Dit branchemagasin fra TechMedia A/S

Medicoteknik

Magasin for Dansk Medicoteknisk Selskab - DMTS



Vi er **under angreb**

Tema: **IT-sikkerhed**

Nr. 2 - April 2023 - 10. årgang



Corona LifeCare®

Specialister i patientmonitorering og database
Tlf. +45 4615 5408 www.coronalifecare.dk



Telehealth Beyond Video





tytocare™

Medidyne MAKING A DIFFERENCE

Medidyne A/S I Tel. +45 35 25 12 48 I www.medidyne.dk



Foto: Hasiefoto.dk

IT-sikkerhed og medicoteknik

Af Thomas Schmidt.
Lektor
- Syddansk Universitet

Ganske som vores biler, fjernsyn, hårde hvidevarer og meget mere er vores nuværende medicotekniske maskinpark, og i særdeleshed morgendagens, en skøn og til tider problematisk sammensmeltning af hardware og software. Derfor sætter vi i dette nummer af Medicoteknik fokus på it- og cybersikkerhed.

Belært af dyrt købte erfaringer er sikkerhedsbevågenhed og forebyggelse blevet en obligatorisk del af daglig drift. Heldigvis har vi ikke set hændelser i vores sundhedsvæsen i samme størrelsesorden som de angreb, der bragte hovedparten af Irlands hospitaler i knæ forrige år. Det skyldes måske lige dele held og godt fodarbejde. Trusselsbilledet for de fleste europæiske sundhedssystemer er i hvert fald nogenlunde homogent.

Deciderede ødelæggelsesangreb bør vi måske ikke frygte p.t., men berigelseskriminalitet som gidseltagning af data og spionage er pågående farer.

Risikoen for kompromittering kan reduceres på forskellig vis - for eksempel ved at tænke sikkerhed ind som et krav, når vi indkøber systemer. Eller mere aktivt ved at udstyre vores systemer med mekanismer, der hjælper os med at opdage og håndtere uønsket aktivitet.

Samarbejde i form af deling af data og informationer om systemsvagheder, angreb og nye aktører er en central del af et bredt og pålideligt forsvar. Her er både europæiske organisationer som European Union Agency for Cybersecurity (ENISA) og Sundhedsdatastyrelsens Decentrale Cyber- og Informationssikkerheds-enhed (DCIS) gode eksempler. Ligeledes har vi både lovgivning og standarder, som ansporer og fordrer indsatser af os.

Men i sidste ende begynder og afhænger god sikkerhed af os som borgere og ansatte. Så hvis du ikke allerede giver dette emne stor opmærksomhed, håber jeg, at dette temanummer kan sætte skub i nogle tanker. Er du allerede dybt involveret i emnet, kan du forhåbentlig finde inspiration til yderligere fordybelse.
Under alle omstændigheder: God fornøjelse med dette nummer af Medicoteknik.



Medicoteknik

Magasin for Dansk Medicoteknisk Selskab - DMTS

Udgiver:
TechMedia A/S
Naverland 35
2600 Glostrup
Telefon 43 24 26 28
www.techmedia.dk
info@techmedia.dk

Ledelse:
Adm. dir. Peter Christensen
Direktør Rikke Marott Schelde

Redaktionel målsætning:
Gennem tekniske artikler og relevante nyheder inden for sundhedsteknologi leverer Medicoteknik vigtig og nyttig viden, der kan styrke faget, både nationalt og internationalt.

Medicoteknik udgives i samarbejde med Dansk Medicoteknisk Selskab og er medlemsblad for foreningens godt 700 medlemmer og andre relevante abonnenter i branchen.

Medicoteknik udkommer 6 gange årligt.

Fagredaktør:
Thomas Schmidt
Lektor
- Syddansk Universitet

Redaktør:
Journalist Søren Bang Hansen
E-mail: bang@bangmedia.dk. Telefon: 61 65 22 22

Ansvarshavende:
Adm. dir. Peter Christensen, TechMedia A/S

Produktion:
TechMedia A/S

Tryk:
PE Offset A/S

Abonnement:
Bestilling og ændring/opsigelse skal sendes til:
abonnement@techmedia.dk

Oplag:
Trykt oplag: 2.490 stk.
Online læsere: 1.168 stk.

Bladsekretær:
Pia Nielsen
E-mail: pn@techmedia.dk
Telefon: 43 24 26 72

Layout:
Helle Hansen
E-mail: hh@techmedia.dk

Annoncer:
Tanja Wulff Dühring
E-mail: twd@techmedia.dk
Telefon: 43 24 26 06

Annoncekoordinering:
Marianne Dieckmann
E-mail: md@techmedia.dk
Telefon: 43 24 26 82

Kontakt DMTS:
Sekretær & kasserer Per Overgaard Rasmussen
Vester Søgade 68 st. th., 1601 København V
E-mail: por@dmts.dk. Telefon: +45 21 39 02 32

Formand Kim Dremstrup
Aalborg Universitet,
Institut for Medicin og Sundhedsteknologi

Næstformand Peter Sommer
Medicoteknisk Leder
- Region Sjælland
Holbæk, Roskilde og Køge

Tilmelding til DMTS:
www.dmts.dk/om-dmts/bliv-medlem-af-dmts/

Citater fra artikler i Medicoteknik skal ske med tydelig kildeangivelse. Enhver form for gengivelse af artikler, herunder illustrationer, forudsætter udgiverens skriftlige tilladelse. Redaktionen kan ikke påtage sig ansvaret for materiale, der indsendes uopfordret.

ISSN 2246-2848 (tryk) - ISSN 2246-2856 (online)

Læs - og del - bladet på: medicotek.dk

NORDISK MILJØMÆRKNING
5041 0309
TRYKSAG

Scan og hent Medicotekniks medieinformation 2023 hér!

Scan med kameraet på din smartphone.









3 Leder

TEMA: IT-sikkerhed

6 Slip for at være cyberkriminelles lækkerbisken

12 »Honeypots« er lokkemad for hackere

17 Komplekse it-systemer er sårbare

20 Digitalisering er både løsningen og truslen

22 Aarhus i offensiven for cybersikkerhed

24 Sammen om sundhed hjemmefra

26 Ny model skal give bedre personlig behandling

28 Myter og mysterier om tatoveringer og MR-scannere



MEDICAL SCANDINAVIA

MERIVAARA

Medical Scandinavia er glade for at kunne oplyse, at vi har fået eneforhandlingen af Merivaara OP-lejer i danmark.

- Merivaara er en finsk virksomhed, som har produceret OP-lejer siden 1901 og sælger i dag deres produkter i over 120 lande.
- Sortimentet spænder fra det helt simple undersøgelsesleje til avancerede operationslejer.
- OP-lejerne Smarter Practico og Grand Promerix har en kort torso-del og kan opbygges ift. operationstype og krav til gennemlysning.
- OP-lejerne Smarter Practico og Grand Promerix kan konfigureres i flere forskellige versioner alt efter behov og økonomi.
- Udover ovennævnte lejer er der også Scandia Prime og Scandia Lite, som er prisbillige undersøgelses- og OP lejer.
- Merivaara er i dag en del af Lojer Group, så man nu dækker et større område indenfor undersøgelse, fysioterapi, kiropraktik, hospitals-senge, dagkirurgi og OP.
- Merivaara lejerne er nordisk design produceret i norden.

www.mscan.dk



Slip for at være cyberkriminelles lækkerbisken

Ved udvikling og indkøb af medicoteknisk udstyr er det afgørende at indtænke it-sikkerheden fra starten. It-standardkrav er en god løsning til sikring af ensartede krav.




Af Stephanie Pause og Søren Jul.
Infrastrukturarkitekter
- Region Syddanmark

Informationsteknologi er blevet en mere integreret del af medicoteknisk udstyr. For eksempel er it afgørende for, at måledata og alarmer når hurtigt frem til sundhedspersonalet, og at data nemt kan deles. Uden fungerende software, opdaterede servere og stabile netværk minimeres udstyrets værdi.

Godt hjulpet af de politiske målsætninger bruges medicoteknisk udstyr i stigende grad også hjemme hos borgeren selv, for eksempel til hjemmemonitorering. Samtidig er hjemmearbejde blevet mere udbredt, så udstyret i større omfang tilgås hjemmefra - ofte via en privat netforbindelse, pc eller mobiltelefon. Det stiller nye tekniske krav til udstyret og åbner for nye angrebsmuligheder, hvilke der skal dæmmes op for. Det danske Center for Cybersikkerhed vurderer, at cybertruslen mod den danske sundhedssektor er høj. Cyberkriminelle og fremmede stater har en interesse i at stjæle værdifuld information og forstyrre patientbehandlingen. Truslen ▶

MEDRAD® Centargo
CT Injection System



PP-M-CEN-DK-0100-1 March 2023

Do less › Care more

I en nylig afstemning blandt Centargo®-brugere*, **erklærede 45 %, at det innovative CT injektionssystem sparer værdifuld tid** takket være dets brugervenlighed og automatiserede funktioner. Mindre tid til at fokusere på procedurer forud for scanningen betyder mere tid til rådighed til at servicere patienterne og et forbedret niveau af personlig behandling.

Sparer værdifuld tid til patientens behandling!

- **Mere tid til patientbehandling**
- **Øget patientgennemstrømning**
- **Mere tid til den næste patient**

Book et møde! Lad os diskutere, hvordan Centargo kan hjælpe dig med at forbedre arbejdsgange og patientbehandling.
Brug qr-koden eller send en mail til Julie Nielsen: julie.brandhoej@bayer.com

Vil du vide mere?
Se en kort video om Centargos funktioner og fordele.

*N=87. Centargo Post Launch Customer Perception, Market Research Report, Performed Nov 2022 by Cerner Enviza on behalf of Bayer Radiology Global (REF-M-CEN-DK-0002).

©2023 Bayer. Bayer AS, Arne Jacobsens Allé 13, 2300 København, Danmark • Tlf. +45 45 23 50 00 • www.bayer.dk



Tjekliste til it-standardkrav

Følgende områder er værd at overveje, når man udarbejder it-standardkrav:

- Logning og overvågning.
- Netværk, både i virksomheden og hos borgerne/medarbejderne.
- Dokumentation, backup og gendannelse.
- Antivirus, penetrationstest og sårbarhedsscanninger.
- Robusthed af løsningen til sikring af tilgængelighed og oppetid.
- Beskyttelse mod uautoriseret adgang, herunder kryptering, adgangsstyring og fjernadgang.
- Hvor lang tid efter en opdatering frigives, bliver den installeret?
- Ansvarsfordeling mellem kunde og leverandør vedrørende it-sikkerheden.

MDR

Koordinationsgruppen for medicinsk udstyr lancerede i maj 2021 en opdateret model, som beskriver, hvornår software skal efterleve kravene i forordningen om medicinsk udstyr (MDR). Det er eksempelvis software, som styrer brugen af medicinsk udstyr, styrer udstyrets funktion eller hjælper den enkelte patient, for eksempel med doseringsanbefalinger.

påvirkes dels af, hvilken holdning eller budskaber cyberaktivister ønsker at promovere, dels af mediebevågenheden. Derfor er spørgsmålet ikke længere, om sundhedssektoren bliver angrebet - men hvordan angrebet sker, og hvor store konsekvenser det har for patientsikkerheden og befolkningens tillid til sundhedsvæsenet.
Derfor er det vigtigt, at medicoteknisk udstyr løbende beskyttes mod nye sårbarheder - og hurtigt kan genetableres efter succesfulde angreb.

Certificering og agilitet

Kravet om højt it-sikkerhedsniveau i medicoteknisk udstyr stiller ofte indkøbere og udviklere i et dilemma. Ude i klinikken har dette udstyr en typisk levetid på omkring 15 år, og i denne periode vil trusselsbilledet ofte ændre sig, så beskyttelsen fra udviklingstidspunktet ikke længere er tilstrækkelig.
En del medicoteknisk software er i dag reguleret efter reglerne i forordningen om medicinsk udstyr (MDR - *se faktaboksen*), som kun i begrænset omfang indeholder krav til it-sikkerhed. Samtidig er certificeringsprocessen efter MDR omkostningsfuld og tidskrævende. Visse certificeringer af medicinsk software omfatter også operativsystem og lignende, så en påkrævet opdatering, der lukker sårbarheder, kan udløse et fornyet behov for certificering.
Disse krav kommer let i vejen for den agilitet, som er nødvendig, hvis udstyret løbende skal tilpasses trusselsniveauet. For at højne beskyttelsen mod cyberangreb er det afgørende, at det medicotekniske udstyr regelmæssigt undersøges for sårbarheder. Operativsystemer, virtualiseringsplatforme, antivirus m.v. skal løbende kunne opdateres. Brud på sikkerheden skal opdages hurtigt, og udstyret skal nemt kunne genetableres efter angreb.

