Logning og monitorering

Hvad sker der i vores IT-systemer?

UNIVERSITY COLLEGE
OF NORTHERN DENMARK

Henrik Munk Hvarregaard
Department of Computer Science

Logning i Danmark – det HELT store billede

”I Danmark skal man kunne færdes frit og trygt. Og en væsentlig forudsætning for det er, at politi og anklagemyndighed har de bedst mulige redskaber til at bekæmpe grov kriminalitet. Revisionen af de danske logningsregler er ikke en blomst, der er groet i regeringens have. Men når vi nu skal ændre reglerne, har ambitionen været at sikre, at vores myndigheder får mulighed for at kunne anvende loggede oplysninger i videst muligt omfang, da det i alvorlige sager om fx drab og voldtægt, kan være et vigtigt bevismiddel. Jeg er derfor glad for, at et flertal i Folketinget i dag har stemt for regeringens lovforslag, som netop sigter efter færrest mulige negative konsekvenser for opklaringen og retsforfølgningen af grov kriminalitet i Danmark”.

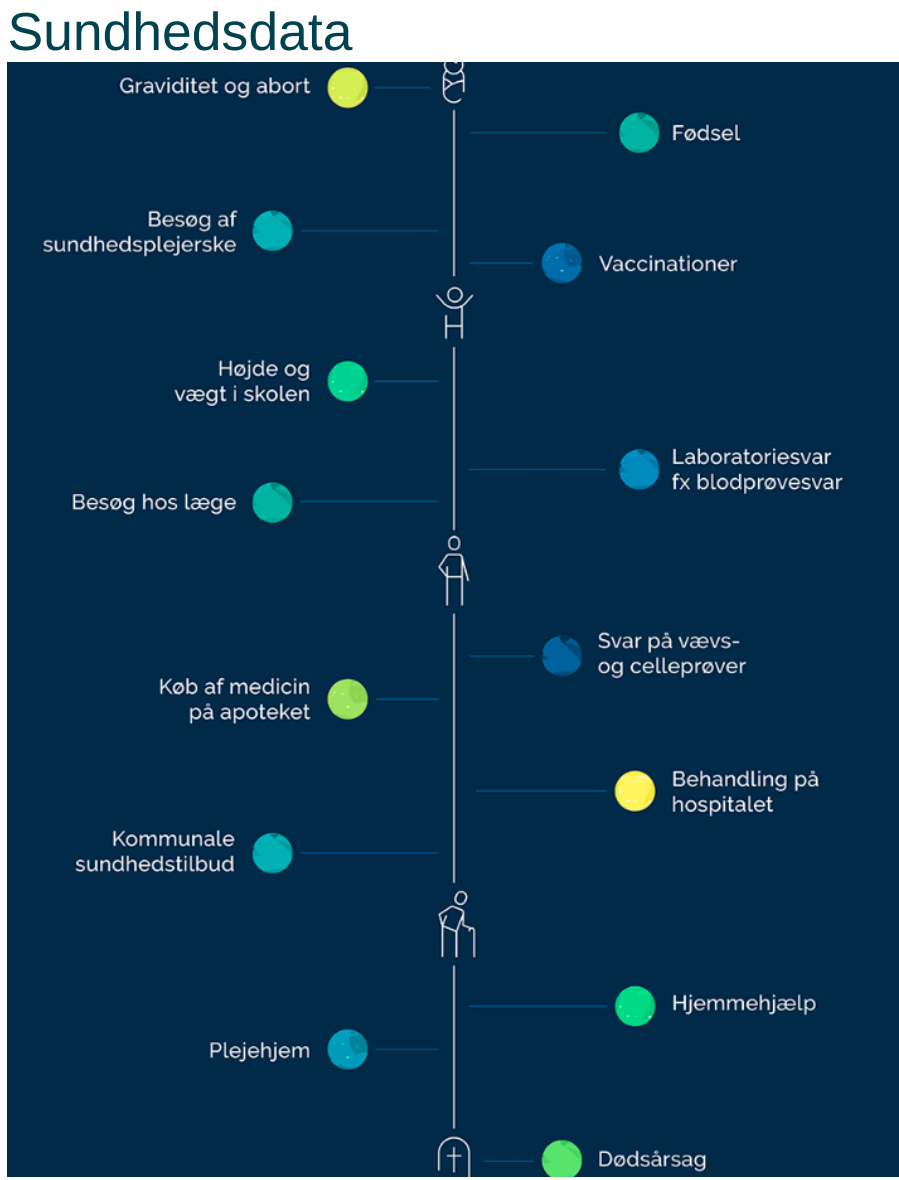
Nick Hækkerup (3. marts 2022)

