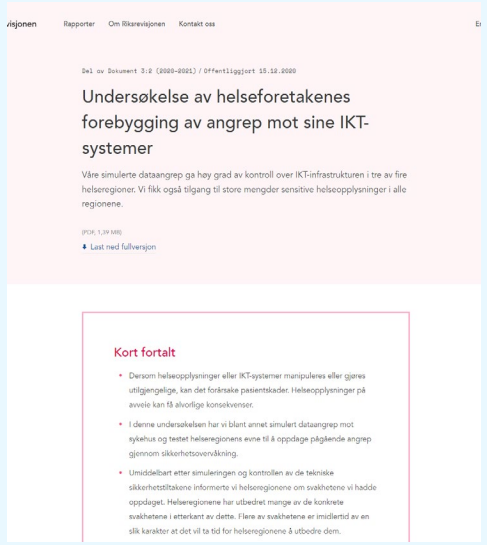
Riksrevisjonen

Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer

Nettverk for informasjonssikkerhet (NIFS)

17. februar 2021



6 Nyheter | Koronaviruset

Helsedata er hackernes nye mål

Koronakrisen har forandret spionenes mål. Hackere fra mange land mistenkes nå for å søke etter sensitive helseopplysninger.

Organiserte kriminelle ser ut til å lete etter alt som kan gi kjapp fortjeneste

Tapon Johansen, sikkerhetssjef i Norse

FAKTA

Ulike typer dataangrep

Koronaviruset | Nyheter 7

BBC | Sign in | Home | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | US Election | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment

Tech

Computer virus alters cancer scan images

4 April 2019

SCIENCE PHOTO LIBRARY

The experimental malware could add fake tumours and other signs of disease to scans

A computer virus that can add fake tumours to medical scan images has been created by cyber-security researchers.

Kartlegging ved fem virksomheter

Hvordan er sykehusene forberedt på IKT-bortfall?

Helsetilsynet TILSYN MED BARNEVERN, SOSIAL- OG HELSETJENESTEN

Information Security Report

Confidential patient data freely accessible on the internet

NEWS WEBSITE OF THE YEAR

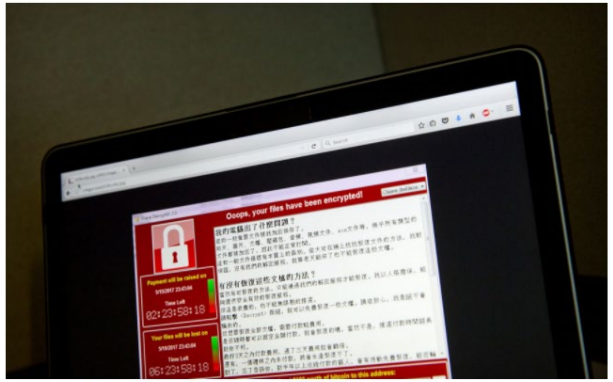
The Telegraph | Coronavirus | News | Politics | Sport | Business | Money | Opinion | Tech | Life | Style | Trav

Gadgets | Innovation | Big tech | Start-ups | Politics of tech | Gaming

Technology Intelligence

WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled

share | Save



A computer hit by the WannaCry attack CREDIT: AP

Mål og problemstillinger

Målet med undersøkelsen har vært å vurdere hvordan helseforetakenes IKT-systemer sikres mot dataangrep, hvordan de regionale helseforetakene understøtter dette arbeidet, og hvordan Helse- og omsorgsdepartementet følger opp.

Problemstillinger:

1. I hvilken grad er helseforetakenes IKT-systemer sikret mot dataangrep?
2. Bidrar de regionale IKT-leverandørene og helseforetakenes sikkerhetsstyring til å opprettholde et forsvarlig sikkerhetsnivå?
3. Hvordan tilrettelegger og følger de regionale helseforetakene opp at helseforetakene kan beskytte seg mot dataangrep?
4. Hvordan er Helse- og omsorgsdepartementets oppfølging og virkemiddelbruk på IKT-sikkerhetsområdet i spesialisthelsetjenesten?

