Projektas

KRIPTOGRAFIJOS TAIKYMO INVENTORIZACIJOS GAIRĖS

(po konsultacijų bus pateikta kalbos tvarkytojai ir maketavimui)

TURINYS

1. ĮVADAS

Kriptografijos taikymo inventorizacija – tai išsamus žemėlapis visų organizacijoje naudojamų kriptografinių sprendimų. Jis yra būtinas norint suprasti, kokie komponentai gali būti pažeidžiami kvantinių grėsmių atžvilgiu, ir užtikrinti galimybę laiku juos atnaujinti ar pakeisti atspariais sprendimais.

Nors teoriškai inventorizacija gali atrodyti paprastas procesas, praktikoje tai yra sudėtingas ir daug laiko reikalaujantis darbas. Daugeliui organizacijų iššūkiu tampa net visų savo informacinių technologijų (pvz., kompiuterių, tinklų, duomenų bazių) ir operacinių technologijų (pvz., gamybos įrenginių, pramonės kontrolės sistemų) išteklių suregistravimas. Dar sudėtingiau nustatyti visus kriptografinius komponentus, kurie gali būti išskaidyti ir paslėpti skirtinguose fizinės įrangos, programinės įrangos ir įterptinės programinės įrangos sluoksniuose.

Nepaisant šių sudėtingumų, inventorizacija yra esminis žingsnis valdant kvantines rizikas ir užtikrinant kriptografinį lankstumą (crypto-agility). Be aiškaus visų algoritmų, protokolų, raktų, sertifikatų, bibliotekų ir jų versijų žemėlapio organizacija negali nustatyti, kur naudojami pažeidžiami algoritmai (pvz., RSA ar ECC), įvertinti priklausomybės nuo kriptografijos ar planuoti nuoseklaus perėjimo prie kvantiniams kompiuteriams atsparių sprendimų.

Svarbu suprasti, kad kvantinės grėsmės pirmiausia paveikia asimetrinę kriptografiją (pvz., RSA, ECC), kuri tampa silpna dėl kvantinių algoritmų. Simetrinė kriptografija (pvz., AES) laikoma atsparesne, tačiau ji taip pat gali būti pažeidžiama, jei naudojami per trumpi raktai ar pasenę algoritmai.

Inventorizacija suteikia organizacijai aiškų ir išsamų visų jos produktuose, sistemose ir paslaugose naudojamų kriptografinių priemonių vaizdą. Tai ne vien techninis „patikrinimo sąrašas“, o strateginis procesas, reikalaujantis automatizuotų įrankių, rankinių patikrų ir glaudaus koordinavimo visoje organizacijoje.

Gairių priede organizacija ras ne tik išsamų inventorizacijos duomenų modelį, bet ir rekomenduojamą inventorizacijos formą, kuri padeda sistemingai surinkti ir struktūrizuoti informaciją apie visus naudojamus kriptografinius komponentus. Tai suteikia galimybę įvertinti jų riziką ir priklausomybę nuo tiekėjų, suplanuoti nuoseklų perėjimą prie postkvantinių sprendimų, užtikrinti kriptografinį lankstumą ir ilgalaikį informacijos saugumą kvantinėje eroje bei laikytis teisės aktų ir vidaus politikos reikalavimų.

2. TIKSLAS IR TAIKYMO SRITIS

Šių Gairių tikslas – apibrėžti pagrindinius reikalavimus ir pateikti gerąją praktiką organizacijoms, vykdančioms kriptografijos taikymo inventorizaciją. Tikimasi, kad Gairės padės organizacijoms tinkamai identifikuoti algoritmus, protokolus, raktus, sertifikatus, bibliotekas ir jų versijas visose IT, OT ir debesijos aplinkose, įvertinti priklausomybę nuo kriptografijos ir pažeidžiamumą kvantinėms rizikoms, o taip pat parengti nuoseklų migracijos prie postkvantinės kriptografijos planą.

