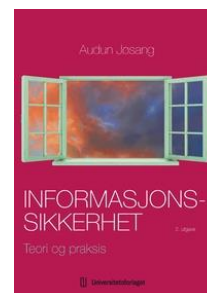




Informasjonssikkerhet: Teori og praksis
2. utgave, 2023, Audun Jøsang

Lærebok på bachelor/masternivå
Universitetsforlaget



Kapittel 1: Grunnleggende begreper for informasjonssikkerhet

- Hva er sikkerhet, informasjonssikkerhet, cybersikkerhet og digital sikkerhet?
- Kilder til krav om informasjonssikkerhet
- Trusler, sårbarheter, hendelser og risiko
- Sikkerhetsmålsettinger og sikkerhetstiltak

Kapittel 2: Angrepsvektorer og skadevare

- Angrepsvektorer
- Skadevare

Kapittel 3: Systemsikkerhet

- Systemarkitektur
- Sikkerhetsoppdatering og patching
- Privilegienivåer for prosesser i mikroprosessen
- Buffer-Overflow, utnyttelser og mottiltak
- Virtualiseringsarkitektur
- Sikker oppstart
- Sidekanaler og skjulte kanaler

Kapittel 4: Kryptografi

- Historie og utvikling av kryptografi
- Symmetriske algoritmer og hash-funksjoner
- Asymmetriske algoritmer
- Digital signatur
- Postkvantekryptografi
- Kryptografi, blokkjeder og energiforbruk

Kapittel 5: Nøkkelhåndtering og PKI

- Utfordringer ved nøkkelhåndtering
- Nøkkelhåndtering og kryptoperioder
- PKI: Infrastruktur for offentlige nøkler
- Tillitsmodeller for PKI
- Sertifikater for offentlige nøkler



Kapittel 6: Nettverkssikkerhet

- Datanett og internett: Grunnleggende nettverksarkitektur
- Kommunikasjonssikkerhet
- Sikkerhetsprotokoller og HTTPS
- VPN (Virtuelle Private Nettverk)
- Datanettsikkerhet
- Brannmurer
- Inntrengingsdeteksjon
- Nettverksarkitektur for datanettsikkerhet
- TLS-inspeksjon

Kapittel 7: Sikkerhet i trådløse nett

- Radiokommunikasjon
- Sikkerhet i wifi
- Sikkerhet i blåtann
- Sikkerhet i mobilnett

Kapittel 8: Brukerautentisering

- Metoder for brukerautentisering
- Passord
- Brikker
- Biometri
- Rammeverk for autentisering

Kapittel 9: Identitets- og tilgangshåndtering

- Silomodellen og fødererte modeller for identitetshåndtering
- Protokoller for identitets- og tilgangshåndtering, OpenIdConnect og OAuth
- Tilgangskontroll

Kapittel 10: Personvern

- Personvern i den digitale tidsalderen
- Personvernivaderende teknologier
- Blokkering av sporing
- GDPR og personopplysningsloven
- DPIA – Vurdering av personvernkonsekvens
- Varsling ved brudd på personvern
- Terminologi for personvern



Kapittel 11: Innebygd informasjonssikkerhet og personvern

- Innebygd informasjonssikkerhet
- Innebygd personvern
- De syv faser for innebygd informasjonssikkerhet og personvern
- Applikasjonssikkerhet
- Sikkerhet i skyen

Kapittel 12: Styring og ledelse og av informasjonssikkerhet

- Nivåer for styring og ledelse av informasjonssikkerhet
- ISMS – Styringssystem for informasjonssikkerhet
- Standarder og rammeverk for informasjonssikkerhet
- Modenhet i styring av informasjonssikkerhet

Kapittel 13: Sikkerhetskultur

- Bygging av sikkerhetskultur
- Innsidetrusselen og ledelsens ansvar
- Personlig integritet
- Sosial manipulering

Kapittel 14: Risikostyring for informasjonssikkerhet

- Hva er risiko og risikostyring
- Prosess for risikostyring
- Prosess for risikovurdering
- Risikoanalyse
- Risikohåndtering

Kapittel 15: Lover og regelverk for informasjonssikkerhet

- Viktigheten av regelverk om informasjonssikkerhet
- Grunnleggende begreper om regelverk
- Sentrale lover for informasjonssikkerhet

Kapittel 16: Beredskap og hendelsesrespons for informasjonssikkerhet

- Beredskapsprinsippene
- Tekniske beredskapsbegreper
- Beredskapsplanlegging
- Hendelsesrespons
- NCSC og sektorvise responsmiljøer
- Digital etterforskning

Kapittel 17: Cyberoperasjoner

- Avanserte cybertrusler
- Digital trusseletterretning
- Sikkerhetstesting av systemer, nettverk og virksomheter
- Cyberkrigføring