

|   |  |
|---|--|
|  <p>Norm for informasjonssikkerhet<br/>www.normen.no</p> | Utgitt med støtte av:<br> |
| <h2>Tiltak for å hindre ondsinnet programvare</h2>  | <b>Støttedokument</b><br><b>Faktaark nr 19</b><br>Versjon: 2.1<br>Dato: 15.12.2010                           |

|  |  |   |  |
|--|--|---|--|
| <b>Målgruppe</b><br><br>Dette faktaarket er spesielt relevant for: | <input type="checkbox"/> Leverandør<br><input checked="" type="checkbox"/> IKT-ansvarlig<br><input type="checkbox"/> Forsker<br><input checked="" type="checkbox"/> Prosjektleder  | <input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator<br><input type="checkbox"/> Virksomhetens leder/ledelse<br><input type="checkbox"/> Forskningsansvarlig | <input type="checkbox"/> Medarbeider/ansatt<br><input checked="" type="checkbox"/> Databehandler<br><input type="checkbox"/> Personvernombud |
| <b>Ansvar</b>  | IKT-ansvarlig er ansvarlig for å gjennomføre beskyttelse mot ondsinnet programvare.  |   |  |
| <b>Gjennomføring</b>   | Tiltak for å hindre ondsinnet programvare skal iverksettes på bakgrunn av risikovurdering og faktisk teknisk løsning.  |   |  |
| <b>Formål</b>  | <ul style="list-style-type: none"> <li>• Hindre utilsiktet endring av helse- og personopplysninger</li> <li>• Hindre utilsiktet utlevering av helse- og personopplysninger</li> <li>• Sørg for at helse- og personopplysninger er tilgjengelig uten driftsforstyrrelser</li> </ul>   |   |  |
| <b>Omfang</b>  | Virksomheten skal iverksette tiltak for å hindre ondsinnet programvare med tanke på om det: <ul style="list-style-type: none"> <li>• tas i bruk usikre nettverk og tjenester</li> <li>• tas i bruk sikrede nettverk og tjenester</li> <li>• tas i bruk andre tilkoblingsløsninger som muliggjør overføring av ondsinnet programvare</li> </ul> |   |  |
| <b>Hjemmel</b>   | Personopplysningsforskriften § 2-13  |   |  |
| <b>Referanser</b>  | <ul style="list-style-type: none"> <li>• Normen pkt 5.5 Etablering og drift av informasjonssystemet</li> <li>• Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet</li> </ul>   |   |  |

| Nr.      | Aktivitet/Beskrivelse  |
|----------|--|
| <b>1</b> | <b>Fastsette behov for tiltak for å hindre ondsinnet programvare</b> <ol style="list-style-type: none"> <li>a) Dokumentere teknisk løsning:             <ul style="list-style-type: none"> <li>- Konfigurasjonskart slik at det klart kommer frem hvilke kilder til ondsinnet programvare som finnes</li> <li>- Beskrivelse av teknisk løsning</li> </ul> </li> <li>b) Gjennomføre risikovurdering av løsningen. For eksempel har følgende valg innvirkning på risiko og vil danne grunnlag for hvilke trusler som vurderes:             <ul style="list-style-type: none"> <li>- Ved å ta i bruk usikre nett og tjenester</li> <li>- Ved å ta i bruk sikrede nett og tjenester</li> <li>- Tilkobling til utstyr lokalt som kan være infisert og overføring av data og program til eksterne lagringsenheter</li> <li>- Oppkobling av fjernaksess fra leverandør</li> <li>- Tilkobling mellom virksomhetens tekniske løsning og databehandlers tekniske løsning</li> </ul> </li> <li>c) Avstemme risiko mot nivå for akseptabel risiko</li> <li>d) Fastsette områder som krever tiltak fordi risiko i løsningen overgår akseptabel risiko</li> <li>e) Dokumentere hvilke områder som krever beskyttelse mot ondsinnet programvare. For eksempel:             <ul style="list-style-type: none"> <li>- Ekstern kommunikasjon</li> <li>- E-post</li> <li>- Leverandører som kobler seg opp mot virksomhetens datautstyr via nettverk eller direkte via medbrakt datautstyr (fjernaksess)</li> </ul> </li> </ol> |

