Fokus på IT-sikkerhed – ledelsens ansvar

af Janne Glæsel og Per Buchwaldt

Janne Glæsel

Per Buchwaldt

I den enkelte organisation – uanset om den er offentlig eller privat – er det nødvendigt, at alle niveauer i organisationen involveres omkring IT-sikkerhed. Først og fremmest er det vigtigt, at det erkendes af ledelsen, at IT-sikkerhed er en forudsætning for stadig vækst og konkurrencekraft, og for at samfundet som helhed kan være vel fungerende. Ledelsen bør sætte IT-sikkerhed højt på dagsordenen, fastlægge en overordnet IT-sikkerhedspolitik for organisationen og retningslinier for medarbejdernes adfærd. Fejlbetjening er en hyppig årsag til svigt i IT-systemer. Derfor er også bedre uddannelse af både brugere og IT-medarbejdere en forudsætning for sikker drift af IT-systemer.

Finanstilsynets vejledning nr. 9054

Den 20. februar 2003 udsendte det danske Finanstilsyn vejledning nr. 9054 om kontrol- og sikringsforanstaltninger på IT-området gældende for alle finansielle virksomheder uanset størrelse.

Det er en vejledning, hvis vigtighed er omvendt proportional med dens længde. Det er en prisværdig kort vejledning og det er en vejledning, som entydigt placerer ansvaret for IT-sikkerheden i danske finansielle institutioner på direktionernes og bestyrelsernes borde.

Vejledningen pålægger bestyrelserne et ansvar for at forholde sig til virksomhedernes IT-anvendelse, IT-organisation og IT-sikkerhed, idet det er fremhævet, at der i vurderingen skal indgå en konkret risikovurdering.

Det fremgår videre af vejledningen, at der skal være funktionsadskillelse i IT-organisa-

Janne Glæsel er advokat (H) og partner i Bech-Bruun Dragsted, hvor hun rådgiver offentlige og private virksomheder om IT-retlige og immaterialretlige forhold. ***Per Buchwaldt*** er civilingeniør, HD og ansat som IT-direktør i Bech-Bruun Dragsted. Han har tidligere i en årrække været IT-direktør i Alm. Brand. Per Buchwaldt er samtidig formand for DANSK IT – tidligere kendt som Dansk Dataforening.

Janne Glæsel og Per Buchwaldt er sammen med 6 andre medlemmer udpeget af Videnskabsminister Helge Sander som medlem af *Rådet for IT-sikkerhed*, der skal styrke hele IT-sikkerhedsarbejdet både i Danmark og i forhold til EU. Janne Glæsel er næstformand for rådet, der blev etableret den 1. januar 2003.

janne.glaesel@bechbruundragsted.com
per.buchwaldt@bechbruundragsted.com

tionen, som i øvrigt skal være klart defineret. Vejledningen stiller også krav om tilstedeværelsen af en IT-sikkerhedspolitik, tilstedeværelsen af forretningsgange i IT-organisationen samt en udarbejdet og afprøvet beredskabsplan.

Ændring af fokus og holdning til IT-sikkerhed

Der er ingen tvivl om, at disse krav for mange virksomheder i den danske finansielle sektor betyder et ændret fokus på og en ændret holdning til IT-sikkerhed. Og man kan vel tilføje – helt nødvendige ændringer. Ikke mindst Danske Banks oplevelser i foråret 2003 viser med al ønskelig tydelighed, hvor sårbare finansielle virksomheder er overfor "ITt-hændelser", selv i virksomheder som arbejder meget professionelt med drift og udvikling af IT-systemer. Hvor galt kunne det ikke være gået i en virksomhed, der ikke havde befundet sig på et så højt sikkerhedsmæssigt niveau som Danske Bank?

Havde Danske Bank ikke haft den nødvendige organisation og et dertil hørende gennemprøvet beredskab, kunne hændelsen formentlig have udviklet sig med langt værre konsekvenser end tilfældet blev. Det er derfor tankevækkende, at mange virksomheder – formentlig også i den finansielle sektor – reelt ikke har haft IT-sikkerhed på bestyrelsens bord. Håndteringen af IT-sikkerhed har i disse virksomheder typisk været overladt til IT-chefer, hvis opgave i denne sammenhæng nok ofte har været defineret til at sikre den interne og eksterne revisions accept af tilstandene; IT-chefer som hverken har haft gennemslagskraften eller ressourcerne til at at opbygge de nødvendige kontrol- og sikringsforanstaltninger. Det er formentlig en konstatering af forhold i denne retning, der har ledt det danske Finanstilsyn til at udgive den nævnte vejledning.

