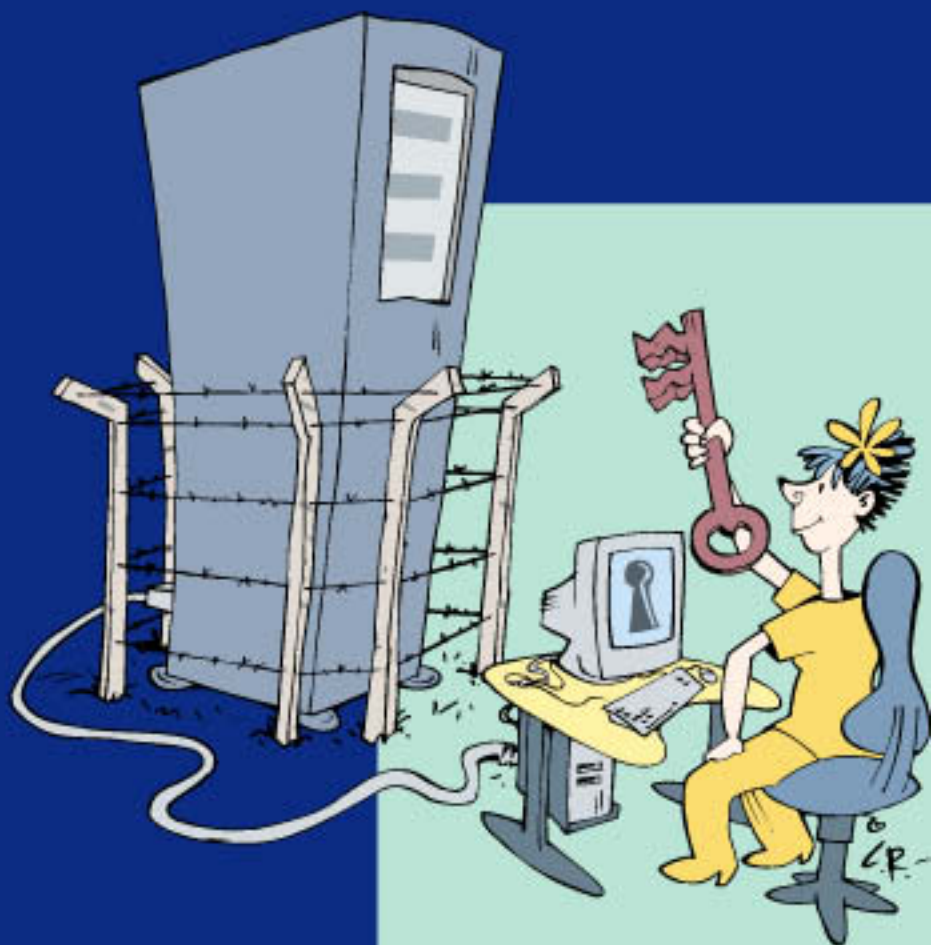


Adgangskontrol til en hjemmeside

En vejledning for tjenesteudbydere



Adgangskontrol til en hjemmeside

- en vejledning for tjenesteudbydere

IT-Sikkerhedsrådet
August 2001

Adgangskontrol til en hjemmeside

- en vejledning for tjenesteudbydere

Publikationen kan købes ved
henvendelse til:
Statens Information
Postboks 1300
2300 København S
Tlf. 3337 9228
Fax 3337 9280
E-post sp@si.dk
Pris ved løssalg 50,- kroner inkl. moms

Publikationen kan også hentes på
IT- og Forskningsministeriets hjemmeside
<http://www.fsk.dk>
ISBN (Internet): 87-90890-64-7

Udgivet af:
IT-Sikkerhedsrådet
c/o IT- og Forskningsministeriet
Bredgade 43
1260 København K
Tlf. 3392 9700
Fax 3332 3501
E-post fsk@fsk.dk

Tryk: K. Larsen & Søn A/S
Oplag: 1.500
ISBN: 87-90890-63-9

Forsideillustration:
Lars Refn

INDHOLD

| | |
|----|--|
| 5 | Forord |
| 7 | Baggrund og indhold |
| 7 | Problemstilling |
| 11 | Formål og målgruppe |
| 12 | Indhold |
| 13 | Adgangskontrol |
| 15 | Trusler |
| 18 | Konsekvenser |
| 23 | Brugerautentificering |
| 27 | Valg af brugerautentificering |
| 27 | Tjenester med få og beskedne konsekvenser |
| 28 | Tjenester med alvorlige konsekvenser |
| 33 | Tjenester med vitale konsekvenser |
| 35 | Bilag 1 Bidragydere |
| 37 | Bilag 2 Forskrifter om adgangskontrol |
| 47 | Bilag 3 Forkortelser og begreber |

FORORD

Når virksomheder og myndigheder udbyder informationstjenester fra en hjemmeside eller i øvrigt etablerer selvbetjeningssystemer via nettet, opstår behovet for at kunne foretage en sikker adgangskontrol for personer, der reserveres adgang til disse tjenester og systemer.

Ofte sikres denne adgangskontrol ved, at brugeren indtaster et password. Alt efter hvordan man vælger og omgås sit password kan en sådan metode være tilstrækkelig. Men ofte vil det være nødvendigt at anvende mere sikre former for adgangskontrol.

Med denne vejledning sætter IT-Sikkerhedsrådet fokus på disse problemer. Vejledningen skitserer, hvad der bør tages hensyn til ved udformning af adgangskontrol, og beskriver en række autentificeringsmetoder, trusler og sårbarheder ved de forskellige metoder.

IT-Sikkerhedsrådet håber, at vejledningens anbefalinger vil være til hjælp for virksomheder og offentlige myndigheder, der står over for at etablere adgangskontrol til hjemmesider og andre informationstjenester.

IT-Sikkerhedsrådet har udarbejdet vejledningen under medvirken af konsulentfirmaet PLS Rambøll Management.

København i august 2001
Mads Bryde Andersen
Professor, dr.jur.
Formand for IT-Sikkerhedsrådet

1 BAGGRUND OG INDHOLD

1.1 Problemstilling

Den stigende anvendelse af internettet har ført til et udbud af mange tjenester fra en hjemmeside, som har en eller anden form for adgangskontrol. Der er i sagens natur en meget stor variation i disse tjenester, for eksempel adgang til e-mails, adgang til informationer, indkøb af varer, bankforretninger, ændring af selvangivelse og indberetning af elforbrug.

Inden for den offentlige sektor arbejdes på mange fronter for at udbyde selvbetjening til borgerne fra myndighedernes hjemmesider. I de tilfælde, hvor der er ikke er særlige lovkrav om skriftlighed og underskrift, vil en adgangskontrol kunne erstatte en elektronisk signatur på en web-blanket eller e-mail fra borgeren. Men det vil selvsagt forudsætte at adgangskontrollen giver en tilstrækkelig sikkerhed.

Det kan konstateres, at der anvendes forskellige former for adgangskontrol, men typisk anvendes en adgangskontrol, hvor brugeren skal indtaste et password for at få adgang til tjenesten. Denne velkendte fremgangsmåde har en række sårbarheder. Sårbarheder som må føre til, at det nærmere overvejes, om denne sikkerhedsmekanisme er tilstrækkelig sikker eller andre mere sikre former for adgangskontrol bør anvendes.

Eksempler

Told & Skats tilbud om ændring af selvangivelse og forskudsregistrering er uden tvivl den mest anvendte selvbetjening på internettet i dag. Cirka 277.000 benyttede internettet til at ændre deres selvangivelse for 2000 og 137.000 til at ændre forskudsregistrering for 2001.

Når borgerne får mulighed for at ændre selvangivelse og forskudsregistrering er det nødvendigt at sikre, at kun rette vedkommende kan foretage disse ændringer. Der er derfor etableret en adgangskontrol.



The screenshot shows a web browser window with the title "Told- og Skat: TastSelv - Microsoft Internet Explorer leveret af Forskningsnetværket". The address bar shows "https://www.skat.dk/portal/2008/PersonAdgang08.htm". The page content includes the heading "Selvangivelse og årsopgørelse for 2000" and a section titled "Adgangskontrol".

Adgangskontrol

Alle oplysninger, som De sender eller modtager, er krypteret med stærk kryptering under transporten.

