SAUGUMO INCIDENTO KRIZIŲ VALDYMO ANALIZĖ

crisis.cybora.cloud

Fintech įmonės kibernetinės atakos ir krizės valdymo nesėkmių ataskaita

Incidento data:	2026-06-11 d.
Paveikta įmonė:	Tarptautinė Fintech įmonė (BMV filialas Lietuvoje)
Dalyvių skaičius:	18 žmonių (5 C-lygio grupės + SOC/IT)
Finansinė žala:	**2 000 000 EUR + ransomware žala**
Incidento tipas:	APT, DDoS, Phishing, Social Engineering, Ransomware, BEC
Rezultatas:	**NKSC perėmė valdymą. Pinigai pavogti.**
Parengė:	CYBORA, MB | Kibernetinio saugumo analizė

Simuliacijos data:	2026-06-11
Dalyviai:	21 asmenų (5 C-lygio grupės: CTO, CISO, AML/LEGAL/COMPLIANCE, CEO, CMO + SOC/IT)
Metodologija:	MEST (Monitor – Evaluate – Stabilize – Transition)
AI analizės įrankiai:	Mistral 7B (turinio sintezė) · gemma-4-12B-it (anomalijos, vertimas LT), Skills.md, design.md formuotas pagal Claude AI
Bendras rezultatas:	**19/105 taškų (18%) – KRITIŠKAI SILPNAS KRIZIŲ VALDYMAS**
Parengė:	CYBORA, MB | Peržiūrėta ir patvirtinta žmogaus eksperto Arūno Girdziušo arg@cybora.tech

Turinys

1. VADOVŲ SUVESTINĖ

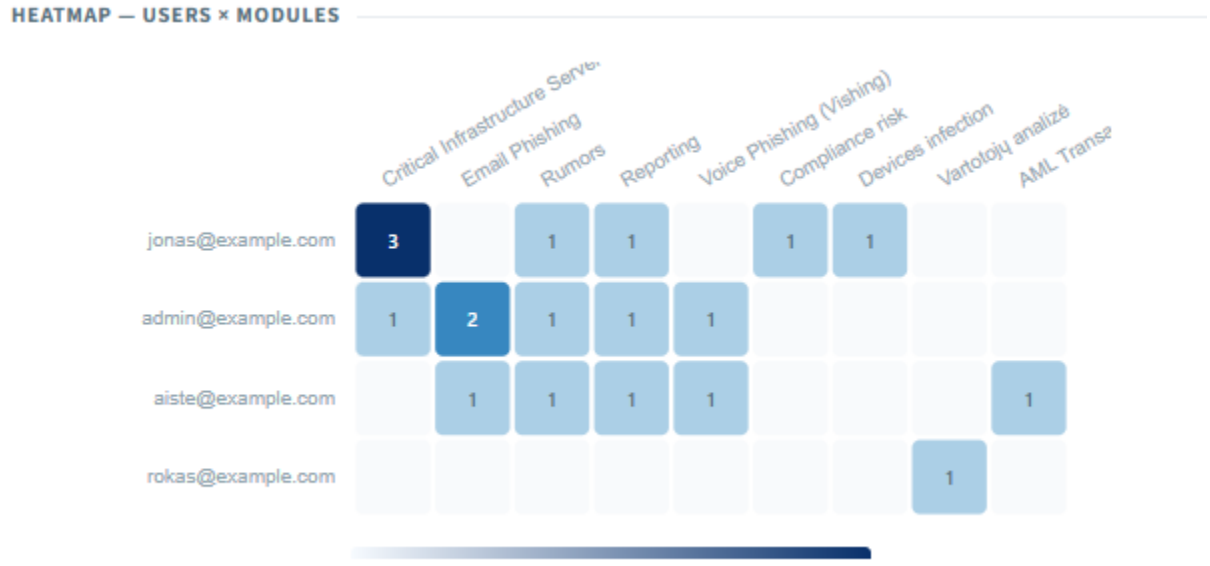
⚠ KRITINIS INCIDENTAS: Dėl kompleksinės kibernetinės atakos ir krizės valdymo nesėkmių buvo prarasta 2 000 000 EUR. Ransomware užblokavo visas sistemas. NKSC buvo priverstas perimti valdymą iš vadovybės.

Šis incidentas yra vadovėlinis APT (Advanced Persistent Threat) pavyzdys, kuriame puolėjai ne tik išnaudojo techninius pažeidžiamumus, bet ir socialinę inžineriją, organizacinę chaosą bei „siloso“ efektą tarp vadovybės grupių.

Pagrindiniai nesėkmės veiksniai:

- Nebuvo paskirto Krizės Orkestratoriaus (Incident Commander) – niekas nepriėmė galutinių sprendimų
- CTO atidėliojo kritinį failover sprendimą 7 minutes – SLA pažeistas
- Krizės valdymo sistema egzistavo, bet neveikė praktiškai
- „Siloso“ efektas – 5 grupės veikė izoliuotai, nekomunikuodamos tarpusavyje
- AML sistema praleido 2M EUR pervedimą be papildomų patikrinimų
- CEO ir CTO pasirašė suklastotą pervedimą neatpažinę klastotės

"Krizės prasideda ne tada, kai to tikitės. Todėl jai pasiruošti nėra laiko – ją reikia valdyti realiu laiku, ir tam būtinas Orkestratorius."