Logning i Danmark – teleselskabernes logs

- Der skal kunne foretages generel og udifferentieret logning, når det vurderes, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed.
- Generelle og udifferentierede logning må dog ikke blive systematisk.
- Når der ikke er grundlag for generel og udifferentieret logning vil teleselskaberne mv. være forpligtede til at foretage målrettet personbestemt og geografisk logning. Eks. målrettet bestemte personer og områder, der vurderes at have en forbindelse til grov kriminalitet.
- Der gælder en pligt for teleselskaberne mv. til generelt og udifferentieret at logge oplysninger om en brugers adgang til internettet (herunder IP-adresser) uafhængigt af, om der foreligger en alvorlig trussel mod den nationale sikkerhed. (Det logges ikke, hvilke hjemmesider man besøger).
- Der skal indhentes en retskendelse for adgang til teleselskabernes logs

Logning i sundhedssektoren

- Når medarbejdere i Sundhedsdatastyrelsen arbejder med sundhedsdata, bliver det logget, så styrelsen til enhver tid kan se, hvilke data de har haft adgang til, og hvordan de har arbejdet med disse data.
- **Når forskere og personale i sundhedsvæsenet arbejder med data, bliver det også logget, så man til enhver tid kan se, hvilke data de har haft adgang til.**

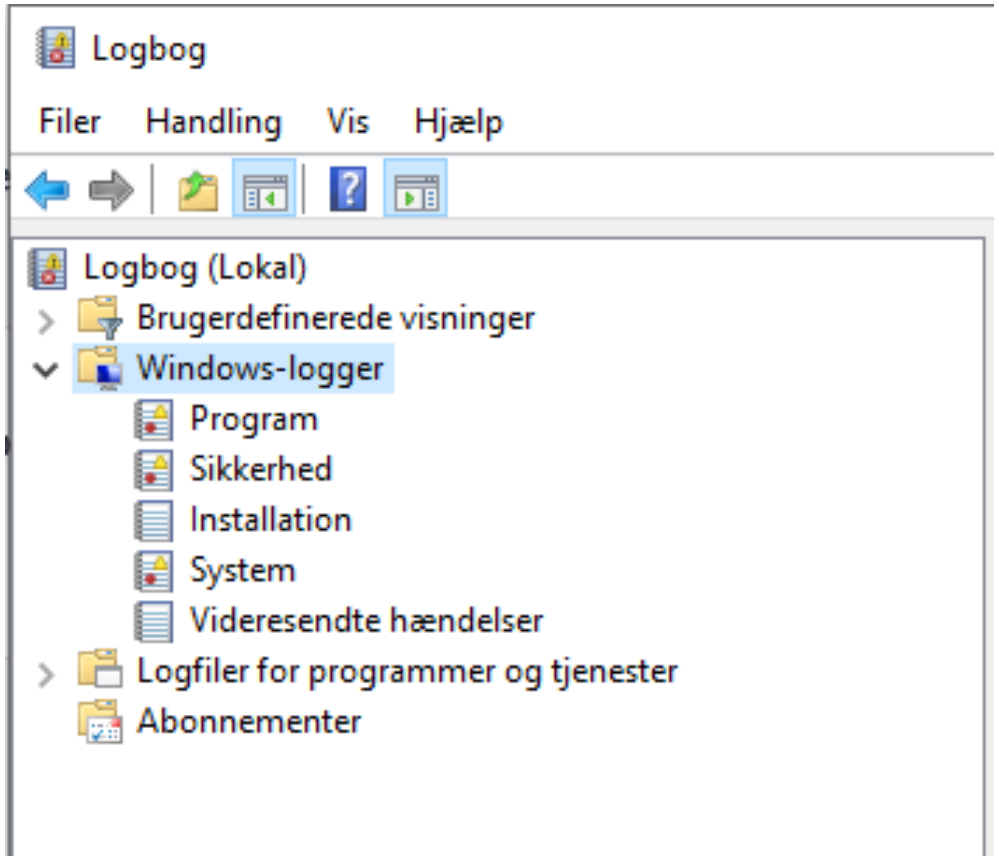


Hvad er en log?

- En (computer)log er en detaljeret registrering af begivenheder, der forekommer på en computer eller et computerbaseret system. Logfiler bruges til at spore, overvåge og analysere aktiviteterne på en computer eller et netværk.
- Logfiler kan indeholde oplysninger om forskellige typer begivenheder, herunder systemhændelser, brugeraktiviteter, fejl og advarsler.
- Logfiler kan indeholde oplysninger som dato og tidspunkt for begivenheden, kilde eller oprindelse, beskrivelse af begivenheden og andre relevante oplysninger.

Hvad er en log?

- Hvilke forskellige typer af logs findes der på en almindelig Windows PC?



Logs på en Windows PC

1. Application Log (Program): Programloggen registrerer begivenheder relateret til specifikke applikationer eller tjenester på din computer. Denne log indeholder oplysninger om fejl, advarsler og vigtige meddelelser fra forskellige applikationer, du bruger.
2. Security Log (Sikkerhed): Sikkerhedsloggen indeholder informationer om sikkerhedsrelaterede begivenheder på din computer. Den registrerer logon- og logoff-aktiviteter, adgangskontrolændringer, forsøg på uautoriseret adgang mm.
3. Setup Log (Installation): Installationsloggen registrerer informationer om installationen af operativsystemet eller applikationer. Denne log bruges til at identificere eventuelle fejl eller problemer under installationsprocessen.
4. System Log (System): Systemloggen registrerer begivenheder og fejl relateret til dit system og operativsystemet. Denne log kan indeholde oplysninger om hardware- eller driverfejl, serviceopstart/afslutning og systemnedbrud. Den hjælper med at overvåge og diagnosticere problemer på dit system.

