De ti vigtigste IT-sikkerhedsinitiativer
- en kortfattet guide for mindre og mellemstore virksomheder

IT-sikkerhed i mindre og store virksomheder
Det er af afgørende betydning for virksomhedernes økonomi, troværdighed og overlevelsesmuligheder, at de får IT-sikkerheden under kontrol. Mindre og mellemstore virksomheder har ofte ikke de nødvendige kompetencer og ressourcer, der skal til for at vurdere, hvilke IT-sikkerhedsinitiativer de har behov for. Det gør ikke virksomhedernes behov for at sikre deres IT-systemer mindre, men det betyder, at det er nødvendigt med en prioritering.

ITEK, Dansk Industri og Ministeriet for Videnskab, Teknologi og Udvikling har med denne lille guide rettet mod de mindre og mellemstore virksomheder forsøgt at pege på de ti ting, som virksomhederne typisk bør give højeste prioritet. Der er lagt vægt på en række initiativer, som er karakteriseret ved, at de er på den ene side kan hæve IT-sikkerheden betydeligt, og på den anden siden ikke koster en bondegård. Det er vigtigt, at virksomheden forholder sig til disse ti punkter. I mange tilfælde behøver virksomheden ikke selv ansætte personale til at varetage opgaverne, men kan vælge at få dem løst af en ekstern partner.

Guiden er en introduktion til IT-sikkerhed, og formålet har ikke været at dække alle facetter af IT-sikkerhed. For at få et mere tilbundsgående indblik i IT-sikkerhed henvises der til de øvrige publikationer, som er udgivet af ITEK og DI, og som kan findes på www.it.di.dk og de øvrige publikationer der er udgivet af Rådet for IT-sikkerhed, og som kan findes på www.it-sikkerhedsraadet.dk.

De ti råd:

IT-sikkerhed er ledelsens ansvar
Ledelsen er ansvarlig for virksomhedens IT-sikkerhed, fordi det til enhver tid er en ledelsesopgave at sørge for at give forretningen de bedste muligheder. Det betyder, at ledelsen skal minimere de omkostninger, der kan opstå i forbindelse med IT-sikkerhedshændelser, og at investeringerne i IT-sikkerhed er i overensstemmelse med værdien af de aktiver, man forsøger at sikre.

Ledelsen skal desuden sikre at virksomheden kan føres videre i det tilfælde, at uheldet er ude, og systemerne går helt eller delvist ned. Ledelsesopgaven omfatter også personalet, og det er vigtigt, at ledelsen sikrer, at personalet hele tiden har tilstrækkelig med viden om IT-sikkerhed til at træffe de rette valg, når de anvender virksomhedens IT-systemer.

Troværdighed og tillid er afgørende for at drive forretning. Det er derfor vigtigt, at virksomheden ikke kommer til at eksponere forretningskritiske informationer, som forskningsresultater og oplysninger om kunder og leverandører. Dette sker i stadig hyppigere grad fordi virksomhederne har voksende elektronisk samspil med eksterne interessenter. I denne betydning bliver virksomhedens IT-sikkerhed en konkurrenceparameter. IT-sikkerhed skal derfor på ledelsens dagsorden og ikke parkeres hos den IT-ansvarlige.

Lav en overordnet IT-sikkerhedspolitik
Ledelsen skal i samarbejde med den personaleansvarlige og den IT-ansvarlige sørge for, at virksomheden udarbejder en overordnet IT-sikkerhedspolitik. Dette skal ske for at sikre, at de ressourcer virksomhederne bruger på IT-sikkerhed, anvendes optimalt. Politikken skal fastslå de

overordnede rammer, indenfor hvilke virksomhedens konkrete IT-sikkerhedsinitiativer skal tages. Politikken skal indrettes således, at den understøtter virksomhedens værdier og forretning, er i overensstemmelse med de gældende retningslinier for virksomheders medarbejdere og er anvendelig i forhold til eksisterende og fremtidige IT-systemer.

Den overordnede politik behøver i omfang ikke at overstige en side. Indholdet bør specificere politikkens formål, en beskrivelse af de typer aktiver som virksomheden skal sikre, samt hvilke overordnede krav sikkerheden skal leve op til - herunder lovgivning, branchespecifik regulering og adfærdskoder.

Identificer aktiverne og vurder risici
Hvis man spørger en virksomhed om hvilke aktiver den er i besiddelse af, vil man ofte få et svar der inkluderer bygninger og produktionsfaciliteter. Men ofte vil virksomheden ikke tænke på at angive dens data, informationer og viden som et aktiv. Dette uagtet at disse aktiver som regel er virksomhedens mest værdifulde og afgørende for virksomhedens forretning.

