



Countermove

Meridian Commerce

Rapport for katastrofeopretningsøvelse

ØVELSESTYPE

Disaster Recovery

SCENARIO

Ransomware eller wiper

DATO FOR ØVELSEN

1. oktober 2026

FORTROLIGT

Denne rapport beskriver beredskabet hos Meridian Commerce, herunder svagheder konstateret under øvelsen. Den er alene bestemt for modtagerorganisationen og dennes rådgivere og må ikke videregives uden skriftligt samtykke. Opbevares og håndteres i overensstemmelse hermed.

Indhold

Ledelsesresumé	3
Hovedpointer	4
Prioriterede indsatser	4
Beredskabsscorekort	6
Vurdering af planen	8
Sådan bedømmes der	10
Runde for runde	12



Meridian Commerce

Ransomware eller wiper

DATO

1. oktober 2026

ALVORLIGHEDSGRAD

Høj

HVORNÅR DET STARTER

Hverdag, midt om natten

HVOR DET STARTER

Bekræftet, afventer erklæring

DELTAGERE

CTO (DR-leder) · Head of Infrastructure · Lead DBA · CISO · Engineering Manager, Commerce · COO

SAMLET BEREDSKAB	RUNDER GENNEMFØRT	BEREDSKABS NIVEAU
86 %	9	Funktionsdygtig

PLAN OG DOKUMENTATION	HOLDETS UDFØRELSE	FORVENTET EFFEKT
84 %	89 %	85 %

Det samlede beredskab er gennemsnittet af disse tre. Plan og dokumentation bedømmer organisationens skriftlige grundlag, som findes før øvelsen går i gang; holdets udførelse er, hvad deltagerne gjorde med det; forventet effekt er, om det ville have virket i det nødvendige omfang og tempo.

Ledelsesresumé

Meridian Commerce gennemførte en tabletop-øvelse inden for Disaster Recovery den 1. oktober 2026 med seks deltagere — CTO, Head of Infrastructure, Lead DBA, CISO, Engineering Manager for Commerce Platform og COO — og testede organisationens evne til at opdage, aktivere, gendanne og genåbne efter et ransomware-angreb på kritisk produktionsinfrastruktur. Øvelsen viste en organisation, der er operationel og i overvejende grad velforberedt: aktivering og eskalering fulgte planen præcist, recovery-rækkefølgen blev overholdt konsekvent selv under tidspres, og clean-room-valideringen samt den formelle forretningsgodkendelse ved genåbning fungerede plankonformt. Disse styrker er reelle og testede. To områder kræver målrettet opmærksomhed. For det første er den kendte og endnu uafhjulpne overskridelse af genoprettelsestiden for checkout og betalinger — dokumenteret i det åbne punkt DR-114 — et konkret beredskabsgab, der materialiserede sig i øvelsen, og som begrænser organisationens evne til at møde sin vigtigste RTO. For det andet mangler overdragelsen af lovpligtige frister fra DR-sporet til Incident Response-sporet en navngiven ansvarlig og et opfølgningsskridt; i øvelsen løb GDPR-anmeldelsesfristen ud uden at blive fulgt. Samlet placerer øvelsen Meridian Commerce i båndet "operationel" — beredskabet holder under pres, men der er identificerede svagheder, der skal lukkes, inden de udgør en alvorlig risiko.

Hovedpointer

- Aktiverings- og eskaleringsprocessen fungerede efter hensigten: CTO aktiverede DRP kl. 02:42 med et dokumenteret grundlag, der præcist identificerede den truede RTO, og stedfortræderkæden var kendt og klar til at træde i kraft.
- Recovery-rækkefølgen og clean-room-kontrollen er organisationens stærkeste tekniske aktiv — teamet fulgte planens sekvens konsekvent og holdt fast i reglen om, at intet system måtte kobles på produktionsnetværket uden CISO's skriftlige sign-off, selv da presset for at åbne steg.
- Den kendte overskridelse af genoprettelsestiden for checkout og betalinger (DR-114) er ikke et hypotetisk risikopunkt, men en i dag eksisterende begrænsning, der i et reelt angreb vil betyde, at den vigtigste RTO ikke kan holdes.
- Overdragelsen af GDPR-anmeldelsesfristen fra DR-sporet til Incident Response-sporet skete uden en navngiven ansvarlig og uden et check-in-punkt, hvilket medførte, at 72-timersfristen udløb ubesvaret — en strukturel svaghed i grænsefladen mellem de to processer.
- Planen mangler navngivne stedfortrædere for Lead DBA, Engineering Manager og CISO, og øvelsen viste, at de improviserede løsninger, der dækkede disse huller, var personafhængige og ikke kan garanteres at holde i et reelt scenarie.

Prioriterede indsatser

Sorteret efter, hvor meget det haster. Høj markerer noget, der ville få en genopretning til at mislykkes eller en forpligtelse til at blive overskredet; middel en reel svaghed med en midlertidig løsning; lav noget, der bør gøres, når resten er på plads.

HØJ

Afhjælp DR-114 inden 1. december 2026: Head of Infrastructure fremlægger og implementerer en konkret plan for at reducere den målte restore-tid for checkout og betalinger til under 2 timer, verificeret ved en ny fuld restore-test med dokumenteret tidsmåling.

Den målte restore-tid på 3 timer og 15 minutter mod en godkendt RTO på 2 timer materialiserede sig direkte i øvelsen og betød, at den vigtigste RTO ikke kunne overholdes. Gabet er dokumenteret og ejet, men uafhjulpet, og deadline 1. december 2026 er allerede aftalt.

HØJ

Etabler en navngiven ansvarlig og et obligatorisk check-in-punkt for lovpligtige frister (herunder GDPR 72-timersreglen) i det formelle overdragelsestrin, når DR-sporet overdrager til Incident Response-sporet, og indsæt dette som et fast punkt i DR-planens lukningstjekliste.

I øvelsen udløb GDPR 72-timersfristen søndag morgen uden at blive fulgt, fordi overdragelsen skete uden en navngiven fristansvarlig og uden et opfølgningsspunkt — et strukturelt plangab, der nu er dokumenteret og ejet af VP Engineering til revision.

HØJ

Tilføj genaktivering og verifikation af alle backup-job, der er sat på pause under hændelsen, som et obligatorisk og navngivet trin i DR-planens lukningstjekliste, med Head of Infrastructure som ansvarlig og et konkret acceptkriterie (verificeret vellykket kørsel plus test-restore dokumenteret med job-id'er).

I øvelsen viste det sig ved failback, at automatiske AMI-snapshot-job i primærregionen ikke havde kørt i fire dage, fordi ingen ejede ansvaret for at genstarte dem — et reproducerbart gab, der kun blev opdaget tilfældigt og ikke ved en planmæssig kontrol.

MIDDEL

Udpeg navngivne stedfortrædere for Lead DBA, Engineering Manager for Commerce Platform og CISO i DR-planen, og validér at disse stedfortrædere kender restore-procedureerne og sign-off-kriterierne ved den næste planlagte DR-øvelse.

Alle tre roller var under pres i øvelsen uden navngivne stedfortrædere; i særdeleshed manglede Lead DBA en stedfortræder midt om natten, da database-restore er en enkeltpunkts-afhængighed i recovery-sekvensen.

