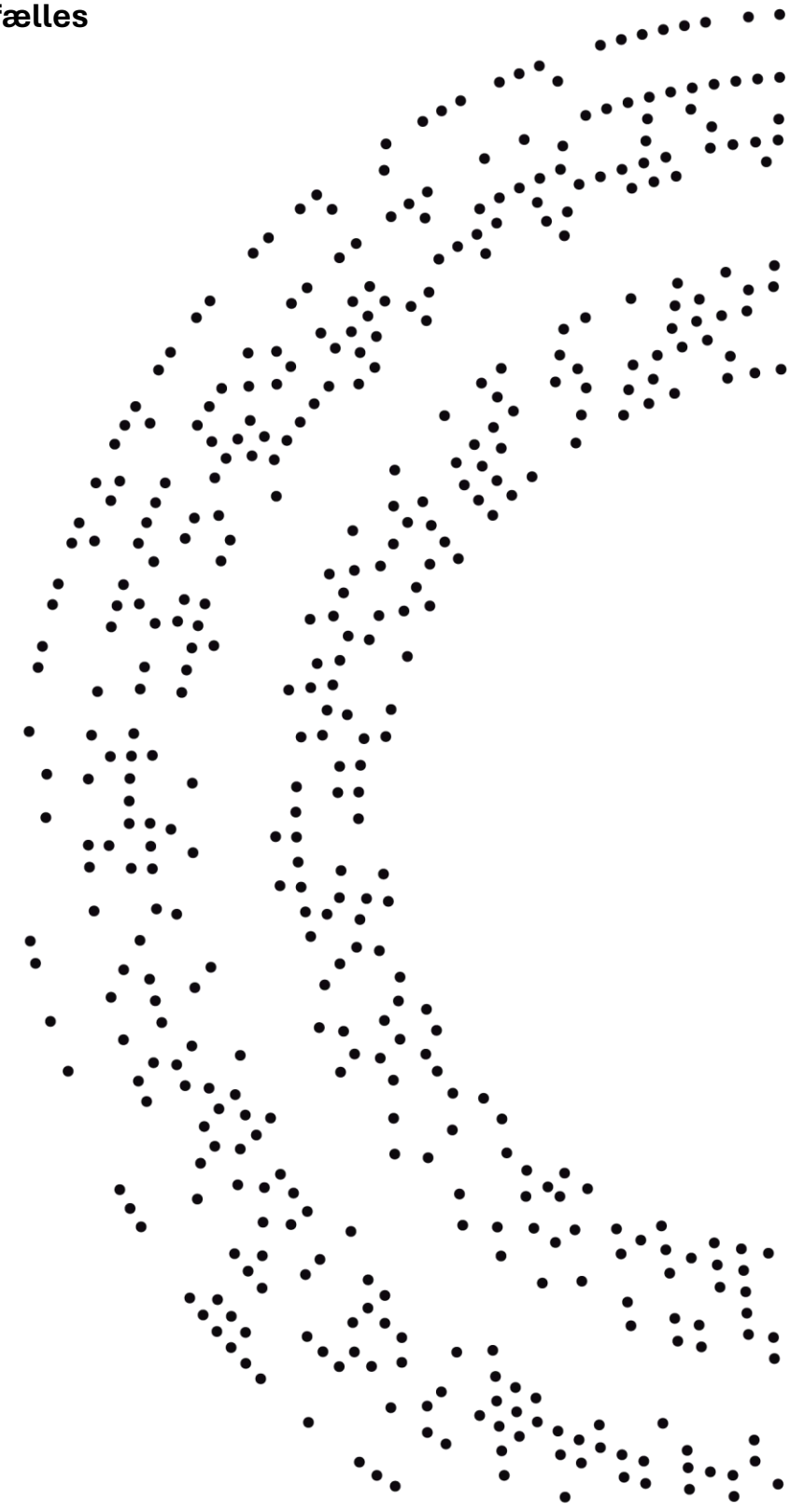
2.1 Teknisk målbillede - Sikkerhed

Inspiration til teknisk målbillede for fælles kommunal IT-drift

08.05.2026 I Version 1.3



Conscia
Secure progress

De samlede dokumenter er udarbejdet som et arbejds- og referencegrundlag. Videreformidling, kopiering eller anvendelse i andre sammenhænge bør ske med omtanke og med kendskab til dokumentets formål og kontekst. Eventuelle udskrifter betragtes som ukontrollerede.

Indhold

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

Dette dokument bygger på de arkitekturprincipper, der er fastlagt i hoveddokumentet, og som er kvalificeret gennem en analyse- og workshopfase med deltagelse fra relevante kommunale aktører. Principperne afspejler dermed både et fagligt perspektiv og de erfaringer og behov, der er identificeret på tværs af kommunerne.

Dokumentet består af udvalgte arkitekturprincipper og tilhørende anbefalinger baseret på erfaringer, analyser, best practice og standarder, som vurderes at være centrale for at understøtte en stabil, sikker og robust fælleskommunal IT-drift.

Dokumentet er et fagligt udgangspunkt for det videre arbejde med at etablere en konkret arkitektur og implementeringsplan i den enkelte IT-serviceorganisation. Dette arbejde forudsætter lokal tilpasning og skal gennemføres i samspil med ejerkommunerne samt med inddragelse af eksisterende producenter og leverandører, hvor det er relevant.

Det endelige ambitionsniveau for sikkerhed, drift og servicemodel fastlægges af den enkelte IT-serviceorganisation på baggrund af ejerkommuners behov, prioriteringer og risikovurderinger.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

1 Introduktion

Digital infrastruktur udgør fundamentet for kommunernes evne til at levere velfærd, service og myndighedsopgaver på en stabil, sikker og tillidsvækkende måde. Når it-systemer fungerer tilgængeligt, integreret og robust, skabes der direkte værdi for borgere, medarbejdere og samarbejdspartnere. Sikkerhed og driftsrobusthed er derfor et strategisk ledelsesanliggende, der har direkte betydning for kommunernes samlede handlekraft og troværdighed.

Dokumentet beskriver, hvordan en fælles IT-serviceorganisation kan opbygge et solidt og fremtidssikret fundament for sikker og ensartet drift på tværs af kommuner gennem enkeltstående løsninger samt klare principper, gennemsigtighed i ansvarsfordelingen, fælles standarder og en moden tilgang til risiko, resiliens og compliance.

Sikkerhedsanbefalingerne er forankret i behovet for at begrænse konsekvenserne af sikkerhedshændelser i en fælles driftssituation, hvor én kompromittering ellers kan påvirke flere kommuner. Derfor er arkitekturen baseret på segmentering, identitetsbaseret adgang og central overvågning, som tilsammen reducerer angrebsflade, begrænser spredning og forbedrer evnen til hurtig detektion og håndtering.

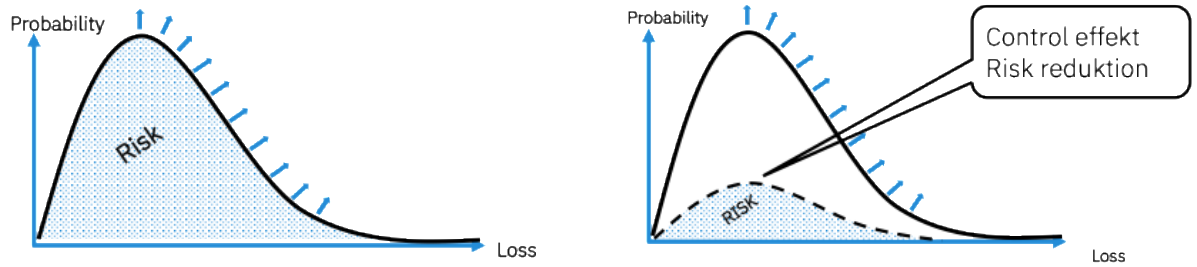
Ambitionen er at opbygge forudsigelighed, styrbarhed og evnen til hurtigt og kontrolleret at reagere på hændelser. En organisation med dybt kendskab til egne systemer, tydeligt placeret ansvar og sikkerhed indarbejdet i arkitekturen fra starten har et solidt grundlag for effektiv håndtering af både hændelser og nye krav og står dermed stærkere i sin samlede drifts- og sikkerhedsevne.
Samtidig er fælles drift en mulighed: en mulighed for at hæve det samlede sikkerhedsniveau, reducere kompleksiteten og sikre, at alle kommuner – uanset størrelse og lokale forudsætninger – har adgang til samme beskyttelse, samme gennemsigtighed og samme professionelle beredskab. Det kræver tydelige fælles rammer, men også respekt for lokale forskelle og den virkelighed, kommunerne opererer i.

Dette dokument fungerer som et styringsgrundlag og en inspirationsramme for ledelsesmæssige beslutninger. Det omsætter krav, best practice og erfaringer til konkrete anbefalinger, der understøtter strategiske valg om organisering, investeringer og prioritering. I læsevejledningen til denne dokumentpakke findes begrebsforklaringer og kildehenvisninger.

2 Security by Design & Sikkerhedsmodenhed

En robust og sikker infrastruktur kræver, at sikkerhed er en integreret del af arkitekturen fra starten. Dette afsnit behandler de principper og konkrete anbefalinger, der tilsammen understøtter en sikkerhedskultur og et teknisk fundament, som er robust og sikkert i forhold til at understøtte IT-serviceorganisationens ambition om at levere ensartet og sikker drift på tværs af kommunerne.

Målsætningen er ikke at opnå en utopisk 100 % beskyttelsesgrad, men at sænke risiko- og konsekvensproduktet til et acceptabelt risikoniveau. Dette gøres blandt andet ved at indtænke security by design, så risikovurderinger bliver en styrende parameter for sikkerhedsindsatsen.



Figuren viser, hvordan en struktureret arkitektur reducerer og isolerer risiko sammenlignet med et ustruktureret miljø.

2.1 Security by Design

Security by design handler om, at sikkerhedshensyn er en integreret del af designprocessen og ikke noget, der tilføjes efterfølgende. Det kræver klare ansvarsforhold, dokumenterede standarder for konfiguration og en systematisk tilgang til vurdering af risikoen ved de services, der eksponeres i infrastrukturen.

