Fra rådet til tinget
TEKNOLOGIRÅDETS NYHEDSBREV TIL FOLKETINGET

Nr. 285 | december 2013

Ny rapport til Europas politikere

Styrk it-sikkerheden

De offentlige it-systemer er ikke sikre nok. Følsomme oplysninger om borgerne bør beskyttes bedre mod fejl, misbrug og kriminalitet. Digitalisering har store fordele, men valg af billige og bekvemme løsninger kan koste dyrt i det lange løb.

Teknologirådet har netop afsluttet en undersøgelse af sikkerhedsproblemerne i EU-landenes offentlige it-systemer. I en rapport til Europaparlamentet vurderes de politiske udfordringer og handlemuligheder. Vurderingerne er baserede på tre cases: Biometriske pas; digitalisering i sundhedssektoren; digitaliserede offentlige indkøb.

Udfordringerne er store: Antallet af 'sikkerhedshændelser' med ulovlig eller utilsigtet brug af følsomme data er stigende. Personlige oplysninger om identitet og helbred er mere tilgængelige end nødvendigt. Sårbarheder indbygges bevidst i it-udstyr. Visse sikkerhedsbrister er negligeret i selve systemernes design og i kontrolrutinerne. De professionelle hackere bliver dygtigere. Håndholdte enheder, som bruges mere og mere, er utilstrækkeligt sikrede.

Anbefalinger

Digitaliseringen af den offentlige sektor kalder på rettidig politisk omhu.

- Vælg sikkert it-design fra starten. Inddrag eksperter og interessenter i en åben vurdering af risiko, pris og anvendelighed.
- Brug de bedst mulige tjeklister og sikkerhedsrutiner. Skærp kravene til operatører, komponenter, programmer og systemer.
- Dataminimering: Beskyt borgernes oplysninger. Undgå at samle og videregive flere personlige data end strengt nødvendigt.
- EU-integration: Brug sikre gateways ved sammenkobling af nationale it-systemer.
- Vedvarende indsats: Sikkerheden skal hele tiden tilpasses til nye trusler og teknologier.

Udgiver:

Teknologirådet

Toldbodgade 12

DK-1253 København K

Tel: 3332 0503

rtt@tekno.dk

Abonnement:

Gratis tilmelding pr. email: rtt@tekno.dk

Tidligere nyhedsbreve findes på www.tekno.dk/rtt.htm

ISSN: 1602-4311

Sårbare systemer

Politikerne har brug for bedre rådgivning, når de skal prioritere mellem sikkerhed, anvendelighed og pris. For at holde trit med både truslerne og den stigende anvendelse af informationsteknologi, må sikkerheden bestandig forbedres.

Politisk kan man på kort sigt forbedre sikkerheden ved at kræve anvendelse af de procedurer, der har vist sig bedst egnede til at lukke huller og styrke beredskabet. Tjeklisterne skal evalueres og bruges systematisk. Modforholdsregler skal være klar, hvis det går galt, og personalet skal være uddannet til at opretholde et højt sikkerhedsniveau.

Desuden kan man implementere princippet om dataminimering: Kun de strengt nødvendige persondata må lagres og videregives.

På længere sigt kan man skærpe kravene til it-producenterne, gøre sikkerhedscertifikater obligatoriske og eventuelt pålægge leverandøren et retsligt ansvar i tilfælde af sikkerhedshuller i software og hardware.

Skræmmende afsløring

Undersøgelsen er udført for Europaparlamentet af Teknologirådet i samarbejde med det hollandske Rathenau Institut og det tyske Institut for Teknologivurdering og Systemanalyse, ITAS.

"Den nye, skræmmende situation er, at sikkerheden er undermineret på alle computere og servere," påpeger Arndt Weber fra ITAS. I et af de hemmelige dokumenter, som whistlebloweren Edward Snowden fra det amerikanske efterretningsagentur NSA har afsløret, står der direkte: "Indsæt sårbarheder i kommercielle krypteringssystemer, it-systemer, netværk og brugernes kommunikationsudstyr".

