HELT SIKKER?

MARIA LILLEMOEN
INFORMASJONSRÅDGIVER VED HØGSKOLEN I GJØVIK

I 1986 kom det første dataviruset som infiserte en PC. Viruset het Brain A, det var skapt av to brødre i Pakistan og hensikten med viruset var å vise at datidens operativsystem, MS DOS, var usikkert. Allerede i 1949 omtalte John von Neumann i et essay hvordan et dataprogram kunne bli designet til å reprodusere seg selv. Datavirus har altså lenge vært omtalt og lagd, men virus er bare en liten del av hva vi som brukere må sikre oss selv og datamaskinen mot i 2012.

Faktum er at vi digitaliserer det vi kan, sikre kilder sier at iPaden til og med har utkonkurrert ukebladene på utedoen på hytta. Digitalisering fører til at vi er mer utsatt enn noensinne for angrep på våre digitale gjenstander, systemer og oss selv. Angrep er én fare, samtidig må IT-systemene vi benytter være av god nok kvalitet for blant annet å sikre personvernet. Mange fikk nok med seg at Kenneth fra Oslo fikk blottlagt selvangivelsen sin og at Altinn måtte stenge løsningen for innlevering av selvangivelsen for alle i Norge i to dager.

Så hva er løsningen? Vi ønsker ikke å gå tilbake til «steinalderen» med penn og papir som hovedredskap i hverdagen. Informasjonssikkerhet er selvfølgelig løsningen! Og informasjonssikkerhet, **det** kan vi på Gjøvik. Basisprinsippene innen informasjonssikkerhet kan oppsummeres i CIA; C for confidentality, I for integrity og A for authentication. Konfidensialitet (C) står for at når vi kommuniserer med andre så skal bare vi forstå hva vi snakker om og forstå beskjeder vi sender. Mange bruker Skype for å kommunisere, det er både enkelt og praktisk, men blant annet Norsk senter for informasjonssikring (NorSiS) anbefaler å ha et bevisst forhold til hva du bruker Skype til. Skal du diskutere forretningshemmeligheter kan det være lurt å finne et annet verktøy. Integritet (I) i informasjonssikkerhet betyr at du skal kunne stole på at informasjonen er korrekt. Det kan være dokumenter som sendes ut til flere ledd i en organisasjon som man må være sikker på at innholdet ikke kan endres umerkelig. Autentisering (A) vil si at du skal vite hvem du snakker med og at ingen sitter i mellom og endrer informasjonen.

Norwegian Information Security laboratory (NISlab) ved Høgskolen i Gjøvik feirer 10 års jubileum i år og aldri har det vært større behov for forskning på informasjonssikkerhet. Utfordringen er at bildet endrer seg konstant, det er en kamp mellom de som lager sikre systemer og angriperne. De fleste har hørt om og kanskje mottatt e-post fra Nigeria der folk blir bedt om å overføre penger. 99,99% av oss svarer aldri på dette, men noen få gjør det og er grunn god nok for svindlerne til å fortsette og pøse ut disse e-postene. En ting er mer eller mindre bevisste handlinger, her handler det om å tenke logisk og spørre seg selv om det er sannsynlig at ukjente ønsker å gi deg ti millioner kroner? En annen type utfordring er botnet. Botnet er nettverk av datamaskiner kontrollert av kriminelle der disse kaprede maskinene kan brukes til kriminelle formål. Det finnes eksempler på at PC-er til intetanende mennesker er blitt brukt til å lagre barneporno på. Da har angriperne funnet en bakdør inn i PC-ene, ofte via usikrede trådløse nettverk eller via utdatert programvare.

NISlab ved Høgskolen i Gjøvik forsker på de tekniske detaljene innen informasjonssikkerhet, de forsker på digital etterforskning, kryptologi og biometri, deriblant sikkerhet av passordsystemer. Dette er uvurderlig kunnskap i dagens samfunn.

Så hva kan man som databruker med helt ordinær IT-kunnskap gjøre? Oppdater programvaren, ha brannmur aktivert og antivirus installert, og bruk sunn fornuft i interaksjonen med andre. Og når det gjelder sosiale medier er det best å formidle hva du har gjort, ikke hva du skal gjøre! For sikkerhets skyld.