MIDDEL

Udvid Okta-valideringsproceduren i DR-planen med den metode, der blev anvendt i øvelsen — System Log-gennemgang 72 timer tilbage, revoke af alle sessioner, rotation af admin-API-tokens og MFA-nulstilling for admin-konti — og angiv CISO som ejer med Security Engineer som udførende.

Okta-valideringen var i øvelsen en kritisk vej, der blokerede hele recovery-sekvensen; metoden blev improviseret på stedet og er endnu ikke indskrevet i planen, hvilket gør den sårbar over for personafhængighed ved næste hændelse.

LAV

Indfør en fast post-hændelseskontrol i DR-planen, der ved failback tilbage til primærregionen kræver verifikation af Aurora cross-region-replikering til primærregionen og aktiv status bekræftet skriftligt af Lead DBA, inden DR-erklæringen kan lukkes.

I øvelsen var Aurora cross-region-replikering til primærregionen ikke aktiv ved failback — det blev opdaget og rettet, men først fordi Lead DBA gennemgik konsollen aktivt, ikke fordi planen foreskrev det som et lukketrin.

Beredskabsscorekort

	DOK	UDF.	EFFEKT	
Aktivering og eskalering 10% CTO aktiverede DRP kl. 02:42 med et skriftligt grundlag i ticketen, der præcist identificerede den truede RTO og hvorfor normal recovery ikke rakte — planens aktiveringskriterier og stedfortræderkæden var kendte og fulgt fra første runde.	4	4	4	4.0
Roller og stedfortrædere 10% CTO, Head of Infrastructure og CISO ejede og udøvede deres roller konsekvent; VP Engineering trådte ind som stedfortræder for CTO og udkast-ejer på afslutningsdokumentet. Planens kendte huller — Lead DBA, Engineering Manager og CISO har ingen navngivne stedfortrædere — var mærkbare under øvelsen, men improviserede løsninger dækkede dem i praksis.	2	3	3	2.7
Kritiske services, RTO og RPO 15% RTO- og RPO-mål for alle kritiske tjenester var kendte og navngivne fra runde 1; CTO eskalerede straks RPO-overskridelsen på ca. 6 timer til COO, og COO traf en formel forretningsbeslutning. Den kendte og uafhjulpne overskridelse af checkout-RTO (DR-114) materialiserede sig som forventet og begrænsede scores på execution.	4	3	3	3.3
Afhængigheder og gendannelsesrækkefølge 15% Teamet fulgte planens rækkefølge nøjagtigt — netværk og Route 53 først, dernæst Okta og AD Connector, efterfulgt af Aurora og applikationsstakken — og holdt konsekvent fast i reglen om, at intet system måtte kobles på produktionsnetværket før CISO's sign-off, selv under tidspres.	4	4	4	4.0
Backup, gendannelse og dataintegritet 15% Lead DBA valgte det cross-region-replikerede Aurora-snapshot fra eu-west-1 dateret kl. 18:00 onsdag som restore-kilde og bekræftede row counts og fravær af krypteringsartefakter; tvetydige AMI'er blev kasseret og erstattet med onsdagens AMI'er plus kode fra et known commit. Det åbne punkt DR-114 — restore-tid på 3t15m mod en RTO på 2 timer — sænker effectiveness, da gabet ikke var lukket inden øvelsen.	3	4	3	3.3
Identitet, privilegeret adgang og clean room 10% Vault blev sealet og alle tokens revoked ved første tegn på aktiv credential-lækage; root- og break-glass-adgang blev begrænset til to navngivne personer; Okta-valideringen (System Log 72 timer tilbage, rotation af alle admin-API-tokens og MFA-nulstilling) resulterede i CISO's skriftlige sign-off kl. 06:09 — clean-room-kontrollen fungerede efter hensigten.	3	4	4	3.7
Validering og genåbning 10% CISO's skriftlige sign-off kl. 09:05 dækkede alle fire planmæssige forudsætninger; Engineering Manager gennemførte smoke test med Stripe test-mode og en reel ordre; COO traf go/no-go kl. 09:20 på dokumenterede kriterier — genåbningen fulgte planens krav præcist og uden uresolverede punkter.	4	4	4	4.0

	DOK	UDF.	EFFEKT	
Interessentkommunikation 5%	3	3	3	3.0
Teamet skiftede plankonformt til Signal-gruppen "Meridian DR Bridge" fra runde 1, COO koordinerede vedligeholdelsesside og kundeservice fra runde 4, og CTO briefede COO løbende. Kundekommunikationen om datatabet blev udskudt og kom i fare for at misse den GDPR-deadline, den var koblet til.				
Leverandørberedskab 5%	3	3	3	3.0
Teamet kendte og navngav eskaleringsvejen til AWS Enterprise Support (Severity 1-case), Stripe-statussiden og break-glass-adgangen til kommunikationsinfrastrukturen; ingen af leverandørerne gav anledning til problemer, og planens kontaktstruktur synes kendt, men blev ikke aktivt afprøvet under pres.				
Dokumentation og regulatorisk overholdelse 5%	2	2	2	2.0
Alle beslutninger og tidspunkter blev løbende logget i incident-ticketen, og afslutningsdokumentets struktur og ejerskab blev fastlagt. GDPR 72-timersfristen løb fra torsdag kl. 02:17, udløb søndag morgen og blev ikke overholdt, fordi overdragelsen fra DR-sporet til Incident Response-sporet skete uden en navngiven fristansvarlig og uden et opfølgningsskridt.				

Dok = Dokumentation Udf. = Udførsel Effekt, hver 0-4. Se "Sådan bedømmes der" senere i rapporten.

Vurdering af planen

Øvelsen er vurderet op mod organisationens egen katastrofeberedskabsplan, som blev stillet til rådighed på forhånd. De to afsnit nedenfor er to selvstændige vurderinger: det første af planen som dokument, det andet af hvor tæt deltagerne arbejdede efter den under øvelsen.

Planen som dokument

GODT DÆKKET

- Aktiveringsstrukturen er præcis og handlingsbar: kriterier, aktiveringskompetence og en trestrengt stedfortræderkæde (CTO -> VP Engineering -> Head of Infrastructure) er entydigt defineret.
- RTO- og RPO-mål for alle kritiske tjenester er eksplicit angivet og forretningsgodkendt, hvilket gjorde det muligt for teamet at referere til dem direkte under øvelsen.
- Recovery-rækkefølgen er konkret og navngiver de systemer, der skal genetableres, og de afhængigheder, der styrer rækkefølgen — herunder Stripe som ekstern afhængighed uden intern recovery-handling.
- Backup-strategien er detaljeret: Aurora continuous backup med seks-timers snapshots og cross-region-replikering til eu-west-1, immutable AMI-snapshots via AWS Backup og Elasticsearch-snapshots til S3, alle med definerede opbevaringsperioder.
- Secure recovery-kravene er klart opstillet med tre forudsætninger (EDR-sweep, credential-rotation og bekræftet restore-kilde), og CISO er entydigt angivet som sign-off-ansvarlig.
- Fallback-kommunikationsstrukturen — Signal-gruppen "Meridian DR Bridge", break-glass-konferencebroen og credentials i Facilities-safen — er defineret og forudsætter ikke, at Okta eller Google Workspace er tilgængeligt.