| Nr. | Aktivitet/Beskrivelse   |
|-----|---|
|     | <ul style="list-style-type: none"> <li>- Lagringsmedier som kobles til virksomhetens datautstyr (minnepinner, CD, løse harddisker, osv)</li> <li>- Meldingsformidling hvor virksomheten sender eller mottar meldinger elektronisk</li> <li>- Oppslag i eksterne katalogtjenester</li> </ul>   |
| 2   | <p><b>Dokumentere tiltakene</b></p> <ul style="list-style-type: none"> <li>a) Beskrive løsning for beskyttelse mot ondsinnet programvare</li> <li>b) Utarbeide prosedyrer for drift av løsningen</li> <li>c) Utarbeide prosedyre for rapportering internt ved deteksjon og håndtering av angrep av ondsinnet programvare</li> </ul>   |
| 3   | <p><b>Installere løsning for aktuelle områder</b></p> <ul style="list-style-type: none"> <li>a) Delegere oppgaver i virksomheten</li> <li>b) Inngå avtaler om utsetting av oppgaver til parter</li> <li>c) Inngå avtaler med leverandør av antivirussystemer (abonnement for kontinuerlig oppdatering av signaturfiler {en signaturfil inneholder oppdateringer som leverandøren av antivirusprogramvare sender sine abonnenter når det oppdages nye virus})</li> <li>d) Iverksette utarbeidede prosedyrer</li> </ul> |
| 4   | <p><b>Kontroll og oppfølging</b></p> <ul style="list-style-type: none"> <li>a) Sikkerhetsrevisjon skal gjennomføres for å påse at løsningen er iht etablerte prosedyrer og konfigurasjonskart</li> <li>b) Risikovurdering skal gjennomføres for å fastslå at løsningen gir beskyttelse som er innenfor fastsatte akseptkriterier</li> <li>c) Avvik fra etablerte krav skal behandles iht prosedyre for avvikshåndtering</li> </ul>  |

## Eksempel

Eksempler på tiltak for å hindre ondsinnet programvare. Det gjøres oppmerksom på at tiltakene må tilpasses den faktiske tekniske løsningen.

### Beskyttelse av teknisk løsning

- a) Arbeidsstasjoner skal kontrolleres ved pålogging eller kontinuerlig hvis de ikke skrus av
- b) Bærbart datautstyr skal kontrolleres før det kobles til nettverk. Dette er en meget aktuell problemstilling fordi signaturfiler hentes på det lokale nettverket ved tilkobling til nettverket. Krav til oppdaterte signaturfiler avhenger av hvordan det bærbare utstyret er benyttet når det ikke er knyttet til nettverket. Tillates tilkobling til andre nettverk, bruk av lagringsenheter, minnepinner, CD, osv, må dette ivaretas
- c) Alle sentrale tjenestemaskiner (servere) skal kontrolleres kontinuerlig
- d) Fjernaksessløsninger skal ha beskyttelsestiltak både hos leverandør og i virksomheten
- e) E-post skal hentes inn til nettverket og ikke automatisk sendes inn i nettverket
- f) Ekstern kommunikasjon skal ha deteksjon av forsøk på angrep
- g) Medisinsk teknisk utstyr og tilhørende servere og arbeidsstasjoner skal ha beskyttelse mot ondsinnet programvare på lik linje med annet datautstyr dersom hensiktsmessig og mulig
- h) Annet utstyr som kan inneholde ondsinnet programvare (f.eks. mobiltelefoner) skal kontrolleres ved tilkobling til nettverk
- i) Beskyttelsestiltakene skal konfigureres slik at bruker ikke kan overstyre kontrollen

### Oppdatering av signaturfiler

- a) Signaturfiler skal hentes inn på en sikker måte for deretter rutinemessig å bli distribuert til klientene

### Kontroll av filer og medier

- a) Alle medier som kobles til arbeidsstasjon eller server (CD, minnepinner, lagringsenheter, osv) skal kontrolleres før filer overføres
- b) Filer og vedlegg til ekstern Internett-e-post (fra virksomheter utenfor Norsk Helsenett) som legges i karantene (fordi vedlegget bryter med policy for hva som er tillatt å sende som vedlegg til e-post; binære filer, krypterte filer, ZIP-filer, m.m.) krever manuell oppheving av karantene
- c) Sikkerhetskopi skal kontrolleres for å sikre at kopi ikke inneholder ondsinnet programvare
- d) Nedlasting av oppdateringer fra Internett skal kontrolleres. Det anbefales at slik nedlasting gjøres gjennom en egen filsluse
- e) Overføring fra filer fra/til supportleverandør (fjernaksess) til/fra virksomheten