NORMEN

Tiltak for å hindre ondsinnet programvare (faktaark 19)

Versjon 3.1

26.09.2018

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler tiltak en virksomhet kan innføre for å hindre utilsiktet endring, utlevering og manglende tilgjengelihet til helse- og personopplysning som følge an ondsinnet programvare. Virksomheten skal iverksette tiltak for å hindre slik programvare der det: • tas i bruk usikre nettverk og tjenester • tas i bruk sikrede nettverk og tjenester • tas i bruk andre tilkoblingsløsninger som muliggjør overføring av ondsinnet programvare Faktaarket har en prosessorientert tilnærming og inneholder eksempel på beskyttelse av teknisk løsning
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er: • IKT-ansvarlig • Prosjektleder • Sikkerhetsleder / sikkerhetskoordinator • Databehandler
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen • Kapittel 5.4 Sikker IT-drift
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Personvernforordningen artikkel 32 Sikkerhet ved behandlingen • Veileder for fjernaksess mellom virksomhet og leverandør

Tiltak for å hindre ondsinnet programvare

Nr.	Aktivitet/Beskrivelse
1	**Fastsette behov for tiltak for å hindre ondsinnet programvare** a) Dokumentere teknisk løsning: - Konfigurasjonskart slik at det klart kommer frem hvilke kilder til ondsinnet programvare som finnes - Beskrivelse av teknisk løsning b) Gjennomføre risikovurdering av løsningen. For eksempel har følgende valg innvirkning på risiko og vil danne grunnlag for hvilke trusler som vurderes: - Ved å ta i bruk usikre nett og tjenester - Ved å ta i bruk sikrede nett og tjenester - Ved å tillate administrative brukere / eleverte privilegier på brukere versus å begrense rettigheter til vanlige brukere - Tilkobling til utstyr lokalt som kan være infisert og overføring av data og program til eksterne lagringsenheter - Oppkobling av fjernaksess fra leverandør - Tilkobling mellom virksomhetens tekniske løsning og databehandlers tekniske løsning c) Avstemme risiko mot nivå for akseptabel risiko d) Fastsette områder som krever tiltak fordi risiko i løsningen overgår akseptabel risiko e) Dokumentere hvilke områder som krever beskyttelse mot ondsinnet programvare. For eksempel: - Ekstern kommunikasjon - E-post - Leverandører som kobler seg opp mot virksomhetens datautstyr via nettverk eller direkte via medbrakt datautstyr (fjernaksess) - Lagringsmedier som kobles til virksomhetens datautstyr (minnepinner, CD, løse harddisker, osv) - Meldingsformidling hvor virksomheten sender eller mottar meldinger elektronisk - Oppslag i eksterne katalogtjenester
2	**Dokumentere tiltakene** a) Beskrive løsning for beskyttelse mot ondsinnet programvare b) Utarbeide prosedyrer for drift av løsningen c) Utarbeide prosedyre for rapportering internt ved deteksjon og håndtering av angrep av ondsinnet programvare d) Etablere en opplæringsplan som bevisstgjør brukere slik at man hindrer spredning av ondsinnet kode

Nr.	Aktivitet/Beskrivelse
3	**Installere løsning for aktuelle områder** a) Delegere oppgaver i virksomheten b) Inngå avtaler om utsetting av oppgaver til parter 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}) d) Iverksette utarbeidede prosedyrer
4	**Kontroll og oppfølging** a) Sikkerhetsrevisjon skal gjennomføres for å påse at løsningen er iht etablerte prosedyrer og konfigurasjonskart b) Risikovurdering skal gjennomføres for å fastslå at løsningen gir beskyttelse som er innenfor fastsatte akseptkriterier c) Avvik fra etablerte krav skal behandles iht prosedyre for avvikshåndtering

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) Utstyr skal kontrolleres kontinuerlig
b) Sikkerhetsoppdateringer skal installeres regelmessig
c) Fjernaksessløsninger skal ha beskyttelsestiltak både hos leverandør og i virksomheten
d) E-post skal hentes inn til nettverket og kontrolleres for ondsinnet programvare og ikke automatisk sendes inn i nettverket
e) Ekstern kommunikasjon skal ha deteksjon av forsøk på angrep.
f) Medisinsk utstyr og tilhørende servere og arbeidsstasjoner skal ha beskyttelse mot ondsinnet programvare. Dersom dette ikke er hensiktsmessig eller mulig skal en risikovurdering vise at nødvendige tiltak er etablert. Se Veileder i personvern og informasjonssikkerhet- medisinsk utstyr.
g) Annet utstyr som kan inneholde ondsinnet programvare (f.eks. mobiltelefoner) skal kontrolleres ved tilkobling til nettverk
h) Beskyttelsestiltakene skal konfigureres slik at bruker ikke kan overstyre kontrollen
i) Monitorering benyttes for å raskt avdekke ondsinnet kode. Monitorertingen bør fange opp varslene som genereres i de ulike tekniske tiltakene og rapporteres slik at hendelsen avdekkes så raskt som mulig.

Oppdatering av sikkerhetsløsninger

a) Oppdateringer til sikkerhetsløsninger skal hentes og installeres på en sikker måte.

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 fra e-post 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 skal kontrolleres for ondsinnet programvare