

Nasjonal
sikkerhetsdag

Felles løft for sikrere
informasjonshåndtering

6 steg til sikrere informasjons- håndtering



©

©

©

©

©

©

©

Nasjonal sikkerhetsdag

Felles løft for sikrere informasjonshåndtering

1 Nasjonal sikkerhetsdag

Norsk senter for informasjonssikring (NorSIS), Post- og teletilsynet og IKT-Norge arrangerer sikkerhetsdagen sammen med viktige støttespillere og aktører i bransjen. Hensikten med sikkerhetsdagen er å bevisstgjøre ansatte og ledere i små og mellomstore bedrifter om informasjonssikkerhet. På denne måten samles myndigheter, bransjen og andre aktører til felles innsats for bedre informasjonssikkerhet. Sammen ønsker vi å fordele ansvar og planlegge konkrete tiltak.

2 Gode hjelpere

NorSIS er en del av regjeringens satsning på informasjonssikkerhet. NorSIS bevisstgjør om trusler, opplyser om tiltak og påvirker til gode holdninger for små og mellomstore bedrifter. På www.norsis.no finner du over 40 praktiske veiledninger om informasjonssikkerhet for bedrifter og hver uke kan du lese flere nyheter om informasjonssikkerhet.

Nettvett.no er et nettsted hvor bedriften din finner grunnleggende informasjon og gode råd om hvordan du sikrer arbeidsplassens tilkobling og bruk av Internett. Nettvett.no er laget av Post- og teletilsynet på oppdrag fra Samferdselsdepartementet og i samarbeid med andre myndigheter, IKT-bransjen og representanter for brukerne.

3 Arrangører

Nasjonal sikkerhetsdag 2011 blir arrangert av

- Post- og teletilsynet,
- NorSIS og
- IKT-Norge.

4 tekniske tips

1. Oppdater operativsystem og programvare

Dagens operativsystem og programvare er store og komplekse, og inneholder feil. Hackeren utnytter disse feilene når de lager ondartet kode (virus og lignende) eller på andre måter ønsker å utnytte din informasjon eller datamaskin. Sørg derfor for å kjøre oppdateringer jevnlig for å unngå kjente farer. Dersom det er mulig benytt automatisk oppdatering.

2. Beskytt deg mot virus og spionprogramvare

Virus er fortsatt en stor trussel og nye virus kommer stadig. Sørg derfor for at antivirusprogrammet du bruker er oppdatert til enhver tid.

3. Installer og oppdater brannmur

Alle har i teorien tilgang til alle datamaskiner som er koplet til Internett. En brannmur er en viktig hindring for at uvedkommende ikke kan utnytte datamaskinen din. Den er et effektivt tiltak for å minimalisere hva en angriper ser på din datamaskin. Uten brannmur kan en hacker enkelt finne ut det meste om deg og dine maskiner.

4. Ta sikkerhetskopi og test at det virker

Ting går galt - vanligvis når det passer dårligst. Med en sikkerhetskopi vil gjenoppretting kunne gå raskt. Uten sikkerhetskopi vil mye informasjon være tapt for alltid.

Ta vare på dine viktigste filer. Kontroller at sikkerhetskopien inneholder de dataene du kopierte. Oppbevar gjerne sikkerhetskopien et annet sted enn hjemme - i tilfelle brann og tyveri.



5 nettvettregler

1. Tenk over hva du deler

Vær bevisst på hva du deler på sosiale medier. Husk at du alltid vil være en representant for den bedriften du jobber for i større eller mindre grad.

2. Oppgi aldri passord eller koder til noen

Passord er din nøkkel til systemer og informasjon. Pass på at uvedkommende aldri får disse.

3. Vær forsiktig ved bruk av e-post

E-post kan komme på avveie om du ikke er forsiktig. Sjekk avsenderadressen og tenk deg om før du sender konfidensiell eller viktig informasjon på e-post.

4. Vær oppmerksom på phishing og spam

Husk at er noe for godt til å være sant - så er det det!

5. Pass på bærbart utstyr

Det er lett å miste minnepinner, mobiltelefoner og bærbare PC-er. Disse inneholder ofte personlig eller konfidensiell informasjon.

6 gode rutiner

1. Sikkerhetsarbeidet må forankres hos ledelsen

For at sikkerhetsarbeidet skal bli prioritert er det vesentlig at ledelsen viser at dette er viktig for bedriften. Mange ting kan oppleves som unødvendig, og da er det viktig at lederen går foran med et godt eksempel. Sikkerhetsarbeidet må gjøres kontinuerlig og bli en naturlig del av hverdagen.

2. Vedta interne sikkerhetsregler

Det er viktig å ha klare og kommuniserte regler for informasjonssikkerhet, slik at de ansatte vet hvordan de skal forholde seg for å behandle bedriftens verdier og informasjon på en trygg og sikker måte. Det er også viktig at hensikten med reglene forklares. En uforståelig regel vil bli sett på som unyttig og vil bli omgått. Lederen bør godkjenne sikkerhetsreglene og sørge for at alle skjønner viktigheten av at de følges.

3. Kjenn din informasjon og sørg for å beskytte viktig informasjon

Informasjonen er en del av virksomhetens verdi. I dagens teknologiske hverdag lagrer vi daglig store mengder informasjon. Det kan være forretningshemmeligheter, patenter, personopplysninger, forretningsplaner, børsinformasjon osv. Enhver virksomhet bør gjøre en vurdering av hvor verdifull deres informasjon er og til enhver tid beskytte den i henhold til hvor viktig den er.





ARRANGØRER:



IKT NORGE



4. Gjennomfør risikovurdering

For å avdekke hvor man er sårbar, og for å finne de viktige og kritiske systemene, er en risikovurdering til stor hjelp. Alt sikkerhetsarbeid bør ta utgangspunkt i en gjennomført risikovurdering. En risikovurdering behøver ikke være et omfattende arbeide. Alle gjør daglig en vurdering av risiko.

5. Gjennomfør opplæring og skap gode holdninger

Informasjonssikkerhet er både teknologi, prosesser og holdninger. For å få best mulig effekt av sikkerhetstiltak er det nødvendig å lære opp de ansatte, samt å bygge opp en god sikkerhetskultur i virksomheten. Ved at de ansatte har fått opplæring har de også en forståelse av hvorfor sikkerhetstiltakene må gjennomføres.

6. Lag og øv på en beredskapsplan

Selv med mange gode sikringstiltak kan det skje uforutsette hendelser. Brann, virusangrep og uhell kan skje – og kan i verste fall få alvorlige konsekvenser. Vær derfor forberedt og tenk igjennom ulike scenarier. Dersom uhellet er ute er det viktig å komme tilbake til normalsituasjon så rask som mulig. En beredskapsplan kan hjelpe til med dette. Øv på forskjellige typer hendelser minimum en gang i året.

For flere veiledninger og råd om disse temaene, sjekk www.nettvett.no og www.norsis.no

