It-sikkerhed: et spørgsmål om dannelse

Det er ved at gå op for verden, at vi alle kan blive udsat for, at computeren eller mobiltelefonen bliver hacket. Hvis vi skal højne it-sikkerheden, må vi alle påtage os et ansvar.

Der *er* en risiko for, at ens computer kan blive hacket. Og det er en risiko for alle: Fra teenagere med mobiltelefoner til sofistikerede it-brugere med lange uddannelser. Den realitet er svær at forholde sig til, for det føles jo som om, det kun er mig selv, der kan se, hvad der er på computeren eller mobiltelefonen foran mig.

Jeg mener, at der er behov for have it-sikkerhed som en del af vores digitale dannelse, så vi håndterer den risiko fornuftigt. Det betyder, at vi både skal sørge for, at den er så lille som muligt, og at vi kan tåle det, hvis uheldet er ude.

Det er længe siden, at data-sikkerhed handlede om at låse kontoret, og man hurtigt opdagede det, hvis en mappe med dokumenter var blevet stjålet. På en computer kan data kopieres, uden at man mærker det, og der kan være brudt ind i ens computer fra internettet, uden at man kan se det. Det er faktisk helt almindeligt, at vi først opdager cyber-angreb længe efter, de har fundet sted.

Alle skal tage deres forholdsregler

Vi har brug for at skabe en kultur og en teknologi, hvor data på den ene siden omgås forsvarligt, og hvor sikkerhed på den anden side ikke er besværligt. Uanset om man er gymnasieelev, forsker, virksomhedsejer eller privatperson, bør man tage nogle enkle forholdsregler for at mindske risikoen. Allerede nu er der to meget simple forholdsregler, som man skal tage – som kan sammenlignes med den måde, du sikrer dit hjem på: Du låser døren og tegner en forsikring. Den låste dør svarer til, at du holder din computer og mobil opdateret, så de værste sikkerhedshuller er dækket – det gør det noget mere besværligt for hackere. En god tommelfingerregel er, at man skal lade sin computer eller mobiltelefon opdatere samme dag, den beder om det, i stedet for at udsætte det dag efter dag, fordi det er lidt besværligt.

Søren Debois er lektor ved IT Universitetet i København, hvor han forsker og underviser i it-sikkerhed og digitalisering.
debois@itu.dk

Og en forsikring svarer til at have sikkerhedskopier, så du ikke mister vigtige data, hvis du bliver hacket. En god tommelfingerregel er, at data, man ikke kan undvære, skal findes *to* steder udover den computer, de "bor" på, for eksempel i skyen *og* på en ekstern disk. På den måde kan man tåle, at man for eksempel bliver hacket og mister både computer-kopien og kopien i skyen, eller at ens hus brænder, og man mister både computer-kopien og den eksterne disk.

Men du skal også spørge dig selv, om dine data, billeder og filer overhovedet kan *tåle* at blive stjålet. Måske har du private billeder, e-mails eller dokumenter, som du *slet ikke* vil have på internettet. Er de måske så følsomme, at det ville være ubærligt om de blev lækket? I så fald skal de slet ikke ligge på en computer, for det er *altid* en mulighed, at den bliver hacket.

Digitale indbrud – ikke kun for specialister

Hvis vi skal højne it-sikkerheden generelt, er den enkeltes indsats vigtig. Der findes i dag websider, der viser hvordan man kan skaffe sig adgang til for eksempel en computer via sikkerhedshuller i styresystemer og programmer, der ikke er opdaterede. Det kræver ingen programmeringserfaring eller særlig indsigt at følge sådan nogle vejledninger.

Man skal derfor være omhyggelige med både egne og andres data. På arbejde håndterer man måske følsomme sundhedsdata; som privatperson billeder af kæresten og børnene. De data er ikke beskyttet, hvis jeg ikke gør en indsats for, at de ikke bliver stjålet og lækket til internettet.

It-sikkerhed er dermed ikke kun et anliggende for eksperter, virksomheder og myndigheder; det er et anliggende for alle. Ligesom sikkerhed i hjemmet eller trafikken handler it-sikkerhed meget om almindelige fornuftige forholdsregler. Det handler om gode vaner – "digital dannelse".

Der forskes i disse dage intensivt i nye metoder til at sikre it-systemer, og det *er* muligt at lave it-systemer, der er meget vanskelige at trænge ind i, for eksempel ved at bruge moderne kryptografi og moderne højniveau-programmeringssprog, der med et slag eliminerer hele klasser af de fejl, der udnyttes af hackere. For de fleste privatpersoner og mindre virksomheder er det imidlertid slet ikke besværet værd at bruge så megen tid og energi på at sikre it-enheder; her vil man komme rigtig langt med de simple forholdsregler nævnt ovenfor. ■