Intervjue med NTNU SOC:

- Spørsmålet om hvordan sikkerhetsdata defineres og prioriteres blir stilt.
    - Sikkerhetsdata prioriteres basert på dekning av en angrepskjede for å sikre etterforskning av potensielle innbrudd eller misbruk. Viktige data som samles inn inkluderer autentiseringsdata (innlogging, utlogging, skalering av privilegier), samt data om programaktivitet på maskiner. I tillegg overvåkes nettverksaktivitet gjennom IDS (Intrusion Detection Systems) og brannmurer som logger angrep.

- Hvor lenge logger lagres?
    - det påpekes at lagringsperioden varierer. Personverdloven er relevant, og lovgivningen krever en rettslig grunnlag og et klart formål med datalagring. Diskusjonen inkluderer også en anbefaling om at personopplysninger lagres mellom 6 til 18 måneder, avhengig av om dataene er anonymiserte eller dekoblet.
    - GDPR nevnes ikke som en begrensning på lagringstid men fokuserer på lovhjemmel og formål for datainnsamlingen. Så lenge formålet med datalagringen er gyldig, er også lagringen tillatt. Eksempelvis, data om studenter ved NTNU oppbevares så lenge de er aktive studenter for å kunne administrere deres eksamener og utdanning.
    - Det påpekes at sikkerhetslogging er essensielt for å kunne bevise integriteten og konfidensialiteten i datasystemer. Selv om GDPR introduserer strenge regler for personvern, tillates det unntak for driftsmonitorering og sikkerhetslogging som er nødvendig for å opprettholde sikkerheten.

- Hvilke teknologier og verktøy som brukes for å overvåke og analysere sikkerhetslogger?
    - Open Search, en open source-versjon av Elasticsearch, brukes for å håndtere store datamengder og distribuere indeksering og søk over flere servere. Dette sammenlignes med praksisen i Horten kommune og Gjøvik kommune, som bruker forskjellige systemer for sikkerhetslogging.

- Kostnadene ved å bruke eksterne versus interne løsninger for datalagring?
    - NTNU, hvor intervjuobjektet er tilknyttet, foretrekker interne løsninger fordi det er mer kostnadseffektivt sammenlignet med skytjenester som Microsoft eller Amazon.
    - Det forklares at de bruker PCI-disker, som gir høy ytelse -REDACTED- per disk, noe som reduserer behovet for personell og akselererer dataanalyse. Dette bidrar til kostnadseffektivitet sammenlignet med eksterne skytjenester, og det anslås at maskinen vil koste -REDACTED- årlig over en -REDACTED- periode.

- Kostnader og ytelse ved å bruke interne løsninger sammenlignet med skytjenester.
    - Det pekes på at selv om skytjenester kan virke som en konkurransedyktig løsning, kan interne løsninger være mer kostnadseffektive og gir bedre kontroll over sikkerheten, spesielt for sensitive data.

- Hvordan NTNU beskytter personopplysninger i sine logger.
    - De følger interne retningslinjer for tilgangskontroll, hvor kun autoriserte personer har tilgang til loggene. Det er et hierarki og deling av tilgang basert på ansattes rolle og nødvendighet for å se visse typer loggdata. Dette sikrer at sensitiv informasjon forblir beskyttet og at tilgangen er strengt regulert.
    - Det blir forklart hvordan NTNU håndterer spesifikke sensitive felter i loggene ved å kryptere dem, slik at de ikke kan leses av uautoriserte personer. Dette gir en ekstra sikkerhetslag og hjelper til med å opprettholde personvernet.
    - logganalyse er sentralt i å oppdage, håndtere og forhindre sikkerhetshendelser. Loggføringen tillater dem å spore og analysere sikkerhetstrusler effektivt, og er avgjørende for å forstå hendelsesforløp og tilpasse sikkerhetstiltak. Det nevnes

også hvordan de håndterer falske alarmer (false positives), som er vanlig i systemer med omfattende logganalyse.

- Hvordan NTNU håndterer sikkerhetsvarsler, inkludert hvordan de loggfører og reagerer på hendelser, samt justering av deres sikkerhetssystemer for å unngå falske positiver.
    - Dette innebærer å finjustere regelsett og bruk av automatisering for å effektivisere håndteringen av sikkerhetshendelser.

- Er det spesifikke sikkerhetshendelser og utfordringer NTNU står overfor?
    - Han nevner at universitetet har hatt store sikkerhetssaker som har involvert utestengelse av personer, men detaljer om disse sakene kan ikke diskuteres.

