



Filoverføring mellom ulike nettverkssoner

Temaark nr 4

Versjon: 1.0

Dato: 11.05.2011

Målgruppe Dette temaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/koordinator <input type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Medarbeider/ansatt	<input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud <input type="checkbox"/> Annet, spesifiser
Ansvar	IKT-Ansvarlig		
Når	Under etablering av et informasjonssystem eller ved endringer		
Formål	Beskrive behovet for å kontrollere nettverkskommunikasjon mellom soner ved filoverføringer		
Omfang	Omfatter all nettverkskommunikasjon innenfor et informasjonssystem		
Hjemmel	Personopplysningsforskriften §§ 2-7 og 2-11		
Referanser	Veileder i sikkerhetsarkitektur: Systemteknisk sikkerhet – Sikkerhetsbarrierer Systemteknisk sikkerhet - Datakommunikasjon		

Bakgrunn

Filoverføring mellom to ulike nettverkssoner byr på en utfordring med tanke på hvor mange nettverksporter skal åpnes, hvilken vei flyter nettverkstrafikken og hvilken risiko som tas. Brukerne av informasjonssystemet bør kunne overføre filer til og fra sikre soner uten at det skaper for mye plunder og heft dersom det er behov. Normalt vil bruk av delte kataloger og åpning av tilhørende nettverksporter i sikkerhetsbarrierene være en praktisk tilnærming, men spørsmålet er da om dette gir uønsket risiko.

Et ytterligere moment er hvem som har tilgang til å overføre filer mellom soner, og hvilken risiko utgjøre det. Bør det være et begrenset antall mennesker som kan overføre filer eller skal alle kunne gjøre det? Og skal den ansatte kunne flytte filer inn og ut av sikre soner uten at filoverføringen logges for sporbarhet og revisjon?

Nr.	Aktivitet/Beskrivelse
1	<p>Filoverføring over ulike soner</p> <ul style="list-style-type: none"> Filoverføring bør styres gjennom brannmur og løsningen bør derfor stå i DMZ på sikkerhetsbarriere Antall kommunikasjonsporter i sikkerhetsbarrierer må holdes til et absolutt minimum Filoverføringen må konfigureres slik at tilgjengelige tjenester ikke øker risikoen for at personopplysninger havner på avveie eller på annen måte kompromitteres. Datakommunikasjonen må initieres fra sikre soner for å forhindre uautorisert trafikk inn i slike soner.
2	<p>Mulige metoder</p> <ul style="list-style-type: none"> Styring av kommunikasjon mellom filserver og brukere – Enveiskommunikasjon er å foretrekke. Benytte ferdige tekniske løsninger for filoverføring, som eksempelvis SSLVPN produkter Etablere løsninger med logging og autentisering av selve filoverføringen, ikke innhold, jf. personopplysningsforskriften kap. 9

Eksempel på løsning:

