Aarhus Universitet

# Bilag 3 – Kundens It-miljø (Kundens eksisterende Infrastruktur)

Drift af Security Operations Centre (SOC)

Aarhus Universitet

# Indholdsfortegnelse

# 1. INDLEDNING

I nærværende bilag beskrives Kundens It-miljø.

Beskrivelsen understøtter Leverandørens opfyldelse af Kontrakten. Beskrivelsen af Kundens It-miljø indeholder ingen selvstændig kravsætning til Leverandøren.

Ved underskrift af Kontrakten beskrives Kundens It-miljø, således som det eksisterer forud for kontraktindgåelsen, herunder hos den Afgivende Leverandør. Beskrivelsen af Applikationen i dette Bilag 3 anses efter kontraktindgåelse som en del af Dokumentationen.

# 2. KUNDENS IT-MILJØ

Nedenfor er en beskrivelse af Kundens it-miljø, både overordnet og med en række detaljer. Bemærk, at der sidst i beskrivelsen er en liste med eksisterende funktionalitet og infrastruktur, der har speciel relevans.

## 2.1 Overordnet teknisk beskrivelse af Kundens It-miljø

Kundens it-afdeling, AU IT, driver Kundens netværksinfrastruktur, identitetsstyring (IdM og AD) og administrative systemer (Studieadministration, HR, Web, ESDH, Økonomisystem, Servicebus, fil, print). Desuden understøtter AU IT forskning og undervisning med en e-læringsplatform (LMS) og en samarbejdsplatform (Microsoft 365). Endelig driver AU IT en lang række servere og services for forskere og studerende.

Rent teknisk har AU IT egne datacentre bygget omkring VMware (virtualiseringsplatform, virtuelt netværk og virtuelle firewalls), Cisco (fysisk infrastruktur) og F5 (loadbalancer). Her drives Microsoft Windows, Linux og Oracle. Datacentrene rummer også storage til filservice.

Kundens netværksinfrastruktur er på samme måde som i datacentrene bygget omkring Cisco. Desuden benyttes Microsoft Azure (med M365/Dynamics og servere/services) og Amazon AWS (servere og services) som cloudleverandører.

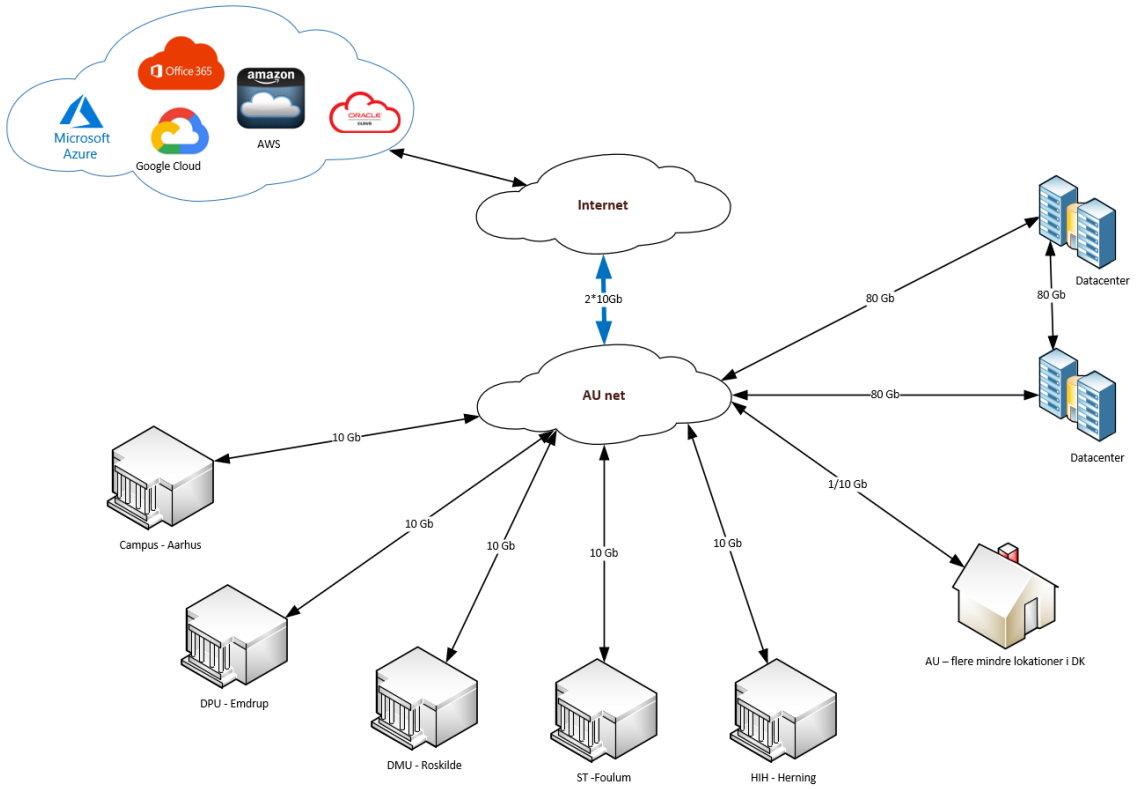
Kunden benytter for nuværende Graylog som log-management løsning. Denne indsamler logdata fra udvalgte kilder som AD/DC, Exchange, F5 loadbalancer, FW, router, switche, Access Points, Cisco Umbrella og Windows Defender AV.