De skal oplyse personnummer og Tast-Selv-kode for enten

- at godkænde eller ændre den afsluttede selvangivelse eller
- at indtaste den udfærdigede selvangivelse eller
- at se resultatet af årsopgørelsen

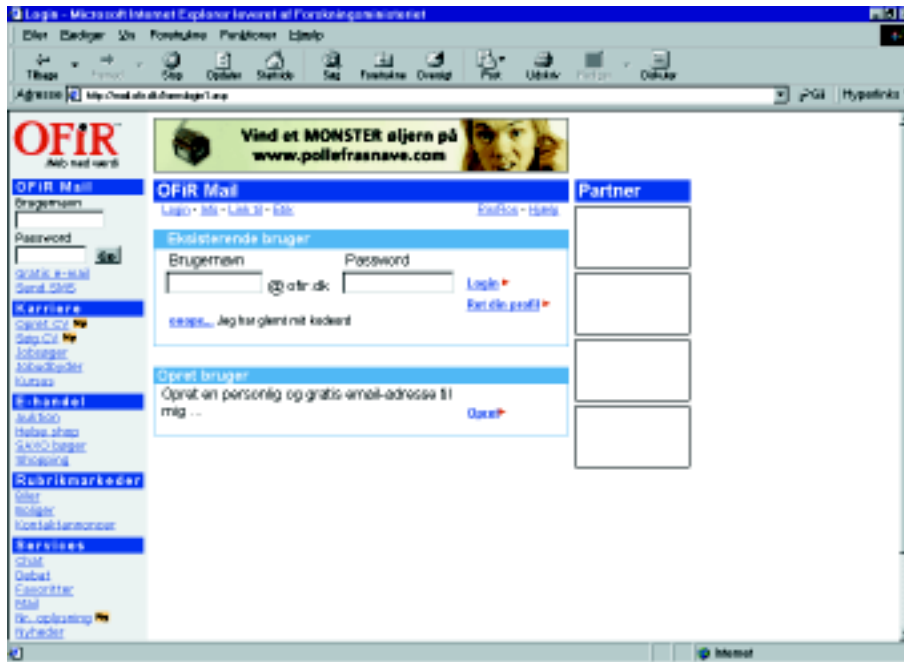
Det er kun Tast-Selv-koden fra selvangivelsen for 2000, der kan benyttes. Ved mere end 5 fejlagtige adgangsforsøg, lukkes der for yderligere forsøg.

Personnummer

Tast-Selv-kode

Borgeren skal indtaste sit personnummer og en Tast-selv-kode. Personnummeret fungerer som bruger-id og Tast-selv-koden som password. Tast-selv-koden sendes til alle borgere trykt på selvangivelsen/ forskudsopgørelsen, og den fornyes ved hver udsendelse.

Et andet eksempel på anvendelse af brugernavn og password er adgang til en gratis e-mail tjeneste:



Brugeren skal indtaste sit brugernavn, som samtidig anvendes som adresse på vedkommendes e-mail kontor, og et selvvalgt password.

Et tredje eksempel er anvendelse af en standard funktionalitet på Internettet, som giver mulighed for at bede brugeren om at gennemføre en adgangskontrol før han får adgang til et dokument. Når brugeren indtaster adressen på et dokument som kræver adgangskontrol får han nedenstående vindue, som her er hentet fra et intranet, som giver adgang til firmaets økonomidata.



Brugeren skal indtaste brugernavn og et password, som returneres til web-serveren.



Ved den indledende adgang til en internetbank bliver brugeren, ud over en adgangskode bedt om at indtaste en „underskriftskode“.

Efterfølgende kan et program på brugerens pc eksempelvis beregne en digital signatur på de øvrige login informationer, som sendes til internetbanken.

1.2 Formål og målgruppe

IT-Sikkerhedsrådet har i denne vejledning sat fokus på adgangskontrol til en hjemmeside. Vejledningen skal ses som en naturlig fortsættelse af rådets øvrige udredninger og vejledninger rettet mod internettet:

- Privatliv på internet
- Praktisk brug af kryptering og digital signatur
- Sikkerhed ved e-post og internet
- Udredning om internet sårbarhed.

Formålet med denne vejledning er at fremlægge en række anbefalinger og overvejelser på baggrund af den aktuelle udformning af adgangskontrol på internettet og de muligheder almindeligt udbredte protokoller og produkter giver. Vejledningen fokuserer på valg af brugerautentificering og kan danne grundlag for udformning af en sikkerhedspolitik for adgangskontrol. Det er således ikke meningen at give en teknisk beskrivelse af forskellige løsninger, og tekniske beskrivelser indgår kun i det omfang de skønnes nødvendige for at give et billede af, hvordan man kan håndtere forskellige adgangskontrolproblemer. Det er i den forbindelse vigtigt at understrege, at vejledningen ikke foreskriver bestemte fremgangsmåder eller produkter for en adgangskontrol.

Som det gælder for andre former for IT-sikkerhedspolitik er beslutningen om at udforme adgangskontrollen til virksomhedens systemer - hvad enten disse opererer i et lukket kredsløb eller via et åbent kommunikationsnet som internet - en del af den samlede sikkerhedspolitik. Det er et ledelsesansvar, at der udformes en sikkerhedspolitik for tjenesten, som

beskriver de fælles kontroller og sikringsforanstaltninger. Det er IT-Sikkerhedsrådets håb, at vejledningen vil tjene til inspiration for den enkelte tjenesteudbyder i udformningen af sin egen adgangskontrol til tjenester og selvbetjening fra en hjemmeside.

Vejledningens målgruppe er tjenesteudbydere - såvel offentlige som private - som ønsker at stille en tjeneste til rådighed fra en hjemmeside, hvor det vurderes ønskeligt eller ligefrem er påkrævet efter lovgivningen, at der etableres en adgangskontrol.

1.3 Indhold

Kapitel 2 giver en generel baggrund for at udforme en adgangskontrol. Kapitlet refererer en række rapporterede angreb, som udgør trusler mod adgangskontrollen. Videre findes, som bidrag til en risikovurdering, en opdeling af tjenester på hjemmesider på baggrund af konsekvenser ved misbrug.

I vejledningens *kapitel 3* defineres brugerautentificering og tre typer for autentificering - password, token med engangskode og certifikat-baseret autentificering - beskrives.

I det afsluttende *kapitel 4* fremlægges IT-Sikkerhedsrådets overvejelser og anbefalinger til valg af brugerautentificering.

2 ADGANGSKONTROL

Adgangskontrol omfatter de sikkerhedsmekanismer, som er nødvendige for at imødegå, at uvedkommende kan misbruge den udbudte tjeneste. Brugerautentificering, som der er vist eksempler på ovenfor, er blot et element heri.

Grundlaget for udformningen af adgangskontrollen er en risikovurdering af tjenesten. Adgangskontrollen skal give en passende sikkerhed i forhold til de trusler, som er kendt eller i øvrigt kan tænkes, og de konsekvenser for tjenesteudbyderen der vil være ved misbrug.

I næste afsnit beskrives først en række trusler og i det efterfølgende afsnit foretages opdeling af tjenester på en hjemmeside på baggrund af hvor alvorlige konsekvenser et misbrug vil have.

Ved udformningen af en adgangskontrol skal udbyder af tjenesten mindst tage stilling til:

- Valg af brugerautentificering (som behandles i de følgende kapitler).
- Arbejdsgange ved oprettelse af brugere, samt for nedlæggelse af brugere.
- Procedure for udlevering af erstatningsadgangskode til brugere, som har glemt eller mistet denne.
- Procedure når en adgangskode kompromitteres.
- Sikring af autentificeringsoplysninger, herunder regler for medarbejderes adgang til at se og opdatere autentificeringsoplysninger.
- Fremgangsmåde ved eventuel etablering af en session, mens brugeren benytter tjenesten.

- Vurdering af om der er behov for kryptering af data under data-transmissionen.
- Tidsbegrænsning for en brugers forbindelse til tjenesten.
- Ansvar og procedurer for sikring af web-server og bagvedliggende IT-systemer mod angreb.
- Behov for logning af brugernes anvendelse af tjenesten.
- Information til brugerne om deres rolle i sikkerheden, for eksempel om anvendelse og beskyttelse af adgangskode.

Når man etablerer en tjeneste fra en hjemmeside, som giver brugeren adgang til at disponere, bliver brugeren og dennes IT-udstyr afgørende for den samlede sikkerhed. Derfor er det vigtigt at definere brugerens rolle i den samlede IT-sikkerhedspolitik.

