Nasjonal sikkerhetsmyndighet

Sjekkliste nr 2 (S-02)
Oppdatert 2016-03-03

Ti viktige tiltak mot dataangrep

Dette dokumentet beskriver ti effektive tekniske tiltak som systemeiere i offentlig 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).

Steg 1: De fire mest effektive tiltakene

1. **Oppgrader program- og maskinvare.** Nyere produktversjoner har tettet flere sikkerhetshull enn eldre versjoner, og de har ofte flere og bedre sikkerhetsfunksjoner.
2. **Installer sikkerhetsoppdateringer så fort som mulig.** Selv de beste produktene har feil og sårbarheter som kan utnyttes av angripere. Systemeiere bør etablere et sentralt styrt regime for oppdatering av applikasjoner, operativsystemer og firmware (f. eks. BIOS-kode).
3. **Ikke tildel administrator-rettigheter til sluttbrukere.** De fleste sluttbrukere har ikke behov for administrator-rettigheter. I et sentralt administrert system kan sluttbrukere få den programvaren de trenger 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, som for eksempel på CD'er og minnepinner.

Studier viser at disse fire tiltakene stopper ca. 80-90% av internett-relaterte angrep. Se også S-01.

Steg 2: Seks tilleggstiltak

5. **Aktiver kodebeskyttelse mot ukjente sårbarheter**. DEP, SEHOP, ASLR og EMET styrker systemet mot sårbarheter i applikasjoner og operativsystemet selv når det ikke finnes en oppdatering.
6. **Herde applikasjoner.** Protected Mode/View for Internet Explorer, Microsoft Office og Adobe Reader begrenser skadeomfanget ved kompromittering. Deaktiver unødvendig mobil kode og makroer.
7. **Bruk klientbrannmur.** Windows Firewall blokkerer all ubedt innkommende trafikk og logger sikkerhetsrelevante hendelser. Inspiser loggfilene regelmessig.
8. **Bruk sikker oppstart og diskkryptering.** Windows Secure Startup og Windows BitLocker bruker TPM-målinger og harddiskkryptering for å oppdage manipulering av oppstartsprosessen og forhindre tap av data fra stjålne/tapte PC'er.
9. **Bruk antivirus/antiskadevare.** Antivirus oppdager og blokkerer kjent skadevare som bl.a. utnytter sårbarheter i epost-programmer og dokumentlesere. Fortrinnsvis bør man bruke et produkt som kan styres sentralt og som virker bra sammen med operativsystemet.
10. **Ikke installer mer funksjonalitet enn nødvendig.** Enhver ny applikasjon og funksjon øker mulighetene for angrep. Få brukere har for eksempel behov for Java Runtime eller JavaScript i Adobe Reader. Også unødvendig programvare må herdes og oppdateres, noe som øker administrasjonsbyrden på systemet.

Søk etter «**U-01**» på NSMs nettsider (www.nsm.stat.no) for **mer informasjon** om disse tiltakene og andre tiltak for sikring av Windows. U-01 inneholder også **eksempler på konfigurasjonsfiler** for flere av de nevnte tiltakene.