Privatlivsfremmende teknologier (PETs)

Appendiks 7
Håndbog i:
Privatlivsimplikationsanalyse

IT- og Telestyrelsen

INDHOLDSFORTEGNELSE

PRIVATLIVSFREMMENDE TEKNOLOGIER

Siden midten af 1990erne er der udviklet en række teknologier, der skal tjene som hjælp for beskyttelsen af privatlivet og ikke virke som en trussel herfor. Det almindeligt anvendte udtryk i denne forbindelse er privacy-enhancing technologies (PETs), dvs. privalivsfremmende eller -forbedrende teknologier. PETs kan hjælpe til med at reducere virkningerne af privacy-invasive technologies (PITs), dvs. privacy-krænkende teknologier. Dette afsnit giver baggrundsinformation om PETs.

Der gennemgås tre kategorier af PETs:

1. Midler til at imødegå privatlivskrænkende teknologier.
2. PETs med anonymitet - midler til at tilvejebringe ægte, usporlig anonymitet.
3. PETs med pseudonymitet - midler til at tilvejebringe stærkt beskyttet pseudonymitet.

Midler til imødegåelse af privatlivskrænkende teknologier

Mange teknologianvendelser indsamler data, sammenholder data, anvender data eller medvirker på anden måde ved overvågning af mennesker og deres adfærd (PITs). Blandt en mængde eksempler kan nævnes overvågningsteknologier (som f.eks. CCTV), registrering af dataspor (som f.eks. overvågning af tasteanslag) og identifikation gennem nægtelse af anonymitet (f.eks. ID på kaldende telefonabonnenter, loyalitetskort og intelligente transportsystemer), data warehousing *(dataopbevaring)* og datamining *(dataopsøgning)* og anvendelse af biometriske oplysninger. I internet-sammenhæng er der ikke så lidt bekymring over de forskellige typer af malware, herunder virus, orme, trojanske heste, keystroke-loggere, 'spyware' og 'phishing'.

Nogle PETs er designet til at modvirke effekten af PITs. Eksempler herpå er spamfiltre, cookie-managers, password managers, personlige firewalls, software til virusbeskyttelse, SSL/TLS *(sikkerhedsprotokoller)* til kanalkryptering og spyware-sweepers. Andre avancerede PET-tjenester viser brugeren af browseren oplysninger om ejeren af en IP-adresse, før de opretter forbindelse. Desuden overvåger de ankommende trafik for mønstre, der indikerer malware og hacking, og overvåger afgående trafik for spyware-relateret transmission.

I nogle projekter kan det være hensigtsmæssigt for virksomhederne at yde rådgivning til deres brugere for at hjælpe disse til at beskytte sig mod malware og for at beskytte deres autentifikatorer (f.eks. kodeord). Der kan være fordele ved at gå endnu længere og tilbyde hjælp til brugerne på områder som f.eks. installation og konfiguration af software, herunder web-browsere, firewalls, antivirus og anti-spyware pakker.

Ved at indarbejde PETs effektivt i et koncept kan man med en ringe stigning i omkostninger reducere presset på privatlivsbeskyttelsen, som hidrører fra programmål eller effektivitetskrav.

PETs med anonymitet

Den første kategori af PETs, som beskrives ovenfor, gør kun lidt i retning af at stoppe akkumuleringen af persondata. Men kan man anvende en anden fremgangsmåde, der går ud på at udelukke personlig identitet ved at sørge for anonymitet. Eksempler herpå er bl.a. anonyme ('Mixmaster') remailers *(genpostere)* og websurfing-systemer samt anonyme mekanismer til e-betaling. (Dog skal man være opmærksom på, at nogle remailers og betalingsmekanismer er betegnet som 'anonyme', selv om de ikke er det, idet det er muligt at spore transaktionerne til de mennesker, som har foretaget dem).

Der er mange omstændigheder, hvorunder virksomhederne kan og bør tillade anonym kommunikation. Eksempler herpå er generelle forespørgsler og levering af generaliserede (i modsætning til personspecifikke) oplysninger.

På den anden side gælder, at mange af virksomhedens centrale forretningsprocesser ikke kan gennemføres med anonyme brugere. Grundene hertil er bl.a., at man ikke er i stand til at forhindre svindel, at der er risiko for uønsket adgang til persondata, og at der er behov for, at visse arter af transaktioner fastholdes og checkes med en persons registreringer.

PETs med pseudonymitet

Med anonymitet forhindres en virksomhed i at kunne identificere den person, som man har med at gøre. Pseudonymitet betegner en situation, hvor personens identitet ikke er åbenbar, men under visse omstændigheder kan afsløres.

Ægte anonymitet har den ulempe, at den kan bruges til at undgå opdagelse af kriminel aktivitet. De fleste mennesker vil være indstillet på at anvende pseudonymitet i stedet for, som en mere afbalanceret form for beskyttelse af beskyttelsen af privatlivet. De kan dog behøve forvisning om, at deres identitet ikke vil blive afsløret uden retmæssig grund.

En pseudonym transaktion er en transaktion, der ikke normalt kan forbindes med en bestemt privatperson. En transaktion er således pseudonym i relation til en privatperson, hvis transaktionsdataene ikke indeholder nogen direkte identifikator for vedkommende person, og kun kan relateres til denne, såfremt der tilknyttes specifikke supplerende data.

For at være effektive skal pseudonyme mekanismer indbefatte juridiske, organisatoriske og tekniske beskyttelsestiltag for at sikre, at forbindelsen mellem

en transaktion og en identificérbar privatperson kun kan knyttes under de rette omstændigheder. Eksempler på relevante teknikker er:

- Anvend 'pseudonymer', og sørg for, at koblingen mellem en personlig identifikator og den person, som anvender den, kun registreres af en 'betroet tredjepart'.
- Undgå at indsamle identifikatorer, og anvend i stedet en af følgende teknikker til risikostyring:
    - sørg for at betaling er modtaget, før de pågældende varer eller tjenesteydelser leveres (dermed autentificeres på grundlag af værdi i stedet for identitet),
    - check en persons kvalifikation eller et relevant karaktertræk hos personen som f.eks. alder, handicap eller uddannelsesmæssig baggrund (også betegnet som attributautentificering, i modsætning til identitetsautentificering).

Pseudonyme teknikker kan resultere i innovative måder, hvorpå man kan behandle grundlæggende problemstillinger i systemdesignet, mens personoplysninger beskyttes. Med sådanne teknologier kan man opnå en sikker identifikation og netopkobling, således at svindel og tab ved tyveri begrænses, og teknologierne muliggør også sikre betalingssystemer, således at de administrative omkostninger ved kontanter undgås, samtidig med at de tillader en høj grad af brugeranonymitet og beskyttelse af privatlivet. Omkostningsbesparelser og beskyttelse af privatlivet behøver ikke at være modsat rettede værdier.