Anskaffelse av sikkerhetsovervåking for Kragerø kommune

Fra Netsecurity

Kins Tech 2023

Adam E. Moen, IT-sjef, Kragerø kommune

Frank Kirkeng, Secure Operations Manager, Netsecurity

Kragerø kommune

10351 innbyggere

495 øyer, holmer og skjær og 4 000 fritidsboliger

IT-drift i Kragerø kommune

- 5 ansatte + 1 lærling + 1,5 prosjektleder
  - 1300 ansatte og 1000 elever/studenter
  - 700 PC og 1100 Chromebooks
  - 500 Mobiler og 150 Nettbrett
  - 50 lokasjoner på sort fiber
- Drifter selv (08:00-15:30)

IT i Kragerø kommune

- 70+ hoved fagsystemer
  60% leveres som sky (SaaS)
  med mål om 90% innen 3 år
- Cisco Meraki
  (sky adm. nettverk)
- Microsoft 365 +
  Google Workspace i
  skolene

IT-sikkerhetsovervåking Anskaffelse høsten 2022

- Innkjøpskontoret AS
  - Kravspek basert på NAV anskaffelse
- 24/7 SOC, SIEM og IRT
- 3 leverandører ga tilbud
  - Netsecurity ble valgt
- Kontrakt skrevet 1.12.22, løsning ferdig implementert 1.1.23

Viktige momenter i anskaffelsen

- **SOC med Aktiv respons**
- Etablerings tiden
- Kompetanse på tilbudt personell
- Garantert responstid
- **Fast pris (ikke per TB logg data)**
- SLA med god betingelser
- SOC i Norge
- Effektiv etablering
- Automatiserte rutiner

Hva overvåker Netsecurity?

Endepunkt

- Cortex XDR klient
  - Overvåker og Analyserer all aktivitet på klient og server
  - Sårbarhetsanalyse av endepunkter
- Respons verktøy

Identitet

- Brukeraktivitet
  - lokal AD
  - Microsoft 365 + Google
- Defender for Office 365
  - Safelink aktivitet

Andre overvåkende tjenester

- Cortex Datalake
- Cisco Meraki
- Cisco Umbrella (OpenDNS)
- Fortigate
- S3 Backup

Leveransen inneholder også

- Hendelsesrapportering (via Teams)
- Månedlig statusmøter
  - Rapport med fokus på anomaliteter
- Dedikert konsulent for oppfølging

24/7-365 Netsecurity Respons

- Isolering av endepunkt (XDR agent)
- Utlogging av Office 365 brukersesjon
- Tvinge passordbytte On-prem AD (og Azure Identity)
- Skanne endepunkter
- Blokkere indikator (filhash, ip, domene etc
- Blokkere applikasjoner
- Blokkere/unblockere brukerkontoer
- Varsle

- E-post Phising Respons tjeneste

Erfaringer med Netsecurity så langt

- Etablering gikk fort (under 1 måned)
- Svært dyktige og kompetanserike
- Lærerikt
- Flere mindre hendelse avverget
- 1 stor hendelse for 1 virksomhetsleder avverget

Takk for meg