HelseCERT

Situasjonsbilde 2018

HENDELSER

Målrettet angrep mot Helse Sør-Øst.

Mandag 8. januar 2018 avdekket HelseCERT at det pågikk unormal aktivitet mot datasystemer i Helse Sør-Øst. Saken ble politianmeldt og er under etterforskning. Innbruddet ble gjennomført ved å utnytte en sårbar applikasjon i regionen. I forkant av angrepet hadde trusselaktøren foretatt skanning for å avdekke mulige svakheter som kunne utnyttes til å gjennomføre et innbrudd. Det er så langt ikke noe som tyder på at innbruddet har hatt direkte konsekvenser for pasientbehandling, pasientsikkerhet eller at pasientdata har kommet på avveie.

WannaCry

Fredag 12. mai 2017 spredde løsepengeviruset WannaCry seg raskt til et stort antall land. Helsesektoren i England ble hardt rammet. 34 prosent av alle helseforetak i England ble påvirket, enten direkte ved at filer ble kryptert, eller indirekte ved at de stengte ned systemene sine for å forhindre angrep. Det er estimert at mer en 19.000 avtaler og et stort antall operasjoner ble kansellert i England som følge av virusangrepet. WannaCry spredte seg ved å utnytte en kjent sårbarhet. Oppdateringen for å lukke sårbarbarheten hadde vært tilgjengelig i to måneder før utbruddet. WannaCry-hendelsen avdekket manglende sikkerhetsoppdateringer også i norsk helsesektor. Mange virksomheter hadde ikke prioritert å installere oppdateringen. Skadeomfanget av WannaCry kunne altså vært langt mer alvorlig enn det faktisk ble.

Løsepengevirus dukker stadig opp

Flere virksomheter har vært rammet av løsepengevirus og nettbanktrojanere. De fleste slike hendelser starter med at ansatte mottar svindel-e-post. Dette skjer ofte på privat e-post, hvor virksomhetens e-post-filtrering ikke har noen effekt. Antall hendelser går imidlertid ned som følge av gode forebyggende tiltak. HelseCERT kjenner ikke til at noen virksomheter i sektoren har betalt løsepenger i forbindelse med et slikt angrep.

Direktørsvindel

Her går en angriper målrettet til verks mot ansatte som jobber med økonomi i en virksomhet. Angriperen kan kombinere telefon og e-post for å lure den ansatte til å betale en faktura. Svindelmetoden har fått navnet sitt etter metoden, der angriperen normalt vil utgi seg for å være direktør eller en person i ledelsen i virksomheten. HelseCERT er kjent med at minst én virksomhet innenfor vår sektor har blitt rammet av denne type svindel og at penger er gått tapt. Tilfellet HelseCERT kjenner til er også omtalt i media.

NotPetya løsepengeviruset

Løsepengeviruset spredte seg ved å infisere en oppdatering av et regnskapsprogram som ble brukt av enkelte bedrifter, hovedsakelig i Ukraina. Deretter spredte viruset seg i interne nett gjennom å utnytte en kjent sårbarhet samt ved å utnytte manglende segmentering og like lokaladministratorpassord. Dette viser at en trusselaktør kan gå målrettet mot en programvare-oppdatering, og dermed utnytte et svakt ledd i en verdikjede

Tjenestenektangrep

HelseCERT er kjent med flere tjenestenektangrep mot tjenester i helsesektoren som har påvirket tilgjengeligheten til systemene. En tjeneste har vært utsatt for gjentatte tjenestenektangrep i en periode på flere måneder. Erfaringer tilsier at det her er viktig med beskyttelse på flere nivåer.

Phishing

Virksomheter med web-basert e-post opplever stadig kompromitterte kontoer fordi ansatte lures til å oppgi sitt personlige passord til en svindel-side. To-faktor-autentisering er et anbefalt tiltak mot denne typen svindel.