2. DALYVIŲ STRUKTŪRA IR SILO EFEKTAS

Pratybose dalyvavo 18 asmenų, padalintų į 5 funkcines grupes. Grupės buvo tyčia izoliuotos, kad simuliuotų realų silo efektą – tipišką organizacinę problemą, kai skyriai dirba nepriklausomai ir nesidalija informacija.

GRUPĖ	ŽMONĖS	VAIDMUO	PASTABOS
CTO	4	Infrastruktūros valdymas, DR, Failover	„SILOSAS“
CISO	4	Saugumo incidentų koordinavimas	„SILOSAS“
AML/LEGAL/COMPLIANCE	4	Reguliacinė atitiktis, finansinė stebėsena	„SILOSAS“
CEO	4	Galutiniai sprendimai, komunikacija su valdyba	„SILOSAS“
CMO	4	Išorės komunikacija, reputacijos valdymas	„SILOSAS“
SOC/IT	1	Techninė stebėsena ir reagavimas (nepakankami įgalinimai)	„SILOSAS“
IŠ VISO	**21**	Dalyviai, padalinti į siloso grupes	IZOLIUOTI

● SILO EFEKTO PADARINYS: Nė viena grupė neturėjo viso paveikslo. CISO nežinojo apie AML problemas. CEO nežinojo apie DDoS. AML nereagavo į pinigų plovimo signalus. Informacija egzistavo – bet ne ten, kur reikėjo.

Įmonė: VISIEMS DARBUOTOJAMS

{1:F01CHASUS33AXXX0000000000} {2:I299BATRLT21XXXXN} {4: :20:USDLIQ20251021

:79:URGENT — USD ACCOUNT FUNDING REQUIRED.

YOUR USD LORO ACCOUNT WITH JPMORGAN (A/C 502-000123-789) IS OVERDRAWN DUE TO MULTIPLE OUTGOING PAYMENTS SENT THIS MORNING TOTALING APPROXIMATELY USD 78 MILLION TO BENEFICIARIES IN ASIA AND THE MIDDLE EAST. CURRENT AVAILABLE BALANCE: USD -12,350,000.

TO CONTINUE PROCESSING OUTGOING PAYMENTS, PLEASE FUND YOUR ACCOUNT IMMEDIATELY VIA MT202 TO:

BENEFICIARY BANK: JPMORGAN CHASE BANK N.A. SWIFT: CHASUS33 FOR CREDIT TO: BATRLT21 USD ACCOUNT REFERENCE: URGENT FUNDING

PLEASE CONFIRM FUNDING DETAILS VIA MT299 QUOTING REF ABOVE.

- TREASURY LIQUIDITY DESK, NEW YORK -}

{1:F01CHASUS33AXXX0000000000} {2:I199BATRLT21XXXXN} {4: :20:CHAS-HOLD-20251021-TR :79:URGENT — PAYMENT ON HOLD DUE TO POSSIBLE SANCTIONS MATCH.

WE HAVE PLACED A HOLD ON THE FOLLOWING OUTWARD USD PAYMENT IN ACCORDANCE WITH OUR SANCTIONS SCREENING & AML CONTROLS. FUNDS HAVE NOT BEEN CREDITED TO THE INTERMEDIARY / BENEFICIARY BANK. DETAILS: SENDER: BALTIC TRUST BANK / A/C 333-222-111 PAYMENT REFERENCE (YOUR REF): BTR-TR-20251020-007 AMOUNT: USD 2 000 000 VALUE DATE: 21 OCT 2025 PAYEE: RUSSIAN EXPORT LTD. (ACCOUNT TR-998877) BENEFICIARY BANK: TURBANK A.S. / SWIFT: TRBKTRISXXX ORIGINATOR ULTIMATE: BALTIC TRADE IMPORT LTD REASON FOR HOLD: OUR SANCTIONS SCREENING IDENTIFIED A **POSSIBLE NAME MATCH** TO AN **OFAC SDN ENTRY** ASSOCIATED WITH THE RUSSIAN FEDERATION. UNDER OUR OBLIGATIONS, WE MUST INVESTIGATE POTENTIAL MATCHES PRIOR TO ONWARD PROCESSING. ACTION REQUIRED:

1. PLEASE CONFIRM WHETHER THE BENEFICIARY OR ANY ULTIMATE/RELATED PARTY IS ON A SANCTIONS LIST (SDN, EU, UK, ETC.).
2. PROVIDE SUPPORTING DOCUMENTATION: COMMERCIAL INVOICE, CONTRACT, PURPOSE OF PAYMENT, BENEFICIAL CORPORATE REGISTRY EXTGRACT, AND ANY KNOW YOUR CUSTOMER (KYC) AS WELL AS UBO INFORMATION AVAILABLE.

