Redigeret af Anders Mørkbak Bruun

ERHVERVSJURA

TRUSLEN BAG SKÆRMEN

IT-SIKKERHED Der er næppe megen tvivl om, at den største risiko mod virksomheders it-sikkerhed sidder ca. 40 cm fra skærmen. Jo højere op i virksomhedens hierarki, der er fokus på it-sikkerhed, jo større er chancen for, at man arbejder seriøst med den bedste måde at sikre data.

LARS BO LANGSTED
Professor, Juridisk Institut, Aalborg Universitet

IDENTITETSTYVERI, *phishing*, *hacking*, industrispionage og meget andet slemt truer derude i *Cyberspace*.

Hver gang der har været et tilfælde – som f.eks. sidste uges angreb ved hjælp af en falsk PBS-mail – flyder medierne over med gode råd og anbefalinger om, hvordan vi som brugere kan forsøge at minimere risikoen for at blive ofre for en "net-tyv".

Vi må aldrig åbne vedhæftede filer, medmindre vi ved, hvad de indeholder, vi skal ikke besvare mails, som vi ikke er helt sikre på karakteren af, vi skal forsøge at undgå "inficerede" hjemmesider (hvordan man så genkender sådan nogle), vi skal altid huske at opdatere vores programmer, og vi skal i det hele taget – som de gode råd altid slutter af med: Tænke os om, når vi kommunikerer elektronisk eller færdes på nettet.

Lidt som når man besværgende siger til sine børn:

»Opfør dig nu ordentligt.«

DET ER ALT sammen meget godt, og det er helt rigtigt, at hvis vi følger rådene, så er risikoen for at blive udsat for kriminelle pirater i rummet trods alt relativ beskeden for den private bruger.

En ting er imidlertid, hvordan vi agerer som privatpersoner, når vi bruger vores egen hjemmecomputer (eller den beskattede firmacomputer, når vi bruger den privat), noget andet er, hvordan virksomhederne håndterer den potentielle it-kriminalitet. Vi ved fra undersøgelser, at virksomhederne bliver udsat for angreb via deres IKT-udstyr, og vi ved også, at de fleste virksomheder har sikkerhedsforanstaltninger af forskellig art.

Det er klogt, idet et "tyveri" der sker gennem virksomhedens it-system kan lamme virksomheden fuldstændigt eller med et slag berøve den alle dens forretningshemmeligheder.

Der findes ikke megen traditionel, fysisk kriminalitet med tilsvarende skadevirkninger.

DET ER IMIDLERTID et spørgsmål, om der er tilstrækkelig fokus på, hvor vanskeligt det er at sikre virksomheden mod virtuelle angreb, og hvor faldgruberne ligger. At den største sikkerhedsrisiko sidder ca. 40 cm fra skærmen, er der vel ingen tvivl om. Uanset hvor godt vi sikrer systemet, vil den menneskelige faktor altid udgøre et problem, og det vil den af mange grunde.

Det er således ikke usædvanligt, at man i virksomheder overlader spørgsmålet om it-sikkerhed til it-afdelingen. Det kan synes fornuftigt – men er farligt.

Der er slet ingen tvivl om, at den rent tekniske sikring af systemerne – filtrering af mails, vedligehold af antivirusprogrammer, opdateringer, automatisk backup m.v. – er i de bedste hænder dér.

Når disse tekniske eksperter imidlertid skal sikre mod dårlig brugeradfærd og uautoriseret adgang til systemet, kan det let gå galt. Hvem kender f.eks. ikke de virksomheder, hvor man skal skifte password hver tredje måned?

Hvordan husker medarbejderne mon deres password efter at have været igennem nogle skift?

Enten skriver de password det ned og har det liggende på en gul *post-it* ved siden af skærmen, eller også vælger de noget, de er sikre på at kunne huske – og kan de det, er det lige så let for uvedkommende at regne det ud.

DET KAN OGSÅ være, at it-afdelingen skriver ud til alle mellemlederne i virksomheden, at de skal registrere alle data, der behandles af medarbejderne, klassificere disse data og registrere, hvilken sikkerhedskategori de forskellige data tilhører – og derfor om de kan sendes med krypterede eller ukrypterede mails, om de kræver særlige logon procedurer at komme ind til, om de kun må bæres på særlige *USB-sticks* med adgangsprogrammel osv. osv.

