Den 14. maj 2012

Smartphones og sikkerhed

Virksomheder bør forholde sig til mobilsikkerhed.

De er ikke til at komme udenom: Smartphones. Disse såkaldte gadgets giver mulighed for at være online med mails og dokumenter hvor som helst på kloden. Til gengæld udgør de også en sikkerhedsrisiko, som mange virksomheder endnu ikke har forholdt sig til.

Smartphones er jo i ordets egentlige forstand mobile, og vi har dem med alle vegne. For mange virksomheder betyder det, at også følsomme oplysninger er med - på café, i forretninger, på besøg hos venner og så videre. Hvad sker der egentlig, hvis uheldet er ude, og medarbejderens smartphone havner i fremmede hænder?

Mens vi gør meget ud af at sikre mails og andre virksomhedsrelaterede ”dokumenter” på arbejdspladsen med blandt andet avanceret fysisk sikring, firewalls, passwords på computeren, VPN til hjemmearbejdspladsen og andre sikkerhedssystemer, er den mobile sikkerhed mange steder helt og holdent lagt i hænderne på den enkelte medarbejder.

For nogle virksomheder er risikoen og skaden ved at miste data på smartphonen minimal. For andre vil der være god fornuft i at bruge ressourcer på at sikre de mobile data. Anbefalingen vil derfor være, at man så vidt muligt får afdækket risikoen: Hvad risikerer vi, hvis uheldet er ude? Hvordan er vores virkelighed; hvor stor er risikoen? Er vi i virkeligheden de bedste til at vurdere risikoen?

Som udgangspunkt er det ikke forkert ikke at lave sikkerhedstiltag, men det er forkert ikke at have forholdt sig til risikoen.

Gode råd om mobilsikkerhed

Alle virksomheder bør forholde sig til risikoen for læk via mobiltelefoner. I det foregående afsnit blev det spørgsmål rejst, hvorvidt man selv er bedst til at vurdere risikoen for datatab, og lidt provokerende kunne en påstand være, at det er man nok ikke! Det kræver et betydeligt overblik at vurdere risici relateret til it-sikkerhed, og det gælder specielt smartphones, som i dag kan opdateres med nye programmer og apps, eksempelvis mens medarbejderne sidder i bussen på vej til arbejde. Hvem har sikret, at disse programmer ikke kompromitterer virksomhedens sikkerhed? Ingen! Hvad nu, hvis den nye opdatering til mailsystemet på telefonen forårsager en fejl? Kan programmet så erstattes af en tidligere version?

Hvis medarbejderne har adgang til at synkronisere mails med tilhørende dokumenter, kontaktpersoner, kalender og så videre til deres smartphones, bør der som det første gøre følgende:

- Udarbejd fælles sikkerhedsretningslinjer som en del af virksomhedens it-politik og informér alle medarbejdere om dem.
- Opsæt automatisk kryptering af alle data på medarbejdernes smartphones.

Visse lidt større virksomheder benytter smartphone-systemer, som er egnet til virksomhedsbrug, hvor det er muligt at centralisere styringen af sikkerheden på medarbejdernes telefoner. Disse systemer fungerer fint sammen med de fleste mailservere og smartphones. Systemerne opsættes som et forbindelsesled mellem mailserveren og mobiltelefonen og styrer således, hvordan medarbejderne må håndtere deres smartphones.

Men – før alt kommer erkendelsen! Og her er pointen, at man udarbejder en fælles politik for, hvad man må, og hvad man ikke må med smartphones. Når medarbejderne har mulighed for at installere alskens programmer fra AppStore og AndroidMarket, så gør de det. I værste fald kan disse programmer kompromittere it-driften eller it-sikkerheden med voldsomme konsekvenser til følge.

BRANDT
STATSAUTORISERET REVISIONSPARTNERSELSKAB