CONTACT: SANCTIONS & AML TEAM — JPMORGAN CHASE (NEW YORK) COMPLIANCE CASE REF: CHAS-SAN-20251020-784 EMAIL: SANCTIONS.TEAM@JPMORGAN.EXAMPLE (SECURE CHANNEL RECOMMENDED) TELEPHONE: (212) 555 1234

PLEASE RESPOND URGENTLY. UNTIL CLEARED, THE PAYMENT WILL REMAIN ON HOLD AND MAY BE SUBJECT TO FREEZING UNDER OFAC REGULATIONS. -}

3. INCIDENTO LAIKO JUOSTA

Pilna įvykių chronologija nuo pirmojo signalo iki NKSC intervencijos:

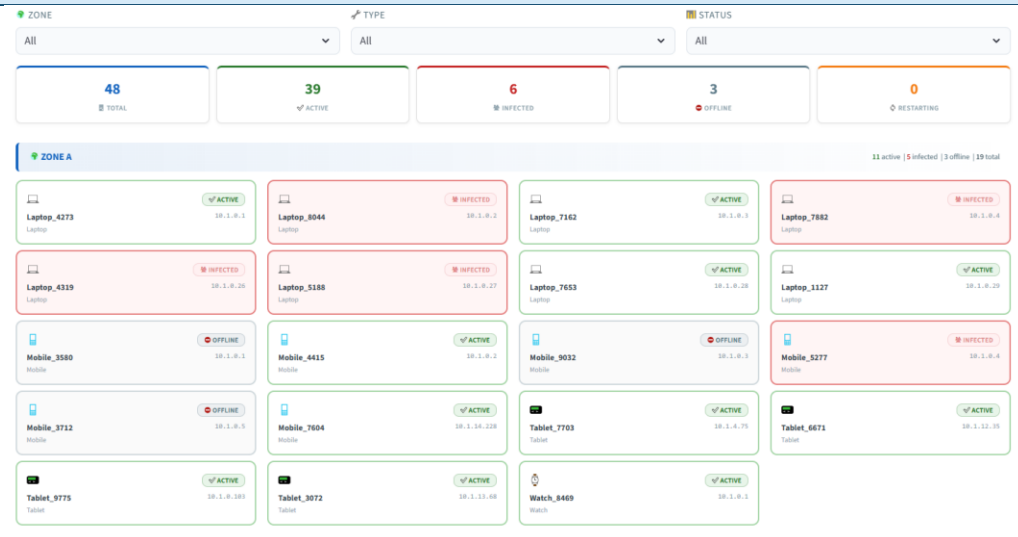
LAIKAS	ĮVYKIS	STATUSAS	TIPO RIZIKA
16:39:22	Padidėjęs apkrovimas API mazguose (CPU 94%, RAM 87%)	SIGNALAS	
16:39:23	Srautas iš Brazilijos (1190 req/min) ir Pakistano (950 req/min) – DDoS požymiai	GRĖSMĖ	
16:39:25	APP-API-02 neatsakantis – 504 Gateway Timeout	KRITINIS	
16:39:30	Auto-scaling nepavyko (CPU limitas)	KRITINIS	
16:39:35	Sistema rekomenduoja FAILOVER į Kauno DC – reikalingas žmogaus sprendimas	SPRENDIMAS	
16:39:38	CTO gauna eskalavimą – DR planas B.2 reikalauja žaliojo šviesofo	VĖLAVIMAS	
16:40–16:46	CTO laukia, sako: "Palaukime 5 min, stebėkime srautą" – neveikiama	KRITINĖ KLAIDA	
16:47:03	SLA pažeidimas – paslaugos neprieinamos >8 min (Login, Payments, Užsakymai)	SLA PAŽEISTAS	
16:48:00	CTO bando aktyvuoti DR – per vėlai, sinchronizacija neveikia	NEEFEKTYVU	
~16:50	Hakeriai pasiekia sistemas ir buhalterinę duomenų bazę	PAŽEIDIMAS	
~17:00	CISO atjungia darbuotoją – tai buvo tik "pritraukiamasis" puolimas	KLAIDA	
~17:10	Policijos pranešimas (suklastotas) atidarytas AML sistemoje – AML užkrėsta	KATASTROFA	
~17:20	2 mln. EUR pervedimas paruoštas hakerių – laukiama parašų	FINANSINĖ ŽALA	
~17:30	CEO ir CTO pasirašo – nepastebėtas suklastotas policijos pranešimas	GALUTINĖ KLAIDA	
~17:35	2 mln. EUR pervesta. Ransomware paleistas visoje sistemoje	ŽLUGIMAS	
~17:36	NKSC perima valdymą. CEO sustabdytas	INTERVENCIJA	

4. PUOLIMO GRANDINĖ (KILL CHAIN ANALIZĖ)

Hakeriai vykdė daugiasluoksnę ataką, naudodami kelias paralelines taktikas vienu metu:

PUOLIMO FAZĖ	APRAŠYMAS	EFEKTAS
1. Žvalgyba (Recon)	Hakeriai tyrinėja tikslinę fintech įmonę, identifikuoja C lygio vadovus	VIDUTINIS
2. Pradinis vektorius (Initial Access)	Suklastoti CV laiškai siunčiami CEO – vienas laiškas užkrėstas. CEO atidaro visus.	VIDUTINIS
3. Įsitvirtinimas (Persistence)	Virusas plinta tinkle – 5 → 20 įrenginių, serveriai persikraunami. Nėra reakcijos.	VIDUTINIS
4. Šoninė judėjimas (Lateral Movement)	Hakeriai pereina į aukštesnio lygio sistemas – buhalterija, AML sistema	VIDUTINIS
5. Dėmesio nukreipimas (Distraction)	DDoS puolimas + suklastotos žinutės = CISO ir CTO dėmesys nukreiptas	AUKŠTAS
6. Socialinė inžinerija (Social Eng.)	Suklastotas policijos pranešimas patenka į AML sistemą. Darbuotojas gauna 100K € užduotį.	AUKŠTAS
7. Finansinis išnaudojimas (Exfiltration)	2M EUR pervedimas paruoštas. CEO ir CTO pasirašo – neatpažino klastotės.	KRITINIS
8. Ransomware	Po pervedimo – ransomware paleistas visoje sistemoje. Sistemos blokuotos.	KRITINIS
9. Pasitraukimas (Exit)	Pinigai pervesti, NKSC perima valdymą. Žala neatstatoma.	

