FLETË KËSHILLASH PËR SIGURINË KIBERNETIKE

SHENJA ALARMI, GABIME TË ZAKONSHME, ZGJIDHJE TË SHPEJTA

Versioni 2025-12-31

αPlan

ID	SEKSIONI	TEMA	PIKAT KYÇE	TERMAT KYÇE	SHENJA ALARMI / GABIM I ZAKONSHËM	BËJE KËTË (PRAKTIKA MË E MIRË)	NËSE S'JE I SIGURT / RAPORTO	NDIKIMI	GJASA	PIKËT E PRIORITETIT	BURIMI
1	**Bazat e Sigurisë Kibernetike**	Pse ka rëndësi siguria kibernetike	Siguria mbron konfidencialitetin, integritetin dhe disponueshmërinë (CIA) e të dhënave dhe sistemeve të biznesit.	CIA triad, rrezik, kërcënim	Të menduarit 'IT-ja merret me sigurinë', prandaj s'kam pse veproj.	Trajtoje sigurinë si pjesë të punës tënde; ndiq politikat dhe raporto incidentet shpejt.	Raporto aktivitetin e dyshimtë menjëherë te siguria ose helpdesk-u i IT-së.	4	3	12 Mesatar	1
2	**Bazat e Sigurisë Kibernetike**	Bazat e zinxhirit të sulmit	Shumica e incidenteve ndjekin hapa si zbulimi, qasja fillestare, ekzekutimi, qëndrueshmëria dhe ndikimi; raportimi i hershëm e këput zinxhirin.	qasje fillestare, malware, qëndrueshmëri	Shpërfillja e anomalive 'të vogla' si kërkesat e papritura të MFA-së.	Raporto anomalitë herët; mos prit derisa të kesh prova.	Nëse merr kërkesa të papritura MFA, raportoji dhe ndrysho fjalëkalimin.	5	3	15 I lartë	2
3	**Bazat e Sigurisë Kibernetike**	Fjalëkalimet kundrejt MFA-së	Fjalëkalimet e forta e unike bashkë me MFA-në ulin rrezikun e marrjes së llogarisë.	MFA, menaxher fjalëkalimesh, credential stuffing	Ripërdorimi i fjalëkalimeve nëpër faqe të ndryshme.	Përdor një menaxher fjalëkalimesh; aktivizo MFA-në kudo që ofrohet.	Nëse dyshon për ripërdorim fjalëkalimi, ndryshoji duke filluar nga email-i dhe SSO.	5	4	20 Kritik	3
4	**Bazat e Sigurisë Kibernetike**	Përditësimet dhe arnimet	Përditësimet në kohë mbyllin dobësitë e njohura që shfrytëzohen nga sulmuesit.	patching, dobësi, CVE	Klikimi i 'më kujto më vonë' pafundësisht.	Instalo përditësimet menjëherë; rindiz kur kërkohet.	Nëse një kërkesë përditësimi duket e dyshimtë, verifikoje përmes app store-it zyrtar ose IT-së.	4	3	12 Mesatar	1
5	**Bazat e Sigurisë Kibernetike**	Kopjet rezervë (çfarë mund të bësh)	Kopjet rezervë mundësojnë rikuperimin nga ransomware ose fshirja aksidentale.	kopje rezervë, ransomware, rikuperim	Ruajtja e kopjes së vetme të skedarëve kritikë në një pajisje lokale.	Ruaje punën në sisteme të miratuara e me kopje rezervë (p.sh. disqet cloud të kompanisë).	Nëse skedarët zhduken ose duken të enkriptuar, shkëpute pajisjen dhe raporto menjëherë.	5	3	15 I lartë	2
6	**Terminologjia e Sigurisë së Informacionit**	Autentikimi kundrejt autorizimit	Autentikimi provon se kush je; autorizimi përcakton çfarë mund të bësh.	authN, authZ, IAM	Të supozosh se hyrja në llogari nënkupton leje për të ndarë të dhëna.	Verifiko të drejtat e qasjes para se të ndash; zbato privilegjin minimal.	Nëse s'je i sigurt, pyet pronarin e të dhënave ose IT-në për qasjen e duhur.	4	3	12 Mesatar	1