Kundens problem?

Når medicoteknisk udstyr ikke lever op til disse krav, bliver det i praksis kunden, der overtager hovedpinen med det sårbare udstyr.
I forbindelse med certificering af det medicotekniske udstyr er det derfor afgørende, at operativsystemet, virtualiseringsplatform, antivirus m.v. ikke bliver bundet ind i certificeringen, så det er muligt at opgradere fra en sårbar eller usupporteret version.
Samtidig skal der i forbindelse med certificeringen tages højde for, at installation hos kunden eller i borgerens hjem ofte kræver en tilpasning af standardudgaven, samt at udstyret kan tilgås fra personlige computere og mobiltelefoner, som kan adskille sig fra det, udstyret er certificeret til.
Samlet set stiller dette store krav til løs-











ningsarkitekturen i det medicotekniske udstyr, til robuste applikationer, omfattende dokumentation og et grundigt testforløb inden certificeringen.

Ensartede krav

Virksomheder kan arbejde struktureret med it-sikkerhed ved at udarbejde et sæt it-standardkrav, som bruges hver gang virksomheden køber nyt medicoteknisk udstyr. Kravene skal afspejle virksomhedens risikovillighed samt det it-miljø, udstyret skal anvendes i. De skal ses som et supplement til de krav, udstyret skal overholde i forhold til MDR. Standardkravene kan omfatte alt fra krav til dokumentation og penetrationstest til den ønskede hyppighed af opdateringer. Fordelen ved at bruge it-standardkrav er, at virksomheden bedre kommer rundt om de vigtigste it-sikkerhedsforhold ved alle indkøb. Forhandlere af medicoteknisk udstyr oplever at blive mødt med mere ensartede krav, uanset hvilket ▶





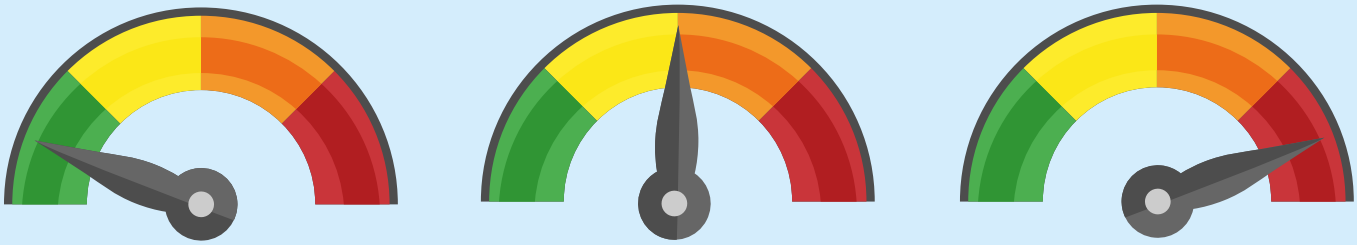
speciale udstyret henvender sig til. Det skaber øget gennemsigtighed og letter dialogen mellem forhandler og kunde. Det bliver nemmere for forhandlere at forstå kundernes it-vision, og hvilken retning kunden ønsker for markedet. Udviklere af medicoteknisk udstyr får også mulighed for at udarbejde roadmaps, som i højere grad matcher kundens behov.
For kunden har it-standardkrav også den fordel, at de i højere grad sikrer, at det indkøbte udstyr passer gnidningsfrit ind i det eksisterende it-miljø. Kunden kan minimere risikoen for uventede ekstraregninger til indkøb af nye pc'er, mobile enheder eller etablering af nye netværk for at benytte det nyindkøbte udstyr.

Samtidig gør standardkravene det nemmere at forvalte og genanskaffe udstyret.

Afgørende parameter

En fleksibel arkitektur, der løbende kan tilpasses den aktuelle cybertrussel, bliver et afgørende konkurrenceparameter for medicoteknisk udstyr.
I Region Syddanmark har vi stort fokus på cybersikkerhed. Vi arbejder med foranstaltninger på mange fronter, og her er it-standardkrav et vigtigt bidrag - og et eksempel på et samarbejde, som kræver mange forskellige fagkompetencer.
Brugen af it-standardkrav gør det nemmere for kunder at stille ensartede krav til it-sikkerheden i det medicotekniske udstyr og dermed mindske antallet af sårbare systemer i sit it-miljø.
Omverdenen er imidlertid ikke statisk, så der er brug for en løbende forbedringsproces for at sikre, at kravene justeres til nye forhold såsom ændret lovgivning, nye cybertrusler og erfaringer fra tidligere anskaffelser.
Samlet set er det vores vurdering, at en tidlig inddragelse af it-sikkerheden i både udvikling og indkøb af medicinsk udstyr er afgørende for, at udstyret kan bruges hos kunden eller hjemme hos borgeren - uden at være en oplagt lækkerbisken for cyberkriminelle.

Små og store trusler



LAV TRUSSEL:

Destruktive cyberangreb

Det er mindre sandsynligt, at den danske sundhedssektor vil blive udsat for forsøg på cyberangreb, hvor den forventede effekt er død, personskade eller ødelæggelse af informationer. En del lande har dog kapacitet, der potentielt kan bruges destruktivt mod samfundsvigtig infrastruktur som sundhedssektoren. Danske myndigheder og virksomheder kan blive ramt som følgevirkning af angreb uden for Danmark, særligt dem som er til stede i konfliktområder.

MIDDEL TRUSSEL:

Cyberaktivisme

Der er udført aktivistiske angreb mod europæiske NATO-lande i forbindelse med krigen i Ukraine. Cyberaktivister går ofte efter symbolske mål. De har kapacitet til at ramme offentlige hjemmesider i sundhedssektoren med DDoS-angreb eller angreb, hvor der indsættes budskaber på hackede hjemmesider. Truslen påvirkes dels af, hvilken holdning eller budskaber aktivister ønsker at promovere, og dels af mediebevågenheden.

MEGET HØJ TRUSSEL:

Cyberkriminalitet

Fremmede stater kan og vil forsøge at stjæle værdifuld information og prøve at forstyrre patientbehandling. Angreb har til formål at tjene penge på afpresning og datatyveri. Store dele af sundhedssektoren er præget af ældre og sårbare systemer, som har ført til, at cyberkriminelle har rettet deres fokus mod disse systemer. Desuden rammes sektoren af tilfældige angreb, som ikke er målrettet sektoren.
Sundhedssektoren i Danmark og udlandet har været ramt af ransomware - herunder WannyCry-angrebet - med direkte konsekvenser for patientbehandlingen.
Angreb mod virksomheder, der forsyner sektoren, for eksempel medicinalvirksomheder kan også påvirke patientbehandlingen.

Kilde: Center for Cybersikkerheds vurdering af cybertruslen mod den danske sundhedssektor, juni 2022.



Trusler gennem tiden

Center for Cybersikkerhed under Forsvarets Efterretningstjeneste definerer cybertrusler således: »Trusler fra cyberangreb, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer eller digitale tjenester«. Trusselsniveauet er baseret på en analyse af aktørernes intention og de menneskelige og materielle ressourcer, aktøren har til rådighed.

Eksempler på cyberangreb:

2015: De første Orangeworm-hackerangreb mod sundhedssektoren. Inficerer røntgen- og MRI-maskiner.

2017: WannaCry. Det britiske sundhedsvæsen er hårdt ramt.

2017: NotPetya. Rammer blandt andet Mærsk og medicinalvirksomheden Merck & Co. Omkostninger: ca. 70 milliarder kroner.

2018: Cyberangreb mod Helse Sør-Øst i Norge. Hackere får adgang til store mængder data.

2018: Hancock Health-hospitalet i USA og patientjournalsystemet Allscripts rammes via fjernadgang.

2020: It-virksomheden GlobalConnect ramt. Påvirker blandt andet medicinproducenten Amgros.

2021: Irlands sundhedsvæsen rammes af ransomware, som lukker it-systemer og kræver månedlangt oprydningsarbejde.

2021: Log4j-sårbarheden i kodesproget JAVA udnyttes verden over.

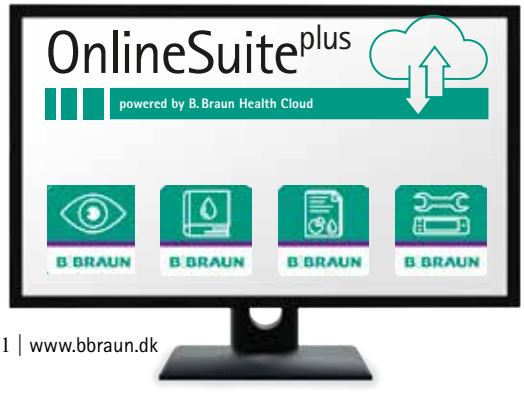
B|BRAUN
SHARING EXPERTISE

GØR DIN HVERDAG NEMMERE MED ONLINESUITE PLUS



Vil du vide mere om, hvordan din hverdag bliver nemmere med OnlineSuite plus?

Kontakt B. Braun Medical allerede i dag.



B. Braun Medical A/S | Dirch Passers Allé 27 | 2000 Frederiksberg | tlf.: 3331 3141 | www.bbraun.dk

»Honeypots« er lokkemad for hackere

For at bekæmpe cybertruslen må vi vide, hvordan hackerne arbejder. Deres metoder kan afsløres med snedige fælder, der tiltrækker hackere som bier til en krukke honning. Disse såkaldte honeypots er derfor et vigtigt forskningsområde.




Af Jens Myrup Pedersen.
Professor - Aalborg Universitet
Shreyas Srinivasa.
Sikkerhedsforsker
- Aalborg Universitet.

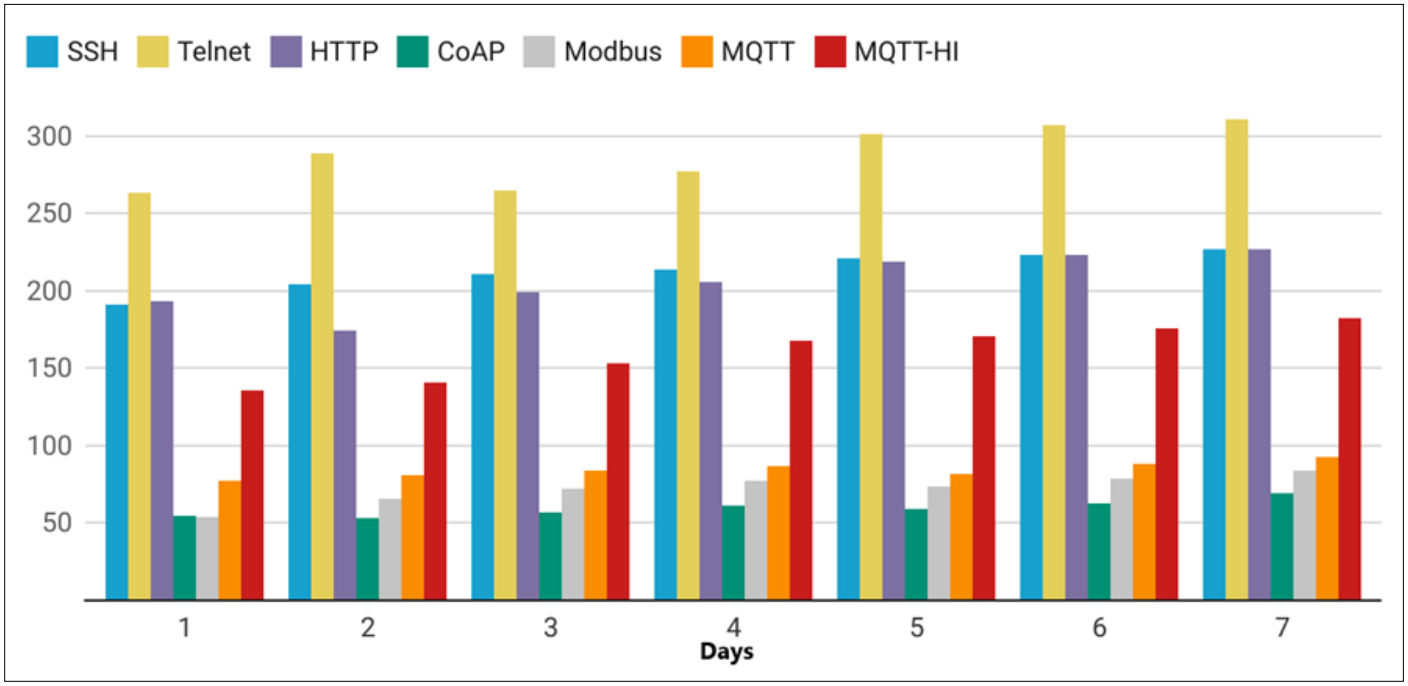
Stadig mere af vores udstyr bliver forbundet til internettet. Det gælder alt fra kameraer, kaffemaskiner og køleskabe til medicinsk udstyr som insulinpumper og pacemakere. Der er masser af fordele ved den udvikling, for det kan hjælpe os til et både sundere, mere komfortabelt og mere bæredygtigt liv.