"Selv om det nok fra begyndelsen har været rettet mod kriminelle, betyder det, at vi ikke længere kan være sikre på, at vores computere kan hemmeligholde fortrolige oplysninger, adgangskoder og produktideer," siger Arndt Weber. "Dertil kommer, at mange af de nye håndholdte enheder med jævne mellemrum sender informationer tilbage til leverandøren. Desuden anvendes mange mobile enheder uden tilstrækkelige adgangskoder, så data kan gå tabt eller blive aflyttet."

Klar og åben prioritering

Politikerne i mange lande har høje ambitioner om digitalisering. It-systemer kan spare tid og penge og samtidig hæve serviceniveauet. Sammenkobling af de nationale systemer kan fremme den europæiske integration.

"Men ofte er der et misforhold mellem de politiske ambitioner og det, man faktisk opnår," påpeger projektleder i Teknologirådet Anders Jacobi, der har koordineret undersøgelsen.

Politikerne vil gerne have så meget som muligt for pengene, men de mangler ofte tilstrækkelig indsigt i teknologierne og sikkerhedsproblemerne. Undersøgelsen har vist, at de politiske beslutninger ofte bliver truffet uden en klar og åben afvejning af de modstridende hensyn til sikkerhed, anvendelighed, samkøring og økonomi.

"Sikkerheden i et it-system er aldrig bedre end det svageste led," siger Anders Jacobi. "Høj sikkerhed kræver ekstra investeringer. I en eller anden grad vil det altid være nødvendigt at afveje og vælge mellem de modstridende hensyn til prisen, sikkerheden, anvendeligheden og ønsket om at kunne koble systemerne sammen på tværs af grænserne."

Derfor er obligatorisk risikovurdering af nye it-projekter en vigtig anbefaling. Interessenterne og offentligheden skal have lejlighed til at kikke politikerne over skuldrene, og uvildige eksperter skal analysere risikoen og vurdere fordele og ulemper ved forskellige udformninger af it-systemerne. Rådgivningen skal omfatte cost/benefit-analyser.

På den måde kan man sikre en åben

Biometriske pas - Case 1

De elektroniske pas med chip til foto og fingeraftryk blev indført i EU under indtryk af terrorangrebet på World Trade Center den 11. september 2001 og de efterfølgende terrorhandlinger i London og Paris. De europæiske politikere ville styrke grænsekontrollen og bekæmpe terrorisme og organiseret kriminalitet. Men de undervurderede i høj grad de tekniske og praktiske problemer, påpeger Linda Kool fra Rathenau Instituttet.

Landene har implementeret EU's forordning på hver sin måde, og de indsamlede data har langt fra samme kvalitet som for eksempel de fingeraftryk der bruges af politiet. De fleste lande lægger større vægt på hurtig og bekvem sagsbehandling end på høj data-kvalitet. Hvis man løser problemet ved at sænke tærsklen for et match mellem person og pas, undergraver man selve formålet, påpeger rapporten.

Krypteringen af de digitale foto er mangelfuld, og chippen kan aflæses på op til 10 meters afstand. Det giver mulighed for identitetstyveri. Fingeraftryk er bedre krypteret, til gengæld nægter myndighederne i nogle lande at udlevere adgangskoderne til visse andre lande.

Rapporten advarer kraftigt mod at samle de mange millioner persondata i centrale databaser og anvende dem til politimæssig efterforskning. Det vil uvægerlig føre til fejl og anklager på forkert grundlag.

Udgiver:

Teknologirådet

Toldbodgade 12

DK-1253 København K

Tel: 3332 0503

rtt@tekno.dk

Abonnement:

Gratis tilmelding pr. email: rtt@tekno.dk

Tidligere nyhedsbreve findes på www.tekno.dk/rtt.htm

ISSN: 1602-4311

evaluering af, hvordan de modstridende hensyn bliver tilgodeset.