7	**Terminologjia e Sigurisë së Informacionit**	Privilegji minimal	Jep qasjen minimale të nevojshme për punën dhe hiq qasjet e papërdorura.	least privilege, RBAC	Mbajtja e të drejtave të administratorit 'për çdo rast'.	Kërko qasje të përkohshme të ngritur vetëm kur nevojitet; rishiko qasjet rregullisht.	Nëse sheh qasje që s'të duhet, kërko heqjen e saj.	4	3	12 Mesatar	2
8	**Terminologjia e Sigurisë së Informacionit**	Klasifikimi i të dhënave	Trajtoji të dhënat sipas ndjeshmërisë së tyre (p.sh. publike, të brendshme, konfidenciale).	klasifikim të dhënash, PII	Dërgimi i të dhënave konfidenciale përmes email-it personal ose mjeteve të bisedës konsumatore.	Përdor mjete dhe etiketa të miratuara; ndaj vetëm me marrës të autorizuar.	Nëse i dërgon të dhënat gabimisht, raporto menjëherë; shpejtësia ka rëndësi.	5	3	15 I lartë	1
9	**Terminologjia e Sigurisë së Informacionit**	Enkriptimi kundrejt hashimit	Enkriptimi është i kthyeshëm me një çelës; hashimi është njëkahësh për kontrolle integriteti.	enkriptim, hashim, çelës	Të supozosh se 'i hashuar' do të thotë 'i enkriptuar'.	Përdor enkriptim të miratuar për të dhënat në qetësi dhe në transit; mbroji çelësat.	Nëse të kërkojnë të ruash sekrete, përdor një menaxher sekretesh, jo dokumente.	4	2	8 I ulët	1
10	**Terminologjia e Sigurisë së Informacionit**	Logjet dhe monitorimi	Logjet ofrojnë prova për zbulim, reagim dhe auditim.	logje, telemetri, SIEM	Çaktivizimi i mjeteve të sigurisë sepse duken 'të zhurmshme'.	Mos i çaktivizo mjetet e sigurisë; raporto problemet te IT/siguria.	Nëse dyshon për kompromentim, ruaj provat; mos i fshi pajisjet.	5	2	10 Ulët-mes.	4
11	**Bazat e IA**	Çfarë është IA-ja (me fjalë të thjeshta)	Sistemet e IA-së mësojnë modele nga të dhënat për të parashikuar ose gjeneruar përmbajtje; rezultatet mund të jenë të gabuara.	machine learning, model, inferencë	Të trajtosh rezultatin e IA-së si fakt të garantuar.	Verifiko rezultatet e IA-së, sidomos numrat, citimet dhe udhëzimet.	Nëse rezultati ka rëndësi të lartë, përdor burime autoritative ose rishikim njerëzor.	4	3	12 Mesatar	5
12	**Bazat e IA**	LLM-të dhe halucinacionet	LLM-të parashikojnë tekstin e mundshëm dhe mund të 'halucinojnë' përgjigje bindëse por të rreme.	LLM, halucinacion	Përdorimi i udhëzimeve të gjeneruara nga IA në prodhim pa rishikim.	Kryqëzo me dokumente të besueshme; testo në mjedise të sigurta.	Nëse s'je i sigurt, konsultohu me një ekspert (SME) ose dokumentacionin zyrtar të shitësit.	4	3	12 Mesatar	6
13	**Bazat e IA**	Përdorimi i sigurt i prompteve	Promptet mund të ekspozojnë informacion të ndjeshëm; supozo se promptet mund të regjistrohen.	prompt, rrjedhje të dhënash	Ngjitja e të dhënave të klientëve, sekreteve ose fjalëkalimeve në mjetet e IA-së.	Përdor mjete IA të miratuara; redakto të dhënat e ndjeshme; ndiq politikën.	Nëse ke ndarë të dhëna të ndjeshme aksidentalisht, raporto sipas politikës.	5	3	15 I lartë	5