Men det kommer ikke uden risici, for der er hackere, som vil os det ondt. Kriminelle kan tage udstyret som gidsel og kræve løsesum for at give adgangen tilbage. Statshackere kan være interesseret i målrettede angreb eller spionage imod enkeltpersoner. Cyberaktivister vil bruge udstyret til at angribe andre systemer forbundet til internettet. Farerne er mange, så der er god grund til at tage cybertruslen alvorligt.

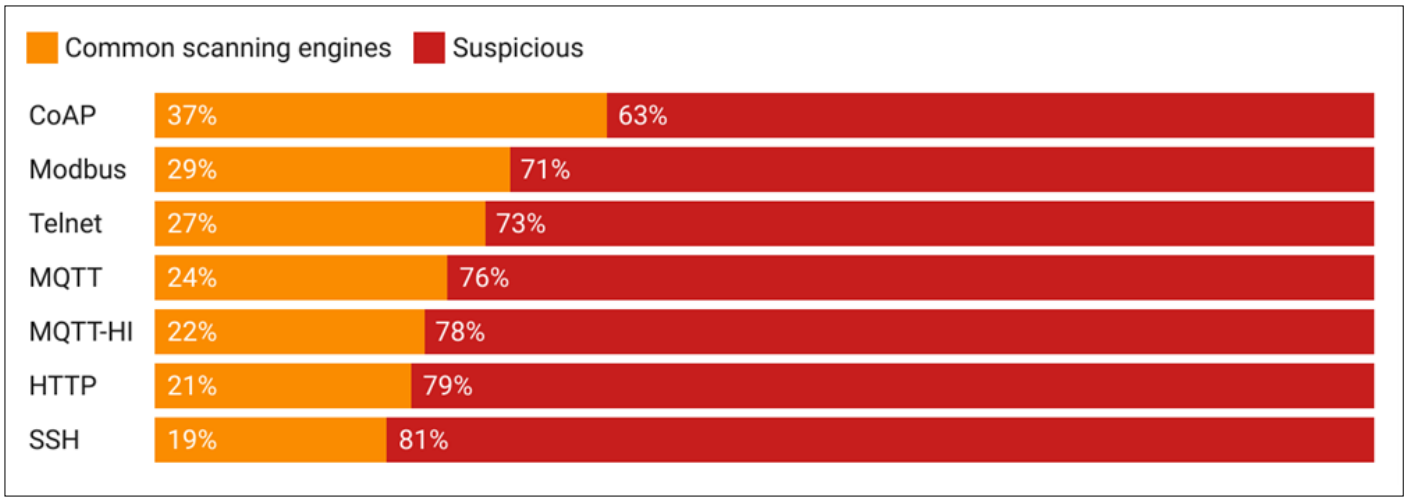
For at kunne adressere cybertruslen bedst muligt er det helt afgørende at vide, hvordan hackerne arbejder. Er der noget særligt udstyr, man går efter i øjeblikket? Er der fundet nogle sårbarheder, som producenterne endnu ikke kender til? Eller er der bestemte grupper, der øger aktiviteterne inden for bestemte områder?

Fordækte fælder

Et af værktøjerne til at forstå, hvordan angrebene løbende udvikler sig, er honeypots. Honeypots er systemer, som udefra ligner og opfører sig som rigtige systemer - for eksempel en computer,



Figur 1. Antal angreb på forskellige protokoller set over en uge.



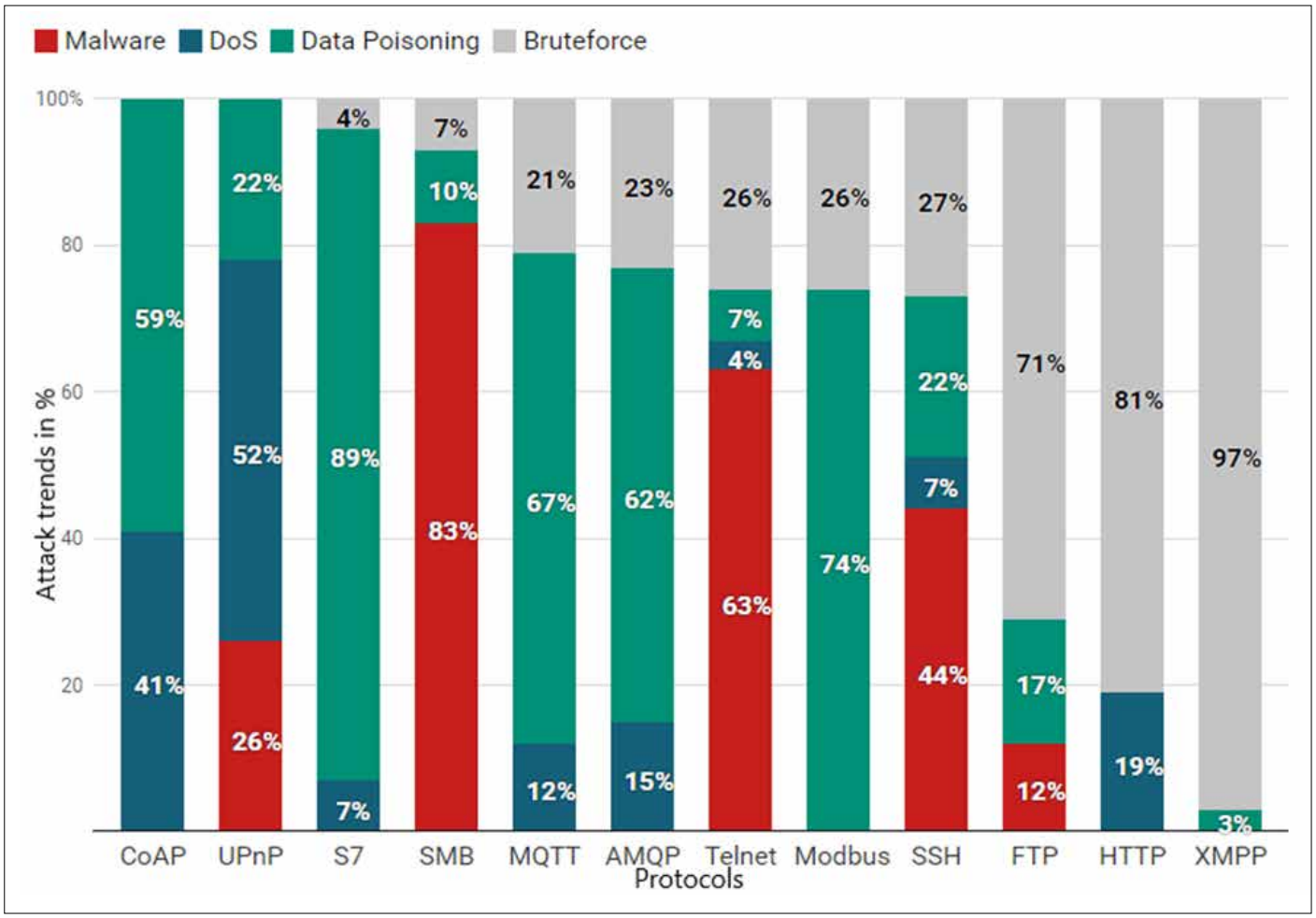
Figur 2. Antallet af angreb, der kommer fra kendte scanning-services, fordelt på protokoller.

et kamera, eller en insulinpumpe - men som i virkeligheden er en fælde, der er sat op for at studere, hvilke angreb der rammer den, og i nogle tilfælde også hvordan hackerne arbejder, når de finder en sådan enhed.
Typisk vil man udstyre dem med standard brugernavne/passwords, hvis der da overhovedet er et password. På den måde får man hackerne indenfor, så man kan se, hvilke kommandoer de bruger m.m. Man kan også bruge honeypots som »sladrehank«, hvor man ikke forbinder dem direkte til internettet, men har dem på indersiden af en organisations netværk. På den måde ved man, at der aldrig bør være aktivitet i den del af ens netværk. Hvis der alligevel er netværkstrafik eller forsøg på at forbinde til disse honeypots, er det tegn på ubudne gæster, som man så kan udforske nærmere.

Skidt fra kanel

Det lyder måske alt sammen meget simpelt, men i virkeligheden er honeypots et stort og selvstændigt forskningsområde. For det er ikke så ligetil at bygge systemer, der vitterligt ligner rigtige systemer og svarer tilbage som sådan. Det er blandt andet vigtigt at undgå »fingerprinting«, altså at de onde hackere er i stand til at se, at der er tale om en honeypot. Ellers risikerer man, at de aldrig kommer igen. Eller endnu værre: At de opfører sig på en anden måde, end de ellers ville gøre, og dermed forurener de opsamlede data.
Tilsvarende er det vigtigt at kunne skelne skidt fra kanel, når man analyserer de data, man indsamler. For det er ikke kun hackere, der kommer på besøg. Der findes en lang række online-tjenester, som løbende scanner internettet og laver ret detaljerede kortlægninger af det, de finder på nettet. Det gælder for eksempel tjenester som Shodan (shodan.io) og ZoomEye (zoomeye.org). Disse sætter ▶





Figur 3. Typer af angreb mod forskellige protokoller gennem april måned 2021.



også spor i vores honeypots, men er ikke udtryk for angreb. Så for at få et retvisende billede af, hvordan hackerne opfører sig, er det nødvendigt at identificere og bortfiltrere den slags søgninger.

To typer

Når man etablerer honeypots, skelner man generelt mellem »low-interaction« og »high-interaction« honeypots.
Med et low-interaction honeypot giver man kun angriberen adgang til den yderste »skal« af systemet. Man kan typisk forbinde med forskellige protokoller, men så snart man er inde, er det meget begrænset, hvad interaktion der sker. Low-interaction honeypots er lette at sætte op, billige at drifte og ret sikre for dem, der etablerer dem. De er også fine til at give et overblik for eksempel over, hvilke protokoller der udsættes for angreb. Men det er meget begrænset, hvad man ellers kan sige om hackernes

adfærd, da de jo netop ikke tillader væsentlig interaktion.
Med et high-interaction honeypot er det muligt at indsamle langt mere data om hackernes adfærd. Her stiller man nemlig et fuldt system til rådighed, hvor hackerne kan interagere (næsten) som om, det var et rigtigt system. Dette afhænger selvfølgelig af, hvor grundigt og præcist systemet svarer til det rigtige system.
Til gengæld kræver det væsentligt flere ressourcer at bygge og vedligeholde high-interaction honeypots. Og risikoen for, at hackerne finder sårbarheder, der kan udnyttes, for eksempel til at komme videre til andre systemer, eller til at udnytte honeypot'en til at angribe andre, bliver også større.

