Gode råd om IT-sikkerhed for mindre virksomheder

Det er afgørende for virksomhedernes økonomi, troværdighed og overlevelsesmuligheder, at der er fokus på IT-sikkerheden.

IT-sikkerheden skal være i orden med henblik på at undgå, at IT-kriminelle stjæler følsomme oplysninger i form af fx kundedata, netbankoplysninger, personaleoplysninger, patenter, mønsterbeskyttelse, rettigheder og andre forretningshemmeligheder som fx kildekode eller tegninger, eller kopierer kontaktoplysninger fra virksomhedernes mailprogram og bruger disse oplysninger til at sende spam.

De gode råd:
I det følgende gives en række gode råd og herunder også praktisk vejledning til, hvordan man som virksomhed sikrer sine systemer. Rådene er skrevet til helt små virksomheder uden egen server.

1 Sørg for at holde IT-systemer opdateret

Sårbarheder i styresystemet (fx Windows XP) og andre programmer (fx Adobe Reader, Adobe Flash, Java og QuickTime) udnyttes ofte af de kriminelle.

Sørg for, at styresystemet og andre programmer bliver opdateret, hvorved sårbarhederne fjernes. Slå om muligt automatisk opdatering til eller check for opdateringer hos producenten.

Det er også muligt via et program at undersøge, om alle programmer er opdaterede. For yderligere information se evt. www.opdaterdinpc.dk, som henvender sig til private borgere.

For at minimere det antal programmer, der skal opdateres, bør virksomheden kun installere de programmer, der er behov for. Samtidig bør virksomhederne med jævne mellemrum undersøge, om de har programmer installeret, som ikke anvendes, og som derfor bør slettes.

Sørg for at benytte software, der ikke er så gammel, at den ikke længere supporteres af leverandøren.

2 Sørg for at installere en sikkerhedspakke

Det anbefales at installere en sikkerhedspakke på virksomhedens pc'ere. Sikkerhedspakken bør indeholde:

En firewall, der primært sikrer mod IT-kriminelle, der forsøger at komme i kontakt med virksomhedens IT-udstyr.

Et antivirusprogram, som undersøger, om der ligger skadelige koder i virksomhedens IT-udstyr.

Et spamfilter, der forhindrer virksomheden i at modtage spammails.

Et phishingfilter, som forhindrer adgangen til en usikker side, hvorfra der fx kan blive installeret skadelige programmer eller stjålet personlige oplysninger.

Virksomheden bør sørge for, at sikkerhedspakken opdateres ofte – helst dagligt og automatisk, for ellers yder den ikke den optimale beskyttelse. Sørg for jævnligt at lave en totalscanning af harddisken.

Virksomheden kan se mere information om sikkerhedspakker og deres kvalitet her: http://www.av-comparatives.org/images/stories/test/corporate/Corporate_May_2009.pdf

Såfremt virksomheden har mere end ca. 5 pc'ere, bør der etableres centrale sikkerhedsløsninger – som fx en central firewall, således at virksomhedens øvrige IT-udstyr – fx netværksudstyr – er beskyttet.

3 Sørg for at indstille sikkerhedsniveauet i browseren

Indstil sikkerhedsniveauet i browseren, så virksomheden altid bliver spurgt, inden informationer, filer og programmer overføres til computeren. Hermed bliver der mulighed for at kontrollere, at der ikke installeres uønsket kode.

Det anbefales, at administratorrettigheder ikke tilknyttes den enkelte bruger, men at alene en udpeget administrator kan sikre, at computerne kan opdateres. Bemærk dog, at det herefter er administratorens ansvar, at operativsystem, antivirusprogram mv. altid er opdateret.

Sørg for automatisk at slette personlige oplysninger, når browseren lukkes ned. Der kan fx være tale om besøgte hjemmesider eller information indtastet herpå.

4 Sørg for at slå krypteringen til på virksomhedens trådløse netværk

Krypteringen beskytter virksomheden mod, at andre bruger netværket, og dermed bruger de ressourcer, som virksomheden betaler for. Vær opmærksom på, at WEP-kryptering ikke er sikker, så brug som minimum WPA- og helst WPA2-kryptering.

IT-kriminelle bruger ofte andres trådløse netværk, når de begår kriminalitet. Derved opnår de, at det er virksomheden, der bliver mistænkt og ikke dem.

Vælg en krypteringsnøgle, som er meget svær at gætte for uvedkommende, og giv eventuelt det trådløse netværk et anonymt navn, eller skjul navnet, så det ikke tiltrækker unødig opmærksomhed.

5 Sørg for at bruge gode og sikre kodeord

Kodeord er den vigtigste beskyttelse af virksomhedens interne fortrolige oplysninger. Sørg for at anvende et langt kodeord, som er svært at gætte. Hold det hemmeligt.

For at opnå ekstra sikkerhed er det en god idé at benytte både store og små bogstaver, tal og symboler i adgangskoder. Et kodeord bør være mindst 8 karakterer langt.

Et godt kodeord er at konstruere en sekvens af tilfældige små og store bogstaver, specialtegn og/eller cifre, som kan huskes uden at skrive det ned. Brug fx en sætning eller en sekvens af ord, som er lette at huske. Vælg fx det første bogstav i ordene fra en linje i en sang:
”Der var engang en abe, den boede i en skov” bliver til ”Dve1adbi1s”.

Et dårligt kodeord er et ord, der kan slås op i en ordbog.

For at øge sikkerheden opfordrer vi til at skifte kodeord regelmæssigt.

6 Sørg for at udvise sikker adfærd på internettet

Virksomheden skal forholde sig kritisk til de hjemmesider, der besøges, de programmer, der downloades og installeres samt de mails, der modtages.

Vær især opmærksom på chat og instant messaging, vedhæftede filer, vedhæftede links, sociale netværk, sider med porno og falske hjemmesider, der udgiver sig for at tilhøre et kendt brand.

Er tilbuddet for godt til at være sandt, er det formentlig svindel. Jobtilbud via mail om lettjente penge er ofte forbundet med kriminalitet. Virksomheden vinder aldrig en uventet lottogevinst, og der skal aldrig betales for at få gevinsten.

Ligeledes er det vigtigt at være opmærksom, når oplysninger skal sendes ud af virksomheden – heraf specielt fortrolige oplysninger. Send kun denne type oplysninger til personer, hvis identitet kan bekræftes.

Såfremt spammails slipper igennem spamfilteret, må de ikke åbnes og bør slettes med det samme.

7 Sørg for at tage sikkerhedskopier af virksomhedens vigtigste informationer

Virksomheden bør vurdere, hvilke informationer der er mest forretningskritiske – personaleoplysninger, patenter, økonomisystemet eller andet.

Da virksomheden altid skal have adgang til disse informationer, skal der tages backup af dem. Virksomheden bør tjekke, at back-up’en virker og kan ligeledes overveje at kryptere denne. Endelig bør virksomheden fastlægge, inden for hvilken tidshorisont backup’en skal kunne reetableres.

8 Søg hjælp fra eksperterne

Når virksomhedens IT-mæssige kompleksitet bliver for stor, eller hvis der opstår en konkret trussel eller sikkerhedshændelse, er det en god ide at kontakte en rådgiver eller IT-support firma.

FINANSRÅDET
DI Organisation for erhvervslivet
DANSK ERHVERV