💡 PASTABA: Puolėjai naudojo klasikinę "triukšmo ir šešėlio" taktiką – DDoS ir virusai buvo triukšmas, o realus tikslas (finansiniai duomenys ir AML sistema) buvo pasiektas per socialinę inžineriją.



5. RTO / RPO / MTTR ANALIZĖ

Įmonė turėjo nustatytus atkūrimo tikslus, tačiau nei vienas iš jų nebuvo pasiektas:

METRIKA	PLANUOTA VERTĖ	REALIAI PASIEKTA	REZULTATAS
RTO (Recovery Time Objective)	60 minučių	**~180+ minučių**	**NEPASIEKTA – 3x viršyta**
RPO (Recovery Point Objective)	120 minučių	Nežinoma (sinchronizacija neveikė)	**NEPASIEKTA – duomenų praradimas**
MTTR (Mean Time To Recover)	30 minučių	Nenustatytas (sistema neatkurta)	**NEPASIEKTA – sistema neatkurta**
SLA Prieinamumas	99.9% (max 8.7h/yr)	~8 min. downtime per incidentą	**PAŽEISTAS SLA**

5.1. Vizualinė RTO/RPO palyginimo diagrama

Planuotų ir realiai pasiektų verčių palyginimas:

METRIKA	PLANAS	REALYBĖ	DELTA
RTO	**60 min**	**180+ min**	**+120 min**
RPO	**120 min**	**Nežinoma**	**Nežinoma**
MTTR	**30 min**	**Nebaigta**	**Nebaigta**

RTO PLANAVIMO NESĖKMIŲ PRIEŽASTYS

1. CTO vėlavimas priimant failover sprendimą (+7 min) = tiesiogiai pažeidė SLA
2. Kauno DC sinchronizacija neveikė = DR aktyvinimas buvo neveiksmingas
3. MTTR 30 min. nebuvo pasiektas, nes sistema buvo visiškai blokuota ransomware
4. Paskutinis failover testas: 2025-03-04 – DALINIS. Tikroji sistema nebuvo pasirengusi.

6. VAIDMENŲ IR ATSAKOMYBIŲ ANALIZĖ

Kiekvienos grupės veiksmai ir jų pasekmės krizės metu:

VAIDMUO	VEIKSMAI / NEVEIKIMAS	PASEKMĖ	ĮVERTINIMAS
CEO	Laukė informacijos, nieko nesiėmė iniciatyvos	Pasirašė suklastotą pervedimą	NEEFEKTYVUS
CTO	Atidėliojo failover sprendimą 7 min., neefektyviai aktyvavo DR	Pasirašė suklastotą pervedimą	NEEFEKTYVUS
CISO	Koordinavo neefektyviai, atjungė netinkamą asmenį	Nepatvirtino pervedimo (teigiamas)	DALINAI
AML/LEGAL/COMPLIANCE	Gavo pranešimą apie pinigų plovimą – nieko nedarė	2M pervedimas praleistas per sistemą	NEEFEKTYVUS
CMO	Perdavė VDAI informaciją, bet toliau nesiėmė veiksmų	Komunikacijos su visuomene nebuvimas	DALINAI
IT/SOC	Stebėjo, generavo alarmą, bet neturėjo įgalinimų veikti	Infrastruktūra pažeista	REAGUOJO

6.1. Krizės Orkestratoriaus nebuvimo pasekmės

❌ KRITINIS TRŪKUMAS: Pratybų metu nebuvo paskirto Krizės Orkestratoriaus (Incident Commander). Tai reiškė, kad: • Niekas neturėjo galutinio sprendimo teisės • Grupės veikė savarankiškai ir prieštaringai • Informacija nebuvo centralizuota • Sprendimai buvo priimami per lėtai arba visai nepriimami • CEO laukė, CTO atidėliojo, CISO koordinavo blogai

Krizės Orkestratoriaus funkcijos:

- Vienas centralizuotas sprendimų priėmimo taškas
- Koordinuoja visų grupių veiksmus realiu laiku
- Turi įgalinimus priimti sprendimus be ilgų diskusijų
- Komunikuoja su valdyba, reguliatoriais ir visuomene
- Valdo laiko ribotą protokolą (pvz., 15 min. sprendimų langai)
- Po incidento – rengia postmortem ataskaitą

