MARSH

MARSH RISK CONSULTING

Cyber risikovurdering

KENDER I JERES VIRKSOMHEDS CYBERRISICI OG HVILKE FORRETNINGSMÆSSIGE KONSEKVENSER, DE KAN HAVE?

At identificere og håndtere sine cyberrisici kan være en udfordring for mange virksomheder. For de fleste er det ikke længere et spørgsmål om, hvem som rammes af et cyberangreb eller et utilsigtet nedbrud i IT-systemerne, men hvordan virksomheden håndterer og minimerer omfanget og konsekvenserne.

RISIKOSTYRING OG CYBERRISICI

Cyberrisici er forretningsrisici, der kan have stor indflydelse for virksomhedens bundlinje og omdømme. Identificering og håndtering af cyberrisici er derfor ikke alene relevant for IT-afdelingen, men et område som bør adresseres af nøglemedarbejdere i alle virksomhedens forretningsområder.

Kendskab til hvordan for eksempel manglende adgang til IT-systemer eller data påvirker forretningen vil give jeres virksomhed mulighed for at:

- Forstå eksponeringen over for cyberrisici
- Identificere uhensigtsmæssige procedurer i nuværende IT-setup
- Iværksætte risikoreducerende tiltag
- Indarbejde håndtering af cyberrisici i beredskabsplaner
- Identificere om virksomheden bør forsikre sig mod de finansielle konsekvenser

DEN MENNESKELIGE FAKTOR

Cyberangreb eller utilsigtede nedbrud i IT-systemerne skyldes ikke altid ondsindede handlinger, men er ofte forårsaget af menneskelige faktorer.

Det kan være en ansat, der åbner en e-mail, som ser ud til at komme fra en samarbejdspartner, men som indeholder en virus. Eller en medarbejder der sender en vigtig mail til en forkert modtager, hvorved data bliver lækket.

En del af virksomhedens håndtering af cyberrisici handler derfor også om, at skabe opmærksomhed på gode digitale vaner hos virksomhedens medarbejdere.

MARSH RISK CONSULTING

Marsh Risk Consulting (MRC) hjælper kunder med at håndtere deres risici og være forberedte på fremtidens risici.

Vi har indgående viden om ”best practice” risikostyring og vi vil gerne bruge vores viden og erfaring til at sikre at jeres virksomhed er klædt på til at håndtere jeres vigtigste risici.

Vi har specialister i cyberrisici både i Danmark og på vores kontorer rundt om i verden der er klare til at give jer kvalificerede råd om lokale forhold. Vi har hjulpet kunder af forskellige størrelser og fra forskellige brancher med at afdække, vurdere og håndtere deres cyberrisici.

800 ISSUE- AND INDUSTRY-SPECIFIC SPECIALISTS

LOCATED IN MORE THAN **40 COUNTRIES** AROUND THE GLOBE

MARSHS ANBEFALEDE METODE

Den mest effektive måde at identificere og håndtere cyberrisici sker ved at skabe en dialog på tværs af virksomhedens forretningsområder.

Marsh foreslår derfor at udarbejde en cyber risikovurdering, hvor deltagere fra forskellige forretningsområder med udgangspunkt i nogle udvalgte scenarier afdækker virksomhedens vigtigste cyberrisici, og diskuterer hvilke konsekvenser de kan have for forretningen.

Målet med risikovurderingen er at undersøge:

- Hvad der kan udløse de identificerede cyberrisici
- Hvor sandsynligt det er, at den enkelte cyberrisiko rammer
- Hvad de forretningsmæssige konsekvenser vil være, hvis cyberrisiciene rammer
- Diskutere risikoreducerende kontroller og tiltag, som allerede findes
- I forbindelse med risikovurderingen vil der blive afholdt en ½-dags workshop

Marsh tilbyder tre typer af cyber risikovurderinger, som varierer i omfang og format. Risikovurderingen vil blive skræddersyet efter jeres behov.

MINI RISIKOVURDERING

Mini risikovurderingen består af et kick-off telefonmøde med relevante personer i virksomheden, hvor der diskuteres, hvilke cyberscenarier der skal medtages i risikovurderingen samt deltagere til workshoppen. På workshoppen af en ½-dags varighed vil jeres top 3 cyberrisici bliver identificeret. Projektet vil blive afsluttet med en rapport som beskriver de identificerede cyberrisici og konsekvenserne heraf samt et generisk risikoregister over cyberrisici.

BASIS RISIKOVURDERING

Basis risikovurderingen består af et kick-off møde, en gennemgang af relevante dokumenter, såsom virksomhedens sikkerhedspolitik, risikokort eller lignende. Inden selve workshoppen vil Marsh interviewe 3 identificerede nøglepersoner i virksomheden.

En ½-dags workshop vil herefter blive afholdt, hvor jeres 3-5 cyberrisici bliver identificeret. Projektet vil blive afsluttet med en rapport som beskriver konklusionerne fra interviews, workshop herunder de identificerede cyberrisici og konsekvenserne.

UDVIDET RISIKOVURDEING

Den udvidede risikovurdering består af et kick-off møde, gennemgang af relevante dokumenter, såsom virksomhedens sikkerhedspolitik, risikokort eller lignende.

Inden selve workshoppen vil Marsh interviewe 3-5 identificerede nøglepersoner i virksomheden.

En ½-dags workshop vil herefter blive afholdt, hvor jeres 5-7 cyberrisici bliver identificeret. Projektet vil blive afsluttet med en rapport som beskriver konklusionerne fra interviews, workshop herunder de identificerede cyberrisici og konsekvenserne. Rapporten indeholder ligeledes en analyse af, om jeres eksisterende forsikringer dækker de finansielle konsekvenser cyberrisiciene kan have.

KONTAKT

For yderligere informationer om de enkelte risikovurderinger kan Jens Erik Nielsen eller Kathrine Tholander kontaktes.

Indhold	Mini risikovurdering	Basis risikovurdering	Udvidet risikovurdering
Kick-off møde	✓	✓	✓
Gennemgang af relevante dokumenter	✗	✓	✓
Interviews med nøglepersoner	✗	✓	✓
En ½-dags workshop	✓	✓	✓
Identificering af top cyberrisici	✓	✓	✓
Rapport m. generisk risikoregister	✓	✓	✓
Forsikringsanalyse	✗	✗	✓

KONTAKT

Ønsker I yderligere information eller en videre dialog om, hvordan vores tilgang og ydelser kan gavne jeres virksomhed, bedes I kontakte din Marsh repræsentant eller følgende:

Jens Erik Nielsen
Head of Marsh Risk Consulting North West
+45 29 13 33 36
jenserik.nielsen@marsh.com

Kathrine Tholander
Assistant Vice President
Cyber Practice
+45 51 36 63 39
Kathrine.Tholander@marsh.com

Marsh A/S
Teknikerbyen 1
2830 Virum
Denmark

CVR 87377016
+45 45 95 95 95
www.marsh.dk
Marsh.denmark@marsh.com