NorSIS

FORSTÅ NSMs GRUNNPRINSIPPER FOR IKT-SIKKERHET

Du har kanskje hørt at Nasjonal sikkerhetsmyndighet (NSM) har gitt ut grunnprinsipper for IKT-sikkerhet. Men hva er egentlig dette?

NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper for hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser.

Grunnprinsippene beskriver hva en virksomhet bør gjøre for å sikre et IKT-system. De beskriver også hvorfor det bør gjøres, men ikke hvordan.

Grunnprinsippene kompletterer men erstatter ikke en virksomhets sikkerhetsstyringsarbeid.

Grunnprinsippene hjelper virksomheter av alle størrelser å bedre forstå, administrere, og redusere sin sikringsrisiko.

1. IDENTIFISER

Dette er grunnlaget for en effektiv implementering av de øvrige grunnprinsippene. Hensikten er å forstå virksomhetens leveranser og tjenester, få oversikten over hvilke teknologiske ressurser som må sikres og de roller og brukere virksomheten består av.

- Kartlegg leveranser og verdikjeder.
- Kartlegg enheter og programvare.
- Kartlegg brukere og behov for tilgang.

2. BESKYTT

Ivareta en sikker tilstand for IKT-miljøet for å motstå eller begrense skaden ved dataangrep.

- Ivareta sikkerhet i anskaffelser og utviklingsprosesser.
- Ivareta sikker design av IKT-miljø.
- Ivareta en sikker konfigurasjon.
- Ha kontroll over IKT-infrastruktur.
- Ha kontroll over opprettelse, bruk og deaktivering av brukerkonti.
- Kontroller bruken av administrative privilegier.
- Kontroller dataflyten inn til virksomheten og mellom sikkerhetssoner.
- Beskytt data ved lagring og kommunikasjon.
- Beskytt e-post og nettleser.
- Etabler hensiktsmessig logging.

3. OPPRETTHOLD OG OPPDAG

Opprettholde den sikre tilstanden i IKT-systemet over tid etterhvert som virksomheten utvikler seg.

Etabler en prosess for endringshåndtering, planlegg implementering av endringer og vurder konsekvensene av disse.

Beskytt IKT-systemene mot skadevare. Bruk gjerne automatiserte verktøy.

Verifiser konfigurasjonen ved bruk av automatisert verktøy for sporing av endringer.

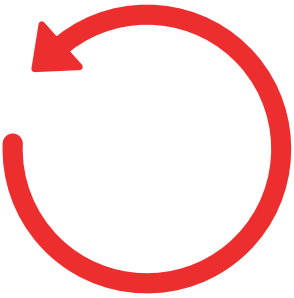
Gjennomfør inntrengingstester og øvelser for å teste den totale styrken i virksomhetens forsvarsmekanismer.

Overvåk og analyser IKT-systemet for å bygge en situasjonsforståelse av handlinger og aktiviteter i nettverket.

Bruk automatiserte verktøy for jevnlig sårbarhetskontroll av infrastrukturen.

Ta sikkerhetskopier, og verifiser at tilbakekopiering er mulig.

4. HÅNDTER OG GJENOPPRETT



Forbered virksomheten på håndtering av hendelser.

Etabler en plan for håndtering av hendelser, og øv planen med de som er involvert.

Vurder og kategoriser hendelser.

Kontroller og håndter hendelser. Loggfør alle aktiviteter underveis.

Etabler varslingslister over kunder, ansatte og andre som er berørt.

Iverksett gjennopprettingsplan. Tiltak vil variere avhengig av type hendelse.

Evaluer og lær av hendelseshåndteringen i etterkant.

https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/