HULLER I PLANEN

- Lead DBA, Engineering Manager for Commerce Platform og CISO har ingen navngivne stedfortrædere; for DBA og CISO er disse kritiske enkeltpunkts-afhængigheder i recovery-sekvensen.
- Det kendte og dokumenterede gab i DR-114 — at den seneste målte restore-tid for checkout og betalinger overstiger den godkendte RTO — fremgår af planen, men der er ingen betinget procedure for, hvad teamet skal gøre, hvis restore-tiden forventes at overskride RTO under en reel hændelse.
- Planen indeholder ingen procedure for validering af Okta-tenantens integritet som del af recovery-sekvensens identitetstrin; metoden til at afgøre, om identity-laget er kompromitteret, er ikke beskrevet.
- Planen beskriver ingen tjekliste for lukning af DR-erklæringen, herunder verifikation af, at alle backup-job, der er sat på pause under hændelsen, er genaktiveret og verificeret kørende.
- Grænsefladen mellem DR-sporet og Incident Response-sporet ved overdragelse af lovpligtige frister er ikke beskrevet — planen definerer ikke, hvem der ejer GDPR-anmeldelsesfristen, når den opstår under en DR-situation, og hvornår og til hvem ansvaret overdrages.

Hvor godt deltagerne fulgte den

STÆRK

Teamet arbejdede fra planen gennem hele øvelsen: recovery-rækkefølgen, secure recovery-kravene, kommunikationsfallback og go/no-go-strukturen for genåbning fulgte alle planens bestemmelser. Det mest konsekvensfulde sted, planen formede teamets adfærd, var beslutningen om at holde fast i "intet kobles på produktionsnetværket før CISO sign-off" selv under stigende tidspres i runde 3-4 — en beslutning, der direkte modsvarer planens secure recovery-krav. Den eneste divergens af betydning var, at AMI-valideringsproceduren og Okta-gennemgangsmetoden måtte improviseres, fordi planen ikke beskriver dem — men improviseringen var i begge tilfælde i planens ånd, ikke imod den.

FULGT

- DRP-aktivering fulgte planens kriterier og stedfortræderkæde præcist, med CTO som aktiverende myndighed og et dokumenteret grundlag.
- Recovery-rækkefølgen — netværk og Route 53, dernæst Okta og AD Connector, Aurora, checkout og betalinger — blev overholdt konsekvent.
- Planens fallback-kommunikationsstruktur (Signal-gruppen "Meridian DR Bridge") blev aktiveret fra runde 1, da Okta's integritet var ukendt.
- CISO's sign-off-forudsætninger (EDR-sweep, restore-kildebekræftelse, credential-rotation, ingen aktive forhændelses-sessioner) blev alle opfyldt og dokumenteret inden produktionskobling.
- COO traf go/no-go-beslutningen for kundevendt genåbning på dokumenterede kriterier, i overensstemmelse med planens rollefordeling.
- CTO eskalerede RPO-overskridelsen til COO som planmæssigt krævet.

AFVEGET FRA

- Okta-valideringsproceduren (System Log-gennemgang, token-rotation, MFA-nulstilling) blev improviseret på stedet, da planen ikke beskriver denne metode — improviseringen var forsvarlig, men er endnu ikke indskrevet i planen.
- Verifikation af AMI-proveniensen måtte løses ad hoc ved kassering af tvetydige snapshots og rekonstruktion fra onsdagens AMI'er plus Git-commit, fordi planen ikke specificerer en procedure for proveniensvalidering af AMI-restore-kilder.
- Lukningstjeklisten for DR-erklæringen — herunder genaktivering af backup-job og verifikation af cross-region-replikering — var ikke planmæssigt defineret og måtte konstrueres løbende i runde 6-8.

Sådan bedømmes der

Ti områder vurderes. Hvert område bedømmes på tre selvstændige akser, og områdets score er gennemsnittet af dem. Områderne vægtes forskelligt, og den vægtede sum giver den samlede beredskabsprocent på forsiden.

De tre akser

Dokumentation	Om der findes et skriftligt, godkendt og findbart grundlag — en plan, runbook eller procedure, som holdet reelt kunne henvise til under øvelsen.
Udførsel	Om holdet rent faktisk gennemførte området: beslutninger truffet, ejere udpeget, den definerede rækkefølge fulgt.
Effekt	Om det, de gjorde, ville have virket i praksis — i det omfang og med den hastighed, hændelsen krævede.

Skalaen 0-4

0 — Ikke etableret	Ingen kendt løsning, dokumentation eller ejer.
1 — Ad hoc	En fremgangsmåde findes, men den er personafhængig, udokumenteret eller ikke godkendt.
2 — Delvist etableret	En proces findes, men den er ufuldstændig, forældet, utestet eller uklart forankret.
3 — Etableret	Dokumenteret, kendt og anvendelig, med mindre huller.
4 — Valideret	Etableret og overbevisende demonstreret under øvelsen — det dokumenterede grundlag var kendt, ejeren udpeget, og det blev anvendt korrekt uden væsentlige huller.

Vægtning

Vægtene afspejler, hvor meget hvert område afgør, om en gendannelse overhovedet lykkes. Gendannelse af data og rækkefølgen af afhængigheder vægter tungere end interessentkommunikation — ikke fordi kommunikation er uvæsentlig, men fordi en fejl der kan rettes op, mens en fejl i de første ikke kan. Det samlede beredskab er den vægtede sum udtrykt som en procentdel af den maksimalt mulige score.

Beredskabsniveauer

Kritisk utilstrækkelig (0-39 %)	En gendannelse ville ikke lykkes. Grundlæggende kapaciteter mangler snarere end at være svage.
Væsentlige mangler (40-59 %)	En gendannelse ville sandsynligvis mislykkes eller overskride tidsrammerne markant. Flere kerneområder skal opbygges, ikke justeres.
Delvist funktionsdygtig (60-74 %)	En gendannelse ville formentlig lykkes for nogle tjenester, men ikke inden for de tider, forretningen forventer.
Funktionsdygtig (75-89 %)	En gendannelse er troværdig og vil sandsynligvis lykkes, med identificerede huller, der bør lukkes.
Robust og valideret (90-100 %)	Gendannelsen er dokumenteret, øvet og dokumenterbar. Det resterende arbejde er finjustering.

Kritiske stopkriterier

Syv forhold betragtes som diskvalificerende uanset den vægtede score. Blev ét af dem observeret under øvelsen, kan

beredskabsniveauet ikke overstige Væsentlige mangler — et højt gennemsnit kan ikke kompensere for, at et af disse mangler.

