Views: 1521

Hvis Du Har Været Udsat For En Sikkerhedsbrist

Hvis du har været udsat for et angreb, er det vigtigt at få:

- Skiftet dine passwords (skift til bl.a. Itslearning, mail og trådløst netværk – Klik her >>)
- Tjekket din maskine igennem – evt. med flere sikkerhedsprogrammer.

For at tjekke din maskine igennem, findes der flere programmer. Du bør læse under afsnittet "programmer" på denne side.

Om Sikkerhed

Som en del af sikkerhed på ens computer bør man have installeret et program, som sikrer en (så godt som muligt) mod misbrug af ens computer. Eksempler på misbrug fra en overtaget computer kan være:

- Brug af computeren til udsendelse af spam
- Brug af computeren, så en eventuel hacker udgiver sig for at være ejer af computeren.

- Låse computeren og kræve løsepenge (ransomware).
- Misbruge personlige oplysninger eks. kodeord, bankinformation osv.)
- …
- …

Man kan ikke altid beskytte sig mod trusler som ovenstående – men man kan sikre sig så godt som muligt. Derfor har DKCERT og de dansk universiteter fremstillet en række videor om udbredte trusler mod informationssikkerheden. Du kan finde dem via dette link – Klik her >>

Ligeledes finder du en rækkke gode råd om sikkerhed på Sikkerdigital.dk – klik her >>

Programmer

En af mulighederne er at installere et program, som beskytter mod virus, malware osv. Der findes en række programmet, man skal betale for (som ansat skal du kontakte IT afdelingen). Der findes også en række gratis, som du kan søge efter. Det kan eks. være.:

- AVG (Win og Mac)
- Bitdefender (Win og Mac)
- Windows Defender (kommer typisk installeret fra start på en Windows 10 PC)
- Avast (Win og Mac)

Ovenstående er gratis software, som selvfølgelig kan have sin berettigelse – dog vil man typisk få et bedre produkt ved at have et betalt beskyttelsesprogram program.

Du kan læse en artikel om nogle af ovenstående programmer – Klik her >>

Der findes også Online programmer, som kan scanne din computer igennem. Igen kan vi ikke anbefale nogle og kan ikke garantere, at de finder de skadelige ting, som kan være på din computer. Nedenfor har vi dog linket til et par af dem, som er på markedet.

- Trend Micro (Mac & Win): https://www.trendmicro.com/en_us/forHome/products/housecall.html
- F-Secure (Win): https://www.f-secure.com/da_DK/web/home_dk/online-scanner
- ESET (Win): https://www.eset.com/us/home/online-scanner/
- Bitdefender (Mac & Win): https://www.bitdefender.com/toolbox/

Din Egen Adfærd

Endvidere handler sikkerhed på din computer ikke kun om virus, malware osv. Den største ”trussel” er dig selv – eller en som misbruger din computer.

Det betyder, at du skal agere på en fornuftig måde. Derfor er der en række gode anbefalinger nedenfor:

- Lås din computer, når du ikke er ved den.
- Brug sikre password – genbrug ikke password flere steder.
- Åben aldrig mails og filer, du ikke forventer at få eller fra personer, du ikke kender.
- Krypter den information, du har på eksterne medier som usb eller eksterne harddisks, hvis det ikke må komme i andres hænder.
- Hold dit software opdateret, ikke kun styresystemet, men også de programmer du

bruger.

- Undgå ukendte netværk. Trådløse gratis netværk på ferien eller andre steder i det offentlige rum er fristende, men også en stor risiko.

Beskyttelse Af Information

Til ansatte er der lavet en sikkerhedspolitik på DMJX, som du kan finde under: DMJX Guide – Intern Service – Telefoner og IT – IT-Sikkerhedspolitik

Desuden anbefaler vi at se videoen fra DKCERT og de danske universiteter – Klik her >>