TILTAKSKORT MOT LØSPENGEVIRUS (RANSOMWARE)

Forutsetninger for å kunne bruke dette tiltakskortet:

Det tas utgangspunkt i at virksomheten møter minimum de minstekravene som beskrevet under, når det gjelder hva den har av ressurser og lokale tilpasninger.

Minstekrav: personell som fungerer som IRT (eks helpdesk) , kriseledelse, beredskapsplan, kommunikasjonsansvarlige, incident manager (hendelsesleder), ledelsessystem

Anbefalt praksis: kommunikasjonsstab, strategisk og operativ kriseledelse, loggfører, IRT, beredskapsplan, kontinuitetsplan, ROS, BIA, DRP (gjenopprettingsplan) , operasjonelt ledelsessystem

Dette kortet viser til de tiltak vi har kommet frem til og hvilke roller som arbeidsoppgavene skal fordeles på. Det vil være lokale variasjoner med tanke på hva man kaller de ulike rollene og gruppene, men dette får være opp til hver enkelt og tilpasse sin virksomhet. Innholdet under er ment som hjelp til å lage et eget tiltakskort tilpasset den enkelte virksomhet.

Beskrivelse av hendelse

Løsepengevirus er et angrep som krypterer filer slik at sluttbruker ikke får åpnet dem lengre. Dette kan oppdages på flere måter, men som regel vises det en beskjed på klientmaskiner om at maskinen er infisert og at man må betale en sum for å låse dem opp igjen.
Det kan også komme trusler om at sensitiv informasjon vil publiseres dersom man ikke betaler.
Det kan også komme varsler fra CERT/Nettverk/Sikkerhetssystemer som viser trafikk eller aktivitet relatert til løsepengevirus.
Hvis man ikke vet omfanget, skal man gå ut fra at dette er av kategori “høy” frem til man har fått oversikt.

Høy:

- Flere sentrale system/servere er infisert
- En høy andel klienter er infisert
- Stadig flere henvendelser fra ansatte eller studenter kommer inn.
- Man vet ikke omfanget

Middels:

- Enkeltsystemer/servere er infisert, og man ser ikke spredning
- Noen klienter er infisert, men ikke spredning p.t.
- Ikke økende antall saker

Lav:

- Enkeltbrukere eller isolerte, lokale systemer er infisert

Varsle til IRT umiddelbart selv om man ikke har oversikt over omfang.

Sikt

Cybersikkerhetssenter for forskning og utdanning

Sjekkliste - håndtering

Kommunikasjon til relevante deler av virksomheten er viktig i alle punktene i lista. Det inkluderer alt fra berørte grupper av sluttbrukere, systemeiere til deler av ledelsen. Normalt vil inkludering av virksomhetens beredskapsorganisasjon hjelpe til med å oppfylle kommunikasjonsbehovet.

Felles for alle punktene er behovet for et godt situasjonsbilde. Flere av tiltakene kan være svært omfattende og bør ikke iverksettes helt ukritisk. Over tid vil omfanget av hendelsen blir klarere, og man bør «begynne på toppen av lista» og verifisere at tidligere vurderinger fremdeles er korrekte.
Det er ikke nødvendigvis sånn at man skal følge listen til punkt og prikke og man må selv ta en vurdering av hvilke tiltak som er hensiktsmessige å gjennomføre ut fra situasjonen.

Uavhengig av hvem som oppdager situasjonen vil varsling og mobilisering være første prioritet. Informasjonsbehovet varierer etter omfang og må vurderes i hvert enkelt tilfelle. Lokalt sikkerhetsresponsteam (IRT) skal alltid varsles. For førstelinje bør det være lav terskel for å melde ifra til IRT.

Sjekkliste lokalt IRT

IRT varsler lokal beredskapsorganisasjon etter interne retningslinjer i virksomheten

IRT varsler videre etter Felles rammeverk for håndtering av alvorlige IKT-hendelser i UH-sektoren til (sektorvis responsmiljø, SRM – Uninett CERT)

- Eksterne
- Kunder av virksomheten
- Det er en fordel å være åpen om hendelsen, som minimum innen ulike samarbeid-fora eller egen sektor (over betrodde kanaler, eksempelvis sektorens IRT-chat).
- Vurdere varsling til eksterne leverandører (eks. skyleverandør)

Koble fra datamaskiner/infrastruktur som er mistenkt infisert (IRT eller tilsvarende vurderer risiko)

- Tidskritisk, må handle raskt
- Stasjonære klienter, bærbare, mobiltelefoner, servere, virtuelle servere i sky.

Vurder utkobling av deler av nettverk (IRT)

Vurder utkobling av hele eller deler av:

- Forbindelsen til Internett
- Forbindelsen til forskningsnettet
- Lokale trådløse nett

Kriseledelse (operativ)

Varsling og mobilisering i virksomheten

- Informasjonsbehovet varierer etter omfang og må vurderes i hvert enkelt tilfelle. Lokalt IRT skal alltid varsles.