Hvad hvert område dækker

Aktivering og eskalering (10%)	Hvem der kan erklære en katastrofe og på hvilket grundlag, hvordan beslutningen eskaleres, og hvor hurtigt planen reelt aktiveres, når kriteriet er opfyldt.
Roller og stedfortrædere (10%)	Om de roller, planen bygger på, er bemandet og forstået, og om navngivne stedfortrædere kan handle, når den primære person ikke kan nås.
Kritiske services, RTO og RPO (15%)	Om de forretningskritiske tjenester er identificeret og prioriteret, med RTO- og RPO-mål, som forretningssiden faktisk har godkendt.
Afhængigheder og gendannelsesrækkefølge (15%)	Om rækkefølgen for gendannelse afspejler reelle tekniske afhængigheder — identitet og netværk før applikationer — frem for at gendanne det, der råber højest.
Backup, gendannelse og dataintegritet (15%)	Om backups findes, fortsat kan tilgås når primærmiljøet ikke kan, og kan gendannes til et kendt godt punkt inden for den nødvendige tid.
Identitet, privilegeret adgang og clean room (10%)	Om identitetstjenester og privilegeret adgang kan reetableres uafhængigt af det kompromitterede miljø, herunder et clean room hvor det er nødvendigt.
Validering og genåbning (10%)	Om gendannede systemer verificeres, før de gives tilbage til brugerne, og om system- og forretningsejere formelt godkender genåbning.
Interessentkommunikation (5%)	Om medarbejdere, kunder, leverandører og ledelse holdes orienteret i en fastlagt kadence gennem kanaler, der overlever selve nedbruddet.
Leverandørberedskab (5%)	Om kritiske leverandører kan nås i henhold til kontrakt, kender deres forpligtelser under en katastrofe og kan eskaleres til uden for normal arbejdstid.
Dokumentation og regulatorisk overholdelse (5%)	Om beslutninger, tidsstempler og evidens registreres undervejs, og om anmeldelsespligter identificeres og overholdes inden for deres frister.

Runde for runde

Fase 1 af 5 · Erklæring & aktivering Torsdag, Dag 1, 02:17

Ransomware opdaget på produktionsservere om natten

SITUATION

Klokken 02:17 natten til torsdag udløser CrowdStrike EDR en kritisk alert på tre produktionsservere i Meridian Commerces AWS-miljø. Security Engineer på vagt bekræfter via PagerDuty-varslingen, at ransomware aktivt krypterer filer på applikationsserverne bag checkout- og betalingsflowet samt på den selvhostede tre-node Elasticsearch-klynge, der driver produktkataloget. Krypteringsprocesserne er stadig aktive. Der er endnu ikke isoleret nogen systemer, og der er ikke foretaget nogen eskalering ud over Security Engineers egen observation.

En indledende gennemgang af EDR-telemetri viser, at de første indikatorer på kompromittering stammer fra ca. 23:45 onsdag aften — altså ca. 2,5 timer inden opdagelsen. I det tidsvindue har der været unormal lateral bevægelse fra en administrativ IAM-session mod Aurora PostgreSQL-klyngen samt Elasticsearch-noderne. Det kan endnu ikke afklares, om selve Aurora-databasen er påvirket af kryptering, men adgangsmønstrene giver alvorlig bekymring. HashiCorp Vault viser ingen fejl, men der er ikke foretaget en verificering af, om credentials er eksfiltreret.

Det er midt om natten. Kontoret er tomt. Meridian Commerce har ingen formel on-call-rota og ingen defineret beslutningskompetence uden for arbejdstid. Security Engineeren har ansvaret for den tekniske observationsrolle via PagerDuty, men har ikke mandat til at iværksætte isolation, DRP-aktivering eller supplier-eskalering. For at nå frem til en beslutning om, hvorvidt dette udgør grundlag for DRP-aktivering, skal relevante ledere kontaktes på personlige telefoner — uden garanti for, at de svarer.

Checkout og betalinger har en RTO på 2 timer og en RPO på 10 minutter. Den senest målte gendannelsestid fra DR-restore-testen i november 2025 var 3 timer og 15 minutter — 1 time og 15 minutter over den godkendte RTO. Dette er dokumenteret i det åbne afhjælpningspunkt DR-114, som endnu ikke er lukket. Med angriberens foothold dateret til 23:45, og kryptering stadig aktiv, er det RTO-vindue for checkout og betalinger allerede under pres, selv før en eventuel katastrofeerklæring er truffet.

HANDLINGER FORETAGET

- Security Engineer isolerer straks de tre berørte servere og de tre Elasticsearch-noder via CrowdStrike network containment. CISO er nået og godkender mundtligt kl. 02:26 — handlingen logges i incident-ticketen med tidspunkt og godkender. CISO erklærer formel hændelse (SEV1) kl. 02:31 og overtager rollen som Incident Commander, indtil ugens IC er vækket.
- CTO er på opkaldet fra 02:35. Vurdering: krypteringen er aktiv, og den målte restore-tid for checkout og betalinger (3t15m, DR-114) ligger over RTO på 2 timer, så normal recovery kan ikke nå RTO. CTO aktiverer DRP kl. 02:42 med et skriftligt grundlag i ticketen: hvilken RTO der er i fare, og hvorfor normal recovery ikke rækker.
- Lead DBA behandler Aurora som kompromitteret: ingen skrivinger, manuelt snapshot

til evidens, og vi udpeger seneste snapshot før 23:45 som kandidat-restorepunkt. Vi samles på Signal-gruppen "Meridian DR Bridge" i stedet for Slack, fordi vi ikke ved, om Okta er kompromitteret.

EVALUERING

DET, DER VIRKEDE

Teamet handlede præcist og hurtigt: isolation af de berørte servere og Elasticsearch-noder via EDR network containment, en mundtlig godkendelse fra CISO logget med tidspunkt og godkender, og en formel DRP-aktivering fra CTO kl. 02:42 med et dokumenteret grundlag — den kendte restore-tid fra DR-114 mod en truet 2-timers RTO. Skiftet til Signal-gruppen "Meridian DR Bridge" som kommunikationskanal, fordi Okta's integritet er ukendt, er et rigtigt og plankonformt valg.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed er at Aurora-databasens tilstand er erklæret "kompromitteret" og et evidens-snapshot er taget, men der er endnu ingen bekræftelse af, at snapshottet faktisk er gennemført og verificeret ukrypteret — og Lead DBA har ingen navngiven stedfortræder i planen, hvilket er et reelt eksponeringsrisiko midt om natten. Herudover er HashiCorp Vault og IAM-credentials ikke aktivt suspenderet eller roteret endnu, selvom den laterale bevægelse stammer fra en administrativ IAM-session: disse credentials er potentielt stadig aktive og angriber-kontrollerede.

FREMADRETTET

Ind i næste fase er det kritiske spørgsmål, om miljøet faktisk kan stabiliseres og erklæres angriber-frit, inden nogen gendannelse påbegyndes — særligt med en ukendt Vault-status og aktive credentials, der endnu ikke er roteret.

Fase 2 af 5 · Inddæmning & stabilisering Torsdag, Dag 1, 03:08

Vault-adgang registrerer aktivitet under isolation

SITUATION

Mens teamet koordinerer på DR Bridge, registrerer HashiCorp Vault's audit-log et vellykket opslag på et administrativt database-credential kl. 02:58 — altså 16 minutter efter DRP-aktiveringen og efter de berørte servere er isoleret. IP-adressen bag opslaget tilhører ikke nogen af de isolerede noder, og den matcher ikke kendte administrative arbejdsstationer. Simultaneously bekræfter Lead DBA, at evidens-snapshottet af Aurora er gennemført, men den automatiske integritetsvalidering er ikke kørt, så det er uafklaret, om snapshottet er taget af et allerede delvist krypteret volumen. Teamet står nu med to samtidige uafklarede spørgsmål: en credential-lækage der tilsyneladende stadig er aktiv, og et restore-punkt hvis renhed ikke er bekræftet.

