Mødeindkaldelse

MedCom
Forskerparken 10
5230 Odense M

Tlf: +45 6543 2030
E-mail: tgj@medcom.dk
www.medcom.dk

10. maj 2021

Mødetitel	SDN-brugergruppemøde
Mødedato	Den 17. maj 2021
Tidspunkt	Kl. 10.00 – 12.00
Sted	Via videokonferenceudstyr: tgj@rooms.medcom.dk Via browser: https://rooms.medcom.dk/webapp/#/?conference=tgj@rooms.medcom.dk
Deltagere	Anders Bjerg Frederiksen, Region Midtjylland Michael Valeur Nielsen, Region Syddanmark Kenneth V. Mogensen, Region Sjælland Kasper Viksø Kegel, Region Sjælland Lars Nyemann-Kofod, Region Hovedstaden Lars Helsberg, Sundhedsdatastyrelsen Peter Spanggaard, Sundhedsdatastyrelsen Jacob Garde, sundhed.dk Kristian Nielsen Foged, Multimed Allan Vistisen, DXC Lasse Christmann, Netic Jan Kondrup, Netic Martin Bagger Brandt, PLO XX, sygehusleverandør Peder Illum, MedCom Lars Hillerup, MedCom Per Abildgaard, MedCom Jesper S. Knudsen, MedCom Tanja Gerner Jusslin, MedCom Lene Taustrup, MedCom (referent)
Afbud	Jan Ostenfeld Michaelsen, Region Nordjylland

DAGSORDEN

Kl. 10.00 – 10.05	**1. Velkomst og præsentation v/ Peder Illum**
Kl. 10.05 – 10.10	**2. Godkendelse af dagsorden (beslutning) v/ Peder Illum**
Kl. 10.10 – 10.30	**3. Cybersikkerhedsinitiativer med relevans for SDN (orientering) v/ DCIS Sund**
Kl. 10.30 – 10.50	**4. FORTROLIGT PUNKT: SDNv4 (drøftelse) v/ Peder Illum**
Kl. 10.50 – 11.00	**5. Sletning i aftalesystemet (drøftelse) v/ Peder Illum**
Kl. 11.00 – 11.10	**6. FORTROLIGT: Kryptering af services (drøftelse) v/ Peder Illum**
Kl. 11.10 – 11.20	**7. Udviklingsønsker (drøftelse) v/ Peder Illum**
Kl. 11.20 – 11.30	**8. Beredskabsøvelse for SDN (drøftelse) v/ Peder Illum**
Kl. 11.30 – 11.40	**9. SDN-temadag (drøftelse) v/ Peder Illum**
Kl. 11.40 – 11.50	**10. Orienteringspunkter (orientering) v/ Peder Illum**
Kl. 11.50 – 11.55	**11. Næste møde (drøftelse) v/ Peder Illum**
Kl. 11.55 – 12.00	**12. Eventuelt v/ Peder Illum**

ORIENTERINGSPUNKTER

Der er desuden en række orienteringspunkter, som kun behandles, hvis der er problemer eller supplerende spørgsmål:

13. Status og opfølgning på drift, service og KPI'er, herunder evaluering af eventuelle hændelser

14. FORTROLIGT: It-revision af SDN, herunder VDX

15. Smokeping-overvågning af IPsec peer-adresser

16. SDN på MedComs hjemmeside

KOMMENTERET DAGSORDEN

1 Velkomst og præsentation v/ Peder Illum

- Velkomst til Lars Hillerup, ny medarbejder hos MedCom

2 Godkendelse af dagsorden (beslutning) v/ Peder Illum

3 Cybersikkerhedsinitiativer med relevans for SDN (orientering) v/ DCIS Sund

Resumé

SDN-brugergruppen præsenteres for status på aktuelle cybersikkerhedsinitiativer med relevans for SDN.

Sagsfremstilling

Under sundhedssektorens strategi for cyber- og informationssikkerhed arbejdes med forskellige initiativer med relevans for SDN. På mødet præsenteres status på bl.a. følgende:

- *Overvågning af trafik i SDN*: På sidste møde i SDN-brugergruppen den 5. oktober 2020 blev DCIS Sunds testforsøg med Darktrace-overvågning af trafik på SDN præsenteret for test af muligheder for tidlig opsporing af anormale trafikmønstre og mønstergenkendelse. Testforsøget skete på baggrund af en POC på det centralt SDN-udstyr. Der var på SDN-brugergruppemødet en drøftelse af mulighed også for overvågning af SDN-MPLS

- *Sårbarhedsskanninger af services i SDN:* På sidste møde i SDN-brugergruppen den 5. oktober 2020 præsenterede DCIS Sund muligheder for sårbarhedsskanning af services i SDN – med afsæt i et initiativ, som omhandler løbende test af sikkerheden i sundhedssektorens systemer og udstyr, herunder i centrale infrastrukturer og systemer som SDN.

