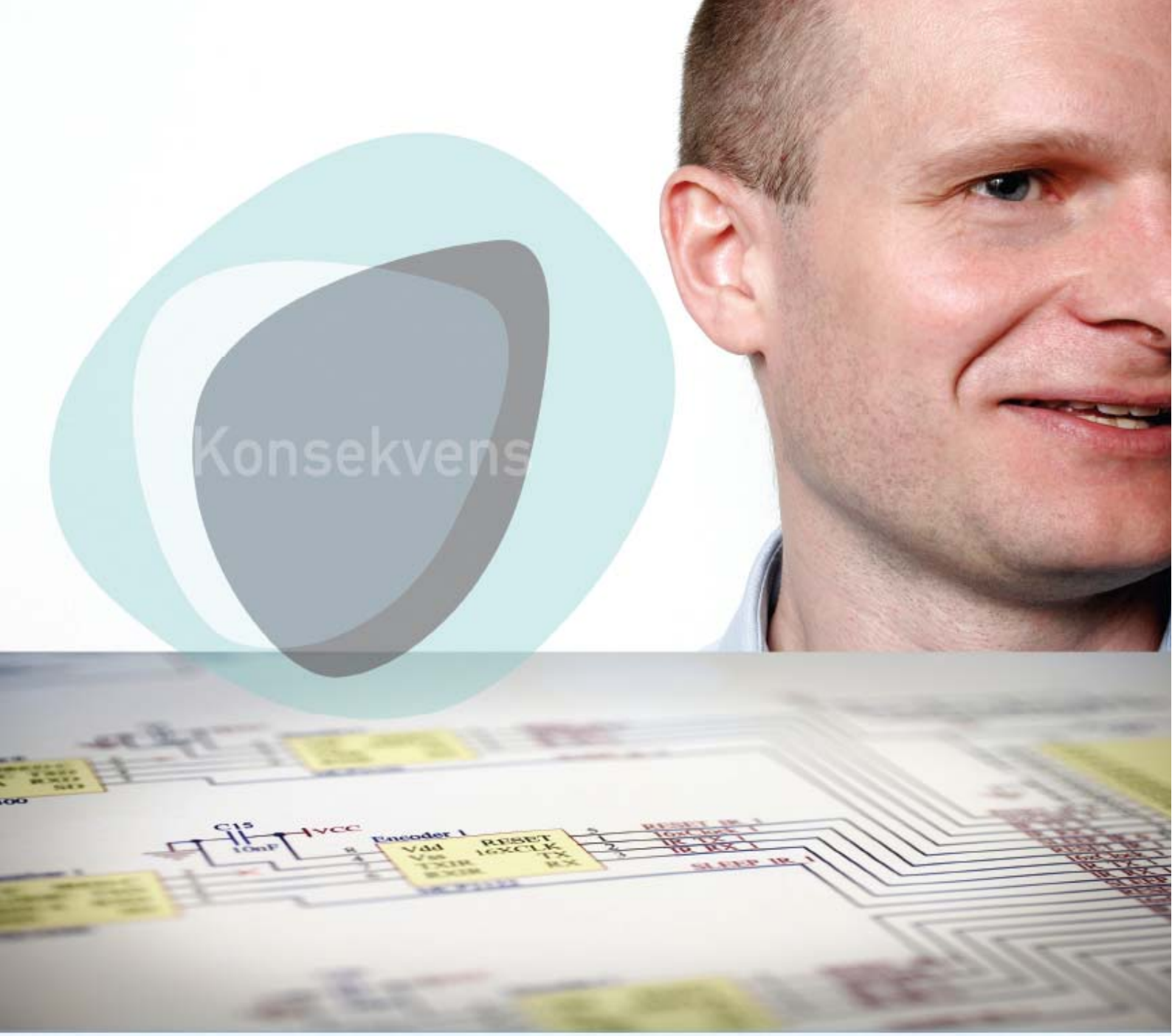


Gemmer I på skjulte data i Office-filer?

