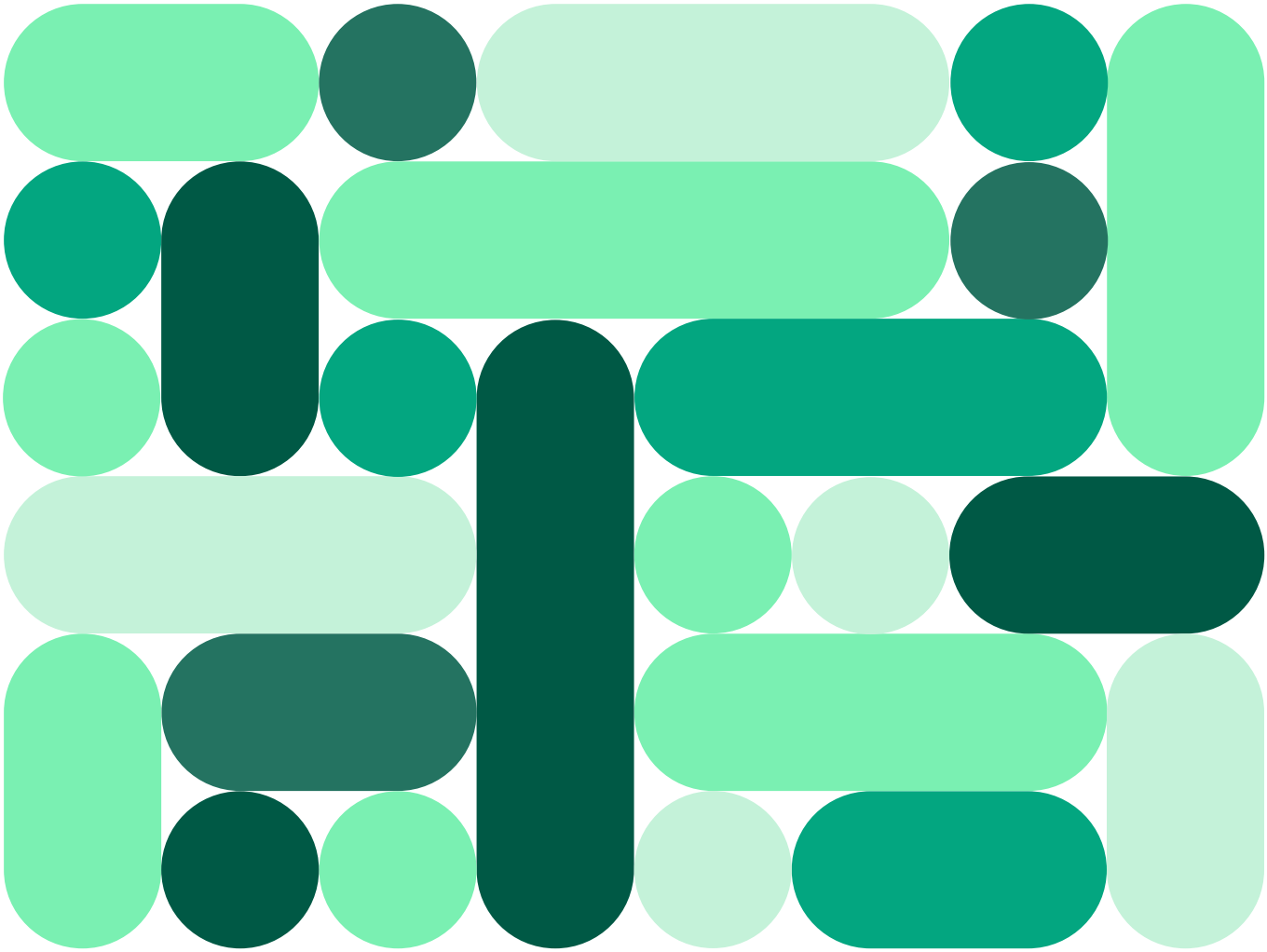
Norsk helsenett
HelseCERT



HelseCERTs situasjonsbilde

August 2022 *post@helsecert.no*

1. HelseCERTs situasjonsvurdering

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Det er meget sannsynlig at virksomheter i helsesektoren blir utsatt for økonomisk motiverte angrep.
- Det er sannsynlig at virksomheter i norsk helsesektor blir truffet av angrep gjennom en verdikjede.
- Det er mulig at skadevarekampanjer påvirker pasientbehandling.
- Det er mulig angrep fra hacktivister vil ramme nettsider og tjenester i sektoren.