Afslører angreb

På Aalborg Universitet har vi arbejdet en del med forskellige typer honeypots. Vi har blandt andet bygget RIoTPot, som er et »hybrid-interaction« honeypot,

Honeypots er systemer, som udefra ligner og opfører sig som rigtige systemer - for eksempel en computer, et kamera, eller en insulinpumpe - men som i virkeligheden er en fælde, der er sat op for at studere, hvilke angreb der rammer den, og i nogle tilfælde også hvordan hackerne arbejder, når de finder en sådan enhed.

der er målrettet de mange enheder, som forbindes til internettet - altså såkaldte »Internet of Things« (IoT) og »Operational Technology« (OT).
Det er et plug-and-play system, hvor visse protokoller emuleres med et low-interaction honeypot, mens udvalgte protokoller, som man er særligt interesseret i, kan emuleres med high-interaction funktionalitet. Det er således muligt at udvikle specifikke plugins, der modsvarer specifikke enheder.
De første resultater fra RIoTPot demonstrerer blandt andet, hvordan man kan se antallet af angreb på forskellige protokoller udvikle sig over en uge *(figur 1)*.
Man kan også se, hvor stor en del af den observerede angrebstrafik der kommer fra de gænge scanning-services, og dermed ikke er indikationer på skadelig trafik. Disse kan ses i *figur 2*.
High-interaction honeypots giver mulighed for langt mere detaljerede analyser af angrebene, hvor man for eksempel kan aflæse alle de kommandoer, en hacker bruger, når vedkommende er inde i systemet og interagerer med det.
Andre eksempler på mulige resultater ses i *figur 3* og *figur 4*. Begge er baseret på et studie, vi lavede over april måned i 2021, hvor vi satte seks forskellige honeypots op:
Figur 3 opsummerer de forskellige typer af angreb mod forskellige protokoller, herunder om der blev forsøgt installeret/uploadet malware, om data i systemet ▶

EE Healthcare

ARC 100
– perfekt til mindre procedurer

ARC 100 DIATERMIAPPARAT
• Lille kompakt 100 watts løsning.
• 5 vævseffekter:
· 1 bipolar koagulation
· 2 monopolære cutting funktioner
· 2 monopolære koagulations funktioner

PRIS: KR. 15.715,-





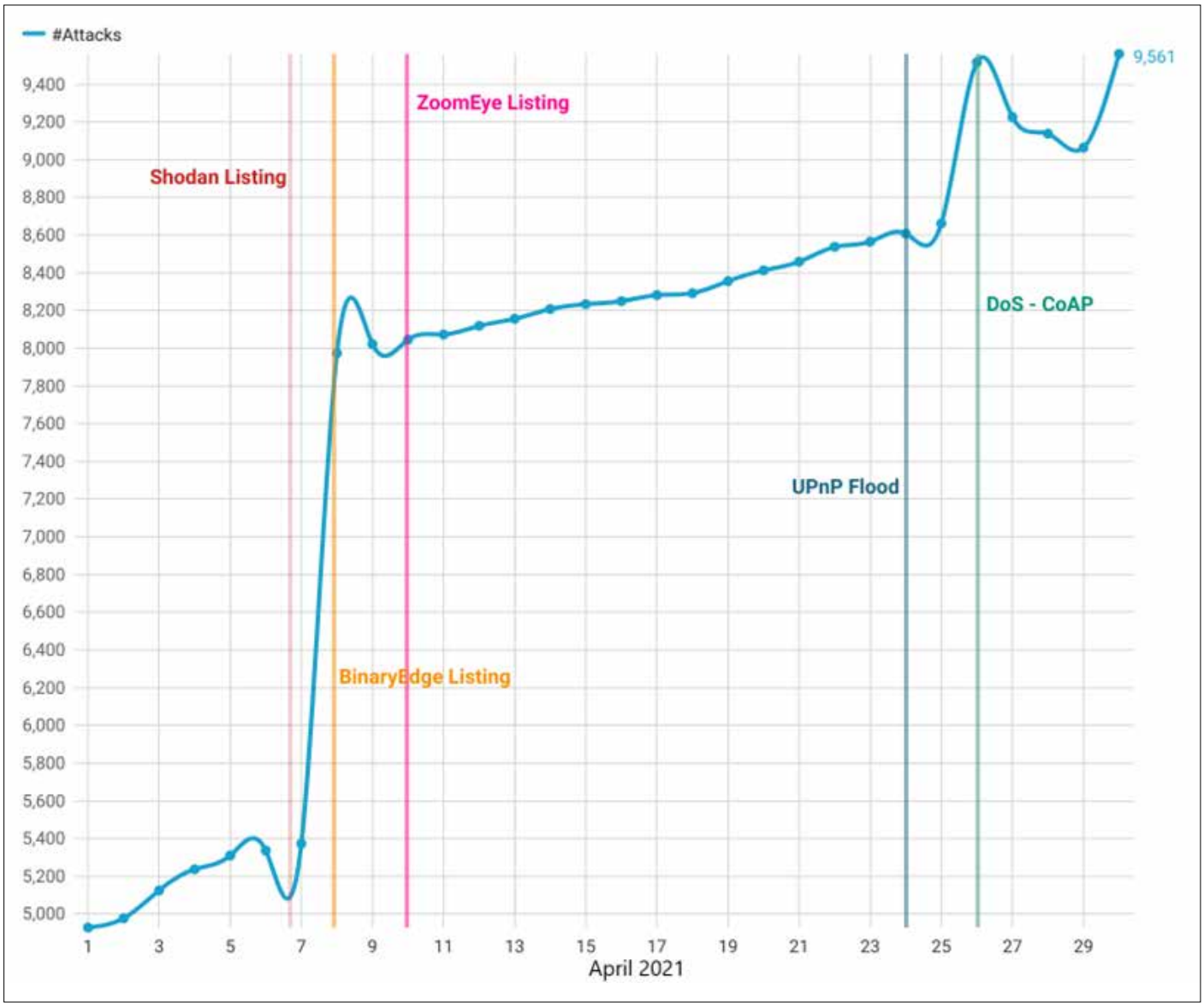
BOWA MEDICAL

Bowa har også et stort udvalg af kabler og adaptere – se mere på **www.ee-healthcare.dk**

SERVICE • PRÆCISION • TILGÆNGELIGHED

EE Healthcare
Gl. Landevej 2 | 2600 Glostrup
Tel +45 28 95 01 93 | info@ee-healthcare.dk | www.ee-healthcare.dk

DANAK
DANAK-logo/reg. Nr. 485
EE Kalibrering tilbyder DANAK-akkrediteret kalibrering og re-verificering af medicinske vægte



Figur 4. Det totale antal angreb mod seks honeypots gennem april 2021 - med indikation af hvornår de blev fundet af forskellige søgemaskiner.

Når man etablerer honeypots, skelner man generelt mellem »low-interaction« og »high-interaction« honeypots.

blev forsøgt ændret (dataforgiftning), eller om der var tale om for eksempel brute-force angreb, hvor man forsøger at gætte brugernavne og passwords.
Figur 4 viser antallet af angreb over tid i løbet af måneden, herunder hvordan antallet af angreb steg, efter vores honeypot var fundet og listet i forskellige søgemaskiner.

Vigtig viden

Dette er blot nogle få eksempler på de indsigter, man kan få ved hjælp af honeypots.
Der er ingen tvivl om, at vi også inden for det medicinske område fortsat vil se, at flere og flere enheder forbindes til internettet. Det giver nogle sikkerhedsmæssige udfordringer, der bør adresseres gennem en række tiltag:

- Sikkerhed skal tænkes ind fra begyndelsen.
- Netværk skal beskyttes og overvåges.
- Systemer og enheder skal løbende opdateres.
- Og man skal have en plan for, hvordan man håndterer angreb på systemer og enheder.

Honeypots kan være en vigtig del af løsningen, fordi viden om angreb og angrebstrends kan hjælpe med at vælge og prioritere de rigtige modforanstaltninger.

Komplekse it-systemer er sårbare

Selv om et enkelt it-system er sikkert, så er sammenbundne - og dermed komplekse - systemer i høj grad sårbare for angreb fra it-kriminelle.



Af Normann Aa. Nielsen.
It-arkitekt, Regional IT
- Region Syddanmark



Når data udveksles på tværs af systemer, kan det let blive sårbart.

Som ung programmør arbejdede jeg i 80'erne med at opbygge et simpelt patientsystem for Arbejdsmedicinsk klinik i Aarhus. Det var på en computer uden forbindelse til omverdenen - i en tid, hvor der endnu ikke fandtes computervirus. Maskinen stod i et aflåst lokale, og den eneste form for sikkerhed handlede om enkel passwordstyring. Det var nemmere i gamle dage!

I dag anses det som et spørgsmål om kort tid, før de store danske systemer i sundhedssektoren bliver hårdt ramt af angreb fra it-kriminelle. En af grundene er den store kompleksitet i it-systemerne.

Mange systemer er sikre nok i sig selv, men når der udveksles data med andre systemer, kan den valgte kommunikationsform være sårbar. Et eksempel er de såkaldte SCADA-systemer, der oprindeligt blev designet til at være åbne, robuste og nemme at bruge og fejlfinde. Derfor vælges disse systemer ofte til overvågning og styring af produktion. I sundhedssektoren kan det være styring af elevatorer, kølesystemer, pumper og lys - eller kontrol og overvågning af udstyr på en operationsstue.

Men disse systemer kritiseres for ikke at være designet med øje for sikkerhed. Så her er en sårbar grundstruktur, hvor kriminelle kan overtage fuld kontrol med systemet - med stor risiko for patienterne.

Sårbar struktur

Der har længe været en forventning om, at kriminelle ikke angriber sundhedssektoren, men ifølge Center for Cybersikkerhed er denne holdning naiv. I dag er risikoen endog meget høj. Så sent som august 2022 blev det engelske sundhedsvæsen udsat for et ransomware-angreb, hvor kritiske patientdata blev krypteret med krav om løsesum.

De fem regioner har som hovedopgaver sundhedsvæsenet, regional udvikling og drift af en række sociale institutioner. Disse områder har mange lokale strukturer, som bindes sammen af et utal af it-systemer, både meget store og meget små. Noget af denne mangfoldighed skyldes, at de fem regioner er selvstændige med hver deres it-strategi, så der ikke altid kan opnås en fælles koordination af indkøb og samkøring af it-systemer.

Samfundets stigende digitalisering har øget risikoen for digitale angreb. Trusler som hackerangreb, virus, ransomware og phishingmails kan ramme alle. Andre trusler er særlige for regionerne, hvor især sundhedsdata og andre personfølsomme data er oplagte mål. Center for Cybersikkerhed vurderer trusselsniveauet som meget alvorligt.

Også fordele

Sundhedsvæsenets kompleksitet giver naturligvis problemer, så ved hvert folketingsvalg får politikere den gode idé, at it-systemerne skal samles. Vi kender debatten om de forskellige elektroniske patientjournaler, og om regionerne skal nedlægges. ▶



Hvis kriminelle tager kontrol over operationsstuen, kan det medføre stor risiko for patienterne. (Foto: David Mark, Pixabay).

I dag anses det som et spørgsmål om kort tid, før de store danske systemer i sundheds-sektoren bliver hårdt ramt af angreb fra it-kriminelle. En af grundene er den store kompleksitet i it-systemerne.

Men stor kompleksitet kan også være en fordel. Fra landbruget ved vi, at høj grad af ensartethed øger sårbarheden over for sygdomme. En artikel i Zetland fortæller om problemer med produktion af bananer, der er udfordret af svampeangreb. Svampene kan brede sig alt for hurtigt i plantagernes monokulturer. Med mere biodiversitet ville angrebet gå langsommere, og måske kunne det afværges.
Hver eneste region oplever dagligt titusindvis af angreb på de forskellige infrastrukturer. Så måske kan man håbe på, at den regionale decentralisering er en hjælp: Hvis et angreb lykkes på én region, vil det være svært at fortsætte til en anden region.

National sårbarhed

Andre it-systemer er nationale og dermed centrale. Hvis de rammes, påvirkes også de decentrale systemer, som er koblet op til disse. En meget vigtig komponent er MitID, som ikke kun bruges af borgerne for at komme ind på banksystemer. MitID er en central komponent for systemer i sundheds-sektoren, som ønsker at forbinde sig med hinanden.
Desværre er MitID også et centralt system, der er følsomt over for sårbarheder. For eksempel fik MitID i oktober 2022 et nedbrud, der gjorde tjenesten komplet utilgængelig i mere end to timer. I dette tidsrum var det ikke muligt for andre systemer at etablere nye forbindelser gennem MitID. Heldigvis blev de to timer ikke kritiske, da allerede oprettede forbindelser kunne fortsætte. Men situationen var alvorlig nok.

Og international ...

Nogle systemer kompliceres ved, at de ikke har en central kerne, men i stedet er opbygget i netværk. Den Nationale Henvisningsformidling (DNHF) er baseret på en såkaldt cloud-løsning, hvor de (krypterede) data gemmes hos et amerikansk it-firma et sted i Holland. Samtidig er løsningen integreret med danske praksissystemer og regionernes sundhedssystemer. Dette giver en risiko for, at udenlandske interesser kan påvirke sikkerheden, uden at den danske regering kan gribe ind.
I det hele taget åbner cloud-løsninger for en kompleksitet, hvor der endnu ikke er klare erfaringer, der kan støtte risikovurderinger. Den danske stat har en række krav til, at nogle it-løsninger skal placeres geografisk i Danmark. Det gælder for eksempel CPR-registeret og MitID. Tanken er, at disse løsninger er så vitale, at de altid skal kunne kontrolleres af danske myndigheder, også i en krisesituation. Alligevel er de sårbare, fordi de har berøringsflader med et utal af systemer, der også kan være interna-

tionale. Dermed er systemerne de facto udstillet i verden. Og dermed sårbare.