Inventorizacija turi apimti visas organizacijos sistemas ir aplinkas, įskaitant vietinę (on-premises) infrastruktūrą, debesijos paslaugas (IaaS/PaaS/SaaS), tinklo įrangą, įterptinę programinę įrangą, IoT ir ICS sprendimus, verslo aplikacijas bei trečiųjų šalių teikiamas paslaugas. Inventorizacijos rezultatai

sudarys prielaidas užtikrinti kriptografinį lankstumą: organizacija aiškiai matys, kur ir kokia kriptografija naudojama, kokios priklausomybės egzistuoja, kurie komponentai yra lengvai keičiami, o kurie laikomi rizikingais ar išskaidytais infrastruktūroje. Tai leis planuoti ir įgyvendinti greitus, koordinuotus kriptografijos pakeitimus, valdyti algoritmų ir bibliotekų gyvavimo ciklą, laiku pereiti prie stipresnių sprendimų ir užtikrinti atitiktį saugumo standartams.

3. APIBRĖŽIMAI IR SUTRUMPINIMAI

CBOM (angl. Cryptography Bill of Materials) – registras, kuriame fiksuojami naudojami kriptografiniai algoritmai, protokolai, raktai, sertifikatai, bibliotekos ir jų versijos.

IaaS (angl. Infrastructure as a Service) – debesijos infrastruktūros paslauga.

ICS (angl. Industrial Control Systems) – pramoninės valdymo sistemos, pvz., SCADA.

IoT (angl. Internet of Things) – daiktų interneto įrenginiai.

KMS (angl. Key Management System) – raktų valdymo sistema.

Kriptografinis lankstumas (angl. crypto-agility) – gebėjimas greitai ir efektyviai pakeisti naudojamus kriptografijos algoritmus, protokolus ar parametrus, išlaikant paslaugų tęstinumą.

PaaS (angl. Platform as a Service) – debesijos platformos paslauga.

PKI (angl. Public Key Infrastructure) – viešojo rakto infrastruktūra.

PQC (angl. post-quantum cryptography) – postkvantinė kriptografija.

SaaS (angl. Software as a Service) – debesijos programinės įrangos paslauga.

SBOM (angl. Software Bill of Materials) – programinės įrangos sudedamųjų dalių sąrašas, fiksuojantis, iš kokių bibliotekų ir komponentų sudaryta programinė įranga.

4. PASIRENGIMAS INVENTORIZACIJAI

4.1. VALDYMAS IR ATSAKOMYBĖS

Pasirengimas inventorizacijai yra vienas kritinių žingsnių, užtikrinančių sklandų perėjimą prie postkvantinės kriptografijos. Šiame etape svarbu aiškiai apibrėžti atsakomybes, paskirti roles ir užtikrinti koordinuotą komandų veiklą. Tvirta valdymo struktūra leidžia vykdyti inventorizaciją nuosekliai, patikimai ir efektyviai.

Lygmuo	Rolė	Veiklos ir atsakomybės
Strateginis	Vadovybė/ kibernetinio saugumo vadovas/Informacijos saugos vadovas (CISO)	Patvirtina inventorizacijos planą, nustato tikslus, prioritetus ir rizikos toleranciją, skiria biudžetą
Operacinis	Inventorizacijos vadovas	Sudaro detalų inventorizacijos planą: apibrėžia tikslus, apimtį, metodiką, terminus, atsakomybės paskirstymą, rizikų valdymą, duomenų kokybės užtikrinimą, koordinuoja veiklas, prižiūri biudžetą
Techninis	IT/OT saugumas, sistemų administratoriai, DevOps, programų komandos	Vykdo faktinę inventorizaciją: renka duomenis apie algoritmus, protokolus, raktus ir sertifikatus ir pan., pildo CBOM, tikrina duomenų kokybę, pildo rezultatų lentelę, naudoja automatizuotus įrankius
Atitiktis	Atitiktis (Governance, Risk, and Compliance) / Teisė	Peržiūri inventorizacijos duomenis, užtikrina teisėtą duomenų tvarkymą, vertina atitiktį reguliavimui