2. Bakgrunn

Formålet med denne rapporten er å gi et kortfattet situasjonsbilde for helsesektoren i Norge. Rapporten kan brukes til å styre arbeidet med informasjonssikkerhet.

Helsetjenesten må sørge for å ivareta sikkerhet og personvern i forvaltningen av helsedata, og sørge for at de tjenestene som inngår i de digitale verdikjedene er tilgjengelige og operative til enhver tid.

I denne rapporten trekker vi fram:

1. Aktuelle trusler og aktuelle anbefalinger
2. Trender (krigen i Ukraina)
3. Sårbarheter for helsesektoren

Rapporten er avgrenset til å beskrive tilsiktede handlinger.

3. Trusler/trusselaktører

3.1. Verdikjedeangrep

Verdikjedeangrep har vokst til å være en av truslene som krever fokus i tiden fremover. En bedrifts verdikjede er ofte uoversiktlig, komplisert og flytende. Et verdikjedeangrep utnytter den økte angrepsflaten bruken av programvare, kode og tilganger fra eksterne medfører.

Det siste året har vi sett eksempler på verdikjedeangrep gjennom alt fra utnyttelse av sårbarheter hos store veletablerte leverandører til sårbarheter i små kodebibliotek. Flere bedrifter i Norden ble rammet av kompromitteringen gjennom Kaseya VSA, og ved ett tilfelle valgte en utvikler bak et programvarebibliotek å selv legge inn destruktiv kode i sitt eget bibliotek for å markere støtte til Ukraina.

Det er ikke snakk om hvis man blir angrepet gjennom en verdikjede, men når. En forsvarbar infrastruktur (se faktaboks på side 6) er en forutsetning for å kunne oppdage, redusere omfanget og håndtere verdikjedeangrep.

3.2. Utpressingsaktører

Det siste året har vi sett mange – og store – destruktive angrep fra utpressingsgrupper. En økning i profesjonalisering og spesialisering gjør at flere aktører spesialiserer seg i enkelte deler av et angrep, og man har fått en oppblomstring av såkalte "Initial Access Brokers"[1].

Den generelle fremgangsmåten er lik som i de siste årene - etter kompromittering jobber trusselaktøren for å få kontroll over så mange av bedriftens systemer som mulig, før sensitive data eksfiltreres og systemene krypteres.

Etter kryptering er det gjerne tre forskjellige metoder som brukes for å tjene penger på angrepet:

- Kreve betalt for dekryptering
- Kreve betalt for at data ikke publiseres
- Presse penger fra personer rammet av datalekkasjen

Irlands helsevesen lamslått

14. mai 2021, nesten på dagen fire år etter Wannacry tok ned datasystemene til det britiske helsevesenet, ble Health Service Executive (HSE) i Irland rammet av en annen type utpressingsskadevare – Conti. Hendelsen forårsaket forsinket behandling av pasienter, estimerte kostnader på flere milliarder norske kroner og publisering av pasientinformasjon

Utpressingsaktører angriper ukritisk alle bedrifter. De fleste regner helsesektoren som et legitimt mål og en sektor der man ofte vil betale siden det står om liv. Det siste året har man sett flere vellykkede angrep fra utpressingsaktører mot helsesektoren i andre land, deriblant Health Service Executive (HSE), helsetjenesten i Irland.

Denne typen angriper er tilpasningsdyktig og er ikke låst til en enkelt måte å skaffe seg tilgang på. De kan være både målrettede og tålmodige. En forsvarbar infrastruktur (se faktaboks på side 6) er, i likhet med for verdikjedeangrep, viktig for å sikre egen virksomhet.