Værktøj til kompleksitet

Inden for cybersikkerhed er det sådan, at mere eksponering giver flere sårbarheder, og ingen it-systemer kan regnes for sikre. Men der findes en række værktøjer, som kan hjælpe med at finde sårbarheder. Et eksempel er CIS-18 sikkerhedskontrollerne, som definerer en række målepunkter til at finde de svage steder i en organisation: Hvilket udstyr har jeg, og hvor er det? Hvad bruger jeg det til? Hvordan opdager jeg forsøg på uautoriseret adgang, og hvad har jeg gjort for at stoppe det? Med andre ord synes disse kontroller at være et udtryk for sund fornuft.

Andre værktøjer er forordninger og lovgivning. EU's forordning »Netværk og Informations Sikkerhed version 2« (NIS2), trådte i kraft 16. januar i år, og EU-landene har 21 måneder til at indføre den. NIS2 ønsker, at EU-landene øger indsatsen for at sikre den kritiske infrastruktur, herunder sundhed, energi, vand og fødevarer, mod it-kriminelle. Blandt andet lægger NIS2 op til et unionssamarbejde, hvor indberettet viden om trusler og modsvar udveksles hurtigt. For at sikre, at NIS2 tages alvorligt, er der fastsat administrative sanktioner for brud på reglerne - blandt andet bøder og eventuelt inddragelse af ledelsesansvar. Det sidste er nyt: Lederen af en privat eller offentlig virksomhed er ikke immun, men kan også blive ramt af sanktioner, hvis reglerne ikke følges.

Nye tider

Måske er det nødvendigt. I 2018 deltog jeg på en konference om den da kommende databeskyttelseslov (GDPR), hvor en hovedtaler erklærede, at hvis han skulle følge denne lov, ville han »være ude af drift inden for et par måneder!«. Så slemt håber jeg ikke, det gik. Og i realiteten er GDPR, sammen med NIS2, værktøjer, der forsøger at sikre de sårbarheder, som opstår i en kompleks verden. GDPR gør det i forhold til persondata, NIS2 gør det i forhold til drift og anlæg.

I 1986 havde jeg et antivirussystem, som sikrede mig mod alle kendte virus. Dengang var der 21!

Nu er verden mere kompleks, og dermed mere sårbar. En aktiv forståelse af dette er nødvendig, så de rette værktøjer kan bruges til en forbedring af sikkerheden. For vi er under angreb.



MitID er et eksempel på et centralt system, der er følsomt over for sårbarheder. I oktober 2022 var tjenesten utilgængelig i over to timer pga. et nedbrud.



MED SPACE^PLUS KAN DU OPDATERE SOFTWARE OG MEDICINLISTER - UANSET HVOR DU ER

reddot winner 2021
iF International Forum Design
DESIGN AWARD 2021

B. Braun Medical A/S | Dirch Passers Allé 27 | 2000 Frederiksberg | tlf.: 3331 3141 | www.bbraun.dk

Digitalisering er både løsningen og truslen

Hvis vi ikke passer på, kan vi digitalisere sundhedsvæsenet ud af én krise - og direkte over i en ny.
Med øget digitalisering følger nemlig en øget sårbarhed over for digitale cyberangreb på vores sundhedsvæsen.



Af Martin Jensen Buch.
Chefkonsulent
- IT-Branchen

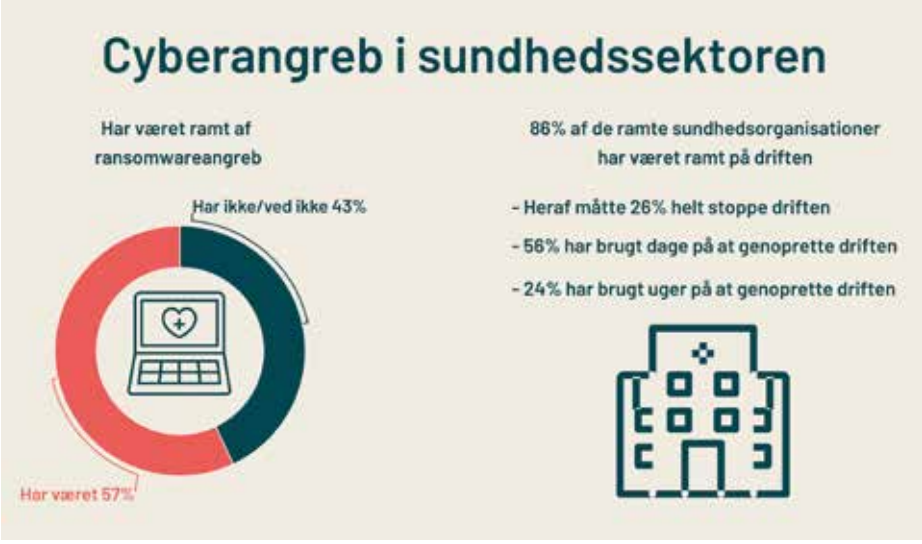
Færre hænder, flere syge og et voksende antal administrative opgaver presser sundhedsvæsenet som aldrig før. De kommende år vil antallet af ældre og borgere med kroniske sygdomme blive fordoblet, og der vil være færre borgere i den arbejdsdygtige alder til at tage hånd om dem.
Det er utopi at tro, at vi kan løse de demografiske udfordringer ved blot at ansætte flere i sundhedsvæsenet. For de ekstra hænder findes ganske enkelt ikke. Lige nu er der over 5000 ubesatte sygeplejestillinger, og dertil skal lægges, at omkring 3200 SOSU'er snart går på pension. Så allerede i dag er der mangel på sundhedsfagligt uddannede, og den udfordring vil kun vokse med tiden.
Digitalisering er, om man vil det eller ej, en væsentlig del af svaret på disse udfordringer. Det er afgørende for vores sundhedsvæsens fremtid, at vi prioriterer en digital indsats, der kan flytte ressourcer fra administration, planlægning og opfølgning over til den vigtige patientkontakt.
Men i takt med at vi bliver mere og mere afhængige af de digitale løsninger, skal vi også være klar på at håndtere de stigende risici, som er knyttet til dem. Primært de sikkerhedsmæssige udfordringer, der følger med.

Vi er under angreb

Ifølge en analyse fra sikkerhedsfirmaet Trend Micro, der har spurgt 2958 beslutningstagere i 26 lande, har 57 procent af sundhedsorganisationerne inden for de seneste år oplevet såkaldte ransomware-angreb, hvor data krypteres med krav om løsesum.
Ligesom et cyberangreb kan lamme en logistikvirksomhed som Mærsk eller en teknologivirksomhed som Demant, kan det også standse al behandling på et hospital.
Allerede i dag bruger vi digitale løsninger til at styre alt fra vagtplaner og patientinformation til medicindosering og behandlingsforløb. Uden adgang til de digitale systemer vil vi ikke vide, hvem der er indlagt, hvad de fejler, hvilken behandling der er planlagt, eller hvem der er på arbejde.
Trend Micro-analysen viser også, at 86 procent af de ramte sundhedsorganisationer har været ramt på driften, mens 26 procent helt har måttet stoppe driften. De fleste har brugt dage (56 procent) eller endda uger (24 procent) på at genoprette funktioner, som blev ramt af hackerangreb.
Den besparelse eller de ekstra hænder, vi kan frikøbe med en øget digitalisering, kan altså nemt blive spist op af de produktionstab, som følger af et hackerangreb.
Men risikoen er ikke bare et kæmpe produktionstab. I sidste ende kan det koste menneskeliv, hvis for eksempel væsent-



Ifølge Trend Micro har 57 procent af sundhedsorganisationerne inden for de seneste år oplevet såkaldte ransomware-angreb, hvor data krypteres med krav om løsesum.



En undersøgelse fra sikkerhedsfirmaet Trend Micro viser, at cyberangreb allerede er et stort problem i sundhedssektoren.



lige sundhedsdata bliver kompromitteret eller ikke er tilgængelige i afgørende situationer.

To angreb dominerer

Indtil nu har sundhedsvæsenet primært været udsat for to typer af cybertrusler:

- Egentlig cyberkriminalitet, der har til formål at afpresse sundhedsvæsenet for penge gennem ransomware-angreb.
- Cyberspionage, hvor udenlandske aktører har været ude efter de værdifulde danske sundhedsdata eller forskningsresultater.

I takt med at den globale sikkerhedssituation er blevet forværret, vurderer Center for Cybersikkerhed også, at risikoen for cyberaktivisme er stigende. Det vil sige angreb, der har til formål at lække fortrolige oplysninger eller blokere for digitale tjenester.
Samlet set er truslen mod sundhedsvæsenet markant stigende.
Sundhedsvæsenet er et meget attraktivt mål for mange hackere. Både fordi her er tale om meget kritisk infrastruktur, og fordi sundhedsvæsenet har adgang til værdifulde data og viden. Samtidig er der stort offentligt fokus på sundhedsvæsenet, hvilket gør, at destruktive angreb kan skabe stor opmærksomhed.



Vi får stadig flere ældre og syge - og færre til at tage sig af dem. Dette misforhold kan kun løses med massiv digitalisering, men hermed bliver vi mere sårbare over for digitale cyberangreb.

Kræver markant indsats

I takt med den øgede digitalisering af sundhedsvæsenet er det derfor afgørende, at sikkerheden følger med.
Regeringen har annonceret store reformer og digitale indsatser i vores sundhedsvæsen, blandt andet en akutpakke, en strukturreform og en sundhedsfond. Alle initiativer, der må formodes at indeholde digitale indsatser.
Hospitalernes økonomi er i forvejen presset af driften, og råderummet til at sikre udvikling og implementering af nye løsninger er lille. Det er derfor afgørende, at de digitale indsatser bakkes op af et øget fokus på cybersikkerhed, og ikke mindst at der følger penge med til en sådan prioritering.
Cybersikkerhed er traditionelt set en af de indsatser, som først bliver klemt i et stramt budget. Det efterlader en stigende »cybergæld«, som skal betales før eller senere.
Vi bliver derfor nødt til at finde midlerne til at investere markant i bedre cybersikkerhed i sundhedsvæsenet. Det er nødvendigt for at betale den cybergæld, der allerede er oparbejdet, men også for at kunne matche den digitale videreudvikling af sundhedsvæsenet, som regeringen har igangsat med en styrkelse af sikkerheden.

Menneskelige fejl

Samtidig har vi brug for at styrke kompetencerne i sundhedsvæsenet gennem obligatoriske kurser i cybersikkerhed. Ikke bare i forhold til spidskompetencer hos nogle få sikkerhedseksperter, men

Uden adgang til digitale systemer vil vi ikke vide, hvem der er indlagt, hvad de fejler, hvilken behandling der er planlagt, eller hvem der er på arbejde.

også de helt generelle kompetencer hos alle sundhedsvæsenets ansatte.
Ifølge Verizon skyldes 82 procent af alle cyberangreb menneskelige fejl, og medarbejderne er og bliver den største sikkerhedsrisiko i de fleste organisationer.
Endelig er der brug for øget koordination og samarbejde mellem myndighederne på tværs af stat, region og kommune. Sundhedsvæsenet er tværgående i sin natur, og det samme er cybertruslerne. Hvad der rammer en kommune i dag, kan ramme et hospital i morgen.
Vi har brug for øget videndeling og et tæt operationelt samarbejde, så der er klarhed om myndighedsansvar, og de offentlige myndigheder lever op til nogle ensartede sikkerhedskrav.
Hvis vi ikke prioriterer disse indsatser for at styrke sundhedsvæsenets cybersikkerhed, vil det digitale løft, der frigiver arbejdskraft, være som at tisse i bukserne. Det vil lune ganske kortvarigt, mens utallige sikkerhedsbrud vil overtage som sundhedsvæsenets nye altoverskyggende krise.