Eksempel på log af adgang til fortroligt dokument

```
Tidspunkt: 2023-05-31 09:23:15
Bruger: jdoe
Handling: Adgang til fortrolig fil
Beskrivelse: Bruger "jdoe" åbnede filen "fortrolig.docx" fra placeringen "C

Tidspunkt: 2023-05-31 09:24:02
Bruger: jdoe
Handling: Redigering af fortrolig fil
Beskrivelse: Bruger "jdoe" foretog ændringer i filen "fortrolig.docx" og ge

Tidspunkt: 2023-05-31 09:27:45
Bruger: jdoe
Handling: Eksport af fortrolig fil
Beskrivelse: Bruger "jdoe" eksporterede filen "fortrolig.docx" til placerin

Tidspunkt: 2023-05-31 09:29:10
Bruger: jdoe
Handling: Sletning af fortrolig fil
Beskrivelse: Bruger "jdoe" slettede filen "fortrolig.docx" fra placeringen
```

Hvad ser vi i loggen?

- Sæt en overskrift på hver kolonne i nedenstående log.
- Hvad ser vi i loggen?
- Hvilken ip-adresse bør vi være opmærksomme på?

```
200 OK              12.55.22.88 jr22          2019-03-18T09:21:17 /login
200 OK              14.56.23.11 rand99        2019-03-18T10:19:22 /login
200 OK              17.33.10.38 afer11        2019-03-18T11:11:44 /login
200 OK              99.12.44.20 rad4          2019-03-18T11:55:51 /login
200 OK              67.34.22.10 bff1          2019-03-18T13:08:59 /login
200 OK              34.55.11.14 hax0r         2019-03-21T16:08:15 /login
401 Unauthorised 49.99.13.16 admin         2019-03-21T21:08:15 /login
401 Unauthorised 49.99.13.16 administrator 2019-03-21T21:08:20 /login
401 Unauthorised 49.99.13.16 anonymous     2019-03-21T21:08:25 /login
401 Unauthorised 49.99.13.16 root          2019-03-21T21:08:30 /login
```

Log management

- Log management (også kendt som logstyring eller loghåndtering) refererer til processen med at arbejde med logfiler fra forskellige kilder, herunder computer- og netværkssystemer, applikationer, sikkerhedsenheder, IoT-enheder mm.
- Almindelige trin i log management:
  - Generering af logs
  - Opsamling af logs
  - Test af logs
  - Lagring/opbevaring af logs
  - Anvendelse af logs
  - Sletning af logs

Log management

- Politik og procedurer skal beskrive alle foregående trin ifm. log management.
- Politikken skal sikre, at gode og anvendelige logs er tilgængelige, at de er læsbare og rækker tilstrækkeligt langt tilbage i tid.
- En måde at udarbejde dækkende politikker og procedurer på, er at udarbejde scenarier over den slags hændelser, man gerne vil kunne undersøge i tilfælde af en hændelse.
- Politikker og procedurer skal afstemmes med dem der skal bruge dem.
- Politikker og procedurer skal afstemmes med hvad de skal bruges til.
- Politikker og procedurer skal afstemmes med gældende lov og regler.

Hvad bør være på plads inden logning?

- Hav et godt overblik over it-arkitekturen (topologi)
- Beskrivelser af alle internetforbindelsespunkter og de regelsæt, de følger (eksempelvis firewallregler).
- Dokumentér alle implementerede logningsløsninger
- Log-niveauet skal være tilstrækkeligt detaljeret og vise de informationer, der er nødvendige
- Klienters rigtige IP-adresser logges (og ikke eksempelvis adresse fra en proxy)
- Samlet overblik over alle de logs, der genereres
- Sæt krav til leverandører om hvilke logs, der skal genereres og hvordan de kan tilgås
- Tilstrækkelig lagerkapacitet til rådighed til opbevaring af logs i valgte tidsperiode

Hvad kan der typisk logges?