2.1.1 Ansvarsmodel for drift og sikkerhed

Det anbefales, at IT-serviceorganisationen etablerer og kommunikerer en klar ansvarsmodel, der beskriver, hvem der har henholdsvis drifts- og sikkerhedsansvaret for de enkelte lag i infrastrukturstakken. Udgangspunktet er shared responsibility-modellen (typisk kendt fra cloudleverandører), hvor ansvaret er fordelt mellem IT-serviceorganisationen og den enkelte kommune afhængigt af, hvilken del af stakken der er tale om.

En RACI-matrix for infrastrukturlagene bør udarbejdes og kommunikeres til alle ejerkommuner, så der etableres en effektiv kommunikations- og handlingsmodel. Det er vigtigt, at modellen reelt efterleves. RACI kan laves både for de helt overordnede infrastruktursområder, men evt. også for scenarier, der må betragtes som ofte forekomne og hvor en ansvarsmodel er formålstjenstlig.

Eksempel scenarie: switch på en kommune lokation går i stykker

Aktivitet	IT-Serviceorganisation	Kommune (lokalt)	Evt. Leverandør
Detektion via central monitorering	**A, R**	I	I
Fejldiagnose: hardware bekræftet defekt	**A, R**	C	C
Bestilling af erstatningsenhed (RMA eller fra fælles lager)	**A, R**	I	R
Fysisk udskiftning: nedmontering, montering, strøm, krydsninger	C	**A, R**	I
Aktivering: enhed kobles på, henter konfiguration via zero-touch / out-of-band	**A, R**	**C**	I

En velfungerende ansvarsmodel reducerer risikoen for, at sikkerhedsansvar falder mellem to stole, og giver IT-serviceorganisationen et klart grundlag for at håndtere incidents, ændringer og evt. leverandørrelationer. Shared responsibility modellen bør desuden indgå som en fast del af kommunikationen i forhold til kommunernes forventninger til driften, så disse er afstemte fra starten.

2.1.2 Hærdning af infrastrukturkomponenter

Alle infrastrukturkomponenter bør deployeres efter dokumenterede og godkendte hærdning-standarder. CIS Benchmarks anbefales som referencegrundlag og er tilgængelige for de fleste relevante platforme, herunder firewalls, switches, routere, load balancere og DNS servere.

En godkendt baseline konfiguration bør som minimum sikre, at alle standardkodeord er ændret, at unødvendige management interfaces er deaktiveret, og at forældede og usikre protokoller som Telnet og SNMPv1/v2 er fjernet inden idriftsættelse. Baseline konfigurationen bør behandles som en levende standard, der opdateres i takt med, at CIS udgiver nye versioner, eller leverandørens anbefalinger ændrer sig.

Afvigelser fra hærdning baseline bør registreres i CMDB med risikoaccept, ejer og opfølgningsdato. Det sikrer synlighed og sporbarhed og giver IT-serviceorganisationen et overblik over de steder i infrastrukturen, hvor der bevidst er valgt et lavere konfigurationsniveau end det, standarderne foreskriver.

2.1.3 Risikobaseret tilgang til serviceeksponering

Det anbefales, at IT-serviceorganisationen indfører en systematisk screeningsproces for alle services, der registreres i CMDB. Screeningen bør kortlægge eksponeringsbredde, autentifikationsmetode, krypteringskrav og de nødvendige sikkerhedskontroller for servicen, og den bør gennemføres som en integreret del af registreringsprocessen og ikke som en separat, efterfølgende aktivitet.

Interneteksponerede services bør automatisk klassificeres som medium- eller højrisiko og kræve dokumenterede sikkerhedskapaciteter, inden de kan ibrugtages. Ingen interneteksponering bør ske,

uden at de relevante kontroller er verificeret og registreret i CMDB. Screeningsresultaterne bør være tilgængelige i CMDB og indgå i det løbende risikoregister.

Tilgangen sikrer, at Zero Trust-principper ikke blot gælder for brugeradgang, men også for services. En service bør beskyttes proportionalt med den risiko, den repræsenterer, og ændringer i eksponeringsomfanget bør udløse en ny screening.

2.2 Teknisk sikkerhedsmodenhed

Teknisk sikkerhedsmodenhed handler om, at de kontroller og kapabiliteter, der beskytter infrastrukturen, er implementerede, ensartede og vedligeholdt. Det indebærer, at alle kommuner i IT-serviceorganisationen har adgang til det samme beskyttelsesniveau, og at centrale sikkerhedsfunktioner som DNS sikkerhed og firewallstyring er drevet af dokumenterede processer frem for enkeltpersoners viden.

2.2.1 Ensartet sikkerhedsniveau på tværs af kommuner

Et centralt mål for IT-serviceorganisationen bør være, at alle ejerkommuner har adgang til de samme sikkerhedskapabiliteter og opnår det samme faktiske beskyttelsesniveau uagtet lokal infrastruktur og lokale valg. Det dækker kapabiliteter som DDoS beskyttelse, webfiltrering og IPS/IDS.

Det anbefales, at alle udgående internetforbindelser fra ejerkommunerne routes igennem IT-serviceorganisationens centrale sikkerhedsplatform, f.eks. via en SASE løsning eller et centraliseret internet exit. Alternativt kan decentrale firewalls med de samme sikkerhedskapabiliteter og politikker anvendes, forudsat at dækning og konfiguration verificeres centralt. Uanset model bør det løbende monitoreres, om alle kommuner faktisk opnår det aftalte beskyttelsesniveau.

DDoS beskyttelse bør implementeres som en fælles kapabilitet, der beskytter alle kommuners interneteksponerede services centralt. Ingen kommune bør stå alene med ansvaret for at mitigere volumbaserede angreb. Afvigelser fra det aftalte sikkerhedsniveau for en enkelt kommune bør identificeres og adresseres proaktivt frem for at vente på, at de manifesterer sig som incidents.

2.2.2 DNS sikkerhed

DNS er en af de mest udnyttede angrebskanaler og bør behandles som en aktiv sikkerhedskontrol frem for blot en navneopløsningstjeneste. Det anbefales, at IT-serviceorganisationen implementerer DNS sikkerhed, DNSSEC og en klar adskillelse af intern og ekstern DNS opløsning.

En DNS sikkerhedsløsning bør implementeres for alle klienter og servere med automatisk opdatering fra threat intelligence-feeds, så kendte C2-domæner, phishing og malware-distribution blokeres automatisk. DNSSEC bør implementeres og valideres for alle kommunernes egne domæner, og zone-signing bør dokumenteres med automatisk nøglerotation.

Intern og ekstern DNS opløsning bør adskilles, f.eks. via split-horizon DNS og med hidden primary-opsætning. Interne systemer bør ikke eksponeres i ekstern DNS, og intern navneopløsning bør ikke

være tilgængelig udefra. En angriber, der kan kortlægge intern infrastruktur via DNS opslag, har en væsentlig fordel i en rekognosceringsproces, og adskillelsen fjerner dette blindspot.

2.2.3 Firewall management og regelsæt administration

Et ukontrolleret voksende firewallregelsæt er en af de hyppigste årsager til uønskede netværksåbninger. Det anbefales, at IT-serviceorganisationen etablerer en formel styringsproces for regelsættet, der sikrer, at regler er dokumenterede, godkendte og løbende revurderede.

Alle firewallregler bør dokumenteres med forretningsbegrundelse, systemejergodkendelse og oprettelsesdato. Regler uden dokumentation bør ikke tillades. Firewallkonfigurationer bør versionsstyres i et centralt repository, og alle ændringer bør spores med forfatter, tidspunkt og godkendelse. Jævnlige review af regelsæt bør identificere og fjerne ubrugte regler, brede any-any åbninger og regler, der modsiger den godkendte zoneringsmodel.

Deny-by-default bør håndhæves ved alle zoneovergange som et grundprincip. Et regelsæt, der er vokset organisk over mange år uden systematisk oprydning, er ikke blot en driftsbyrde, men også en sikkerhedsrisiko, da omfanget af uønskede åbninger er ukendt.

Det må forventes at der inden for den kommende årrække i større udstrækning vil blive anvendt AI til at generere regelsæt elementer dynamisk. I den forbindelse er det vigtigt, at der etableres sporbarhed (kommentarer, navne og beskrivelser) og guardrails igennem, så ændringer ikke sker uhensigtsmæssigt. Der er en konflikt imellem AI 'kreativitet' og den ønskede determinisme i sikkerhedsregelsættet, hvilket der skal tages højde for i løsningen. Den p.t. mest oplagte løsning er anvendelse af en MCP server, der translatere AI-politikker, via guardrails, til deterministiske udfald.

2.2.4 Resiliens og service kontinuitet

Resiliens handler om evnen til at opretholde kritiske services under og efter et nedbrud, uanset om det skyldes hardwarefejl, menneskelige fejl eller et målrettet angreb. For en IT-serviceorganisation, der betjener mange kommuner, er det afgørende, at redundans og genopretningsevne er systematisk planlagt og testet frem for tilfældigt fordelt.

2.2.5 Redundans i ejerkommunernes opkoblinger

Kritiske services i driftscenteret bør kunne nås fra en ejerkommune via multiple WAN-forbindelser, f.eks. internet VPN, MPLS eller fiber, for de lokationer, hvor konsekvensen af et nedbrud vurderes at have uacceptable følger. Behovet for WAN-redundans bør vurderes og dokumenteres pr. lokation baseret på en klassifikation af konsekvens ved nedbrud.

Redundante WAN-forbindelser bør leveres af separate udbydere med fysisk uafhængige ruter. Uafhængighed bør verificeres, så ruterne ikke deler fysisk infrastruktur som kabelruter eller fordeling. Lokationer med samfundskritiske services bør have et højere redundanskrav end lokationer med primært administrative funktioner.

Failover indgår som en aktiv og systematisk del af driften og afprøves regelmæssigt for at sikre dokumenteret funktionalitet. Redundante forbindelser bidrager dermed til reel driftsrobusthed og tillid i løsningen. Failovertid måles og vurderes løbende op mod det fastlagte RTO for de services, kommunen anvender via forbindelsen.

