Sjekkliste nr 1 (S-01)
Oppdatert 2016-03-03

Fire effektive tiltak mot dataangrep

Dette dokumentet beskriver fire enkle, men effektive tekniske tiltak som systemeiere i offentlige sektor bør benytte for å beskytte sine ugraderte systemer mot internett-relaterte dataangrep. Tiltakene er beskrevet mer detaljert i NSMs dokument U-01 (se lenke nederst).

De mest vanlige dataangrep skjer via infiserte e-poster, nettsider, eller USB-minnepinner. De fleste av disse angrepene er teknisk sett relativt enkle å stoppe. NSM har i flere tiår utviklet tekniske sikkerhetstiltak for beskyttelse av nasjonens graderte systemer. Ut i fra disse og andre erfaringer ser vi at virksomheter enkelt kan stanse de mest vanlige angrepene (ca. 80-90%) med fire tekniske tiltak:

1. **Oppgrader program- og maskinvare.** Nyere produktversjoner har tettet flere sikkerhetshull enn eldre versjoner, og de har ofte flere og bedre sikkerhetsfunksjoner. Dette gjelder både program- og maskinvare. Windows 7 og Windows 8 har for eksempel vesentlig flere og mer tidsriktige sikkerhetsfunksjoner enn Windows XP. Også siste versjon av Internet Explorer, Microsoft Office og Adobe Reader er vesentlig sikrere enn tidligere versjoner.

2. **Installere sikkerhetsoppdateringer så fort som mulig.** Selv de beste produktene har feil og sårbarheter som kan bli utnyttet av angripere. Systemeiere bør etablere et sentralt styrt regime for oppdatering av applikasjoner, operativsystemer og firmware (f. eks. BIOS-kode). Dette er viktig fordi kunnskap om nyoppdagede sårbarheter spres raskt. Derfor bør systemeiere være tilsvarende raske med å installere sikkerhetsoppdateringer som fjerner eller motvirker sårbarhetene. Man bør prioritere å holde operativsystemet oppdatert, deretter applikasjoner som leser eksterne data, bl.a. Office-pakker, PDF-lesere og nettlesere. Produkter som ikke lar seg oppdatere bør unngås.

3. **Ikke tildel administrator-rettigheter til sluttbrukere.** De fleste sluttbrukere har ikke behov for administrator-rettigheter. Dessverre gir altfor mange virksomheter brukerne (og angriperne) skriverettigheter til systemområder. Dette er unødvendig, og man lar i så fall datamaskinen være ganske åpen for angriperne. Man bør derfor fjerne administrator-rettigheter fra vanlige kontorbrukere, og distribuere virksomhetsgodkjent programvare fra et felles distribusjonspunkt.

4. **Blokker kjøring av ikke-autoriserte programmer** («hvitelisting»). Bruk verktøy som Windows AppLocker for å kontrollere at sluttbrukere kun får kjøre godkjente applikasjoner. Blokker spesielt programmer utenfor godkjente mapper og på flyttbare media, for eksempel på CD'er og minnepinner. Dette kan enklest oppnås ved å angi at programmer i mappene *C:\Programfiler* og *C:\Windows* kan kjøres mens programvare i andre mapper skal blokkeres. Eksempelvis er programmer på USB-minnepinner eller i e-postvedlegg ofte en kilde til angrep. Med AppLocker vil ikke disse ukjente programmene kunne kjøres. Brukere kan likevel fortsatt bruke minnepinner til dataoverføring (.doc, .ppt, .pdf mm).

Søk etter «**S-02**» og «**U-01**» på NSMs nettsider (www.nsm.stat.no) for **mer informasjon** om sikring av ugraderte systemer i offentlig sektor. U-01 inneholder **eksempler på konfigurasjonsfiler** for flere av de angitte tiltakene.

Se også australske myndigheters empiriske målinger av effektiviteten til 35 utvalgte sikkerhetstiltak mot internett-relaterte angrep: www.dsd.gov.au/infosec/top35mitigationstrategies.htm.