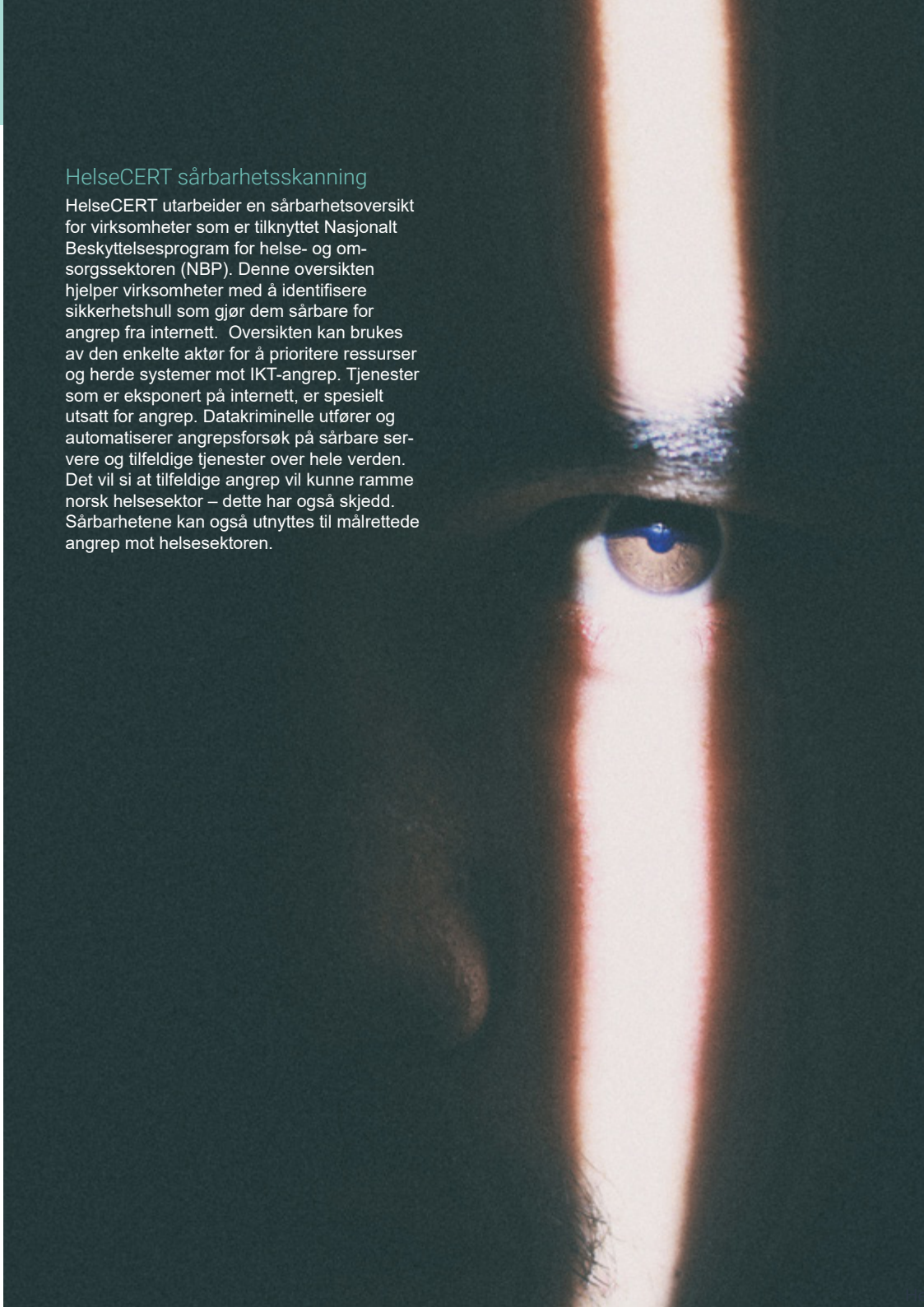
USB-infeksjoner

Flere sykehus har opplevd at maskiner blir infisert med ormen Conficker fra 2008. Dette skyldes både at maskinene kjører utdaterte operativsystem og at minnepinner ikke blir skannet for ondsinnet kode før de blir koblet til utstyret.