4.2. INVENTORIZACIJOS PLANAVIMAS IR ETAPAI

Prieš pradedant inventorizaciją, organizacija turi preliminariai suplanuoti laiką ir etapus, net jei tikslus kriptografinių sprendimų kompleksiškumas dar nežinomas. Laiko planavimas remiasi organizacijos dydžiu, ankstesnėmis žiniomis apie sistemas, kritinių sistemų identifikavimu ir numatomu darbo apimčių įvertinimu. Planavime rekomenduojama įtraukti 10–15 % laiko rezervą, kad būtų galima koreguoti planą pagal faktinius inventorizacijos rezultatus.

Preliminarus laikotarpis pagal organizacijos dydį:

- Maža organizacija: iki 8 savaičių
- Vidutinė organizacija: iki 12 savaičių
- Didelė organizacija: iki 20 savaičių

Etapus rekomenduojama planuoti taip, kad jie dalinai persidengtų. Pvz., duomenų kokybės peržiūrą galima pradėti, kai turima pirmoji 20–30 % įrašų dalis. Skubiose situacijose inventorizuojamos tik svarbiausios sistemos („TOP kritinės“) per 4–6 savaites. Lygiagrečiai galima taikyti „*Vendor first*“ metodiką – tiekėjams siunčiami klausimynai dėl *crypto agility* ir jų perėjimo prie PQC planų, kas leidžia sutrumpinti vertinimo etapą iki 0,5–1 savaitės.

Eil. Nr.	Etapas	Veiklos	Pastabos/ rezultatų kriterijai
1.	Aptikimas (*angl.* discovery)	Automatizuoti skenavimai, konfigūracijų analizė, TLS/SSH/IPsec auditas, kodų paieška (repo), naudojami automatizuoti įrankiai bei rankinis patikrinimas	Padengta ≥85–90 % sistemų, iš jų ≥95 % – atviros internetui. Identifikuotos PKI/KMS sistemos.

2.	Inventorizavimas (*angl.* Inventory)	Duomenų suvedimas arba automatinis surinkimas į vieną registrą	Visiems įrašams užpildomi privalomi laukai: sistema, protokolas, algoritmai, galiojimo data, savininkas, priklausomybė nuo tiekėjo ir kt.
3.	Duomenų kokybės peržiūra (*angl.* Data Quality Review)	Privalomų laukų tikrinimas, formatų validacija, dublikatų šalinimas, duomenų patikrinimas prieš vertinimą	100 % įrašų turi galiojimo datą (YYYY MM DD arba „N/A“), savininką ir nurodytą priklausomybę nuo tiekėjo. Pašalinti dublikatai, suvienodinamos reikšmės.
4.	Vertinimas (*angl.* Assessment)	Algoritmų būklė, crypto-agility, tiekėjų priklausomybė, rizikos balai, kritinių sistemų žymėjimas, analizė prioritetams nustatyti	Kiekvienam įrašui priskiriamas kvantinio atsparumo balas (0 = neatsparus, 1 = dalinai atsparus, 2 = pilnai atsparus) ir rekomendacija (*„būtina / neprivaloma (keisti ilgį) / nebūtina“).*
5.	Ataskaitos ir sprendimai (*angl.* Reporting & Decisions)	Migracijos prioritetų, terminų, sąnaudų, KPI nustatymas ir veiksmų plano pateikimas vadovybei	Oficialiai patvirtintas migracijos planas, kuriame nustatyta: pirmoji bandomoji versija (MVP), migracijos etapai („bangos“) ir sistemos priklausomybės, kad būtų galima saugiai ir valdomai pereiti prie naujų kriptografinių sprendimų. Nustatomi rodikliai, biudžetas ir atsakomybės (RACI).
6.	Palaikymas (*angl.* Maintenance)	Periodiškas atnaujinimas (pvz., kas ketvirtį) ir integracija su CMDB/SBOM, delta“ atnaujinimai – tik nauji arba pasikeitę įrašai (sertifikatai, bibliotekų versijos), atliekami kas mėnesį (1–2 d.)	Nuolatinis inventorizacijos palaikymas

