Kim Normann Andersen
Professor, Department of IT Management, CBS, Howitzvej 60, 2000 Frederiksberg
Tel. 3815-2437, Mobil 2479-4328, E-mail andersen@cbs.dk

18. oktober 2014

Notat vedr. Sikkerhedsproblemer i håndtering af persondata i.f.m. det offentliges digitale kommunikation med borgerne

Dette notat er udarbejdet i.f.m. høring om offentlige myndigheders behandling af persondata. Det understreges at indholdet i notatet ikke er et angreb på den digitale kommunikation, men derimod et bidrag til at få fokuseret sikkerhedsberedskabet derhen, hvor der er mest digital kommunikation og lagring af data og aktuelt mindst opmærksomhed om sikkerhedsproblemerne.

Sikkerhed i kommunikation på nettet indeholder bl.a. hensyn til autencitet af kommunikationen, kriseberedskab, risiko for hackerangreb, lagring og sporbarhed af kommunikation, legitimitet af sikkerhedsprocedurer og forudsigelighed af kommunikationen.

Myndigheder og borgere har et symmetrisk ønske om autencitet, men ikke desto mindre har vores kortlægning af digital post vist at myndighederne kan ændre i dele af dokumenterne efter de er modtaget og lagret. Vores undersøgelser har også afdækket, at borgerne ikke har sikkerhed for at de digitale henvendelser besvares ad digital vej. Jeg henviser til vores rapporter om digital post for uddybning af disse resultater.

Det ultimative krav til sikkerhedsprocedurer er fraværet af sikkerhedsbrist og forståelse af sikkerhedsprocedurerne. Jeg finder det vigtigt at understrege, at med massiv digital kommunikation fra mange personer og institutioner, er det uundgåeligt at der vil ske sikkerhedsbrist og at kommunikationen af sikkerhedsprocedurer for håndtering af persondata m.v. via nettet ikke bliver overholdt 100% af alle led og personer.

Sikkerhedsudfordringerne for den digitale kommunikation, hvor personfølsomme data kan indgå, mellem borgerne og den digitale offentlige sektor kan inddeles i tre hovedgrupper:

1. Digital post mellem offentlige organisationer og borgerne, hvor der indgår myndighedsfunktioner
2. Digital post mellem offentlige organisationer og borgerne, hvor der ikke indgår myndighedsfunktioner
3. Digital kommunikation ad andre kanaler end digital post

I min optik er sikkerhedsproblemerne store i alle tre felter, men de udspiller sig meget forskelligt og med store forskelle i trusselsniveauet.

November deadline for tilslutning til digital post er for borgernes vedkommende sat til 1. november. Det drejer sig dog kun om den kommunikation der knytter sig til gruppe 1 (digital post mellem offentlige organisationer og borgerne hvor der indgår myndighedsfunktioner). De andre typer

digital kommunikation, hvor sikkerhedsudfordringerne er større, er langt mere omfattende kommunikationskanaler og ikke omfattet af 1. november deadline.

I den første gruppe (digital post mellem offentlige organisationer og borgerne hvor der indgår myndighedsfunktioner) er risikoen knyttet til systemniveau, hvor frygten og risikoberedskabet for hackerangreb er størst og den mest umiddelbare. Det andet sikkerhedsproblem i denne gruppe er de ansattes of borgernes faktiske brug af nemID og opbevaringen af nemID koderne. Denne individuelle sikkerhedsudfordring er på linie med sikkerhedsudfordring i.f.t. opbevaring af pinkoder. Eksempelvis kunne man forestille sig at borgerne og ansatte tager billeder af nemID koderne og lagrer dette mobiltelefon eller andre medier.

I den anden gruppe (digital post mellem offentlige organisationer og borgerne hvor der ikke indgår myndighedsfunktioner) er den største sikkerhedsrisiko uforudsigeligheden i kommunikationen. Nogle offentlige myndigheder vil vælge at bruge digital post til modtagelse og forsendelse af digital post for områder hvor der ikke indgår myndighedskommunikation. Den største risiko i denne gruppe er at sikkerhedsoplæringen ikke omfatter de ansatte i denne gruppe og der er betydelig risiko for at der udvikles parallelle registre og dobbelt lagring af kommunikation på lokale og mobile enheder.

I den tredje og sidste gruppe (digital kommunikation ad andre kanaler end digital post) vil en stor del af den digitale kommunikation fra nogle kommuner og andre offentlige myndigheder fortsat ske. Aftalen om digital post pålægger ikke kommunerne at skrotte eksisterende digitale kommunikationskanaler, hvorfor kommunerne vil vælge den kanal der er billigst og bedst til den ikke-myndighedsnære kommunikation. Nogle offentlige organisationer har fravalgt og vil fortsat fravælge digital post som den foretrukne kanal da denne er dyrere og mere besværlig end andre, eksisterende digitale kanaler. Borgerne og det offentlige vil derfor skulle håndtere flere digitale kommunikationsveje. Sikkerhed i den tredje gruppe har stort set ingen opmærksomhed i den offentlige debat, selv om det er her langt den største digitale kommunikation sker. Det gælder eksempelvis kommunikationen mellem elever, forældre og skolerne, hvor nemID er en mulighed, men ikke obligatorisk.

Ud fra hensynet til pris og kvalitet kommer digital post ikke ind som første valget i alle offentlige organisationer. Derfor kan sikkerhedsproblemerne totalt set være forøget med introduktionen af digital post. De eksisterende kanaler og de sikkerhedsproblemer, der knytter sig til dem vil fortsat være der, men vil være genstand for mindre opmærksomhed. Der kommer hertil en ny, og mere systemisk sikkerhedstrussel ind for digital post og nemID, hvor hackerangreb og usikkerhed om hvilke andre kanaler man skal bruge når digital post ikke fungerer trænger sig mest på.