NASJONAL
SIKKERHETSMYNDIGHET

Hvordan forebygge, oppdage og håndtere dataangrep

HÅNDTERING AV
DIGITAL SPIONASJE

INNHOLD

INFORMASJONEN DIN ER ETTERTRAKTET

Dette temaheftet er laget for å gi noen tips på hvordan man kan forebygge og oppdage angrepsforsøk, samt gi støtte i de første fasene etter at et målrettet data-angrep er oppdaget. Målet er å hjelpe offer for denne type angrep, slik at de typiske fellene i startfasen unngås. De vanligste feilene kan være til hinder for senere analyse og håndtering av situasjonen.

HVA ER DIGITAL SPIONASJE?

Det er langt enklere å infiltrere datasystemer enn å innhente informasjon ved å bruke spesialtrente agenter. Infiltreringen omtales gjerne som «hacking» eller «datainnbrudd». I realiteten er målrettede angrep spionasje. Dette kan kalles «digital spionasje» eller «cyberspionasje».

Noen er villig til å bruke tid og ressurser på akkurat din virksomhet som etterretningsmål. En vanlig reaksjon hos virksomheter som utsettes for digital spionasje er «vi har da ingenting av verdi for andre» eller «vi forstår ikke hvorfor vi utsettes for dette». Din egen verdiforståelse samsvarer ikke nødvendigvis med motpartens. Digital spionasje er et tydelig tegn på at aktøren mener du har noe som er av verdi.

HVEM ER AKTØRENE?

STATLIGE AKTØRER eller aktører med statlig tilknytning som utfører mer eller mindre målrettede etterretningsoperasjoner mot enkeltindivider eller virksomheter, i den hensikt å tilegne seg kunnskap.

KRIMINELLE NETTVERK som utfører informasjonstyveri, gjerne i den hensikt å tilrettelegge for svindel eller annen økonomisk motivert kriminalitet.

KAOTISKE AKTØRER eller aktivister som utfører informasjonstyveri med påfølgende lekkasjer til allmennheten, enten motivert av idealisme eller politisk overbevisning, eller ut fra et ønske om å forårsake kaos eller for å få oppmerksomhet.

HVORDAN KOMMER DE SEG INN I SYSTEMET

En aktør kan enten operere målrettet, eller være mer opportunistisk i sin tilnærming. De blinker deg ut som et spesifikt mål, eller kaster garnet og ser hvilken fisk som går i maskene.

Metodene de ulike aktørene benytter er som oftest en variasjon av følgende:

- Epost med dokumentvedlegg med skjult spionprogramvare.
  - Eposten kan se ut til å komme fra noen du stoler påInneholder ofte en lenke som du blir fristet til å klikke på eller et vedlegg med tilsynelatende interessant innhold
- Direkte innbrudd i sårbare, eksponerte tjenester.
- Bruk av kompromitterte, legitime websider for spredning av spionprogramvare.

FOREBYGGENDE TILTAK OG ROBUSTE SYSTEMER

Å bygge robusthet gjør deg i stand til å møte trusler på en bedre måte. Et robust system kjennetegnes av:

En **driftsavdeling** med:

- god oversikt over eget nettverk og egne systemer
- som holder kontroll på tilgang og segmentering
- som sørger for at alle systemer er så godt oppdatert som overhode mulig til en hver tid

En **sikkerhetsavdeling** med:

- gode overvåkningssystemer
- dyktige folk som jakter på inntrengere og unormal oppførsel
- som sørger for at så mye som mulig av uønsket aktivitet i nettverk og systemer blir oppdaget

En **beredskapsplan** som:

- tydelig avklarer ansvarsforhold
- tydelig avklarer eskaleringsrutiner ved sikkerhetshendelser
- er konkret nok til å gi besluttende og utøvende personell støtte til håndtering av slike hendelser

HVA KAN DU SOM ANSATT GJØRE?

- Bruk sunn fornuft
- Ikke klikk på lenker i eposter. Du kan eventuelt kopiere adressen manuelt
- Hvis noen du kjenner sender deg en mail som virker mistenkelig, ikke klikk på lenken
- Ikke åpne vedlegg om du ikke kjenner avsenderen
- Hvis du kjenner avsender, men er usikker – ring vedkommende og sjekk om de faktisk har sendt deg noe
- Sjekk om avsenderen er riktig. Eks: Feilstavet, slutter på .com i stedet for .no, bruker gmail eller yahoo i stedet for jobb-epost.

HVORDAN OPPDAGE FORSØKENE?

Å skru på logging er det første viktige steget. Logging er avgjørende ved kartlegging og håndtering av eventuelle infiltrasjonsforsøk. Brannmurlogger, netflow og logger fra ulike sikkerhetsløsninger, kan også være nyttige.

