IT sikkerhedsmøde tirsdag d. 23. januar 2018

Uddrag fra mødet :

Eksperter advarer om "kæmpe sikkerhedshul" på din computer

IT-kriminelle finder hele tiden nye måder at tjene penge på – og en af de metoder, der er blevet ekstremt udbredt er såkaldt "ransomware". Skadelig software der låser dine filer og kræver løsepenge for at få adgang til dem igen.

Dansk politi advarer forbrydere; Vi er klar med et "supervåben".
Der peges på flere ting der kan føre til ransomware. It-sikkerhedseksperten nævner bl.a. et specifikt problem, der er et "kæmpe sikkerhedshul" på folks computere. At brugerne ikke har opdateret programmet Adobe Flash Player.
Anbefalingen er derfor, at man opdateret programmet jævnligt, og hvis man er i tvivl om, hvorvidt man har den nyeste version, så slet den gamle udgave og installer igen.

Guf for hackere;

Du betaler med din egen sikkerhed, hvis du bruger den lette løsning og logger ind med Facebook i steder for at oprette et nyt login.
Det kan føles mere bøvlet at oprette en ny profil, når man eksempelvis vil bruge Netflix, men ifølge eksperterne er det bedre end at logge ind via Facebook. Hver 3. i DK bruger Netflix.
Hvis nogen har adgang til din Facebook-konto, har de adgang til alt muligt andet. Lad være med at bruge Facebook som en sikkerhedsmekanisme, for det er det bestemt ikke, siger Rådet for Digital Sikkerhed.
Det nytter ikke noget at have samme password til NemID og Facebook.
Høj sikkerhed kræver forskellige passwords, og det er ifølge sikkerhedseksperten langt bedre at koncentrere sig om, hvordan man husker de forskellige passwords, end hvordan man laver et nemt et.

Pas på når du slutter smart hjemmeudstyr til nettet.

Stadig mere hjemmeelektronik kan kobles på nettet, men det kan være en åben virtuel dør for hackere.
Hvert eneste apparat der er forbundet med internettet, kan nemlig hackes og dermed overtages af andre.
Computere og mobiltelefoner ved de fleste, at man bør beskytte, og de er bygget på en måde at de nemt kan opdateres og sikres. For typen af opkoblede enheder er der slet ikke den samme fokus på sikkerhed. Mange apparater er lavet af små, uafhængige producenter, som har mere fokus på at få tingene ud over rampen end på sikkerhed.

Kriminelle og aktivister får adgang til flere og bedre cyberværktøjer.

Det er en fortsat tendens, at viden og værktøjer til at hacke bliver tilgængelige for flere.
Hackerværktøj bliver delt og handlet på internettet, og når f.eks. ny malware eller viden om sårbarheder bliver delt, er hackerne hurtige til at udnytte og videreudvikle dem. Ofte er de hurtigere end virksomheder og myndigheder er til at beskytte sig mod sårbarhederne.