UiT Norges arktiske universitet

Retningslinje for IKT-sikkerhetsarkitektur

Fastsatt av:	IT-direktør	Dato:	16.01.2023
Ansvarlig enhet:	ADM/ITA	Id:	
Sist endret av:		Dato:	
Erstatter:	Ny	Arkivref.:	2023/965

Formål
Formålet med denne retningslinjen er å definere en overordnet arkitektur som legger til rette for at UiT kan beskytte sin informasjon og sine informasjonssystemer på en formålstjenlig måte. Viktige elementer innen informasjonssikkerhet er

- Konfidensialitet (informasjon er bare tilgjengelig for de som skal ha tilgang).
- Integritet (informasjon er korrekt og fullstendig).
- Tilgjengelighet (informasjon er tilgjengelig innenfor de krav som er satt).

Retningslinjen må ses i sammenheng med Ledelsessystemet for informasjonssikkerhet og personvern. Teksten har sitt utgangspunkt i Uninetts (nå SIKT) UFS nr. 122 fra 2009.

IKT-sikkerhetsarkitekturen skal tilfredsstille følgende overordnede krav:

- Sikkerhets- og risikonivåer skal være forankret i ledelsen og basert på vurderinger av risiko og sårbarhet (ROS-vurderinger)
- De tekniske løsningene skal oppfylle kravene som stilles i Ledelsessystemet
- Det skal tas hensyn til relevante regulative krav og veiledere, samt NSMs grunnprinsipper for IKT-sikkerhet.
- Sikkerhetsarkitekturen skal understøtte institusjonens formål og målsetninger som fastlagt i universitetsloven, samt institusjonens forhold til tredjeparter.
- De tekniske løsningene skal ha tilstrekkelig kapasitet og motstandsdyktighet mot feilsituasjoner (redundans).
- De tekniske løsningene skal ha tilstrekkelig høy kvalitet.

Virkeområde
Retningslinjen gjelder hele UiT

Ansvar, myndighet og oppgavefordeling
IT-direktør: Fastsetter og vedtar denne retningslinjen.
It-avdelingen: Ivaretar at rutiner for it-systemer og -tjenester er i overenstemmelse med denne retningslinjen.
CSIRT/operativ sikkerhetsgruppe: Årlig revisjon av denne retningslinjen.

Definisjoner og forkortelser

(Det meste defineres fortløpende i teksten.)