Et særligt spørgsmål i den forbindelse er brugerens retsstilling i de tilfælde, hvor der sker uberettiget brug af en tjeneste, der eksklusivt er forbeholdt brugeren. Hvis tjenesten muliggør et forbrug, som brugeren betaler for, vil den adgangskontrolforanstaltning, der understøtter dette, i juridisk forstand blive betragtet som et betalingsmiddel i henhold til lov om visse betalingsmidler. Dette betyder blandt andet, at de særlige regler om hæftelse for uberettiget brug i lovens § 11, finder anvendelse for brugeren. Men også selv om man befinder sig uden for denne lov, kan der opstå vanskelige juridiske spørgsmål om, hvorvidt den legitimerede bruger i juridisk forstand „hæfter“ for uberettiget brug af tjenesten. Dette kan for eksempel tænkes, når en tredjemand uberettiget gør brug af tjenesten i brugerens navn. Disse spørgsmål kan ikke (alene) løses i IT-sikkerhedspolitikken, men må i givet fald afklares ved en aftale mellem brugeren og tjenesteleverandøren.

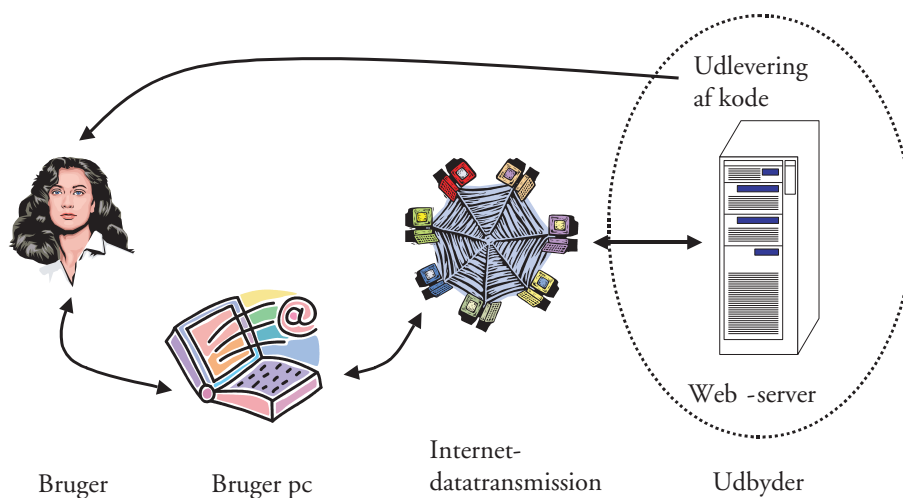
Ikke mindst i lyset af de vanskelige juridiske spørgsmål, der kan opstå ved uberettiget brug af adgangskoder med videre, bør tjenesteudbyderen søge at tilrettelægge tjenesten på en sådan måde, at fejl og uregelmæssig-

heder opdages og korrigeres, før de påfører brugeren uoprettelige skader. I den forbindelse er det vigtigt, at tjenesteudbyderen på en forståelig og klar måde informerer brugeren om de retlige risici herved - herunder for at uønskede forpligtelser kan gøres gældende mod brugeren - og om brugerens eget ansvar for at reducere disse risici.

2.1 Trusler

I det følgende omtales en række trusler fra kendte angreb. Listen er ikke udtømmende og kan derfor ikke anvendes som checkliste for sikring af en tjeneste, men er alene tænkt som et bidrag til en samlet risikoanalyse.

Fremgangsmåden for autentificering er kun en del af den samlede adgangskontrol. Da adgangskontrollen foregår over Internettet i et åbent miljø, er det nødvendigt at se på hele kommunikationen, som kan illustreres således:



I hvert af de fire led er der behov for sikkerhedsforanstaltninger for at opnå en sikker adgangskontrol.

Brugeren skal opbevare og anvende adgangskoden på en sådan måde, at sikkerheden i adgangskontrollen ikke kompromitteres. Her må hele

forløbet af adgangskontrollen inddrages, det vil sige udlevering af adgangskode med videre, anvendelse af adgangskode samt ændring/udløb af adgangskode. *Brugerens pc* kræver beskyttelse, da den vil indeholde programmer og data, som indgår i autentificeringen. Data skal *transmitteres over internettet*, og risikoen for, at de kan komme til uvedkommendes kendskab, må indgå i udformningen af adgangskontrollen. Hos *udbyderen* må der etableres sikkerhed for, at en indtrænger ikke kan få adgang til oplysninger hverken fra web-server eller fra udbyderens IT-systemer gennem angreb på denne.

Brugeren

Et password kan gøres tilgængelig for en angriber ved uforsigtighed, idet det skrives ned eller opbevares på pc'en. Passwords kan også franarres en bruger ved „social engineering“, hvor en angriber ved henvendelse til brugeren for eksempel giver sig ud for administrator eller revisor, som skal have oplyst password.

Brugere kan blive narret til at tro, at de befinder sig på en web-side, hvor de skal oplyse brugernavn og password, men som i virkeligheden er en maskeret web-side, som er oprettet for at indsamle login data.

PC - klient

En pc i hjemmet har typisk ikke en adgangskontrol, og andre brugere af pc'en kan derfor læse web-sider fra tjenesten eller anvende en adgangskontrol som er lagret på pc'en.

En indtrænger kan anbringe et program - en såkaldt trojansk hest - på brugerens pc. Programmet kan for eksempel sendes med en e-mail under falsk påskud, som får brugeren til uden at vide det at installere programmet. Kendte eksempler på sådanne programmer er Back Orifice og Netbus. Programmet sender besked til indtrængerens, når brugeren anvender internettet, og indtrængerens får her mulighed for at kommunikere med

pc'en. Programmet giver for eksempel en indtrænger mulighed for at opsnappe brugernavn og password. En anden metode til at understøtte retsstridig indtrænger består i at anbringe en Keystroke Recorder, som aflæser det enkelte tastetryk på pc'ens tastatur og dermed kan opsnappe såvel brugernavn som password.

I nogle tilfælde opbevares login data i en cookie på brugerens pc, og der er rapporteret om angreb, hvor en web-server uberettiget kan få sendt en cookie fra en anden server.

Internet - datatransmission

Der er udviklet Packet Sniffer programmer, som kan kopiere datapakker fra transmissionen over internettet. Programmet kan således opsnappe datapakker, som indeholder brugernavn og password. En række sniffer programmer kan frit downloades fra internettet.

Selv om både brugernavn og password er krypteret og derfor ikke kan læses, kan det alligevel være værdifuldt for en angriber at skaffe sig disse data. Hvis angriberen kan fastslå, at der er tale om login data, kan de krypterede data anvendes til et såkaldt replay angreb, hvor dataene kan sendes igen, og angriberen kan dermed i visse tilfælde få adgang på den oprindelige brugers vegne.

Informationer, der sendes over internettet, kan aflyttes af uvedkommende med adgang til access-linjer (fra telefonstik til central), til en router eller anden server på nettet.

Udbyder - Web-server

Password kan franarres en udbyder ved at en angriber henvender sig til udbyderen, for eksempel dennes help desk, og ved „social engineering“ får udleveret en brugers password.

Der er rapporteret om en lang række hacker-angreb på web-servere, som har givet adgang til informationer og funktioner på serveren. I en række angreb har indtrængerer fået „root-access“ til serveren og dermed fri adgang til serverens filer. Angreb har derudover givet adgang til password-filer og med anvendelse af Password Cracker programmer - som er tilgængelige på internettet - er der mulighed for at afsløre krypterede password. Indtrængerne har anvendt sårbarheder i udbredte standard-programmer, der benyttes til registrering af domænenavne af registratorer verden over. Et af disse er programmet BIND (Berkeley Internet Name Domain). Der er også rapporteret om sårbarheder i Sendmail og Microsoft Internet Information Server. Videre er anvendt sårbarheder i CGI programmer (Common Gateway Interface) og manglende ændring af et standard root/administrator password i forskellige produkter.

Der er udviklet skanner programmer - ligeledes tilgængelige på internettet - som kan afsøge en web-server for en lang række kendte sårbarheder. Skanner programmer giver en indtrænger mulighed for med stor hast at afsøge et stort antal web-servere og finde eventuelle servere med sårbarheder, der kan udnyttes. Et kendt eksempel er SATAN, Security Administrator's Tool for Analyzing Networks, der skanner web-servere for fejlkonfiguration og sårbarheder i sikkerheden.

