

Gode sikkerhedssystemer fejler intelligent

Usmidige sikkerhedssystemer medfører dårlig sikkerhed. Derfor bør vi interessere os mere for, hvor gode systemerne er til at fejle, for fejle det gør de. Før eller siden. Kort sagt, er smidighed og evnen til at fejle en nøgle til at optimere sikkerhedssystemer.

Af Finn Kjær Jensen

Et par måneder efter 11. september 2001 løb en person gennem metaldetektoren i Sea-Tac Airport i Seattle og forsvandt i mængden. Utjekket på mere end én måde. Alle terminaler måtte tømme: gates, butikker, caféer osv. Og alle passagerer skulle genscreenes, herunder passagerer som allerede var gået om bord på flyene. Passagerer i tusindtallet måtte tilbage til start, driften af den interne undergrundsbane blev indstillet, alle flyafgange blev følgelig forsinkede og fly-

trafikken omlagt. Resultatet var utilfredshed, uro og usikkerhed.

Mekaniske kontra organiske systemer

Problemet med lufthavnssikkerhed og andre sikkerhedssystemer er, at når et sådant sikkerhedssystem fejler, så fejler det uhensigtsmæssigt, usmidigt. Det kollapser. Systemet er "sprødt". Det vil sige, at når det fejler, så fejler det fatalt. Det hele ramler og ikke blot dele af systemet. Systemets ufleksibilitet og uorganiske opbygning får det til at falde sammen som et ikkejordskælvsikkert højhus. Systemet er uden elasticitet. Det er opbygget af stive strukturer, der gør det sårbart og umuligt at genopbygge hurtigt.

Derfor er det på tide at tænke sikkerhed og sikkerhedssystemer på en ny måde. Måske skal løsninger på sikkerhedsmæssige problemer i mindre grad søges i ny teknologi og i højere grad søges med naturen som forbillede. Mekanisk kontra organisk sikkerhed, for nu at stille det forenklet op. Ofte antages avancerede teknologiske foranstaltninger at udgøre bedre løsninger end mindre avancerede. Men er dette velbegrunderet?

Intelligent sikkerhed

Ser vi for eksempel på hvor godt et sikkerhedssystem er til at fejle, så taler meget for at organiske systemer er mekanisk overlegne. Det gælder også i forhold til højteknologiske systemer. Og det at fejle "intelligent" bør være et centralt parameter for sikkerhedssystemer, foreslår Bruce Schneier, en af verdens førende og mere ukonventionelle sikkerhedseksperter.

Bruce Schneier har i sine skrivelser en lang række indsigtsfulde betragtninger om sikkerhed og sikkerhedssystemer. Han minder blandt andet om, at sikkerhedssystemer er anderledes end andre systemer, idet deres primære værdi ikke ligger i det, de muliggør, men i det, de umuliggør. Ifølge Bruce Schneier udgør koblingerne mellem systemer generelt et svagt led i enhver sikkerhedskæde, og han betoner at ingen sikkerhed er stærkere end det svageste led. Han fremkommer endvidere med påstanden om at sikkerhed er en konstant afvejning af fordele og ulemper, et såkaldt cost-benefit-kompromis. At en reduceret risiko på ét område almindeligvis betyder en forøget risiko på et an-

det område (blandt andet tyverisikring af luksusbiler ført til bilkapringer) fører til hans pointe om at det er meget vanskeligt at dokumentere om et sikkerhedssystem virker. For hvorledes måler man noget, som ikke sker?

På den baggrund introducerer Schneier ideen om, at se et sikkerhedssystemets evne til at fejle som en slags lakmus-prøve på dets generelle værdi.

De uundgåelige fejl

Vi bør interessere os meget mere for, hvor gode sikkerhedssystemer er til at fejle, for fejle det gør de. Før eller siden. Der gives ingen definitiv sikkerhed og ingen teknologiske tricks, der fjerner alle sikkerhedsrisici. Alle sikkerhedssystemer fejler. Hvilket både hverdagen og historien til fulde dokumenterer. Spørgsmålet vi bør stille, er altså ikke blot, hvornår de fejler, men i høj grad også hvordan de fejler. Vi bør stille krav til deres fejlevne. Med Schneiers ord må vi kort sagt udvikle sikkerhedssystemer, der fejler intelligent.

Alt for mange sikkerhedssystemer bryder sammen, når de bryder sammen ét sted. Et mindre problem ét sted, bliver hurtigt til et stort problem

over alt, og et stort problem, bliver hurtigt til en katastrofe. Dette gælder eksempelvis for atomkraftværker, for computernetværk med videre. Det er som med en bunker. Den kan have masser af beton og være solidt armeret, men bryder man først ind ét sted, da er den besejret. Bunkeren har kun ét "sikkerhedstrick".

Smidighed er sikkerhed

Organiske systemer derimod er robuste og dynamiske, idet de indretter sig smidigt og fleksibelt efter omgivelserne og kan tåle fejl. En enkelt fejl betyder ikke en kaskade af andre fejl og et totalt sammenbrud. Organiske systemer fejler også, men fejlene gøres tydelige, opdages hurtigt og gør at systemet kan genskabes.

Med afsæt i Schneier kan følgende tre råd foreslås:

Gør sikkerhedssystemet så enkelt som muligt

fra elektricitetsnettet til elektroniske netværk. Mange systemer fejler, og fejler fatalt, fordi de er for komplekse og uigenkennskuelige at styre. Opbyg derfor systemerne så de er nemme at håndtere i praksis, så det er nemt at opdage og korrigerer fejl. Decen-

traliser sikkerhedssystemet. Undgå systemer med kun én indgang, én kommandocentral, én hjerne. Fålden den, falder det hele. Sikkerhed bør nok tænkes i et helhedsperspektiv og koordineres, men systemet bør være opbygget af decentrale elementer, der på varierende og overlappende vis bidrager til sikkerheden.

Befolk sikkerhedssystemerne. Lad ikke systemet bero udelukkende på teknologi, men lad mennesker tage de væsentlige beslutninger. Mennesker begår fejl, naturligvis, men de kan langt bedre end maskiner korrigerer i forhold til ændrede omstændigheder, og de kan lære af deres fejl.

Der er stor forskel på noget, der kan gå galt og noget, der absolut ikke kan gå galt. Når det utænkkelige alligevel sker, så er det næsten altid umuligt at genoprette. Så når det nu før eller siden går galt, hvorfor så ikke opbygge nogle systemer, hvor det går galt på en begavet måde.

Den fortravlede person i Sea-Tac Airport i Seattle viste sig i øvrigt at være en ivrig afbudsrejsende.

Litteratur:

Beyond Fear af Bruce Schneier, Copernicus Boks 2003.