4.3. INVENTORIZACIJOS ATLIKIMO METODO PARINKIMAS

Prieš pradedant faktinę inventorizaciją, būtina apsvarstyti ir pasirinkti tinkamiausius duomenų rinkimo metodus. Tinkamai parinktas metodas užtikrina, kad surinkta informacija apie kriptografinius algoritmus, raktus, sertifikatus ir konfigūracijas būtų tiksliai dokumentuota, išsami ir patikima. Metodo pasirinkimas priklauso nuo organizacijos dydžio, infrastruktūros sudėtingumo, turimų išteklių ir norimo tikslumo lygio.

Netinkamai parinktas metodas gali sukelti duomenų spragas, neaptiktas pažeidžiamumo zonas arba netikslų įvertinimą dėl crypto-agility ir PQC pasirengimo. Todėl rekomenduojama derinti skirtingus

metodus – rankinius tikrinimus su automatizuotomis priemonėmis – siekiant optimalios aprėpties ir tikslumo balanso.
Metodų pasirinkimas gali būti etapinis ir palaipsnis: dažnai pradedama nuo automatizuotų skenavimų, o rankinis tikrinimas taikomas kritinėms ar sunkiau aptinkamoms sistemoms.
Toliau pateikiama metodų lentelė su pagrindinėmis charakteristikomis, priemonėmis ir svarbiausiomis pastabomis. Kiekviena įrankių kategorija naudoja skirtingas technikas ir turi savų „aklųjų zonų“. Nė vienas įrankis ar metodas negali aptikti visko, todėl kelių metodų kombinacija užtikrina tikrai išsamią inventorizaciją.

Metodas	Aprašymas	Priemonės	Pastabos
Rankinis	Kriptografinių priemonių, programų, įrenginių ar bibliotekų patikrinimas žmogaus jėgomis, dokumentuojant kiekvieną elementą	Tikrinimas pagal sąrašus (checklists), fizinis serverių patikrinimas, konfigūracijų analizė, dokumentų peržiūra	Tinkamas mažoms organizacijoms arba specifinėms sistemoms, kur automatiniai įrankiai nepritaikomi. Užtikrina didelį tikslumą, tačiau yra lėtas ir imlus laikui
Automatizuotomis priemonėmis	Inventorizacija atliekama naudojant specializuotą programinę įrangą arba skriptus, kurie surenka informaciją apie kriptografinius algoritmus, raktus, sertifikatus ir konfigūracijas	Pažeidžiamumų skaneriai, SIEM, CMDB, KMS/PKI ir skriptai (PowerShell, Python), taip pat naudotojų paskyrų ir prieigos teisių prie kriptografinių išteklių patikrinimas naudojant AD, LDAP arba automatizuotus skriptus	Leidžia padengti didesnę infrastruktūrą greičiau, mažina žmogiškųjų klaidų riziką, galima reguliariai atnaujinti inventorizacijos duomenis. Reikalinga tam tikra automatizacijos patirtis ir įrankių konfigūracija

4.4. DOKUMENTAVIMO REIKALAVIMAI

Kriptografinių priemonių inventorizacijos rezultatus galima pateikti Excel, Konfigūracijos valdymo duomenų bazės (CMDB) arba kitomis tinkamomis formomis. Svarbu, kad būtų įtraukti visi sistemos komponentai. Inventorizacijos rengimo metu galima vadovautis Gairių priede pateikta lentele, kuri pateikia rekomenduojamą inventorizacijos formą.
Kriptografijos inventorizaciją galima rengti ir pagal SBOM arba CBOM. CBOM ypač tinkamas, kai inventorizacija vykdoma automatizuotomis priemonėmis (pvz., skeneriais ar agentais), kurie automatiškai aptinka naudojamus kriptografinius algoritmus iš programinės įrangos kodo, konfigūracijų ar tinklo srautų. Tokiu atveju CBOM gali būti dinamiškai pildomas ir nuolat atnaujinamas.

