WHITEPAPER

Sådan kan du arbejde med din virksomheds it-beredskab

DBI
BRAND OG SIKRING

WHITEPAPER

Sådan kan du arbejde med din virksomheds it-beredskab

I perioden 2019-2020 har Dansk Brand- og sikringsteknisk Institut (DBI) i samarbejde med Alexandra Instituttet arbejdet på resultatkontraktprojektet, Fremtidens Cybersikkerhed.

DBI foretog i vinteren 2019 og foråret 2020 empiriske undersøgelser, der har haft til hensigt at give indsigt i Små og Mellemstore Virksomheders (SMV'er) holdning til it-sikkerhed. Resultaterne af undersøgelserne har dannet baggrund for en konkret it-sikkerhedsydelse til at opnå større grad af it-sikkerhed i danske organisationer, som lanceres ved udgangen af projektperioden.

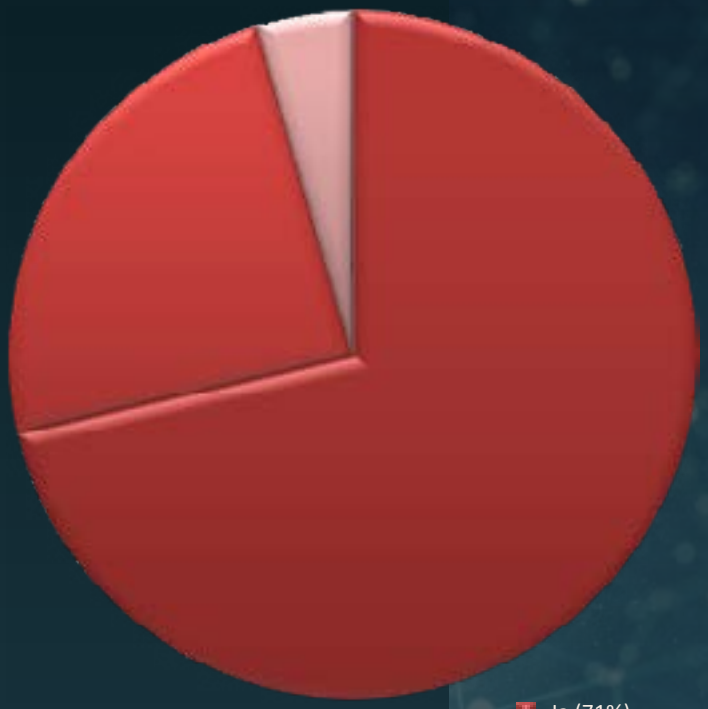
I nærværende publikation vil vi uddrage og konkludere på væsentlige pointer fra undersøgelserne med henblik på at belyse nogle af udfordringerne forbundet med implementering af it-sikkerhed i SMV'er. Pointerne vil blive sammenholdt med DBI's tidligere erfaringer fra arbejdet med it-beredskabsplanlægning og SMV'er som primært kundesegment for afslutningsvist at præsentere den ydelse, som vi har udviklet i projektperioden, der skal være med til at hjælpe organisationerne i arbejdet med it-sikkerhed i fremtiden.

DBI

Mere end 100 personer i forskellige funktioner fra en bred vifte af brancher – herunder blandt andre social- og sundhedsvæsen samt finansierings- og forsikringsbranchen – har deltaget i en spørgeskemaundersøgelse om deres holdning til it-sikkerhed. Foruden en spørgeskemaundersøgelse, har DBI i løbet af foråret 2020 gennemført en række interviews med henblik på at kortlægge blandt andet motivation og praksis i relation til it-sikkerhed i mindre organisationer. Disse undersøgelser har således udgjort datagrundlaget for følgende analyser og konklusioner.

I spørgeskemaundersøgelsen oplevede vi, at langt de fleste af respondenterne svarede, at den daglige drift på deres arbejdsplads afhang af informationsteknologi. 7 ud af 10 mente således, at det ville få væsentlige konsekvenser for deres organisation, hvis data blev hacket eller delt – noget som en femtedel af deltagerne har erfaringer omkring fra tidligere sikkerhedshændelser.
Knap 65% af de adspurgte havde ved tidspunktet for spørgeskemaundersøgelsen et ledelsesansvar i den organisation, hvor de var ansat. Her var det bemærkelsesværdigt, at størstedelen af denne gruppe var opmærksomme på, at det ville volde organisationen væsentlige problemer, hvis der skulle ske datalæk eller hacking, men samtidig var kun 25% indstillet på at it-sikkerhedsbudgettet ville stige i det kommende år (2020).
Resultaterne indikerer altså, at der er en kløft mellem bevidsthed og handling på dette område, hvilket blandt andet kan skyldes mangel på ledelsesopbakning, økonomisk prioritering eller kompetencer til styrkelse af området. I sit arbejde med SMV-segmentet, har DBI dog erfaret, at dette ofte skyldes en mangel på viden om, hvordan man kan arbejde med it-sikkerhed på en kosteffektiv måde, samt manglende prioritering og forståelse af it-sikkerhedsområdet som et konkurrenceparameter for organisationen.