14	**Bazat e IA**	Trajnimi kundrejt inferencës	Trajnimi e ndërton modelin; inferenca është përdorimi i tij; rreziqet ndryshojnë për secilën.	trajnim, inferencë, fine-tuning	Ngarkimi i datasetave pronësore në mjete të pamiratuara.	Përdor mjedise të miratuara për punën me modele; dokumento burimet e të dhënave.	Nëse prejardhja e të dhënave është e paqartë, ndalo dhe përshkallëzo.	4	2	8 I ulët	6
15	**Bazat e IA**	Hyrjet si sipërfaqe sulmi	Sistemet e IA-së mund të manipulohen përmes hyrjeve të krijuara me qëllim (p.sh. prompt injection).	prompt injection, hyrje armiqësore	Ndjekja verbërisht e lidhjeve ose komandave të sugjeruara nga IA.	Trajtoje rezultatin e IA-së si hyrje të pabesueshme; validoje para se të veprosh.	Nëse IA jep udhëzime të papritura në nivel sistemi, ndalo dhe raporto.	5	2	10 Ulët-mes.	6
16	**IA në Sigurinë Kibernetike**	IA si mbrojtës (ku ndihmon)	IA mund të ndihmojë me triazhin e alarmeve, zbulimin e anomalive dhe përmbledhjen, nën mbikëqyrje njerëzore.	SOAR, SIEM, zbulim anomalish	Të supozosh se zbulimi me IA është 'vendose dhe harroje'.	Përdore IA-në për të fuqizuar analistët; mbaj akordim, validim dhe gjurmë auditimi.	Nëse vendimet e IA-së prekin klientët, kërko porta rishikimi njerëzor.	4	2	8 I ulët	5
17	**IA në Sigurinë Kibernetike**	IA si objektiv	Sulmuesit mund të përpiqen me data poisoning, vjedhje modeli ose sulme inference ndaj sistemeve të IA-së.	data poisoning, model extraction, inversion	Ekspozimi i API-ve të modelit pa kufij shpejtësie ose monitorim abuzimi.	Zbato autentikim, kufizim (throttling), regjistrim dhe monitorim te endpoint-et e IA-së.	Nëse sjellja e modelit ndryshon papritur, heto ndryshimet në të dhëna/prompte.	5	2	10 Ulët-mes.	6
18	**IA në Sigurinë Kibernetike**	Rreziku i shadow AI	Mjetet e pamiratuara të IA-së mund të rrjedhin të dhëna dhe të anashkalojnë qeverisjen.	shadow AI, qeverisje	Punonjësit që përdorin llogari personale IA për të dhëna pune.	Ofro mjete të miratuara; trajno stafin për përdorimin e lejuar; monitoro daljen.	Nëse të nevojitet një aftësi, kërko një zgjidhje të miratuar.	4	3	12 Mesatar	5
19	**IA në Sigurinë Kibernetike**	Përdorimi i sigurt i kopilotëve të IA-së	Kopilotët mund të sugjerojnë kod ose konfigurime të pasigurta.	secure SDLC, rishikim kodi	Pranimi i sugjerimeve të kodit pa rishikim sigurie.	Përdor standarde të kodimit të sigurt; ekzekuto SAST/DAST; bëj rishikim nga kolegët.	Nëse s'je i sigurt, konsultohu me inxhinierinë e sigurisë ose AppSec.	5	2	10 Ulët-mes.	1
20	**IA në Sigurinë Kibernetike**	IA dhe reagimi ndaj incidenteve	IA mund të përshpejtojë përmbledhjet e hetimit, por trajtimi i provave dhe vendimet mbeten të drejtuara nga njeriu.	reagim ndaj incidenteve, zinxhir ruajtjeje	Lejimi i IA-së të mbishkruajë ose transformojë provat origjinale.	Ruaj origjinalet; përdore IA-në mbi kopje; dokumento hapat.	Nëse dyshohet një incident, ndiq playbook-et e reagimit (IR).	5	2	10 Ulët-mes.	4

