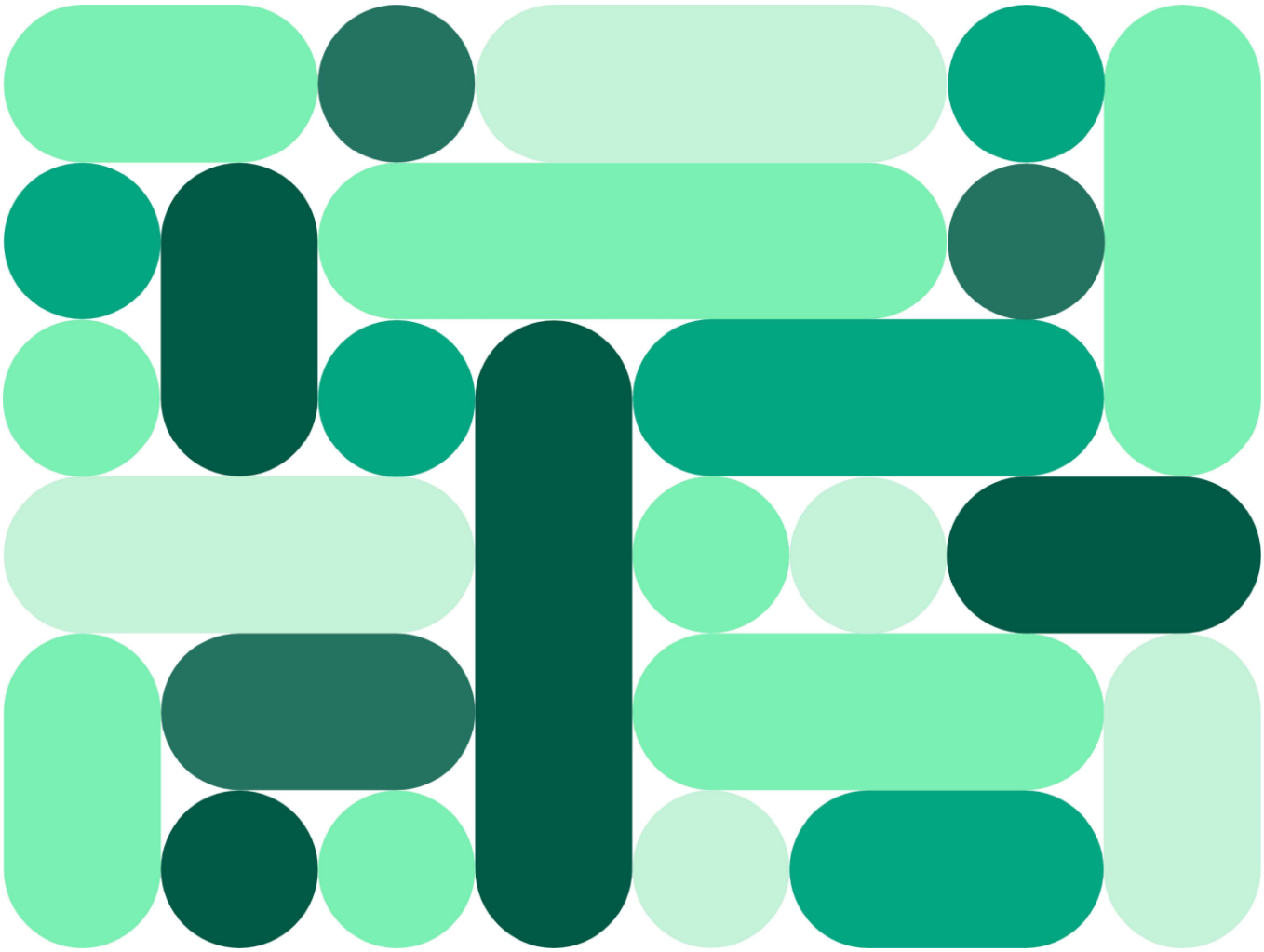
Norsk helsenett
HelseCERT



HelseCERTs situasjonsbilde

Januar 2024

post@helsecert.no

Trusselvurdering 1. tertial 2024

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Vi mener det er sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra aktører som et ledd i det generelle arbeidet til statlige eller stats-sponsede etterretningstjenester.
- Vi mener det er meget sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra organiserte kriminelle grupper.
- Vi mener det er meget sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra hacktivister. Typisk tjenestenektangrep.