Vejledning om risici ved skjulte data i Office-filer

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

>

Gemmer I på skjulte data i Office-filer?
Vejledning om risici ved skjulte data i Office-filer

Udgivet af:
IT- & Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

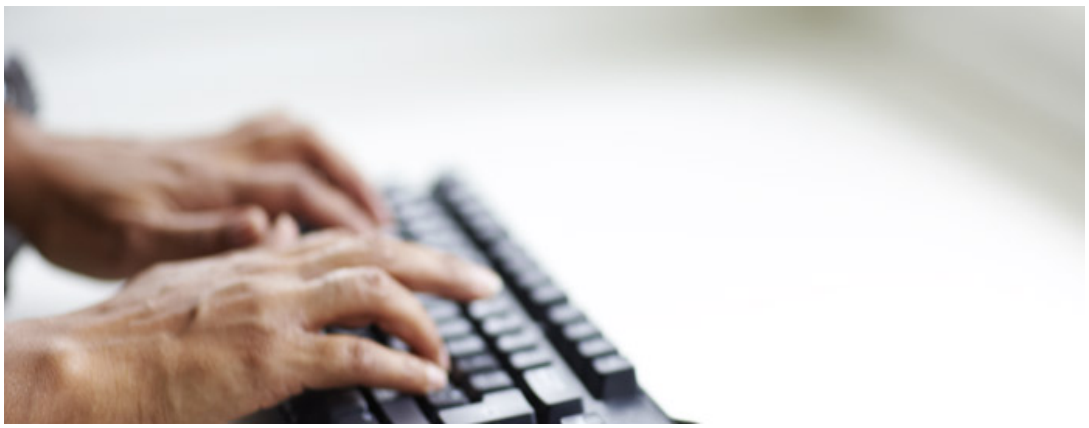
Telefon: 3545 0000
Fax: 3545 0010

Publikationen kan hentes
på It- & Telestyrelsens
Hjemmeside: http://www.itst.dk

>

Gemmer I på skjulte data i Office-filer?

Vejledning om risici ved skjulte data i Office-filer



IT- & Telestyrelsen
november 2007

Indhold >

Baggrund

>

Office-pakker tilbyder tæt dataintegration og holder eksempelvis styr på hvem, der har redigeret et dokument. Denne funktionalitet gør det enklere at anvende myndighedens information og letter arbejdet med at styre ændringer i eksempelvis regneark og dokumenter. Office-pakker er produkter som Microsoft Office, OpenOffice, IBM Lotus Smartsuite, Apple iWork og lignende.

Denne funktionalitet påfører dog også organisationen en risiko for utilsigtet eksponering, når uvedkommende får adgang til denne ekstra information. Der er tale om to typer af problemstillinger. Den ene problemstilling vedrører utilsigtet fremfindelse af metadata i Office-filer såsom forfatter, drev- og stinavne på institutionens net samt ændringer i teksten eller tekst, som er slettet. Den anden problemstilling vedrører den ekstra information, som indeholdes i såkaldte indlejrede objekter i Office-filer. Indlejrede objekter kan for eksempel vise en graf, men bagved indeholder den et komplet sæt af data, som anvendes til at danne grafen. Ved et klik på objektet vil de bagvedliggende data kunne fremfindes.

Det er ikke tale om teoretiske risici: I marts 2004 kom det eksempelvis frem, hvilke virksomheder SCO Group havde tænkt sig at sagsøge i forbindelse med en strid om softwarerettigheder. Dokumentrettelserne i Word lå skjult i den offentliggjorte fil som metadata, og kunne efterfølgende fremfindes af enhver. Problemstillingen med skjulte data er dog ikke isoleret til Office-filer. I juni 2006 kom den amerikanske televirksomhed AT&T til at offentliggøre utilsigtet information i nogle PDFdokumenter. Dette skyldes, at overstregningen i PDF kunne fjernes igen.

Ud over kompromittering af fortroligheden, kan skjult information i filer udgøre en sikkerhedsrisiko. I metadata kan der ligge drev- og stinavne til servere og printere. Denne information kan anvendes til at identificere virksomhedens it-infrastruktur og dermed være nyttig for hackere.

Denne vejledning beskriver, hvad myndigheder skal være opmærksom på i forbindelse med skjulte data, og er rettet mod myndighedens it-sikkerhedsfunktion.