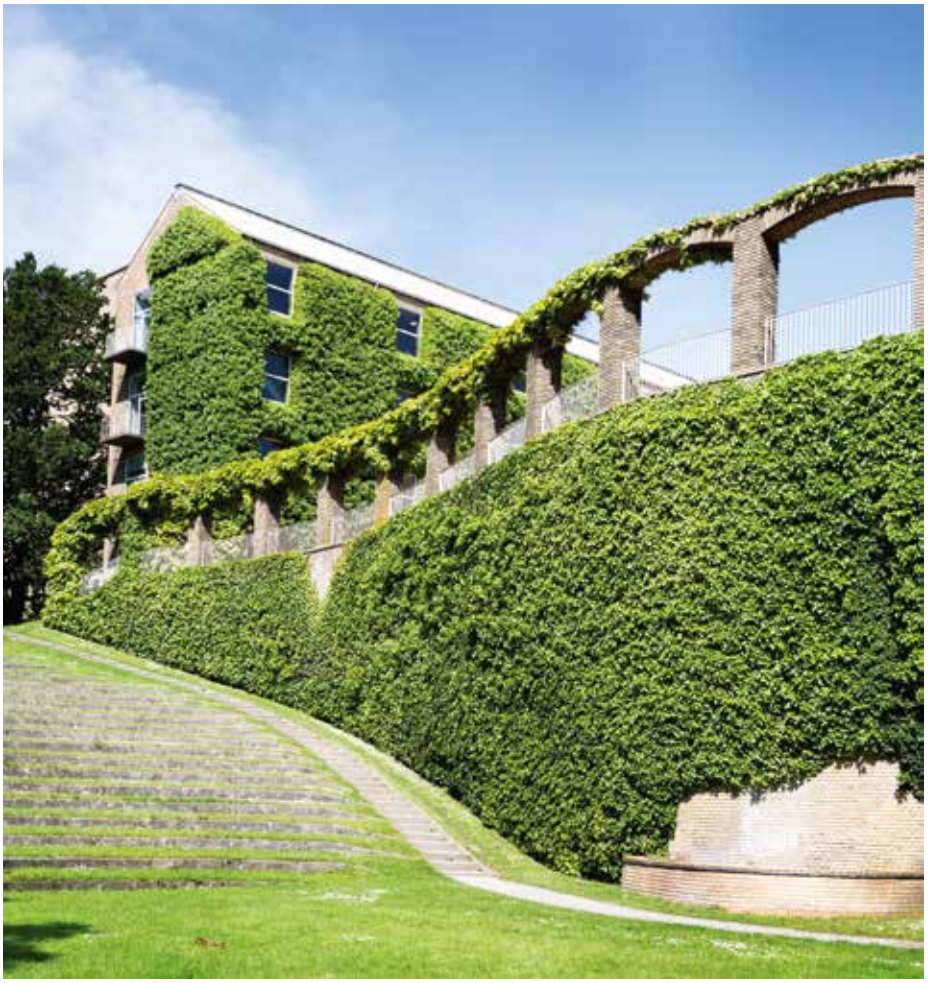
Aarhus i offensiven for cybersikkerhed

Et kraftcenter for forskning, innovation og erhvervsudvikling skal bringe Danmark i front inden for cybersikkerhed. Målet er at beskytte både virksomheder og offentlige institutioner mod digitale angreb.



Af Henriette Stevnhøj.
Kommunikations-medarbejder
- Aarhus Universitet
Aarhus Kommune har bidraget til teksten

Truslen mod cybersikkerhed kræver, at offentlige myndigheder, vidensinstitutioner og virksomheder tager ansvar for at styrke sikkerheden. Aarhus har allerede en styrkeposition på området, og nu skrues der endnu mere op for samarbejdet mellem myndigheder, vidensinstitutioner og erhvervslivet i Aarhus i form af et kraftcenter inden for cybersikkerhed, »Security Tech Space«.
Bag det planlagte center står Aarhus Kommune, Aarhus Universitet og toneangivende it-virksomheder i Aarhus. Forventningen er, at parterne vil stå endnu stærkere gennem et tæt og systematisk samarbejde med fokus på forskning, innovation og erhvervsudvikling.
Security Tech Space vil være et supplement til det eksisterende Center for Cybersikkerhed under Forsvaret. Det forventes oprettet i IT-Byen Katrinebjerg i Aarhus, der er et af landets største it-videns- og innovationsmiljøer.



Aarhus Universitet har nogle af verdens dygtigste forskere inden for cybersikkerhed. (Foto: Lars Kruse/Aarhus Universitet).

Åbenlyst behov

Security Tech Space skal fokusere på virksomhedssiden af cyber- og informationssikkerhed i form af viden fra den nyeste forskning, uddannelse og efteruddannelse, rekruttering, iværksætteri mv. Hertil kommer branding og eksport af danske kompetencer og produkter inden for cybersikkerhed.
Borgmester Jacob Bundsgaard siger om initiativet:
- Truslen fra cyberkriminalitet og cyberspionage er højere end nogensinde, og vores lokale og nationale behov for at styrke området er åbenlyst. Aarhus og Østjylland udgør allerede i dag et stærkt miljø inden for cyber- og informationssikkerhed, og det rummer store fremtidsperspektiver. Samtidig kan vi med en målrettet indsats udfolde et markant erhvervspotentiale på området med store, internationale ambitioner.
Rektor ved Aarhus Universitet, Brian Bech Nielsen, ser frem til samarbejdet:
- Det ligger i naturlig forlængelse af Aarhus Universitets virke i samfundet, at universitetet leverer forskningsbaseret viden til at sikre større cybersikkerhed for virksomheder - og dermed borgere i Aarhus. Men det er ikke alene pligten, som driver universitetet. Det er også ambitionen om at være med til at skabe løsninger, som kan betrygge os i, at vi bor i et sikkert hjørne af Danmark. AU har nogle af verdens dygtigste forskere inden for cybersikkerhed, og vi glæder os til at bidrage.

Lokale virksomheder

Hos softwarevirksomheden Systematic, som udvikler kritisk it-infrastruktur til blandt andet forsvar og sundhedsvæsen, ser CEO Michael Holm positivt på etableringen af et kraftcenter for cybersikkerhed i byen:

- Som verden udvikler sig, stiger behovet for beskyttelse af kritisk infrastruktur, som i dag er et reelt mål for destruktive kræfter med et ønske om at destabilisere samfundet eller berige sig selv. Aarhus og Østjylland er base for nogle af Danmarks største it-virksomheder inden for forsvars- og sundhedsteknologi, der er stærkt afhængige af datasikkerhed og beskyttelse. At samle praktisk erfaring, ekspertise og viden om cybersikkerhed i et stærkt forsknings- og innovationsmiljø i Aarhus vil gavne virksomheder og offentlige institutioner over hele landet - for slet ikke at tale om det internationale fokus, et sådan center vil tiltrække, siger Michael Holm.

Henrik Skovfoged, business unit lead, Trifork Security, supplerer:

- Jeg ser en kæmpe styrke i, at vi kan samarbejde omkring cybersikkerhed på tværs af det private og det offentlige. En af de ting, vi mangler i Danmark, er det, jeg kalder »håndværkere«, der kan være med til at implementere en ordentlig form for cybersikkerhed ude i virksomhederne. Det er samtidig vigtigt, at vi også har dialog mellem universitetet og erhvervslivet omkring uddannelse, fordi vi både har behov for nogle meget dygtige uddannede inden for kryptering og avancerede former for cybersikkerhed, men også pragmatikerne, der kan implementere.

Kræver statsligt engagement

I forbindelse med forhandlingerne om et nyt forsvarsforlig fremhæver Aarhus Kommune behovet for statsligt engagement til en styrkelse af cybersikkerhed gennem etablering af Security Tech Space i Aarhus. De væsentligste pointer i den forbindelse er følgende:

- Aarhus Universitet huser stærke forskningsmiljøer på det natur- og teknisk videnskabelige område inden for cybersikkerhed. Som eksempel er Institut for Datalogi placeret i top tre på forskningsfeltet kryptologi på verdensplan, ligesom Alexandra Instituttet i Aarhus rådgiver virksomheder i hele Danmark om innovativ brug af it-sikkerhedsteknologier.
- Der er en række stærke it-sikkerheds- og blockchainvirksomheder - flere udsprunget af det aarhusianske universitetsmiljø - der arbejder med it-sikkerhed på meget højt niveau. Det aarhusianske miljø har blandt andet været med til at udvikle NemID og MitID-løsningerne.
- Aarhus Universitet har som et af sine særlige strategiske fokusområder at uddanne endnu flere it-specialister og ingeniører, og universitetet vil i de kommende år gennemføre en markant udbygning af et nyt techcampus på Katrinebjerg.
- Forskerparken INCUBA huser over 200 startups, scaleups og etablerede virksomheder som for eksempel Concordium, Partisia og Bankdata. I disse år udvider INCUBA med 22.000 kvadratmeter på Katrinebjerg i Aarhus - designet til at huse scaleups og udviklingsteams fra førende it- og techvirksomheder.
- På baggrund af Aarhus' styrkeposition på området, samt det øgede trusselsbillede, tog Aarhus Kommune allerede i august initiativ til oprettelsen af et konsortium for cyber- og informationssikkerhed med deltagelse af vidensinstitutioner, offentlige myndigheder, lokale og internationale virksomheder samt interesseorganisationer inden for it-sikkerhedsområdet.



Det planlagte center bygger på et tæt samarbejde mellem Aarhus Kommune, Aarhus Universitet og toneangivende it-virksomheder i Aarhus. (Foto: Lars Kruse/Aarhus Universitet).



Digitale angreb

- Aarhus Kommune afværger dagligt ca. 25.000-30.000 målrettede digitale angreb på Aarhus Kommunes medarbejdere.
- Her er blandt andet tale om såkaldte phishing attacks, spoof attacks, malware attacks og lignende.
- Region Midtjylland oplyste i november, at der alene i uge 45 blev afværget 145 millioner angreb imod Aarhus Universitetshospital.

Sammen om **sundhed hjemmefra**

Med »Det Digitale Sundhedscenter« kan borgere med kroniske sygdomme (eller risiko for at udvikle dem) og sundhedsprofessionelle være sammen om sundhed hjemmefra.




Af Anna-Britt Krog.
It-projektleder og
Marie Damgaard Starklint.
Projektmedarbejder - begge fra
Syddansk Sundhedsinnovation

20 kommuner, flere patientforeninger og Region Syddanmark står bag Det Digitale Sundhedscenter, som blev etableret i 2015. Det har siden dannet ramme om digitale patientuddannelser og livsstilsforløb, som støtter borgere med kronisk sygdom og borgere med behov for sundere vaner med at mestre deres sygdom og sundhed, så de kan leve et godt liv med forbedret livskvalitet.

> **Appen fremmer den gode dialog, hvor borgeren i højere grad bliver medspiller, og dialogen tager udgangspunkt i borgerens behov.**
>
> *Fagperson.*

Omdrejningspunktet for Det Digitale Sundhedscenter er udvikling og integration af digitale løsninger i og på tværs af kommunernes sundhedscentre, så digitale løsninger understøtter og supplerer sundhedsfremmende og forebyggende tilbud, som sundhedscentrene allerede tilbyder. I en tid med stor mangel på sundhedsfaglige og et stigende antal kronikere sikrer partnerskabet ressourceudnyttelse på tværs af kommuner.

Kommunerne finansierer driften af Det Digitale Sundhedscenter i fællesskab. Region Syddanmark har en koordinerende rolle i udvikling, afprøvning og udbredelse af konceptet, og regionen agerer således som et bindeled mellem de udførende kommuner og øvrige partnere.

»Mit liv - min sundhed«

Digitale tilbud kan tiltrække målgrupper, som normalt ikke bruger kommunale tilbud. Derfor udviklede borgere, sundhedsfaglige fra partnerskabskommuner, patientforeninger og app-bureauet Makeable sammen første version af appen »Mit liv - min sundhed« tilbage i januar 2019. Borgerne har via appen adgang til digitale forløb hjemmefra, og flere får derved mulighed for at deltage i sundhedsfremmende tilbud.
Denne første version blev udviklet som borgerens indgang til støtte og viden om type 2-diabetes - og som et dialogstøtteredskab mellem borgeren og de fagpersoner, der støtter borgeren i hverdagen.

I dag er appen videreudviklet med flere digitale patientuddannelser og livsstilsforløb af mere forebyggende karakter, som gør det muligt for borgere at vælge forløb inden for følgende områder:

- Sunde vaner (livsstilsforløb).
- Rygestop (livsstilsforløb).
- KOL (patientuddannelse).
- Type 2-diabetes (patientuddannelse).
- Hjertesygdom (patientuddannelse).
- Smertehåndtering (patientuddannelse under udarbejdelse).

Brugercentreret udvikling

Brugerinvolvering er grundlaget, når Det Digitale Sundhedscenter udvikler tilbud til borgerne. Patientforeninger og fagpersoner som diætister, sygeplejersker, fysioterapeuter og psykologer har været involveret i at skabe det faglige indhold til alle appens forløb. Der er også lagt vægt på at kombinere viden med, at brugerne arbejder aktivt med refleksionsøvelser, quiz, visuelle virkemidler m.v.
- Vi lægger vægt på, at appens indhold



Tidslinje for Det Digitale Sundhedscenter, 2015-2024.