Information om opdagede sårbarheder offentliggøres løbende af CERT - www.cert.org.

2.2 Konsekvenser

En vurdering af, hvilke konsekvenser det vil have, hvis en tjeneste kan benyttes af personer, som ikke er berettiget hertil, må selvsagt vurderes konkret for den pågældende tjeneste. Konsekvenserne ved misbrug af en internettjeneste kan være:

- Økonomiske tab for tjenesteudbyder og/eller bruger.
- Afsløring af information om tjenesteudbyders eller brugers forhold.
- Overtrædelse af lovgivning eller misligholdelse af en indgået kontrakt.

- Tab af troværdighed og tillid.

Nedenfor har IT-Sikkerhedsrådet opstillet tre grupper af tjenester med stigende konsekvenser for tjenesteudbyder og bruger, hvis tjenesten misbruges.

Der er ikke særlig støtte for en sådan opdeling i lovgivning med videre. Behandling af adgangskontrol har specielt været behandlet i relation til adgang til personoplysninger, hvor det i persondataloven (tidligere registerlovene) hedder, at den dataansvarlige skal træffe fornødne sikkerhedsforanstaltninger blandt andet mod at oplysninger kommer til uvedkommendes kendskab. I bilag 2 findes en oversigt over nogle af de regler, der findes om adgangskontrol til åbne tjenester i forskellige love og retsfor skrifter.

I det følgende er tjenester på hjemmesider opdelt i tre grupper med stigende konsekvenser, hvis tjenesten misbruges. Disse tre grupper er alene vejledende for udbyders vurdering af sin egen tjeneste.

Få og beskedne konsekvenser

Den første gruppe er tjenester, hvor det må vurderes at misbrug alene vil have få eller beskedne konsekvenser.

Til denne gruppe hører:

- Tjenester, som stiller oplysninger, der er offentlig tilgængelige, til rådighed, men hvor udbyderen ønsker at kende brugeren, for eksempel for at etablere en abonnementsordning.
- Tjenester, hvor udbyderen efter aftale med brugeren ønsker at kende brugerne og registrere deres anvendelse af tjenesten, for eksempel til brug for brugerstatistik eller til markedsføring.
- Kommercielle tjenester, hvor udbyderen ønsker at erhverve en mindre betaling for anvendelse af tjenesten.

Alvorlige konsekvenser

Den næste gruppe udgør tjenester, hvor det vurderes, at misbrug kan have alvorlige konsekvenser. Inden for denne gruppe er der tale om en meget stor variation af tjenester, som vil høre til denne gruppe. Inden for denne gruppe er der behov for nærmere at vurdere, om der er tale om risiko for mindre alvorlige konsekvenser, eller om der er risiko for mere alvorlige konsekvenser.

Til denne gruppe hører:

- Tjenester, hvor der igangsættes databehandling med økonomiske konsekvenser, for eksempel ansøgninger og varekøb.
- Tjenester, hvor der er behov for sikkerhed for at kunne identificere den person, som indberetter oplysninger, for eksempel med henblik på offentliggørelse eller sagsbehandling.
- Tjenester, som giver adgang til personoplysninger, og hvor det i henhold til persondataloven skal sikres, at oplysningerne ikke kommer til uvedkommendes kendskab.
- Tjenester, der giver adgang til interne oplysninger og oplysninger der efter lovgivning er fortrolige og underlagt tavshedspligt.
- Tjenester, der kun er adgang til mod betaling.
- Tjenester, hvor misbrug vil medføre et alvorligt tab af tillid og troværdighed.

Vitale konsekvenser

Til denne gruppe hører tjenester, hvor det må vurderes, at det vil have så betydelige konsekvenser, at tjenesten misbruges, at adgangskontrollen må betragtes som kritisk for tjenesteudbyderen.

Til denne gruppe hører:

- Tjenester, hvor det vil have meget væsentlige økonomiske konsekvenser, hvis der kan ske misbrug.

- Tjenester, som giver adgang til hemmelige forretningskritiske oplysninger.
- Tjenester, som har betydning for statens sikkerhed og rigets forsvar.
- Tjenester, som giver adgang til følsomme personoplysninger, herunder oplysninger der giver indblik i en persons rent private forhold.
- Tjenester, hvor misbrug vil føre til betydeligt tab af tillid og troværdighed.

3 BRUGERAUTENTIFICERING

Når en bruger ønsker at anvende en udbudt tjeneste på nettet, gennemføres en brugerautentificering før brugeren får adgang til tjenesten. Brugerautentificering verificerer brugerens identitet, men giver ikke i sig selv klarhed over, hvilke databehandlinger brugerne må udføre.

Brugeren skal forud for autentificeringen være autoriseret til bestemte anvendelser. Forud for anvendelse af tjenesten skal der gennemføres en autorisation, hvor brugeren får tildelt rettigheder til bestemte typer af anvendelser af tjenesten. Traditionelt skelner man mellem, om brugeren må se data - eller om han også har ret til at ændre og slette data. Endvidere vil brugeren skulle autoriseres til kun at have adgang til bestemte data, for eksempel vil en bruger af en Internettjeneste typisk kun have adgang til egne data.

Brugerautentificering kan gennemføres på en række forskellige måder. Grundlæggende taler man om, at autentificeringen kan ske ud fra tre forskellige mekanismer:

- Noget brugeren *ved*, for eksempel et password.
- Noget brugeren *har*, for eksempel et chipkort.
- Noget brugeren *er*, for eksempel et fingeraftryk som biometrisk kode.

Når brugerautentificeringen sker ved, at brugeren indtaster et brugernavn og et password, baserer man sig således på noget brugeren ved - nemlig hans password.

Hvis brugeren for at få adgang til tjenesten skal være besiddelse af en særlig „enhed“, for eksempel et chip-kort, kræver brugerautentificering noget, brugeren har. Et andet eksempel på noget brugeren har er nøglefiler som opbevares på harddisken på brugerens pc.

Anvendelse af „noget brugeren er“ - typisk i form af en biometrisk kode - har efter IT-Sikkerhedsrådets vurdering ikke en sådan udbredelse, at det kan inddrages i en aktuell vejledning om adgangskontrol. En biometrisk kode åbner mulighed for en væsentlig forøgelse af sikkerheden. Det vil derfor være hensigtsmæssigt at inddrage biometriske koder, når de bliver almindeligt tilgængelige.

I praktiske løsninger på brugerautentificering vil man ofte anvende en kombination af flere løsninger. For eksempel vil man ved brug af et chip-kort som regel anvende en pin-kode (password), som giver adgang til chip-kortets informationer, og dermed kombinere noget, brugeren har, (chip-kortet) med noget, brugeren ved (pin-koden).

Nedenfor er beskrevet tre typer for autentificering, som vil blive anvendt som udgangspunkt for vejledningens anbefalinger og overvejelser:

- password,
- token med engangskode,
- certifikat-baseret autentificering.

Password

Den første type anvender den velkendte fremgangsmåde med et brugernavn og et password. Fremgangsmåden omtales som statisk password, fordi det udleverede eller valgte password kan anvendes uændret over en længere tidsperiode. Sikkerheden baserer sig på, at password kun er kendt af bruger og udbyder.

I HTTP protokollen, der er den netværksprotokol, som overfører alle datafiler på Internettet, findes en simpel form for brugerautentificering med password, som kaldes for „Basic Authentication“. Når brugeren ønsker adgang til et dokument, som er beskyttet af Basic Authentication, sender serveren en kode til brugerens browser, som præsenterer brugeren for en dialogboks, hvor der skal indtastes et brugernavn og password.

Brugernavn og password verificeres af web-serveren og den kan returnere dokumentet, hvis verifikationen er OK.

Brugerautentificering med password implementeres dog typisk på en hjemmeside med en HTML form.

Token med engangskode

I den anden type brugerautentificering, som kan kaldes *token med engangskode*, har brugeren en token som leverer et engangspassord. Når brugeren skal anvende et password som led i autentificeringen, for at få adgang til tjenesten eller for at aktivere den anvendte token, kaldes fremgangsmåden for en to faktor autentificering: Man kombinerer noget brugeren har, en token, med noget brugeren ved, et password.

