



# ARBEJDSPLADSENS TRYGGE RAMMER

**Hov! Hvem er du? I hvilken afdeling arbejder du? Det er de færreste der bliver anråbt på gangen med de ord. Men det er nødvendigt at have mere fokus på hvilke personer, der bliver lukket ind i organisationen både ad hoveddøren men også gennem de elektroniske veje. Det og meget mere skal sikkerhedsstandard DS 484 – med medarbejdernes hjælp – sikre.**

For det handler ikke kun om den fysiske sikkerhed i ministerierne og institutionerne. I en større organisation er det svært at vide, hvem der går ind og ud, er på besøg, til møder og hvem der potentielt kunne stjæle dokumenter eller viden fra organisationen.

## Få tjekket sikkerheden

Som alt andet kan sikkerheden også tjekkes. Princippet er også kendt fra detailhandlens brug af såkaldte 'mystery shoppers'. En 'mystery shopper' er hyret gennem et konsulentfirma til at tjekke butikens serviceniveau ved at udgive sig for at være kunde. Ved test af organisationens sikkerhed handler det ikke om at tjekke serviceniveau, men derimod om at tjekke den fysiske sikkerhed og datasikkerheden.

Sikkerhedstjekket har teoretisk baggrund i 'social engineering', der handler om at manipulere og misbruge godtroende personers viden og grundlæggende ønske om at hjælpe andre. For det er det, et sikkerhedstjek går ud på – misbrug af godtroende og medarbejdere, der gerne vil hjælpe.

## Den største svaghed

Henrik Zangenberg, der er managing director hos konsulentfirmaet Gartner, har som led i et projekt om 'security awareness' lavet et såkaldt kontrolleret indbrud hos en større erhvervsvirksomhed i Danmark. 'Security awareness' handler om at sætte fokus på virksomhedens sikkerhed, og at finde hullerne, der kan misbruges.

Det kontrollerede indbrud bliver aftalt med ledelsen, og det handler om, at konsulenten skal komme ind i virksomheden og finde et navngivent fortroligt dokument, uden at have et adgangskort eller passwords. Formålet er at få konkrete bud på forbedringer og ord på de sikkerhedshuller, der er i virksomhedens sikkerhedsprocedurer. Vel at mærke udelukkende ved at benytte sig af manipulation.

"Den største svaghed for sikkerheden i en virksomhed er, at medarbejderne gerne vil hjælpe," siger Henrik Zangenberg. "Det er omgangsformen og den virksomhedskultur vi har i Danmark, der gør det let at bruge 'social engineering' og dermed manipulere medarbejderne."

## Det kontrollerede indbrud

Det var ikke svært for Henrik Zangenberg at lave det kontrollerede indbrud. Han skulle bare udnytte medarbejdernes gode tro og behjælpelighed.

Konkret lod han som om, han havde glemt sit adgangskort og udnyttede en godtroende medarbejder, der lukkede ham ind. Han gik rundt på gangene og fandt et modelokale med en intern telefonliste og en telefon. Den fulgte han systematisk. Ringede

op og udgav sig for at være fra it-afdelingen. Under dække af et generelt problem på serveren og af gerne at ville afhjælpe dette problem for brugeren fik han lokket et brugernavn og et password ud af en godtroende medarbejder. Det krævede en håndfuld opringninger, men det lykkedes.

Derpå fandt han et tomt kontor, hvor computeren stod tændt uden at være låst. Han hørte nabokontoret om kollegaen snart var tilbage, og ved at stikke en løgn om et møde, der åbenbart var glemt, fik han lov til at vente i det tomme kontor. Med døren lukket, et brugernavn og et password var det ingen sag at finde det navngivne fortrolige dokument i det centrale dokumenthåndterings-system.

Alt i alt tog missionen halvanden time. Uden brug af vold, hærværk eller andre korporlige metoder, kunne han træde ud af virksomheden med rapporten gemt på en usb-nøgle klar til at afrapportere sikkerhedsbristen til sin kunde. Og han mener at kunne gentage sit kontrollerede indbrud uden problemer.

## Medarbejderen skal være med

En test som denne kan gøre sikkerhedsproblemerne konkrete. For i en travl hverdag kan det være svært at se det fornuftige – og ikke det besværlige – i at huske at låse computeren, lukke den åbne dør i stueetagen, der lukker frisk luft ind eller at spørge den ukendte kollega på trappen i hvilket kontor hun arbejder, før hun lukkes ind. Den udfordring kender Lone Strøm, der er vicedirektør og ansvarlig for implementeringen af sikkerhedsstandard DS 484 i Økonomistyrelsen. "Der er brug for konkrete eksempler og illustrationer for at medarbejderne forstår vigtigheden af at implementere en sikkerhedsstandard som DS 484," siger hun.

Men når en omfattende standard som DS 484 skal implementeres, så kræver det omfattende planlægning og udvikling af kreative metoder for at involvere medarbejderne i standardens budskab om at håndtere data og sikkerhed på fornuftig vis.

## En quiz skal der til

I Økonomistyrelsen blev der derfor lavet en intern kampagne, hvor medarbejderne kunne deltage i en konkurrence ved at fotografere eventuelle brud på sikkerheden eller være med i en quiz på intranettet om sikkerhed.

Informationssikkerhed handler nemlig både om organisatorisk og teknisk sikkerhed, og begge skal udtænkes og gentænkes med et vist interval. "Vi kan sikre vores data nok så meget ved at implementere, overvåge og løbende ajourføre forskellige foranstaltninger bestående af tekniske kontroller, politikker, praksis, procedurer og organisatoriske tiltag," siger Lone Strøm. "Men vigtigst af alt er, at vi får medarbejderne til at huske sikkerheden i det daglige arbejde."