Hvad skal en stakkels mellemleder med det?

Medmindre man er ansat i PET eller i en finansiel virksomhed, kan det være mere end vanskeligt at gennemskue relevansen af denne "ordre", og derfor vil efterlevelsen høre til de lavere prioriterede opgaver i den kommende tid – og det bliver den så ved med.

UDEN PÅ NOGEN måde at ville kloge mig på, hvorledes man teknisk set kan bedre datasikkerheden, er der ingen tvivl om, at jo højere op i virksomhedens hierarki, der er fokus også på it-sikkerhed, jo større er chancen for, at man arbejder seriøst med den bedste måde at sikre net-op denne virksomheds data.

Der afsættes så de fornødne midler ikke blot til den tekniske side af sagen, men også til "oplæring" af medarbejderne, og frem for alt øger det medarbejdernes bevidsthed om vigtigheden af databeskyttelsen, hvilket kan virke umådeligt fremmende for deres prioritering af opgaven.

I DEN NYE selskabslov fra 2009 har man da også "ophøjet" kravet om, at bestyrelsen bl.a. skal påse, at »der er etableret de fornødne procedurer for risikostyring og interne kontroller« fra et punkt i forretningsordenen til at være med i lovens hovedbestemmelse om en bestyrelses pligter.

I reglerne om god selskabsledelse fra april i år hedder det tilsvarende, at en »effektiv risikostyring og intern kontrol er en forudsætning for, at det øverste ledelsesorgan og direktionen hensigtsmæssigt kan udføre de opgaver, der påhviler disse organer. Det er derfor væsentligt, at det øverste ledelsesorgan påser, at der er en effektiv risikostyring og effektive interne kontroller«.

TILSVARENDE fremhæver revisorernes revisionsstandard for overvejelser i forbindelse med afdækning af besvigelser, at en risikofaktor bl.a. er »utilstrækkelig forståelse i den daglige ledelse for informationsteknologi, hvilket giver informationsteknologimedarbejderen mulighed for misbrug«.

Som nævnt ovenfor giver det desværre også meget let udefrakommende lettere spil, ganske enkelt fordi den daglige ledelse – det vil typisk sige en eller flere direktører – ikke har fornøden fokus på it-området, og dermed heller ikke på it-sikkerheden.

Også af den grund (og fordi de eneste, der kan sige til direktøren, hvad han skal beskæftige sig med, er bestyrelsen) er det vigtigt, at bestyrelsen tager emnet op og forholder sig til det faktiske niveau for it-sikkerheden, det ønskede niveau for it-sikkerheden og sørger for, at der igangsættes fornuftige tiltag, der kan ses og forstås af de enkelte medarbejdere.

DEN ALMINDELIGE bestyrelsespassivitet i forhold til it-sikkerhed i almindelige virksomheder vil næppe være ansvarspådragende for de enkelte bestyrelsesmedlemmer, selvom virksomheden eller tredjemand måtte lide et tab, der kunne være undgået ved en større fokus fra bestyrelsens side. Men omvendt kan det ikke afvises, at bestyrelsen i en virksomhed, hvor spørgsmål om datasikkerhed er helt central, og hvor bestyrelsen intet foretager sig i relation til sikkerhed, i værste fald vil kunne ende med et erstatnings- eller strafansvar.

Der er således ingen grund til at tøve:

Kære bestyrelsesmedlem, hvordan ser det ud med it-sikkerheden i det selskab, du sidder i bestyrelsen for? ■

HOVEDPUNKTER

- I den nye selskabslov fra 2009 kræves det, at bestyrelsen skal påse, at der i virksomheden findes de fornødne kontroller af it-sikkerheden.
- Reglerne om god selskabsledelse fra i år understreger ligeledes behovet for, at det øverste ledelsesorgan påser, at der er effektive interne kontroller.

FARE Ansatte udgør den største trussel mod it-sikkerheden i virksomheder. Modelfoto: Michael Altschul