Metoder

- Tekniske kontroller
  - Uttrekk og analyse av data fra IKT-systemer
  - Angrepssimulering
  - Dokumentanalyse
  - Møter
- Styring
  - Dokumentanalyse, spørrebrev og intervju
- Sikkerhetsatferd
  - Dokumentanalyse
  - Dybdeintervju med ledere og ansatte
  - Phishingtest
  - Analyse av statistikk og konkrete avviksmeldinger

Simulerte dataangrep

- En metodisk utvikling over tid – gir dybde i revisjonen.
- Samarbeid med helseregionene har vært godt, men ikke nødvendig for å lykkes med de simulerte angrepene.
- Revisjonen har ikke forsøkt å fullbyrde angrepene og har dermed ikke testet regionenes fulle beredskap.

Simulerte dataangrep

Tilgang til informasjon?

Tilgang til mer informasjon?

Manipulere informasjon?

Slette informasjon?

Slå ut systemer?

Simulerte dataangrep – resultater

I tre av fire regioner fikk vi **høy grad av kontroll** over viktige IKT-systemer, og dermed tilganger som kunne utnyttes til å:

- stjele store mengder sensitive helse- og personopplysninger
- slette opplysninger som er nødvendige for pasientbehandlingen
- manipulere opplysninger om pasientene
- stoppe systemer og utstyr som er kritiske for driften av sykehusene

Høy grad av kontroll – nødvendig?

- De simulerte angrepene viser også at en angriper kan gjøre betydelig skade selv uten kontroll over IKT-systemene.
- *For eksempel:* I alle helseregioner fant vi store mengder sensitive opplysninger som var tilgjengelige for alle (inkludert alle ansatte).

Svak evne til å oppdage angrep

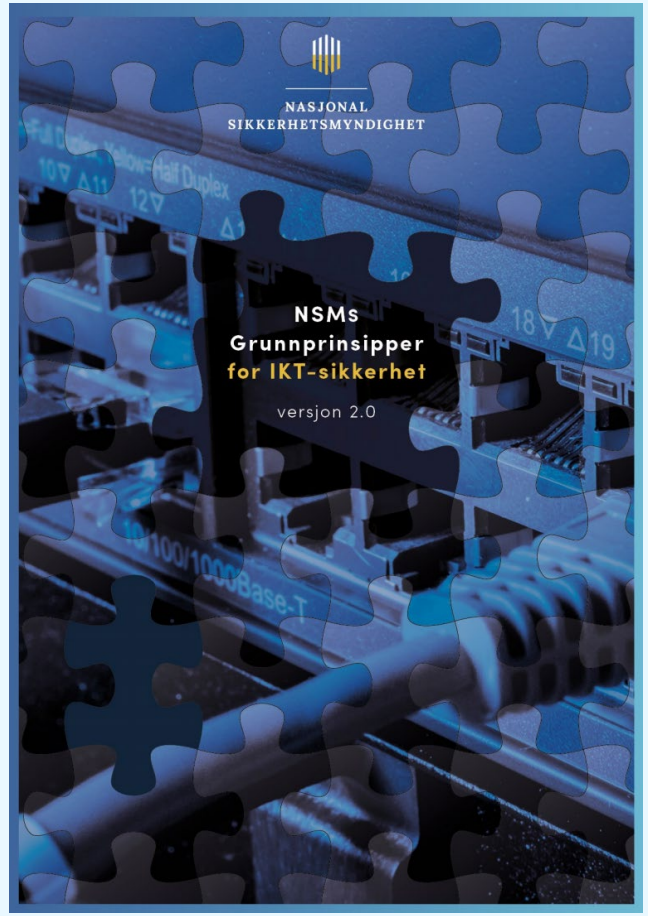
- En region oppdaget flere av våre aktiviteter, mens de andre tre oppdaget lite eller ingenting.
  - Dette til tross for at vi benyttet støyende metoder og verktøy.
- Flere av regionene samler inn loggdata, men har ikke system for å sortere og tolke dataene slik at sikkerhetsbrudd kan oppdages fortløpende.