Illustrasjonsbilde: Larm Rmah

HelseCERT sårbarhetsskanning

HelseCERT utarbeider en sårbarhetsoversikt for virksomheter som er tilknyttet Nasjonalt Beskyttelsesprogram for helse- og omsorgssektoren (NBP). Denne oversikten hjelper virksomheter med å identifisere sikkerhetshull som gjør dem sårbare for angrep fra internett. Oversikten kan brukes av den enkelte aktør for å prioritere ressurser og herde systemer mot IKT-angrep. Tjenester som er eksponert på internett, er spesielt utsatt for angrep. Datakriminelle utfører og automatiserer angrepsforsøk på sårbare servere og tilfeldige tjenester over hele verden. Det vil si at tilfeldige angrep vil kunne ramme norsk helsesektor – dette har også skjedd. Sårbarhetene kan også utnyttes til målrettede angrep mot helsesektoren.



DETTE MÅ DU GJØRE

Disse tiltakene vil redusere risikoen for at din virksomhet blir rammet av cyberangrep.

Sikkerhetskultur

Jobb med å bygge en god sikkerhetskultur i virksomheten. Gjennomfør opplæring og bevisstgjør ansatte.

Oppdatering

Oppgrader program- og maskinvare for å ta i bruk ny sikkerhetsfunksjonalitet og lukke sikkhetshull.

To-faktor

Innfør to-faktor-autentisering for tjenester tilgjengelig på internett for å hindre misbruk av kompromitterte eller dårlige passord.

DMARC

Beskytt e-post-domener med DMARC, som blokkerer uautorisert e-post og hindrer misbruk av domene.

Sårbarhetsskanning

Gjennomfør sårbarhetsskanning for å oppdage sårbare maskiner i eget nettverk.

Passord

Etabler en god passordpolicy og gi opplæring i hvordan å lage gode passord. Unngå gjenbruk.

Administratorkontoer

Beskytt administratorkontoer. Unngå at brukere har administratorrettigheter. Bruk LAPS for lokal admin.

Applikasjonshvitelisting

Applikasjonshvitelisting vil hindre kjøring av uautorisert programvare.

Segmentering

Benytt klientbrannmur for å unngå intern spredning. Segmenter nettverket ditt, ikke glem servere.

Tormod Ryeng og Andreas Løhre tester medisinskteknisk utstyr under en inntrengingstest.

HelseCERT inntrengingstesting

HelseCERT gjennomfører inntrengingstesting for virksomheter i helse- og omsorgssektoren. Inntrengingstesting er et kontrollert dataangrep som prøver ut motstandskraften i IKT-systemer. Formålet med testen er å identifisere reelle sårbarheter i virksomhetens datasystemer. Resultatet av testen gir virksomheten et godt utgangspunkt for å øke sikkerheten i egne systemer.

SÅRBARHETER

Faren for å bli rammet av ondsinnet kode og digitale angrep øker hvis man lar være å iverksette anbefalte sikringstiltak.

Den økte digitaliseringen av samfunnet introduserer nye sårbarheter. Pasientsikkerheten blir mer og mer avhengig av god informasjonssikkerhet. Vi erfarer at det er krevende for virksomheter å ha en komplett oversikt over egne systemer og mulige sårbarheter. Krav til tilgjengelighet fører til at systemer som sentral driftsovervåkningsanlegg (SD-anlegg), medisinteknisk utstyr og ulike typer velferdsteknologi kobles til internett. Våre erfaringer fra inntrengingstesting i sektoren viser at slike systemer kan utnyttes for å komme seg inn i et ellers godt sikret nett.

HelseCERTs sårbarhetsskanning (se faktaboks) avdekker utstyr i helsesektoren som mangler sikkerhetsoppdateringer, interne systemer som er eksponert på internett og andre sårbarheter som alle utgjør en risiko for virksomheten. Vår erfaring er at virksomheter bruker alt for lang tid på å fjerne sårbarheter etter at de er blitt varslet.

Brukere med utvidede rettigheter i kombinasjon med svake passord utgjør en stor risiko for mange virksomheter. Manglende eller for dårlig implementert nettverkssegmentering bidrar også til at virksomhetene blir sårbare. Dette avdekkes under HelseCERTs inntrengingstesting (se faktaboks) i helse- og omsorgssektoren.

Det publiseres mye informasjon om utfordringene vi står overfor og om hvilke tiltak som reduserer risikoen for å bli utsatt for digital kriminalitet. HelseCERT, NSM NorCERT, NorSIS og flere andre publiserer informasjon om effektive tiltak som reduserer risikoen for å bli påvirket av dataangrep. Vi skulle gjerne sett at arbeidet med å implementere disse tiltakene hadde gått raskere. Det er viktig at virksomheter forstår konsekvensene og risikoen ved å ikke gjennomføre tiltak og lukke sårbarheter.