- Hvordan NTNU planlegger å møte fremtidige sikkerhetsutfordringer ved å implementere en ny modell for logganalyse?
    - Dette vil involvere bruk av mikroanalyser basert på spesifikke loggkilder for å forbedre nøyaktigheten og redusere antall falske positiver. Automatisering og eskalering av prosesser nevnes også som nøkkelstrategier for å håndtere det store volumet av loggdata mer effektivt.

- Hvordan har dere tolket og tilpasset dere til nasjonale og eventuelle internasjonale retningslinjer?
    - De følger en rekke standarder, inkludert ISO-27001 og ISO-27002, samt NSM's grunnprinsipper for IKT-sikkerhet og NISTs cybersecurity framework. Det nevnes også at de forholder seg til sikkerhetsloven, e-forvaltningsloven, og

personvernloven (GDPR), samt et nytt direktiv kalt NIST-2 som vil bli implementert i norsk lov. Deres styringssystem, som er basert på ISO-27001, inneholder strenge krav som former deres retningslinjer og politikk rundt sikkerhetslogging.

- Hvordan evaluerer dere effektiviteten av deres sikkerhetslogging og overvåkningspraksiser?
    - Det blir besvart med at de ikke direkte måler effektiviteten basert på loggdata alene. I stedet gjennomfører de en "after action review" etter hendelser for å identifisere eventuelle mangler i dokumentasjon, logging, eller uklarheter. Dette fører til en evaluering av hva som fungerte bra og hva som kunne forbedres, og funnene fra disse gjennomgangene brukes til å forbedre deres deteksjonsmekanismer.

- hvordan gjør NTNU vurderinger etter hendelser for å forbedre sikkerhetslogging og overvåkning.
    - De utfører ikke penetrasjonstester (pentests) regelmessig som en del av deres standard praksis, men fokuserer på kontinuerlig sårbarhetsscanning av sitt nettverk. De nevner bruk av Microsofts angrepsrammeverk og rapporter om trusler for å sikre at de er forberedt på kjente teknikker brukt i cyberangrep.
    - NTNU holder seg oppdatert om de nyeste truslene og sikkerhetstrender gjennom ulike kanaler. De bruker informasjon fra hendelsesrapporter og trusler for å justere sine sikkerhetslogging og alarmberedskap. Dette hjelper dem å sikre at de har dekning for aktuelle trusler i deres alarmeringssystem.

- Hvordan håndterer NTNU falske alarmer og sikrer at ekte trusler ikke overses.
    - De understreker viktigheten av å ikke frykte å deaktivere irrelevante alarmer og å gjennomgå alarmer regelmessig for å vurdere deres relevans. Det nevnes også at

effektiv loggehåndtering innebærer selektiv logging der kun relevant data lagres, og unyttig data kastes etter en kort periode, typisk etter syv dager.

- hvordan automatiserer NTNU sletting av data som ikke lenger er nyttige eller nødvendige.
    - De opprettholder loggdata for en kort periode for operasjonell bruk, og deretter blir data som ikke lenger er relevante slettet automatisk. Automatisering spiller en nøkkelrolle i å sikre at datahåndteringsprosesser ikke er avhengige av manuell inngripen.

- Diskusjonen avslutter med hvordan NTNU sikrer at deres sikkerhetspersonell har nødvendig opplæring og kompetanse for å håndtere sikkerhetshendelser
    - De organiserer interne seminarer kalt -REDACTED- hvor ansatte kan dele kunnskap og diskutere komplekse sikkerhetssaker. De legger også stor vekt på kontinuerlig profesjonell utvikling gjennom tilgang til faglitteratur, deltakelse i virtuelle toppmøter og tekniske kurs.

Horten kommune intervju oppsummering:

- Kan du beskrive Horten kommunes generelle tilnærming til sikkerhetslogging?
    - Hva slags logger de lagrer:
        - standardiserte ADR-logger: Endringer til filer, nettverk, registerendringer, prosesser og den aktiviteten som typisk kommer fra ADR.
        - Sikkerhetslogger for både PCer og klienter lagres på servere.
        - De implementerer audit policies for å logge både feilede og vellykkede påloggінger.
        - Skylogging: De lagrer også skyllogging som inkluderer data relatert til identitet og pålogging som er inkludert i Microsoft.
        - Nettverkslogging: gjennom brannmur

        - Possisjonslogging: denne funksjonen er inbygget i NTRA-ID eller HR-radet.
        - E-poster logges kun med headerinformasjon som avsender, mottaker, emnefelt og IP-adresse.

