Løsepengevirus

TEMARAPPORT

NASJONAL SIKKERHETSMYNDIGHET

POLITIET KRIPOS

Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet(sikkerhetsloven). NSM skal gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid. **Nasjonalt cybersikkerhetssenter (NCSC)** ble etablert 2018. Senteret bidrar til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberangrep.

Kripos er den nasjonale politienheten for bekjempelse av organisert og annen alvorlig kriminalitet. I januar 2019 etablerte Kripos **Nasjonalt cyberkrimsenter (NC3),** som er det nasjonale senteret for forebygging, avdekking og bekjempelse av trusler og kriminalitet i det digitale rom. Senteret utvikler metoder og gir bistand til politidistriktene samt etterforsker egne saker innen cyberkriminalitet.

NSM og Kripos samarbeider tett i **Felles cyberkoordineringssenter (FCKS)**, og har sammen utarbeidet denne temarapporten om løsepengevirus.

Hva er løsepengevirus?

Løsepengevirus er en type skadevare som brukes til å kryptere filer hos et mål, og deretter kreve penger for å dekryptere dem. Der et tjenestenektangrep hindrer andre å få tilgang til et offers data, hindrer et løsepengevirus offeret selv å få tilgang til sine egne data. Kriminelle utnytter kryptering i vinnings hensikt ved at personen eller virksomheten som er rammet overtales til å betale for å gjenopprette tilgangen til sine data. I noen tilfeller opplever ofre som betaler at de blir rekompromittert.

Det er høy aktivitet med løsepengevirus i Europa. Europeiske politistyrker har også økt sin respons med bakgrunn i utviklingen og i en bekymring knyttet til utviklingen fremover.

Mange ulike klasser av løsepengevirus er identifisert. Flere av dem har vært i bruk i flere år, og demonstrerer at trusselen virusene representerer er vedvarende. Europeisk politi ser i noen tilfeller indikasjoner på høy grad av organisering hos de kriminelle aktørene, som gir dem høy kompetanse og kapasitet.

> Det finnes to typer løsepengevirus. Den første typen krypterer filene på en datamaskin eller et nettverk, mens den andre typen låser skjermen. Begge typer krever betaling av løsepenger for å kunne bruke datamaskinen normalt igjen. Denne betalingen kreves ofte i en kryptovaluta som Bitcoin.

Gjerningspersonene skaffer seg ulovlig tilgang til systemer de ønsker å infisere med løsepengevirus på ulike måter. Mål kan infiseres gjennom epostvedlegg i phishingkampanjer, og aktører kan begå datainnbrudd for å plante virus. Betalingen av løsepengene til utpresserne skjer ved bruk av kryptovaluta, noe som gjør transaksjonene vanskelig å spore.

Løsepengevirus er attraktivt for kriminelle på grunn av lav risiko for å bli identifisert og straffeforfulgt, og mulighet for høy profitt. Antallet registrerte tilfeller av løsepengevirus globalt har

økt hvert år siden 2013, og hadde en nedgang først i 2018. Selv med nedgang vedvarer trusselen, og antallet ofre er fortsatt høyt. Europol klassifiserer i dag løsepengevirus som den største trusselen etterforskere møter, blant alle typer nettkriminalitet. Løsepengevirus antas å ha kostet den globale økonomien 90 milliarder kroner i 2019.