Offentliggørelse af filer på hjemmesider

>

I forbindelse med offentliggørelse af filer på hjemmesider bør metadata fjernes. Dette kan eksempelvis gøres ved at konvertere dokumentet til PDF og sikre sig, at metadata er fjernet ved konverteringen. Bemærk, at konvertering til PDF ikke i sig selv er en garanti mod fjernelse af skjulte metadata. Firmaet Adobe, som tilbyder PDF, har udarbejdet en vejledning om fjernelse af metadata i PDF: http://www.adobe.com/devnet/acrobat/pdfs/Redaction.pdf.

En anden metode til at fjerne metadata fra Office-filer er at anvende et program til at fjerne skjulte data. For eksempel OpenOffice http://documentation.openoffice.org/online_help/htmlhelp/text/shared/optionen/01030300.html og Microsoft Office http://support.microsoft.com/kb/834427, der begge tilbyder et sådant program. Disse værktøjer fjerner dog ikke indlejrede objekter (OLE) i Office-filer.

Særlig opmærksomhed skal dog gives indlejrede objekter, da de typisk indeholder langt mere information end nødvendigt. En typisk fejl er, at et indlejret regneark anvendes til at vise en graf, som illustrerer bagvedliggende data i regnearket. Når det sker, kan enhver se det bagvedliggende talgrundlag for grafen ved at redigere det objekt i Office-pakken.

Gode råd ved forsendelse af filer uden for myndigheden >

Medmindre særlige hensyn taler herfor, bør metadata fjernes, inden filer sendes pr. mail uden for myndigheden.

Dette kan eksempelvis gøres ved at konvertere dokumentet til PDF og sikre sig, at metadata er fjernet ved konverteringen. Bemærk, at konvertering til PDF ikke i sig selv er en garanti mod fjernelse af skjulte metadata. Firmaet Adobe, som tilbyder PDF har udarbejdet en vejledning om fjernelse af metadata i PDF: http://www.adobe.com/devnet/acrobat/pdfs/Redaction.pdf.

En anden metode til at fjerne metadata fra Office-filer er at anvende et program til at fjerne skjulte data. For eksempel OpenOffice http://documentation.openoffice.org/online_help/htmlhelp/text/shared/optionen/01030300.html og Microsoft Office http://support.microsoft.com/kb/834427, der begge tilbyder et sådant program. Disse værktøjer fjerner dog ikke indlejrede objekter (OLE) i Office-filer.

Særlig opmærksomhed skal dog gives indlejrede objekter, da de typisk indeholder langt mere information end nødvendigt. En typisk fejl er, at et indlejret regneark anvendes til at vise en graf, som illustrerer bagvedliggende data i regnearket. Når det sker, kan enhver se det bagvedliggende talgrundlag for grafen ved at redigere det objekt i Office-pakken.

Fælles for ovennævnte metoder er, at de kræver aktiv handling af brugeren for at fjerne de skjulte data. Opmærksomheden henledes på, at netop til fjernelse af metadata i filer, som sendes pr. mail, findes der en lang række tredjepartsprodukter, som automatisk scanner mails og fjerner informationen inden forsendelse. Et eksempel på denne type produkter er http://www.payneconsulting.com/products/metadataent.

Opsummering

>

Office-filer er som udgangspunkt ikke sikre nok til udsendelse og offentliggørelse af elektroniske dokumenter. Tekstbehandlingsformater indeholder eksempelvis en række oplysninger og spor, som nemt kan opspores af læseren.

Hvis modtageren ikke skal kunne arbejde med filen, kan det sikres mod f.eks. rettelser og ændringer ved at konvertere filen til en sikret PDF-fil, før det bliver publiceret. Man skal dog i den forbindelse altid sikre, at man konverterer til en tilgængelig PDF-fil. IT- og Telestyrelsens vejledning om tilgængelighed og PDF-filer kan hentes på http://www.oio.dk/files/Tilgengelige_PDF_-_vejledning.pdf.

Hvis man følger de anvisninger, der her er angivet om de enkelte formater, samt den detaljerede procedure i den separate vejledning, kan man som organisation sikre en pålidelig elektronisk dokumentudveksling.