HANDLINGER
FORETAGET

- IC (CISO) beslutter kl. 03:12 at seale Vault og revoke alle aktive tokens — vi accepterer, at det forsinker gendannelsen, fordi en aktiv credential-lækage gør enhver restore usikker. Head of Infrastructure blokerer den ukendte IP i security groups og NACL, og alle aktive IAM-sessioner for administrative roller revokes. Root- og break-glass-adgang flyttes til to navngivne personer.
- CISO starter en EDR-sweep af hele miljøet for at finde den node, der foretog opslaget; indtil den er fundet, betragter vi hele primærregionen som utroværdig.

- Lead DBA kører integritetsvalideringen på evidens-snapshottet, men vi planlægger ikke restore på det. Restore-kilden bliver i stedet det cross-region-replikerede Aurora-snapshot i eu-west-1 fra kl. 18:00 onsdag — før det tidligste kompromitteringsindikator kl. 23:45. Det giver et datatab på ca. 6 timer, som vi bevidst accepterer frem for at risikere at gendanne angriberens fodfæste. CTO noterer, at det overskrider RPO på 15 minutter, og at det skal forelægges COO.

EVALUERING

DET, DER VIRKEDE

Teamet reagerede hurtigt og resolut på Vault-aktiviteten: en begrundet beslutning om at seale Vault og revoke alle aktive tokens, blokering af den ukendte IP i security groups og NACL, og en klar to-persons-model for root- og break-glass-adgang. Valget af det cross-region-replikerede Aurora-snapshot fra eu-west-1 som restore-kilde — frem for et snapshot med ukendt integritet — er plankonformt og sikkerhedsmæssigt forsvarligt, og CTO's eskalering af RPO-overskridelsen til COO er korrekt.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed er, at Okta SSO's tilstand stadig er uafklaret: hvis den administrative IAM-session, der drev den laterale bevægelse, var autentificeret via Okta, er det muligt, at angriberens persistence-punkt ligger der — og en EDR-sweep af EC2-noder finder ikke en kompromitteret identity-tjeneste. Teamet har ikke beskrevet, hvem der ejer Okta-validering, eller hvordan den afklares, inden identity-laget genanvendes i gendannelsessekvensen, som ifølge planen kræver Okta som andet trin.

FREMADRETTET

Ind i næste fase er det centrale spørgsmål, om miljøet kan erklæres tilstrækkeligt stabilt og angriber-frit til, at gendannelse kan påbegyndes — CISO's sign-off på fravær af persistence er en planmæssig forudsætning, og Okta-afklaringen er den manglende brik, der kan blokere hele recovery-sekvensen.

Fase 3 af 5 · Genopretning & reetablering Torsdag, Dag 1, 04:41

EDR-sweep afslutter — Okta-status blokerer recovery

SITUATION

EDR-sweepen af primærregionen er nu afsluttet og finder ingen yderligere aktive krypteringsprocesser på EC2-noderne — men rapporten indeholder en markering: CrowdStrike kan ikke give clean-bill-of-health på identity-laget, fordi Okta-tenanten og AD Connector faller uden for EDR-dækningen. CISO kan dermed endnu ikke udstede den planmæssige sikkerhedsgodkendelse, der er en forudsætning for at genoprette systemerne, da det ikke kan udelukkes, at angriberen har plantet persistence i identity-laget. Recovery-sekvensen ifølge planen kræver, at Networking og DNS genetableres først og dernæst Okta og AD Connector — og det punkt er nu det direkte blokeringspunkt for alle efterfølgende skridt, herunder Aurora-restore og Checkout og betalinger.

HANDLINGER
FORETAGET

- CISO ejer Okta-valideringen og uddelegerer udførelsen til den vagthavende Security Engineer. Metode: gennemgang af Okta System Log 72 timer tilbage for admin-ændringer, nye API-tokens, ændrede MFA-faktorer og nye IdP-regler. Alle Okta-

sessioner revokes, alle admin-API-tokens roteres, og MFA nulstilles for de 11 admin-konti. Mål: sign-off eller afvisning senest kl. 06:00.

- Vi kører parallelt, men uden at bryde planens rækkefølge for reconnect: Head of Infrastructure genetablerer netværk og Route 53 i eu-west-1, og Lead DBA starter Aurora-restore fra snapshotet kl. 18:00 ind i en isoleret VPC. Intet gendannet system kobles på produktionsnetværket, før CISO har givet sign-off.
- Fallback: viser Okta tegn på kompromittering, kører vi gendannelsen alene på de to break-glass-konti, og CTO træffer den beslutning. Engineering Manager forbereder checkout-stakken, så den kan deployes, så snart databasen er klar.

EVALUERING

DET, DER VIRKEDE

Teamet leverer et solidt og struktureret svar på blokeringsproblemet: CISO ejer Okta-valideringen med en klar metode (System Log-gennemgang 72 timer tilbage, revoke af alle sessioner, rotation af admin-API-tokens og MFA-nulstilling for 11 admin-konti) og en konkret deadline kl. 06:00. Det parallelle spor — netværk og Route 53 i eu-west-1 samt Aurora-restore til isoleret VPC — er plankonformt og viser, at teamet forstår, at "intet kobles på produktionsnetværket før CISO sign-off" er den afgørende kontrol.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed er, at Aurora-restore beskrives som igangsat fra snapshotet kl. 18:00 onsdag, men der er ikke angivet en navngiven ejer for at verificere, at restore-kilden faktisk predaterer det tidligste kendte kompromitteringsindikator kl. 23:45 — det er Lead DBA's ansvar ifølge planen, og DBA har ingen navngiven stedfortræder. Derudover er det uafklaret, om Engineering Manager's forberedelse af checkout-stakken sker fra immutable AMI-snapshots taget før 23:45, eller om der benyttes images af ukendt proveniens, hvilket er en direkte forudsætning ifølge planens secure recovery-krav.

FREMADRETTET

Ind i næste fase — validering og forretningsgenoptagelse — er de to kritiske spørgsmål: hvornår CISO's Okta sign-off foreligger (og hvad fallback-beslutningen konkret indebærer for recovery-sekvensen), og om samtlige restore-kilder er bekræftet rene og dateret før kompromitteringstidspunktet, inden noget system kobles på produktionsnetværket.

Fase 4 af 5 · Validering & genoptagelse Torsdag, Dag 1, 06:14

Okta sign-off klar — AMI-provenienschek blokerer deploy

SITUATION

Klokken 06:02 afleverer Security Engineer Okta-rapporten til CISO: ingen tegn på kompromittering i identity-laget — ingen nye IdP-regler, ingen ukendte admin-API-tokens, ingen ændrede MFA-faktorer i 72-timersvinduet. CISO udsteder kl. 06:09 den planmæssige sikkerhedsgodkendelse for identity-laget og giver grønt lys til at koble netværk og Aurora-restore på produktionsnetværket i eu-west-1. Men i samme øjeblik melder Engineering Manager, at de AMI-snapshots, der skal danne grundlag for checkout- og betalingsstakken, ikke er entydigt datostemplede i AWS Backup-konsollen: tre af de ni relevante AMI'er viser en "created"-timestamp efter kl. 23:45 onsdag, og det er uklart, om de er taget automatisk af det planlagte nattejob eller er et artefakt fra angriberens aktivitet i det tidsrum. Ingen af de tre AMI'er kan bruges, før proveniens er bekræftet —

og checkout og betalinger kan ikke deployes på de resterende seks alene.