CBOM tampa vertingu įrankiu ne tik siekiant tinkamai suplanuoti migraciją prie postkvantinės kriptografijos, bet ir atliekant rizikų analizę bei užtikrinant atitikimą teisės aktams ir standartams (compliance).

5. INVENTORIZACIJOS ATLIKIMAS

5.1. INVENTORIZACIJOS SRITYS IR TIPINĖS SISTEMOS

Atliekant kriptografinių priemonių inventorizaciją, svarbu aiškiai apsibrėžti inventorizacijos sritis **ir** apimtį. Pradedant inventorizaciją nuo sistemų ir infrastruktūros, lengviau nustatyti, kur tiksliai naudojama kriptografija, ir vėliau surinkti informaciją apie konkrečius algoritmus, raktus, sertifikatus bei kitus objektus.
Lentelėje pateikiamos pagrindinės sritys ir tipinės sistemos, kuriose organizacijose naudojama kriptografija. Ji gali būti naudojama kaip kontrolinis sąrašas: organizacija turėtų pereiti per kiekvieną sritį, identifikuoti turimas sistemas, užfiksuoti naudojamus algoritmus ir įvertinti pasirengimą pereiti prie postkvantinės kriptografijos.

Sistema	Aprašymas (kas tikrinama)	Pavyzdžiai
Fiziniai įrenginiai	Kokie kriptografiniai algoritmai ir funkcijos naudojami aparatinėje įrangoje	HSM (Hardware Security Module), TPM (Trusted Platform Module), serveriai, tinklo įrenginiai, kriptografinius raktus generuojantys įrenginiai
Programinė įranga (on-premises)	Serverių, naudotojų ir infrastruktūrinės programos, įskaitant integruotas kriptografines bibliotekas, naudojamas šifravimui, autentifikacijai ir duomenų vientisumui užtikrinti	El. pašto serveriai, VPN programinė įranga, duomenų bazės, failų šifravimo programos.
Taikomosios programos (applications)	Naudojamos verslo ir naudotojų aplikacijos, kuriose integruota kriptografija, šifravimas, autentifikacija ar duomenų vientisumo kontrolė.	Verslo valdymo programos, internetinės platformos, mobiliosios aplikacijos, SaaS aplikacijos
Bibliotekos	Palaikomi algoritmai, licencija, versija	OpenSSL, Bouncy Castle, Microsoft CryptoAPI, libsodium.
Įterptasis kodas (embedded code / firmware)	Įrenginiai ar programos, kur kriptografija integruota į firmware arba mikrokontrolerius (MCU).	Daiktų interneto (IoT) įrenginiai, tinklo įrenginiai, medicininė įranga, automobilių elektroninė valdymo sistema
Tinklas ir duomenų perdavimas	Kokie kriptografiniai algoritmai, saugumo protokolai naudojami ryšio perdavimo metu vietinėje infrastruktūroje arba debesijoje.	TLS/SSL, IPsec, VPN tuneliai, šifruoti Wi-Fi tinklai, SNMPv3, NETCONF/SSH
Debesijos paslaugos	Kriptografinės funkcijos debesijos infrastruktūros, platformos ir paslaugų	AWS KMS, Azure Key Vault, GCP Cloud KMS, SaaS el.