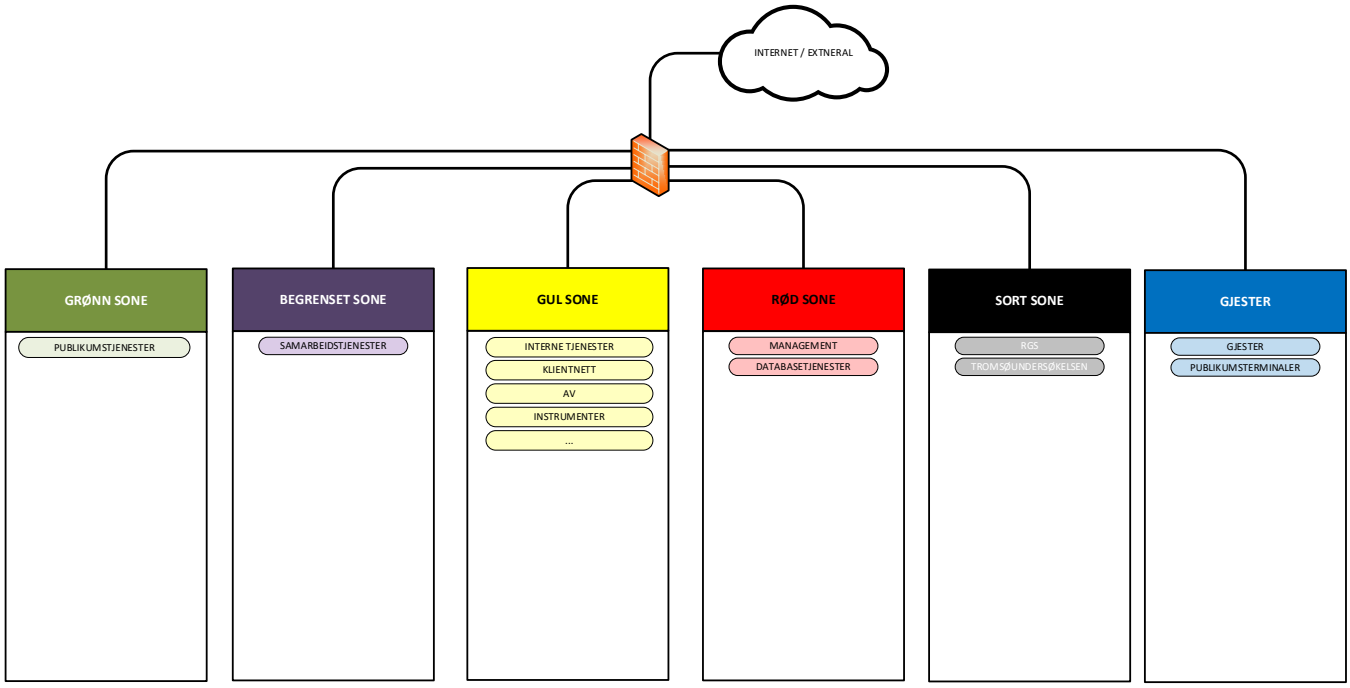
Sikkerhetsarkitekturen er basert på følgende prinsipper:

- Nettet skal deles inn i **soner** og **sikkerhetsklasser**.
- Det skal finnes et klart skille mellom tjenere og klienter.
- Tjenere og klienter skal plasseres i relevante sikkerhetsklasser med tilhørende interne sikkerhetstiltak basert på risiko- og sårbarhetsvurderinger (ROS-vurderinger).
- Tilgangen til tjenester skal reguleres gjennom bruk av **sikkerhetsbarrierer**.
- Alle tjenere og klienter skal behandles etter de samme prinsipper uavhengig om det er fysiske maskiner eller virtualiserte systemer og om de er satt opp i lokal infrastruktur eller skytjenester.

Inndeling i soner, sikkerhetsklasser og segmenter

- Inndeling i soner og klasser skal være basert på ROS-vurderinger.
- Systemeier er ansvarlig for klassifisering og plassering av systemet.
- Inndeling i **soner** skal benyttes som et prinsipp for sikkerhetsarkitekturen. En sone definerer et minimums sikkerhetsnivå. UiT har identifisert følgende soner: *Åpen* (grønn), *begrenset*, *intern* (gul), *fortrolig* (rød), *strengt fortrolig* (sort) samt en egen sone for *gjester*. Disse er i hovedsak navngitt og fargekodet etter mønster fra konfidensialitetsklassene i Retningslinje for klassifisering av informasjon ved UiT. Begrenset sone er et spesialtilfelle som ikke matcher en enkelt konfidensialitetsklasse.
- En sone har i utgangspunktet ikke tilgang til en sone med høyere sikkerhetsnivå med mindre det er eksplisitt tillatt.
- En sone med høyere sikkerhetsnivå har ikke nødvendigvis tilgang til en sone med lavere sikkerhetsnivå.
- Hver sone vil inneholde ett eller flere **nettverkssegmenter** (f. eks vlan)
- Nettverkssegmenter innenfor en og samme sone kan ha forskjellige krav til sikkerhet. Segmenter innenfor en sone som har felles krav til sikkerhet kan grupperes i en **sikkerhetsklasse**.
- Nettverkssegmenter i samme sone eller sikkerhetsklasse er ikke nødvendigvis fullt tilgjengelige for hverandre.
- Enheter i samme sikkerhetsklasse er ikke nødvendigvis tilgjengelig for hverandre.

