DALK

DANSK ALARMKOMMUNIKATION

NIS2-Compliance og Datasikkerhed

DANSK ALARMKOMMUNIKATION

NIS2 Compliance og Datasikkerhed

Hos Dalko ønsker vi at give vores kunder mest mulig gennemsigtighed i vores arbejde generelt og med datasikkerhed i særdeleshed, så man som kunde er tryg ved den måde, vi arbejder med kundernes data.

NIS2-direktivet er et EU-direktiv, som sætter en ny standard for Net- og InformationsSikkerhed i EU og dermed i Danmark.

Det handler blandt andet om, hvordan virksomheder beskytter deres kundedata og deres systemer mod cyberangreb.

I Dalko arbejder vi med kundedata på to niveauer – kundedata og kundekommunikation i administrationen på det ene niveau, og data i evalinkplatformen, som håndteres af vores schweiziske partner, Sitasys i den anden.

Sitasys er ISO27001 certificeret, som i sig selv sikrer, at evalinkplatformen lever op til en lang række af de krav, der er indeholdt i NIS2, men platformen er i sit udgangspunkt designet til at gå længere end NIS2-direktivet kræver.

Opsummering

Dalko sikrer kundedata på administrationssiden ved at anvende 2FA og gennem en robust IT-sikkerhedspolitik, som ansatte skal efterleve.

evalinkplatformen drives af Sitasys, som er ISO27001 certficeret, og evalinkplatformen er designet til at have højere datasikkerhed end NIS2 og ISO-standarderne lægger op til.

Data er således krypteret både i transit og hvile, og krypteringsnøgler er udelukkende ejet af Sitasys.

evalink arbejder desuden med ekstrem redundans, med tre primære tilgængelighedzoner i Frankfurt med failover til tre tilgængelighedszoner i Dublin.

Datareplikering er på under 1 sekund mellem områder og regioner, hvilket sikrer minimalt potentielt datatab i tilfælde af en katastrofe.

Den neurale opbygning af systemet betyder samtidigt, at der ikke eksister et single-point-of-failure, hvilket sikrer en uovertruffen systemstabilitet.

Derudover gennemgår evalink årligt en omfattende ekstern sikkerhedstest af et anerkendt firma af cybersikkerhedseksperter.

På de følgende sider, fremgår en række af de mest centrale dele af sikkerhedselementer i så tydelige detaljer, vi kan dele, uden at det kompromitterer sikkerheden.

Del gerne dette dokument med de kunder, som har spørgsmål til NIS2.

Med venlig hilsen

Mikkel Schøler

Mikkel Schøler

CSO

DANSK ALARMKOMMUNIKATION

1. KUNDEDATA

Kundedata indgår i Dalkos eksterne ordre- og økonomistyresystem, hvor der anvendes 2FA for at øge sikkerheden mest muligt.

Mailadgang foregår ligeledes med 2FA.

Derudover skal Dalkos ansatte følge Dalkos IT-politik, der udleveres til alle medarbejder ved ansættelsen. Brud på IT-politikken kan få ansættelsesretslige konsekvenser.

I tilfælde af mistanke om brud på datasikkerheden er Dalkos direktør ansvarlig for at rapportere brud til de korrekte instanser, ligesom evt. berørte parter vil blive informeret hurtigst muligt og evt. afbødende tiltag vil blive iværksat.

2. EVALINKPLATFORMEN

Tekniske foranstaltninger til adskillelse af kundedata i evalink

evalink opererer på en **multi-tenant arkitektur** med streng tenantisolering håndhævet på både applikations- og databaselagene.

Isolering af applikationslag

Al dataadgang styres af evalinks egenudviklede **Talos IAM-system**, som håndhæver detaljerede autorisationsregler. Hver anmodning er begrænset til den godkendte tenants ID, hvilket sikrer, at ingen data fra en tenant nogensinde eksponeres for en anden.

Isolerede databaselag

Kundedata findes i AWS Aurora i en delt database, men de er logisk partitioneret på skema- og rækkeniveau. Alle forespørgsler passerer gennem applikationslogik, der håndhæver tenantgrænser uden direkte databaseadgang for tenants.

Netværks- og infrastrukturkontrol

Aurora-databaser kører i sikrede AWS VPC'er med strenge netværksrestriktioner. Yderligere netværksisolering er implementeret, hvor det er nødvendigt.

Indeslutning af fejl og sårbarheder

Systemdesignet sikrer, at fejlkonfigurationer eller sårbarheder, der påvirker en tenant ikke kan påvirke en anden. Logisk adskillelse, strenge IAM-rollepolitikker og automatiseret tilladelseskontrol forhindrer krydstenant risiko.

Test og overvågning

Tenantadskillelse valideres via:

- Automatiserede testsuiter og sikkerhedsscanning
- Kodegennemgange med fokus på håndhævelse af adgangskontrol
- Periodiske penetrationstest og sikkerhedsrevisioner
- Kontinuerlig overvågning via AWS GuardDuty, CloudWatch og Security Hub

Eventuelle uregelmæssigheder udløser beskeder og hændelsesresponsprocesser.

