SÅNN ØKER DU IT-SIKKERHETEN I VIRKSOMHETEN

Ved å følge disse anbefalingene kan du avverge mange forsøk på datakriminalitet.

Serit sine beste råd til IT-ansvarlig:

1. Gi alle medarbeidere en grunnleggende innføring i IT-sikkerhet
   - Se gjerne ovelse.no for øvingspakker fra NorSIS.
2. Sikre identitet
   - Aktiver to-faktor-autentisering.
   - Unngå at alle tjenester bruker egne kontoer, gjenbruk AD-konto/skykonto der det er mulig.
3. Sikre nettverk
   - Kontroller regler i brannmuren.
   - Isoler ulike tjenester og servere til egne nettverkssoner.
4. Sikre maskinvare
   - Oppdater antivirus og sikkerhetsprogramvare.
5. Sikre e-post
   - Kontroller og still inn SPF, DKIM, DMARC
   - Aktiver anti-phishing/anti-spam der det er mulig
6. Kontroller backup og gjenoppretting regelmessig
7. Aktiver overvåking og opprett automatiske varslinger
8. Ha en handlingsplan klar før dere blir angrepet

Dette må en handlingsplan inneholde:

1. **Isoler de infiserte enhetene**
   - Koble fra nettverk og kommunikasjonslinjer for å hindre spredning til andre enheter.
2. **Varsling**
   - Aktuelle varslingspunkter kan være IT-leverandør, politiet, NSM og berørte brukere.
3. **Handling**
   - Rådfør deg med IT-leverandør for å få inntrengerne ut av systemene dine.
4. **Gjenopprett**
   - Har dere backup kan arbeidet med å gjenopprette starte nå. De kritiske systemene bør prioriteres.
5. **Kommunikasjon**
   - GDPR-lovgivningen er tydelig på at alle berørte må varsles. Med tanke på omfanget må en også ha en plan for hvorvidt og hvordan bedriften også skal dele informasjon med offentligheten.

Trenger du hjelp? Du finner ditt nærmeste Serit-kontor på www.serit.no.