Det, der kan undre, er, hvorfor den øverste ledelse af virksomheder ikke mere "uhjulpet" engagerer sig i håndteringen af IT-sikkerhed. Er det fordi virksomhedsledere alene ser IT-sikkerhed som bureaukrati og omkostninger? Eller er det fordi virksomhedsledere har en anden opfattelse af risikoen for at opleve IT-sikkerhedsproblemer eller ganske enkelt har vanskeligt ved at forstå problemstillingerne og betydningen af IT-sikkerhed?

Øget sikkerhed kan medføre en mere effektiv ressourceudnyttelse

Danske Banks oplevelser burde betyde, at virksomhedsledere – herunder i særdeleshed ledere i finansielle virksomheder – fremover engagerer sig på samme måde, som når de bedømmer forretningsmæssige risici, kreditværdighed eller udviklingsprojekter. Gribes et sådant engagement rigtig an, kan et øget fokus på IT-sikkerhed faktisk resultere i parallelle gevinster i form af mere effektive forretningsgange og mere effektiv ressourceudnyttelse.

Eksempelvis vil en øget sikkerhed omkring idriftsættelse af nye eller reviderede IT-systemer – det der i fagsproget kaldes ændringskontrol – resultere i bedre oppetid på grund af et færre antal systemfejl.

Eller for at tage et eksempel i den helt anden ende af skalaen – så vil central opdatering af koden i den nye generation mobiltelefoner dels øge disses sikre funktion, dels give anledning til en standardisering af anskaffelsen af mobiltelefoner og dermed åbne for, at anskaffelsen af sådanne enheder kan ske indenfor rammekontrakter med tilhørende volumenrabatter.

I det hele taget er der grund til i virksomhederne at fokusere på sikkerheden og økonomien omkring mobile enheder. Den reelle pris på en ny mobiltelefon med indbygget PDA og adgang til at fungere over nettet overstiger jo

efterhånden prisen på en stationær pc'er. Det er "telefoner", der vil få fuld adgang til virksomhedernes interne netværk, således at mails og kalenderoplysninger modtages umiddelbart over de nye GPRS netværk, som mobiltelefonselskaberne nu udbyder, ligesom der vil kunne etableres fuld adgang til virksomhedernes systemer – for eksempel systemer til skadesopgørelse eller systemer til pensionsrådgivning. Det betyder, at der vil kunne opnås nogle helt nye fordele i forsikringsselskaberne. Men det betyder også introduktionen af nye sikkerhedsrisici, hvor mobiltelefoner skal håndteres på samme vis som pc'ere – hvordan distribueres der software, hvordan skabes der sikker adgang, hvordan undgår man at stjålne mobiltelefoners software bliver tilgængelig for andre, hvordan testes nye mobiltelefoner – fortsæt selv listen.

Svarene på disse spørgsmål vil gå hånd i hånd med en øget sikkerhed.

IT-sikkerhed er også et spørgsmål om branchesamarbejde

Danske Banks håndtering af nedbruddet i foråret 2003 viser, at et væsentligt element i minimeringen af konsekvenserne for bankens kunder var et samarbejde med andre bankdatacentre om håndtering af eksempelvis lønudbetaling. Så udover, at de enkelte virksomheder i den finansielle sektor skal overveje, hvordan IT-sikkerheden i virksomheden skal håndteres, så er der også grund til at pege på behovet for at brancher overvejer, hvorledes samarbejder kan etableres, således at konsekvenserne af kritiske IT-nedbrud kan minimeres. Det forekommer eksempelvis nærliggende at overveje, hvorledes pensionsudbetalinger fra liv- og pensionsforsikringsselskaber kan sikres i tilfælde af et større nedbrud hos selskaber af denne art.

Der er hjælp at hente

Når virksomhederne og deres ledelser engagerer sig i forbedring af IT-sikkerheden er det, på dette som på andre områder, ikke nødvendigt at opfinde den dybe tallerken igen. Der findes udmærkede standarder på området – fra standardiseringsorganisationer og fra mange leverandører ligesom der efterhånden findes et righoldigt sortiment af publikationer. Virksomhedernes ledelser kan derfor udmærket tillade sig at instruere deres sikkerhedsansvarlige i at tage udgangspunkt i sådanne standarder – en første opgave for den øverste ledelse kan derfor være at få identificeret de relevante standarder på området