- *Joes sandbox:* Der arbejdes med opsætning af en central awareness-postkasse, hvortil mistænkelige mails kan sende med henblik på vurdering. IOC'er vil automatisk blive sendt til MISP.

Det indstilles, at SDN-brugergruppen

- Tager orienteringen til efterretning

4 FORTROLIGT: SDNv4 (drøftelse) v/ Peder Illum

Fortroligt punkt.

5 Sletning af aftaler (drøftelse) v/ Peder Illum

Resumé
SDN-brugergruppen drøfter forslag til justering af metode til sletning af aftaler, services og klienter i aftalesystemet.

Sagsfremstilling
I aftalesystemet er annullering af aftaler, services og klienter implementeret, så den tilsluttede part efterfølgende har mulighed for at gendanne, hvis annulleringen var en fejl. Før annulleringen af en aftale bliver den tilsluttede part spurgt til en bekræftelse på annulleringen.

Dette giver imidlertid den uhensigtsmæssige konsekvens, at der i aftalesystemet kan være IP-adresser, som ikke bliver frigivet.

Derfor er der behov for at drøfte 'annullering i aftalesystemet' vs. en egentlig sletning med henblik på eventuel udvikling og implementering af justeret metode til sletning.

Den eventuelle udvikling indgår i listen over udviklingsønsker.

Det indstilles, at SDN-brugergruppen

- Drøfter fordele og ulemper ved ændret metode til sletning af aftaler i aftalesystemet

6 FORTROLIGT: Kryptering af services (beslutning) v/ Peder Illum

Fortroligt punkt.

7 Udviklingsønsker

Bilag 7.1: Liste med udviklingsønsker

Resumé
SDN-brugergruppen præsenteres for status på udviklingsønsker.

Sagsfremstilling
SDN-brugergruppen præsenteres og drøfter opsamlede udviklingsønsker, som fremgår af bilag 7.1 – er de fortsat aktuelle – og er der nye ønsker?

Det indstilles, at SDN-brugergruppen

- Drøfter status på udviklingslisten med henblik på prioritering

8 Beredskabsøvelse for SDN

Resumé
SDN-brugergruppen orienteres om den årlige beredskabsøvelse for SDN, VDX og KIH med henblik på at drøfte cases for SDN.

Sagsfremstilling

Som en del af årshjulet for Informationssikkerhed øves MedComs beredskabsplan. Årets øvelse blev afholdt den 19. november 2020 og var del af den første og tværgående cyberøvelse gennemført af Center for Cybersikkerhed og de 6 samfundskritiske sektorer (tele, energi, finans, sundhed, transport og søfart).

Formålet med øvelsen var at undersøge og afprøve kommunikation og videndeling mellem myndighederne og virksomhederne i tilfælde af et større cyberangreb, som påvirker flere sektorer samtidig.

Casen var et fiktivt cyberangreb. DCIS Sundhed koordinerede øvelsen for sundhed - og nøglemedarbejder hos MedCom planlagde, hvordan casen kunne udmøntes i en hændelse for primært SDN.

Øvelsen for MedCom blev afviklet som både en skrivebordsøvelse samt en reel simulering af, at en autoriseret bruger oprettede falske brugere, klienter og services i andre organisationer i SDN-aftalesystemet.

Et væsentligt delmål for MedCom var således at teste, om overvågning og alarmering på fejlede loginforsøg virkede - og om hændelsesloggen ville kunne være med til at afdække angrebets omfang, som sammen med øvrige indspil, ville resultere i de nødvendige handlinger.

Simuleringen af loginforsøg viste, at overvågningen, log og den tekniske opsætning af alarmer i log management-systemet samt reaktionen og samarbejdet med SDN-leverandøren fungerede.

Center for Cybersikkerhed planlægger at afholde en tværgående cyberøvelse hvert andet år – og DCIS Sund en årlig beredskabsøvelse. Til begge forventer MedCom at deltage, hvilket også vil indbefatte udarbejdelse af case relevant for SDN.

SDN-brugergruppen inviteres derfor til at supplere listen over mulige cases udarbejdet tidligere i regi af SDN-brugergruppen:

- *Case 1:* Brud på fortrolighed, som er udløst af, at en medarbejder hos driftsleverandøren har kigget i SDN-MPLS-trafik
- *Case 2:* Brud på fortrolighed, som kan udløse brud på tilgængelighed. Bruddet er udløst af, at Cisco annoncerer en high risk på IP-sec kryptering– men uden kendt løsning
- *Case 3*: Brud på fortrolighed udløst af et DoS-angreb fra en organisation på SDN

Det indstilles, at SDN-brugergruppen
- Tager orienteringen til efterretning
- Drøfter yderligere cases til fremtidige beredskabsøvelser

9 SDN-temadag v/ Peder Illum (drøftelse)

Resumé
SDN-brugergruppen inviteres til drøftelse af en kommende SDN-temadag.