7. TEIGIAMI IR NEIGIAMI ASPEKTAI

✓ TEIGIAMI ASPEKTAI (Plusai)	✗ KRITINĖS KLAIDOS (Minusai)
✓ SOC ir IT komanda turėjo stebėsenos įrankius	✗ Nebuvo paskirto Krizės Orkestratoriaus (Incident Commander)
✓ NKSC sureagavo ir galiausiai perėmė valdymą	✗ CTO atidėliojo kritinį failover sprendimą 7 minutes
✓ Buvo sukurta incidentų valdymo grupė (nors vėlai)	✗ Krizės valdymo sistema neveikė – grupė tik svarstė
✓ CISO bandė koordinuoti veiksmus	✗ Silo efektas – komandos nebendravo tarpusavyje
✓ Sistemos automatiškai sugeneravo alarmą ir rekomendacijas	✗ CEO laukė informacijos, nieko nesako ir nesiima veiksmų
✓ DR planas B.2 egzistavo (nors nebuvo efektyviai panaudotas)	✗ AML sistema veikė izoliuotai – nepastebėjo 2M pervedimo
✓ Failover infrastruktūra buvo paruošta (Kauno DC)	✗ Darbuotojai atidarinėjo nežinomos kilmės el. laiškus su CV
✓ Eskalavimo grandinė egzistavo (CEO, CISO informuoti)	✗ CISO atjungė ne tą asmenį (puolimo maskaradas nepastebėtas)
	✗ Ransomware buvo paleistas neapsaugotoje sistemoje
	✗ Suklastotas policijos pranešimas nebuvo atpažintas
	✗ Kauno DC sinchronizacija neveikė (nepasirengta)
	✗ Finansinė autorizacija be saugumo papildomo patvirtinimo

8. REKOMENDACIJOS

Šios rekomendacijos turi būti įgyvendintos prioritetine tvarka:

PRIORITETAS	REKOMENDACIJA	APRAŠYMAS
KRITINIS	**Paskirti Krizės Orkestratorių**	Vienas asmuo, kuris priima galutinį sprendimą krizės metu. Aiški komandų grandinė.
KRITINIS	**Reguliarūs DR/Failover testavimai**	Bent kas ketvirtį – pilnas testas su laiko matavimais ir failover sinchronizacijos patikrinimu.
KRITINIS	**Multi-faktorinė autorizacija finansiniams pavedimams**	Kiekvienas pavedimas >100K turi reikalauti bent 3 nepriklausomų patvirtinimų + OTP.
AUKŠTAS	**Silo efekto šalinimas – kryžminiai mokymai**	Kiekvienas C lygio vadovas turi žinoti kito vaidmenį krizės metu. Kryžminės pratybos.
AUKŠTAS	**El. laiškų saugumo mokymai**	Phishing simuliacijos, sandboxing sprendimas, "Zero Trust" el. pašto politika.
AUKŠTAS	**Incidentų valdymo procedūrų atnaujinimas**	Aiškūs sprendimų medžiai kiekvienam scenarijui – DDoS, ransomware, duomenų nutekėjimas.
VIDUTINIS	**AML sistemos izoliavimas ir stebėsena**	AML sistema turi automatiškai blokuoti didelius pavedimus krizės metu ir reikalauti papildomo patvirtinimo.
VIDUTINIS	**SOC įgalinimas veikti savarankiškai**	SOC komanda turi turėti aiškius įgalinimus izoliuoti mazgus be CTO patvirtinimo krizinėmis situacijomis.
VIDUTINIS	**Komunikacijos planas su NKSC ir VDAI**	Automatizuotas pranešimas reguliatorams per pirmąsias 30 min. nuo incidento.

9. KAS TURĖJO BŪTI ATLIKTA – PAGAL KRIZIŲ VALDYMO METODOLOGIJĄ

9.1. Pirmos 5 minutės (16:39–16:44)

- ✓ NEDELSIANT: Paskirti Krizės Orkestratorių (pvz., CISO arba dedikuotas Incident Commander)
- ✓ NEDELSIANT: Aktyvuoti Incidentų Valdymo Grupę (IVG) su aiškiais vaidmenimis
- ✓ NEDELSIANT: CTO turi patvirtinti FAILOVER sprendimą – nesvarstyti, veikti
- ✓ NEDELSIANT: SOC izoliuoja pažeistus segmentus (network segmentation)
- ✓ NEDELSIANT: Pranešti CEO apie SLA rizikos lygį

9.2. 5–15 minutės (16:44–16:54)

- ✓ Aktyvuoti DR planą B.2 – visas komandas turi veikti pagal iš anksto nustatytą protokolą
- ✓ AML sistema: automatiškai blokuoti visus pavedimus >100K iki incidento pabaigos
- ✓ Pranešti NKSC (per 30 min. – reikalavimas pagal LR KĮ)
- ✓ CMO: Paruošti vidinę ir išorinę komunikaciją
- ✓ Visi grupių vadovai praneša IVG koordinatoriui kas 5 minutes

9.3. 15–60 minutės

- ✓ Pilnas forensic tyrimas pradedamas nuo pirmo pažeisto kompiuterio
- ✓ Visos sistemos audituojamos – ieškoma šoninės judėjimo pėdsakų
- ✓ Valdyba ir teisinis skyrius informuojami apie galimą duomenų nutekėjimą
- ✓ Pradedamas ransomware atidavimo sprendimo procesas (su teisine konsultacija)
- ✓ Pradedamas RTO matavimas – tikslinis atstatymas per nustatytą laiką

💡 ESMINIS PRINCIPAS: "Krizės prasideda nuo tada, kai nelaukiate, kad ji prasidės. Todėl jai pasiruošti nėra laiko – ją reikia valdyti ir suprasti kas yra Orkestratorius." Krizių valdymas nėra planavimas krizės metu – tai pasiruošimas prieš ją.