HANDLINGER FORETAGET

- De tre tvetydige AMI'er kasseres — vi bruger ikke tid på at bevise, at de er rene. Engineering Manager henter i stedet AMI'erne fra natten til onsdag for de tre servere (AWS Backup beholder 14 dage) og deployer den seneste applikationskode oven på dem fra vores Git-repo via CI/CD, så vi ikke er afhængige af noget, der er bygget efter 23:45. CISO godkender, at kilden er fra før kompromitteringen, og at koden er bygget fra et kendt commit. Beslutningen logges i ticketen.
- CTO briefer COO kl. 06:30: checkout og betalinger forventes tilbage ca. 09:30 — altså en overskridelse af RTO på 2 timer, som vi kendte fra DR-114 — og ca. 6 timers ordredatat fra onsdag aften er tabt. COO beslutter, at webshoppen viser en vedligeholdelsesside indtil da, og at kundeservice åbner kl. 08 med et fælles svar.

EVALUERING

DET, DER VIRKEDE

Teamet træffer en klar og velbegrundet beslutning om at kassere de tre tvetydige AMI'er frem for at forsøge at validere dem — det er plankonformt og fjerner en reel persistence-risiko. Brugen af onsdag-nattes AMI'er kombineret med genopbygning af applikationskoden fra et kendt commit i Git-repo'et er en forsvarlig og dokumenteret metode, og CISO's eksplicitte godkendelse af restore-kilden og commit-proveniens er netop den sign-off, planens secure recovery-krav foreskriver.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed i dette trin er, at Aurora-restoren til isoleret VPC har kørt siden trin 3, men der er endnu ingen bekræftelse af, at databasen er valideret ren og data-integriteten kontrolleret, inden den kobles på produktionsnetværket — Lead DBA ejer det ansvar, men en konkret verifikationsprocedure og forventet tidspunkt er ikke nævnt. COO's vedligeholdelsesside og kundeservice-beslutning er rigtig, men den forudsætter, at 09:30-estimatet holder, og det estimat er ikke underbygget af en opdateret tidslinje fra Head of Infrastructure og Lead DBA.

FREMADRETTET

Ind i den afsluttende fase er de kritiske spørgsmål: hvornår Aurora-integritetsvalideringen er afsluttet og godkendt af Lead DBA, om CrowdStrike EDR bekræfter de gendannede systemer som rene inden produktionskobling, og om COO har den forretningsgodkendelse, der svarer til planens go/no-go-beslutning for genåbning af kundevendte tjenester.

Fase 5 af 5 · Normal drift Torsdag, Dag 1, 08:55

Aurora-restore valideret — genåbning kræver formel go/no-go

SITUATION

Klokken 08:47 melder Lead DBA, at Aurora-restoren i den isolerede VPC er gennemført og integritetsvalideringen bestået: row counts stemmer på tværs af kritiske tabeller, ingen krypteringsartefakter er fundet, og restore-kilden er bekræftet dateret til kl. 18:00 onsdag — forud for det tidligste kendte kompromitteringsindikator. CrowdStrike EDR-sweepen af de gendannede applikationsservere og databasenoden er ligeledes afsluttet uden fund. Teamet er teknisk set klar til at koble checkout- og betalingsstakken på

produktionsnetværket i eu-west-1 — men ingen af de formelle lukkeprocedurer er endnu gennemført: CISO's endelige sign-off på hele det gendannede miljø foreligger ikke skriftligt, COO har ikke truffet den formelle go/no-go-beslutning for kundevedt genåbning, og vedligeholdelsessiden er stadig aktiv. Kundeservice har siden kl. 08:00 håndteret indgående henvendelser med det aftalte fællessvar, og presset for at åbne stiger.

HANDLINGER FORETAGET

- CISO udsteder skriftligt sign-off kl. 09:05, der dækker: EDR-sweep uden fund på alle gendannede systemer, restore-kilder dateret før 23:45, alle administrative credentials roteret (Vault er re-keyed, IAM- og Okta-admin-credentials er nye) og ingen aktive sessioner fra før hændelsen.
- Engineering Manager kører en smoke test af hele checkout-flowet med en testordre via Stripe i test-mode og derefter én rigtig ordre på et internt kort. Begge lykkes.
- COO træffer go/no-go kl. 09:20 på disse kriterier: CISO-sign-off foreligger, smoke testen er bestået, og kundeservice er klar. Beslutning: go. Webshoppen åbnes kl. 09:30, og vedligeholdelsessiden fjernes. Planens skærpede overvågning i 72 timer starter med et dagligt standup kl. 09:00.
- Kommunikation om datatabet på ca. 6 timers ordrer tager vi i morgen, når vi har overblik over præcis hvilke ordrer der er ramt.

EVALUERING

DET, DER VIRKEDE

Teamet lukker valideringsfasen korrekt og plankonformt: CISO's skriftlige sign-off kl. 09:05 dækker alle planens fire forudsætninger — EDR-sweep uden fund, bekræftede restore-kilder, roterede credentials og ingen aktive forhændelses-sessioner. COO's go/no-go kl. 09:20 på dokumenterede kriterier og Engineering Manager's smoke test med både Stripe test-mode og en reel ordre er præcis den forretningsgodkendelse og tekniske validering, planen kræver inden kundevedt genåbning.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed, der nu trænger sig på, er kommunikationen om datatabet: teamet udskyder den til "i morgen", men ca. 6 timers ordredata er tabt, og berørte kunder samt potentielt GDPR- og PCI-DSS-relaterede myndigheder kan have krav, der ikke venter til næste dag — det er Incident Response-sporet ved siden af DR, og det er uafklaret, hvem der ejer det, og om der er en deadline, der løber. Derudover er det åbne punkt DR-114 (den målte restore-tid på 3t15m over RTO) endnu ikke formelt lukket eller eskaleret med en ny ejers deadline, selvom øvelsen har eksponeret netop det problem i praksis.

FREMADRETTET

Ind i den formelle afslutning af DR-situationen mangler teamet at adressere to ting: en plan for at migrere væk fra midlertidige recovery-arrangementer og genskabe normal redundans, backup-rutiner og overvågning i primærregionen — og en formel lukning af DR-erklæringen med dokumenteret tidspunkt, ejer og status på alle åbne punkter, herunder DR-114 og koordinering med Incident Response-sporet.