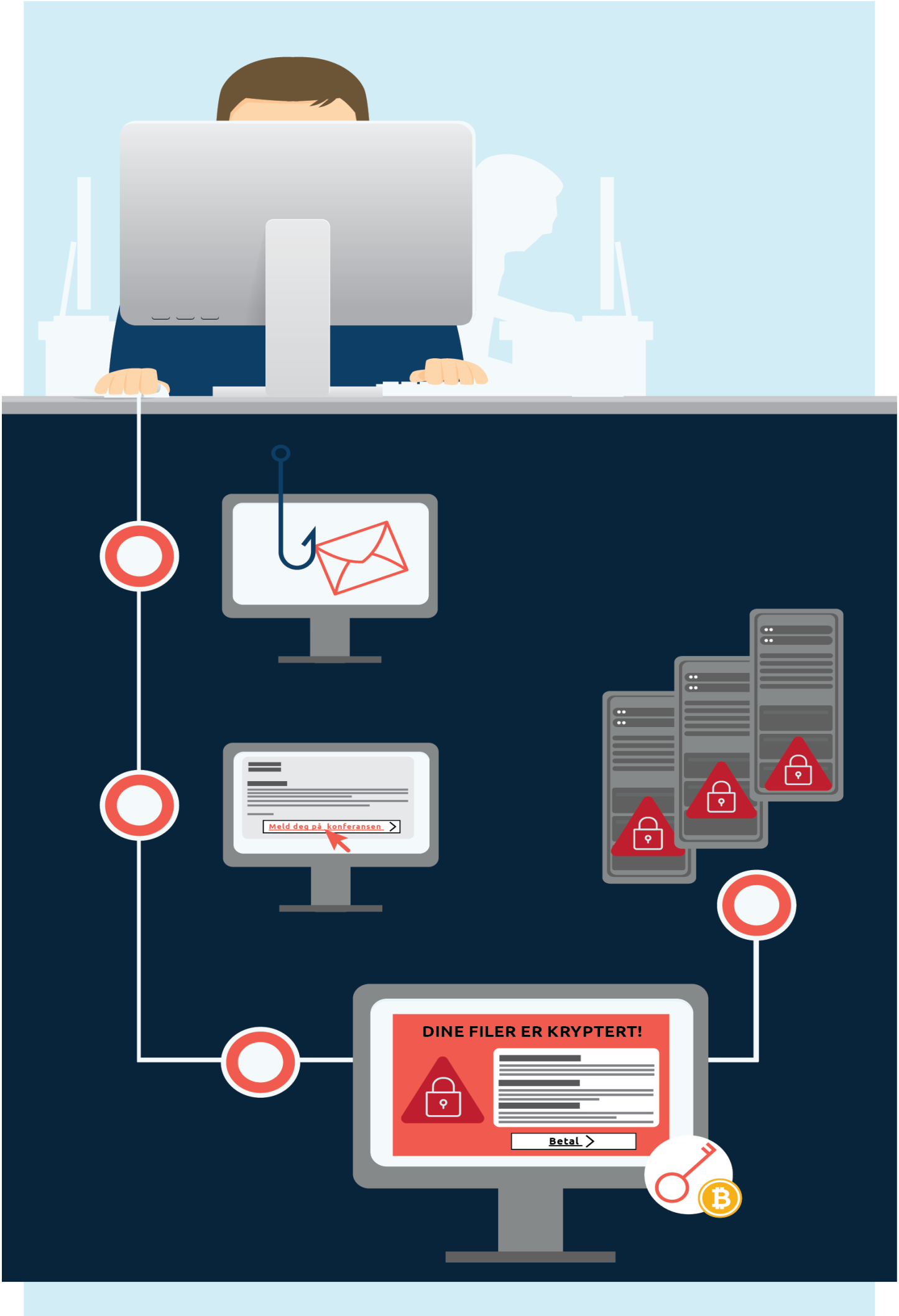
Utviklingen over de siste femten årene kan forstås som vekslende perioder med utpressingsaktivitet og skadevareutvikling. Løsepengevirus er likevel under kontinuerlig utvikling. Inaktive virus blir også videreutviklet, forbedret og tatt i bruk på ny.

Gjennom de siste årenes utvikling har en todeling av løsepengevirusmarkedet blitt framtredende. Løsepengevirus som rettes mot mange enkeltpersoner, har lavere løsepengesummer, og utgjør en liten del av løsepengevirusmarkedet. Den største delen av markedet består av målrettede angrep mot bedrifter og andre virksomheter, med høyere løsepengesummer. Slike målrettede angrep øker. Noe av nedgangen i antallet tilfeller totalt kan tilskrives denne endringen i hvem som rammes.

Mål som Norsk Hydro samsvarer med den typen mål som brorparten av løsepengevirusmarkedet er rettet mot, og som det er mulig vil inntreffe også i løpet av året som kommer. Bedrifter og organisasjoner som har tidskritiske prosesser er utsatte mål, fordi nedetid kan være svært kostbart for virksomheten. Dette øker betalingsviljen og sjansen for at utpresserne lykkes. Det er kjent at det har blitt framsatt krav om opptil to millioner euro i løsepenger.

Hvis berørte systemer leverer kritiske tjenester, kan dette ha alvorlige omdømme-, økonomi- og sikkerhetsmessige konsekvenser for berørte virksomheter og deres kunder. Selv om virksomheten har en nylig sikkerhetskopi av systemet, kan det fortsatt ta lang tid å gjenopprette normal drift.

Industrikontrollsystemer i sektorer som energi, jordbruk og luftfart blir i økende grad tilkoblet til, og dermed tilgjengelig fra, internett. Dette har skapt et industrielt "tingenes internett", og har bidratt til å øke sårbarhetsflaten i slike systemer betraktelig. Kompleksiteten i systemene, kombinert med den relativt raske implementeringen, bidrar til at det er vanskelig å beholde oversikt og sikre systemene. Dette bidrar til at sårbarheten i systemene kan være stor, uten at systemeier nødvendigvis er klar over det før en hendelse inntreffer. Nettverkene som utgjør det industrielle tingenes internett er sårbare for truslene som blant annet løsepengevirus utgjør.


Meld deg på konferansen
DINE FILER ER KRYPTERT!
Betal

Kan man forebygge løsepengevirus?

Norske bedrifter vil sannsynligvis fortsatt være utsatt for løsepengevirus i tiden framover. Bedrifter med tidskritiske prosesser vurderes som spesielt utsatt. Også andre norske organisasjoner og offentlig administrasjon kan være sårbare for angrep med løsepengevirus. Det er mulig at kriminelle aktører kan angripe flere bedrifter eller organisasjoner i samme land på samme tidspunkt.