Princippet om dataminimering

På langt sigt kan man udvikle computere, der isolerer databaser fra internettet. Med den nuværende teknologi vil det gå ud over systemets anvendelighed.

Men meget kan opnås ved at følge princippet om dataminimering, påpeger Anders Jacobi. Man skal lade være med at samle, generere og gemme flere data end de strengt nødvendige til formålet.

Der er mange muligheder for at identificere en person uden at gøre uvedkommende informationer tilgængelige: Decentral lagring af data, brug af pseudonymer, anonymisering, blokering af link til personoplysninger. Rapporten foreslår, at man opretter en vidensbase for disse teknikker, ofte betegnet 'Privacy by Design'. Den foreslår også, at man gør dem obligatoriske i offentlige it-systemer.

Et eksempel på det modsatte er de elektroniske pas med chip, der gemmer digitale fotos og fingeraftryk: "Man lægger en masse data ind nu, som man ikke rigtig bruger. Dertil kommer, at det er en fælleseuropæisk lovgivning, men man har glemt at tænke på, at den bliver implementeret meget forskelligt i de enkelte lande. Der er forskellige standarder for, hvordan man for eksempel gemmer fingeraftryk og optager digitale billeder. Det giver store sikkerhedsudfordringer," siger Anders Jacobi.

Gør det rigtigt fra starten

De elektroniske pas blev indført for at forbedre grænsekontrollen og bekæmpe terror og organiseret kriminalitet. Et andet formål er at automatisere paskontrollen.

Men hvis man på forhånd havde inddraget eksperter og interessenter i en åben og grundig overvejelse af fordele, ulemper og risici, kunne man have undgået mange problemer.

Problemerne spænder fra banale vanskeligheder, som for eksempel at genkende en person, der har fået en ansigtsløftning, via utilstrækkelig beskyttelse mod hackere og identitetstyve, til alvorlig risiko for, at de indsamlede informationer bliver misbrugt til utilsigtede formål.

"Det handler om at lave nogle ordentlige analyser af sikkerheden og beskyttelsen af personlige følsomme oplysninger inden man laver nye systemer, så man gør det rigtigt fra starten. Det lyder banalt, men det er faktisk vigtigt," siger Anders Jacobi.

Digitalisering i sundhedssektoren - Case 2

Der er store fordele ved it-systemer i sundhedssektoren, hvis de fungerer godt og er sikre. De kan føre til bedre behandling af patienterne, bedre overblik, færre fejl, mindre omkostninger og bedre forebyggelse.

Men det er helt afgørende, at alle parter kan have tillid til systemet. Patienterne skal beskyttes mod misbrug af deres helbredsoplysninger, enten de skyldes ulovlig indtrængen, systemfejl, forkert brug eller dårlige sikkerhedsprocedurer. Et stort anlagt britisk it-system måtte delvis opgives i 2011 på grund af utilstrækkelig datasikkerhed og modvilje fra det sundhedsfaglige personale og befolkningen i almindelighed.

De nationale systemer er meget forskellige. Rapporten anbefaler en gradvis tilnærmelse mellem systemerne, bygget på aftaler om principper og minimumsstandarder. Sikkerheden skal kontinuert overvåges og tilpasses til nye teknologier og nye trusler.

Sammenkoblingen af de nationale systemer kan med fordel ske gennem kontrolpunkter med gateway-servere, som automatisk tager højde for de forskellige identifikationssystemer og giver adgang til relevante oplysninger uden at sprede fortrolige data unødigt.

Samkøring af data kan afsløre identiteten

Et særligt problem er, at selv om man har anonymiseret personer, så kan de genidentificeres, når man samkører et sæt data med en anden database. Det kan for eksempel ske, når man anvender elektroniske patientjournaler til forskning, statistik og sundhedskampagner.

