Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Tiltak for å hindre ondsinnet programvare

Støttedokument
Faktaark nr 19
Versjon: 3.1
Dato: 26.09.2018

Formål	• Hindre utilsiktet endring av helse- og personopplysninger • Hindre utilsiktet utlevering av helse- og personopplysninger • Sørge for at helse- og personopplysninger er tilgjengelig uten driftsforstyrrelser		
Ansvar	IKT-ansvarlig er ansvarlig for å gjennomføre beskyttelse mot ondsinnet programvare.		
Gjennomføring	Tiltak for å hindre ondsinnet programvare skal iverksettes på bakgrunn av risikovurdering og faktisk teknisk løsning.		
Omfang	Virksomheten skal iverksette tiltak for å hindre ondsinnet programvare med tanke på om 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		
Målgruppe Dette faktaarket er spesielt relevant for:	☐ Leverandør ☒ IKT-ansvarlig ☐ Forsker ☒ Prosjektleder	☒ Sikkerhetsleder / sikkerhetskoordinator ☐ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☐ Medarbeider/ansatt ☒ Databehandler ☐ Personvernombud
Hjemmel	Personvernforordningen artikkel 32		
Referanser	• Normen pkt. 5.4 Etablering og drift av informasjonssystemet • Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet		

Merknad 26.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

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

Nr.	Aktivitet/Beskrivelse
	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
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.

<u>Beskyttelse av teknisk løsning</u>

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

Anbefalte tiltak fra Nasjonal sikkerhetsmyndighet (NSM)

NSM har utarbeidet en sjekkliste med 10 viktige tiltak mot dataangrep. Vi anbefaler alle virksomheter som et minimum å implementere de 4 mest effektive tiltakene fra denne sjekklisten:

a) Oppgrader program- og maskinvare
b) Installer sikkerhetsoppdateringer så fort som mulig
c) Ikke tildel administrator-rettigheter til sluttbrukere
d) Blokker kjøring av ikke-autoriserte programmer («hvitelisting»)

Hele sjekklisten med forklaring er tilgjengelig på NSM sine sider og kan lastes ned her