For å hindre at skadevaren med løsepengevirus blir kjørt gjelder de samme forholdsreglene som for å beskytte seg mot annen skadevare. Sørger man for at programvare og maskinvare er oppdatert, og sikkerhetsfunksjonene aktivert er et godt grunnlag lagt. Ved å skaffe seg oversikt over programvare det er behov for i virksomheten, kan all øvrig programvare sperres av. Slik vil man kunne hindre en vanlig måte å få uønskede koder og programvare i systemene. I tillegg til kontroll av dataflyt, ved bruk av brannmurer med logging for å filtrere og kontrollere trafikk mellom ulike sikkerhetssoner og mot internett, utgjør disse tiltakene en god forebyggende strategi mot skadevare.

Viktige spørsmål

Om man blir utsatt for løsepengevirus, er det viktig å spørre seg:

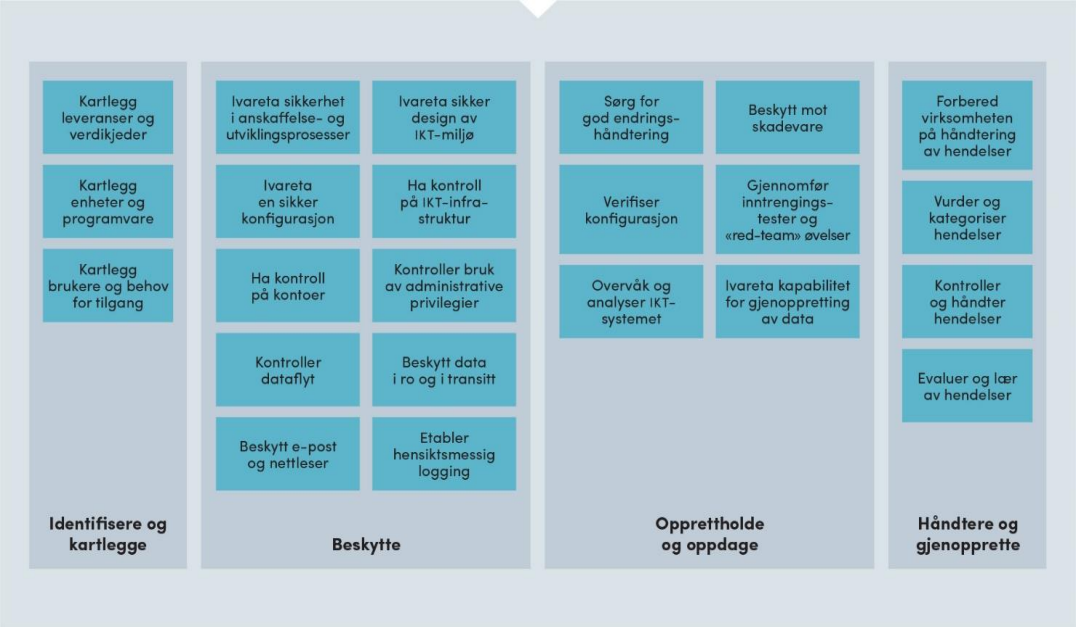
- Hvor mange andre varianter av løsepengeviruset er fortsatt i systemet, og venter på å bli aktivert?
- Hvordan skal vi fjerne dem?
- Hvordan kan vi advare brukerne?
- Ble andre typer skadevare distribuert samtidig?
- Hva slags type skadevare er det?
- Når blir de aktivert?

Figur 1 - faktaboks med spørsmål for utsatte virksomheter

Dersom et løsepengevirus er installert finnes det flere gode tiltak for å redusere konsekvensene. God tilgangs- og rettighetsstyring bidrar til å begrense spredningen av skadevaren. Testede sikkerhetskopieringsløsninger, der sikkerhetskopier av data ikke er tilgjengelig for maskiner utsatt for løsepengevirus, reduserer skadeomfanget ved et eventuelt løsepengevirusangrep.

Sårbarheter i én del av et nettverksbasert system forplanter seg til resten av systemet, og god kontroll på systemets oppbygning og datatrafikken mellom delsystemene er et sentralt ledd i god sikkerhetsstyring. Det anbefales at trafikken til og fra de mest sensitive delsystemene begrenses til kun de aller mest nødvendige protokoller og porter, og at disse sensitive delsystemene har egne nettverksoner. Disse bør kobles fra de øvrige systemene når man oppdager en kompromittering. For mer informasjon, se NSMs råd for beskyttelse mot løsepengevirus (https://www.nsm.stat.no/blogg/beskyttelse-mot-losepengevirus/) og grunnprinsipper for IKT-

sikkerhet (https://www.nsm.stat.no/grunnprinsipper-ikt).



Figur 2 - NSMs grunnprinsipper for IKT-sikkerhet

Om virksomheten likevel blir utsatt for løsepengevirus er det viktig å anmelde forholdet til politiet. Anmeldelse er også viktig i et allmennpreventivt og avskrekkende perspektiv, slik at den opplevde og reelle risikoen for å bli identifisert øker.