    - Hvordan personvern balanseres med loggaktiviteter i horten kommune (Hvor mye data blir logget):
        - loggene primært lagrer metadata og ikke innholdet av kommunikasjon som e-post eller nettverkstrafikk. Tilgang til loggene er begrenset til autoriserte personer, og loggene gjennomgås ikke rutinemessig, men kun ved spesielle anledninger.

- Hvordan har dere prioritert hva som skal logges, og hvor lenge det skal logges? Og hvordan balanserer dere dette mot personverns krav?
    - Prioriteringen av hva som skal logges baseres på Microsofts beste praksiser, og innsikter fra penetrasjonstester. Balansen mellom logging og personvern er viktig, og de følger personvernsforordningen som tillater lagring av persondata for tekniske og sikkerhetsmessige formål.
    - Han påpeker at selv om de har muligheten, logges ikke unødvendig persondata, og det er strenge retningslinjer for hva som kan gjøres med de innsamlede dataene.
    - De har interne policyer rundt bruk av ansattes maskiner og e-post. Han nevner også tekniske løsninger og verktøy brukt for sikkerhetslogging, herunder bruk av Elastic og et egenutviklet serverjern.

- Hvilke tekniske løsninger og verktøy benytter dere for sikkerhetslogging, og hvordan valgte dere disse?
    - De bruker Elastic og serverjern som de har selv satt opp.

    - Valg av tekniske løsninger begrunnes med anbefalinger fra Reddit community og andre kilder, samt evnen til å skalere og tilpasse til forretningsbehov.

- Hvordan har dere satt opp lagring og håndtering av loggdata for å sikre både tilgjengelighet og konfidensialitet?
    - De ligger mest vekt på konfidensialitet. De bruker kryptering både under dataoverføring og lagring, og har strenge tilgangskontroller til loggserveren.
    - I integritet i logghåndtering, de tar hensyn til potensielle brudd i loggsekvensen og sentraliserer loggdata for å forhindre tap ved lokale slettinger. Kryptering av loggdata bidrar også til integritet.
    - De fokuserer ikke veldig på tilgjengelighet.

- Hvordan har dere tolket og tilpasset dere til nasjonale og eventuelle internasjonale retningslinjer eller lovgivning relatert til sikkerhetslogging? Er det noen standarder dere følger eller er sertifiserte i (eks. ISO 27001)?
    - Det finnes ikke spesifikke lovkrav for loggføring, men at de følger Personvernsforordningen (GDPR i Norge) og interne policyer.
    - De følger ikke spesifikt ISO-standarden, men mange av deres praksiser samsvarer med den. De baserer seg også på en best practice guide fra Microsoft.
    - de har mappet sine praksiser mot Nasjonal Sikkerhetsmyndighets (NSM) grunnprinsipper, som også er anbefalinger snarere enn krav.
    - for helseopplysninger finnes det lovpålagt logging, men denne håndteres av leverandører og fagsystemer. Han anbefaler å rådføre seg med HelseCert for spesifikke anbefalinger om logging i helsesektoren.

- Har dere utfordringer knyttet til rettshåndhevelsesforespørsler, som politiets behov for tilgang til historiske data? Hvis ja, hvordan håndterer dere disse?
    - Det utfordringer knyttet til rettshåndhevelse og politiets forespørsler om tilgang til historiske data, spesielt i forhold til EKOM-loven. Han nevner at politiet noen

ganger overser å inkludere NKOM i IP-sporingssaker, og at det er vanskelig å identifisere enkeltpersoner basert på IP-adresser.
    - Han understreker at det kun er i tilfeller med domstolskjenning at de kan utlevere informasjon, og at de må nekte politiet tilgang til datalogger med mindre en domstol er involvert.
    - Han nevner at de håndterer anmodninger fra politiet og at de må være forsiktige med å ikke bryte personvernlovgivningen. Han nevner også at politiet noen ganger forsøker å unngå domstols prosessen.

- Har det vært noen spesifikke hendelser som har påvirket deres praksis eller politikk for sikkerhetslogging?
    - Hendelser og pentester påvirker deres praksis og politikk for sikkerhetslogging. De justerer loggingen basert på oppdagelser gjort under sikkerhetstester.