10. IŠVADOS

1	**Organizaciniai trūkumai buvo svarbiausia nesėkmės priežastis – ne techniniai.** Infrastruktūra turėjo DR ir failover – bet organizacija neturėjo Orkestratoriaus. Sistema buvo, bet neveikė.
2	**Silo efektas yra realus ir pavojingas.** Kai komandos nebendravo, hakeriai galėjo ramiai vykdyti ataką. Kiekviena grupė turėjo dalį paveikslo – bet niekas nematė viso.
3	**RTO 60 min., RPO 120 min., MTTR 30 min. – NEBUVO PASIEKTA.** Plano turėjimas nėra pakankamas. Jei planas nėra reguliariai testuojamas ir darbuotojai nėra apmokomi, jis neveiks krizės metu.
4	**Socialinė inžinerija buvo efektyvesnė nei techninė ataka.** Suklastotas policijos pranešimas ir CV laiškai – ne techniniai išnaudojimai – padėjo pasiekti didžiausią žalą. Žmogiškasis faktorius yra silpniausia grandis.
5	**AML ir finansinė kontrolė turėjo sustabdyti ataką.** 2M EUR pervedimas turėjo būti automatiškai sustabdytas krizės metu. AML sistema veikė izoliuotai ir praleido pervedimą.
6	**Ši pratybų patirtis yra neįkainojama.** Kontroliuojamoje aplinkoje išmoktos pamokos – bet kokia kaina – yra pigesnės nei realus incidentas. Rekomenduojama organizuoti reguliarias krizių valdymo pratybas su Orkestratoriumi.

MEST METODOLOGIJOS
SIMULIACIJOS VERTINIMO ATASKAITA

Monitor · Evaluate · Stabilize · Transition

Simuliacijos data:	2026-06-11
Dalyviai:	21 asmenų (5 C-lygio grupės: CTO, CISO, AML/LEGAL/COMPLIANCE, CEO, CMO + SOC/IT)
Metodologija:	MEST (Monitor – Evaluate – Stabilize – Transition)
AI analizės įrankiai:	Mistral 7B (turinio sintezė) · gemma-4-12B-it (anomalijos, vertimas LT), Skills.md, design.md formuotas pagal Claude AI
Bendras rezultatas:	**19/105 taškų (18%) – KRITIŠKAI SILPNAS KRIZIŲ VALDYMAS**
Parengė:	CYBORA, MB | Peržiūrėta ir patvirtinta žmogaus eksperto Arūno Girdziušo arg@cybora.tech

1. MEST METODOLOGIJOS APŽVALGA

MEST – praktinė keturių fazių krizių valdymo metodika, skirta greitam reagavimui į IT incidentus, kibernetines krizes ir organizacinius sutrikimus. Ji naudojama kaip supaprastintas, bet struktūruotas modelis, kai reikia aiškios veiksmų sekos be ISO lygio biurokratijos.

#	FAZĖ	TIKSLAS	PAGRINDINIAI VEIKSMAI
1	MONITOR	Kuo greičiau aptikti krizę ir suprasti jos mastą	SIEM/SOC alertai, log stebėjimas, anomalijų aptikimas, incidento klasifikavimas
2	EVALUATE	Suprasti priežastį, riziką ir galimus veiksmus	RCA analizė, SLA rizika, komunikacijos planas, AI scenarijai
3	STABILIZE	Sustabdyti krizės plitimą ir atkurti pagrindines funkcijas	Izoliavimas, workarounds, DR aktyvavimas, nuolatinis statuso atnaujinimas
4	TRANSITION	Grąžinti į pilną veikimą ir užkirsti kelią pasikartojimui	PIR, forensics, reguliatorių pranešimas, dokumentacija, prevencija

Standartiniai atitikmens: MEST Transition fazė integruojama su ISO 27001 A.16 (Incident Management), ISO 22301 (Business Continuity) ir NIST CSF Recover funkcija.

2. AI ĮRANKIŲ PANAUDOJIMAS ANALIZĖJE

Simuliacijos vertinimo ataskaitoje buvo panaudoti šie dirbtinio intelekto įrankiai duomenų apdorojimui, anomalijų aptikimui ir lietuviško turinio formavimui:

AI ĮRANKIS / AGENTAS	FUNKCIJA	PANAUDOJIMAS	TAIKYMAS ANALIZĖJE
Mistral 7B (llama.cpp, local)	**Teksto analizė ir turinio formavimas**	Incidentų aprašymų sintezė, ataskaitų teksto generavimas, MEST fazių vertinimo tekstai	*Simuliacijos ataskaita, rekomendacijų blokai*
google/gemma-4-12B-it	**Anomalijų aptikimas ir klasifikavimas**	Log failų analizė, srautų anomalijų identifikavimas, elgesio modelių koreliacija	*Monitor fazės vertinimas, KYC neatitikimų analizė*
google/gemma-4-12B-it	**Vertimas į lietuvių kalbą**	Techninių terminų ir incidentų aprašymų vertimas į taisyklingą lietuvių kalbą	*Visos lentelės, išvados, pastabos*
Žmogaus peržiūra	**Galutinė patikra ir patvirtinimas**	Visas AI sugeneruotas turinys buvo peržiūrėtas ir patvirtintas žmogaus eksperto prieš įtraukiant į ataskaitą	*Visi skyriai – galutinis patvirtinimas*

> ⚠ **SVARBI PASTABA – Žmogaus patvirtinimas**
>
> Visas AI sugeneruotas turinys (teksto sintezė, vertimas, anomalijų klasifikavimas) buvo kruopščiai peržiūrėtas ir patvirtintas kibernetinio saugumo eksperto prieš įtraukiant į galutinę ataskaitą. AI įrankiai naudoti kaip pagalbinė priemonė – galutinis sprendimas ir atsakomybė išlieka žmogui.

