INFORMASJONSSIKKERHET – INNHOLD (FORELØPIG)

Lærebok på bachelor/masternivå

Tittel: *Informasjonssikkerhet: Teori og praksis*
Forfatter: *Audun Jøsang*

Kommer ut i august 2021

Kapittel 1: Grunnleggende begreper for informasjonssikkerhet

- Hva er sikkerhet, hva er informasjonssikkerhet?
- Utvikling av fagområdet for informasjonssikkerhet
- Trusler, sårbarheter, hendelser og risiko
- Sikkerhetsmålsettinger og sikkerhetstiltak
- Øvingsoppgaver om grunnleggende begreper

Kapittel 2: Systemsikkerhet

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

Kapittel 3: Kryptografi

- Historie og utvikling av kryptografi
- Symmetriske algoritmer og hash-funksjoner
- Asymmetriske algoritmer
- Digital signatur
- Postkvantekryptografi
- Anvendelser
- Øvingsoppgaver om kryptografi

Kapittel 4: Nøkkelhåndtering og PKI

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

INFORMASJONSSIKKERHET – INNHOLD (FORELØPIG)

Kapittel 5: Nettverkssikkerhet

- Grunnleggende nettverksarkitektur
- Kommunikasjonssikkerhet
- Sikkerhetsprotokoller og HTTPS
- VPN (Virtuelle Private Nettverk)
- Datanettsikkerhet
- Brannmurer
- Inntrengingsdeteksjon
- Nettverksarkitektur for datanettsikkerhet
- TLS-inspeksjon
- Øvingsoppgaver om nettverkssikkerhet

Kapittel 6: Brukerautentisering

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

Kapittel 7: Identitets- og tilgangshåndering

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

Kapittel 8: Personvern

- Hva er personopplysningsvern
- GDPR og personopplysningsloven
- DPIA – Vurdering av personvernkonsekvens
- Innebygd personvern
- Markedet for personopplysninger
- Øvingsoppgaver for personvern

Kapittel 9: Innebygd informasjonssikkerhet og personvern

- Innebygd informasjonssikkerhet
- Innebygd prsonvern
- Sikker systemutvikling
- Applikasjonssikkerhet
- Sikkerhet i skyen
- Øvingsoppgaver for innebygd informasjonssikkerhet

INFORMASJONSSIKKERHET – INNHOLD (FORELØPIG)

Kapittel 10: Styring og ledelse og av informasjonssikkerhet

- Styringsnivåer for informasjonssikkerhet
- ISMS – Ledelsessystem for informasjonssikkerhet
- Standarder og rammeverk for informasjonssikkerhet
- Modenhet i styring av informasjonssikkerhet
- Øvingsoppgaver for ledelse og styring av informasjonssikkerhet

Kapittel 11: Sikkerhetskultur

- Bygging av sikkerhetskultur
- Innsidetrusselen
- Sosial manipulering
- Sikkerhetsbrukervennlighet
- Øvingsoppgaver for ledelse og styring av informasjonssikkerhet

Kapittel 12: Risikostyring for informasjonssikkerhet

- Risikotyper
- Prosess for risikostyring
- Prosess for risikovurdering
- Risikoanalyse
- Risikohåndtering
- Øvingsoppgaver for risikostyring

Kapittel 13: Beredskap og hendelsesrespons for informasjonssikkerhet

- Beredskapsplanlegging
- Hendelsesrespons
- NCSC og sektorvise responsmiljøer
- Digital etterforskning
- Øvingsoppgaver for hendelsesrepons og beredskap

Kapittel 14: Cyberoperasjoner

- Angrepsvektorer
- Skadevare
- Avanserte trusler
- Digital trusseletterretning
- Cyberkrigføring
- Øvingsoppgaver for cyberoperasjoner