- Basert på deres erfaringer, hva ville dere anbefale Gjøvik kommune å fokusere på når de utvikler eller forbedrer sin sikkerhetsloggingsstrategi?
    - De anbefaler Gjøvik kommune å sentralisere sine logger og etablere en god audit policy basert på Microsofts anbefalinger. Det er også mulig å kjøpe sikkerhetslogging som en tjeneste (MDR).

- Er det noen spesifikke innsikter dere har lært som dere mener er kritiske for suksessen med sikkerhetslogging i en kommunal kontekst?
    - Han understreker viktigheten av å logge tilstrekkelige mengder data. Mange betaler for mengden de logger og ender opp med å logge for lite, noe som kan føre til mangelfull informasjon ved sikkerhetsbrudd. Det er også viktig å sikre at logging skjer på alle servere og systemer for å unngå blindsoner.

- Har dere planer om å gjøre endringer eller forbedringer i deres sikkerhetsloggingspraksiser?
    - De har fremtidige planer for forbedring av sikkerhetsloggingspraksiser. De har studenter fra Høgskolen i Kristiania som deltar i et purple teaming-prosjekt. Prosjektet involverer hacking og beskyttelse, hvor målet er å forbedre tidlig deteksjon av mistenkelig aktivitet og utvikle regler for å identifisere slike aktiviteter. Dette er en del av en kontinuerlig innsats for å forsterke og forbedre sikkerhetsloggingsstrategiene.

- Ser dere noen nye trender eller teknologier som kan påvirke hvordan kommuner bør tenke rundt sikkerhetslogging i fremtiden?
    - Ja, Sky! skyløsninger påvirker sikkerhetslogging. Tradisjonelt har organisasjoner hatt full kontroll over sine logger når løsningene er lokalt baserte. Med skyløsninger flyttes mye av denne kontrollen bort, og tilgang til detaljerte logger blir begrenset. Mange skyleverandører tilbyr ikke innsikt i logger, noe som skaper utfordringer for organisasjoner i å opprettholde god sikkerhetspraksis.
    - Det er få skyleverandører, unntatt Microsoft, som tillater tilgang til detaljerte logger. Dette presenterer en utfordring siden applikasjonslogger ofte ikke er rettet mot sikkerhet og kan mangle varsel om mistenkelig aktivitet.

- Hvor lenge logger bør lagres?
    - Han anbefaler å lagre logger i minst 13 måneder for å dekke typiske årlige sykluser og gi tilstrekkelig tid til hendelsesontering.
    - Noen organisasjoner kun lagrer logger i 90 dager, noe som kan være for kort for å identifisere og forstå langvarige sikkerhetsbrudd.
    - Det er utfordringer med å søke i logger eldre enn 90 dager, spesielt i Microsofts Log Analytics, noe som kan være upraktisk og krever spesifikk kompetanse.
    - Anbefaler å undersøke hva markedet tilbyr og sammenligne det med interne behov for logging. Minimum ett år med logglagring anbefales, basert på incident

response rapporter som viser at angripere ofte har vært aktive i systemet i flere måneder.

- Logger også er nyttige for vanlig drift, ikke bare for sikkerhetsformål. De kan gi innsikt i tidligere driftsproblemer og bidra til effektiv problemløsning. Et halvt år med logglagring kan være tilstrekkelig for en effektiv hendelsesrespons, men det er viktig å ha detaljert informasjon om hvilke brukerkontoer og servere som har vært involvert i en sikkerhetshendelse.
- kvaliteten på logger kan påvirke evnen til å håndtere sikkerhetshendelser. Med gode logger kan man være mer presis i å identifisere hvilke deler av systemet som har vært kompromittert, noe som kan redusere behovet for å gjenopprette hele systemet.
- verdien av logger ligger i deres brukbarhet for å identifisere kompromitterte deler av nettverket. Logger som ikke gir nok informasjon til å gjøre en effektiv hendelsesrespons, har begrenset verdi til tross for lengre lagringstid.
- Østre Toten-kommunen brukte et par år på å komme seg etter et cyberangrep. Hendelser som dette har ført til økt fokus på sikkerhetslogging. Horten kommune har brukt -REDACTED- kroner på lagring over -REDACTED- år, noe som er en del av deres investering i sikkerhetslogging.
- Andre kommuner har varierte kostnader for sine sikkerhetsloggingsløsninger, fra en halv million til halvannen million kroner. Disse tallene kan variere avhengig av kommunenes størrelse.