2.2.6 Redundans i kritiske fysiske komponenter

Væsentlige og kritiske infrastrukturkomponenter bør opbygges med lokal redundans i form af high-availability konfiguration og dual power. Hvilke komponenter der kræver redundans, bør vurderes ud fra en individuel kritikalitetsbetragtning og registreres i CMDB, så overblikket ikke er personafhængigt.

Alle komponenter, der er klassificeret som kritiske i CMDB, bør opbygges med high availability og dual power, og redundans konfigurationen bør verificeres og dokumenteres. Strømredundans via dual PSU og UPS bør implementeres for alle kritiske komponenter i driftscenteret, da strømfejl på én forsyningsvej ikke bør medføre nedbrud.

Redundanskrav bør indgå som et fast anskaffelseskriterium for infrastrukturkomponenter, der er klassificeret som kritiske. Komponenter, der ikke kan leveres med HA, bør kun anskaffes med en dokumenteret risikoaccept, så bevidste valg om lavere redundansniveau er synlige og ejet.

2.2.7 Redundans i kritiske services

Kritiske services bør deployeres med logisk redundans i driftscenteret via load balancere, softwareredundans eller tilsvarende mekanismer. Alle services, der er klassificeret som kritiske i CMDB, bør deployeres bag en load balancer med mindst to aktive backend noder, så nedbrud på én node ikke medfører serviceudfald.

Stateful services som Active Directory, DNS og databaser bør konfigureres med softwareredundans, f.eks. via AD-replikering, og failover bør testes og dokumenteres med målt failover-tid. AD og DNS er fundamentale for al brugerautentifikation og netværkskommunikation, og et nedbrud af disse services uden redundans har øjeblikkelig og bred brugerkonsekvens.

Kapacitet på redundante services bør dimensioneres til at kunne håndtere fuld load på tilbageværende noder ved nedbrud på én node. Redundans uden kapacitetsmargin betyder, at servicen degraderer ved failover og dermed ikke lever op til den tilsigtede resiliens.

2.2.8 Backup og recovery af infrastrukturkonfigurationer

Konfigurationer af alle infrastrukturkomponenter bør versionsstyres og sikkerhedskopieres automatisk, og recovery bør testes og dokumenteres. Det anbefales, at konfigurationsbackup gemmes dagligt i et versionsstyret repository adskilt fra produktionsmiljøet, og at backuppen er beskyttet mod ransomware via immutable storage eller en offsite kopi i et separat miljø.

Recovery af en infrastrukturkonfiguration bør være en dokumenteret og testet proces med målt genoprettelsestid. Processen bør beskrives i en runbook, der er tilgængelig uden adgang til produktionssystemerne, da en situation, der kræver konfigurationsgenopretning, ofte er den situation, hvor adgangen til produktionssystemerne er begrænset.

En firewallkonfiguration, der aldrig er eksporteret, og som kun kendes indgående af én medarbejder, som måske ikke længere er ansat, er et velkendt scenarie, men en tilstand, som IT-serviceorganisationen bør arbejde aktivt på at eliminere.

2.3 Sikkerhedspolitik og håndhævelse

En teknisk stærk infrastruktur understøttes af klare politikker, veldokumenterede processer og løbende verifikation af, at kontrollerne faktisk virker. Nedenstående områder danner fundamentet for en styringsmodel, der sikrer, at infrastruktursikkerheden er konsistent, sporbar og auditérbar.

2.3.1 Compliance med de tekniske minimumskrav til infrastruktur

Tekniske minimumskrav bør kortlægges fuldt ud og oversættes til konkrete tekniske kontroller for alle relevante infrastrukturkomponenter og driftsdomæner. Det er ikke tilstrækkeligt at kende kravene; de skal mappes til specifikke systemer, have en ansvarlig ejer og en verificerbar implementering.

Compliance-status bør være synlig i et centralt dashboard og opdateres jævnligt. Krav til logning, kryptering og adgangsstyring bør verificeres på alle relevante infrastrukturkomponenter, inklusiv netværksudstyr og sikkerhedsinfrastruktur, og ikke kun på servere og klienter.

Dokumentation for efterlevelse bør kunne fremvises samlet ved ekstern auditering. Evidens, der skal samles manuelt ved audit, er et tegn på, at compliance-arbejdet ikke er integreret i den løbende drift. Minimumskrav, der er downloadet og gemt i en Teams-mappe, men ikke omsat til konkrete kontroller, giver ingen reel sikkerhed og ingen dokumenterbar efterlevelse.

AI generet kode og workloads vil formodentlig finde vej ind i den fælles infrastruktur i den nære fremtid. Disse bør være isoleret som de øvrige ift. zero-trust principperne, men også i endnu højere grad være genstand for gennemsyn, da angrebsfladen i disse på nuværende tidspunkt er uforbeholdent meget større end gængse.

AI baseret konfiguration (f.eks. via automation, agenter og lign.) bør desuden underkastes de samme validering og auditeringskrav som elementer genereret af mennesker. Dvs. der skal være sporbarhed, identitets attribution samt formål i en form for log. Der bør i den sammenhæng laves en AI sikkerhedspolitik der omfatter disse elementer. Det kunne f.eks. være elementer som HITL (Human in the loop) principper, eller tilsvarende.

2.3.2 Netværksdokumentation og konfigurationsstyring

Netværksdokumentation bør være komplet, opdateret og versionsstyret. Dokumentationen bør være tilstrækkelig til at en ny medarbejder kan drifte og fejlsøge infrastrukturen uden at trække på kolleger med lokalkendskab. Personafhængig viden om netværkstopologien er en operationel og sikkerhedsmæssig risiko.

Netværksdiagrammer bør opdateres kontinuerligt og versionsstyres i et centralt repository tilgængeligt for IT-serviceorganisationen. IP-adresseoversigt, VLAN-register og firewall-zoneoversigt bør

vedligeholdes og synkroniseres med CMDB, og afvigelser bør identificeres automatisk ved jævnlige scans.

Runbooks for kritiske infrastrukturprocedurer, f.eks. firewall failover, DNS fejl og certifikatfornyelse, bør dokumenteres og gøres tilgængelige offline. Under et cybersikkerhedsincident er adgang til systemer og dokumentation ofte begrænset, og en offline runbook kan være forskellen på en kontrolleret og en kaotisk genopretning.

2.3.3 Regelsæt governance og firewall audit

Firewall-regelsættet bør underlægges formel governance med regelmæssige uafhængige audits. Regelkvalitet, overholdelse af zoneringsmodellen og håndhævelsen af deny-by-default princippet bør verificeres systematisk og ikke kun når der opstår et problem.

En halvårlig uafhængig audit af regelsæt bør gennemgå alle firewall regler og identificere brede åbninger, forældede regler og afvigelser fra den godkendte zoneringsmodel. Fund bør behandles som sikkerhedssårbarheder med definerede frister frem for som administrative optimeringer.

Anvendelsesgraden af sikkerhed funktionalitet påtrykt sikkerheds regler (IPS, TLS inspektion mv.) bør endvidere vurderes løbende, med en ambition om at have alle de tilgængelige kapabiliteter i anvendelse.

Automatiserede regelanalyseværktøjer kan løbende identificere redundante, overlappede (shadowed) og for brede regler samt integrere med change management processen. Et regelsæt, der ikke auditeres, vokser hurtigt ukontrolleret, og omfanget af uønskede åbninger forbliver ukendt. Dette vil over tid stærkt vanskeliggøre en smidig drift for en IT-serviceorganisation.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

3 Overvågning og Auditering

3.1 Logkilder og dækning

En IT-serviceorganisation, der betjener mange kommuner, er nødt til at have visibilitet ned i de enkelte medlemmers netværkstelemetri, så det er muligt at overvåge og analysere infrastrukturen. Logning er her fundamentet for alt fra fejlfinding og kapacitetsstyring til sikkerhedsdetektion og compliance. Det forudsætter, at logkilder er kortlagt og konfigureret, at telemetri opsamles systematisk, og at den tekniske kvalitet af logs er høj nok til, at de faktisk kan anvendes til de tiltænkte formål.

Det anbefales, at IT-serviceorganisationerne sikrer den nødvendige tekniske kvalitet og mængde af logs og telemetri for at kunne levere en effektiv drift og sikkerhedsovervågning.

Den tekniske logkvalitet fra netværksudstyr (f.eks. routere, switche, firewalls, VPN og loadbalancere) samt sikkerhedsinfrastruktur (WAF, proxy, DNS sikkerhed, MFA og Endpoint Detection and Response (EDR) (out of scope)) bør være standardiseret, ensartet og af dokumenterbart høj kvalitet, så data kan korreleres på tværs af kilder og anvendes til overvågning, hændelseshåndtering, compliance og efterforskning.

- Standardiseret format og felter: Logdata skal følge en fælles struktur (f.eks. CEF/LEEF/JSON efter valgt standard) med konsistente feltnavne og værdier på tværs af leverandører og platforme.
- Korrekte og synkroniserede tidsstempler: Alle kilder skal anvende NTP og logge med tidszone/UTC, så hændelser kan korreleres i tidslinjer på tværs af systemer.
- Entydig identifikation: Logs skal som minimum indeholde kilde (hostname/device id), miljø, systemtype samt relevante identifikatorer, f.eks. bruger-/servicekonto, session id, request id eller flow id, hvor det er muligt.
- Tilstrækkelig detaljeringsgrad: Hændelser skal logges på et niveau, der muliggør triage og root cause analyse (f.eks. allow/deny, policyregel, port/protokol, NAT samt certifikat-, auth- og konfigurationsændringer).
- Dataintegritet og fuldstændighed: Logtransport skal være robust (evt. lokalt bufferet) og understøtte detektion af tab/duplikering; kritiske kilder må ikke "droppe" events ved load.
- Berigelse og normalisering: Relevante felter bør beriges (f.eks. asset-/CMDB kontekst, geografi, kritikalitet og netværkszone) og normaliseres til et fælles "sprog" for alarmer og dashboards.
- Kvalitetskontrol: Der skal være løbende validering af logkilder (volumentjek samt sanity check af indhold) samt klare krav til udbedring ved afvigelser.
- Retention og sporbarhed: Opbevaringsperioder og adgangskontrol skal være defineret i henhold til compliancekrav, og logs skal kunne genskabes/revideres ved audit.