Håndtering af hændelser

I tilfælde af mistanke om kompromittering af dataadskillelse følger Sitasys sin **hændelsesresponsplan**, som omfatter indeslutning, rodårsagsanalyse, kundeunderretning og afhjælpning.

Integration af forebyggelse af datatab (DLP)

evalinks DLP-strategi supplerer tenantisoleringen:

- **Redundant, fejltolerant infrastruktur** implementeret på tværs af to AWS-regioner (Frankfurt og Dublin) med tre tilgængelighedszoner (AZ) hver.
- **Automatisk failover** (<60s for AZ-fejl, <90s RTO for regional failover) sikrer, at der ikke er noget single point of failure.
- **Replikering i realtid på tværs af regioner** (≤1s RPO) sikrer minimalt datatab.
- **Replikerings- og integritetskontroller**: Mindst fire kopier i AZ og seks kopier på tværs af regioner i alt af hver write operation.
- **Kryptering**: AES-256 i hvile og TLS 1.2+ under overførsel, anvendt på alle replikeringskanaler.
- **Governance**: Strenge mindste-privilegie adgangspolitikker, sikkerhedstræning for alle medarbejdere og overvågede slutpunkter.

Anvendte sikkerhedsteknologier

- **Firewalls**: AWS Web Application Firewall (AWS WAF) og AWS Network Firewall giver perimeterfiltrering, dyb pakkeinspektion og regler, der kan tilpasses, for at blokere ondsindet trafik.
- **DDoS-beskyttelse**: AWS Shield Advanced afbøder volumetriske og applikationslags DDoS-angreb.

- VLAN-ækvivalent isolering: AWS Virtual Private Clouds (VPC'er) med subnets, Sikkerhedsgrupper og netværks-ACL'er håndhæver netværkssegmentering mellem miljøer og services.
- Proxytjenester: Load Balancers afslutter TLS, filtrerer indgående anmodninger og beskytter interne tjenester.
- API Management: evalink driver sin egen API-gateway-implementering, der håndhæver authentication, autorisation og anmodningsbegrænsning for alle offentlige API'er.
- Identitetsbaserede webtjenester (IDWS): Talos IAM (evalinks egenudviklede identitets- og access management system) giver finkornet adgangskontrol for alle brugere, tjenester og tenants.

Håndtering af almindelige angrebsscenarier

- DDoS-angreb: Afbødes af AWS Shield og AWS WAF med rate based-regler, registrering af uregelmæssigheder og trafikfiltrering.
- De 10 største sårbarheder i OWASP: Løst via sikker kodningspraksis, SAST/DAST-scanninger, peer-kodegennemgange og automatiseret container image scanning.
- Man-in-the-middle-angreb: Forhindres ved at gennemtvinge TLS 1.2+ på tværs af al kommunikation (intern og ekstern) med udfasede protokoller deaktiveret.
- Rettighedseskalering: Forhindres gennem rollebaseret adgangskontrol, IAM-politikker med mindste-privilegie rettigheder og godkendelse af flere personer for kritiske ændringer.

Modstandsdygtighed over for fremtidige sårbarheder

Evalinks arkitektur adskiller strengt front-end fra backend-tjenester og datalag. Alle anmodninger passerer gennem godkendte API'er med validering og godkendelseskontrol på serversiden, hvilket sikrer, at front-end-sårbarheder ikke kan kompromittere underliggende data.

Detektion, overvågning og reaktion på indtrængen

- Registrering af indtrængen: AWS GuardDuty analyserer løbende VPC-flowlogfiler, CloudTrail-hændelser og DNS-logfiler for ondsindet aktivitet.
- Sikkerhedsovervågning: AWS Security Hub samler resultater fra GuardDuty, AWS Config og sårbarhedsscanninger for centraliseret synlighed.
- Operationel overvågning: AWS CloudWatch sporer systemets ydeevne, fejlrater og netværksuregelmæssigheder og genererer advarsler om sikkerheds- eller tilgængelighedshændelser.
- Ændringsovervågning: AWS CloudTrail logger alle konfigurationsændringer på netværksinfrastruktur, IAM-roller og sikkerhedsgrupper.

Eksempler på angrebsafbødning i praksis

- DDoS-simuleringstests bekræftede AWS Shields evne til at absorbere og afbøde volumetriske angreb uden nedetid.
- Regelmæssig scanning af sårbarheder opdager og afhjælper risici i OWASP-klassen som f.eks. SQL-injektion og Cross-Site scripting før udrulning.

- TLS-konfigurationer testes med jævne mellemrum for at sikre modstandsdygtighed over for MITM-angreb og certifikater fornyes automatisk.

Datakvalitet og integritet i evalink

evalink er designet med robust validering, datastyring og integritetskontroller, der opererer konsekvent på tværs af brugergrænsefladen, back-end-tjenester og API'er for at sikre nøjagtighed, konsistens og fuldstændighed af data.