Virksomheden skal identificere aktiver og estimere deres værdi. Efterfølgende skal virksomheden vurdere, hvilke økonomiske konsekvenser det vil have, hvis aktivet ødelægges helt eller delvist. Virksomheden skal gøre den største indsats for at sikre de aktiver, som der er størst afhængighed af, og som har størst risiko for at blive ødelagt. For de vigtigste aktiver skal der udarbejdes en beredskabsplan, så forretningen kan fortsættes, selv om dele af IT-systemerne ikke fungerer i en periode.

Virksomheden skal altså kortlægge på hvilke måder den er afhængig af IT og derefter udarbejde og implementere en plan der har til formål at beskytte dens aktiver i et omfang svarende til deres værdi.

Skab en IT-sikkerhedskultur
Blandt virksomhedens medarbejdere skal der skabes en IT-sikkerhedskultur gennem uddannelse, adfærd, ændret moral, opmærksomhedsskabende initiativer og en operationel af medarbejderne godkendt og forstået IT-sikkerhedspolitik. Formålet med at skabe en sikkerhedskultur i virksomheden er, at enhver, der interagerer med IT-systemerne, hele tiden er bevidst om relevante sikkerhedsrisici, at fortage præventive handlinger, som kan minimere risikoen for en IT-sikkerhedshændelse og at forbedre sikkerheden i eksisterende IT-systemer. Et andet formål er at sikre, at virksomhedens politik faktisk lever op til medarbejdernes rettigheder.

Det betyder, at man fra den tekniske side skal indtænke IT-sikkerhed i enhver udvikling af eksisterende systemer. IT-sikkerhed er ikke noget, som man bare kan tilføje en dag man har tid og råd. Det er noget, der skal integreres med IT-systemerne og bygges op sammen med IT-systemerne.

I forhold til de almindelige brugere er det vigtigt at sikre, at disse er uddannede til at forstå, hvilken risiko deres handlinger udgør. Enhver ansat bør tænke på IT-sikkerhed i forhold til de opgaver, vedkommende løser for virksomheden. Enhver ansat bør kende til og efterleve virksomhedens IT-sikkerhedspolitik. I praksis kan dette ske ved, at man udarbejder en IT-sikkerhedspjece til alle medarbejdere, med gode råd om passwords, antivirus, internetadgang og e-mail. Hermed skærpes opmærksomheden og ansvaret præciseres og fordeles.

Virksomheden kan siges at have en IT-sikkerhedskultur, når medarbejderne tænker på og opfører

sig på nye måder, der tager højde for IT-sikkerhed.

IT-sikkerhedsansvarlig
Ledelsen skal gøre en person i virksomheden ansvarlig for virksomhedens IT-sikkerhed. Afhængig af virksomhedens størrelse og behov kan denne person naturligvis beskæftige sig med andre opgaver end IT-sikkerhed. Personen skal koordinere virksomhedens IT-sikkerhedsinitiativer. Formålet er at ledelsen gennem én person kan sikre, at dens IT-sikkerhedspolitik føres ud i livet i overensstemmelse med forretningsstrategien.

Den ansvarlige skal være med til at udforme og vedligeholde virksomhedens IT-sikkerhedspolitik. Herunder skal personen tage initiativ til revision af politik og strategi og indgå i samspil med den personaleansvarlige om at skabe de fornødne informationsinitiativer blandt medarbejderne.

På den tekniske side skal den ansvarlige have kendskab til virksomhedens IT-systemer og sørge for, at disse er ordentligt dokumenterede. Den ansvarlige skal enten selv følge udviklingen på området eller sørge for at nogle andre gør det. Formålet er, at identificere nye trusler mod virksomhedens eksisterende IT-systemer og på denne baggrund være i stand til at vurdere hvilke fremtidige initiativer, der skal tages. Den ansvarlige skal også tage højde for systemernes fysiske sikkerhed.

Opdatering af software
At arbejde med IT-sikkerhed er en kontinuerlig proces. Der findes hele tiden nye huller i eksisterende software, nyt software har ofte nye huller, der findes hele tiden nye metoder til at angribe systemerne på og endelig er mange systemer ikke sat op på den måde som det var tiltænkt fra producentens side. Sådanne huller kan give virksomheden store omkostninger hvis de ikke lukkes i tide.

Virksomheden skal derfor have et overblik over hvilke typer software den er i besiddelse af, og måden det er konfigureret på, skal være dokumenteret. Det kan være en meget stor opgave og i det omfang der skal prioriteres, skal man sikre de aktiver, som virksomheden er mest afhængighed af, og som har størst risiko for at blive ødelagt. Yderligere skal virksomheden udvikle en rutine, der sikrer at den er informeret om, hvornår der offentliggøres nye trusler og IT-sikkerhedsbaserede opdateringer til den pågældende software.