Appen har en netværksfunktion med aktiviteter og tilbud - og mulighed for at finde støtte og fællesskab i ens nærområde.

Jeg har nået mit mål: at leve godt med min hjertesygdom. Min hjertesygdom fylder fortsat mindre og mindre. Det er nu faktisk blevet nemmere at tage på arbejde.

Borger.

præsenteres visuelt, hvor video, tegninger og billeder erstatter tekst, hvor det er muligt. Appen skal kunne favne både de sårbare, men også de ressourcestærke, via mulighed for en række individuelle tilpasninger, fortæller Carsten Jensen, projektleder i Syddansk Sundhedsinnovation.
Borgerne kan bruge appløsningen alene, i samspil med individuel kontakt med sundhedsfaglige eller som led i holdundervisning. Borgerne tilrettelægger dermed deres forløb ud fra egne specifikke behov, motivation for livsstilsændringer og hverdagsliv.
Appens indhold præsenteres visuelt med udgangspunkt i de individuelle tilpasninger, borgeren foretager på fire grundlæggende områder: Min dag, Min krop, Forløb og Tanker.

Portal for fagpersoner

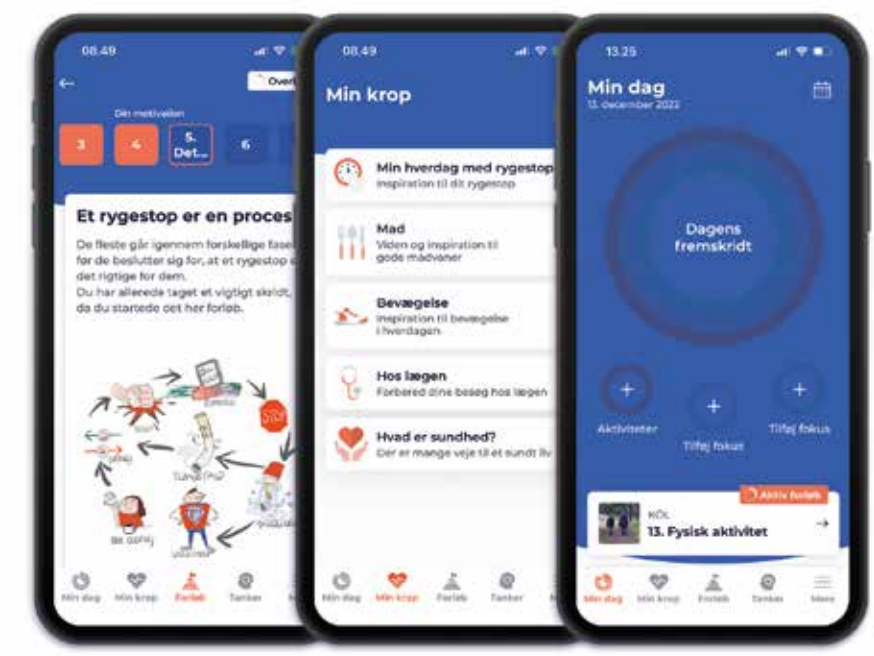
Kommunerne kan via hjemmesiden for Det Digitale Sundhedscenter finde og anvende materiale som vejledninger, guides, dokumenter og videofilm. Og fagpersoner på tværs af partnerskabet kan udveksle erfaringer og sparre på tværs i de nedsatte erfagrupper. Det tætte samarbejde mellem kommuner, patientforeninger og region bidrager således til løbende udvikling og fremdrift i projektet, og understøtter implementering i de involverede kommuner.
- Vi har fået rigtig mange gode inputs, også til hvordan vi sikrer implementering i de involverede kommuner, siger Anna-Britt Krog, som er it-projektleder i Syddansk Sundhedsinnovation.
Både hjemmesidens og appens indhold redigeres i WordPress, som blandt andet anvendes til at føre statistik over forløb, som er startet og afsluttet i appen.
Kombineret med løbende interviews og spørgeskemaundersøgelser med borgere og fagpersoner giver det grundlag for tæt monitorering af udbredelsen af - og tilfredsheden med - de digitale tilbud.

Alle kommuner skal med ombord

Visionen bag Det Digitale Sundhedscenter er løbende at udvikle og udbrede konceptet, så det bliver en integreret del af sundhedstilbuddet i alle landets 98 kommuner. Og ikke mindst: At det bliver borgernes foretrukne portal til at få hjælp til sundhedsudfordringer.
Næste skridt er derfor at udvikle digitale tilbud til flere målgrupper, så endnu flere borgere kan forebygge kronisk sygdom - og leve et liv med høj livskvalitet trods kronisk sygdom.
Mere information:
www.detdigitalesundhedscenter.dk



Overblik over projekter, som er udviklet og er under udvikling, samt tværgående fokusområder og metoder.



Her ses nogle eksempler på appens visuelle præsentation.

Ny model skal give **bedre personlig behandling**

Den nye »PhaseV«-model for kliniske studier bygger på data, der leveres direkte fra borgerne. Modellen skal sikre, at patienterne får den rette personlige behandling - også over tid.



Patienten skriver løbende helbredsoplysninger ind i en app. Hermed samles data over en længere periode, så både behandler og patient kan følge forløbet.



Af Lotte Overbjerg.
Journalist
- Danish Life Science Cluster

Teknologien har nået et niveau, der kan få afgørende betydning for fremtidens udvikling af behandlingsformer. Potentialet for at indsamle data er vokset betragteligt, og det betyder, at behandlinger og medicin i højere grad kan tilpasses den enkelte patient.
Med data leveret direkte fra patienten skal der skabes en helt ny model for kliniske studier af medicin, som vil gavne både borgere, producenter og sundhedsvæsenet. Det er målet for innovationsprojektet PhaseV (Fase 5), der skal udvikle en ny »golden standard« for kliniske studier.
- Med PhaseV skaber vi en tættere forbindelse mellem kliniker og patient. Vi klinikere får en meget bedre indsigt i, hvordan patienterne tager imod den behandling, vi giver dem, og samtidig får patienterne måske værktøjer til at passe bedre på sig selv, siger Klaus Kirketerp-Møller, overlæge ved Bispebjerg Hospital.

Følger over tid

PhaseV er et tværsektorielt projekt, der er støttet af Innovationsfonden. I projektet deltager både virksomheder, klinikere og forskere.
Projektet skal udvikle en række løsninger til, hvordan patienter, borgere og pårørende kan indberette data for, hvordan en patient reagerer på en given behandlingsform. Dataopsamlingen skal forløbe over en længere periode - måske flere år - og patienterne kan indberette data, når de for eksempel oplever en forværring, i stedet for at vente til næste lægebesøg.
PhaseV udvikler tre forskellige apps, der skal opsamle data om patienter med henholdsvis svær overvægt, diabetiske fodsår og kronisk nældefeber.
Her er tale om omkostningstunge kroniske lidelser. For eksempel estimeres de årlige behandlingsomkostninger til svær overvægt alene at overstige 15 milliarder kroner for kommuner og regioner.

Patienten i fokus

Blandt partnerne i projektet er Copenhagen Institute for Futures Studies, som understreger vigtigheden af at fokusere på den enkelte borger.
- Borgeren skal tilbage i centrum, og den menneskelige faktor skal fylde, siger Bogi Eliasen, director of health.
Samme toner lyder fra Novartis, som er en af projektets store private partnere:
- Vi skal gøre kliniske studier hurtigere, mere fleksible og mere præcise til gavn for borgerne. Målet er, at vi i fremtiden kan tilpasse behandlingen til den enkelte borger og sætte ind, inden de bliver alvorligt syge, siger Frederik Nielsen, medicinsk rådgiver i Novartis.
CEO i virksomheden Monsenso, Thomas Lethenborg, som skal udvikle den

digitale platform, hvor brugerne skal indberette data, tilføjer:
- Vi ved, at alle patienter er forskellige, og optimalt bør de tilbydes skræddersyede behandlinger. Med PhaseV's løsning kommer vi helt tæt på de enkelte borgere og deres reaktioner og oplevelser i forbindelse med en behandling. Derfor får vi et vigtigt billede af, hvilke behandlingsformer der passer til hvilke patienter, siger han.

Deler gerne data

Da PhaseV blev præsenteret på WHINN-festivalen hos Danish Life Science Cluster i slutningen af 2022, spurgte flere af tilhørerne i salen til ejerskab og deling af borgernes data. Hvordan får man borgerne til at dele deres data, og hvem vil så eje data, blev der spurgt.
Project director Trine Rolighed Thomsen fra Teknologisk Institut har arbejdet med borgerdata i en årrække, og hendes erfaring viser, at langt de fleste borgere er positive over for at dele deres personlige sundhedsdata med sundhedssektoren:
- Alle de patienter og borgere, vi har været i kontakt med, vil gerne dele deres data, hvis der er en chance for, at de kan være med til at skabe bedre behandling for dem selv eller andre. Vores opgave i projektet bliver så at få patienterne til at holde fast i kontinuerligt at indberette data over en længere periode. Det bliver en udfordring.



Klinikere og behandlere kan løbende monitorere patientens indrapportering og dermed følge udviklingen - også når der er lang tid til næste lægebesøg.



Projektet er bredt funderet med mange vigtige partnere. Her ses fra venstre: Trine Rolighed Thomsen (Teknologisk Institut og Aalborg Universitet), Klaus Kirketerp-Møller (Bispebjerg Hospital), Frederik Knud Nielsen (Novartis) og Bogi Eliasen (Copenhagen Institute for Futures Studies).

»PhaseV«

Projektet løber i tre år og har et samlet budget på 48,2 millioner kroner. Heraf kommer 24 millioner fra Innovationsfonden.
Læs mere på: Phasev.dk.

Partnere i projektet er:

- Monsenso
- Danish Life Science Cluster
- Teknologisk Institut
- Bispebjerg Hospital
- Novartis
- Novo Nordisk
- Copenhagen Institute for Futures Studies
- Steno Diabetes Center Aarhus
- Aarhus kommune
- Aarhus Universitet
- Forskningsenheden for Almen Praksis
- Alexandra Instituttet.



HUSK

Medicoteknik kan også læses online

Få besked hver gang en ny udgave er tilgængelig.

Tilmeld dig på TechMedia.dk

Nyttig viden fra TechMedia

Myter og mysterier om tatoveringer og MR-scannere



Det har længe været kendt, at MR-scanninger kan skabe smerte, ubehag og hudreaktioner hos tatoverede patienter. Ifølge Kasper Alsing og hans vejledere, der forsker i problematikken, kalder en sejlivet myte stadig på forklaring. Det har blandt andet diagnostiske konsekvenser. Derfor har han sat sig for at tage livet af myten og blive klogere på problemet.



Af Camilla Beer Arnsberg.
Kommunikationskonsulent
- Radiograf Rådet

På sit kvistkontor på Bispebjerg Hospital har Kasper Alsing en skotøjsæske med magnetisk tatoveringsblæk. Han er læge ved Tatoveringsklinikken på dermatologisk afdeling på Bispebjerg Hospital, og blækket er omdrejningspunktet i hans ph.d.-projekt. Her forsøger han og resten af forskningsteamet at løse de mysterier, der omgærder MR-scanninger og tatoveringer. Projektet udføres i samarbejde med hans vejledere: overlæge i diagnostisk radiologi Helle Hjorth Johannesen, MR-fysiker Rasmus Hvass Hansen og professor i dermatologi Jørgen Serup.
- Man er ikke rigtig i tvivl, siger Kasper Alsing, mens han fører en magnet ned i skotøjsæsken.
Uden at komme i direkte kontakt med blækflaskerne suger magneten den nærmeste flaske til sig.
- Det svarer stort set til, at der er knuste tavlemagneter i blækket, fortæller han.

