

Sikkerhetstiltak

Bruk tilgjengelige sikkerhetsmekanismer

- Bruk gode passord og endre alle standardpassord
- Del nettverk i separate soner og implementer nettverksfiltrering
- Deaktiver tjenester som ikke er i bruk

Innfør gode rutiner for oppdatering av systemer

- Hold all infrastruktur, operativsystem og programvare oppdatert med nyeste sikkerhetsoppdateringer
- Unngå bruk av operativsystem og programvare som ikke lenger vedlikeholdes av produsent

Innfør gode rutiner for håndtering av brukerkontoer

- Begrens antall administratorer til et minimum
- Gi brukere kun de rettigheter de faktisk trenger
- Unngå bruk av upersonlige kontoer og deaktiver kontoer som ikke skal være i bruk

Still krav til gode passord

- Alle passord bør inneholde en kombinasjon av store og små bokstaver, tall og spesialtegn
- Unngå lagring av passord i sårbare formater (f.eks. LM)

Tiltak som reduserer skadefølgene av uautorisert fysisk tilgang

- Beskytt informasjon med kryptering
- Benytt klienter uten harddisker (f.eks. tynnklienter)
- Pass godt på bærbare enheter som datamaskin, mobiltelefon, nettbrett og minnepinner

Nasjonal sikkerhetsmyndighet

Telefon 67 86 40 00
post@nsm.stat.no
Postboks 14
1306 Bærum Postterminal

www.nsm.stat.no

Inntrengingstesting



Inntrengingstesting av informasjonssystemer

Hvorfor inntrengingsteste?

Hvorfor

Formålet med inntrengingstesting er først og fremst å hjelpe den enkelte virksomhet med å kartlegge svakheter for å styrke sikkerheten i sine egne informasjonssystemer.

Hvordan

Gjennom inntrengingstesting søker NSM å utprøve motstandskraften i informasjonssystemer gjennom målrettede søk, analyse og forsøksvis utnyttelse av identifiserte sårbarheter, feil og mangler. Slik kan det kontrolleres om tekniske mekanismer oppfyller gjeldende krav, og om det fremkommer andre svakheter som gjør informasjonssystemene sårbare.

Hvordan foregår en inntrengingstest?

Anmodning

Når NSM mottar en anmodning om å få gjennomført en inntrengingstest fra en virksomhet, avholdes det som regel et gjensidig informasjonsmøte. Virksomheten utsteder så en samtykkeerklæring, som formelt starter prosessen.

Planleggingsfasen

NSM utarbeider så en testplan i samarbeid med virksomheten. Planen inneholder blant annet testens omfang, avgrensninger, risikovurdering og overordnet fremgangsmåte. Planen godkjennes av virksomheten og NSM før testen iverksettes.

Sluttrapporten

I etterkant av testen utarbeider NSM en rapport til virksomheten, der testens resultater og eventuelle anbefalinger presenteres. Rapporten hjelper virksomheten med å innta en proaktiv holdning og styrke sikkerheten i sine informasjonssystemer ved å implementere sårbarhetsreducerende tiltak.



Få hjelp av NSM til å finne svakheter i dine informasjonssystemer

Spørsmål og svar omkring inntrengingstesting

Hvem kan anmode NSM om å gjennomføre inntrengingstesting?

Virksomheter underlagt sikkerhetsloven kan anmode NSM om å gjennomføre inntrengingstester i egne og underlagte virksomheters informasjonssystemer.

Vil en inntrengingstest føre til mange dyre og kompliserte krav fra NSM?

En inntrengingstest er et frivillig tilbud fra NSM, hvor NSM gir anbefalte tiltak. Det blir ikke stilt krav.

Hvem foretar inntrengingstesten?

Inntrengingstesting utføres av personell fra NSM som har høyeste sikkerhetsklarering, og som har gjennomført et omfattende opplæringsprogram med tilhørende sertifiseringer.

For mer informasjon

Kontakt pentest@nsm.stat.no