

Oppdatering, sikkerhetskopiering og utfasing av operasjonell teknologi

To viktige sikkerhetstiltak er oppdatering og sikkerhetskopier.

Oppdaterte operativsystemer og programvare gjør jobben vanskeligere for angripere dersom de først er inne i et nettverk. Utdaterte systemer har ofte kritiske sårbarheter som kan utnyttes for å utvide rettigheter og bevege seg rundt i nettverket. Oppdatering er derfor et kjempeviktig tiltak.

Å holde operativsystem og annen programvare i OT-nettverk oppdatert har likevel utfordringer. Eksisterende utstyr kan for eksempel være avhengig av en spesifikk programvareversjon. Oppdatering kan føre også til nedetid, både ventet og uventet.

Noen ganger er det heller ikke mulig å oppgradere operativsystemet uten å bytte ut maskinen det kjører på. For å unngå dette, er det viktig å ha en plan for utfasing av eldre OT- og IT-utstyr.

Installer oppdateringer der det lar seg gjøre og under kontrollerte omstendigheter. Helst i regelmessige vedlikeholdsvinduer, for å være sikker på at det blir gjort og gir minst mulig nedetid.

Sikkerhetskopier:

Blir man utsatt for løsepengevirus (ransomware), fører det til nedetid. Med sikkerhetskopier kan man minimere den nedetiden. Uten sikkerhetskopier er man prisgitt angriper, ellers må alt settes opp igjen fra grunnen av.

Om sikkerhetskopier skal være en fungerende sikring, er det viktig med rutiner for å ta dem jevnlig, at man øver på å bruke dem og har kopiene lagret en plass angriper ikke får ødelagt dem.

Angripere prioriterer ofte sikkerhetskopisystemer. Derfor er det viktig å ha en trygg løsning som de ikke kan overskrive, for eksempel gjennom at kopiene oppbevares isolert. Her anbefaler vi [3-2-1-metoden](#).

Dersom man er avhengig av leverandør for sikkerhetskopiering, er det viktig at man avtaler hvilke roller og ansvarsområder hver part har.

Anbefalinger:

Etabler rutiner for oppdatering av OT- og IT-utstyr i OT-soner:

For utstyr som nås direkte fra internett:

- Må kunne oppdateres umiddelbart dersom nye kritiske sårbarheter dukker opp
- Må oppdateres regelmessig utenom dette

For internt utstyr:

- Enheter som kan oppdateres bør oppdateres rutinemessig og ikke sjeldnere enn hvert kvartal

Fas ut eldre operativsystemer og produkter:

Bytt ut operativsystemer og produkter før de ikke lenger støttes av produsent.

Følg [3-2-1 metoden](#) for sikkerhetskopiering:

Etabler rutiner for sikkerhetskopiering av OT- og IT-utstyr i OT-soner og følg 3-2-1 metoden.

Kort oppsummert innebærer det:

- Sikkerhetskopier bør oppbevares isolert utenfor OT-sonen
- Verifiser rutinemessig at sikkerhetskopier tas og at de kan gjenopprettes fra
- Man må ha rutiner for å gjenopprette fra sikkerhetskopier. Disse må øves på årlig.