Magnetisk blæk

På opslagstavlen over hans skrivebord hænger en illustration fra Tattoo Ole - Danmarks og endda verdens ældste stadig fungerende tattoo-shop, som åbnede i 1884. Ligesom tatoveringskunsten er gammel, er kendskabet til problematikken omkring MR og tatoveringer heller ikke nyt, forklarer Kasper Alsing:
- Det er helt velkendt, at der kan være problemer med ubehag, brændende fornemmelser og smerter i tatoveringer under MR-scanninger. Den første publikation,



Kasper Alsing holder en magnet. Noget tatoveringsblæk er så magnetisk, at flasken hurtigt tiltrækkes. (Foto: Camilla Beer Arnsberg).

der nævner det, stammer fra 1987. På et tidspunkt opstod den opfattelse, at der opstår en termisk forbrænding i tatoveringen, og den er gået fra mund til mund lige siden. Men jeg tror, at det er en myte, siger Kasper Alsing.
Ifølge Kasper Alsing var det meste tatoveringsblæk metalbaseret, når man kigger nogle årtier tilbage i tiden. Derimod er størstedelen af traditionelt tatoveringsblæk i dag syntetisk fremstillet, mens cirka 20 procent af blæktyperne stadig er baseret på såkaldte jernoxider. Og det er netop de blæktyper, der kan skabe problemer under MR-scanninger, forklarer han:
- Man anvender jernoxider, fordi de er både billige og nemme at skaffe. Man kan mere eller mindre grave det op fra undergrunden, knuse det og blande det med vand eller alkohol, så har man en farve. Sådan er nogle af de ældste hulemalerier, såsom dem i Lascaux-hulerne i Frankrig, lavet. Det er især jordmineraler, vi finder i blækket, og det er problematisk, da de kan være stærkt magnetiske, lyder det fra Kasper Alsing.

Permanent makeup

Fordi jernoxidbaseret blæk er velegnet til at fremme naturlige farvenuancer, anvendes disse typisk i permanent makeup tatoveringer såsom øjenbryn og eyeliner. Det er, forklarer Kasper Alsing, et felt, der i disse år oplever eksplosiv vækst, og kvinder med permanent makeup er også overrepræsenteret i de tilfælde, hvor der indrapporteres ubehag i tatoveringer under MR-scanninger, fortæller han.
- Det er ret nemt at finde ud af, om det her er i blækket, siger Kasper Alsing og kigger på de små stykker af mineralet, magnetit, der ligger i hans håndflade. Materialet er så magnetisk, at han har identificeret de problematiske blæktyper ved helt lavpraktisk at sætte en magnet til hver flaske, han har fået fingrene i. Dem, der har vist sig at være magnetiske, er efterfølgende blevet sendt til kemisk analyse. Og det magnetiske blæk har også været en tur i MR-scanneren, fortæller han:
- Når vi tager magnetisk blæk ind i MR-scanneren, kan vi simpelthen se, hvordan blækket rejser sig i en pigget krystalform i petriskålen i retning mod magnetfeltet. Det er ret vildt.

Brændende fornemmelse

Patienter, der føler smerter i deres tatovering under MRI, beskriver, at de oplever en brændende fornemmelse i huden, og i op til 48 timer efter scanningen kan der forekomme hudrødme og hævelse i og omkring tatoveringen.
Følelsen af, at det brænder i tatoveringen, har formentlig, mener Kasper Alsing, ført til fortællingen om, at det skyldes termisk forbrænding, forårsaget af radiofrekvensbølgerne, som skaber en strøm i huden. Men det er misledende, indskyder han, fordi mange andre påvirkninger end varme kan give en brændende fornemmelse. Både kulde, mekanisk træk, nervestimulering og ætsning kan således skabe en følelse af, at det brænder.
- Der er ingen tilfælde, hvor der har været brud på huden, fortæller Kasper Alsing og viser et foto af en tatovering, der er rød og hævet efter en MR-scanning.
- Det tyder også på, at forklaringen ikke er termisk forbrænding. Vi har lavet både et dyrestudie og ex vivo-studie, og vi har ikke kunnet detektere nogen form for temperaturstigning efter MR-scanning. Vi har på alle måder, både scanningsmæssigt og i udvalget af blæk med et højt jernindhold, forsøgt at fremprovokere en temperaturstigning.



Problemet med smerter og ubehag opstår især ved mørke eller sorte tatoveringer.

Magnetfelt eller radiobølger?

Ifølge Kasper Alsing kan det enten være MR-scannerens statiske magnetfelt eller radiofrekvensbølgerne, der forårsager en reaktion hos nogle patienter. Aktuelt arbejder han derfor på forskellige teorier for, hvad der egentligt sker i tatoveringen, når patienten oplever ubehag.
Selv hælder han mest til teorien om, at der er tale om perifer nervestimulering, som skabes mellem de magnetiske partikler og MR-feltet:
- Det statiske magnetfelt kan skabe et ▶



Tatoveringer og MR-scanninger

15-20 procent af alle europæere har en eller flere tatoveringer, og forekomsten er højest i aldersgruppen 18-29 år.
Indtil introduktionen af organiske pigmenter for et par årtier siden var jernoxider dominerende i tatovørblæk. Jernoxider er magnetiske og mistænkes derfor for at være årsagen til ubehag under MR-scanning.
Forekomsten af ubehag er dog sjælden såvel som underrapporteret, og en tidligere undersøgelse anslår, at sandsynligheden for den type bivirkning ved MR er 0,17 procent.
Gennemgange af tilfælde med ubehag viser, at det oftest forekommer i mørke eller sorte tatoveringer. De fleste rapporterede tilfælde er foregået i MR-scannere med et 1.5-T magnetfelt, men det er også dokumenteret, at hudreaktioner kan opstå ved så lavt som et 0.5-T magnetfelt.
Kilde: Alsing et al.: »Tattoo complications and magnetic resonance imaging: a comprehensive review of literature«, publiceret i Acta Radiologica, 61. bind, nr. 12 2020.



Ifølge Kasper Alsing er der et stabilt højt antal danskere, der får en eller flere tatoveringer. Særligt permanent makeup er et felt i vækst, forklarer han. (Foto: Camilla Beer Arnsberg).



Kvinder med permanent makeup er overrepræsenteret i de tilfælde, hvor der indrapporteres ubehag i tatoveringer under MR-scanninger.

mekanisk træk, som skaber en vævsirritation, fordi der bliver trukket i alle de magnetiske partikler i huden. En anden forklaring kan være den, jeg kalder »shot gun-effekten«: At det tatoveringsblæk, der ligger indeni en celle, trækkes ud igennem cellevæggen forårsaget af magnetfeltet, og så dør cellen.
Ifølge Kasper Alsing antyder hverken den gældende forklaringsmodel eller hans teorier, at det er farligt at blive MR-scannet, når man er tatoveret. Dertil kommer, at fænomenet er sjældent.
Imidlertid skaber både myter og uvidenhed omkring problemet i sig selv et problem, mener han:
- Jeg ved, at nogle ikke ønsker at lade patienter MR-scanne, fordi de er bange for, at det kan være smertefuldt eller farligt for dem. Det er potentielt set et reelt problem for den enkelte, som derved ikke har adgang til den type billeddiagnostik, der kan være en hjørnesten i deres udredning eller prognose. Derfor er der brug for viden og vejledning.

Nervøse patienter

Anne Dorte Blankholm er radiograf, ph.d. og MR-ekspert og arbejder som klinisk specialist og forsker på Aarhus Universitetshospital. Hun har ikke selv oplevet personale, der har undladt at MR-scanne patienter på grund af tatoveringer, og ifølge hende bør det heller ikke forekomme:
- En tatovering bør aldrig være en kontraindikation for en MR-scanning. Men det er jo patienternes eget valg, om de vil scannes. De kan være nervøse, hvis de før har oplevet ubehag, eller hvis de har googlet problemet og læst alle de ammestuehistorier, der er på internettet. Og det kan være svært at sortere i, hvad der er rigtig og forkert information, fortæller Anne Dorte Blankholm.
Derfor mener hun også, at problematikken stiller krav til, hvad man som radiograf bør vide og informere om:
- Som radiograf i MR bør man være forberedt på situationen, hvor patienten er nervøs eller har spørgsmål til tatoveringer. Det handler om at kommunikere, at det er ekstremt sjældent og ufarligt, og at de kan trykke på alarmknappen, hvis de oplever det mindste ubehag.

Artefakter

På sin computer har Kasper Alsing en mappe med MR-billeder. Tatoveringer med et højt indhold af jernoxid kan forårsage artefakter (forstyrrelser i billedet), forklarer han, mens han åbner et billede af en patient, der har fået tatoveret permanent eyeliner.
- De danner tydeligt artefakter, og at tatoveringer kan gøre det, kan i princippet være et diagnostisk problem, siger Kasper Alsing.
Ifølge Anne Dorte Blankholm er det heldigvis sjældent, at permanent makeup giver artefakter. Hun uddyber dog, at sådanne artefakter potentielt kan være et problem, hvis de er tæt på det område, man undersøger. Som radiograf kan man, siger hun, justere på MR-scanningsparametrene, men det løser sjældent problemet helt.
Spørger man Anne Dorte Blankholm, er der mange andre områder indenfor MR-sikkerhed, der udgør større risici, såsom piercinger, implantater og tøj, der er produceret ved hjælp af nanoteknologi og derfor indeholder metal. Men det betyder ikke, understreger hun, at man kan lukke øjnene for problematikken med tatoveringer:
- Det er også sjældent, at kontraststof forårsager en allergisk reaktion, men det skal vi også vide noget om. Det samme gælder tatoveringer. Lige nu er det et område, der er meget præget af storytelling, så det er kærkomment, hvis vi kan få noget mere evidensbaseret viden. Der er behov for mere forskning på området.

Stort mørketal

Der er imidlertid en varig udfordring i at løse problemerne. Datagrundlaget er



Mineralet magnetit er stærkt magnetisk og findes i nogle typer tatoveringsblæk, fortæller Kasper Alsing. (Foto: Camilla Beer Arnsberg).

med Kasper Alsings ord nemlig sparsomt. Faktisk er der siden 1987 i publicerede artikler kun omtalt 18 tilfælde i tatoveringer under MR på verdensplan. Ifølge Kasper Alsing betyder det, at der eksisterer et stort mørketal, og det gør det sværere at finde frem til den egentlige forklaring og problemets reelle omfang.

Heller ikke Anne Dorte Blankholm har svært ved at forestille sig, at det er et underrapporteret fænomen:

- Utilsigtede hændelser i MR er generelt underrapporterede, og det er et problem på verdensplan. Når det er sagt, så ved vi, at forskellige farver kan indeholde metal, men tilfælde med problemer med tatoveringer i relation til MR forekommer heldigvis sjældent, siger hun.

Kasper Alsing mener, at der generelt har manglet en akademisk interesse i tatoveringer. Tatoveringsklinikken på Bispebjerg var da også den første af sin slags i verden, da den åbnede i 2008. Derfor håber han også på at blive den første, der systematisk får undersøgt problemet. Men til det har han brug for at kende de tilfælde, der opstår på MR-afdelinger:

- Hvis man som radiograf eller læge oplever, at en patient får reaktioner i sin tatovering under MR, vil jeg derfor altid opfordre til, at de kontakter os - så tilfældet kan registreres og omfanget vurderes. Selv den mindste reaktion vil jeg gerne høre om.

Et mysterium

De næste to år er for Kasper Alsing reserveret til at finde ud af, hvilke teorier og mekanismer der forklarer relationen mellem tatoveringer og MR-scanninger. Og der er nok at tage fat på.

Alle rapporterede tilfælde beskriver, at den ubehagelige fornemmelse opstår øjeblikkeligt, når scanningen går i gang. Men nogle patienter oplever ikke ubehag ved første MR-scanning, men først ved tredje eller fjerde scanning. Og dermed har mysteriet en ekstra komponent, forklarer Kasper Alsing:

- Hvorfor det sker, er mig en gåde. Om det magnetiske materiale skal orientere sig på en bestemt måde, før det reagerer, eller hvordan det hænger sammen, der er jeg svar skyldig. Der er ingen af de forklaringsmodeller, der florerer, som kan forklare det. Vi ved heller ikke, hvor meget blæk, der skal til, før det skaber en respons. Der er rigtig meget, der stadig er ubesvaret.



Artiklen er tidligere bragt i fagbladet Radiografen i juni 2022.

Find hele bladet på Radiograf.dk, eller scan QR-koden.

Afsender: TechMedia A/S, Naverland 35, DK-2600 Glostrup

VINGMED









Vi har fået en lille ny...

- Vingmed kan nu også tilbyde et transportabelt varmesvøbetæppe på batteri med indbygget konsol. Desuden er der stor fokus på vores akutbord som bl.a. kan leveres med indbygget monitorering

- **Kuvøser** i støjsvagt nyt design
- **Akutbord** med bl.a. indbygget monitor
- **Vugger** med hæve-/sænke og vippefunktion
- **Varmetæpper** – hurtig opvarmning – ny teknologi
- **Fototerapi/icterus** – kontakt os om mulighederne

Dorte Pilgaard · Peter Thorsen
dp@vingmed.dk · pt@vingmed.dk
40 44 99 08 · 40 44 39 75