	sluoksniuose (IaaS, PaaS, SaaS): duomenų šifravimas, raktų valdymas, autentifikacija, prieigos kontrolė	paštas, cloud database encryption
Duomenų saugyklos ir duomenų bazės	Duomenų šifravimas diske, duomenų bazėse, failų sistemose, raktų valdymas ir prieigos kontrolė	Šifruotos SQL / NoSQL duomenų bazės, failų sistemos (BitLocker, LUKS), cloud storage (S3 šifravimas, Azure Storage Encryption)
Atsarginės kopijos ir archyvai	Kaip šifruojami ir saugomi backup'ai, archyvuoti duomenys, naudojamos raktų valdymo priemonės	Backup sprendimai (Veeam, Commvault), archyvavimo sistemos, ilgalaikių saugyklų šifravimas
Viešojo rakto infrastruktūra (PKI)	Kaip organizacijoje valdomi sertifikatai: raktų išdavimas, atnaujinimas, pasirašymas, OCSP/CRL paslaugos. Įvertinama, kokie algoritmai naudojami, raktų ilgiai, sertifikatų galiojimo trukmė, ar sistema palaiko postkvantinį perėjimą	Vidinė PKI (pvz., ADCS), išoriniai CA (GlobalSign, DigiCert), kvalifikuoti sertifikatai (QES), OCSP serveriai
Autentifikacija ir prieigos kontrolė	Naudotojų, sistemų ir paslaugų autentifikacija, naudojami protokolai bei stiprumas	Active Directory, LDAP, 2FA/MFA, FIDO2/U2F raktai, SSO sprendimai
Programinės įrangos pasirašymas	Kaip užtikrinamas programų autentiškumas ir vientisumas	OS ir aplikacijų atnaujinimų parašai, mobiliosios aplikacijos, skriptų pasirašymas
Dokumentų ir duomenų pasirašymas	Kaip naudojami elektroniniai parašai ir užtikrinamas duomenų vientisumas	PDF pasirašymas, teisinių dokumentų, sutarčių, eIDAS parašai.
Pramonės valdymo ir IoT sistemos	Kriptografija, naudojama pramonės automatizavimo, IoT ir automobilių valdymo sistemose	SCADA kontroleriai, IoT platformos, automobilių ECU
Fizinės prieigos kontrolės ir identifikavimo sistemos	Kaip naudojama kriptografija prieigos kontrolės infrastruktūroje	Kortelės, RFID/NFC sprendimai, biometriniai vartai, durų valdikliai
Virtualizacijos platformos ir specializuota infrastruktūra	Kokie šifravimo mechanizmai taikomi virtualizacijos ir specializuotuose sprendimuose.	VM šifravimas, vSphere Native Key Provider, Hyper-V, Xen, KVM
Raktų valdymo sistemos	Centralizuotas raktų ir slaptų duomenų saugojimas, valdymas ir gyvavimo ciklo kontrolė, naudotojų ir rolės prieigos teisės.	HashiCorp Vault, CyberArk, Thales CipherTrust

5.2. INVENTORIZACIJOS OBJEKTAI

Šioje lentelėje pateikiami pagrindiniai kriptografiniai objektai, kuriuos organizacijoje rekomenduojama inventorizuoti. Tikslinga registruoti ne tik objektų pavadinimus, bet ir jų versijas, konfigūraciją, naudojimo paskirtį, galiojimo datas bei kitus svarbius parametrus.

Kiekvienas objektas turi būti inventorizuojamas kiekvienoje sistemoje, kur jis naudojamas. Tai užtikrina, kad inventorizacija apimtų visus kriptografinius išteklius ir padėtų tiksliai įvertinti riziką bei pasirengimą pereiti prie postkvantinės kriptografijos.