Deretter blir neste steg å analysere informasjonen og finne mistenkelige oppføringer i loggene. Når man har logger på plass er det mulig å agere på informasjon som NSM NorCERT sender ut med tips til hva man skal se etter for å avdekke hendelser.

TRAFIKKLOGGER

Ved hjelp av trafikklogger kan man avdekke nettverkstrafikk generert av trusselaktør.

- **Webtrafikklogger / proxylogger**
  Logger over websurfing (HTTP TCP/80) ut på Internett fra eget nettverk. Om mulig med SSL-inspeksjon.
- **Netflow**
  Netflow-logger gir full oversikt over all nettverkstrafikk på egne systemer. Analyse av trafikkmønster hjelper med å skaffe oversikt over omfang og tidslinje for hendelser. Netflow er trafikkflytdata som inneholder metainformasjon om nettverkstrafikken på et gitt punkt i nettverket. Eksempel på slik metainformasjon er:
  - interne og eksterne adresser
  - tidspunkt og trafikkmengde.
- **DNS-logging / Passiv DNS**
  Dette er logger som viser oppslag av domener, hvilke adresser som domenet peker til og har pekt til tidligere.
  Se etter:
  - Domener
  - IP-adresser

  DNS-oppføringer kan variere hyppig over tid. En historisk oversikt over hvilke domener som er knyttet til hvilke adresser, kan derfor være avgjørende for å avdekke omfang av infiltrasjon.
  I visse tilfeller vil aktiviteten til angriper ikke vises i webtrafikkloggene, men kan likevel vises i DNS-logger.
- **Webaksesslogger mot egne web-servere**
  Logger med detaljert oversikt over websurfing (HTTP TCP/80) fra Internett mot egne webservere.
  Noen ganger kan man finne spor i webaksessloggene av aktivitet mot virksomhetens nettsider utført av angriper. Informasjonen her kan brukes til å skreddersy "lure-eposter" rettet mot virksomhetens medarbeidere.

HVA KAN VIRKSOMHETEN DIN GJØRE?

- Sørg for å holde programvare og operativsystemet oppdatert
- Ikke tildel sluttbrukere administratorrettigheter
- Hold brukerne bevisste
- Bruk gode passord og endre standardpassord på nye enheter, slå på to-faktor autentisering der det er mulig
- Et viktig tiltak som IT-administratorer kan gjøre for å oppdage at man er utsatt for datainnbrudd er logging, mer informasjon om dette nedenfor

AUTENTISERINGSLOGGER

Disse loggene gir innsikt i hvilke brukere som hatt tilgang til ulike tjenester. Ved å undersøke disse loggene kan man oppdage eventuelle mistenkelige innlogginger. Mistenkelige innlogginger kan oppdages ved å se på avvik fra normal aktivitet.
Avvik kan for eksempel være innlogging fra forskjellige steder i verden kort tid etter hverandre.

ADMINISTRASJONSLOGGER

Logger som dokumenterer administrative endringer av virksomhetens IKT-systemer, som typisk utføres av systemadministrator. I et datainnbrudd vil angriper gjerne forsøke å skaffe seg bruker- eller objekt-tilgang med administrative rettigheter.

Overvåkning av administrasjonslogger for opprettelse og endring av brukere vil kunne avdekke uautorisert brukeradministrasjon. For eksempel kan angriper opprette nye brukere på domenekontroller med utvidede rettigheter, for deretter å slette disse brukerne.

SIKKERHETSLOGGER

Sikkerhetsprodukter og -løsninger vil ofte produsere logger for sikkerhetshendelser som disse har reagert på. Noen av disse sikkerhetsløsningene vil stoppe uønsket aktivitet, og det er da særdeles viktig å logge hva som blir stoppet og om mulig sette aktuell data (som for eksempel mistenkelige filer) i karantene for videre undersøkelse.