Nedenfor beskrives Kundens miljø i tal og med flere detaljer.

## 2.2 Netværk overordnet

### *2.2.1 Internetforbindelser*

Kunden har en traditionel internetforbindelse via DeiC. Alle lokationer kan tilbydes alle tjenester og alle netværk igennem denne infrastruktur. Internetforbindelsen er på 2 x 10 Gb/s. Alle eksterne lokationer er forbundet med enten sort fiber eller kapacitetsforbindelser.




Figur: Kundens netværk

Aktive netporte: 45.000.

### *2.2.2 Trådløst netværk*

Det trådløse netværk er etableret med en central controllerbaseret Cisco løsning:

- WiFi AP: 4.000.

Dagligt har Kunden imellem 20.000-25.000 klienter på trådløst netværk, samtidigt.

### *2.2.3 DHCP*

Kunden foretrækker og benytter DHCP til alle endpoints, men håndterer også undtagelser.

### *2.2.4 VPN*

Adgang til Kundens netværk er via en Cisco VPN-løsning.

## 2.3 Klienter og klientnet

Ansatte er forbundet med netværket via 802.1x og er på forskellige vlan alt efter brugerens arbejdsopgaver.

Studerende har kun adgang til trådløst netværk via. Eduroam SSID.

Forskningsenheder er segmenteret på baggrund af fakultet og formål.

Klienterne er Windows (Windows 7 og frem), macOS og forskellige udgaver af Linux.
Der benyttes også VDI, dels på en VMware Horizon platform og dels i Azure.

Antallet af klienter:

- Windows maskiner: 13.500.
- Mac maskiner: 3.100.
- Linux maskiner: 250
- VDI: 100

## 2.4 Brugere

Antal af ansatte regnet i FTE (Full Time Employee): 8.300
Antal studerende: 38.000

## 2.5 Identity Management

### *2.5.1 NetIQ IdM*

Kunden har en Identity Management løsning, der på baggrund af data fra studieadministrative og HR-systemer vedligeholder et samlet overblik over personer med behov for adgang til it-services ved Kunden.

## 2.6 Servere

Kunden har omkring 1.600 virtuelle servere kørende på VMware fordelt på 49 fysiske hosts med 2 PB storage. OS er Windows (Windows 2012 og frem) og forskellige Linux versioner. Total har Kunden omkring 100 fysiske servere.

Kunden har desuden 11 Oracle SPARC S7 servere.

## 2.7 Backup

Kunden har backup leveret som SaaS.

## 2.8 Cloud

Azure er primær cloud mens andre cloududbydere benyttes i mindre omfang.
Kunden har en VPN-forbindelse mellem Kundens netværk og visse af Kundens services i Azure.

## 2.9 ID og login

Kunden bruger on-premise og Azure AD og med MFA. Kunden har ét AD domæne. Alt efter hvilke rettigheder en bruger skal have, kan det kræves at brugeren har flere konti.

Antallet af konti i AD:

- 70.000 brugerkonti
- 300 administrative konti (til medarbejdere i drift og support – funktionsadskillelse)
- 650 servicekonti.
- 150 gMSA konti.

## 2.10 Service Management system

Kunden benytter Cherwell som internt Service Management system.

## 2.11 Softwarefunktionalitet og infrastruktur med relation til SOC'en

Nedenfor er der fremhævet software og infrastruktur, der har specielt relevans for SOC'en.

### *2.11.1 Eksisterende softwarefunktionalitet*

Kunden har en Microsoft platform og herunder specifikt en A5-aftale, der dækker nøglekomponenterne

- MS Defender for Endpoint
- MS Defender for Identity
- MS Defender for O365 (Plan 1 & 2)
- MS Defender for Cloud Apps
- Microsoft 365 Defender

Derudover har Kunden MS Sentinel som SIEM/SOAR-platform.

Til MDM (Mobile Device Management) benyttes Microsoft Intune.

### *2.11.2 Eksisterende infrastruktur*

Kundens netværksinfrastruktur består af følgende hovedkomponenter:

- Cisco Catalyst switch netværk
- Cisco Firepower platform (NGFW) med understøttelse af IDS/IPS, avanceret malware detektering, URL-filtrering
- F5 load balancer
- VMware NSX-T firewall
- Cisco ASA klassisk Edge firewall
- Cisco DNS beskyttelse i form af Cisco Umbrella

Netværket påtænkes udbygget med:

- Cisco DNA-center samt Cisco SDA

Dette gøres på baggrund af et ønske om identitetsbaseret netværk.

### *2.11.3 Kundens SOC*

Kunden SOC er bemandet på hverdage fra 8-16 og håndterer kommunikationen internt ved Kunden. For nuværende består Kundens SOC af 2 fuldtidsansatte personer samt 2 tilknyttede personer, der deltager i SOC'en efter behov indenfor deres specialer.