3. SIMULIACIJOS VEIKSMŲ VERTINIMO LENTELĖ

Žemiau pateikiama pilna kiekvienoje MEST fazėje tikrintų veiksmų lentelė su rezultatais, balais ir stebėjimais iš simuliacijos:

✓ TAIP – Atlikta	⚠ DALINIS – Iš dalies	✗ NE – Neatlikta	Balas 0–5 (5 = pilnai atlikta)

MEST FAZĖ	TIKRINAMAS VEIKSMAS	GRUPĖ (Vaidmuo)	ATLIKTA SIMULIACIJOS METU?	BALAS (0–5)	PASTABOS / STEBĖJIMAS
1 M – MONITOR (Stebėti) | Incidento aptikimas ir klasifikavimas					
MONITOR	Realaus laiko logų / SIEM alertų stebėjimas ir anomalijų aptikimas (CPU, srautas)	SOC / IT	**TAIP**	**4/5** GERAI	*SOC fiksavo CPU 94% ir neįprastą srautą. Alarmų generavimas veikė. Tačiau eskalavimas pavėluotas.*
MONITOR	Incidento klasifikavimas (kritinis / aukštas / vidutinis) ir pirminis žemėlapis	SOC / IT	**DALINIS**	**2/5** SILPNAI	*Klasifikavimas nebuvo formaliai paskelbtas. Informacija nebuvo perduota komandoms struktūruotai.*
MONITOR	DDoS srauto identifikavimas ir šaltinių žemėlapis (Brazilija 1190 r/m, Pakistanas 950 r/m)	SOC / IT	**TAIP**	**4/5** GERAI	*Srautas identifikuotas. Tačiau blokavimo sprendimas nebuvo priimtas laiku.*
MONITOR	Phishing laiškų (CV su virusu) aptikimas ir eskalavimas IT/CISO	CISO	**NE**	**1/5** NEPASIEKTA	*CEO atidarė visus laiškus. CISO buvo informuotas vėlai. Nėra automatinės sandboxing sistemos.*
MONITOR	Pradinis situacijos pranešimas Krizės Orkestriatoriui	Visi	**NE**	**0/5** NEPASIEKTA	*Orkestratorius nebuvo paskirtas – todėl centralizuotas pranešimas niekam nebuvo siunčiamas.*
2 E – EVALUATE (Įvertinti) | Priežasčių analizė ir rizikos vertinimas					
EVALUATE	Šaknies priežasties analizė (RCA) – kas sukėlė incidentą?	CTO / SOC	**NE**	**1/5** NEPASIEKTA	*CTO vietoj RCA iniciatyvos pasakė „laukti 5 min". Priežastis*

MEST FAZĖ	TIKRINAMAS VEIKSMAS	GRUPĖ (Vaidmuo)	ATLIKTA SIMULIACIJOS METU?	BALAS (0–5)	PASTABOS / STEBĖJIMAS
					nebuvo formalizuota.
EVALUATE	SLA pažeidimo rizikos įvertinimas ir laiko žemėlapis	CTO / CEO	**DALINIS**	**2/5** SILPNAI	*Sistema generavo perspėjimą „SLA breached in 6 min". CTO žinojo, bet nesiėmė veiksmų.*
EVALUATE	Finansinės žalos ir klientų poveikio įvertinimas	CEO / AML	**NE**	**0/5** NEPASIEKTA	*Nei CEO, nei AML nevertino finansinės žalos realiu laiku. 2M EUR pavedimas nepastebėtas.*
EVALUATE	Komunikacijos plano parengimas (vidinis + išorinis + reguliatoriai)	CMO / LEGAL	**NE**	**1/5** NEPASIEKTA	*CMO gavo VDAI pranešimą, perdavė LEGAL – toliau nieko. Komunikacijos planas nebuvo sudarytas.*
EVALUATE	KYC/AML duomenų neatitikimų grėsmės vertinimas (suklastoti dokumentai)	AML / COMPLIANCE	**NE**	**0/5** NEPASIEKTA	*AML turėjo duomenis apie klastotes. Niekas nevertino galimos sąsajos su ataka.*
EVALUATE	Atakos vektoriaus (socialinė inžinerija + DDoS + ransomware) identifikavimas	CISO	**DALINIS**	**2/5** SILPNAI	*CISO dirbo su atskirais simptomais, bet nematė viso paveikslo. Holistinė analizė nebuvo atlikta.*
3 S – STABILIZE (Stabilizuoti) | Krizės plitimo sustabdymas					
STABILIZE	Failover aktyvavimas į Kauno DC (DR planas B.2)	CTO	**DALINIS**	**1/5** NEPASIEKTA	*Aktyvuotas 8 min. vėliau nei reikėjo. Sinchronizacija neveikė – failover buvo neefektyvus.*
STABILIZE	Pažeistų tinklo segmentų izoliavimas (network segmentation)	CISO / IT	**DALINIS**	**2/5** SILPNAI	*CISO atjungė darbuotoją, bet tai buvo klaidingas tikslas (atakos maskaradas). Tikri mazgai neizuliuoti.*