- Tidspunkt: Registrerer tidspunktet for den logførte begivenhed. Dette inkluderer både dato og tid.
- Kilde-IP eller kilde-identifikator: Angiver kildeadressen for enheden/brugeren, der udførte handlingen.
- Bruger: Navnet på brugeren, der udførte handlingen eller var involveret i begivenheden.
- Handling: Beskrivelse af den udførte handling, såsom login, adgang til en fil eller en systemhændelse.
- Beskrivelse: Yderligere detaljer om begivenheden, herunder specifikke oplysninger om handlingen eller hændelsen.
- Resultat: Resultatet af handlingen, f.eks. om det var vellykket eller mislykket.
- Kritikalitetsniveau: Angiver kritikaliteten af begivenheden, f.eks. advarsel, fejl, eller et almindeligt systemevent.
- Placering: Hvor begivenheden fandt sted, såsom filsti, IP-adresse, applikationsnavn eller systemnavn.
- Logtype: Angiver typen af log, f.eks. sikkerhedslog, applikationslog eller systemlog.
- Protokol: Angiver den protokol, der blev brugt i forbindelse med begivenheden, f.eks. HTTP, FTP eller SSH.
- Destination-IP: Angiver destinationen for handlingen, f.eks. IP-adressen for en server eller en filsti.

Generering af logs

- Det begynder ofte med en risikovurdering….
  - Enhver organisation skal løbende vurdere hvilke logs, der er relevante, hvis der skal prioriteres ud fra et ressourcemæssigt perspektiv.
  - Her tager man organisationens opgaver/forretning, krav til performance og driftssikkerhed, sårbarheder og trusselsbilledet i betragtning.
  - Man laver overvejelser vedrørende risici, organisationen påfører sig ved udnyttelsen af digitaliseringsmuligheder
  - Der skal tages stilling til eventuelle regler, love, branchestandarder og lignende, som organisationen kan være underlagt. Noget regulering kan pålægge organisationen særlige krav til logning, herunder hvad der ikke må logges, hvor lang tid logs må opbevares osv.

Generering af logs – Governance, risk og compliance

Opsamling af logs

- Der skal etableres et system, der samler alle logs ét centralt sted. Logpolitik og procedurer bør sikre følgende krav til logs:
  - **Tidsstempling**. For at logs i centrale log-systemer og på decentrale enheder senere skal kunne anvendes og korreleres, er det altafgørende, at logs sker med en tidsstempling, der er synkroniseret fra en central tidsserver.
  - **Dataintegritet**. Det skal sikres, at der ikke kan blive manipuleret med logdata. Det gælder beskyttelse imod, at medarbejdere med privilegerede rettigheder, eksterne samarbejdspartnere og udefrakommende angribere kan slette, ændre eller tilføje data i loggen.
  - **Dokumentér**. Der skal udarbejdes dokumentation for, hvorfra der logges, og hvad der logges. Det giver overblik over hvilke data, der er til rådighed i tilfælde af en hændelse.

Test af logs

- Loggene skal testes løbende.
  - Når logning er opsat, er det vigtigt at teste, om logningen er korrekt, om det er de rigtige data, der gemmes, og om de bliver gemt så længe, som det er defineret i organisationens politik.
  - Det skal også testes, om der kan uddrages de ønskede informationer i forbindelse med en eventuelt sikkerhedshændelse. Kan man eksempelvis identificere hvem, der har gjort hvad hvornår?

Lagring/opbevaring af logs

- En hændelse opdages ikke altid, mens den står på. Derfor skal logs gemmes.
- Som udgangspunkt bør logs opbevares minimum 13 måneder, medmindre der er lovgivning, der kræver noget andet.
- Der skal etableret de rette sikkerhedsforanstaltninger til at beskytte loggenes fortrolighed, integritet og tilgængelighed (CIA / FIT)
- Det bør sikres, at ingen medarbejdere har mulighed for at manipulere med loggen, uden at det kan opdages.
- Der skal tages stilling til, hvordan logs skal sikkerhedskopieres (eks. vha. samme procedure som for andre sensitive informationer i organisationen).

