ALBARAN

multisys

INFORMASJONSSIKKERHET – REISERÅD

Risiko

På reise, særlig til Asia (spesielt Kina), øst-europeiske land og Russland, er det en betydelig risiko å ha med PC, nettbrett og mobiltelefon. Årsaken er at e-tjenestene i mange land vil forsøke å ta kontroll over utstyret via Wi-Fi, Bluetooth eller ved fysisk tilgang, og installere skjult programvare som vil sette fremmede i stand til å kunne laste ned alle filer, lese all e-post, kontrollere mikrofon og kamera og trenge inn i bedriftens datasystemer når du kommer hjem. Vær oppmerksom på at også virksomheter og andre aktører kan operere på samme vis. Om du trenger PC, nettbrett, mobiltelefon o.l. på reisen, bør du følge disse rådene:

- **Bruk alltid temporært utstyr**
  Ta aldri med det utstyret du vanligvis bruker på jobb eller privat. Sørg for at bedriften din har låneutstyr som leveres inn umiddelbart når du kommer tilbake for rensing og sikker sletting av evt. skadevare
- **Unngå å ta med konfidensiell informasjon**
  Om du likevel trenger det; lagre informasjonen kryptert på et nettbrett du alltid har med deg. Men, sørg for at Wi-Fi, SIM kort eller Bluetooth aldri er aktivert på nettbrettet. Sett på fly modus. Legg aldri konfidensiell informasjon igjen på hotellet, selv ikke i låst safe.
- **Unngå å bruke nettjenestene dine som krever passord**
  F.eks. nettbanken, bedriftens nettverk, sky-tjenester og andre tjenester du bruker på nettet med passord-pålogging. Om noen har installert skadevare på PCen din vil passord og pålogging kunne stjeles.
- **Bruk en midlertidig e-post konto**
  Bruk f.eks. en g-mail konto opprettet for reisen, men send/motta aldri konfidensiell informasjon.
- **Ta aldri imot dokumenter, presentasjoner o.l. på minnepinner**
  La heller aldri noen lagre noe på dine egne minnepinner om du ikke kan stole 100% på giveren.
  Husk også at ved oppkobling mot fremviser (projektor), kan man få lastet inn uønsket programvare.
- **Vær forsiktig med kryptering.**
  I en del land er det forbudt å medbringe utstyr eller programvare for kryptering. F.eks. for kryptering av e-post, SMS eller mobiltelefonen. Krypter derfor evt. filer på forhånd.
- **Isoler temporært IT utstyr så fort du kommer hjem.**
  Sørg for at utstyret ikke kobles opp i bedriftens nettverk eller hjemme, eller at filer blir importert eller kopiert før de er sjekket med antivirus program. Bruk profesjonelle til å rense temporært utstyr før det brukes igjen.

Vurderingstabell:

Oppgaver	Behov				
	Minnep. kryptert	PC uten internett	PC med internett	Nettbrett u.internett	Mob.tlf.
Sende/motta e-post					
Konfidensielle dokumenter	*)				
Telefon/SMS					
Presentasjoner	*)				
Skrive dokumenter					
Bilder	*)				
Bruke regneark					
Tegninger	*)				
Nettsider m. passord			Aldri		Aldri

RØDT: Aldri lagre/behandle konfidensiell informasjon på dette utstyret.
GRØNT: Kan lagre/behandle konfidensiell informasjon på dette utstyret.

*) Konfidensiell informasjon på minnepinner må bare vises på PC eller nettbrett **uten** internett tilkobling.

Formål:
Forhindre tap av konfidensiell informasjon

Trusler:
Hacking. Tyveri av IT utstyr. Avlytting. Overvåking. Konkurrenter. E-tjenester.

Sårbarheter:
Usikrede nettverk og upålitelige teleoperatører. Usikre hotellrom.

Konsekvenser:
Tap av medbrakt informasjon. Potensielt tap av all informasjon vedr. viktige verdier lagret i nettverk og på servere hjemme.

Sannsynlighet:
Stor

Tiltak:
Alltid bruke temporært utstyr på reiser. Aldri lagre konfidensiell informasjon på usikret utstyr.
Aldri kommunisere konfidensiell informasjon i e-post, SMS og med mobiltelefon.