MEST FAZĖ	TIKRINAMAS VEIKSMAS	GRUPĖ (Vaidmuo)	ATLIKTA SIMULIACIJOS METU?	BALAS (0–5)	PASTABOS / STEBĖJIMAS
STABILIZE	AML sistemos „krizės režimas" – dideli pervedimai blokuojami automatiškai	AML	NE	0/5 NEPASIEKTA	*AML sistema veikė normaliu režimu krizės metu. 2M EUR pavedimas praleistas.*
STABILIZE	Ransomware plitimo sulaikymas (endpoint izoliavimas)	CISO / IT	NE	0/5 NEPASIEKTA	*Ransomware buvo paleistas netrukdomas. Nė vienas mazgas nebuvo izoliuotas laiku.*
STABILIZE	Krizės valdymo grupės (IVG) aktyvavimas su aiškiu Orkestratoriumi	CEO / CISO	NE	0/5 NEPASIEKTA	*IVG buvo sukurta, bet be Orkestratoriaus. Grupė tik diskutavo – sprendimų nepriėmė.*
STABILIZE	Nuolatinis statuso atnaujinimas vadovybei kas 5 min.	Visi	NE	0/5 NEPASIEKTA	*Komunikacija buvo chaotiška ir fragmentiška. CEO lauké informacijos, kurios negavo.*
4 T – TRANSITION (Perėjimas) | Atkūrimas ir prevencija					
TRANSITION	Pilnas paslaugų atkūrimas (Login, Payments, Internal API)	CTO / IT	NE	0/5 NEPASIEKTA	*Sistema neatkurta. NKSC perėmė valdymą ir pradėjo atkūrimo procesą.*
TRANSITION	Post-Incident Review (PIR) / Postmortem pradžia	Visi	NE	0/5 NEPASIEKTA	*PIR nebuvo inicijuotas pratybų metu. Turėjo būti pradėtas iš karto po stabilizacijos.*
TRANSITION	Pranešimas reguliatorius: NKSC, VDAI (per 72 val. pagal GDPR)	LEGAL / CMO	DALINIS	1/5 NEPASIEKTA	*NKSC buvo informuotas tik tada, kai patys atėjo. VDAI pranešimas nebuvo inicijuotas.*
TRANSITION	Forensic tyrimo ir įrodymų išsaugojimo pradžia	CISO / IT	NE	0/5 NEPASIEKTA	*Įrodymų rinkimas nepradėtas. Sistemos persikrovė – dalies logų prarastas.*

MEST FAZĖ	TIKRINAMAS VEIKSMAS	GRUPĖ (Vaidmuo)	ATLIKTA SIMULIACIJOS METU?	BALAS (0–5)	PASTABOS / STEBĖJIMAS
TRANSITION	Vidinė komunikacija darbuotojams ir klientams	CMO / CEO	**NE**	**0/5** NEPASIEKTA	*Jokios oficialios komunikacijos nebuvo paskelbta nei darbuotojams, nei klientams.*

4. SUVESTINĖ – EFEKTYVUMO REZULTATAI PAGAL MEST FAZĘ

Kiekvienos MEST fazės efektyvumo suvestinė, pagrįsta surinktais balais simuliacijos metu:

MEST FAZĖ	VEIKSMŲ SK.	SURINKTI TAŠKAI	MAKS. TAŠKAI	EFEKTYVUMAS	ĮVERTINIMAS
M – Monitor	4	9/20	20	45%	SILPNAI
E – Evaluate	6	6/30	30	20%	KRITIŠKAI SILPNAI
S – Stabilize	6	3/30	30	10%	KRITIŠKAI SILPNAI
T – Transition	5	1/25	25	4%	KRITIŠKAI SILPNAI
IŠ VISO	21	19/105	105	18%	KRITIŠKAI SILPNAI

GALUTINIS VERDIKTAS: 18% EFEKTYVUMAS – SISTEMINĖ KRIZIŲ VALDYMO NESĖKMĖ

Pagrindinė priežastis – Krizės Orkestratoriaus nebuvimas. Visos MEST fazės buvo vykdomos chaotiškai, be centralizuoto koordinavimo. Stabilize fazė pasiekė tik 10% efektyvumą – tai reiškia, kad krizė nebuvo sulaikyta, o tik stebima.

5. PAGRINDINIAI STEBĖJIMAI IR IŠVADOS

Monitor fazė (45%) – Aptikimas veikė, eskalavimas – ne

- SOC turėjo stebėjimo įrankius ir identifikavo anomalijas – tai buvo teigiama.
- Tačiau informacija nebuvo struktūruotai perduota Orkestriatoriui, nes jo nebuvo.
- Phishing laiškų (CEO) aptikimas nebuvo automatizuotas – žmogiškoji klaida.

Evaluate fazė (20%) – Analizė nebuvo atlikta

- Nė viena grupė neatliko formalios RCA ar rizikos vertinimo.
- AML turėjo KYC neatitikimų duomenis, bet nesusiejo jų su ataka.
- Silo efektas neleido suformuoti viso incidento paveikslo.

Stabilize fazė (10%) – Kritiškai silpna

- Failover aktyvuotas per vėlai, sinchronizacija neveikė.
- AML sistema veikė normaliu režimu – 2M EUR pervedimas praleistas.
- Ransomware plito netrukdomas – endpoint izoliavimas neatliktas.
- IVG be Orkestratoriaus = diskusijų grupė, ne sprendimų centras.

Transition fazė (4%) – Praktiškai neatlikta

- Sistemos neatkurtos – NKSC perėmė iš išorės.
- Forensic tyrimas nepradėtas, įrodymai gali būti prarasti.
- Reguliatoriai (NKSC, VDAI) nebuvo laiku informuoti.