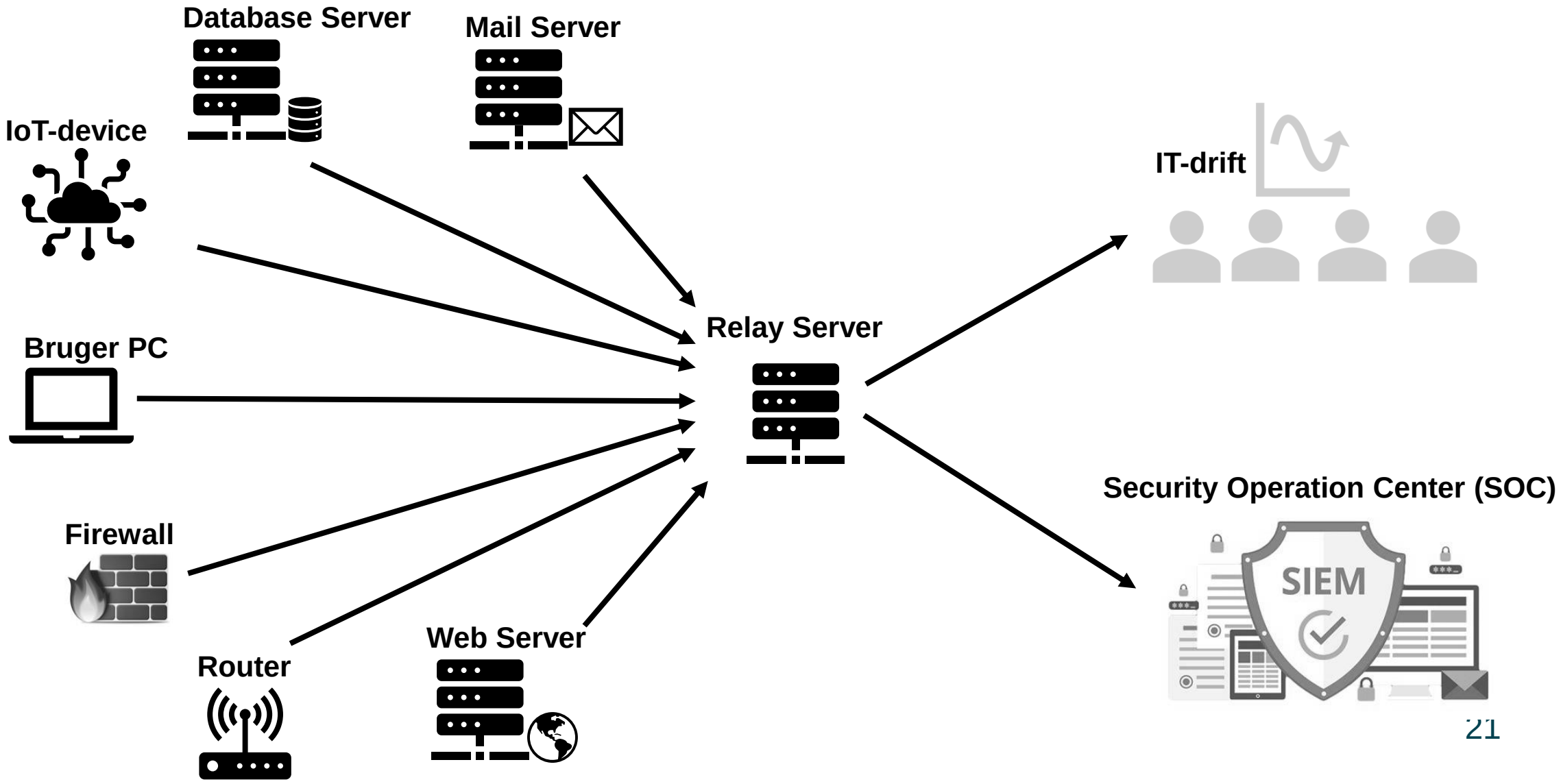
Anvendelse af logs

- Logs kan anvendes proaktivt til driftsoptimering og til løbende at opdage uregelmæssigheder og uhensigtsmæssigheder i organisationens systemer.
- Logs er et værdifuldt værktøj, når man skal analysere en it-sikkerhedshændelse
- Organisationens politik og procedure for logning bør indeholde retningslinjer for, hvordan de forskellige logs konkret kan anvendes
  - Skal en bestemt log eksempelvis gennemgås regelmæssigt?
  - Skal den kun anvendes ved et sikkerhedsbrist?
  - Skal den anvendes ved driftsforstyrelser mm.?
  - Skal logs manuelt gennemgås eller skal de være værktøjsunderstøttet?
  - Skal gennemgangen foretages internt eller ved eksterne partnere?

Sletning af logs

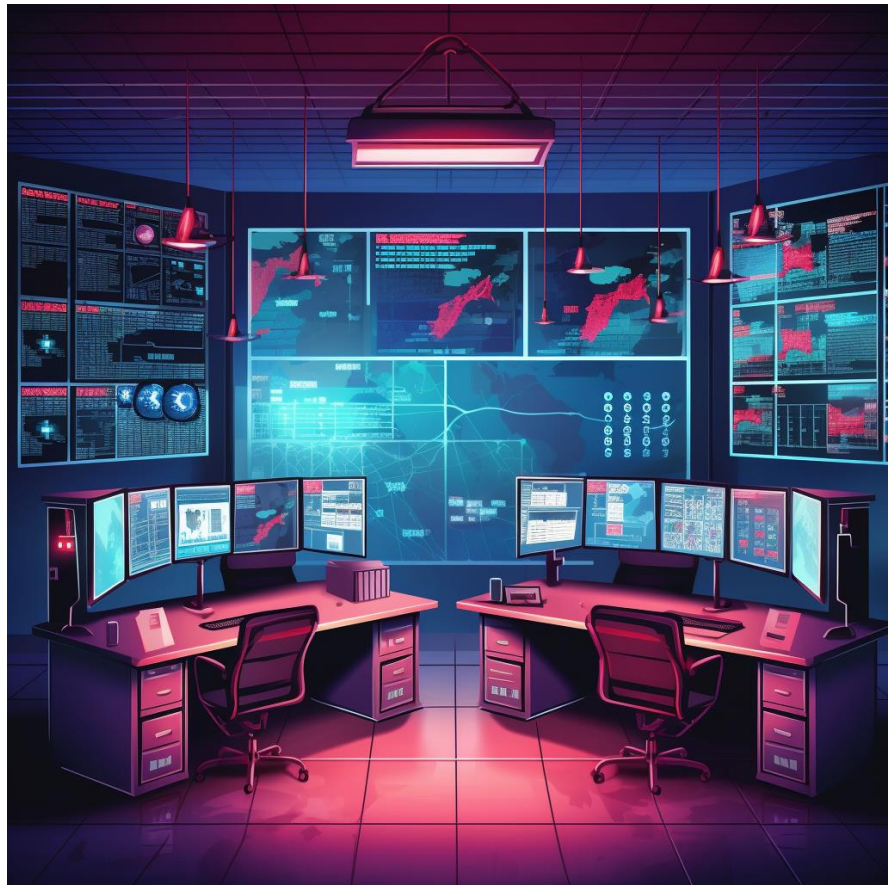
- Når logs slettes, skal organisationen sikre sig, at de slettes helt fra alle de lagermedier.
- Det gælder decentrale enheder (firewalls mm.), sikkerhedskopier og analyseplatforme
- Sletning bør følge en fast beskrevet procedure, og organisationen bør jævnligt sikre sig at denne følges.