Der findes en række muligheder for token med engangspassord, blandt andet:

- Brugeren kan få tilsendt en papirliste, som indeholder en række passwords.
- Brugeren kan have et „skrabelod“ eller elektronisk enhed, hvor der anvendes ét password ad gangen.
- Brugeren kan have en elektronisk enhed, som med faste korte tidsintervaller oplyser det password, der kan anvendes.
- Brugeren kan have en elektronisk enhed, som kan foretage en beregning på et tal (en *challenge*), som serveren sender (også kaldet dynamisk password).

Der findes ikke standarder eller bredt implementerede løsninger med token med engangskode, men der findes et udbud af produkter fra en række leverandører. Det vil her være nødvendigt at foretage en vurdering af den pågældende løsning i forhold til tjenesten.

Certifikat-baseret autentificering

I den tredje type brugerautentificering, som vi kalder *certifikat-baseret autentificering*, har brugeren et certifikat og en tilhørende privat nøgle, der kan identificere ham. Certifikatet er udstedt af et certificeringscenter (nøglecenter eller CA) og udgør en dokumentation for, at den, der anvender den til certifikatet hørende private nøgle, er den person, som fremgår af certifikatet. Certifikat-baseret autentificering er tilsvarende en to-faktor autentificering, idet den baserer sig på, at brugeren kender et password, som giver adgang til at anvende en privat nøgle, der opbevares på pc eller et chip-kort.

Autentificeringen benytter en såkaldt „*challenge - response*“ model. Det vil sige, serveren sender en meddelelse (en *challenge*), som brugerens pc besvarer (*response*). Før enkrypteringen med den private nøgle af svaret skal brugeren angive et password. Det udfærdigede response sendes retur til serveren, eventuelt sammen med certifikatet. Da meddelelsen (*challenge*) og svaret (*response*) er forskellig ved hver logon, er der også ved certifikat-baseret autentificeringen tale om, at der benyttes en engangskode.

I SSL version 3 (Secure Socket Layer) protokollen, som er implementeret i nye versioner af de almindeligt udbredte browsere, findes en klient autentificering, som kan gennemføre en certifikat-baseret autentificering, hvis brugeren har installeret et certifikat og privat nøgle.

4 VALG AF BRUGERAUTENTIFICERING

Der er ingen enkel løsning på valg af brugerautentificering, som giver en fuldstændig sikkerhed. Uanset hvad valget falder på vil der altid være en risiko for, at sikkerheden kan brydes. I det følgende fremlægges en række overvejelser og anbefalinger med udgangspunkt i de tre grupper, som blev opstillet ovenfor i kapitel 2. For hver gruppe anbefales brugerautentificering og en række øvrige sikkerhedsforanstaltninger, der kan bruges vejledende i udformningen af adgangskontrollen.

4.1 Tjenester med få og beskedne konsekvenser

På dette niveau indføres adgangskontrollen typisk for at etablere en brugerregistrering for eksempel med henblik på at kunne føre statistik over den enkelte brugers anvendelse af tjenesten. Det antages således, at der ikke er et særligt behov for at beskytte de oplysninger, der gives adgang til.

En autentificering med brugernavn og password vil kunne anvendes. Password kan vælges af brugeren og indtastes ved første besøg. Det bemærkes i den forbindelse, at Datatilsynet har udtalt, at personnummer ikke kan anvendes som password, jævnfør nærmere bilag 2 side 44.

En sådan løsning med et statisk password er sårbar overfor en lang række trusler - som er omtalt oven for i afsnit 2.1 - og der er derfor kun etableret en meget begrænset sikkerhed.

I mange sammenhænge kan der være et ønske om at kunne bruge informationer om, hvad brugeren har bedt om tidligere, og etablere en session. Med en session menes tidsrummet for en åben forbindelse mellem to enheder, som gennemfører en datatransmission, og som derved kan knytte en række forespørgsler fra tjenesten og svar fra brugeren sammen. Da HTTP protokollen behandler hver „request“ (forespørgsel) uafhængigt

af eventuelt tidligere dataudveksling, er det nødvendigt at etablere en session ovenpå dataudvekslingen. På internettet findes forskellige løsninger, som kan anvendes, for eksempel:

- Anvendelse af en angivelse i URL, der giver identifikation af sessionen.
- Anvendelse af cookies til at opbevare information, der giver identifikation af sessionen.
- Anvendelse af SSL.

4.2 Tjenester med alvorlige konsekvenser

I denne gruppe af tjenester er der behov for at autorisere brugere og skabe sikkerhed, for at kun autoriserede brugere har adgang til den pågældende tjeneste. Behovet har dog ikke vital betydning for tjenesteudbyderen.

Password

For sådanne tjenester vil en autentificering med password som regel skulle anvendes som minimumskrav. Der findes en række forskellige praktiske implementeringer af password-autentificering på internettet i dag:

- password vælges af brugeren og indtastes på hjemmesiden ved tilmelding til tjenesten,
- ved tilmelding til tjenesten på hjemmesiden angives e-mail adresse, og password sendes med e-mail til brugeren,
- ved tilmelding til tjenesten fremsendes password med almindelig post,
- for at forenkle brugen af internettjenesten returneres login data i en særlig cookie, som hentes fra brugerens pc ved kommende anvendelser.

Brugen af passwords indebærer en række beslutninger om, hvilke procedurer, der skal følges omkring anvendelsen. Man må i den forbindelse sondre mellem udlevering af førstegangs password, og fornyelse af password.

Når det gælder førstegangs password bør den udstedende instans sørge for, at password fremsendes ad særskilt kanal, for eksempel med almindelig post eller med e-mail. Ved fremsendelsen bør det klart beskrives, hvordan dette første password kan ændres, og at ændring skal ske ved brugerens første login.

Når det gælder den løbende fornyelse af et password kan man overveje, om det kan overlades til brugeren at sørge for ændringer, eller om nye passwords skal pålægges af den systemansvarlige. Begge løsninger har sine fordele og ulemper. Hvis brugeren selv kan vælge password, er der åbnet mulighed for, at denne vælger password, som er lette at gætte eller afsløre med et password cracker program. Omvendt er der ved det udleverede password risiko for, at brugeren opgiver at huske det og derfor skriver det ned, eventuelt på en huskeseddel klistret på pc'en. Det er IT-Sikkerhedsrådets opfattelse, at der her er tale om en grundlæggende sårbarhed ved password-autentificering, og at ingen af mulighederne har en klar fordel.

Ved indtastning må det indtastede password ikke være synligt på skærmen.

Tjenesteudbyderen bør informere om, at kun brugeren må kende det anvendte password, og vejlede om og så vidt muligt kontrollere, at brugeren skal udforme sit password i overensstemmelse med almindelige anbefalinger:

- vælg lange password på mindst 8 tegn,
- brug flere tegn end A - å, det vil sige tal og eventuelt tegn som & og \$, samt både små og store bogstaver,
- vælg intetsigende password og undgå helt almindelige navne og ord, der findes i en ordbog,
- konstruer et password, der er lette at huske, men svære at gætte - man kan for eksempel benytte kendte sange eller udtryk, således kan 2born2be huskes ud fra „to be or not to be“, eller indsætte tal og tegn i almindelige ord som i jule!2mand,
- når password udskiftes skal man undgå password, der tidligere er anvendt eller anvende løbenummer som i kv48+df1, kv48+df2 og så videre,

- anvend kun samme password til tjenester med beskedne konsekvenser.

Det er IT-Sikkerhedsrådets vurdering, at anvendelse af cookies til opbevaring af login data rummer betydelige sårbarheder. Da den enkelte cookie findes på brugerens pc, undergraves den grundlæggende sikkerhed ved statisk password, som noget, som kun brugeren ved. Denne fremgangsmåde bør derfor kun anvendes for mindre kritiske tjenester.

Login data, herunder password, bør ikke sendes i klartekst eller blot kodet med teknikken „UUENCODE“ eller lignende. Password bør under transmissionen være krypteret for at beskytte mod aflytning.

SSL (Secure Socket Layer) protokollen tilbyder en krypteret transmission mellem pc og web-server. Med SSL foretages en identifikation af web-server og pc samt en udveksling af en krypteringsnøgle for en session. Der opnås således samtidig en sikring af sessionen. SSL er standard i nyere versioner af browsere og web-software, og det forekommer derfor IT-Sikkerhedsrådet naturligt, at SSL anvendes ved alle tjenester, hvor det vurderes, at en adgangskontrol er ønskelig.