[1] **Initial Access Brokers**: Cyberkriminelle som spesialiserer seg på å skaffe tilgang til virksomheter, og deretter selger tilgangen videre til andre aktører.

3.3. Svindlere

Tall fra internasjonale organisasjoner viser at svindel medfører store økonomiske tap for bedrifter. Profesjonelle svindelgrupper kjører operasjoner der de gjør grundig forarbeid og lærer seg å kjenne offeret sitt. I likhet med utpressingsgruppene varierer metodene og målene.

Svindlene vi ser kan grovt grupperes slik:

Fakturasvindel - hvor svindlerne forsøker å skaffe legitime fakturaer og endrer kontonummer på disse.

Direktørsvindel - hvor de forfalsker kommunikasjon så den ser ut til å komme fra en direktør som trenger en "konfidensiell hastebetaling".

Leverandør hacket

En leverandør i sektoren fikk i løpet av det siste året e-postserveren sin hacket. Angriper brukte serveren til å sende ut e-poster med skadevare til drøyt 600 mottakere. Sannsynlig årsak til kompromitteringen var en godt kjent, og varslet, sårbarhet på serveren.

Skadevare i ambulanser

Rett før påsken 2022 ble det oppdaget skadevare på utstyr brukt til flåtestyring av ambulanser i Helse Nord. Saken ble oppdaget da man mottok høyere mobilregninger enn forventet og begynte å undersøke årsaken. Det er flere grunner til at hendelsen kunne oppstå, men det har vært svikt i flere ledd, herunder at det var mangelfull forvaltning og drift, samt sårbar konfigurasjon av enhetene.

Business Email Compromise - hvor svindler skaffer tilgang til e-postkommunikasjon for å skreddersy svindler basert på innsideinformasjon.

Her er det viktig at virksomheter har sikkerhetstiltak og gode rutiner på plass for å sikre hvor de overfører penger. Vi har publisert et sett med tiltak[1] for å sikre at alle betalinger er legitime og går til korrekt mottaker.

3.4. Spionasje

Forskningsdata er et verdifullt mål for trusselaktører. Sykehus og andre helseinstitusjoner som bidrar til, og har tilgang til forskningsdata, må være forberedt på at trusselaktører aktivt forsøker å skaffe tilgang til disse. Dette har spesielt vært dagsaktuelt under COVID-19-pandemien og vil fortsette å være aktuelt framover.

Britiske NCSC, kanadiske CCC og amerikanske NSA og CISA ga sommeren 2020 ut en rapport[2] som beskrev hvordan APT29, en statlig russisk gruppe,

[1] Helsecert.no -> anbefalte tiltak -> svindelbekjempelse https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/anbefalte-sikkerhetstiltak/svindelbekjempelse
[2] Advisory: APT29 targets COVID-19 vaccine development, https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

aktivt jobbet for å skaffe tilveie forskningsdata om COVID-19. Nord-koreanske hackere har også rettet seg mot vaksineforskning.

De siste årene har vi også i Norge sett flere eksempler av målrettede phishingforsøk mot helsesektoren av ulike APT-grupper. Etter utbruddet av krigen i Ukraina har vi sett målrettet phishingkampanjer fra gruppen SEABORGIUM mot en virksomhet i helsesektoren. SEABORGIUM knyttes til russiske statlige interesser. Forsøkene vi er kjent med har ikke vært vellykkede, men aktøren er kjent for å være utholdende og kan fortsette angrepsforsøkene mot samme virksomhet over tid. Ved vellykkede angrep tilegner trusselaktøren seg innloggingsdetaljer eller annen informasjon som kan utnyttes til å få tilgang til sensitiv informasjon og systemer.

Også med denne typen angriper er en forsvarbar infrastruktur (se faktaboks på side 6) nøkkelen for å forebygge, oppdage og håndtere angrep.