Behandler jeres it-systemer data, som ville medføre væsentlige problemer for jer, hvis de bliver delt eller hacket?



Hele 20% af respondenterne i spørgeskemaundersøgelsen var ikke klar over, eller i stand til at sige med sikkerhed, om der reelt var sket it-sikkerhedsbrud, som havde påvirket den normale drift i organisationen. Dette var på trods af en bevidsthed omkring størrelsen på skadesvirkningerne, som følger af en kompromittering af it-systemer. Dette indikerer, at der er mangel på kommunikation omkring konsekvenserne af it-sikkerhedsbrud i organisationerne. Manglende italesættelse af konsekvenser var netop, sammenholdt med en forståelse af nødvendigheden af it-sikkerhed, afgørende parametre for mindre organisationer, når det kom til investeringsvillighed på området. Det handler med andre ord om, at den it-sikkerhedsansvarlige skal kunne italesætte emnet som værende relevant og vedkommende for organisationen, før villigheden til at investere i tiltag på området vil foreligge. Dette taler for et øget fokus på en forandring af organisationernes generelle risikoforståelse og sikkerhedskultur.

Det anslås, at omkring halvdelen af alle realiserede it-sikkerhedshændelser skyldes menneskelig uopmærksomhed, og derfor udgør adfærden hos medarbejderne i en organisation en potentielt stor risiko for it-sikkerheden.
Da vi i spørgeskemaundersøgelsen spurgte til, hvilke udfordringer de så i forhold til at forsvare sig mod it-sikkerhedsbrud, svarede 27% af respondenterne, at dette skyldtes en lav sikkerhedsbevidsthed blandt medarbejdere, mens 15% pegede på manglende politikker på området. Tekniske løsninger kan ikke stå alene, når det kommer til it-sikkerhed, men må nødvendigvis suppleres med uddannelse og træning af medarbejdere. Noget, som 86 % af de adspurgte var enige i.
Er medarbejderne ikke en del af det samlede forsvar mod it-sikkerhedshændelser, risikerer man, at eksterne parter er de første til at varsle organisationen om en hændelse, hvilket kan stille omdømmet i en sårbar position. For 33% af organisationerne i spørgeskemaundersøgelsen var dette tilfældet, hvis de havde oplevet brud på it-sikkerheden.
Det er muligt at undgå denne type hændelser ved at have klare procedurer for, hvad der skal ske i tilfælde af brud. Dette skal beskrives i en it-beredskabsplan, som alle medarbejdere bør kende.

Det kan være en stor opgave at tage hul på, når man skal lave en plan for implementering af it-sikkerhed i en organisation. For mange sikkerhedsansvarlige er det ukendt land at beskæftige sig med it-sikkerhed, og det kan derfor virke nærmest uoverskueligt at komme i gang. Heldigvis har DBI erfaret, at organisationer generelt set er motiveret for at lære nyt om it-sikkerhed og behovet for selvsamme, og der er derfor en stor velvilje i forhold til at løfte området.
For at opnå et holistisk forsvar mod it-sikkerhedshændelser, er det altafgørende at tænke medarbejderne ind som en væsentlig del af dette. Hvis medarbejderne skal udgøre et effektivt forsvar, er det vigtigt at huske på, at organisationers kompleksitet og behov varierer, og derfor bør man have en forståelse for medarbejdernes virkelighed, inden planerne defineres. På den måde undgår man, at it-sikkerhedsarbejdet ikke kommer til at føles som en klods om benet på medarbejderne, men i stedet som en hjælp til at sikre dem i deres hverdag.

DBI

Medarbejderne skal tage ansvar, være i besiddelse af sund skepsis og vide, hvad de skal gøre, hvis noget ikke helt er, som det plejer at være. Det handler om at gøre den enkelte bevidst om den rolle, som vedkommende spiller i den store sammenhæng. Samtidig skal man som ansvarshavende på området være opmærksom på, at usikker adfærd i forbindelse med it er tabubelagt, og der kan derfor også være et stort arbejde forbundet med at bryde med tabuet uden at skabe en nulfejlskultur. Derfor er en væsentlig del af beredskabsarbejde også uddannelse og træning af medarbejdere samt evaluering af tidligere hændelser med henblik på at uddrage læring fra hændelser og lukke sårbarheder.