Kategorija	Aprašymas	Pavyzdžiai	Kokius duomenis rinkti
Šifravimo algoritmai	Algoritmai, naudojami duomenims šifruoti ar iššifruoti	AES, RSA, ECC, ChaCha20	Pavadinimas, versija, naudojimo paskirtis (duomenų šifravimas, ryšio apsauga, saugomų duomenų apsauga), konfigūracija
Kriptografiniai protokolai	Protokolai, užtikrinantys saugų ryšį ar duomenų perdavimą	TLS 1.2/1.3, IPsec, S/MIME, SSH	Pavadinimas, versija, konfigūracija, naudojimo paskirtis
Elektroninių parašų algoritmai	Algoritmai, skirti skaitmeniniam pasirašymui ir tapatybės patvirtinimui	RSA-PSS, ECDSA, EdDSA	Pavadinimas, raktų ilgis, naudojimo paskirtis
Skaitmeniniai sertifikatai	Sertifikatai, naudojami tapatybės patvirtinimui ir saugiam ryšiui	X.509 sertifikatai, naudojami, viešojo rakto infrastruktūroje (PKI)	Tipas, galiojimo data, išdavusi institucija, naudojimo paskirtis (pasirašymas, autentifikacija)
Kriptografiniai raktai	Raktai, naudojami šifravimui, pasirašymui ar autentifikacijai	Simetriniai raktai, asimetriniai raktai, kriptografiniai raktai, maišos pagrindu veikiantys raktai	Tipas, ilgis, galiojimo data, naudojimo paskirtis, kur naudojamas (sistemoje/funkcijoje), prieigos kontrolė
Raktų valdymo sistemos	Įrenginiai ar programinės priemonės, skirtos raktams generuoti, saugoti ir tvarkyti	HSM, KMS, TPM	Pavadinimas, naudojami algoritmai, valdymo politika, prieigos kontrolė
Kriptografinės bibliotekos	Bibliotekos, įgyvendinančios kriptografiją programose	OpenSSL, Bouncy Castle, libsodium	Pavadinimas, versija, palaikomi algoritmai, licencija
Šifruoto saugojimo sprendimai	Duomenų saugojimo įrankiai su integruota šifravimo funkcija	BitLocker, VeraCrypt, AWS KMS + S3 šifravimas	Pavadinimas, naudojami algoritmai, versija, naudojimo paskirtis
Tapatybės ir autentifikacijos priemonės	Priemonės, užtikrinančios vartotojų tapatybę ir prieigos kontrolę	LDAP, Active Directory, SSO sprendimai, MFA	Pavadinimas, autentifikacijos metodai, palaikomi protokolai, naudojimo paskirtis

Kriptografinių funkcijų įrankiai	Programos ar įrankiai, naudojami kriptografiniams veiksmams atlikti	Vienkrypčių algoritmų (Hash) įrankiai, PGP, GnuPG, OpenSSL komandinės eilutės įrankiai	Pavadinimas, versija, palaikomos funkcijos, naudojimo paskirtis
Sertifikavimo institucijos (CA)	Institucijos, išduodančios ir valdančios sertifikatus	GlobalSign, DigiCert, Registrų centras	Pavadinimas, tipas (root, intermediate), sertifikatų galiojimo laikotarpis, naudojimo paskirtis (sertifikatų išdavimas, valdymas, patikimumo užtikrinimas)
Auditavimo ir žurnalo šifravimas	Priemonės, užtikrinančios žurnalo įrašų saugumą	Syslog su TLS, ELK + šifravimas	Pavadinimas, naudojami algoritmai, konfigūracija, galiojimo laikotarpis, susiję raktai/sertifikatai

Siekiant supaprastinti inventorizacijos procesą ir užtikrinti, kad kiekvienas kriptografinis objektas būtų patikrintas visose sistemose, rekomenduojama parengti matricą, kurioje objektai būtų susieti su atitinkamomis sistemomis ir jų naudojimo kontekstu, pavyzdžiui:

		SISTEMOS/SRITYS			
KRIPTOGRAFINIAI OBJEKTAI		Serveriai	VPN	Mobilios aplikacijos	IoT įrenginiai
	AES	✓	✓	✗	✗
	RSA	✓	✓	✗	✗
	ECDSA	✗	✓	✓	✗
	TLS 1.3	✓	✓	✓	✓

