# En ordbog – for en sikkerheds skyld!

**by Mette Nielsen - tirsdag, maj 05, 2015**

http://perspektiv.tdc.dk/en-ordbog-en-sikkerheds-skyld/

# En ordbog – for en sikkerheds skyld!

## Virus. Malware. Ransomware. Firewall. Phishing. Botnet. Zero Day Exploit. Social Engineering. Spam. Er du overvældet? Listen med udtryk, der har at gøre med din it-sikkerhed, er lang og indviklet. Her får du hjælp til at finde vej i termerne – for en sikkerheds skyld!

En nylig undersøgelse fra Dansk IT tegner et billede af it-sikkerheden i danske virksomheder. Heraf fremgår det, at 68% af de it-ansvarlige mener, at det er den enkelte brugers manglende kendskab til it-sikkerhed, der er den største udfordring for virksomheden it-sikkerhed. Desuden har malware og phishing ramt hhv. 69% og 60% af virksomhederne. Dette er meget høje tal, som ingen ville acceptere, hvis der var tale om indbrud eller hærværk i hjemmet. En af grundene til de høje tal kan være, at det er svært for den enkelte at forstå, hvad truslerne egentlig er og hvad it-sikkerhed handler om.

Som computerbruger støder du på nye og indviklede sikkerheds- og trusselsudtryk overalt på din vej. En besked fra it-afdelingen kan derfor også fremstå kryptisk. Fortvivl ej! Her får du en liste over de mest anvendte termer samt en forklaring, der kan hjælpe dig på vej. Hvis du forstår, hvad der menes med de forskellige udtryk og termer, vil du være bedre i stand til at hjælpe sikkerheden på vej.

> Som computerbruger støder du på nye og indviklede sikkerheds- og trusselsudtryk overalt på din vej

## Din ordbog til sikkerhed

**Malware (skadelig kode):** Begrebet er sammensat af de engelske ord ”Malicious Software”, og det er en fællesbetegnelse for programmer med ondsindet indhold. Malware omfatter for eksempel virus, orme, trojanere, crimeware, spyware og adware.

**Virus:** Et program, som uden din tilladelse ændrer måden, hvorpå din pc arbejder. En virus spreder sig ved at forbinde sig selv til en fil eller program. Når denne fil eller program så flyttes fra én pc til en anden, for eksempel via mail eller USB-nøgle, så spredes virussen. Virus på computeren kan være særdeles skadelig.

**Kryptering:** Et udtryk for, at man gør information ulæselig for alle andre end modtageren af informationen. Kryptering anvendes til at højne sikkerheden for udveksling af informationer.

**Ransomware:** En type malware, der krypterer data på en computers harddisk. Efterfølgende vil de it-kriminelle så forlange en løsesum for at genskabe de krypterede data. Offeret vil ikke kunne åbne de krypterede filer uden den korrekte dekrypteringsnøgle. Først når løsesummen er betalt, vil den it-kriminelle (måske) sende den nødvendige nøgle, der kræves for at dekryptere de "kidnappede" filer.

Læs også: Ransomware imod kommunerne – what's next?

**Spam:** Uopfordrede mails, oftest sendt med kommercielle motiver. Det vil sige personer eller firmaer, som ønsker at sælge dig noget, som du ikke har bedt om. Spam sendes typisk som masseforsendelser, selvom dette ikke altid fremgår tydeligt af mailen.

**Sårbarheder (eller sikkerhedshuller):** Små fejl i programmer, der kan udnyttes til uretmæssigt at få adgang til din computer. Som regel vil det foregå uden din viden eller accept. Producenter af programmerne retter disse fejl løbende, men det er op til dig og din virksomhed at sørge for at foretage opdateringer.

**Firewall:** En enhed, der analyserer og filtrerer netværkstrafik på baggrund af et sæt regler, som skal forhindre ondsindet trafik i at trænge ind i et netværk. Din firewall skal løbende vedligeholdes for at yde størst mulig beskyttelse. Den mest udbredte anvendelse af firewalls er som forbindelse til internettet. En firewall skal ikke alene blokere for indgående trafik, men bør også filtrere udgående trafik, således at alle meddelelser – udefra og indefra – kontrolleres og blokeres, hvis de ikke lever op til de aktuelle sikkerhedskrav.

**Social Engineering:** Kunsten at manipulere personer til at udføre bestemte handlinger eller til at røbe fortrolige informationer, som fx brugernavn og adgangskode til en computer. I de fleste tilfælde vil kontakten mellem angriberen og offeret ikke være fysisk, men ske via telefon eller mail.

**Phishing:** En teknik, hvor en it-kriminel via en forfalsket webside eller mail udgiver sig for at være en betroet virksomhed eller organisation. Eller afsenderadressen kan forfalskes til at fremstå, som om beskeden kommer fra en ven eller bekendt. Formålet er at aflure personfølsomme informationer fra offeret, såsom kreditkortoplysninger.

Læs også: Du deler kontor med din største it-trussel

**Botnet:** En samling af computere, som er blevet inficeret med malware, og som kan fjernstyres af it-kriminelle til at få adgang til meget stor kommunikations- og regnekraft, som derefter kan benyttes til kriminelle formål. Botnets kan således fx benyttes til at udsende spam-mails og installere mere malware på computerne, eller de kan anvendes til DDoS-angreb.

**DDoS:** Står for "Distributed Denial of Service" og dækker over et angreb, hvor mange computere

samtidig kommunikerer med en server eller et system, hvorved det overbelastes og bryder ned.

Læs også: DDoS-angreb er blevet kraftigere

**Zero Day Exploit:** Udnyttelse af et sikkerhedshul, som der endnu ikke eksisterer en rettelse til.

Link: Læs en længere ordbog med forklaringer på sikkerhedsverdenens termer