I relation til uddannelse af medarbejdere, er det DBI's erfaring, at mange organisationer vælger at lade nyansatte læse op på en generisk it-sikkerhedspolitik, som mange ikke vil kunne relatere til deres dagligdag. Dertil kommer, at it-sikkerhedspolitikken sjældent bliver fulgt til dørs med træning og heller ikke genopfriskes på lige fod med anden hændelsesforebyggende uddannelse, som eksempelvis brandbekæmpelse, førstehjælp eller evakueringsøvelser.

Fordi en it-sikkerhedshændelse også kan have væsentlige konsekvenser for økonomien, medarbejderes sikkerhed og kunderelationer på en arbejdsplads, er det vigtigt, at organisationer begynder at anskue denne type hændelser som risikable på linje med hændelser, vi kender fra den fysiske verden. Denne forståelse er central i den fortælling, som organisationen skal have omkring konsekvenserne af it-sikkerhedshændelser, og derfor bør den blive indarbejdet i den eksisterende sikkerhedskultur, som også omfatter de fysiske hændelser.

Til at imødekomme udfordringer omkring SMV'ers it-beredskab (eller mangel på samme) har DBI udviklet en dynamisk it-beredskabsplan, som kan tilgås online via platformen, DigitaltBeredskab.dk.

Nogle af de største udfordringer forbundet med implementering af it-sikkerhed, er at gøre det vedkommende for dem, det handler om – nemlig medarbejderne. DBI's dynamiske platform er et opgør med støvede ringbind og kompliceret fagsprog. Platformen gør det nemt at tilpasse, plukke og tilføje i den generiske plan, så den bliver relevant og praksisnær både i opbygning og sprogbrug. Det hjælper både den ansvarshavende, såvel som folkene på gulvet til at forstå, hvorfor it-beredskab er vigtigt, og hvad de skal gøre, når uheldet er ude. Foruden at gøre beredskabsplanen til et dynamisk online dokument, kan DigitaltBeredskab.dk anvendes som en kommunikationsplatform og være handlingsanvisende for medarbejdere i tilfælde af hændelser – det kan være, at man eksempelvis ønsker at notificere medarbejdere i tilfælde af nedbrud på it-systemer, vil varsle dem om serviceperioder i forbindelse med opdateringer eller ønsker at lave øvelser med henblik på at træne deres awareness.

It-beredskabsplanen er et udgangspunkt for it-beredskabsplanlægningen, som er udarbejdet i tråd med punkterne om styring af informationssikkerhedsbrud og informationssikkerhedskontinuitet i informationssikkerhedsstandarden, ISO 27001. Dette er med henblik på at gøre det lettere for organisationer, der arbejder hen mod at blive

compliant med ISO 27001. For dem hvor dette ikke er et mål, vil værktøjet alligevel være medvirkende til at gøre det nemmere at implementere og øge it-sikkerheden i organisationen, da standarden sikrer, at man kommer hele vejen rundt i it-beredskabsarbejdet.

It-beredskabsplanen er således operativt funderet og tager fat i håndteringen både før, under og i efterspillet af en it-sikkerhedshændelse. Organisationer kan på den måde få hjælp til det forebyggende arbejde som led i sin risikostyring, blive klædt på til at håndtere hændelser på bedst muligt vis, når de indtræffer, samt finde støtte til genoprettelse af drift for at minimere en sikkerhedshændelses omkostninger.

DBI's online it-beredskabsplan kan med fordel kombineres med organisationens generelle beredskabsplan og andre relevante planer, som eksempelvis forretningskontinuitets- eller krisehåndteringsplanen. På den måde vil der være en rød tråd i organisationens beredskabsarbejde.

At tage en ensartet tilgang til sin beredskabsplanlægning er en fordel, hvis man ønsker at opbygge en robust og fleksibel forretning, der kan håndtere potentielle hændelser og it-sikkerhedsbrud.

It-beredskabsplanen kan naturligvis tilpasses eksisterende it-sikkerhedspolitikker, og i samarbejde med en rådgiver kan organisationer således få hjælp til at tilpasse it-beredskabet til den aktuelle kontekst. Enhver organisation – uanset størrelse, kompleksitet og sektor – vil derfor kunne drage nytte af en dynamisk it-beredskabsplan på DigitaltBeredskab.dk.

DBI - Dansk Brand- og sikringsteknisk Institut

Jernholmen 12
2650 Hvidovre
+45 3634 9000
dbi@brandogsikring.dk
www.brandogsikring.dk