NorSIS

10 ANBEFALTE TILTAK

Regjeringen la i januar 2019 fram en ny nasjonal strategi for digital sikkerhet. Som en del av tiltaksplanen som følger strategien er det anbefalt 10 tiltak for å øke virksomheters egenevne til digital sikkerhet.

LEDELSE

Digital sikkerhet må være en del av virksomhetens IKT-systemer og tjenester. Virksomhetene bør etabler aktiviteter for sikkerhetsstyring som en del av den ordinære virksomhetsstyringen, med tydelige krav og forventninger til sikkerhet.

Tips: *Etabler tilstrekkelig systematikk for sikkerhetsstyring, og sørg for at en fagperson støtter ledelsen i arbeidet.*

RISIKOSTYRING

Etabler en prosess for risikostyring som en del av en helhetlig styringsstruktur i virksomheten. Prosessen må være kjent i virksomheten, og målet må være at de ansatte kjenner virksomhetens risikostyring, hvordan beslutninger fattes og hva som er akseptabel risiko

Tips: *Inkluder digital sikkerhet i virksomhetens risikoarbeid. Etabler tydelig ansvar og effektive rapporteringslinjer til ledelsen og styret.*

KARTLEGG VERDIER OG VERDIKJEDER

Å kjenne sin egen virksomhet er viktig for å drive effektivt og levere gode tjenester. Kartlegging av mål, leveranser og tjenester vil bidra til at viktige verdikjeder, informasjon og avhengigheter blir identifisert og vurdert.

Tips: *Lag en oversikt over virksomhetens sentrale mål, hvilke verdier og verdikjeder som inngår, hvor viktige data lagres og hvem som har tilgang til disse dataene.*

NorSIS

INKLUDER DIGITAL SIKKERHET I KULTUREN

Ansattes kunnskaper og holdninger er vesentlig for at virksomheter kan operere sikkert. Det er derfor viktig å sørge for at ansatte har nødvendig informasjon, kunnskap og ferdigheter til å opprettholde ønsket sikkerhetsnivå. En virksomhetsledelse må kommunisere mål og prioriteringer for digital sikkerhet tydelig og effektivt, og fremstå som gode rollefigurer.

Tips: *Kartlegg virksomhetens sikkerhetskultur og identifiser hva som kan forbedres. Fastsett ønsket kultur og gjennomfør tilpasset treningsprogram jevnlig for å fremme god sikkerhetskultur.*

LEVERANDØRKONTROLL

Ved kjøp av IKT-tjenester og IKT-produkter er det viktig at sikkerheten blir ivaretatt på et nivå som virksomhetens ledelse er komfortabel med. Det må stilles krav til produkter og leverandører slik at sikkerheten er ivaretatt i hele produktets eller tjenestens levetid.

Tips: *Sats på god bestillerkompetanse, og gjør en risikovurdering som forankres hos ledelsen.*

KONTROLL PÅ NETTVERK OG SYSTEMKOMPONENTER

Virksomhetens nettverk og systemkomponenter vil være utsatt for ytre og indre påvirkninger. Dette kan være skadelig programvare som kan skade maskiner og nettverk, eller planlagte endringer. Virksomheten må innføre tiltak for beskyttelse mot skadevare, overvåkning og analyse av IKT-systemet og håndtering av endringer.

Tips: *Installer sikkerhetsoppdateringer så raskt som mulig. Beskytt trådløse nettverk med sterke sikkerhetsmekanismer. Planlegg og dokumenter endringer. Skru på logging og kontroller viktige logger jevnlig.*

SIKKER KONFIGURASJON

For at ansatte skal jobbe effektivt og ha tillit til arbeidsverktøyene, må IKT-systemene kunne stoles på. Dette gjøres ved å etablere tillitsverdige systemer og tjenester, konfigurere og tilpasse maskin- og programvare og verifisere at konfigurasjonen er riktig.

Tips: *Oppgrader program- og maskinvare. Fjern unødvendig kompleksitet og ubrukt funksjonalitet. Blokker kjøring av ikke-autoriserte programmer.*

NorSIS

E-POST OG WEB-SIKKERHET

Alle virksomheter må ha kontroll på egne data og tjenester for å ivareta behov for kvalitet og sikkerhet. E-post og websikkerhet bør ha et særskilt fokus da mange av truslene fra internett kommer inn via disse kanalene. Virksomheten bør ha kontroll på informasjonsflyten som går til og fra eget nettverk, samt innad i eget nettverk. Data og tjenester må beskyttes både når det ligger lagret hos virksomheten, eller hos en tjenesteleverandør, og når data formidles over ulike informasjonskanaler som over internett.

Tips: *Bruk kun siste versjon av nettlesere. Beskytt e-post med DMARC. Krypter viktig informasjon når den lagres på bærbare medier og når den sendes over nettet.*

TILGANGSKONTROLL

Tilgangen til virksomhetens data og tjenester må kontrolleres slik at det ikke blir misbrukt av uvedkommende. Dette gjøres ved å ha kontroll på kontoer, kontrollere bruk av administrative privilegier, sørge for sikker pålogging og jevnlig gjennomgå tilgangsrettigheter. Fysisk tilgang til nettverk og informasjonssystemer, inkludert datarom, bør tilgangsstyres på lik linje med logiske tilganger.

Tips: *Endre standard passord og ikke tildel sluttbrukere administratorrettigheter. Bruk totrinnsbekreftelse, eller som et minimum sterke passord.*

HENDELSESBEREDSKAP

Alle virksomheter må være forberedt på å håndtere hendelser når dette oppstår ved å utvikle og implementere effektive prosesser for hendelseshåndtering. Dette gjøres ved å oppdage hendelser hurtig, kontrollere og fjerne hendelsesårsaken effektivt, og gjenopprette tilliten til systemer og nettverk. Prosessene inkluderer planverk, definerte roller, øving, kommunikasjon og ledelsesoversikt.

Tips: *Etabler en beredskapsplan for ulike typer hendelser og gjennomfør øvinger som tester planen.*

Les mer om den nasjonale strategien her: https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/