Du deler kontor med din største it-trussel

by Mette Nielsen - tirsdag, marts 24, 2015

http://perspektiv.tdc.dk/du-deler-kontor-med-din-stoerste-trussel/

Du deler kontor med din største it-trussel

Når vi snakker om cybertrusler, så tænker vi tit på skumle kriminelle, der er skjult bag netværk og internet. Men truslen kan også sidde lige ved siden af dig på kontoret. Måske er truslen dig selv! Sikkerhedsorganisationen DK Cert peger på, at 79 % af de it-sikkerhedsansvarlige mener, at den største it-sikkerhedstrussel skal findes i brugerne selv. En stor del af it-sikkerheden handler derfor om at have den rigtige indstilling til internettet: nemlig at være opmærksom og varsom.

Klokken er ni om morgenen, og Jens møder på sit arbejde. Han starter med at lave sig en kop kaffe. Han tænder for computeren og taster sit password, som er hans fødselsdato. Han åbner sin mailboks og bliver positivt overrasket over en af sine mails, som kommer fra banken: ”Tillykke med fødselsdagen!”. Han trykker glad på linket i mailen. Senere modtager han en mail fra sin søster. Han synes godt nok, at der er mange stavefejl i mailen, men den var nok bare skrevet lidt hurtigt. Hun har sendt ham en zip-fil, som han klikker på for at åbne og derefter gemmer.

Efter at have brugt formiddagen med personfølsomme løndata i et excel-skema, som han midlertidigt har gemt på skrivebordet, går han til frokostpause. Da han kommer tilbage er alle hans og kollegernes filer blevet krypteret, gjort ubrugelige og henover skærmen er der en besked, der kræver en løsesum, hvis de vil have deres filer igen. Jens forstår ikke, hvordan han kan være blevet hacket.

Frygten for indbrud og tyveri af ejendom gør, at vi udøver sikker adfærd, når vi forlader kontoret. Vi lukker for vinduerne, vi tænder alarmen, og vi låser døren. Men adfærden i relation til internettet bør være lige så varsom. Det giver ikke mening at være mere bange for, at tyven får fingrene i vores sparegris – for hvad hvis han gør vores filer ubrugelige, får adgang til personfølsomme oplysninger eller vores forskning?

Ransomware og Advanced Persistent Threats

Eksemplet med Jens ovenfor er sket flere steder, end man umiddelbart skulle tro. I virkeligheden var mailen fra banken falsk og zip-filen fra søsteren var en virus. Afsenderne fingerede kun, at komme fra Jens’ bank og kontaktliste. Dette eksempel er slet ikke opspind. Det er hverdag for mange computerbrugere i Danmark. Der er tale om såkaldt ”ransomware”.

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

De sidste måneder har ransomware hærget og angrebet mindst seks kommuner: Gribskov, Nordfyns, Fredensborg og Faxe Kommune, samt to fortsat unavngivne. Når man bliver inficeret med ransomware, så bliver filerne krypteret, og en truende besked på skærmen kræver penge af brugeren, før man kan få adgang til filerne igen. Når computeren er med i et delt netværk, gør det derved, at hvis én computer bliver inficeret, kan malwaren inficere andre.

En anden form for trussel, der i 2014 blev mere udbredt, er ”Advanced Persistent Threats (APT)”, som i højere grad er en malware, der bruges ved spionage. APT går for eksempel efter forskningsresultater, firmakritiske data eller personfølsomme data. Sikkerhedseksperter vurderer, at der går gennemsnitligt otte måneder fra angrebets start, til det bliver opdaget.

Hvad kan du gøre?

Selv med en rigtig god it-sikkerhedspolitik er der ingen garanti for, at arbejdspladsen aldrig vil blive angrebet. Hackerne bliver ved med at finde nye smuthuller. Men hvis medarbejderne får en indføring i, hvordan de skal forholde sig til elektronisk kommunikation, kan virksomheden hurtigt reducere risikoen for ovennævnte type angreb.

Læs også: IT-sikkerhed, er det mit problem?

5 ting DU kan gøre for at undgå virus på din arbejdsplads:

1. **Sørg for at have gode kodeord**
   Hvis dit password er ”123456”, ”abc”, din fødselsdato eller lignende, så er det meget nemt for hackere at gætte. Sørg for at skifte dine passwords regelmæssigt og benyt både store bogstaver, små bogstaver og tal.
2. **Følg it-sikkerhedspolitikken**
   Sørg for at bekendtgøre dig med it-reglerne og sikkerhedspolitikken. Følg regelsættet og hav det gerne stående et sted, hvor du kan se det dagligt.
3. **Hvis noget virker mærkeligt, så er det mærkeligt**
   Sørg for at opbygge en sund skepsis. Hvis noget virker for godt til at være sandt, så er det det sikkert også. Vær fx opmærksom og på vagt ved ”underlige” henvendelser, mail fra fremmede eller uventede mails fra venner og bekendte.
4. **Krypter og tag backup af dine filer**
   Skulle uheldet være ude, er det først rigtig skidt, hvis store mængder data går tabt eller bliver stjålet. Krypter personfølsomme, firmakritiske eller andre fortrolige dokumenter og tag backup af alt, hvad du laver.
5. **Hvis du er i tvivl…**
   … Så er du ikke i tvivl. Hvis en mail, en vedhæftet fil eller et link ser mærkelig ud, så åbn ikke filen eller tryk ikke på linket. Hvis arbejdspladsen har et antivirusprogram, kan du scanne filen for virus, inden du åbner den. Og sidst, men ikke mindst – hvis din computer begynder at opføre sig mærkeligt, så gå med det samme til din it-afdeling.

Link: DK Cert: Brugerne svækker sikkerheden