LOGISK INNDELING AV SIKKERHETSSONER OG SIKKERHETSKLASSER I NETTVERKET VED UIT



UiT Norges arktiske universitet

REVIDERT: 13.01.2023 10:21

Sikkerhetsbarrierer

En sikkerhetsbarriere er en samling av premisser som må tilfredsstilles for å få tilgang til ressurser i en gitt sone eller sikkerhetsklasse. Sikkerhetsbarrieren kan bestå av ett eller flere av følgende elementer (listen er ikke uttømmende):

- brannmur
- pakkefilter på ruter
- applikasjonsportnere, slik som proxyer, jumphost og terminaltjenere
- autentiseringsløsninger
- VPN-løsninger
- krav til klienter
- krav til tjenere

I tillegg kommer ansvarliggjøring av brukere ved hjelp av administrative tiltak, herunder retningslinjer, rutiner og lignende.

Anvendelser av soner

Sonebegrepet beskriver i første rekke hvordan trafikk skal begrenses *inn* mot utstyr i sona. De videre sikkerhetsklassene innenfor hver sone vil i tillegg beskrive hvordan trafikk skal begrenses *ut* fra sona og mot f.eks. Internett.

0	Åpen (grønn)	Publikumstjenester. F.eks. web, DNS, NTP, studentforeninger. Tilgjengelig for Internett.
1	Begrenset	Tjenester som kun skal nås av eksterne samarbeidspartnere, f.eks. BAS, UH-AD, instrumenthotell, tjenester for Samas
2	Intern (gul)	Virksomhetsinterne nettverkssegmenter som brukes av ansatte og andre som er tilknyttet institusjonen. F. eks. interne tjenere, klienter, skrivere, AV, instrumenter. Kan ikke nås direkte fra maskiner utenfor institusjonen
3	Fortrolig (rød)	Kritiske systemer, dvs. systemer som håndterer fortrolige personopplysninger eller virksomhetskritisk informasjon. F. eks databaser, management, OT-utstyr
4	Strengt fortrolig (sort)	Strengeste sikkerhetsnivå. Brukes unntaksmessig. F. eks. RGS
5	Gjester	Nett vi tilbyr og drifter for gjester og partnere som ikke er en del av institusjonen. Utstyr i sona skal ikke ha noen rettigheter inn mot UiTs interne soner. F. eks. gjester, publikumsterminaler

Ved innføring av IPv6 vil det bli lagt tekniske sperrer slik at trafikk fra Internett ikke kan slippe inn til sikkerhetssone 2-4 (gul, rød, sort). Vi vil derfor velge å implementere dette strengt også for IPv4.

Krav til tjenere
Disse er beskrevet i egen retningslinje. Stikkord fra denne er at alle tjenere skal ha god systemadministrasjon slik som sikkerhetsoppdateringer, stopp av unødvendige tjenester, lokal herding, lokal brannmur og sentralisert logging.

Krav til klienter
I alle soner skal klienter skilles fra dedikerte tjenere, dvs. at klienter og tjenere skal befinne seg i forskjellige nettverkssegmenter. Klienter vil videre deles inn i sikkerhetsklasser der hver enkelt klasse kan ha ytterligere krav til klientene. F. eks "ansattnett" der alle maskiner skal være sentralt administrert. Disse kravene er beskrevet i egne retningslinjer.

Autentisering og tilgangskontroll
Med tilgangskontroll forstås en sikkerhetsbarriere en klient må passere for å få tilgang til ressurser i en spesifikk sone og sikkerhetsklasse.

Som overordnete prinsipper gjelder følgende:

- Tilgang skal gis bare etter behov
- Det skal foreligge tilstrekkelige mekanismer for logging og sporbarhet.

Krav til mekanismer innenfor de ulike soner og sikkerhetsklasser ligger i egen retningslinje

Referanser
Ledelsessystem for informasjonssikkerhet: https://uit.no/sikkerhet