Sagsfremstilling
Den årlige SDN-temadag blev grundet Corona aflyst.

SDN-brugergruppen inviteres til drøftelse af indhold en kommende SDN-temadag, herunder timing og indhold.

Det indstilles, at SDN-brugergruppen

- Drøfter afholdelse af en SDN-temadag

10 Orienteringspunkter (orientering) v/ Peder Illum

Resumé
SDN-brugergruppen stiller eventuelle spørgsmål til orienteringspunkterne.

Sagsfremstilling
Til dagsordenen er en række orienteringspunkter, som kun behandles, hvis der er problemer eller supplerende spørgsmål. Disse fremgår i nedenstående under 'orienteringspunkter'.

11 Næste møde (beslutning) v/ Peder Illum

Kommende møder i 2021:

- Videomøde den 4. oktober 2021 kl. 10.00-12.00

Drøftelse af forslag til punkter for næste møde, herunder emner til inspirationsindlæg:

- Risikovurdering
- Opfølgning på implementering af dashboard over aftaler uden trafik

12 Eventuelt v/ Peder Illum

ORIENTERINGSPUNKTER

Der er desuden en række orienteringspunkter, som kun behandles, hvis der er problemer eller supplerende spørgsmål:

13 Opfølgning fra seneste møde og sidste nyt

- SDN-tilslutning- og databehandleraftaler er indgået

- Den 16. marts 2021 blev implementeret en funktion i aftalesystemet til migrering af aftaler mod en service fra én serviceudbyder til en anden serviceudbyder. Baggrunden for udviklingen af funktionen har været et ønske om en mere smidig metode til migrering af aftaler fra en serviceudbyder til en anden serviceudbyder.

14 Status og opfølgning på drift, servicemål og KPI'er – herunder evaluering af eventuelle hændelser

Bilag 14.1: Driftsafrapportering SDN inkl. KPI'er

Resumé
Driftsstatus præsenteres.

Sagsfremstilling
Overordnet driftsstatus:

- Driften af SDN har været stabil den sidste periode. De aftalte servicemål er indfriet, og der har ikke været major incidents.

De 4 core-switches (ASR og SW 1 og 2) forventes opgraderet efter sommerferien 2021.

Driftsrapportering inkl. udviklingen i KPI'er fremgår af bilag 14.1.

Det indstilles, at SDN-brugergruppen

- Tager status på drift til efterretning

15 FORTROLIGT: It-revision af SDN, herunder VDX

Fortroligt punkt.

16 Smokeping-overvågning af IPsec peer-adresser

Resumé
SDN-brugergruppen præsenteres for status på Smokeping-overvågning af IPsec peer-adresser.

Sagsfremstilling
MedCom har i samarbejde med SDN-leverandøren Netic udviklet og implementeret en løsning til overvågning af IPsec peer-adresser i Smokeping.

Tidligere har Smokeping-overvågning kun været mulig for services på SDN. Med opsætning af en ekstern Smokeping-server kan der også spørges mod adresser uden for SDN.

Det betyder, at organisationer med adgang til SDN via VPN-forbindelser får nu har mulighed for at tilføje deres organisations VPN-peer-adresse i aftalesystemet. Adressen vil herefter fremgå af Smokeping – under forudsætning af, at der er de rette tilladelser i firewall.

For Org. admin i aftalesystemet er det muligt at se, om services er tilmeldt Smokeping ved at lave en eksport af oplysninger under organisationens services. I kolonnerne med [PING_xxx] kan man se, om services er tilmeldt (1) eller ej (0).

Muligheden vil blive udmeldt til de tilsluttede parter.

Det indstilles, at SDN-brugergruppen

- Tager orienteringen til efterretning

17 SDN på MedComs hjemmeside

Resumé
SDN-brugergruppen ved behov sender forslag til eventuelle forbedringsmuligheder til MedComs hjemmeside med fokus på SDN-support- og drift.

Sagsfremstilling
MedCom har på sin hjemmeside indhold om SDN:

- Generelt om SDN: https://medcom.dk/systemforvaltning/sundhedsdatanet-sdn
- Drift: https://medcom.dk/systemforvaltning/sundhedsdatanet-sdn/drift
- Support: https://medcom.dk/opslag/support/sundhedsdatanettet-sdn
- Startpakke: https://medcom.dk/systemforvaltning/sundhedsdatanet-sdn/startpakke
- Infrastruktur: https://medcom.dk/systemforvaltning/sundhedsdatanet-sdn/infrastruktur
- SDN-brugergruppe: https://medcom.dk/systemforvaltning/sundhedsdatanet-sdn/sdn-brugergruppe

Siderne findes også i engelsk version pga. udenlandske tilsluttede parter.

Det indstilles, at SDN-brugergruppen

- Ved behov sender forslag til ønsker og forbedringsmuligheder for SDN-indhold på MedComs hjemmeside