Mængden af almindelige logs og sikkerhedslogs overgår hurtigt, hvad man som menneske kan overskue. Det er derfor oplagt at tilføje en AI komponent til sortering og flagning af incidents. Det ligger ud over scopet for dette dokument at beskrive det i detaljer her, men det er et område, IT-serviceorganisationerne bør være opmærksomme på.

3.1.1 Logkilderegister

Alle relevante logkilder bør være identificeret, registreret og aktivt konfigureret til logafsendelse. Det omfatter netværksudstyr, servere, endpoints, applikationer, cloud-tjenester og SaaS platforme. Et centralt logkilderegister, vedligeholdt i CMDB eller tilsvarende, giver overblik over, hvad der logger, hvad der logges, og om logs faktisk modtages korrekt.

Uden et logkilderegister kan det ikke vides, hvad der ikke logger. En firewall, der sender logs til et system, der ikke længere eksisterer, en ny server, der ikke har logget i f.eks. seks måneder, eller en SaaS tjeneste, hvis audit logs aldrig er blevet aktiveret, er alle eksempler på huller, der ikke opdages uden systematisk styring.

3.1.2 Netværkstelemetri

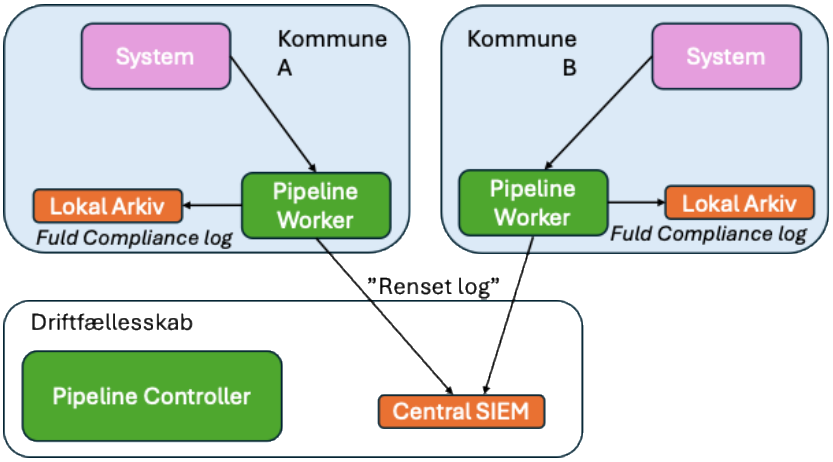
Netflow eller tilsvarende flowtelemetri bør opsamles fra alle netværksenheder, ikke kun fra internet edgen. Intern segmenttrafik, øst-vest flows og trafik i distributionslaget er også centrale datakilder for detektion af lateral bevægelse, data exfiltration og anomalier i kommunikationsmønstre.

Netflow bør konfigureres på alle core- og edge switche og sendes til en dedikeret flowcollector, der evt. filtrerer og videreender til SIEM. Telemetri, der kun dækker nord-syd-trafik, giver et ufuldstændigt billede og efterlader intern trafik som et muligt blind spot. Under et incident, hvor det er nødvendigt at rekonstruere et kommunikationsmønster, vil fraværet af intern telemetri være en begrænsning. Flowdata har også en driftsmæssig fordel, idet man reelt kortlægger, hvordan applikationer kommunikerer, hvilket er en stor fordel i mange driftsituationer.

3.1.3 Telemetri pipeline

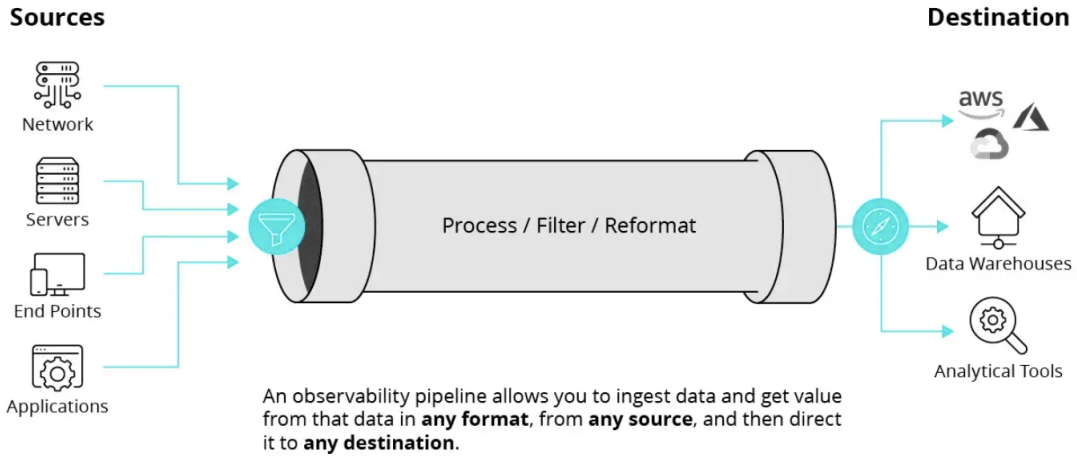
Det anbefales, at IT-serviceorganisationerne etablerer en telemetri- og logpipeline for at håndtere den forskelligartede infrastruktur samt de unikke behov for beskyttelse af personoplysninger, som de enkelte medlemmer bidrager med.

I en telemetri- og logpipeline sendes alle logs og flowdata til en arbejdsnode, der via et centralt regelsæt bestemmer, hvor data, og evt. med hvilke ændringer, skal sendes hen. F.eks. kan en log sendes både til et eksisterende SIEM system og til et nyt centralt system under indfasning. Det er desuden muligt at fjerne henførbare data fra logs, der sendes til den centrale enhed, men stadig sende en kopi til et koldt, lokalt arkiv (evt. hos den enkelte kommune) af hensyn til compliance.



Figur 1 – Eksempel på hvordan loghåndtering kunne se ud, med både en eller flere kommune specifikke log/SIEM systemer og et centraliseret system.

Dette giver løbende driftsfleksibilitet og reducerer risikoen for log-/SIEM vendor lock-in. Telemetri- og logpipelines er bl.a. ifølge Gartner et nøgleelement i opbygningen af centraliseret overvågning, og herunder er vist en funktionel skitse af, hvordan pipelinen fungerer. Der findes en række forskellige tekniske løsninger hertil.



3.1.4 Log- og transportformat standardisering

Alle logs bør leveres i et standardiseret format og transporteres sikkert. JSON eller syslog RFC 5424 anbefales som logformat, og transport bør ske via TLS 1.2 eller nyere. De tekniske minimumskrav, , indeholder konkrete anvisninger for logtransport.

Ukrypteret logtransport via UDP syslog eller telnetbaserede protokoller er generelt ikke acceptabelt i IT-serviceorganisationerne. Logs, der sendes ukrypteret, kan aflyttes og manipuleres, og logs, der ankommer i ustrukturerede formater uden fælles feltnavnskonventioner, kan ikke korreleres effektivt på tværs af kilder. Standardisering er en teknisk forudsætning for effektiv SIEM integration.

3.2 NOC og SOC parathed

NOC- og SOC parathed forudsætter, at det tekniske og organisatoriske fundament er etableret og veldokumenteret, før overtagelsen af driften. Det omfatter en stabil telemetri- og logpipeline, ensartet alarmering samt klare snitflader mellem drift, sikkerhed og eventuelle eksterne leverandører. Overvågningsdata skal være tilgængelige i realtid og af en kvalitet, der muliggør effektiv fejlfinding, hændelseshåndtering og eskalation.

Der skal være definerede drifts- og beredskabsprocesser, herunder klare ansvarsforhold, eskalationsveje og kontaktpunkter, så hændelser kan håndteres konsistent og rettidigt.

Alarmer skal være klassificerede og prioriterede (f.eks. efter kritikalitet og påvirkning; det kan f.eks. omfatte samfundskritisk infrastruktur), så NOC og SOC kan fokusere på relevante hændelser og undgå alarmtræthed.

Samlet set skal paratheden sikre, at både daglig drift og sikkerhedshændelser kan håndteres struktureret, dokumenterbart og i overensstemmelse med gældende compliance- og beredskabskrav.

Det anbefales, at hver kommune gennemfører et SOC/NOC-onboarding forløb, der defineres af IT-serviceorganisationen ift. de services som tilbydes.

3.2.1 Alarmering og NOC-funktion

Alle netværks- og infrastrukturkomponenter bør overvåges via en centraliseret overvågningsplatform med definerede tærskler, eskalationsregler og on-call procedurer. Overvågningen bør være klassifikationsbaseret og differentieret efter systemkritikalitet, så kritiske infrastrukturkomponenter som AD, firewall og VPN behandles med passende prioritet og responstid. Det kan på sigt også omfatte andre services, f.eks. hjemmepleje og varmestyring, som kan være relevante at overvåge. Her bevæger vi os over i observability området, som er en korrelering af netværkskomponenter og server- og dataelementer.

En overvågningsplatform, der alarmerer generisk uden skelnen mellem kritisk og ikke-kritisk infrastruktur, fører til alarmtræthed og langsommere respons på reelle hændelser. On-call procedurer bør dokumenteres med definerede eskaleringsniveauer og kontaktlister, og platformen bør fra starten designes til at understøtte multi-tenant drift.

Som nævnt tidligere bør en AI understøttet model for NOC og SOC kraftigt overvejes, da håndtering af incident ellers vil være vanskeligt at producere i realtid.

3.2.2 Tidsynkronisering

Det anbefales, at alle logkilder leverer, tidsstempler i UTC og synkroniseres fra en fælles, troværdig NTP-kilde. I IT-serviceorganisationens kontekst anbefales det, at IT-serviceorganisationen etablerer interne NTP-servere, der tracker mod en pålidelig kilde, og at alle kommuners systemer synkroniseres mod disse.

Tidsafvigelser mellem logkilder gør det vanskeligt eller umuligt at konstruere en sammenhængende tidslinje under incidentanalyse. Logs, der anvender lokal tidszone, logs uden dato eller systemer, der er synkroniseret mod disparate NTP-kilder, kan afvige med minutter eller mere, hvilket reelt gør korrelation på tværs af systemer upålidelig.