Fase 5 af 5 · Normal drift Torsdag, Dag 1, 14:35

Migration til primærregion afslører manglende redundans

SITUATION

Head of Infrastructure fremlægger en statusoversigt for migrationen tilbage til primærregionen: netværk og Route 53 kan failback inden for to timer, men den selvhostede tre-node Elasticsearch-klynge er stadig isoleret og uklar i sin tilstand — ingen af de tre noder er godkendt til genopbygning, og der er ikke taget stilling til, om de skal genopbygges fra nattens S3-snapshot eller fra scratch med ny AMI. Samtidig rapporterer Lead DBA, at de løbende Aurora-snapshots og cross-region-replikering til eu-west-1 fortsat er konfigureret med eu-west-1 som primær — replikering tilbage mod primærregionen er aldrig blevet initieret, så RPO-beskyttelsen i primærregionen er i øjeblikket ikke aktiv. Den skærpede 72-timers overvågning kører, men ingen har formelt dokumenteret, hvornår normale backup-rutiner og redundans er genoprettet — og DR-erklæringen er endnu ikke lukket.

HANDLINGER FORETAGET

- Vi bliver i eu-west-1 under de 72 timers skærpede overvågning. Failback til primærregionen planlægges til mandag i et aftalt servicevindue; Head of Infrastructure ejer planen, og CTO erklærer primærregionen klar, når CISO har godkendt den.
- Lead DBA starter i dag replikering fra eu-west-1 tilbage til primærregionen, så RPO-beskyttelsen er aktiv igen inden kl. 18. Elasticsearch genopbygges fra en ren AMI og genindekseres fra Aurora, som er kilden til produktkataloget — vi bruger ikke nattens S3-snapshot, fordi vi ikke kan bekræfte, at det er taget før 23:45.
- CTO lukker DR-erklæringen, når tre kriterier er opfyldt: failback gennemført, RPO-beskyttelse aktiv i begge regioner, og backup-jobs verificeret kørende. DR-114 får en ny deadline: Head of Infrastructure fremlægger en plan for at nå under 2 timers restore-tid inden 1. december.
- Kundekommunikationen om datatabet overdrages til Incident Response-sporet: CISO som IC ejer den sammen med Legal, inklusive vurderingen af GDPR-anmeldelse inden for 72 timer.

EVALUERING

DET, DER VIRKEDE

Teamet leverer en klar og struktureret tilbagevendsplan: Head of Infrastructure ejer failback-planen til mandag i et aftalt servicevindue, Lead DBA genetablerer Aurora-replikering til primærregionen inden kl. 18 i dag, og Elasticsearch genopbygges fra ren AMI med Aurora som indekserings-kilde — en forsvarlig beslutning, der undgår S3-snapshottet af ukendt proveniensalder. CTO's tre lukkekriterierne for DR-erklæringen er konkrete og ejede, og overdragelsen af kundekommunikation og GDPR-vurdering til Incident Response-sporet under CISO og Legal er korrekt.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed er, at DR-erklæringen ikke lukkes, før failback er gennemført mandag — men det er tre dage frem, og der er ingen dokumenteret beskrivelse af, hvem der kører det formelle lukkedokument, hvad det skal indeholde, og hvem der modtager det. En DR-lukning er ikke blot en teknisk konstatering fra CTO: planen forudsætter, at alle åbne punkter, herunder DR-114's nye deadline og koordineringen med Incident Response-sporet, er dokumenteret i et afslutningsdokument med tidspunkt, ejer og status — det er endnu ikke beskrevet.

FREMADRETTET

Teamet er tæt på en formel afslutning: beskriv konkret, hvem der udarbejder og godkender DR-afslutningsdokumentet, hvad det minimum skal indeholde, og hvordan det distribueres — det er den sidste brik, der mangler, inden DR-situationen kan erklæres formelt lukket.

Fase 5 af 5 · Normal drift Torsdag, Dag 1, 16:50

DR-afslutningsdokument skal udarbejdes og godkendes

SITUATION

Head of Infrastructure melder kl. 16:42, at Aurora-replikeringen fra eu-west-1 tilbage til primærregionen er verificeret aktiv, og at Elasticsearch-genopbygningen fra ren AMI er igangsat og forventes færdig inden midnat. Dermed er ét af CTO's tre lukkekriterierne for DR-erklæringen opfyldt — men CTO efterspørger nu det konkrete afslutningsdokument, og det er uklart, hvem der faktisk skriver det, hvad det minimum skal indeholde, og hvem der skal modtage og godkende det, inden DR-situationen formelt kan erklæres lukket. CISO påpeger desuden, at en status på Incident Response-sporet — herunder om GDPR-anmeldelsesfristen på 72 timer er adresseret — skal fremgå af dokumentet, før hun kan sætte sin underskrift på det.

HANDLINGER
FORETAGET

- CTO ejer DR-afslutningsdokumentet; VP Engineering skriver udkastet. Det skal være klar til godkendelse tirsdag kl. 12, dagen efter failback.
- Indhold som minimum: tidslinje med alle beslutninger og tidspunkter fra ticketen, restore-kilder og deres datering, status på de tre lukkekriterier, åbne punkter med ejer og deadline (DR-114, Elasticsearch-genopbygningen og failback), datatabet på ca. 6 timer samt et afsnit om Incident Response-sporet.
- CISO og Legal leverer afsnittet om Incident Response-sporet: om GDPR-vurderingen er foretaget, om der er anmeldt, og hvornår kunderne er informeret. CTO og CISO godkender og underskriver. COO, Legal og CEO får kopi, inden CTO erklærer DR-situationen lukket.
- Vi afholder et evalueringsmøde inden for 14 dage, hvor erfaringerne bliver til konkrete ændringer i DR-planen.

EVALUERING

DET, DER VIRKEDE

Teamet lukker fasen med præcision og komplethed: CTO ejer afslutningsdokumentet, VP Engineering skriver udkastet med en konkret godkendelsesdeadline (tirsdag kl. 12), og indholdet dækker alle væsentlige elementer — tidslinje, restore-kilder, lukkekriterier, åbne punkter med ejere og deadlines, datatab og IR-sporet. Distributionslisten (COO, Legal, CEO) og det dobbelte godkendelseskrav fra CTO og CISO er korrekt og plankonformt.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed er, at CISO's bidrag om IR-sporet — herunder GDPR-anmeldelse og kundekommunikation — er beskrevet som noget, der "leveres", men uden en konkret deadline, der er koblet til afslutningsdokumentets godkendelse tirsdag: hvis CISO og Legal ikke leverer afsnittet rettidigt, kan CTO ikke underskrive, og det er et uadresseret afhængighedspunkt i tidslinjen.

FREMADRETTET

DR-situationen nærmer sig en formel afslutning; det, der nu driver øvelsen frem mod mandag, er failback i servicevinduet — og om de to tilbageværende lukkekriterier (RPO-beskyttelse aktiv i begge regioner og backup-jobs verificeret kørende) er opfyldt og dokumenteret inden afslutningsdokumentet underskrives tirsdag.