Kilde: Pixabay

Tekniske kontroller

Utvalgte områder, bl.a. basert på NSM Grunnprinsipper for IKT-sikkerhet:

1. Oversikt over utstyr og programvare
2. Kontroll med kontoer og tilgangsrettigheter
3. Sikker konfigurasjon av utstyr og programvare
4. Sikkerhetsoppdateringer og sårbarhetsskanning
5. Kontroll med kommunikasjon i nettverket
6. Logging og overvåking for å oppdage angrep



Kilde: NSM

Tekniske kontroller – resultater

- Vesentlige svakheter i alle de utvalgte tiltakene i alle regioner.
- De vil ta tid å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.
- Alle regionene har utfordringer med å etterleve sentrale krav til informasjonssikkerhet i lov og forskrift.

Kjente svakheter

- Viktig å jobbe jevnt og systematisk med sikkerhet.
- Helseregionene prioriterer ikke opprydding, f. eks i gamle kontoer, tilganger og personopplysninger.
- Kompleksiteten vanskeliggjør opprydding – det utfordrende å ha oversikt over verdier, avhengigheter og sårbarheter.
    - Kun et av tre helseforetak mener de har oversikt over sine personopplysninger.

Uklar ansvars- og rollefordeling

- Uklarheter i fordeling av ansvar og oppgaver vanskeliggjør forbedring.
- Det er uklarheter mellom IKT-leverandørene og helseforetakene om:
  - hvem som skal gjøre nødvendig opprydding og forbedringstiltak
  - hvordan ansvaret for sikkerheten i medisinsk-teknisk utstyr skal fordeles

Sikkerhetsatferd

- Svak sikkerhetsatferden blant helse- og IKT-personell.
  - Kontrollene avdekket uheldig praksis blant annet knyttet til:
    - Valg av enkle passord
    - Praksis med unntak fra krav i styringssystemet
    - Deling av tilganger
    - Svak tilgangsstyring
    - Ulik håndtering av sensitive opplysninger
    - Uautorisert fysisk tilgang
    - Slurv og bruk av snarveier
  - Phishingtesten og dybdeintervjuene indikerte også varierende grad av bevissthet blant de ansatte

Mulige årsaker til uheldig sikkerhetsatferd

- Mangelfull kunnskap om sikker atferd
  - Hva er et godt passord?
  - Hvor skal opplysninger lagres?
  - Hvem har tilgang til området jeg lagrer på?
- Tungvinte systemer og andre hindringer
- Ansatte savner tilpasset opplæring - hovedsakelig nettkurs
- Konflikt med andre hensyn

Styring på regionalt nivå

- Økt ledelsesoppmerksomhet, men mangelfull informasjon
  - Få interne kontroller (revisjoner og sikkerhetsøvelser)
  - Manglende sammenstilling av risiko på virksomhetsnivå
  - Lite informasjon om informasjonssikkerhetsavvik
    - Tilbøyelighet til å melde informasjonssikkerhetsavvik
    - Manglende analyser
- RHF-ene benytter ikke virkemiddelapparatet godt nok
  - Stilt få egne krav til HF og regionale IKT-leverandører
  - Få formelle samarbeidsarenaer
  - Felleseide Sykehusinnkjøp HFs ansvar

Positiv utvikling på enkeltområder

- Helseregionene har arbeidet med sikkerhetsorganisering og -styring.
- Informasjonssikkerhet prioriteres i økende grad i HF-ene.
- De regionale IKT-leverandørene har bygget opp egne fagmiljø.
- Iverksatt større forbedringsprosjekter.
- Opprettet regionale samarbeidsforum for informasjonssikkerhet.

Spørsmål?
Kommentarer?