Virksomheden skal tage backup
Det er en kilde til betydelige omkostninger, hvis man mister sin elektroniske ordrebog og det er til stor irritation for medarbejderne, når en fil, man har arbejdet med i en længere periode, forsvinder eller ødelægges. Det er på den anden side umuligt at forhindre, at noget sådant kan ske. Derfor skal virksomheden tage backup af alle data og systemer på en struktureret måde.

Virksomhederne bør specificere, hvem der er ansvarlige for, at der tages backup. Der bør tages fuld backup hver uge og desuden hver dag tages backup af de ændringer, der er sket siden dagen før. Virksomheden skal lave en politik for, hvor længe backup medier skal gemmes og dermed også for, hvornår backup medier kan genanvendes. Virksomheden skal desuden med jævne mellemrum kontrollere, at backupen ikke er fejlbehæftet og indeholder f.eks. virus. Virksomheden skal opbevare backupen hensigtsmæssigt på virksomheden og desuden bevare en kopi af backupen på et sikkert sted udenfor virksomheden. Der skal med jævne mellemrum gennemføres retableringsøvelser, der sikrer, at backupen kan anvendes efter en ulykkessituation.

Antivirussoftware
En af de trusler mod virksomhedens IT-systemer, der historisk har forvoldt mest skade, er udbredelsen af virus. En virus er et program, som sætter sig fast på et andet program, en fil eller del af computeren. En virus kan have mange forskellige virkninger alt efter hvilken virus, der er tale om. I nogle tilfælde viser virusen bare et billede på skærmen, som man ikke kan komme af med. I andre tilfælde sløver den computeren eller sletter indholdet af harddisken.

De typiske kilder til smitte er, at man får nye ting ind på sin computer. Det kan være alt lige fra filer på disketter over mails til temporære filer, der lagres på disken i forbindelse med besøg på en hjemmeside. Typiske tegn på, at man er inficeret med en virus, er, at filer pludselig ændrer størrelse eller navn, at der dukker nye og ukendte programmer op, at der er mindre ledig hukommelse end der burde være eller at der sker underlige ting, der får computeren til at virke ustabil.

Virksomheden skal installere antivirussoftware - især på de computere, som har størst risiko for at blive angrebet: mailserveren og klienterne. Et sådant program kan finde en virus allerede når den forsøger at sætte sig fast på computeren og passivisere den. Da mængden af virus er eksplosivt stigende, er det vigtigt, at virksomheden har rutiner for løbende opdateringer af programmet, således at det også kan passivisere de nyeste vira. De fleste antivirusprogrammer fanger foruden virus også andre skadelige programmer som orme og trojanske heste.

Virksomheden skal have en firewall
Når virksomheden åbner sig ud af til for at kommunikere med omverdenen, indebærer dette også at omverdenen kan kommunikere ind i virksomheden. Det er hele formålet med kommunikation. Men når et elektronisk netværk åbnes, er det vigtigt, at have klarhed over gennem hvilke kanaler man kommunikerer. Har man ikke kontrol over dette, kan omverdenen nemlig kommunikere gennem kanaler, man ikke var klar over og dermed få adgang til aktiver de ikke burde have adgang til. Dette kan føre til tyveri eller ødelæggelse af data, med store omkostninger for virksomheden til følge.

Elektronisk kommunikation foregår ved, at man i sit elektroniske netværk åbner en eller flere porte, som kommunikationen kan foregå igennem. Det svarer i den fysiske verden til, at man tager stilling til, om man vil modtage gæster af både hoveddøren og udhusdøren, eller om man kun vil modtage dem gennem hoveddøren. Hvis man selv vil være herre over den måde kommunikationen foregår, skal man kun åbne de porte, som man ønsker at kommunikerer igennem.

I alt for mange tilfælde har virksomheden ikke styr på hvilke porte den har åbnet for kommunikation. Virksomheden bør derfor lave en liste over, hvilke porte den har åbne. Herefter bør virksomheden vurdere, hvilke porte den har behov for at have åbne. Endelig bør virksomheden installere en firewall, som kan anvendes til at lukke de porte, der ikke er behov for at have åbne.

Virksomheden skal læse sine logfiler
Når en computer kontakter en anden computer udveksler de to computere navne og informationer om, hvilke aktiviteter de gerne vil foretage sig med hinanden. Disse navne og oplysninger skriver computerne ned i forskellige dokumenter, kaldet logfiler. Virksomhedens IT-systemer genererer en række logfiler for en række forskellige forhold computerne og netværket.

Ved at læse disse informationer kan en kyndig person ofte se om virksomheden er udsat for forsøg på uvedkommende indtrængning. Denne viden kan spare virksomheden for mange penge. Enhver virksomhed bør derfor udpege en person, som hver dag læser, de logfiler, som virksomheden finder,

er af størst betydning. Virksomhedens IT-sikkerhedsinitiativer bør afspejle de forsøg på indtrængen, som virksomheden har været udsat for.