3.5. Sabotasje

Ukrainas strømforsyning ble i 2015 utsatt for en serie destruktive angrep som resulterte i blackout over store deler av landet. Angrepene er blitt attribuert til russiske statlige grupper. Angrepene var satt opp til å ramme størst mulig del av landet samtidig.

Russland forsøkte å gjenta samme typen angrep i april 2022, men denne gangen ble angrepet avverget.

Vi registrerer at cyber er brukt til sabotasje av kritisk infrastruktur. Dette er så langt ikke observert innen helse, men må vurderes som et mulig mål.

Forsvarbar infrastruktur

I forsvarbar infrastruktur[1] kontrollerer man hva som kan snakke hvor, logger hva som skjer, har oversikt over hva som er på nettverket og hvem som er ansvarlig for det og man har avinstallert systemer og tjenester som ikke er i bruk. Målet er et oppdatert nettverk hvor inntrenginger kan oppdages, ettergåes og fjernes.

En forsvarbar infrastruktur er summen av mange sikringsmekanismer som til sammen gjør det mulig å forebygge, oppdage og håndtere cyberangrep på en profesjonell måte. Vi anbefaler et sett med tiltak for å oppnå en forsvarbar infrastruktur på helsecert.no[2].

4. Krigen i Ukraina

4.1. Bakgrunn

Russland har invadert Ukraina med militær makt. I innledende faser gjennomførte Russland strategisk utplassering av militære styrker langs den Ukrainske grensen. Samtidig så man eksempler på cyberangrep mot digitale tjenester i Ukraina. Cyberangrepene dreide seg i hovedsak om tjenestenektangrep mot offentlige nettsider. I tillegg har man sett bruk av destruktiv skadevare som er ment for ødeleggelse av IT-systemer. Russland har det siste tiåret bygd opp betydelige kapabiliteter til å gjennomføre cyberoperasjoner, noe de nasjonale sikkerhetsmyndighetene har beskrevet i sine årlige rapporter.

Russland underlegges nå en rekke sanksjoner fra verdenssamfunnet. Et utfall av dette kan være bruk av cyberoperasjoner som gjengjeldelse.

4.2. Situasjonsbilde – Ukraina

Situasjonen 24. februar var kaotisk og uoversiktlig og har siden stabilisert seg noe. Situasjonsbildet kan imidlertid endre seg raskt.

Det har flere ganger under konflikten vært brukt destruktiv skadevare.

PST varslet i mars om en økt etterretningstrussel mot Norge.

Gitt situasjonen vi står i med mye usikkerhet, og mulighet for at cyberangrep mot ukrainske mål direkte eller indirekte kan ramme tredjeparter vurderer vi at risikoen mot virksomheter i helsesektoren er forhøyet.

---

[1] Richard Bejtlich, Defensible Network Architecture
https://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html
[2] Helsecert.no → anbefalte sikkerhetstiltak
https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/anbefalte-sikkerhetstiltak

4.2.1. Tjenestenektangrep mot norske virksomheter

I sommer ble en rekke norske virksomheter utsatt for tjenestenektangrep fra ulike pro-russiske grupper. Lister over nettsider som skulle bli angrepet ble som regel publisert på ulike nettsider/sosiale medier i forkant av angrepene. Motivasjonen bak angrepene har vært variasjoner av støtte til Russland mot NATO.

Angrepene har vært kortvarige og primært rettet mot nettsteder. Disse ble bredt omtalt i media. Vi er ikke kjent med virksomheter som har rapportert om alvorlige konsekvenser.

Vi forventer at slike angrep vil kunne skje igjen.

Tjenestenektangrep

Sommeren 2022 ble Norge truffet av en stor runde tjenestenektangrep. Motivet for angrepene var en misforståelse rundt leveranse av varer til Svalbard som følge av sanksjoner mot Russland. Flere nettsteder ble rammet og opplevde kortere nedetid, men angrepene var ellers uten nevneverdige samfunnsmessige konsekvenser.