Bakgrunn

Formålet med denne rapporten er å gi et kortfattet situasjonsbilde for helse- og kommunesektoren 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. Kommunesektoren må sørge for at innbyggertjenester er tilgjengelige og har redundans etter kritikalitet.

I denne rapporten trekker vi fram:

- Masseutnyttelse av sårbarheter
- Ransomware
- Spionasje
- Politisk motivert hacktivisme
- Svindel
- Angrepsmetoder

Rapporten er avgrenset til å beskrive tilsiktede handlinger.

Situasjonsrapport

Masseutnyttelse av sårbarheter

Vi ser at tiden fra en sårbarhet blir kjent, til den utnyttes i store angrepsbølger ofte er svært kort. Et eksempel på dette er ransomwaregruppen Clop som utnyttet en sårbarhet i filoverføringsløsningen MOVEit i juni i 2023 til å angripe mange hundre virksomheter med ransomware[1]. I dette tilfellet ble sårbarheten utnyttet allerede før en oppdatering var tilgjengelig.

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

Et annet eksempel, som i stor grad traff helse- og kommunesektor, er utnyttelsen av en sårbarhet i Netscaler ADC (CVE-2023-3519)[1] som ble brukt til å plante webshell. Aktiv oppfølging førte i det tilfellet til at mange webshell ble stengt før angriperne rakk å bruke de til videre angrep. Også i dette tilfellet ble sårbarheten raskt utnyttet i omfattende automatiserte angrep.

Denne trenden med kort tid fra sårbarheter blir kjent, til de utnyttes i store automatiserte angrep betyr at man må ha gode rutiner for å fikse sårbarheter, og ha et godt dybdeforsvar så fotfeste for angriper ikke betyr at alt er tapt.

Ransomware

Ransomware, ofte kombinert med eksfiltrasjon av data for å true med offentliggjøring er fortsatt den vanligste, og mest alvorlige sluttformen vi ser for økonomisk motivert kriminalitet. Dette er en dimensjonerende trussel man må ta høyde for, både i sikring og planverk.

Spionasje

De hemmelige tjenestene trekker i sine rapporter fram spionasje som en stor trussel mot Norge. Vi vurderer forskning, helse- og personopplysninger, informasjon om politiske beslutninger og beredskaps- og krisehåndteringsevne som de mest sannsynlige spionasjemålene i sektoren. Statlige aktører har store ressurser til sin rådighet og vi forventer å se spionasjeforsøk framover.

Politisk motivert hacktivisme

Russlands invasjon av Ukraina har ført til store endringer i det politiske landskapet. Mens Russlands statlige offensive cyberoperasjoner primært har vært rettet mot Ukraina har vi sett en ny trend med hacktivistgrupper på begge sider i konflikten.

Flere grupper som støtter Russland har gjennomført en rekke DDoS-angrep mot land de anser som fiendtlige. DDoS-angrepene har i liten grad vært vedvarende over lang tid, og vi vurderer at deres primærmotivasjon til nå har vært oppmerksomhet. Denne trenden ble på ny aktualisert med oppblussing av konflikten i Gaza.

Svindel

Svindel er fortsatt en stor del av bildet innen cyberkriminalitet. Det er få nye trender her. Vi henviser til vårt webinar[2] om temaet for de som ønsker en repetisjon av hvilke typer svindler

[1] https://www.shadowserver.org/news/technical-summary-of-observed-citrix-cve-2023-3519-incidents/
[2] https://www.nhn.no/tjenester/helsecert/webinarer

man typisk kan bli utsatt for. Slike svindler er enormt lukrative og representerer samlet, mye større verdier enn ransomwaregruppers antatte inntjening.