Sett førstemøte – få oversikt over omfanget og verifisere.
Personvernombud bør involveres i kriseledelsen

Varsling av myndigheter i samråd med IRT om situasjonen:

- Politiet
- Datatilsynet (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/nar-skal-jeg-melde-avvik/)
- KD (opprett kommunikasjonskanal mot dem)

Informasjon til ansatte/studenter

○ Lokale klientnett ○ Lokale servernett ○ VPN-nett Dette kan få store konsekvenser for primærvirksomheten, husk involvering av beredskapsorganisasjonen. Vurder passordbytte ○ Alle kontoer på tjenere og tjenester ○ Ressurskrevende, sjekk for kompromittering først Reinstallasjon Sjekk om fastvare er berørt (avansert tiltak, søk råd hos Cybersikkerhetssenteret/SRM) Sikkerhetskopier Gjenoppretting – vurdere bytting av passord, se om løsepengeviruset kan fjernes, om det lar seg gjøre med restore og reinstallering av systemer. Systemovervåkning (vurder bistand fra SRM) Læring av hendelsen – forebygging og deling av erfaringer Avvikshåndtering Finne ut hvilken type virus det er (ihht. rutiner) for å få mer informasjon om hvordan det fungerer, hvilke filer den har tatt og kryptert (evt. kan man finne ut om det er mulig å fjerne og «friskmelde» system?)	Håndtering av media Beslutningstaking ved oppdatert informasjon (dette må ikke ta for lang tid) Kontinuitetsplan for aktuell(e) tjeneste(r) iverksettes/aktiveres Betaling av løsepenger er noe vi ikke anbefaler (jf. NSM sine anbefalinger, se punkt 5: Tiltak mot digital utpressing (løsepengeangrep) og andre angrep - Nasjonal sikkerhetsmyndighet (nsm.no)) Informere når situasjonen er tilbake til normal Læring av hendelsen – forebygging og deling av erfaringer Avvikshåndtering Bistå myndigheter i forbindelse med etterforskning

Ressurser
Eget IRT, teamet som har utviklet og vedlikeholdt tjeneste som er infisert, PVO, tjenesteansvarlig, systemeier, sektorvis responsmiljø (SRM).

Det er viktig å tenke redundans i roller – for å sikre at man ikke har enkeltpersonsårbarheter. Ha personell som kan ta over oppgaver ved frafall.

Vi forutsetter at alle organisasjoner har et IRT på plass, og en strategisk og/eller operativ kriseledelse som raskt kan kalles sammen og behandle krisen organisatorisk.

- Varsling: Kan man raskt og enkelt varsle alle brukere?
- Sporing: Har man systemer som kan fange opp angrep og/eller omfang?
- Mottak: Har man et mottaksapparat for slike hendelser? (IRT/OBL/SBL/Annet?)
- Varighet: Hva vil konsekvensen være ved at personell blir opptatt i krisen?

Støtteapparat som sørger for ivaretagelse av personell med tanke på hviletid, mat og drikke og psykososial støtte. HR-direktør/representant har ansvaret for dette.

Mandat / Rollebeskrivelser

Helpdesk/førstelinje

Rollebeskrivelse: Mottaksenhet for hendelser som kommer inn (førstelinje). De må få informasjon om hvordan de skal svare på henvendelser.

Mandat: Videreformidling av informasjon til IRT ved hendelser.

IRT (Incident Response Team):

Rollebeskrivelse: jobbe med overvåkning og håndtering av sikkerhetshendelser

Mandat: IRT bør ha myndighet til å reagere raskt og ta ned vesentlige deler av infrastrukturen. Dette må forankres i ledelsen, slik at man ikke taper kritisk tid under hendelsen. Aksjoner inkluderer, men er ikke begrenset til:

- Tvunget passordskifte hos brukerne
- Nedstenging av servere, tjenester eller nettverkstilgang

Operativ kriseledelse/stab:

Rollebeskrivelse: ledende og koordinerende støtteenhet som sikrer effektiv hendelseshåndtering

Mandat: Kommunikasjon til relevante deler av virksomheten - ansatte og studenter, formidle informasjon ved hjelp av presse- og publikumskontakt.

Strategisk kriseledelse/stab:

Rollebeskrivelse: utarbeide strategi for hendelseshåndtering og læringspunkter i etterkant?

Mandat: Be om rapporter, oppfølgingsarbeid (særlig i etterkant)

På nivå høy: mandat til å beslutte nedstenging av system. (mtp omfang)

Kommunikasjonsavdeling:

Rollebeskrivelse: Har ansvar for mediekontakt og svare på henvendelser som kommer fra eksternt hold.

Mandat: Skal kun gis frigitt informasjon, slik at de kan "svare med det de vet" og ikke frigir informasjon som ikke skal frigis.

Loggfører:

Skal føre oversikt over alle hendelser under håndtering

Loggføres med tidspunkt, avsender, mottaker, innhold i melding, gjennomførte tiltak

Loggføring

Tydeliggjøring av: ansvar, rullering, lagring, formidling, gjennomgang i etterkant

Det må være tydelig ansvarsfordeling på hvem som loggfører hendelser.

For å ikke slite ut loggfører bør det være jevnlig rullering.

Anbefaler digital loggføring, så fremt dette er gjennomførbart. Ha analogt verktøy tilgjengelig ved bortfall av digitale løsninger.

Varsling og rapportering

- Uninett CERT (SRM) - De eskalerer evt. videre til NCSC og KD (Report a security incident | Uninett , Kontakt NCSC - Nasjonal sikkerhetsmyndighet (nsm.no))
- Lokal kriseledelse ved organisasjonen, lokal IRT, ansvarlig team for løsningen, PVO, tjenestansvarlig, systemeier
- Varsling til eksterne myndigheter jf. sikkerhetsloven § 4-5. Også virksomhetssikkerhetsforskriften § 8 har krav om varsling til andre som kan berøres av hendelsen.
- GDPR og personopplysningsloven (varslingsplikt)

Versjon

1.1 Oppdatert 30.09.2022: Oppdatert design
1.0 Oppdatert 23.11.2021: Tiltakskort opprettet