3.2.3 Log opbevaring

Det anbefales, at IT-serviceorganisationerne arbejder med to parallelle lagringslag: varme logs, der er tilgængelige til on-demand-søgning og korrelation i SIEM, og et koldt compliancearkiv med minimum 13 måneders retention i overensstemmelse med NIS2-kravene. Skelnen mellem kolde og varme logs gør det ofte langt mere omkostningseffektivt at opnå den nødvendige retentionstid, som er defineret i kravene.

Varme logs bør være tilgængelige i minimum 90 dage og indekserede til effektiv søgning. Det kolde arkiv bør opbevares på separate og integritetssikrede storageløsninger, adskilt fra produktionsmiljøet, så logs ikke kan manipuleres eller slettes ved et sikkerhedsincident.

Logs og overvågning kan gå begge veje, således kommunerne også kan tilgå egne logs. En konkret mulighed er, at IT-serviceorganisationen bistår med log- og SIEM delen af et lokalt system, mens den enkelte kommune fortsat har driftsansvaret for selve systemet. Der bør ligeledes være beskrevet en proces for, hvordan udlevering af logs foregår til kommunen fra IT-serviceorganisationen i en sådan case. Dette kan evt. teknisk løses via multi-tenancy i logningsplatformen.

Det er vigtigt at understrege, at logs omtalt her kan have både sikkerheds-, drifts- eller auditkarakter. Det er således ikke begrænset til en enkelt kategori af logs, men er i højere grad baseret på en system-til-system vurdering af logbehov.

3.2.4 SIEM implementering

En SIEM løsning er forudsætningen for systematisk sikkerhedsdetektion. Det anbefales, at der implementeres et aktivt og vedligeholdt regelsæt, der dækker alle relevante logkilder, og at korrelationsregler er klassifikationsbaserede og struktureret efter kategorier i MITRE ATT&CK-frameworket for at sikre systematisk dækning af relevante angrebsvektorer. En sådan strukturering er efterhånden de-facto standard i industrien og hjælper med at fastholde en rød tråd i sikkerhedsreaktionen og overvågningen.

3.2.5 Hændelseshåndtering og dokumentation

En formaliseret hændelseshåndteringsproces bør implementeres med definerede roller, eskalations flows og krav til dokumentation. Alle sikkerhedshændelser bør dokumenteres i et ITSM-system med fuld sporbarhed, og NIS2-rapporteringsforpligtelsen bør håndteres med definerede tidsfrister og klare ansvarlige.

Incident Response playbooks for de mest sandsynlige hændelsestyper, såsom ransomware, credential compromise og DDoS (f.eks. i eksamenssituationer), bør udarbejdes. NIS2 stiller krav om tidlig varsling inden for 24 timer, foreløbig rapport inden for 72 timer og endelig rapport inden for 1 måned. Disse

frister er vanskelige at overholde, hvis processen ikke er forberedt, testet og kendt af alle involverede parter.

3.2.6 Driftsmodel

En veldefineret driftsmodel for SOC/NOC-funktionen er en forudsætning for, at fælles overvågning kan fungere i praksis. Modellen bør dokumentere rollefordelingen mellem den enkelte kommune og IT-serviceorganisationen, herunder kommunens ansvar for tilføjelse af logkilder og IT-serviceorganisationens ansvar for detektion og eskalation. SLA-krav, eskalationsveje samt onboarding proces for nye logkilder og ejere bør være klart beskrevet.

3.2.7 Threat Intelligence

IT-serviceorganisationen bør abonnere på relevante threat intelligence feeds, f.eks. sektorspecifikke feeds fra Center for Cybersikkerhed (CFCS) og kommercielle leverandører, og feeds bør integreres direkte i SIEM og øvrige detektionskontroller. IOC'er (Indicators of Compromise) og TTP'er (Tactics, Techniques and Procedures) bør anvendes aktivt til at tilpasse korrelationsregler og prioritere detektionsindsatsen.

Threat intelligence, der konsumeres manuelt af enkeltpersoner og deles i f.eks. en Teams kanal, men ikke integreres i sikkerhedskontrollerne, har begrænset operationel effekt. Under hændelser som SolarWinds og Log4Shell var evnen til hurtigt at vurdere eksponering og iværksætte mitigerende tiltag direkte afhængig af, at Threat Intelligence var integreret i overvågningsplatformene.

3.2.8 Compliance

Compliance er en operationel forpligtelse, der kræver, at de rette kontroller er implementeret, at de virker efter hensigten, og at der foreligger evidens for efterlevelse. For IT-serviceorganisationerne er NIS2-compliance ikke valgfrit, og konsekvenserne af manglende efterlevelse kan være betydelige. Det anbefales at lægge sig op ad standardiserede rammeværker, herunder CIS o.l., i forhold til teknisk opfyldelse af krav.

3.2.9 Audit log-dækning og adgangssporing

Alle privilegerede handlinger, autentifikationshændelser og ændringer i kritiske systemer bør logges og auditeres systematisk. Adgangssporing bør dække samtlige administrative konti, servicekonti og tredjepartsadgange.

Manglende audit logging på privilegerede adgange er en af de hyppigste årsager til, at insiderhændelser og kompromitterede konti ikke opdages eller ikke kan efterforskes effektivt. Hvis det ikke er muligt at efterspore, hvem der oprettede en AD-konto, ændrede en firewallregel eller tilgik et kritisk fagsystem, er der ingen reel sporbarhed af de handlinger, der udgør den største risiko.

3.2.10 NIS2-compliance og rapporteringsparathed

Organisationen bør have fuldt overblik over NIS2-forpligtelser og en operationaliseret rapporteringsproces med definerede roller, interne tidsfrister og skabeloner. Tidlig varsling inden for 24 timer, foreløbig rapport inden for 72 timer og endelig rapport inden for en måned er de centrale frister, og processen bør testes, inden den første gang skal anvendes under reelle omstændigheder.

3.2.11 Kryptografisk asset management

Et komplet register over krypteringsanvendelse, inkl. certifikater, TLS-versioner og cipher suites med udløbsdatoer og ansvarlige, bør vedligeholdes og synkroniseres med CMDB. Certifikatudløb, der opdages, fordi brugere oplever fejl i browseren, er en driftsmæssig og sikkerhedsmæssig svaghed, der kan og bør elimineres via automatiseret certifikatovervågning og fornyelse.

IT-serviceorganisationerne bør desuden begynde at forholde sig til Post-Quantum Cryptography og udarbejde et roadmap, der er afstemt med EU's roadmap og statens vejledning. Der er udsigt til, at dette bliver et reguleret område, og at det finder vej ind i NIS2. Derfor er det relevant at kende den kryptografi, der er i brug, og at kunne skifte kryptografi uden større indvirkning (kryptoagilitet) til en del af infrastrukturdesignet.

3.2.12 Compliance med minimumskrav

De tekniske minimumskrav bør kortlægges fuldt ud og omsættes til konkrete tekniske og organisatoriske kontroller på tværs af alle relevante systemer og driftsdomæner. Det er ikke tilstrækkeligt, at kravene er kendte. De skal mappes til specifikke systemer, have en ansvarlig ejer og en verificerbar implementering.

Compliance status bør verificeres løbende og dokumenteres med evidens, der kan fremvises ved ekstern auditering. For IT-serviceorganisationer med ansvar for mange kommuners infrastruktur er systematisk og dokumenterbar efterlevelse af minimumskravene en grundlæggende forventning fra myndighedernes side.

4 Kategorisering af IT-systemer

En IT-serviceorganisation, der betjener mange kommuner, er afhængig af at have et præcist og opdateret billede af, hvilke systemer der er i drift, hvem der ejer dem, hvilke data de behandler, og hvilken risiko de repræsenterer. Uden dette grundlag er det ikke muligt at træffe drifts- og sikkerhedsmæssige beslutninger på et kvalificeret grundlag, hvilket er afgørende for at styre ændringer kontrolleret og reagere effektivt ved incidents.

Dette afsnit beskriver de anbefalinger, der understøtter en veldrevet systemregistrering, en ensartet klassifikationstaksonomi og en CMDB platform, der fungerer som den autoritative kilde til styrende data på tværs af IT-serviceorganisationens kommuner.

4.1 CMDB og systemregistrering

En CMDB er kun så nyttig som kvaliteten af de data, den indeholder. Et register, der er ufuldstændigt, forældet eller ikke anvendes som styrende kilde for drift og sikkerhed, giver en falsk tryghed. Det anbefales, at IT-serviceorganisationen etablerer klare krav til registreringsdækning og -kvalitet og håndhæver disse teknisk frem for at basere sig på manuelle opdateringsprocesser.

4.1.1 Registreringsdækning og -kvalitet

Alle systemer bør være registreret i CMDB med et komplet og vedligeholdt datasæt, herunder systemejer, klassifikation, driftsansvarlig, datakategori og netværkszone. Det er ikke tilstrækkeligt, at systemer registreres ved nyanskaffelse og derefter ikke vedligeholdes. CMDB data forældes desværre ofte hurtigt i et dynamisk driftsmiljø, og forældede data er i mange situationer værre end ingen data, idet de giver et misvisende grundlag for beslutninger.

Obligatoriske felter bør ikke kunne stå tomme. En ny service bør ikke kunne ibrugtages uden et komplet CMDB opslag, og ændringer i ejerskab, klassifikation eller zoneplacering bør udløse en opdateringsproces. Fuldstændighed bør verificeres jævnligt via automatiserede scanninger mod kilder som Active Directory, netværksregistrering og eventuelt cloud inventar, så systemer, der er idriftsat uden registrering, også opdages proaktivt.

CMDB data bør være den autoritative kilde til systemejerskab, zoneplacering og klassifikation og bør anvendes aktivt af sikkerhed, drift og change management. En CMDB, der kun bruges som opslagsværktøj og ikke som styrende kilde, er et godt stykke ad vejen, men er ikke fuldt modnet til at understøtte IT-serviceorganisationens behov.

4.1.2 Livscyklusstyring og -mærkning

Alle systemer bør mærkes med livscyklusstatus, og der bør være en defineret proces for håndtering af systemer, der nærmer sig end-of-support. EOL dato bør registreres i CMDB for alle relevante systemer, og systemer med end-of-support dato inden for de næste 12 måneder bør automatisk flagges og indgå i en eskalationsproces med en dokumenteret plan for opgradering eller udfasning.

