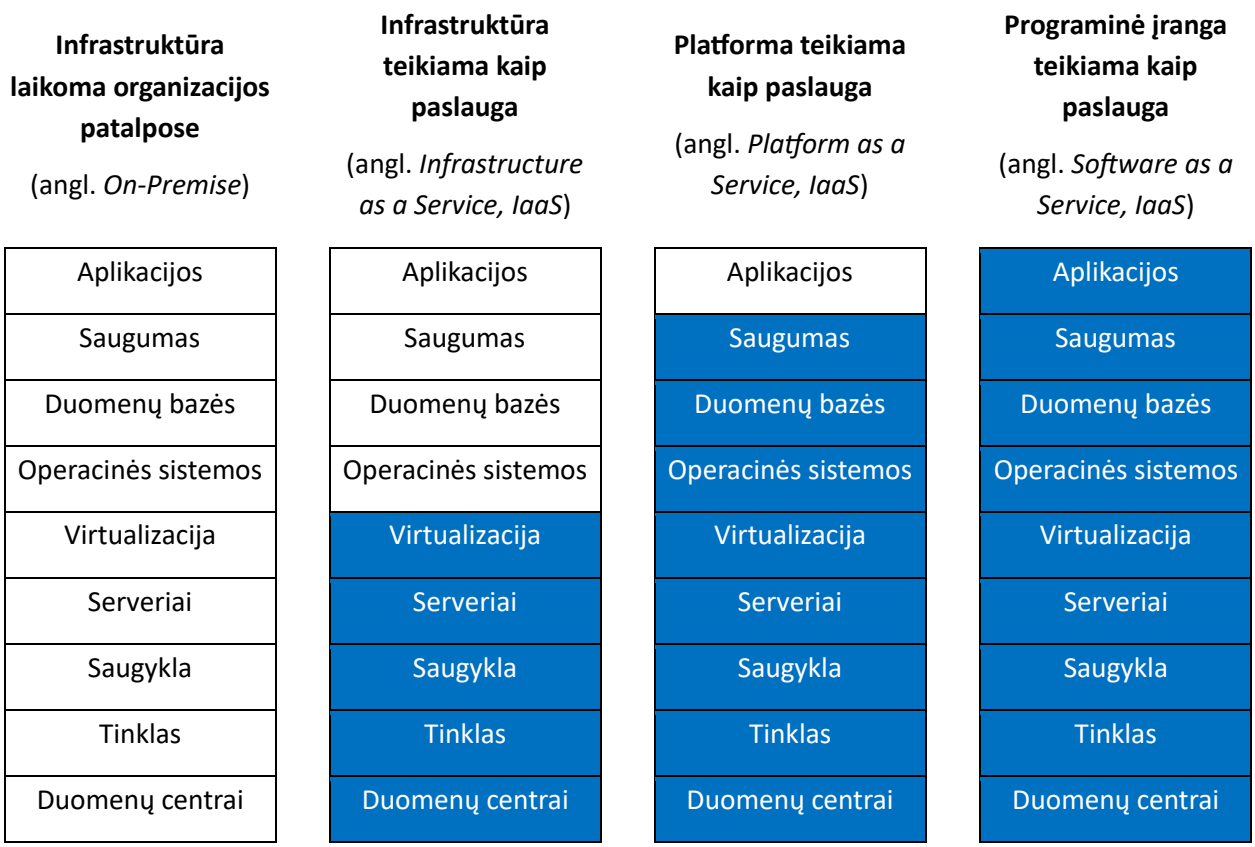
2. „Debesija-pirmiausia“ saugumo modelis:

Debesijos technologijų naudojimas gali žymiai palengvinti saugumo priemonių diegimą ir valdymą. Pavyzdžiui, Debesijos saugumo būklės valdymo (angl. *Cloud Security Posture Management*) sprendimai leidžia automatiškai stebėti ir valdyti saugumo konfigūracijas, Valdomos saugumo paslaugos (angl. *Managed Security Services*) gali suteikti prieigą prie pažangių saugumo technologijų be didelių pradinių investicijų.

3. Paskirstytos atsakomybės modelis:

Paskirstytos atsakomybės modelis (angl. *Shared Responsibility Model*) reikalauja supratimo, už kokius saugumo užtikrinimo aspektus atsako debesijos tiekėjas, o už kokius lieka atsakinga pati organizacija. Įprastai už paties „debesies“ saugumą ir patikimą paslaugų veikimą (ši atsakomybė apibrėžiama per paslaugų lygio susitarimus (SLA)) atsako debesijos tiekėjas, o organizacija atsako už tai, kas vyksta debesijoje patalpintose ir organizacijos valdomose sistemose, pavyzdžiui, už pačios organizacijos sukurtų duomenų saugumą.

Nacionalinis kibernetinio saugumo centras (NKSC) yra parengęs gaires[2] organizacijos debesijos paslaugų saugumui užtikrinti, jose yra pateikta schema (1 pav.), vaizduojanti, kas yra atsakingas ir kas ką valdo įvairiuose debesijos paslaugų modelių lygiuose.



1 pav. Atsakomybės pasiskirstymas įvairiuose debesijos paslaugų teikimo modeliuose (šaltinis: Nacionalinio kibernetinio saugumo centro gairės)

4. Duomenų privatumo ir saugumo užtikrinimas yra nuolatinis procesas

Šiuolaikinių duomenų privatumo ir saugumo priemonių diegimas elektroninėse parduotuvėse reikalauja sistemiško požiūrio ir laipsniško diegimo. Saugumo užtikrinimas yra nuolatinis procesas, todėl reguliarūs saugumo auditai, personalo mokymai ir technologijų atnaujinimai yra būtini elektroninės prekybos sistemoms. Investicijos į pažangias duomenų saugumo ir privatumo technologijas ne tik apsaugo nuo teisinių rizikų, bet ir kuria ilgalaikę vertę per klientų pasitikėjimo duomenų tvarkymu stiprinimą.

---

[2] Adresas internete: https://www.nksc.lt/doc/biuleteniai/Rekomendacija-8.pdf