En god skabelon for arbejdet er den nye vejledning 9054 fra det danske Finanstilsyn nævnt ovenfor, der så at sige sætter overskrifterne. Et udgangspunkt for det mere detaillerede arbejde med IT-sikkerhed kan – i Danmark – være Dansk Standards DS 484-1 Norm for edb-sikkerhed, basale krav og DS 484-2 Norm for edb-sikkerhed, skærpede krav, hvor førstnævnte tager udgangspunkt i den internationalt anerkendte standard fra British Standard BS 7799 Information security management. Derudover eksisterer der flere publikationer, som den øverste ledelse kan benytte til hurtigt at få et overblik over de aktuelle problemstillinger på IT-sikkerhedsområdet – DANSK IT har i samarbejde med KPMG udgivet publikationen "IT-sikkerhed i små og mellemstore virksomheder", som også godt kan inspirere ledelsen i større virksomheder. Og Dansk Industri har udgivet "Ledelse af IT sikkerhed – for forretningens skyld" og "Trusler mod virksomhedens IT-sikkerhed".

Brugerinvolvering er et must

Som nævnt indledningsvist har der i hvert fald i nogle virksomheder været en tendens til, at arbejdet med IT-sikkerhed har været begrænset til IT-afdelingen. Det har måske til en vis

grad givet mening, hvor brugerne af IT-systemer – sagt lidt for firkantet – alene skulle være opmærksomme på, at sikkerhedskoder skulle opbevares og anvendes fortroligt.

Den tid er forbi!

Brugere af IT-systemer er i dag en af de vigtigste kilder til sikring af et sikkert IT-miljø. Ligesom i trafikken skal brugere, der bevæger sig på internettet være opmærksomme på, hvilke risici de påtager sig – hvor færdes de, hvilke oplysninger afgives, hvilke filer downloades, downloades der ulovlige musik- og filmfiler, som virksomheden kan risikere et erstatningskrav omkring, videredistribueres sådanne filer, er medarbejderne koblet til fildelingsmekanismer, optræder medarbejderne i chat rooms med virksomhedens ip-adresse, hvilke filer sender medarbejderne ud af virksomheden, er man bevidst om, at hjemme-pc'ere kan udgøre en sikkerhedsrisiko, hvis de også anvendes direkte på nettet, kobler man sine bærbare pc'ere på andre netværk osv.?

Hertil kommer, at risikobilledet er under konstant forandring, hvorfor virksomhedernes beskyttelsesmekanismer risikerer at være bagud. I sådanne situationer vil det alene være medarbejdernes fornuftige adfærd, der vil kunne forhindre sikkerhedsbrud.

Fra centralt hold vil der kunne iværksættes forholdsregler til imødegåelse af trusler af den her nævnte karakter. IT-chefen kan imidlertid sjældent løfte den opgave det er, at påvirke adfærd og værdier i virksomheden. Processen med at gøre IT-sikkerhed til alles anliggende kræver ledelsens klare opbakning. Sikkerheden står og falder for en stor dels vedkommende med medarbejdernes adfærd.

IT-sikkerhed som karrierevej

Som bekendt kommer ingenting af ingenting – undtagen lommeuld. Forbedret IT-sikkerhed kræver ledelsesengagement og ressourcer. Det er væsentligt, at virksomhederne råder over IT-sikkerhedsekspertise, der er uddannelsesmæssigt ajour og som betragter IT-sikkerhed som et karrierevalg. Tidligere var der i en del virksomheder en tendens til at IT-sikkerhed blev overladt til medarbejdere, som på forskellig vis var blevet "til overs" i organisationerne eller som måske blev placeret indenfor området i en retrætestilling. Det er et fuldtidsarbejde at holde sig ajour med udviklingen indenfor IT-sikkerhed – der er derfor ikke længere plads til medarbejdere, som ikke er uddannet og ajour. Gør IT-sikkerhed til en karrierevej og ikke et sidespor.

Mange – især mindre virksomheder – vil formentlig ikke kunne tiltrække kvalificerede fuldtids IT-medarbejdere, hvorfor opgaven bør overvejes outsourcet. I øvrigt på linie med andre opgaver i mindre IT-organisationer. Initiativer af denne art kræver også et engagement fra virksomhedernes øverste ledelse – og i øvrigt omhyggeligt formulerede aftaler med leverandører.

IT-sikkerhed er en del af god ledelsesskik

En fornuftig IT-sikkerhed vil være en nødvendig forudsætning for overlevelse, men vil også kunnegå hånd i hånd med effektiv virksomhedsdrift. Opgaven og ansvaret ligger på ledelsens bord og skal løftes som en del af god ledelsesskik.