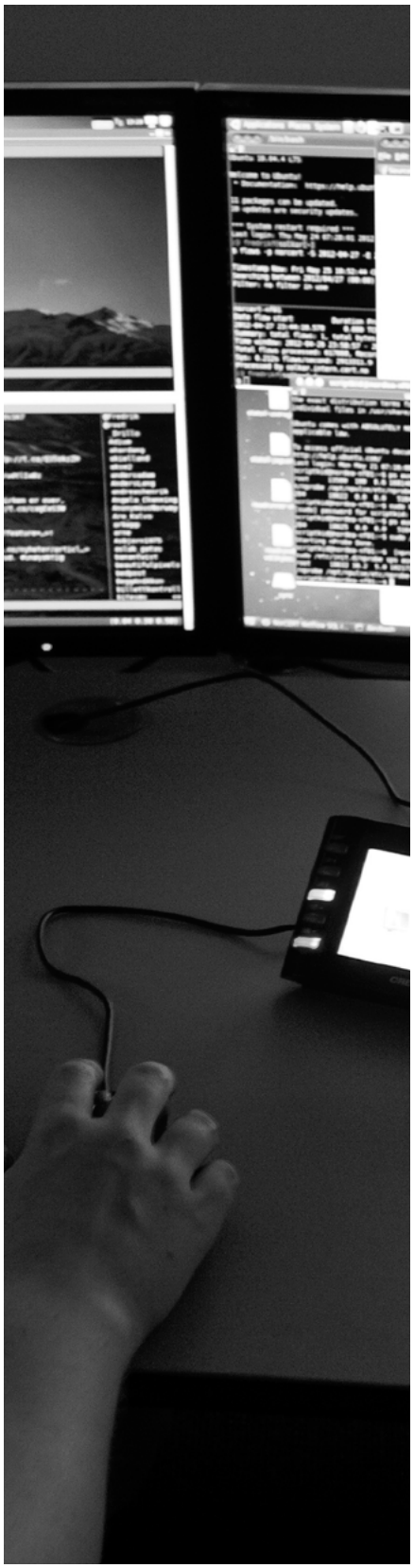
NorCERT kan hjelpe utsatte virksomheter med å analysere skadevare som har blitt stoppet på vei inn til virksomheten. Analyse vil kunne avdekke ytterligere informasjon om infiltrasjonsforsøket som igjen kan bidra til å avdekke andre relaterte hendelser.

E-POSTLOGGER

E-post blir ofte benyttet i digital spionasje. Analyse av teknisk informasjon om leveranse og innhold i e-post er sentralt i hendelseshåndteringen.

Slik analyse bidrar med informasjonen metode og infrastruktur benyttet av angriper. Logging av e-postleveranser må gjøres på en slik måte at man effektivt kan søke etter mistenkelige e-poster basert på teknisk informasjon. Dette kan være:

- Avsenderadresser
- Emner
- Vedleggsnavn



HVA TRENGER NSM NORCERT OG HVORFOR ?

Når angrepet er et faktum kan NSM NorCERT hjelpe din virksomhet med å håndtere hendelsen. For å kunne bistå best mulig ønsker vi relevant informasjon som beskrevet nedenfor:

HVA	HVORFOR
Rask oppsummering og tidslinje for hendelsen	Gir oss en god start for oppdatert situasjonsbilde i saken
Vurdering av hendelsen. Hvor alvorlig er det	Nyttig for oss å vite hvor alvorlig dere mener saken er, da dere kjenner egne verdier best
Hva er mottakernes rolle(r)?	Dette kan gi et innblikk i hva angriper er ute etter, og dermed hvor man bør lete etter flere spor
Mistenkelig e-post mottatt: • Kopi av e-posten med fulle mailheadere og eventuelle vedlegg • Vedlegg bør zippes og passordbeskyttes, eventuelt PGP-krypteres	Mailheadere er en god kilde til • informasjon rundt hendelser. • kan knytte separate hendelser sammen • kryptering sikrer konfidensialitet
Bruker har klikket på en mistenkelig lenke: • Kopi av logger for webtraffikk (proxy-logger) • DNS/PassivDNS-logger • eventuelt brannmurlogger	Kan bekrefte eller avkrefte om vedkommende har trykket på den ondsinnede lenken
Bruker har surfet på infisert nettside: • Kopi av logger for webtraffikk (proxy-logger) i det aktuelle tidsrommet • kopi av eventuell skadevare som har blitt lastet ned	Offeret kan ha blitt videresendt via en rekke nettsider. Slike logger kan bidra til å finne kilden til infeksjonen
En oversikt over undersøkelser virksomheten har utført selv	Selv undersøkelser med negative resultater er greit å ha med her for å få et oppdatert situasjonsbilde
Oversikt over mistenkt kompromitterte maskiner. **FØR** man gjør egne undersøkelser eller slår av maskin en anbefaler vi sikring av minne og harddisk	Minneanalyse kan bidra med å raskt identifisere kjørende skadevare og oppkoblinger. Diskanalyse vil være mer tidkrevende, men man vil kunne kartlegge mer av angripers aktivitet
Hvilken informasjon i denne saken kan deles videre med våre samarbeidspartnere?	Deling av teknisk informasjon er nyttig. Har samar beidspartnere sett noe lignende? Man kan da ha mulighet til å finne ny triggerinformasjon