PRIORITETI = NDIKIMI (1-5) x GJASA (1-5)

- **8** I ulët
- **10** Ulët-mes.
- **12** Mesatar
- **15** I lartë
- **20** Kritik

BURIMET

1. NIST Cybersecurity Framework
2. NIST CSF 2.0 (CSWP 29)
3. CISA - Recognize & Report Phishing
4. NIST SP 800-61r3 - Incident Response
5. NIST AI Risk Management Framework
6. NIST AI 100-1 (AI RMF)
7. CISA - Phishing Guidance
8. CISA - Avoiding Social Engineering

Fjalori i plotë, skenarët e punuar dhe një kuiz i shkurtër ndodhen në fletoren shoqëruese (skedat Fjalori, Skenarët dhe Mini Kuizi).

Shënim: Ky material u krijua në kuadër të projektit 'U.S. Cybersecurity Leadership in AI for Albania', financuar nga Departamenti i Shtetit i Shteteve të Bashkuara. Opinionet, gjetjet dhe përfundimet e paraqitura këtu janë të autorëve dhe nuk pasqyrojnë domosdoshmërisht ato të Departamentit të Shtetit të Shteteve të Bashkuara.

FLETË KËSHILLASH PËR SIGURINË KIBERNETIKE

SHENJA ALARMI, GABIME TË ZAKONSHME, ZGJIDHJE TË SHPEJTA

Versioni 2025-12-31

αPlan

ID	SEKSIONI	TEMA	PIKAT KYÇE	TERMAT KYÇE	SHENJA ALARMI / GABIM I ZAKONSHËM	BËJE KËTË (PRAKTIKA MË E MIRË)	NËSE S'JE I SIGURT / RAPORTO	NDIKIMI	GJASA	PIKËT E PRIORITETIT	BURIMI
21	**Bazat e Inxhinierisë Sociale**	Çfarë është inxhinieria sociale	Manipulimi i njerëzve shpesh është më i lehtë se hakimi i sistemeve.	inxhinieri sociale, bindje	Kërkesa që anashkalojnë procesin për shkak urgjence.	Ngadalëso; verifiko identitetin dhe autorizimin.	Kur ndihesh nën presion, këmbëngul te hapat standarde të verifikimit.	5	4	20 Kritik	3
22	**Bazat e Inxhinierisë Sociale**	Phishing (email)	Phishing-u të josh të klikosh lidhje, të hapësh bashkëngjitje ose të ndash informacion.	phishing, spoofing	Bashkëngjitje e papritur, domen i mospërputhur, kërkesë urgjente pagese.	Parashiko lidhjet me kujdes; verifiko dërguesin; raporto përmes metodës sate të phishing-ut.	Nëse ke klikuar ose hapur diçka, raporto menjëherë dhe ndiq udhëzimet e IT-së.	5	4	20 Kritik	7
23	**Bazat e Inxhinierisë Sociale**	Vishing dhe smishing	Phishing-u me zë dhe SMS shfrytëzon besimin dhe urgjencën.	vishing, smishing	Caller ID duket legjitim; kërkon OTP ose fjalëkalim.	Mos ndaj kurrë fjalëkalime/OTP; telefono prapa me një numër të besueshëm nga direktoria.	Nëse ke ndarë informacion, raporto dhe rivendos kredencialet menjëherë.	5	3	15 I lartë	8
24	**Bazat e Inxhinierisë Sociale**	Pretexting dhe imitim	Sulmuesit mund të paraqiten si IT, drejtues, shitës ose punonjës të rinj.	pretexting, imitim	Kërkesa të pazakonta për qasje, fatura, karta dhurate ose transfertë parash.	Ndiq rrjedhat e miratimit; verifiko përmes një kanali dytësor.	Nëse dikush këmbëngul të anashkalojë kontrollet, përshkallëzoje te menaxheri/siguria.	5	3	15 I lartë	8