Passwordfilen på serveren må forudsættes at være særlig beskyttet, så den ikke er umiddelbar tilgængelig hverken for medarbejdere eller en udefrakommende indtrænger, for eksempel ved at password krypteres eller gemmes som en hashværdi, ved at passwordfilen placeres isoleret eller ved en særlig adgangskontrol.

For tjenester med mere alvorlige konsekvenser er det IT-Sikkerhedsrådets opfattelse, at password ikke udgør en tilstrækkelig stærk adgangskontrol. En række trusler betyder at password i almindelighed anses for en relativ svag form for brugerautentificering. For tjenester med mere alvorlige konsekvenser må det derfor anbefales at etablere en adgangskontrol, som imødegår trusler som password er sårbare overfor. IT-Sikkerhedsrådet vil her pege på token med engangskode og certifikat-baseret autentificering, som er beskrevet ovenfor. Hvilken autentificering, der anvendes, vil bero

på en vurdering af den konkrete tjeneste, samt på de praktiske og økonomiske muligheder.

For disse tjenester bør transmission af login data - og øvrige data - være krypteret med stærk kryptering. SSL har mulighed for at kryptere med 128 bit nøgle, og dette bør være minimum. Det betyder også, at tidligere versioner af SSL, som krypterer med en 40 bit nøgle ikke bør anvendes.

Selvom der med disse former for autentificering er etableret en stærkere autentificering, skal det bemærkes, at der ikke hermed er iværksat sikkerhedsforanstaltninger, som imødegår installation af en trojansk hest på brugerens pc, der kan aflæse data, herunder login data.

Token med engangskode

Token med engangskode imødegår en række af de nævnte trusler og giver en forøget sikkerhed, idet brugeren skal være i besiddelse af en token. Såfremt man etablerer brugerautentificeringen som en to-faktor autentificering må det vurderes, at der opnås en betydelig sikkerhed. Denne kan for eksempel etableres ved at anvende en elektronisk token, der, beskyttet ved en pin-kode, kan aflevere et engangspassword,

Udleveringen af henholdsvis password og token bør ske af adskilte kanaler, for eksempel kan password fremsendes i forseglede kuverter med almindelig post. Det bør tilstræbes, at token udleveres ved personligt fremmøde for at sikre, at den kommer rette vedkommende i hænde. Tjenesten bør først åbnes for brugeren, når han har bekræftet, at han har modtaget password og token.

Certifikat-baseret autentificering

Med udbredelse af en Public Key Infrastructure (PKI) og etablering af certificeringscentre (nøglecentre) vil det blive en realistisk mulighed at anvende certifikat-baseret autentificering.

Et afgørende led i sikkerheden ved certifikat-baseret autentificering er udstedelse af certifikatet og generering af den tilhørende private nøgle. Ved tjenester med mere alvorlige konsekvenser, bør der ved udleveringen etableres en høj grad af sikkerhed for identifikation af brugeren ved udleveringen. Der bør som udgangspunkt kræves personlig fremmøde. For tjenester med mindre alvorlige konsekvenser, hvor man ønsker at anvende certifikat-baseret autentificering, kan mindre sikre procedurer anvendes, for eksempel udlevering ved elektronisk overførsel på baggrund af en henvendelse med almindelig post.

Ved modtagelse af en certifikat-baseret adgangskode skal udbyder ved hver autentificering foretage en kontrol af, om certifikatet fortsat er gyldigt. Herunder bør det kontrolleres, om certifikatet er trukket tilbage (revokeret). Udbyder kan ved tjenester med mindre alvorlige konsekvenser vælge en procedure, hvor der sker en mindre hyppig kontrol af medsendte certifikater.

Også ved en certifikat-baseret autentificering skal der ske en autorisation af brugeren. Den kan bestå i, at alle brugere som autentificerer sig med et certifikat af en bestemt type, har adgang til nærmere angivne funktioner. Det er dog IT-Sikkerhedsrådets opfattelse, at det er nødvendigt for en sikker adgangskontrol, at der forud for en brugers adgang til en tjeneste gennemføres en tilmelding til tjenesten med et angivet certifikat samt en registrering og autorisation af brugeren. IT-Sikkerhedsrådet kan dog ikke se noget til hinder for, at et certifikat til autentificering anvendes ved flere offentlige selvbetjeninger.

Ved anvendelse af certifikat-baseret autentificering er det IT-Sikkerhedsrådets opfattelse, at nøglepar, som anvendes til at afgive elektronisk signatur, ikke bør anvendes til brugerautentificering. IT-Sikkerhedsrådet finder for det første, at det bør være uomtvisteligt klart for brugeren, når denne igangsætter en elektronisk signatur ved at aktivere sin personlige nøgle. Endvidere indebærer en dobbelt anvendelse til signatur og autentificering en risiko for, at den private nøgle kan kompromitteres i forbindelse med adgangskontrol, hvor en kendt tekst underskrives. IT-Sikkerhedsrådet vil derfor anbefale, at der enten anvendes nøglepar og certifikater som alene

anvendes til brugerautentificering, eller at der anvendes et særskilt nøglepar til autentificering, for eksempel samme nøglepar som anvendes i forbindelse med hemmeligholdelse. (Se Anbefaling af Specifikation for certifikater i FSK-projektet fra Forum for Digital Signatur).

4.3 Tjenester med vitale konsekvenser

I denne klasse vurderes det, at der vil være tale om vitale konsekvenser ved sikkerhedsbrud. Det er IT-Sikkerhedsrådets opfattelse, at man, i lyset af de bemærkninger, der er gjort ovenfor under 2.1. om de forskelligartede trusler mod adgangskontrolsystemer, bør være meget tilbageholdende med at etablere adgang til sådanne tjenester fra en hjemmeside baseret på adgangskontrol. Beslutter man sig herfor er det i alle tilfælde nødvendigt at iværksætte solide foranstaltninger til beskyttelse mod angreb.

Såfremt man baserer sig på adgangskontrol, bør der være tale om en afgrænset brugerkreds, hvor det er muligt at installere særligt programmel og udstyr hos brugerne og derved opnå en høj grad af sikkerhed for brugerens adfærd.

Ved anvendelse af certifikat-baseret autentificering kan sikkerheden øges, ved at den private nøgle opbevares på et chip-kort, og at dannelse af svar (response) sker i chip-kortet. Opbevaring på et chip-kort giver en høj sikkerhed for, at certifikatet og den tilhørende private nøgle ikke kan læses af uvedkommende. Selvom adgangen til chip-kortet alene er beskyttet af en pin-kode, betyder kombinationen af kort og pin-kode, at det er vanskeligt uretmæssigt at tilegne sig begge - idet brugeren forudsættes at hemmeligholde sin pin-kode på betryggende vis. Endvidere er anvendelsen af chip-kort en sikkerhedsforanstaltning over for en trojansk hest, idet den private nøgle opbevares adskilt fra pc'en.

BILAG 1 BIDRAGYDERE

I udarbejdelse af vejledningen har følgende bidraget med oplysninger og vurderinger af adgangskontrol:

Flemming Langgaard og Preben Andersen, DK-CERT
Flemming Hansen, KommuneData
Jan Krogh Jensen, TeleDanmark Internet
Kurt Hansen, Told & Skat.

Et udkast til vejledningen har været sendt til høring i IT-Sikkerhedsrådets panel af særlig sagkyndige og til Datatilsynet i april/maj måned 2001.

BILAG 2 FORSKRIFTER OM ADGANGSKONTROL

CPR - Det Centrale Personregister

Private virksomheder, foreninger med videre har efter CPR-loven mulighed for at foretage forskellige søgninger på personer, veje, boliger og myndigheder i hele landet eller inden for en kommune eller et post-distrikt. Brugerens adgang til forespørgselssystemet etableres via en internetadresse og forudsætter godkendelse af Indenrigsministeriet. Brugernes betaling for tjenesten sker med månedsabonnement og efter forbrug af de enkelt søgninger.

Søgning af personoplysninger i systemet forudsætter, at brugeren - ligesom ved adresseforespørgsel til et folkeregister - foretager en entydig identifikation af den søgte person. Dette sker ved indtastning af navn samt personnummer, fødedato eller adresse. Matcher to eller flere personer de angivne søgekriterier, videregives der ikke personoplysninger.

De personoplysninger, der videregives til brugeren, svarer til de oplysninger et folkeregister videregiver ved besvarelse af en adresseforespørgsel.

Kommunikationen med systemet er krypteret.

Uddrag fra Indenrigsministeriets standardvilkår for adgang til forespørgselssystemet af 1. juli 2000.