Indsamling af logs fra forskellige enheder

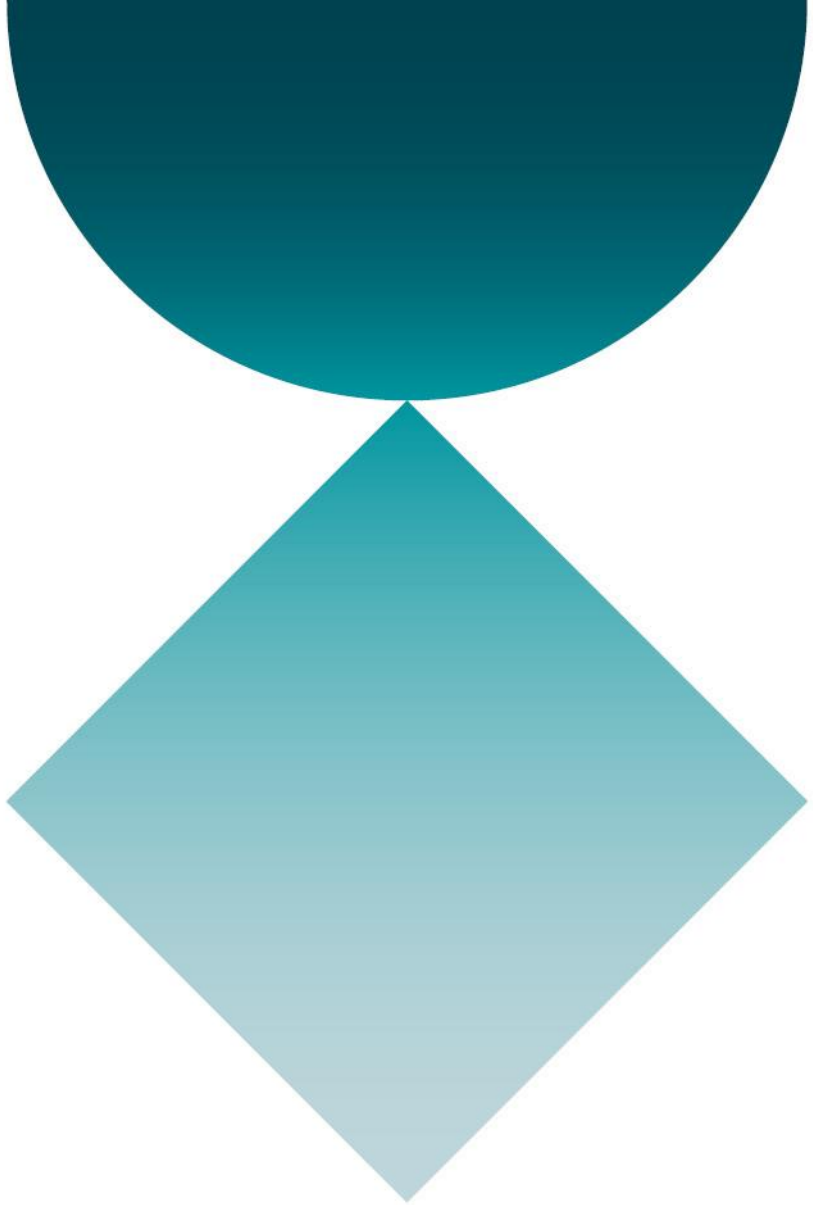


IT-drift og overvågning

- IT-drift, overvågning og sikkerhed anvender forskellige systemer til at synliggøre driftsstatus og performance.
- Typisk anvendes der forskellige visualiseringsværktøjer, hvor både driftsmedarbejdere og eks. produktionsmedarbejdere kan følge med i, hvad der sker.



