

Privacy som arkitekturprincip

IT-sikkerhed, fx som formuleret i DS484 eller ISO 17799 / ISO 27001, varetager først og fremmest dataejerens interesse. Ved [privacy](#) varetages derimod interessen for det enkelte individ, som informationen vedrører. Privatlivets fred udgør en af samfundets grundlæggende værdier, men der er mange forskellige meninger om, hvor grænsen går, når privatlivet skal beskyttes. Forskellige personer har forskellig opfattelse af begrebet privatliv, og ofte afvejes beskyttelsen af private informationer i forhold til andre behov, som fx sikring af transaktioner eller bekæmpelse af kriminalitet.

Privacy som forretningsparameter

Behovet for privacy beskyttelse i forbindelse med brug af elektroniske tjenester har i en årrække haft en begrænset opmærksomhed hos den almindelige forbruger, men nu er udviklingen vendt: Stigningen i it-baseret kriminalitet som fx identitetstyveri og spam har gjort det tydeligt, at beskyttelse af private informationer spiller en væsentlig rolle for individets sikkerhed og integritet, og forbrugerne ser i større grad på, om deres personlige informationer er i fare.

Principper for privacy

Dansk Industris Privacy Taskforce, som omfatter repræsentanter for Forbrugerrådet, Finansrådet, Institut for Menneskerettigheder, Digital Rights og en række af industriens specialister har udgivet notatet [Principper for privacy](#), som sætter scenen for den vigtige debat om privacy i Danmark.

Forbrugernes ønske om en nem og sikker privacy beskyttelse skaber et stærkt behov for tjenester, hvor privacy-hensynet kan varetages, uden at sætte funktionalitet eller sikkerhed over styr.

Læs mere om dette emne på www.zebranet.dk

Allan Bo Rasmussen
Direktør



Ved markedsføring af nye digitale servicetilbud er der således kommet fokus på løsningernes evne til at give kunderne en personlig service uden at kompromittere deres integritet. Kunderne forventer, at en seriøs serviceleverandør medvirker til at beskytte kundens privacy. Det betyder i praksis, at leverandøren ved enhver transaktion skal minimere sit behov for personlige oplysninger om kunden, og behandle de afgivne informationer på en sådan måde, at kunden er beskyttet mod krænkelse og kriminalitet.

Et grundlæggende brugerkrav til alle privacy-relaterede løsninger er, at de foruden at give sikkerhed og tryghed, samtidig skal være nemme at anvende, både konceptuelt og praktisk. Det betyder fx, at fordelene ved at anvende privacy løsningen skal være attraktive, og at anvendelsen ikke må være forbundet med ulemper eller udgifter, som får brugeren til at fravælge beskyttelsen.

Privacy-aware design

Der lanceres i disse år en lang række teknologier, som åbner mulighed for nye innovative tjenester, men som også kan true brugerens privacy, hvis ikke anvendelsesscenariet og de bagved liggende systemer og registre designes med privacy for øje. Vi behøver blot at tænke på biometri, RFID og positionsbestemmelse med GSM og GPS.

Samtidig oplever vi et stigende udbud af teknologiske produkter, der kan tilføje privacy-beskyttelse til eksisterende it-løsninger, eller hjælpe forbrugeren til at "forsvare" sig mod systemer, der ikke formodes at opfylde hans forventninger til privacy-beskyttelse.

Når disse byggesten skal sammensættes til produkter og tjenester, som kan vinde bred accept blandt forbrugerne, møder designerne ofte de klassiske barrierer i et umodent marked: Privacy begreberne er endnu ikke afklaret hos den almindelige forbruger - og slet ikke rodfæstet i den gængse it-praksis. En vigtig forudsætning for design af gode privacy-løsninger er fx at have en accepteret referenceramme for beskrivelsen af privacy behov i forskellige situationer og kulturelle sammenhænge.

Arkitektur for privacy

Privacy-området har hidtil været et fragmenteret marked, præget af inkompatible løsninger med ringe brugervenlighed. Gennem samarbejde mellem industri og forskningsmiljøer kan der etableres et fælles grundlag for udviklingen, som skaber konvergens i løsningerne, og gør det nemmere for systemejerne at opfylde kravet om privatlivsbeskyttelse.

Der er brug for en overordnet arkitektur for privacy, som tager udgangspunkt i samfundets og individets behov, og organiserer begreber, teknologier og komponenter, som baggrund for udvikling af privacy relaterede produkter og tjenester. Arkitekturen skal fx definere rammer for anvendelsen af nye teknologier som fx anonymisering, sletning og biometri, så de kan understøtte opfyldelsen af komplekse markedskrav til fremtidens IKT-løsninger.