Oprettelse og ændring af kundeforhold

Anmodning om terminaladgang til CPR Søg sker ved skriftlig henvendelse til Indenrigsministeriet, CPR-kontoret, Datavej 20, Postboks 269, 3460 Birkerød, eventuelt ved anvendelse af bestillingsblanket. Eventuelle ændringer i kundeforholdet skal ligeledes ske ved skriftlig henvendelse til Indenrigsministeriet, CPR-kontoret.

Ved behandlingen af en sådan henvendelse tager Indenrigsministeriet stilling til, om CPR-lovens betingelser for at give adgang til elektroniske enkeltforespørgsler samt reglerne om sikkerhedsforanstaltninger er opfyldt, forinden der etableres terminaladgang for kunden til CPR.

Ved etablering af terminaladgangen udveksles nødvendige oplysninger om blandt andet kommunikations- og adgangsforhold.

Regler for autorisation og adgangskontrol

Kunden skal udpege en sikkerhedsansvarlig, der er ansvarlig for overholdelse af nærværende vilkår samt for, at kun de medarbejdere, for hvem det er nødvendigt at benytte terminalen i forbindelse med udførelsen af deres arbejde, må autoriseres til at rette forespørgsler til CPR.

CPR-kontoret udsteder én autorisationskode (personkode og kendeord) til hver enkelt medarbejder, der skal have adgang til CPR. Kendeordene er hemmelige. De skal udskiftes ved den enkelte medarbejders første adgang til CPR til et personligt og fortroligt kendeord, der kun kendes af den pågældende medarbejder. Ved tilbagelevering af autorisationen skal kendeordet ændres til et fortroligt kendeord, der kun kendes af den sikkerhedsansvarlige.

Den sikkerhedsansvarlige skal føre en fortegnelse over de medarbejdere, der har fået autorisation, med angivelse af tidspunkt for autorisationens påbegyndelse og senere ophør. Fortegnelsen opbevares i aflåst skab hos den sikkerhedsansvarlige, og kopi heraf skal efter anmodning udleveres til Indenrigsministeriet.

Den enkelte medarbejder skal overholde følgende regler vedrørende kendeordet:

- kendeordet skal være personligt,
- kendeordet må ikke deles med, lånes ud eller oplyses til andre,
- kendeordet skal udskiftes efter højst 90 dages brug,
- længden af kendeordet skal være på mindst 6 og højst 8 karakterer,

- kendeordet skal bestå af en blanding af tal og bogstaver (dog ikke ü, æ, ø, å eller andre specielle bogstaver),
- kendeordet må ikke genbruges,
- kendeordet må ikke indeholde løbenummer (for eksempel peter1, peter2, etcetera),
- kendeordet må ikke bestå af eget eller familiens navn, initialer, fødselsdato, personnummer, bilnummer, bilmærke eller andet, der er nemt at gætte for andre, og
- kendeordet skal ændres, hvis det er eller kunne være blevet kendt af andre,
- medarbejdere må ikke forlade terminalen eller lokalet uden at lukke sig ud af CPR-systemet.

Autorisationskoden vil blive spærret efter 5 mislykkede forsøg på at indtaste den rigtige autorisationskode. Koder, der er blevet spærret eller glemt, vil først igen kunne benyttes efter skriftlig henvendelse til Indenrigsministeriet og mod betaling, medmindre der er etableret en særlig procedure, hvor den sikkerhedsansvarlige selv kan genåbne for adgangen.

Alle forespørgsler logges i CPR. Registreringen indeholder oplysning om personkode, tidspunkt samt hvilke oplysninger, der er forespurgt på i CPR. Denne registrering danner grundlag for udskrift i tilfælde, hvor der er mistanke om misbrug af terminaladgangen til CPR.

Fra CPR udskrives hver måned en statistik over terminalanvendelsen (transaktionsstatistik). Statistikken angiver for hver terminaloperatør, hvilke transaktionstyper den pågældende har anvendt samt antallet af gange den enkelte transaktionstype har været anvendt.

Transaktionsstatistikken sendes til den sikkerhedsansvarlige hos kunden og skal kontrolleres af denne.

Den sikkerhedsansvarlige kan i forbindelse med kontrol af medarbejdernes anvendelse af terminalsystemet anmode om, at der fra CPR mod betaling

udskrives en liste over terminaltrafikken for én eller flere personkoder for en bestemt afgrænset tidsperiode.

Krav til datakommunikation

Der er ingen særlige krav til datakommunikationen. Dog skal omstillingscentralen/netværksudbyderen være anerkendt. Datakommunikationen vil være krypteret.“

Den elektroniske udgave af statstidende

Adgang til den elektroniske udgave af Statstidende er fri, idet oplysningerne er offentligt tilgængelig. Såfremt en person ønsker at abonnere på kundegørelser i elektronisk form skal vedkommende dog meldes til systemet og benytte brugernavn og adgangskode eller en avanceret elektronisk signatur baseret på et kvalificeret certifikat. Informationsleverandører skal for at få adgang til at levere data elektronisk tilmeldes systemet og benytte brugernavn og adgangskode.

Uddrag af bekendtgørelse om opbygningen, driften og brugen af Statstidende nr. 799 af 24. august 2000:

Kapitel 3. Sikkerhedsforanstaltninger

§ 7. For udgivers anlæg, som benyttes til administration og offentliggørelse af databasen, gælder de sikkerhedsforskrifter, der er anført i nærværende kapitel.

Stk. 2. Reglerne om sikkerhedsforanstaltninger gennemgås én gang årligt med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold hos udgiver.

§ 8. Når en person via internettet har haft almindelig, offentlig adgang til databasen, må der ikke foretages registrering heraf med efterfølgende mulighed for at konstatere, hvem som har brugt systemet, jævnfør dog stk. 2.

Stk. 2. Udgiver skal foretage en registrering af alle uautoriserede adgangsforsøg til databasen.

Stk. 3. Læserne af det elektroniske Statstidende skal af udgiver tilbydes krypteret kommunikation, som sikrer fortrolighed og autencitet af de leverede oplysninger.

§ 9. Såfremt en person ønsker at abonnere på kundgørelser i elektronisk form, kan udgiver stille krav om, at vedkommende meldes til systemet og benytter brugernavn og adgangskode eller en avanceret elektronisk signatur baseret på et kvalificeret certifikat, jævnfør lov om elektronisk signatur. Sidstnævnte mulighed er dog ikke implementeret i systemet fra bekendtgørelsens ikrafttrædelse.

§ 10. Informationsleverandøren skal for at få adgang til at levere data elektronisk tilmeldes systemet og benytte brugernavn og adgangskode eller en avanceret elektronisk signatur baseret på et kvalificeret certifikat, jævnfør lov om elektronisk signatur. Sidstnævnte mulighed er dog ikke implementeret i systemet fra bekendtgørelsens ikrafttræden.

Stk. 2. I forbindelse med tilmeldingen fremsendes brugernavn og adgangskode pr. post for at give en rimelig sikkerhed for, at den tilmeldtes identitet er korrekt. Såfremt informationsleverandøren ønsker at benytte en avanceret elektronisk signatur, jævnfør stk.1, skal vedkommende signere en tilmelding, som indsendes til udgiver sammen med det tilhørende certifikat.

Stk. 3. Ved hver levering af data elektronisk skal der foretages følgende:

- 1) En sikker identifikation af den enkelte leverandør ved anvendelse af det tildelte brugernavn og autorisationskode eller en avanceret elektronisk signatur baseret på et kvalificeret certifikat.
- 2) Maskinel registrering (logging) af samtlige data.

Stk. 4. Ved levering via Internettet skal der etableres særlige sikkerhedsforanstaltninger (for eksempel kryptering), som sikrer, at data ikke kommer til uvedkommendes kendskab.

§ 11. Kun de personer, som udgiver autoriserer hertil, må have adgang til de redaktionelle og systemadministrative funktioner. Forsøg på at benytte funktioner, hvortil brugeren ikke er autoriseret, afvises af systemet.

Stk. 2. De autoriserede brugere tildeles enten et brugernavn og en personlig og fortrolig adgangskode eller benytter en avanceret elektronisk signatur baseret på et kvalificeret certifikat, jævnfør lov om elektronisk signatur. Sidstnævnte mulighed er dog ikke implementeret i systemet fra bekendtgørelsens ikrafttræden.