Der skal udvikles bedre metoder til at løse dette problem, og man bør overveje at give de berørte personer ret til at nægte samkøring, siger rapporten.

Brugernes tillid kan også forbedres ved at indføre obligatoriske, offentlige sikkerhedsvurderinger, som det allerede kendes i USA og Storbritannien.

Sammenkobling af it-systemer

Når it-systemer flettes sammen, opstår der mange problemer. De 28 EU-lande har forskellige sprog, love, teknologier, regler og ID-systemer. Beskyttelsen af data og personlige rettigheder giver derfor både tekniske og juridiske problemer.

En fuldstændig integration på højt sikkerhedsniveau har lange udsigter. I mellemtiden gælder det om at minimere de data der udveksles, så de ikke kan komme ud, hvor de ikke skal være.

Udgiver:

Teknologirådet

Toldbodgade 12

DK-1253 København K

Tel: 3332 0503

rtt@tekno.dk

Abonnement:

Gratis tilmelding pr. email: rtt@tekno.dk

Tidligere nyhedsbreve findes på www.tekno.dk/rtt.htm

ISSN: 1602-4311

Bestandigt nye udfordringer

Rapporten understreger, at it-sikkerhed er et dynamisk begreb. Sikkerhedsforanstaltningerne skal hele tiden justeres i et kapløb med hackere, cyberkriminelle og eventuelt fremmede magter. Desuden ændrer teknologierne sig hastigt.

For eksempel har den hurtige udbredelse af smartphones og andre enheder med netforbindelse åbnet nye muligheder for hacking og anden kriminalitet. Den udbredte brug af internettet som lager (Cloud Computing) er en sikkerhedsudfordring, der netop nu diskuteres intenst af sikkerhedseksperter.

Digitalisering af offentlige indkøb - Case 3

EU-kommissionen presser på for at få gennemført elektroniske udbud af de offentlige indkøb i EU senest i 2016. Det vil give store besparelser og få flere virksomheder til at deltage, mener kommissæren for det indre marked, Michel Barnier.

Men der er udbredt skepsis i mange EU-lande. Denne modvilje bør undersøges grundigt, siger Arnd Weber, ITAS.

"Er de samlede omkostninger virkelig mindre end i et papirbaseret system? Giver det mening at centralisere udbudsrunderne? Hvad er risikoen og omkostningerne ved en sådan centralisering i fremtiden?" spørger han.

Dokumenterne i et tilbudsmateriale skal kunne holde i en retssag. Derfor skal de sikres mod hackerangreb og manipulation. Risikoen for, at nogen skaffer sig adgang til at læse andres bud før de afgiver deres eget, kan imødegås ved en avanceret teknik: De indsendte bud krypteres, og dechifreringsnøglerne udleveres kun til afsenderen. Denne har ikke mulighed for at ændre teksten. På den anden side kan teksten ikke læses af andre før afsenderen udleverer nøglen – efter deadline.

Metoden er besværlig og fordyrende. Men den forhindrer, at man kan snyde ved at betale en hacker eller bestikke en insider.

Fra rådet til tinget er skrevet og redigeret af journalist Ebbe Sønderriis.

Kontakt: Projektleder Jørgen Madsen, jm@tekno.dk, tlf. 3078 5168.

De sidste fem numre af Fra rådet til tinget

Nr. 284: Dronerne er her!
Nr. 283: Strategisk energiplan – Forsinkelse koster dyrt
Nr. 282: Øget brug af medicinske selvtest
Nr. 281: Syntesebiologi til debat
Nr. 280: Borgerne om brugerbetaling, ventetidsgaranti og krav til patienterne

Udgiver:

Teknologirådet

Toldbodgade 12

DK-1253 København K

Tel: 3332 0503

rtt@tekno.dk

Abonnement:

Gratis tilmelding pr. email: rtt@tekno.dk

Tidligere nyhedsbreve findes på www.tekno.dk/rtt.htm

ISSN: 1602-4311