Ordbog

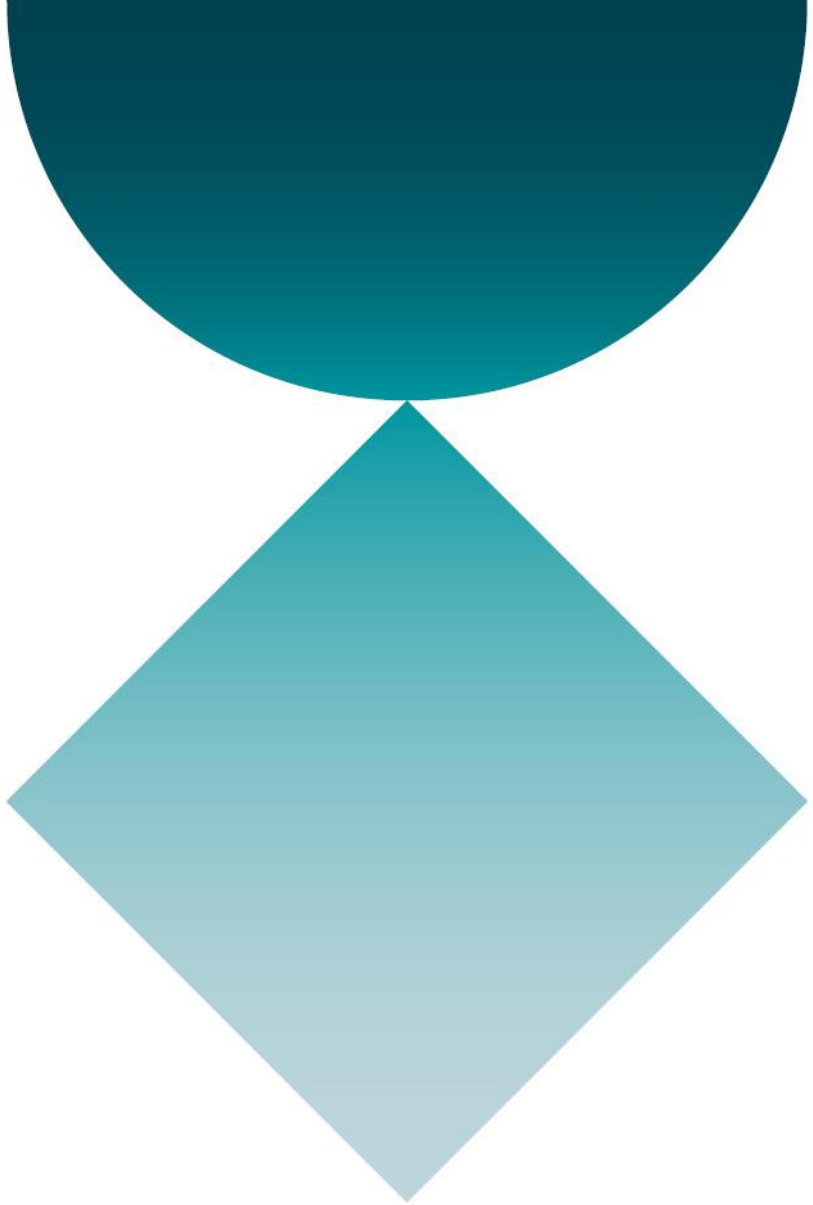


UNIVERSITY COLLEGE
OF NORTHERN DENMARK

Henrik Munk Hvarregaard
Department of Computer Science

Ord	Forklaring
CIA / FIT	Fortrolighed, Integritet, Tilgængelighed (Confidentiality, Integrity, Availability) **Fortrolighed** handler om at holde oplysninger hemmelige og sikre, at de ikke gøres tilgængelige eller videregives til uautoriserede personer, enheder eller processer. **Integritet** handler om at holde oplysninger nøjagtige og fuldstændige. **Tilgængelighed** handler om at holde information tilgængelig og anvendelig ved anmodning fra en autoriseret enhed.
IoT	IoT (Internet of Things) er et koncept, hvor fysiske objekter er forbundet til internettet og har evnen til at indsamle og udveksle data
Log	Detaljeret registrering af begivenheder, der forekommer på en computer eller et computerbaseret system.
Log management / logstyring / loghåndtering	Refererer til processen med at indsamle, analysere, gemme og opbevare logfiler fra forskellige kilder, herunder computer- og netværkssystemer, applikationer, sikkerhedsenheder, IoT-enheder mm.
Risikovurdering	Risikovurdering er en proces, der identificerer og vurderer potentielle trusler og sandsynligheden for skade for at informere beslutninger om risikohåndtering.
SIEM	SIEM (Security Information and Event Management) er en sikkerhedsteknologi og tilgang, der kombinerer logstyring, sikkerhedsinformation og hændelseshåndtering. Det giver mulighed for indsamling, korrelation, analyse og rapportering af logfiler og sikkerhedshændelser fra forskellige kilder i realtid.
VPN	VPN (Virtual Private Network) er en teknologi, der opretter en sikker forbindelse over et offentligt netværk, såsom internettet, for at beskytte privatliv og sikkerhed