25	**Bazat e Inxhinierisë Sociale**	Inxhinieria sociale fizike	Tailgating-u dhe shikimi mbi sup mund të anashkalojnë kontrollet dixhitale.	tailgating, badge, tavolinë e pastër	Dikush pa badge që kërkon ta lësh të hyjë.	Mos fut të tjerë me badge-in tënd; shoqëro vizitorët; blloko ekranin kur largohesh.	Raporto sjelljen fizike të dyshimtë te siguria/objektet.	4	2	8 I ulët	1
26	**Inxhinieria Sociale në Epokën e IA-së**	Phishing i shkruar nga IA	IA gjeneruese mund të prodhojë mesazhe më bindëse e të personalizuara në shkallë të gjerë.	phishing me IA, spearphishing	Mesazhe me gramatikë perfekte por me kërkesa ose kohë të pazakonta.	Verifiko kërkesat përmes një kanali të veçantë e të besuar; trajtoji lidhjet/bashkëngjitjet si armiqësore.	Nëse një mesazh duket i personalizuar në mënyrë të pazakontë, raportoje për analizë.	5	4	20 Kritik	7
27	**Inxhinieria Sociale në Epokën e IA-së**	Deepfake (video/audio)	Deepfake-t mund të imitojnë drejtues ose kolegë për të kërkuar veprime të ndjeshme.	deepfake, klonim zëri	Një telefonatë/video me urgjencë; refuzon telefonatën prapa; frazim i pazakontë.	Përdor verifikim me telefonatë prapa dhe rrjedha miratimi; kërko konfirmim me shkrim.	Nëse dyshohet, ruaj provat (aq sa lejon politika) dhe raporto.	5	3	15 I lartë	5
28	**Inxhinieria Sociale në Epokën e IA-së**	Identitete sintetike	Sulmuesit mund të krijojnë persona realiste duke përdorur foto e profile të gjeneruara nga IA.	identitet sintetik, OSINT	Kontakt i ri me histori minimale që kërkon qasje ose favore.	Verifiko identitetin përmes menaxhimit HR/shitës; përdor kanale zyrtare.	Nëse s'je i sigurt, mos u angazho; përcille te siguria.	4	3	12 Mesatar	3
29	**Inxhinieria Sociale në Epokën e IA-së**	BEC + IA	IA mund t'i ndihmojë sulmuesit të imitojnë stilin e shkrimit për të kërkuar pagesa ose të dhëna.	BEC, mashtrim me fatura	Kërkesa për ndryshim pagese vetëm përmes email-it.	Konfirmo ndryshimet përmes numrave të telefonit të njohur; kërko miratim të dyfishtë.	Nëse është dërguar një pagesë, kontakto financën dhe sigurinë menjëherë.	5	3	15 I lartë	3
30	**Inxhinieria Sociale në Epokën e IA-së**	Zbulim i ndihmuar nga IA	Sulmuesit mund të përdorin IA-në për të shkallëzuar kërkimin mbi organigramat dhe shitësit.	reconnaissance, OSINT	Ndarja e tepërt e detajeve të brendshme në media sociale.	Kufizo informacionin publik; ndiq udhëzimet e zbulimit të informacionit.	Nëse vëren informacion të ndjeshëm publik, kërko heqjen e tij dhe njofto sigurinë.	4	2	8 I ulët	1
31	**Bazat e Sigurisë Kibernetike**	Raportimi i incidenteve	Raportimi i shpejtë ul ndikimin; nuk pritet ta hetosh vetë.	incident, përshkallëzim	Të përpiqesh ta 'rregullosh vetë' dhe të vonosh raportimin.	Përdor kanalet zyrtare të incidenteve; ruaj shënime/pamje ekrani nëse është e sigurt.	Raporto menjëherë me çfarë pe, kur, dhe cila pajisje/aplikacion u përfshi.	5	3	15 I lartë	4
