SikkerhedsBranchen

Vejledning om sikker e-mail jævnfør GDPR

Datatilsynet har strammet reglerne for sikring af mailkorrespondence, så både virksomheder, som offentlige myndigheder, fra 1. januar 2019 skal kryptere mails indeholdende fortrolige og følsomme personoplysninger. Du skal kunne dokumentere, at krypteringen foregår.

Baggrunden for stramningen er GDPR's krav om risikovurdering sammenholdt med, at det alt for ofte sker at store mængder følsomme personoplysninger bliver sendt ud til de forkerte. Offentlige myndigheder har faktisk skullet leve op til krav om kryptering siden 2000, men har jo henset til de mange sager ikke gjort det. Nu strammer man op og udstrækker kravet til også at omfatte alle private virksomheder. Man kan sige, at Datatilsynet i dette tilfælde overtager risikovurderingen for virksomhederne.

Hvad er omfattet

Du har kun ansvaret for de mails, der sendes fra din organisation og ud i verden. Mails internt i organisationen regnes allerede for sikret, da de aldrig forlader jeres server. Du har heller ikke ansvaret for hvordan andre svarer på mails fra jeres organisation, så du er ikke forpligtet til at tilbyde en model hvor der også kan svares krypteret.

Formuleringen "fortrolige og følsomme personoplysninger" er ikke præcist defineret fra Datatilsynet. SikkerhedsBranchen anbefaler at man tolker den som CPR-nummer og alt, der måtte være mere følsomt end det. Det kan for eksempel være:

- Konto- og lønoplysninger
- Straffeattest
- Fysiske karakteristika
- Billeder
- Helbredsmæssige og seksuelle forhold
- Genetiske og biometriske data
- Fagforeningsmæssigt tilhørsforhold
- Racemæssig og etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning

Tekniske løsninger

Som dataansvarlig skal du starte med at analysere din organisations behov for at kryptere mails. Hvis I kun meget sjældent sender særlige personoplysninger i mails er det måske nok at en enkelt afdeling eller nogle få udvalgte personer har mulighed for at

kryptere. Omvendt vil der være virksomheder, der nærmest kun udsender mails med særlige personoplysninger, og som derfor vil have glæde af en løsning, der krypterer alle mails i hele organisationen automatisk.

Der findes flere forskellige former for kryptering og en del forskellige softwareløsninger alt efter jeres behov. Nogle mailprogrammer har allerede indbygget mulighed for kryptering. Det gælder for eksempel Office 365's Outlook, som anvendes i mange danske virksomheder.

SikkerhedsBranchen anbefaler at du kontakter din it-udbyder og spørger til de muligheder, der passer bedst til dit behov og dit nuværende system. Husk i den forbindelse at du skal kunne dokumentere at du lever op til dit ansvar om kryptering.

Du kan læse meget mere om de forskellige former for kryptering og de nye krav i Datatilsynet vejledning "Transmission af personoplysninger via e-mail," som du finder her: https://www.datatilsynet.dk/emner/persondatasikkerhed/transmission-af-personoplysninger-via-e-mail/