Svindel representerer likevel en mindre trussel enn ransomwaregrupper siden de sjelden påvirker oppetiden til systemer og tjenester.

Angrepsmetoder

Enten man utsettes for ransomware, spionasje eller et annet type angrep er angriper avhengig av et fotfeste i virksomheten som angripes. Denne listen viser hvilke angrepsformer vi mener det er viktigst å sørge for at man har sikringer på plass mot. At man har dybdeforsvar på plass, er helt avgjørende. Her fokuserer vi likevel på inngangsvektoren da god sikring her vil kunne stoppe angrepene i en tidlig fase.

Fjernpålogging
Fjernpålogging er alle virksomhetssystemer som gir tilgang videre inn, eller informasjonssystemer som gir tilgang til sensitiv informasjon. Her ser vi at trusselaktører rutinemessig skanner etter eksponerte systemer, f.eks. RDP, og over tid forsøker å logge inn med potensielle brukernavn og passord-kombinasjoner. Forsøkene kan gå over uker og måneder og vellykkede innlogginger fører til videre angrep. Slike eksponerte systemer må sikres, for eksempel med flerfaktor. Her ser vi også en ny trend hvor phishingangrep nå inneholder funksjonalitet for å omgå flerfaktor. Innlogginger må sikres med phishingresistent autentisering[1] (se eget webinar om dette) for å sikre mot denne trusselen.

Sårbare systemer
Vi har lenge sett at kjente sårbarheter brukes aktivt for å angripe virksomheter som ikke har oppdatert disse. Sårbarhetene kan være gamle, men vi ser også angripere som spesialiserer seg etter nye sårbarheter som slippes, og tiden fra en sårbarhet blir offentlig kjent, til vi ser aktive angrepsforsøk synker. Her er det viktig med gode rutiner for vedlikehold og patching av systemer. Spesielt systemer som er eksponert mot internett. Logging er også viktig for å sikre sporbarhet og for å kunne verifisere om man har blitt angrepet i tiden før man får patchet en sårbarhet.

E-post
E-post har lenge vært en mye brukt angrepsmetode. Både for sosial manipulasjon, phishing og skadevare via linker og vedlegg. Denne trenden forventer vi vil fortsette i overskuelig framtid. Hvordan slike angrep utføres vil utvikle seg over tid, noe vi har sett eksempel på nylig med phishing som omgår MFA. Tilstrekkelig sikring her, er når ansatte kan gjøre feil uten at dette automatisk gir angriper fotfeste. (Slik sikring er et supplement til sikkerhetsopplæring og ikke en erstatning)

[1] https://www.nhn.no/tjenester/helsecert/webinarer (se 08.12.23 Phishingresistent autentisering)

USB-baserte angrep
Vi har også opplevd en økning i USB-baserte angrep. Disse kan grovt deles inn i to grupper:

- Tilfeller hvor USB er blitt infisert med skadevare utenfor virksomheten. Skadevaren kjøres deretter (uforvarende) når ansatte bruker samme minnepenn på virksomhetssystemer.
- Tilfeller hvor angriper fysisk tar med seg skadevare via USB og forsøker å opprette fotfeste i bedrifter.

Av disse anser vi den første som en ny normal, og den andre som mindre vanlig.

Verdikjedeangrep
Vi ser en økende trend hvor angripere går etter selskaper som lager programvare, eller er tjenesteleverandør for å kunne angripe kunder av disse.

Ord og uttrykk

For ukjente ord og uttrykk henviser vi først til vår liste over faguttrykk: https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/publikasjoner/ordliste

Deretter til online-søk.

Er det et uttrykk du savner etter begge disse metodene ta gjerne kontakt med oss på post@helsecert.no!

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%)*