Ingen systemer bør være i produktion i end-of-life-tilstand uden en aktiv og dokumenteret risikoaccept, hvor systemejer og it-sikkerhedsansvarlig er godkendere. En risikoaccept uden udløbsdato og revisionsforpligtelse er ikke en acceptabel forvaltning af et EOL-system. Livscyklusstatus bør indgå som en fast del af den løbende kapacitets- og risikorapportering, så ledelsen har et aktuelt billede af den tekniske gæld i systemporteføljen.

En hyppig udfordring er, at EOL-overblikket er begrænset til serveroperativsystemer (primært Microsoft), mens netværksudstyr, applikationer og middleware ikke er systematisk mærket. Det anbefales, at livscyklusdækningen udvides til alle systemtyper, der er registreret i CMDB.

4.2 Dokumentation

Dokumentation er fundamentet for effektiv drift, struktureret sikkerhedsarbejde og kontrolleret forandringsstyring. Mangelfuld dokumentation er ikke blot en operationel ulempe, men også en sikkerhedsrisiko. Viden, der kun eksisterer i enkeltpersoners hoveder, er sårbar ved personaleskift og kan være vanskelig at anvende effektivt under tidspres.

4.2.1 Netværksdokumentation

Netværksdokumentation bør være komplet, opdateret og versionsstyret. Den bør dække topologi, IP-adressering, VLAN-register, firewall zoner og overgange mellem zoner. Dokumentationen bør ideelt set være synkroniseret med CMDB, og afvigelser bør identificeres automatisk.

Netværksdiagrammer bør opdateres ved alle infrastrukturændringer og versionsstyres centralt. IP-adresseoversigt, VLAN-register og subnetting bør dokumenteres (f.eks. i et IP Address Management, IPAM) og synkroniseres med CMDB, og konflikter samt ikke-tildelte adresser bør identificeres via automatiserede scans. Et netværksdiagram, der ikke opdateres, bliver hurtigt misvisende og kan i en incident-situation lede fejlfindingen i den forkerte retning, hvilket ikke er hensigtsmæssigt i en samlet drift.

Drifts runbooks for kritiske netværksprocedurer bør være tilgængelige offline og løbende opdaterede. Under et cybersikkerhedsincident eller ved simple strømafbrydelser er adgang til systemer og dokumentation ofte begrænset. En offline runbook, der er opdateret og testet, kan være forskellen på en kontrolleret og en kaotisk genopretning.

4.2.2 Sikkerhedsdokumentation

Sikkerhedsdokumentation bør være komplet og vedligeholdt for alle kritiske systemer. Den bør dække trusselovervejelser, sikkerhedskontroller og eventuel risikoaccept. Dokumentationen bør knyttes til CMDB elementerne, så der er en direkte kobling mellem systemregistreringen og sikkerhedstilstanden for det pågældende system.

Alle systemer, der er klassificeret som kritiske, bør have en opdateret sikkerhedsvurdering tilknyttet CMDB'en, herunder kendte risici og afhjælpende kontroller. Risikoaccept for systemer, der afviger fra gældende sikkerhedspolitik, bør dokumenteres med systemejer, godkendelsesdato og eventuel revisionsdato, så det er klart, hvem der har accepteret hvilken risiko, og hvornår.

Sikkerhedsdokumentation bør indgå som en del af change management processen. Væsentlige ændringer bør kræve en opdateret sikkerhedsvurdering inden godkendelse. Dokumentation, der er spredt i projektarkiver og på personlige drev og ikke er knyttet til CMDB, er reelt utilgængelig i de situationer, hvor den er mest nødvendig.

4.2.3 Driftsdokumentation

Driftsdokumentation bør være komplet og vedligeholdt for alle væsentlige systemer og dække driftsansvar, SLA'er, afhængigheder, backup-procedurer og eskalations flows. Runbooks for kritiske driftsprocedurer bør testes og gøres tilgængelige offline.

Alle systemer, der er klassificeret som væsentlige eller kritiske, bør have en opdateret driftsrunbook, der beskriver normale driftsprocedurer, kendte fejlscenarier og eskalations flows. SLA'er bør dokumenteres i CMDB og afspejle den forretningskritikalitet, der er tildelt ved klassifikation, herunder konsekvenserne af nedetid, for eksempel for kritisk infrastruktur.

Driftsdokumentation, der er spredt i e-mails, Teams-filer og personlige drev uden central adgang, er ikke tilgængelig under et incident. Det anbefales, at driftsdokumentation versionsstyres og gennemgås jævnligt, og at "gammel" dokumentation udløser en advarsel i CMDB.

4.3 Klassifikationstaksonomi og -struktur

En klassifikationstaksonomi er grundlaget for at omsætte sikkerhedspolitik til tekniske krav: Hvilken zone skal systemet placeres i, hvilken redundans er nødvendig, hvilke logningskrav gælder, og hvilke adgangskontroller er obligatoriske? For at taksonomien har denne effekt, skal den være fælles, konsistent og obligatorisk.

4.3.1 Ensartet klassifikationsbrug

En fælles klassifikationstaksonomi bør defineres, kommunikeres og anvendes konsekvent på tværs af alle kommuner i IT-serviceorganisationen. Klassifikation bør være obligatorisk, og intet bør kunne oprettes i CMDB uden klassifikation. En klassifikationsmodel med definerede niveauer, f.eks. kritisk, væsentlig, standard og lavkritisk, bør vedtages og dokumenteres med klare kriterier for, hvornår et system tilhører hvert niveau.

Alle CMDB elementer bør kræve en godkendt klassifikation. Klassifikationsændringer bør kræve systemejergodkendelse og logges med tidspunkt og begrundelse, så der er fuld sporbarhed på klassifikationshistorikken.

En klassifikationsmodel, der er vedtaget centralt, men fortolkes forskelligt lokalt, giver et misvisende billede af porteføljens risikoprofil og underminerer de styringsprocesser, der bygger på klassifikationsdata.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

4.3.2 Struktureret CMDB platform

En veldefineret og teknisk solid CMDB platform er forudsætningen for, at registreringsdækning, klassifikation og dokumentation kan fungere som beskrevet. Platformen bør være multi-tenant, understøtte automatisk opdatering via et integrationslag og fungere som den autoritative kilde til styrende data for drift og sikkerhed på tværs af IT-serviceorganisationens kommuner.

CMDB platformen bør konfigureres med en fælles datamodel, der dækker alle kommuner, men med tenant-separation. Data bør opdateres automatisk via integrationer med Active Directory, netværksscanning, cloud platforme, deployment pipelines mv. Manuel opdatering bør være undtagelsen og ikke reglen, da manuel opdatering ofte medfører data, der ikke er løbende opdaterede, og som er inkonsistente.

API-adgang til CMDB data bør være tilgængelig for godkendte interne systemer som SIEM, overvågningsplatform og change management. Det muliggør automatiseret sikkerhedsvalidering baseret på aktuelle registerdata og eliminerer behovet for periodiske manuelle dataeksporter som grundlag for sikkerhedsbeslutninger.

4.4 Netværk og segmentering

Systemklassifikation og netværkssegmentering bør ikke behandles som to adskilte discipliner. Klassifikationen af et system bør direkte bestemme kravene til netværkszone og redundans, og disse krav bør håndhæves teknisk frem for at bero på manuelle vurderinger og lokalkendskab.

4.4.1 Netværkssegmentering baseret på systemklassifikation

Systemplacering i netværkszoner bør være direkte afledt af systemklassifikationen i CMDB. Zoneplaceringspolitikken bør formaliseres og håndhæves teknisk. Et system, der er klassificeret som kritisk infrastruktur, bør kun kunne ibrugtages i den dertil dedikerede zone, og omvendt bør ikke-godkendt udstyr ikke tillades adgang til zonen. Afvigelser herfra bør kræve en eksplicit og dokumenteret godkendelse.

Jævnlige stikprøver bør sammenligne faktisk zoneplacering med CMDB registreringen og flagge afvigelser til review. Change management processen bør kræve en dokumenteret klassifikations- og zoneplaceringsvurdering for alle nye systemer og ved væsentlige arkitekturændringer.

Systemer, der er placeret i forkerte zoner, er ikke blot en politikoverskridelse. De repræsenterer også en sikkerhedsrisiko, da eksponeringsbredden for systemet ikke svarer til det forventede beskyttelsesniveau. Et system med personfølsomme data i gæstenettet er, sat på spidsen, et eksempel på konsekvensen af manglende kobling mellem klassifikation og zoneplacering.

4.4.2 Redundans og kritikalitetsmærkning

Alle systemers redundanskrav bør dokumenteres i CMDB og afledes af systemklassifikationen. Faktisk redundansstatus bør registreres og verificeres, og afvigelser mellem krav og faktisk tilstand bør være synlige og adresseres med en ejer og eventuelt en deadline for udbedring.

Klassifikationsmodellen bør definere eksplicitte redundanskrav pr. niveau. Et system, der er klassificeret som kritisk, bør have et dokumenteret krav om HA og eventuelt dual power som en del af klassifikationsdefinitionen. Redundansstatus bør registreres i CMDB for alle væsentlige og kritiske systemer og verificeres ved jævnlige reviews.

Systemer med kendte redundansmangler i forhold til klassifikationskravet bør være synlige i CMDB og indgå i en adresseringsplan. Et overblik over redundansmangler er relevant for driftsstyring og et nødvendigt grundlag for at prioritere investeringer i infrastrukturrobusthed.

4.5 Automatisering og transition

CMDB data er mest værdifulde, når de er aktuelle, maskinlæsbare og integreret med de systemer, der anvender dem. En CMDB, der opdateres manuelt og kun tilgås via brugergrænsefladen, leverer ikke den strategiske og operationelle værdi, der er mulig. Nedenstående områder beskriver de integrations- og automatiseringselementer, der løfter CMDB fra et register til et styringsværktøj.

4.5.1 Afhængighedskortlægning

Afhængigheder mellem systemer bør kortlægges og registreres i CMDB på et niveau, der muliggør konsekvensanalyse ved ændringer og nedbrud. Data om afhængigheder bør opdateres løbende og anvendes aktivt i change management og incident response.