5. Sårbarheter

NSM peker i sine rapporter på at det generelle sikkerhetsnivået i IKT-systemer hos norske virksomheter er for lavt, og at det i de fleste tilfeller er tekniske sårbarheter som utnyttes for å kompromittere systemer. Lukking av kjente sårbarheter er derfor et viktig bidrag til å redusere risiko for å bli kompromittert. Rapporten "HelseCERT tilbakeblikk" inneholder statistikken med oversikt over sårbarheter. Den sendes ut i begynnelsen av hvert tertial til alle medlemmer i Nasjonalt beskyttelsesprogram (NBP). Vi henviser til den om man ønsker tallgrunnlag.

Gjennom vår sårbarhetskanning ser vi en nedadgående trend når det gjelder mengden sårbarheter i norsk helsesektor. Dette gjelder for sårbarheter i kategoriene kritisk, høy og medium, og er en utvikling i riktig retning. Imidlertid oppdager vi fortsatt sårbarheter med alvorlig kritikalitet som står åpne, og har gjort dette over tid. Aktiv oppfølging av slike sårbarheter vil også framover være et fokusområde i HelseCERT.

6. Bilag

6.1. Ord og uttrykk

- **APT:** Advanced persistent threat. Primært brukt om statsstøttede grupper som driver med offensive, digitale operasjoner.
- **BEC:** Business Email Compromise er et angrep hvor en angriper får tilgang til en e-postkonto i en virksomhet, og bruker denne for å lure ansatte i bedriften til å gjennomføre feilaktige utbetalinger.
- **Initial Access Brokers**: Cyberkriminelle som spesialiserer seg på å skaffe tilgang til virksomheter, og deretter selger tilgangen videre til andre aktører.
- **Nasjonalt beskyttelsesprogram (NBP)** – HelseCERTs program for å bidra til å forebygge, oppdage og håndtere cyberangrep i helsesektoren. NBP er en gratis tjeneste for virksomheter i sektoren hvor man får tilgang til en rekke tjenester fra HelseCERT ved å delta. For mer informasjon se våre nettsider[1].
- **Passordspraying:** Med passordspraying angriper man mange brukere med noen få utvalgte passord. Det viser seg at hvis en virksomhet har mange nok ansatte vil noen med stor sannsynlighet bruke noen gjentagende passord som kan gjettes. Eksempel på dette er passord som bruker en kombinasjon av årstid og årstall, for eksempel; "Vinter2021".
- **Utpressingsaktører /-grupper**: Grupper som stjeler informasjon og/eller bruker utpressingsskadevare for deretter å kreve betalt for å låse opp informasjon og/eller for å ikke offentliggjøre informasjonen.
- **Utpressingsskadevare:** Ondsinnet kode som krypterer informasjon, og deretter krever penger for at informasjonen skal bli dekryptert. Man betaler i den forventningen om at man får nøkkelen for å låse opp sin eiendel (informasjonen)
- **Verdikjede:** Verdikjeder brukes til å definere kjeden som er med på å skape varer/tjenester (verdier) i en virksomhet og inkluderer underleverandører. Lange verdikjeder oppstår når en underleverandør bruker en annen underleverandør, som igjen bruker en annen underleverandør. En lang verdikjede bidrar til en større angrepsflate som trusselaktører kan utnytte til å angripe en virksomhet, og det kan være vanskelig å danne seg et totalt risikobilde for virksomheten som er på toppen.

[1] Helsecert.no -> Nasjonalt beskyttelsesprogram
https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/nasjonalt-beskyttelsesprogram-nbp

6.2. Sannsynlighetsord

Vurderinger vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte, er det benyttet sannsynlighetsord (se tabell)

Meget sannsynlig	*Det er meget god grunn til å forvente…*	*(>90%)*
Sannsynlig	*Det er grunn til å forvente…*	*(60-90%)*
Mulig	*Det er like sannsynlig som usannsynlig…*	*(40-60%)*
Lite sannsynlig	*Det er liten grunn til å forvente…*	*(10-40%)*
Svært lite sannsynlig	*Det er svært liten grunn til å forvente…*	*(<10%)*