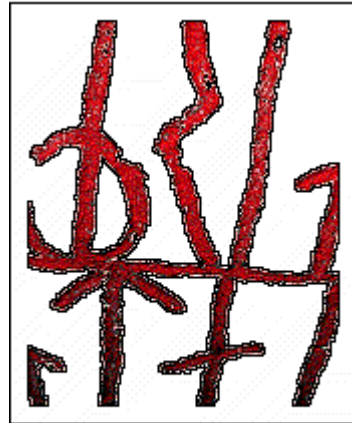


dagaz



Malmö 2001-04-23

Vet bankerna själva hur säkra deras IT-system är?

Banker och andra företag som erbjuder finansiella tjänster över Internet förtjänar inte kundernas förtroende. All försäkran om att man håller en hög säkerhetsnivå på sina Internettjänster är en kraftig överskattning. Idag har exempelvis ingen bank låtit sina tekniska lösningar bli granskade enligt fastställda standarder som ITSEC eller Common Criteria, utan de säkerhetslösningar som används är främst inriktade på kryptering och befintliga driftsrutiner.

I dagarna har det blivit offentligt att finansinspektionen kommer att genomföra en stor granskning av IT-systemen hos finansiella institut. Detta borde inte vara något bekymmer för en verksamhet som tar säkerhetsriskerna på allvar, men vår uppfattning är att så inte är fallet. Ett tydligt exempel på detta är att de tjänster som erbjuds för att utföra banktjänster över Internet, inte har blivit utvärderade enligt standarder som ITSEC eller Common Criteria.

De krav som finansinspektionen ställer på finansiella verksamheter är idag väldigt generella och omfattar inte några starka krav på informationssäkerhet. Ambitionen är att hålla fast principen att självreglering och lösningar som bygger på företagets eget ansvarstagande och delaktighet är att föredra. Frågan är om branschen är mogen att ta itu med dessa frågor, när avkastningskraven väger högre än säkerhetskraven. Vi är dock övertygade om att de företag som inte tar itu med säkerhetsproblemen, riskerar att sin framtida existens och därmed kundernas ekonomi.

När det gäller förhållandet mellan bankerna och dess kunder har de idag oftast en generös policy för hur kunderna skall hållas skadelösa för incidenter. Samtidigt kan man dock finna villkor som ställer orimliga krav. Det gäller bl.a. avtalsvillkor där banken friskriver sig för driftsavbrott och störningar i bankens datasystem och kommunikation mellan kunden och banken. Detta betyder i klarspråk att kunden erbjuds en teknisk lösning av sin bank som inte är upprättad eller utvärderad enligt etablerade standarder för informationssäkerhet samtidigt som kunden skall ta hela risken för fel som inträffar hos banken. Villkoren är skrämmande, inte minst med den bankkoncentration som vi ser idag!

Vår uppfattning är att informationssäkerheten för finansiella tjänster inte handlar om att enbart upprätthålla den personliga integriteten för kunden, utan även möjligheten att kunna utföra finansiella tjänster vilket blir allt svårare att utföra med manuell betjäning. Det måste finnas en klar och tydlig målbild hos bankerna när det gäller informationssäkerhet. Detta är inte något alternativ för verksamhetens fortsatta existens, utan en överlevnadsfråga.

Att utvärdera produkter och systemlösningar enligt standarder som ITSEC och Common Criteria, ger en tydlig signal på att säkerhet är viktigt. Bortser man från detta tvingar man sina kunder att ta onödigt stora risker, vilket bankerna underlåter sig att göra idag. Är inte säkerheten viktigare än så, förtjänar de inte att få kundernas förtroende.

John Wallhoff och Kjell Lautrup
Informationssäkerhetskonsulter på Dagaz AB

För mer information kontakta gärna:

John Wallhoff, john.wallhoff@dagaz.se, tel: 0709-279764 eller

Kjell Lautrup, kjell.lautrup@dagaz.se, tel: 0709-279755

Informationssäkerhetskonsulter, Dagaz AB

Dagaz AB Flexibelt företag - mycket kunskap

Förmågan att utnyttja möjligheterna som den snabba tekniska utvecklingen skapar, ställer höga krav på helhetssyn och teknisk kompetens. Både när det gäller att bygga nya eller utveckla existerande lösningar. Dagaz är ett flexibelt konsultbolag med erfarna konsulter som arbetar med informationssäkerhet och kommunikation. Konsulternas spetskompetens ger våra kunder stöd i den snabba utvecklingen. Vi har kontor i Stockholm och Malmö.

Besök gärna vår hemsida www.dagaz.se för mer information.

Dagaz AB

Box 38080
100 64 STOCKHOLM
tel. 08-55606260
fax. 08-55607260

Slagthuset
211 20 MALMÖ
040-108665
040-108666

WEB: www.dagaz.se
e-post: info@dagaz.se