Alle kritiske og væsentlige systemer bør have registrerede afhængigheder i CMDB, f.eks. databaser, DNS, CRL-services og øvrige infrastrukturafhængigheder. Det bør være muligt at identificere, hvilke services der påvirkes ved nedbrud på et givet system, og change management processen bør anvende afhængighedsdata til automatisk at identificere potentielt påvirkede systemer og ejere ved en planlagt ændring.

Afhængighedskortlægning bidrager til en effektiv incident response. Under et ransomwareangreb er evnen til hurtigt at afgrænse påvirkning og prioritere genopretning direkte afhængig af, at afhængighedsdata er tilgængelige og aktuelle. Uden kortlægning opdages konsekvenser reaktivt, og genopretningen bliver længere og mere kaotisk end nødvendigt.

4.5.2 API-adgang til data i systemregister

CMDB bør eksponere et veldefineret og sikret API, der muliggør integration med IT-serviceorganisationens sikkerhedsplatforme, overvågning og automatiseringsværktøjer. API-adgang bør være rollebaseret, og al adgang bør auditeres.

SIEM, overvågningsplatform og vulnerability management bør integrere direkte med CMDB via API og berige alerts og fund med kontekst som systemejer, klassifikation og zone uden manuel dataindtastning. Automatiserede workflows bør anvende CMDB API til at validere ny infrastruktur mod gældende zoneplacerings- og klassifikationspolitik, inden idriftsættelse godkendes.

En CMDB uden API-adgang er typisk afskåret fra det automatiserede sikkerhedsøkosystem og bliver således mere et opslagsværk. Sikkerhedsplatforme, der ikke kender ejerskab, klassifikation og zone for

de systemer, de overvåger, opererer med et strukturelt blindspot, der er vanskeligt at kompensere for med manuel indsats i en IT-serviceorganisation af den pågældende størrelse.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.

5 Zonemodeller & Zero Trust

En velfungerende netværksarkitektur er forudsætningen for, at et IT-serviceorganisation kan levere sikker og skalerbar drift på tværs af kommuner. Det kræver både en gennemtænkt zoneringsmodel, en pragmatisk tilgang til Zero Trust og en adgangsstyringsmodel, der er forberedt til fælles drift. Dette afsnit behandler de arkitekturelle principper og konkrete anbefalinger, der tilsammen udgør det tekniske fundament for sikker netværksdrift.

5.1 Zonemodel og arkitektur

Effektiv netværkssegmentering kræver mere end blot VLAN-opdeling. En formel zoneringsmodel definerer, hvilke systemer der hører hjemme hvor, hvilke trafikflows der er tilladt på tværs af zoner, og hvem der er ansvarlig for hvert segment. For IT-serviceorganisationer med mange kommuner som medlemmer er dette særligt kritisk, da der både skal være adskillelse mellem kommunernes miljøer og et fælles princip for zoneinddeling internt i hvert miljø.

5.1.1 Zone/segmenteringsmodel

Det anbefales, at IT-serviceorganisationerne etablerer og dokumenterer en formaliseret zoneringsmodel som det arkitekturelle fundament for netværkssikkerheden. Modellen bør operere med klart adskilte sikkerhedszoner, tilpasset de dataklassificeringer og systemer, der befinder sig i hvert segment. Typiske zoner i en kommunal kontekst inkluderer gæstenetværk, DMZ, skolenetværk, administration, OT/IoT, kritisk infrastruktur og management. Disse kan være inddelt i flere subzoner.

For at zoneringsmodellen har reel værdi, kræver det, at den vedligeholdes løbende og ikke blot er et arkivdokument. Alle systemer skal være registreret med zoneangivelse i CMDB, trafikpolitikker mellem zoner skal være dokumenteret i begge retninger, og ændringer i zoneringsmodellen skal gennemgå et formelt change management forløb med en sikkerhedsvurdering inden implementering.

Et centralt element er koblingen til de øvrige dele af sikkerhedsarkitekturen: Zoneringsmodellen skal være i sync med firewallkonfigurationen, og afvigelser fra den godkendte model skal registreres og adresseres systematisk.

5.1.2 Klassifikationsbaseret zoneplacering

Systemplacering i netværkszoner bør være direkte afledt af systemklassifikationen i CMDB frem for at bero på lokalkendskab og ad hoc-vurderinger. Det anbefales, at IT-serviceorganisationerne formaliserer en zoneplaceringspolitik, hvor hvert klassifikationsniveau medfører et defineret krav til netværkszone. Dette behøver ikke at være en omfattende øvelse, da antallet af sikkerhedszoner ikke behøver at være unødigt stort.

I praksis betyder det, at nye systemer ikke kan ibrugtages uden en dokumenteret vurdering af korrekt zoneplacering, og at systemer, der ikke opfylder kravene til korrekt zoneplacering, kræver en eksplicit godkendelse.

5.1.3 DMZ-arkitektur og ekstern eksponeringsstyring

Alle interneteksponerede services bør placeres bag tekniske værn, der reducerer deres attack surface mest muligt. Det inkluderer firewall, WAF, DDoS beskyttelse, geoblokering og loadbalancere. Som udgangspunkt bør ingen service være direkte eksponeret mod internettet uden et relevant udsnit af disse værn.

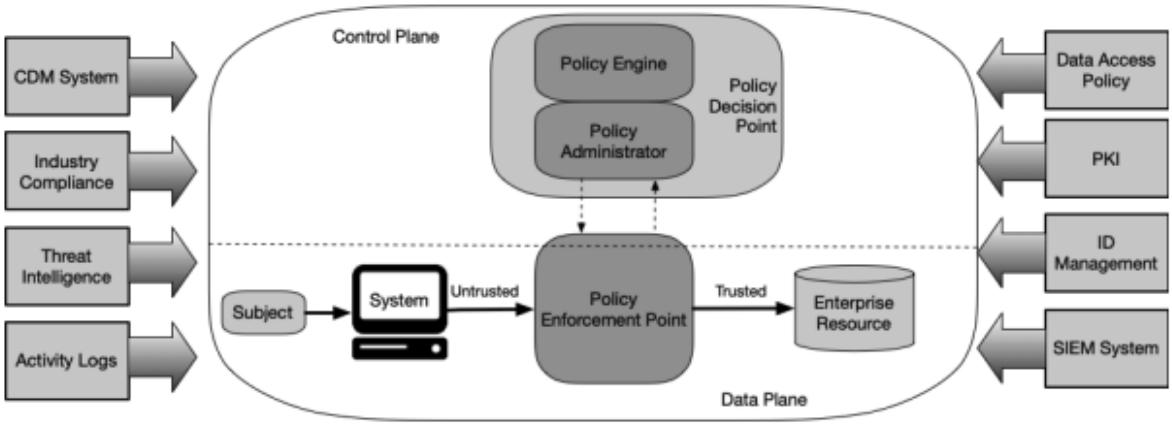
Det anbefales desuden, at IT-serviceorganisationerne implementerer en ekstern attack surface management løsning, der kontinuerligt scanner og alarmerer ved uautoriserede eksponeringer. En ny eksponering uden godkendelse bør automatisk trigge et incident. På den måde opnås et løbende overblik over, hvad der er synligt fra internettet, og uautoriserede eksponeringer opdages hurtigt frem for reaktivt.

5.2 Zero Trust

Zero Trust er et arkitekturprincip, som det anbefales, at IT-serviceorganisationerne designer ud fra: Ingen bruger, enhed eller netværkstrafik er betroet som udgangspunkt, uanset om den befinder sig inden for eller uden for netværksperiferien. For IT-serviceorganisationer, der skal huse mange kommuners data og systemer, er Zero Trust principper særligt relevante, da en kompromitteret enhed i én kommunes miljø ikke må kunne bevæge sig frit over i en anden kommunes services.

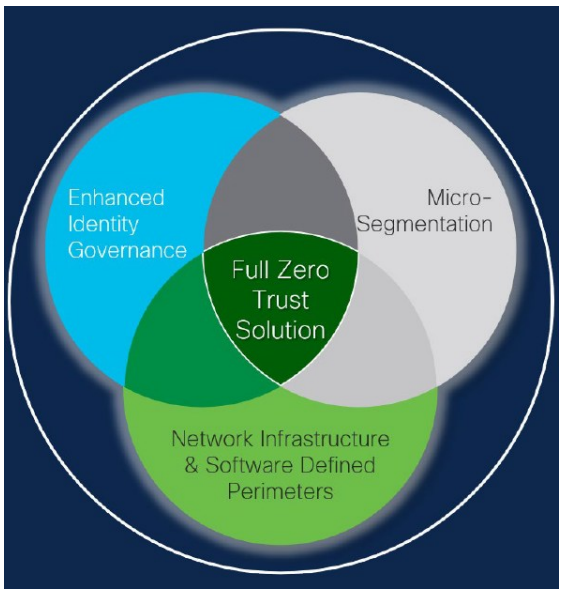
Implementering af Zero Trust sker typisk i mindre etaper og i kombination. Det anbefales, at IT-serviceorganisationerne planlægger en adoptionstakt, der tager højde for den eksisterende infrastruktur og de tekniske forudsætninger hos ejerkommunerne.

Herunder ses NISTs repræsentation af et ZTNA-paradigme. I forhold til IT-serviceorganisationerne er det væsentlige, at der samles en fælles control plane, dvs. en orkestrering af policies, via et (eller et fåtal) centrale PDP (policy decision point), og at den tekniske håndhævelse (Policy Enforcement Point) både centralt og decentralt indeholder de samme høje sikkerhedskapabiliteter på tværs af ejerkommunerne.



Bemærk, at Zero Trust kan tilvejebringes via flere forskellige veje afhængigt af use case og kapabiliteter, f.eks. via softwaredefinerede perimetre eller via stærk identitetsimplementering og TLS-kryptering i

konkrete services. Zero Trust bliver derfor ofte et produkt af en kombination af processer, forskellige tekniske sikkerhedsprodukter og services.



Forskellige områder i forhold til at skabe en Zero Trust-løsning

5.2.1 Identitetssikring af brugere og adgang

Adgang til ressourcer bør baseres på bruger- og eventuel enhedsidentitet frem for netværksplacering. Dette kan etableres på flere måder, og det anbefales, at IT-serviceorganisationerne anvender en kombination afhængigt af det konkrete miljø og den eksisterende infrastruktur. Det er vigtigt at pointere, at teknisk identitetssikring kan foretages på flere måder, der alle er valide. IT-serviceorganisationerne kan overveje at stille flere kapabiliteter til rådighed for ejerkommunerne, som derefter kan vælge den løsning, der er bedst egnet i forhold til konkrete use cases.