6. BAIGIAMOSIOS NUOSTATOS

Inventorizacijos rezultatai sudaro pagrindą tolimesniems organizacijos veiksmams ir sprendimams dėl kriptografinių sprendimų valdymo. Surinkta informacija leidžia identifikuoti infrastruktūros silpnąsias vietas, nustatyti prioritetines sritis ir kritines sistemas, kuriose naudojama kriptografija, bei įvertinti naudojamų algoritmų, protokolų, raktų, sertifikatų, bibliotekų ir kitų kriptografinių objektų saugumą ir galiojančius konfigūracijos parametrus. Inventorizacija suteikia galimybę planuoti migraciją prie postkvantinės kriptografijos priemonių, užtikrinti atitiktį teisės aktams, standartams ir organizacijos vidaus politikoms, taip pat dokumentuoti visus pokyčius ir sprendimus dėl kriptografinių sprendimų valdymo.

Siekiant užtikrinti, kad inventorizacijos duomenys būtų išsamūs ir aktualūs, kiekvieną kriptografinį objektą rekomenduojama tikrinti visose susijusiose sistemose, įskaitant fizinius įrenginius, programinę įrangą, taikomąsias programas, bibliotekas, įterptąjį kodą, tinklą, duomenų saugyklas,

debesis, PKI, autentifikacijos ir prieigos kontrolės sistemas bei kitas kritines infrastruktūros sritis. Tokiu būdu organizacija užtikrina, kad visi algoritmai, protokolai, raktai, sertifikatai, raktų valdymo sistemos ir kiti kriptografiniai komponentai būtų tinkamai inventorizuoti, o jų naudojimo kontekstas ir galimas poveikis saugumui būtų įvertintas.

Nuosekliai ir periodiškai atnaujinta inventorizacija ne tik sudaro pagrindą organizacijos kriptografinių priemonių valdymui, bet ir leidžia visapusiškai stiprinti kibernetinį atsparumą, užtikrinti sistemų saugumą, efektyvų resursų panaudojimą ir rizikų valdymą. Reguliarus inventorizacijos duomenų atnaujinimas po infrastruktūros pokyčių, naujų sistemų diegimo ar migracijos projektų užtikrina, kad organizacija nuolat turėtų tikslų ir patikimą vaizdą apie savo kriptografinius išteklius bei jų naudojimą.

7. PRIEDAS. KRIPTOGRAFIJOS TAIKYMO INVENTORIZACIJOS FORMA

Inventorizacijos forma pateikiama atskirame Excel faile. Ji skirta sistemingai surinkti ir struktūrizuoti informaciją apie visus organizacijoje naudojamus kriptografinius komponentus, įvertinti jų riziką, priklausomybę nuo tiekėjų ir suplanuoti nuoseklų perėjimą prie postkvantinių sprendimų. Pateikta struktūra užtikrina, kad inventorizacija būtų išsami, nuosekli ir atitiktų gairių tikslus, palengvindama organizacijos darbą bei stiprindama ilgalaikį informacijos saugumą kvantinėje eroje.

Be inventorizacijos formos, šiame priede taip pat pateikiamas detalus inventorizacijos duomenų modelis, kuriuo organizacija turėtų vadovautis renkant duomenis apie taikomą kriptografiją, įskaitant algoritmus, protokolus, sertifikatus, raktų valdymo sprendimus ir kitus komponentus.

Papildomai pateikiamas kriptografinių algoritmų sąrašas ir jų kvantinio atsparumo vertinimas, kuris padeda identifikuoti sprendimus, neatsparius kvantinėms grėsmėms, ir priimti pagrįstus sprendimus dėl jų atnaujinimo ar pakeitimo postkvantiniais algoritmais. Šis vertinimas leidžia nustatyti kritinius kriptografinius elementus, suplanuoti sistemingą migraciją ir užtikrinti ilgalaikį organizacijos informacijos saugumą kvantinėje eroje.