Stk. 3. Udgiver er forpligtet til at give samtlige autoriserede brugere den fornødne instruktion i behandlingen af data, herunder at gøre alle bekendt med reglerne om sikkerhedsforanstaltninger.

Stk. 4. Udgiver må kun autorisere personer, for hvem en udvidet adgang er nødvendig for udførelsen af deres arbejde, og de enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for. Hvert halve år kontrollerer udgiver, at de autoriserede personer fortsat opfylder betingelserne.

Stk. 5. Autorisationen skal angive, i hvilket omfang brugerne må forespørge, masseudtrække, inddatere eller slette oplysninger samt oprette eller ændre meddelelser. I alle tilfælde, hvor der sker en oprettelse eller ændring af meddelelser, skal der foretages en maskinel registrering (logging) af data.

Stk. 6. Udgiver skal en gang om måneden udskrive meddelelse om de transaktioner, hvorved en autoriseret bruger har foretaget masseudtræk og i tilknytning hertil foretage en stikprøvekontrol af formålet med disse transaktioner.

§ 12. Følgende sikkerhedskrav er gældende for abonnenter (§9), informationsleverandører (§10) og autoriserede brugere (§11) ved benyttelse af systemet:

- 1) indtastning af adgangskode skal ske ikke-læsbart,
- 2) den tildelte adgangskode skal udskiftes mindst en gang årligt,
- 3) samtlige brugergrupper, som har logget sig ind på systemet, vil efter længere tids inaktivitet blive logget ud af systemet,
- 4) der foretages en maskinel registrering (logging) af alle uautoriserede adgangsforsøg. Såfremt der indenfor en fastsat periode er registreret flere på hinanden følgende uautoriserede adgangsforsøg fra et givet brugernavn, skal der udskrives meddelelse herom, og brugeren blokeres for yderligere forsøg. Umiddelbart herefter foretages kontrol af udgiver.

Persondataloven

Datatilsynet har i forbindelse med vurdering af planerne for elektronisk borgerservice i Københavns Kommune besvaret en række spørgsmål. Der er derved udstukket vejledende retningslinier for graden af sikkerhed i identifikationen af en borger i forbindelse med kommunikation af forskellige typer af personoplysninger.

Brev af 7. september 2000 til Cap Gemini. Se www.datatilsynet.dk, i „Værd at vide“ under „Borgerbetjening“.

På vegne af Københavns Kommune og Cap Gemini, har Cap Gemini i brev af 14. juli 2000 fremsendt en række spørgsmål til Datatilsynet, som er formuleret på baggrund af drøftelser på et møde den 5. juli 2000 hvori deltog repræsentanter for Forskningsministeriet, Københavns Kommune, Cap Gemini og Datatilsynet.

1. *„Er det tilstrækkeligt at borgeren identificerer sig med ID og adgangskode (fx udsendt sammen med Skatteoplysninger) for at kunne læse/modtage fortrolige oplysninger fra Kommunens web-server?“*

Datatilsynet finder, at den anførte identifikationsmetode normalt vil være tilstrækkelig.

2. *„Er det tilstrækkeligt at borgeren identificerer sig med ID og adgangskode (fx udsendt sammen med Skatteoplysninger) for at kunne læse/modtage følsomme oplysninger fra Kommunens web-server?“*

Datatilsynet vil ikke afvise, at den anførte identifikationsmetode vil kunne være tilstrækkelig. Tilsynet anbefaler dog at øge sikkerheden gennem anvendelse af certifikat/digital signatur.

3. *„Stiller persondataloven mv. nogen krav til indsendelse af fortrolige persondata fra en borgers pc til web-serveren udover kryptering af data. Skal borgeren fx identificere sig således at meddelelsesautenticitet opnås? Hvis ja, er identifikation med ID og adgangskode tilstrækkelig.“*

Datatilsynet finder, at borgeren skal identificere sig, og at ID og adgangskode i denne situation normalt vil være tilstrækkelig. Tilsynet anbefaler dog at øge sikkerheden gennem anvendelse af certifikat/digital signatur.

4. *„Stiller persondataloven mv. nogen krav til indsendelse af følsomme persondata fra en borgers pc til web-serveren udover kryptering af data. Skal borgeren fx identificere sig således at meddelelsesautenticitet opnås? Hvis ja, er identifikation med ID og adgangskode tilstrækkelig.“*

Datatilsynet finder, at borgeren skal identificere sig, og at der i denne situation bør anvendes certifikat/digital signatur.

5. *„Kan CPR-nr. bruges som brugernavn eller skal det være et ID uden indholdsmæssig betydning? Det kan nævnes at der i løsningen er lagt op*

til at CPR-nr. optræder på samtlige web-sider med fortrolige eller følsomme data.“

Datatilsynet accepterer anvendelse af CPR-nr. som brugernavn, men CPR-nr. må ikke transmitteres ukrypteret over det åbne Internet.

6. *„Den almindelige arbejdsgang for borgeren er at denne henter en web-side delvist udfyldt med personoplysninger, supplerer med yderligere oplysninger og sender siden tilbage til kommunens web-server. Denne procedure gentages eventuelt for en anden ydelse.“*

Som det fremgår af de foregående svar, skal der samlet set skal være den fornødne sikkerhed for at personoplysninger ikke kommer uvedkommende i hænde, og at personoplysninger ikke forringes eller tilintetgøres. Den første betingelse findes opfyldt ved at sikre, at oplysninger transmitteres i forsvarligt krypteret form. Den anden betingelse findes opfyldt ved som minimum at anvende brugerid og adgangskode ved indsendelse af fortrolige oplysninger og anvendelse af certifikat/signatur ved indsendelse af følsomme oplysninger.

Endelig forespørger Cap Gemini og Københavns Kommune om rækkevidden af en identifikation i forbindelse med logon under hensyntagen til at borgeren kan tænkes at gøre brug af borgerservice fra egen pc, andres pc eller en offentlig tilgængelig pc.

Datatilsynet kan godkende en brugervenlig løsning, som baseres på, at en identifikation via logon eller certifikat er gyldig i en hel session og dermed først ophæves ved timeout eller ved nedlukning af browseren. Det er dog en forudsætning, at brugeren i alle relevante skærbilleder tydeligt gøres opmærksom på, hvorledes han sikkerhedsmæssigt forsvarligt skal logge af systemet.

BILAG 3 FORKORTELSER OG BEGREBER

| | |
|---------------------------------|--|
| Adgangskontrol | Fremgangsmåder, som skal sikre at ressourcer i et IT system kun kan blive anvendt af autoriserede enheder på autoriserede måder. |
| Autentificering | Den handling som verificerer en påstået identitet. |
| Autorisation | Tildeling af rettigheder, som omfatter tildeling af adgang baseret på adgangsrettigheder. |
| CA, Certificeringscenter | Certification Authority. Udsteder af certifikater. Kaldes i Lov om elektroniske signaturer for nøglecenter. |
| Certifikat | En formateret meddelelse som angiver en bestemt identitet samt en nøgle (nøglecertifikat) eller attributter (attributcertifikat) som knyttes til denne identitet, underskrevet med en digital signatur af et CA (nøglecenter). |
| Chipkort | Kort, typisk i kreditkortstørrelse, i hvilket der er indbygget en halvlederchip, som er i stand til at udføre visse, avancerede databehandlingsfunktioner, for eksempel enkryptering eller afgivelse af digital signatur. |
| Cookies | En samling af data om brugere, som gemmes på brugerens pc. Cookies er en udvidelse af protokollen HTTP. |
| HTML | Hyper Text Markup Language. Det sprog, eller markeringer i teksten, som anvendes på internettet til at bestemme udseende på web-sider. |

| | |
|-----------------|--|
| HTTP | Hyper Text Transfer Protocol. Den protokol - regelsæt for kommunikation mellem to parter - som anvendes ved udveksling af web-sider på internettet. |
| Password | Et antal tegn som anvendes til autentificerings-information. |
| Pinkode | Et password som alene består af tal, typisk 4. |
| SSL | Secure Socket Layer. En sikkerhedsprotokol ved kommunikation mellem en web-server og en bruger pc, som sikrer meddelelsesautenticitet og kryptering. |
| Token | En identitets token er en enhed, for eksempel et chipkort eller en metalnøgle, som anvendes til identitets autentificering. |
| URL | Uniform Ressource Location. Adresse for en web server på internettet, for eksempel www.fsk.dk . |