Ensartet validering på tværs af alle lag

- **Validering på brugergrænsefladeniveau**: Validering af formularer på klientsiden håndhæver dataformater, obligatoriske felter og forretningsregler før afsendelse.
- **Back-end-validering**: Alle indgående data valideres igen på servicelaget for at sikre integritet uanset kilde, hvilket forhindrer omgåelse af regler på klientsiden.
- **Validering på API-niveau**: Anmodninger til offentlige og interne API'er gennemgår de samme forretningsregelkontroller og valideringer af dataformater som brugergrænsefladen, hvilket sikrer ensartet håndhævelse på tværs af alle inputkanaler.

Ekstern datavalidering

- Hvor det er relevant, kan data valideres mod **eksterne autoritative kilder** (f.eks. adresseverifikationstjenester, geolokaliserings-API'er) for at sikre nøjagtighed.

Foruddefinerede værdilister

- Drop-down lister og foruddefinerede værdisæt bruges, hvor det er muligt, til at standardisere indtastninger og reducere indtastningsfejl.
- Disse lister administreres centralt, hvilket sikrer, at opdateringer anvendes konsekvent på tværs af systemet.

Forebyggelse af modstridende data

- Forretningsregler anvendes på applikationslaget for at forhindre modstridende indtastninger (f.eks. gensidigt udelukkende konfigurationsindstillinger eller driftstilstande).
- Konflikter registreres i realtid, og brugerne bliver bedt om at rette dem, før data gemmes

Begrænset brug af fritekstfelter

- Fritekstindtastning minimeres og bruges kun, når strukturerede data ikke er praktiske.
- Hvor der findes fritekstfelter, kan de indeholde tegnbegrænsninger, rensnings- og formateringsregler for at opretholde ensartethed og sikkerhed.

Påkrævede felter

- Nøgledatafelter markeres som obligatoriske og valideres, før data gemmes, hvilket sikrer fuldstændighed af væsentlige poster.

Kontinuerlig overvågning og integritetssikring

- Automatiserede integritetskontroller kører med jævne mellemrum for at registrere uregelmæssigheder eller overtrædelser af dataregler.
- Overvågningslogfiler registrerer alle ændringer, og der er tilgængelige tilbagerulningsprocedurer til genoprettelse fra fejlagtige opdateringer.

Fortrolighed

evalink sikrer fortrolighed af alle kundedata og alarmsignaler gennem følgende foranstaltninger:

- **Kryptering under overførsel:** Al kommunikation mellem klienter, tjenester og API'er krypteres ved hjælp af **TLS 1.2 eller højere**. Forældede protokoller (f.eks. SSL, TLS 1.0/1.1) er eksplicit deaktiveret. Alarmsignaler transmitteres over sikre TLS-kanaler for at forhindre interception eller tampering under transport.
- **Kryptering i hvile:** Alle persistent lagervolumener, herunder databaser og object storage, krypteres med **AES-256-krypteringsnøgler**, der administreres via AWS Key Management Service (KMS).
- **Adgangskontrol:** Rollebaseret adgangskontrol (RBAC) sikrer, at brugere og administratorer kun kan få adgang til data, der er relevante for deres roller. Adgang håndhæves på både program- og databaselagene.
- **Netværksisolering:** Kundevendte tjenester er beskyttet af vores egen API-gateway-implementering, netværksfirewalls og VPC-adskillelse for at forhindre uautoriseret adgang.

Integritet

evalink sikrer dataenes rigtighed og troværdighed gennem:

- **Databasebegrænsninger og unikke nøgler:** Undgå duplikering, og sørg for, at business rules håndhæves på databaseniveau.
- **Valideringsregler:** Anvendes konsekvent på tværs af brugergrænsefladen, backend-tjenester og API'er for at forhindre indtastning af ugyldige eller modstridende data.
- **Revisionslogning:** Alle ændringer i konfiguration og alarmhåndtering logges med tidsstempel og bruger-ID.
- **Sikker udviklingslivscyklus:** Kodeændringer gennemgår sikker kodegennemgang, automatiseret test (herunder OWASP Top-10 sårbarhedskontrol) og integritetsvalidering før implementering.

Tilgængelighed

evalink er designet til høj tilgængelighed og fejltolerance:

- **Multi-regionsudrulning:** Produktionsarbejdsbelastninger kører aktivt i mindst to AWS-regioner, som hver har tre uafhængige AZ.
- **Automatisk failover:** I tilfælde af en AZ-fejl failover, har services en fail over på <60 sekunder; i tilfælde af et fuld regionalt udfald, fuldføres failover på tværs af regioner på <90 sekunder.
- **Replikering i realtid:** Datareplikering mellem områder har en RPO på ≤1 sekund, hvilket sikrer minimalt datatab i en katastrofe.
- **DDoS-beskyttelse:** Flere lag af DDoS-afbødning er implementeret, herunder AWS Shield og rate-begrænsning på API-gateway-niveau.7

- Kontinuerlig overvågning: GuardDuty, CloudWatch og intern alarmering overvåger løbende tjenestens tilstand og sikkerhedstilstand.