Log eksempler



UNIVERSITY COLLEGE
OF NORTHERN DENMARK

Henrik Munk Hvarregaard
Department of Computer Science

Eksempel på log fra firewall

- 2023-05-31 10:45:02 Firewall: Connection denied from 192.168.1.100 to 203.0.113.5, port 22 (SSH)
- 2023-05-31 10:47:15 Firewall: Intrusion Prevention System (IPS) detected and blocked a potential SQL injection attack from 172.16.0.50
- 2023-05-31 10:50:32 Firewall: NAT translation created - Source: 192.168.1.200, Destination: 203.0.113.10, Original Port: 5000, Translated Port: 3000
- 2023-05-31 10:55:21 Firewall: VPN tunnel established with remote site 45.67.89.10
- 2023-05-31 11:02:43 Firewall: Connection allowed from 192.168.1.50 to 203.0.113.20, port 80 (HTTP)

Eksempel på log fra router

- Jun 1 08:15:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
- Jun 1 08:15:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
- Jun 1 08:20:12: %SEC-6-IPACCESSLOGP: List 1 denied tcp 192.168.1.10(49876) -> 203.0.113.5(80), 1 packet
- Jun 1 08:25:32: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.1.20)
- Jun 1 08:30:55: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
- Jun 1 08:30:57: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Eksempel på log fra IoT-device

- 2023-05-31 14:25:10 Device: Temperature reading: 25.6°C
- 2023-05-31 14:30:22 Device: Humidity reading: 54%
- 2023-05-31 14:35:40 Device: Error - Connection lost with the server
- 2023-05-31 14:40:55 Device: Warning - Low battery level: 15%
- 2023-05-31 14:45:10 Device: Motion detected in the vicinity
- 2023-05-31 14:50:30 Device: Firmware update successful

Eksempel på log fra mail server

- May 31 15:10:22 mailserver postfix/smtpd[1234]: connect from mail.example.com[192.168.1.100]
- May 31 15:10:24 mailserver postfix/smtpd[1234]: 452 4.3.1 Insufficient system resources
- May 31 15:10:30 mailserver postfix/smtpd[1234]: disconnect from mail.example.com[192.168.1.100]
- May 31 15:11:05 mailserver postfix/cleanup[5678]: E45F123A1B: message-id=123456789@example.com
- May 31 15:11:10 mailserver postfix/qmgr[9876]: E45F123A1B: from=<sender@example.com>, to=<recipient@example.com>, status=sent (250 2.0.0 Ok: queued as ABCD1234)
- May 31 15:11:15 mailserver postfix/smtp[8765]: 250 2.0.0 Ok: queued as ABCD1234
- May 31 15:11:20 mailserver postfix/smtp[8765]: connect to mx.example.net[203.0.113.5]:25: Connection timed out
- May 31 15:11:25 mailserver postfix/smtp[8765]: ABCD1234: to=<recipient2@example.net>, relay=none, delay=5.1, delays=0.1/0.1/5/0, dsn=4.4.1, status=deferred (connect to mx.example.net[203.0.113.5]:25: Connection timed out)

Eksempel på log fra database server

- 2023-05-31 16:05:12 Database: Connection established from user 'admin' at IP address 192.168.1.10
- 2023-05-31 16:05:15 Database: SELECT query executed successfully on table 'customers’
- 2023-05-31 16:05:22 Database: Error - Table 'orders' does not exist
- 2023-05-31 16:05:30 Database: UPDATE query executed on table 'products', 10 rows affected
- 2023-05-31 16:05:35 Database: Transaction committed successfully
- 2023-05-31 16:05:40 Database: Backup operation started
- 2023-05-31 16:05:55 Database: Backup completed, file saved as 'backup_20230531.bak'

Eksempel på log fra bruger pc

- 2023-05-31 17:30:12 User Client: User 'john.doe' logged in
- 2023-05-31 17:32:05 User Client: Application 'Word' started
- 2023-05-31 17:33:40 User Client: File 'report.docx' opened in 'Word’
- 2023-05-31 17:35:15 User Client: File 'presentation.pptx' saved
- 2023-05-31 17:38:20 User Client: Error - Failed to connect to network printer
- 2023-05-31 17:40:10 User Client: System update started
- 2023-05-31 17:45:25 User Client: System update completed successfully
- 2023-05-31 17:50:30 User Client: User 'john.doe' logged out

Referencer

- Center for cybersikkerhed: Logning – en del af et godt cyberforsvar
  - https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/vejledning-logning-2023.pdf
- Justitsministeriet: nye regler for logning
  - https://www.justitsministeriet.dk/pressemeddelelse/flertal-i-folketinget-vedtager-nye-regler-for-logning/
- Logging Cheat Sheet
  - https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html
- Sundhedsstyrelsen: beskyttelse af sundhedsdata
  - https://sundhedsdatastyrelsen.dk/da/borger/beskyttelse_af_sundhedsdata