32	**Terminologjia e Sigurisë së Informacionit**	PII kundrejt të dhënave të ndjeshme	PII identifikon një person; të dhënat e ndjeshme mund të përfshijnë kredenciale, të dhëna financiare, shëndetësore e më shumë.	PII, PHI, PCI	Ndarja e spreadsheet-eve me të dhëna klientësh gjerësisht.	Minimizo ndarjen; përdor transferim të sigurt; zbato parimin 'need-to-know'.	Nëse trajtimi i të dhënave është i paqartë, konsultohu me privatësinë/sigurinë.	5	3	15 I lartë	1
33	**Bazat e IA**	Paragjykimi dhe drejtësia	IA mund të pasqyrojë paragjykime nga të dhënat e trajnimit; rezultatet duhet të monitorohen.	paragjykim, drejtësi, drift	Të supozosh se vendimet e IA-së janë 'objektive'.	Testo rezultatet për drejtësi; dokumento kufizimet.	Nëse vendimet prekin njerëz, shto rishikim njerëzor dhe rrugë ankimi.	4	2	8 I ulët	6
34	**IA në Sigurinë Kibernetike**	Siguria e tubacioneve të të dhënave të IA-së	Të dhënat e përdorura për IA janë me vlerë të lartë; mbroji prejardhjen, qasjen dhe integritetin.	data pipeline, prejardhje	Përdorimi i datasetave të panjohura ose vendndodhjeve të pamenaxhuara të ruajtjes.	Kontrollo qasjen; versiono datasetet; valido hyrjet; monitoro ndryshimet.	Nëse zbulon ndërhyrje (tampering), ndalo tubacionin dhe përshkallëzo.	5	2	10 Ulët-mes.	6
35	**Bazat e Inxhinierisë Sociale**	Autoriteti dhe urgjenca si nxitës	Sulmuesit shfrytëzojnë autoritetin dhe urgjencën për të anashkaluar kontrollet.	urgjencë, autoritet, reciprocitet	Kërcënime si 'llogaria do të mbyllet sot' që kërkojnë veprim të menjëhershëm.	Ndalo; verifiko; kërko një kolegu një vështrim të dytë.	Nëse ndihesh i nxituar, kjo është shenjë për të ngadalësuar.	5	4	20 Kritik	8
36	**Inxhinieria Sociale në Epokën e IA-së**	Playbook i verifikimit	Përdor verifikim identiteti me shumë hapa për kërkesa të ndjeshme, sidomos ato të marra dixhitalisht.	kanal i veçantë, verifikim	Kërkesa vjen përmes bisedës/videos duke kërkuar qasje ose pagesë.	Telefono prapa duke përdorur direktorinë; kërko tiketë/miratim; konfirmo me menaxherin.	Nëse verifikimi dështon, ndalo dhe raporto.	5	4	20 Kritik	3

PRIORITETI = NDIKIMI (1-5) x GJASA (1-5)

- **8** I ulët
- **10** Ulët-mes.
- **12** Mesatar
- **15** I lartë
- **20** Kritik

BURIMET

1. NIST Cybersecurity Framework
2. NIST CSF 2.0 (CSWP 29)
3. CISA - Recognize & Report Phishing
4. NIST SP 800-61r3 - Incident Response
5. NIST AI Risk Management Framework
6. NIST AI 100-1 (AI RMF)
7. CISA - Phishing Guidance
8. CISA - Avoiding Social Engineering

Fjalori i plotë, skenarët e punuar dhe një kuiz i shkurtër ndodhen në fletoren shoqëruese (skedat Fjalori, Skenarët dhe Mini Kuizi).

Shënim: Ky material u krijua në kuadër të projektit 'U.S. Cybersecurity Leadership in AI for Albania', financuar nga Departamenti i Shtetit i Shteteve të Bashkuara. Opinionet, gjetjet dhe përfundimet e paraqitura këtu janë të autorëve dhe nuk pasqyrojnë domosdoshmërisht ato të Departamentit të Shtetit të Shteteve të Bashkuara.