Relevante tilgange inkluderer VDI-miljøer, SASE/VPN-overlay i upriviligeret zone samt 802.1X-baseret adgang baseret på enhedscertifikater. En SASE/VPN-løsning, der kræver både bruger- og enhedscertifikat for adgang til interne ressourcer, er en moderne implementering af identitetsbaseret adgangsstyring. Suppleret med en NAC-løsning, der automatisk placerer enheder i dedikerede VLAN, opnås en robust identitetsbaseret adgangskontrol. En VDI-/terminalserverløsning bør som minimum overvejes i forhold til administrationssegmentet.

AI agenter der handler på vegne af brugere, fra laptops eller servere, bør have deres eget identitetsparadigme, da sporbarhed og ansvar eller bliver umuliggjort. Det er ligeledes nødvendigt ift. en korrekte segmenterings model, hvor der ikke opstår et skred af rettigheder.

5.2.2 MFA og Betinget adgang

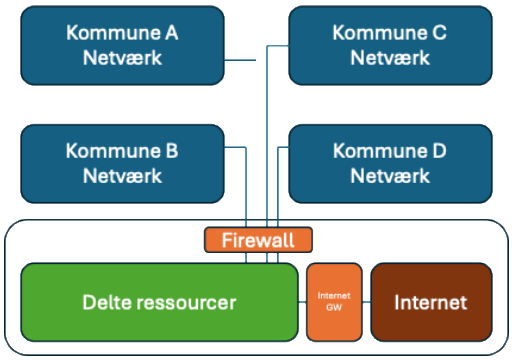
Det anbefales, at der anvendes MFA (Multifactor Authentication) og conditional access på alle væsentlige systemer for alle brugere. Conditional access-politikker bør som minimum kræve MFA og evt. en MDM-registreret (Mobile Device Management) enhed for adgang til alle O365-tjenester og interne applikationer.

Conditional access-politikker bør desuden blokere adgang fra ikke-godkendte lande og fra enheder, der ikke opfylder compliance-krav.

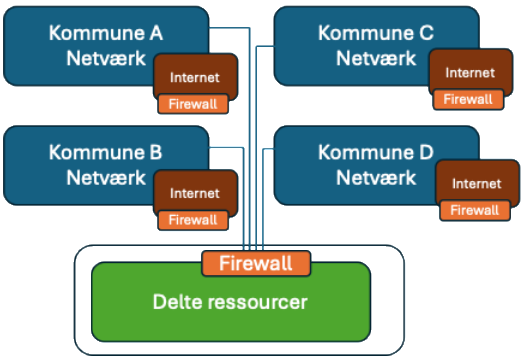
5.2.3 Sikring af trafik

Al netværkstrafik bør inspiceres løbende for identitet, trusler og sårbarheder. Det kræver, at TLS-inspektion er aktiveret på alle udgående og indgående flows, f.eks. via en next-gen firewall eller en SASE løsning, da krypteret trafik ellers udgør et blindspot i detektionen.

Inspektion mod internettet kan foretages enten centralt eller decentralt afhængigt af deployment. Det er væsentligt, at den samme høje sikkerhed implementeres ensartet i begge tilfælde, hvilket stiller krav til sikkerhedsorkestreringen. Begge modeller og/eller hybrider er valide design patterns.



Model med centraliseret internet breakout



Model med decentraliseret internet breakout

Model	Fordel	Ulempe
Central model	Lettere at drifte Lettere at fejlsøge Samme høje sikkerhedsniveau for alle ejerkommuner.	Enkelt stort fejldomæne (HW, SW, DDoS, configuration mv.) Backhaul af alt trafik til centralt knudepunkt kan introducere kapacitetsudfordringer
Decentral model	Robust model med stærk resiliens ift. enkeltnedbrud Individuel og let skalerbarhed ift. de enkelte sites. Sikkerhedsfunktionalitet kan tilbydes decentralt (f.eks. isolering af et lokal CTS netværk)	Mere ressourcetung at drifte, opgradere og på sigt udskifte.

IDS/IPS-signaturer bør opdateres automatisk og dække alle zoneovergange, herunder øst-vest trafik i datacenteret. DNS trafik bør inspiceres og filtreres via DNS sikkerhed med automatisk opdatering af bloklisten fra sektorspecifikke og kommercielle feeds. DNS er en hyppigt anvendt kanal til C2-kommunikation og dataeksfiltration og er derfor både en implementeringsmæssigt lavthængende frugt og et væsentligt sikkerhedsbidrag.

5.2.4 Device trust og endpoint compliance

Alle enheder bør valideres løbende mod definerede compliance-krav som betingelse for netværksadgang. Enhedsidentitet bør være certifikatbaseret og administreres centralt via IT-serviceorganisationets PKI.

I praksis betyder det, at en MDM (f.eks. Intune) compliance-politik kræver opdateret OS, aktiveret BitLocker og aktiv EDR-agent, og at enheder, der ikke opfylder kravene, nægtes adgang via conditional access. 802.1X med enhedscertifikater udstedt fra et fælles PKI anbefales som adgangsbetingelse på alle managed devices, da dette er en enklere implementering. IoT-enheder og lignende bør også behandles under et NAC-paradigme, men det kan variere fra løsning til løsning, hvad der er muligt.

5.3 Adgangsstyring

Adgangsstyring er et af de mest kritiske kontrolområder i en IT-serviceorganisation. En kompromitteret administrativ konto eller en åben gæstezone kan have vidtgående konsekvenser for alle medlemmer. Nedenstående områder danner tilsammen fundamentet for en robust og skalerbar adgangsstyringsmodel.

5.3.1 Gæstenetværk og gæstestyring

Gæstenetværk bør være isoleret i en dedikeret zone med internet only-adgang og ingen adgang til interne ressourcer (jf. minimumskrav). Adskillelsen bør verificeres regelmæssigt frem for blot at bero på konfigurationsantagelser.

Gæsteoprettelse bør ske via en selvbetjeningsportal, evt. med sponsorgodkendelse (for sporbarhed), og med automatisk udløb. Gæstetrafik bør generelt logges inden for lovgivningens rammer (logningsbekendtgørelsen).

Leverandørers serviceadgang bør ligeledes ske via en dedikeret og begrænset zone frem for det generelle interne netværk.

5.3.2 PAM og administrativ adgang

Privilegeret adgang bør styres centralt via en PAM-løsning med just-in-time-adgang, session recording og automatisk adgangskoderotation for alle privilegerede konti og servicekonti. Direkte login med privilegerede konti bør være teknisk blokeret, så al privilegeret adgang sker via PAM-løsningen og dermed er sporbar og tidsbegrænset.

Just-in-time-adgang betyder, at privilegerede rettigheder kun tildeles i et defineret tidsvindue og tilbagekaldes automatisk. Alle privilegerede sessioner bør optages og arkiveres, så optagelserne kan fremvises ved incidentanalyse eller auditering. Delte adminkonti uden individuel sporbarhed bør elimineres.

5.3.3 AD-federering og fælles PKI

Det anbefales, at IT-serviceorganisation etablerer et fælles PKI til at understøtte sikkerhedsfunktionalitet på tværs af kommunerne. Et fælles PKI muliggør certifikatbaseret enhedsidentitet til 802.1X, klientautentifikation og TLS-tjenester uden at kræve et centraliseret AD.

Ejerkommunernes AD-miljøer kan bibeholdes som decentrale services, eventuelt forbundet via AD-federering, hvis det anses fordelagtigt. Det giver brugere mulighed for at tilgå ressourcer på tværs af kommunemiljøer uden separate konti. Der findes i dag flere eksempler på sådanne services, der kræver interkommunalt login til fælles systemer.

Et centralt certifikatstyringssystem integreret med CMDB anbefales, så alle certifikater er registreret med udløbsdato, ansvarligt og tilknyttet system. Reaktiv håndtering af certifikatudløb er en hyppig kilde til driftsforstyrrelser og bør erstattes af automatisk fornyelse og proaktiv monitorering.

5.4 Mikrosegmentering

Mikrosegmentering handler om at begrænse lateral bevægelse inden for netværket: Selv hvis en angriber opnår fodfæste i et system, bør vedkommende ikke frit kunne bevæge sig til øvrige systemer. Det er særligt relevant i IT-serviceorganisationer, hvor mange kommuners workloads befinder sig i på den samme driftsplatform.

5.5 Workloads i datacenteret

Workloads på driftsplatformen bør mikrosegmenteres med eksplicitte tilladelsespolitikker for al øst-vest trafik. Udgangspunktet bør være, at ingen server kan kommunikere med andre servere uden en godkendt trafikpolitik. Det kræver, at alle applikationsflows er kortlagt og dokumenteret, inden segmenteringspolitikken implementeres.

En SDN-løsning med distribueret firewall muliggør håndhævelse af trafikpolitikker direkte på hypervisor-niveau uafhængigt af VLAN-design. Det giver en granularitet, der ikke kan opnås med traditionel VLAN-baseret segmentering, og det begrænser ransomware spredning effektivt: En kompromitteret applikationsserver kan ikke nå øvrige workloads uden en eksplicit godkendt trafikpolitik.

5.6 Deny by default

Deny by default bør implementeres som grundprincip på tværs af alle zoneovergange og segmenter. Det betyder, at alle firewallpolitikker er whitelist-baserede, at der ikke eksisterer brede any-any regler, og at al trafik, der ikke eksplicit er godkendt, blokeres og logges.

Nye kommunikationsflows bør kræve en formelt godkendt firewall change request med dokumenteret forretningsbegrundelse og systemejergodkendelse inden implementering. Regelsættet bør gennemgås kvartalsvist for overflødige og forældede regler, og ubrugte regler bør automatisk flagges til review. Et ukontrolleret voksende regelsæt er vanskelig at auditere og øger risikoen for utilsigtede åbninger.

Den gældende version af materialet er den publicerede PDF, stillet til rådighed af KL/Conscia.