HelseCERT ser at virksomheter som implementerer anbefalte tiltak, har færre hendelser med f.eks. løsepengevirus

TRUSLER

Nasjonale trusselvurderinger trekker frem digital spionasje som den største risikofaktoren. Norske virksomheter utsettes daglig for fremmed etterretningsvirksomhet og avanserte datanettverksoperasjoner med stort skadepotensial. Dataangrepet mot Helse Sør-Øst i januar 2018 viser at også helsesektoren blir rammet av angrep fra avanserte trusselaktører.

Pasientsikkerheten er avhengig av god IKT-sikkerhet. Digitale angrep kan med letthet forårsake nedetid på kritiske systemer i helsesektoren og påvirker dermed pasientsikkerheten. Denne trenden vil fortsette å øke i takt med digitaliseringen av helsetjenestene. Økt bruk av underleverandører og utsetting av tjenester fører til en økning av lange, uoversiktlige og svake verdikjeder. Disse kan kriminelle utnytte. Det kan for eksempel være sikkerhetshull i programvare eller manglende kunnskap hos underleverandører. På den måten får trusselaktørene tilgang til en større angrepsflate.

Truslene vi ser mest av i helsesektoren nå, er digital kriminalitet som fisking etter sensitiv informasjon, såkalt phishing, direktørsvindel, løsepengevirus og tjenestenektangrep

Målrettede angrep fra avanserte trusselaktører utgjør den største trusselen mot vår sektor. Dette er aktører som har stor kompetanse og kapasitet. De benytter seg oftest av metoder der de utnytter sårbarheter i tjenester som finnes på internett eller gjennom bruk av målrettede e-poster. Dette er kriminalitet som virksomhetene enkelt kan sette inn effektive tiltak mot, slik at det blir vanskeligere for trusselaktørerene å lykkes med angrepene sine. Det er viktig at virksomheter forstår risikoen ved å ikke lukke kjente sikkerhetshull i egen infrastruktur, særlig knyttet til systemer og tjenester som er tilgjengelig fra internett. Det er også viktig at virksomheten prioriterer å bygge opp en god sikkerhetskultur.

DEFINISJONER

Tjenestenektangrep (eng: Distributed Denial of Service attack– DDoS)

Er angrep hvor man hindrer at noen eller noe (f. eks. en person eller et system) får tilgang til informasjon, eller ressurser de skal ha tilgang til, ved at tjenesten "bombarderes" med trafikkmengder langt ut over det den er designet for å takle i en normal belastningssituasjon. Et vellykket tjenestenektangrep vil på den måten føre til brudd på tilgjengeligheten til informasjonen/ressursen.

Direktørsvindel (eng: CEO-fraud)

Direktørsvindel, eller CEO-fraud, er svindel utført ved hjelp av e-post eller telefon/SMS fra personer som utgir seg for å være i ledelsen i virksomheten. Målet med direktørsvindel er å lure en økonomimedarbeider til å betale en faktura eller overføre penger til en konto, vanligvis i utlandet (kilde: nettvett.no). Direktørsvindel omtales noen steder som BEC, altså Business Email Compromise.

Løsepengevirus (eng: ransomware)

Løsepengevirus er ondsinnet kode som krypterer data/informasjon og deretter krever løsepenger for at informasjonen skal bli dekryptert.

Verdikjede

Verdikjeder brukes til å definere kjeden som er med på å skape varer/tjenester (verdier) i en virksomhet og inkluderer underleverandører. En lang verdikjede bidrar til en større angrepsflate som trusselaktører kan utnytte til å angripe en virksomhet.

HelseCERT

HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. HelseCERTs oppgave er å øke sektorens evne til å oppdage, forebygge og håndtere ondsinnede inntrengingsforsøk og andre uønskede IKT-hendelser. HelseCERT skal spre kunnskap om IKT-trusler og beskyttelsesmekanismer. Trafikken i Helsenettet blir kontinuerlig monitorert av HelseCERT.

Spørsmål? Send en e-post til post@helsecert.no

www.nhn.no/helsecert