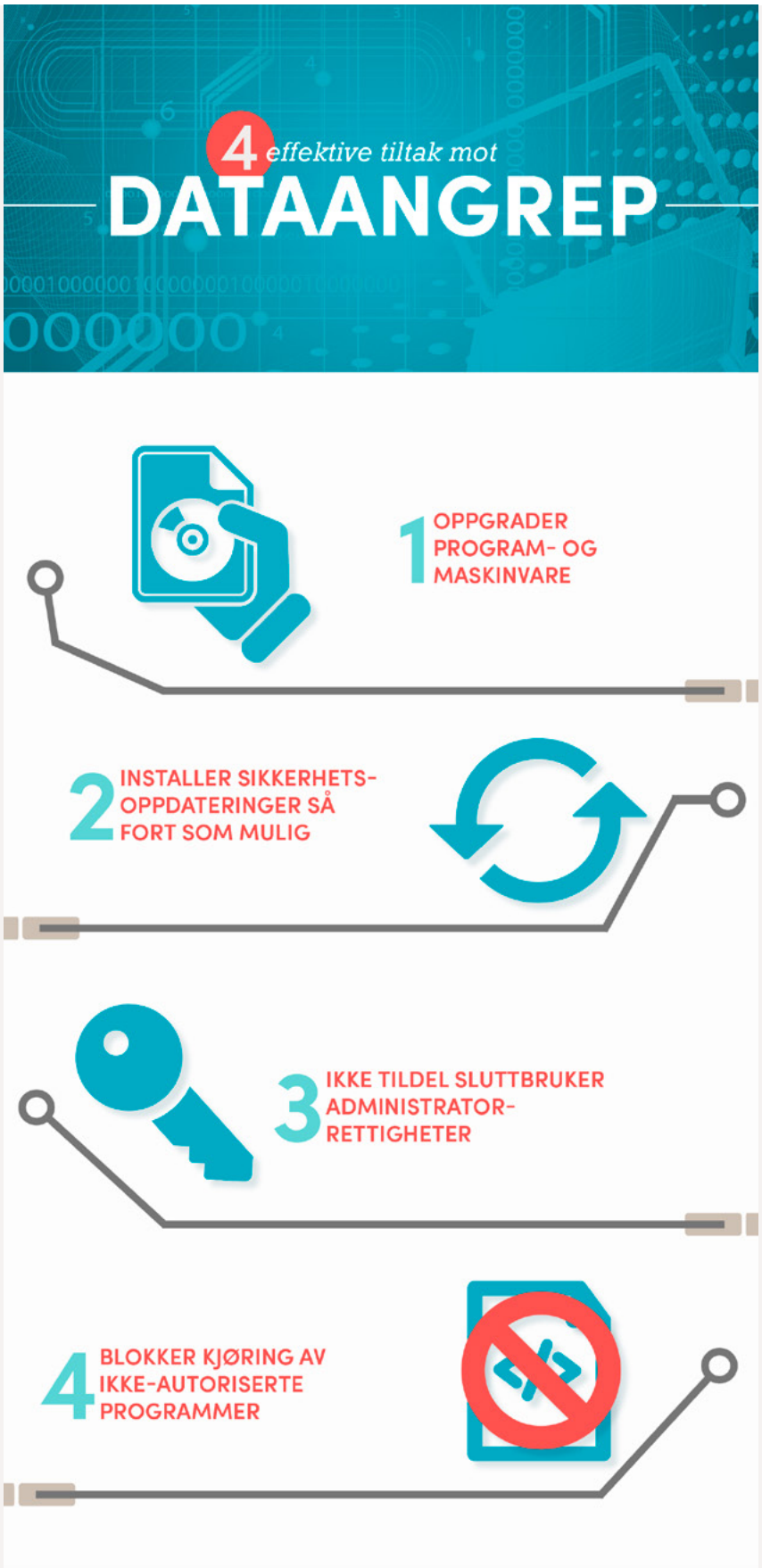
OPPRYDDING

Opprydding av kompromitterte systemer må planlegges og gjennomføres på en kontrollert måte. Analysen av hendelsen bør gi et fullstendig bilde av alle infiserte systemer. Dersom man går glipp av et kompromittert system gir dette angriper en ny mulighet til å gjenopprette kontroll over systemet.

- Isoler kompromitterte systemer fra nettverket
- Klargjør diskbilder og minnedump av alle kompromitterte systemer. Reinstaller med rene backups
- Endre alle passord for å sikre at angriper ikke kan benytte samme passord for å skaffe seg tilgang igjen

Se også NSMs FIRE EFFEKTIVE TILTAK MOT **DATAANGREP:**

Last ned hele veiledningen på NSMs nettsider. Søk etter: S-01



Studier viser at disse fire tiltakene stopper ca. **80-90%** av internett-relaterte angrep

For mer informasjon se NSMs nettsider **www.nsm.stat.no.** Søk etter S-01 og S-02 som omhandler tema.

NASJONAL SIKKERHETSMYNDIGHET

NorCERT – Operativ avdeling
Postboks 814
1306 Sandvika

post@cert.no
www.cert.no