Fase 5 af 5 · Normal drift Mandag, Dag 5, 11:20

Failback gennemført — backup-jobs kræver verifikation

SITUATION

Klokken 11:05 mandag bekræfter Head of Infrastructure, at failback til primærregionen er gennemført i servicevinduet: Route 53 peger på primærregionen, og Elasticsearch-genopbygningen er verificeret komplet og indekseret fra Aurora. Men da Head of Infrastructure gennemgår AWS Backup-konsollen for at kvittere for det tredje og sidste lukkekriterie — at backup-jobs er verificeret kørende — viser det sig, at de automatiske nattens AMI-snapshot-jobs i primærregionen ikke har kørt siden torsdag: jobs'ene er sat på pause, sandsynligvis som en sikkerhedsforanstaltning under hændelsen, og ingen har eksplicit genaktiveret dem. Aurora-snapshotsekvensen og cross-region-replikering er aktiv, men applikationsserver-AMI'erne har et fire dage langt hul. Afslutningsdokumentet skal godkendes af CTO og CISO om 40 minutter, og CISO har endnu ikke leveret IR-sporafsnittet om GDPR-vurderingen.

HANDLINGER FORETAGET

- Til referatet: godkendelsen af afslutningsdokumentet er aftalt til tirsdag kl. 12, ikke i dag. Den deadline holder vi, men vi godkender ikke et dokument med huller.
- Head of Infrastructure genaktiverer AMI-jobbene nu og starter en on-demand backup af alle applikationsservere med det samme. Acceptkriteriet for "verificeret kørende" er: én vellykket kørsel af hvert jobtype logget i AWS Backup, plus en test-restore af én AMI i en isoleret VPC. Det dokumenteres med skærbilleder og job-id'er i ticketen inden i aften.
- Hullet i AMI-backup fra torsdag til mandag noteres som et lukket punkt i afslutningsdokumentet, når den første kørsel er verificeret — og som et læringspunkt: ingen havde ansvaret for at genstarte jobs, der blev sat på pause under hændelsen. Det bliver et punkt i planens tjekliste for lukning.
- CISO leverer IR-afsnittet senest tirsdag kl. 09. Er det ikke klar, eskalerer CTO til CEO, og lukningen udskydes.

EVALUERING

DET, DER VIRKEDE

Teamet håndterer backup-hullet præcist og uden tøven: Head of Infrastructure genaktiverer AMI-jobbene og starter en on-demand backup med et konkret acceptkriterie — én verificeret vellykket kørsel af hvert jobtype plus en test-restore i isoleret VPC, dokumenteret med skærbilleder og job-id'er i ticketen. Beslutningen om at holde tirsdag kl. 12 som godkendelsesdeadline frem for at underskrive et ufuldstændigt dokument er rigtig prioritering, og eskaleringsstien til CEO, hvis CISO ikke leverer til kl. 09, giver CTO reel håndtag på det uadresserede afhængigheds punkt.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed er, at backup-hullet fra torsdag til mandag registreres som et lukket punkt, men den interne årsag — at ingen ejede ansvaret for at genstarte pausede

jobs — endnu ikke er omdannet til en konkret planændring. Notationen som et "læringspunkt" til tjeklisten er god intention, men der er ingen navngiven ejer af tjeklisteopgaven og ingen deadline for, hvornår planen er opdateret med den nye kontrol; det risikerer at ende som en hensigt uden effekt.

FREMADRETTET

Ind mod afslutningsdokumentets godkendelse tirsdag kl. 12 er der ét tilbageværende åbent spørgsmål: om CISO og Legal's IR-afsnit — herunder GDPR-vurderingens status og kundekommunikationens afsendelse — er klar og dækker alle tre lukkekriterierne, så CTO kan sætte sin underskrift og erklære DR-situationen formelt lukket.

Fase 5 af 5 · Normal drift Tirsdag, Dag 6, 08:47

CISO-afsnit forsinket — lukning truet

SITUATION

Klokken 08:47 tirsdag morgen melder CISO, at IR-afsnittet ikke er klar til den aftalte leveringsfrist kl. 09:00: Legal har endnu ikke afgivet en skriftlig vurdering af, om datatabet på ca. 6 timers ordredata udgør en anmeldepligtig hændelse under GDPR, og kundekommunikationen er formuleret, men ikke godkendt til afsendelse. CISO kan ikke sætte sin underskrift på afslutningsdokumentet, før det afsnit er komplet — og CTO's godkendelse af hele dokumentet er aftalt til kl. 12:00. Samtidig bekræfter Head of Infrastructure, at on-demand AMI-backup-kørslen er gennemført og verificeret med succesfulde job-id'er, og at test-restore i isoleret VPC er dokumenteret med skærmbilleder — det tredje og sidste lukkekriterie er dermed teknisk opfyldt og klar til at indgå i dokumentet.

HANDLINGER FORETAGET

- CTO eskalerer til CEO kl. 08:55. Vi konstaterer, at 72-timersfristen regnes fra, da vi blev bekendt med bruddet torsdag kl. 02:17, og at den derfor udløb søndag morgen. Ingen fulgte den frist, efter at den blev overdraget til Incident Response-sporet.
- CEO beslutter, at Legal og CISO anmelder til Datatilsynet i dag inden kl. 15, med en forklaring på forsinkelsen. Kundekommunikationen godkendes af Legal og sendes i dag til de kunder, hvis ordrer onsdag aften er tabt.
- DR-afslutningen: CTO godkender kl. 12 den tekniske del — failback, RPO-beskyttelse i begge regioner og verificerede backup-jobs. DR-situationen erklæres lukket med ét åbent punkt: IR-afsnittet, som CISO ejer, med deadline torsdag. VP Engineering ejer opdateringen af DR-planen med to nye punkter: genstart af pausede backup-jobs som fast trin ved lukning, og en navngiven ejer af lovpligtige frister, når et spor overdrages mellem DR og Incident Response.

EVALUERING

DET, DER VIRKEDE

Teamet lukker DR-situationen med rette prioritering og klart ejerskab: CTO godkender den tekniske del kl. 12 på baggrund af tre verificerede lukkekriterier, DR-erklæringen lukkes formelt med ét dokumenteret åbent punkt under CISO's ejerskab, og VP Engineering får konkrete opdateringsopgaver til DR-planen — genstart af pausede backup-jobs som fast lukningstrin og en navngiven ejer af lovpligtige frister ved overdragelse mellem DR og Incident Response. Beslutningen om at anmelde til Datatilsynet i dag inden kl. 15 med en forklaring på forsinkelsen er den eneste realistiske håndtering af en frist, der allerede er

overskredet.

VÆSENTLIGSTE MANGEL

Den væsentligste svaghed, som øvelsen har afdækket, er strukturel: GDPR 72-timersfristen løb fra torsdag kl. 02:17, udløb søndag morgen, og ingen fulgte den — fordi overdragelsen fra DR-sporet til Incident Response-sporet skete uden en navngiven ejer af fristen og uden et check-in-punkt, der sikrede, at fristen blev overholdt. Det er ikke et isoleret hændelsesforløbsproblem; det er et plangab, der nu er dokumenteret og ejet af VP Engineering til revision.

FREMADRETTET

DR-situationen er hermed formelt lukket med dokumenteret grundlag: CTO og CISO underskriver afslutningsdokumentet, COO, Legal og CEO modtager kopi, og de to tilbageværende åbne punkter — IR-afsnittet (CISO, deadline torsdag) og DR-114-remediering (Head of Infrastructure, deadline 1. december) — er registreret med ejere og deadlines. Evalueringsmødet inden for 14 dage konsoliderer læringspunkterne i en revideret plan.