Beredskab

IT Relation A/S

Maj 2023

ITRelation
Closer to Customers

Introduktion og formål

Dette dokument har til formål, på et overordnet plan at beskrive IT Relations beredskab og hvodan IT Relation arbejder med planer og procedurer. De faktiske beredskabsplaner, procedurer og handlingsplaner indeholder personinformation og tekniske detaljer, som ikke kan deles uden for IT Relation. Nærværende dokument har således fokus på at beskrive omfanget og anvendelse af beredskabsplaner uden at beskrive alle detaljer fra selve beredskabsplanerne.

Derudover indeholder dokumentet information til IT Relations kunder om nødvendige kritiske foranstaltninger og handlinger IT Relation kan aktivere for at mindske konsekvens og sandsynlighed på kunders miljø ved et cybercrime angreb.

Formål med beredskabsplaner

Formålet med IT Relations beredskabsplaner er at beskrive, hvordan IT Relation håndterer en katastrofesituation. Dette gør, at organisationen er forberedt, inden en situation skulle indtræffe.

Som supplement til planerne arbejder IT Relation løbende med tiltag, som skal medvirke til at nedsætte risici og modvirke, at en katastrofesituation skulle opstå. Disse tiltag omhandler de fysiske, tekniske og organisatoriske foranstaltninger, der er gældende i IT Relation. Disse er beskrevet i separate interne dokumenter.

IT Relations arbejde med beredskabsplaner

Arbejdet med beredskabsplaner er forankret i Compliance & Security, der er en funktion, som har fokus på IT-sikkerhed og Compliance på alle IT-miljøer, IT Relation har et ansvar for.

Compliance & Security er ansvarlig for at:

- beskrive beredskabsplaner.
- udvikle og forbedre eksisterende beredskabsplaner.
- teste beredskabsplaner/uddannelse af personale.
- evaluere beredskabsplaner.
- arbejde med risikovurderinger og risikoplaner.
- udbrede viden om beredskabsplaner og forankre planerne i leverancen.

Arbejdet udføres løbende og som en del af IT Relations årshjul for IT-sikkerhed. Arbejdet udføres ikke alene af Compliance & Security, men i et tæt samarbejde med medarbejdere fra leveranceorganisationen samt IT Relations sikkerhedsgruppe.

Planer

IT Relation arbejder med en samlet beredskabsplan:

- Beredskabs- og katastrofeplan.

Beredskabsplanen har til formål at håndtere den taktiske ledelse af et beredskab, på baggrund af en kritisk situation hvor de normale procedurer og processer ikke er tilstrækkelige.
Udover beredskabsplanen arbejdes med handlingsplaner og procedurer. Handlingsplaner adresserer kendte, konkrete risiko scenarier, og har til formål at handle effektivt og korrekt i en konkret situation. Procedurerne en taktisk tilgang til en konkret opgave, og er med til at sikre ensartet kvalitet og resultat.

Beredskabsplaner, handlingsplaner og procedurerne er beskrevet nærmere nedenfor.

Beredskabsplaner

IT Relation har valgt at arbejde en samlet beredskabsplan. Det skal sikre, at i en katastrofesituation, at man kun skal kigge et sted for at finde beredskabsplanen. Det sikrer, at man ikke taber unødvendig tid på at finde den rigtige plan, og kan starte krisehåndteringen omgående.

Beredskabs- og katastrofeplan
Planen har til formål at forberede IT Relation til at kunne håndtere en katastrofesituation, som kan medføre, at store dele af IT-miljøerne er sat ud af funktion. Her er blandt andet beskrevet faser for etablering af nøddrift og efterfølgende overgang til normaldrift. Hændelser der aktiverer beredskabsplanen kan være et kritisk nedbrud som ikke er kontrol eller en kritisk sikkerhedshændelse

Planen har flere fælles elementer, som omfatter følgende områder:

- Hvordan er beredskabsledelsen organiseret (roller og ansvar).
- Hvordan iværksættes beredskabet og hjælp til vurdering af, om beredskab skal iværksættes.
- Kategorisering af driftshændelser/cybercrime-hændelser.
- Informationsprocedure internt og eksternt.
- Styring af beredskabsplanens fremdrift.
- "Lessons learned".
- Henvisning til procedurer, handlingsplaner og nødplaner, der kan være relevante at iværksætte.
- Kontaktlister, internt og leverandører.

Beredskab mod Cybercrime

Truslen for Cybercrime hændelser har gennem de seneste år været stærkt stigende, og risikoen for at blive offer er reel og sandsynlig. Cybercrimehændelser kan få alvorlig konsekvens for virksomheden både for brud på tilgængelighed for virksomhedens IT-systemer for fortrolighed på data.

IT Relation har derfor indbygget nødvendige foranstaltninger i deres planer, for at mindske risikoen for et alvorligt angreb, samt mindske konsekvenserne ved et alle aktivt angreb. Foranstaltningerne kan virke voldsomme, men er nødvendige for at beskytte kunden.

1. Stoppe et igangværende Ransomware angreb

Ved et kritisk Ransomware angreb vil hackeren aktivere kryptering af virksomhedens data og systemer. IT Relation vil som handling for at stoppe angrebet og mindske konsekvensen lukke for Internet adgang fra virksomhedens servere eller helt lukke servere ned.

2. Nød håndtering af 0-dags sårbarheder
   Der frigives jævnligt information om 0-dags sårbarheder til operativsystemer og applikationer. 0-dags sårbarhed betyder at sårbarheden allerede udnyttes. Hvis IT Relation vurderer at sårbarheden er så kritisk at IT Relations kunder kan blive ramt af alvorlige konsekvenser, indeholder IT Relations planer mulighed for at nedlukke kunders IT-system inden et angreb rammer kunden. Herefter er målet at mitigere 0-dags sårbarhed inden systemet sættes i drift igen.

Ovenstående handlinger kan i yderste konsekvens aktiveres uden kundens forudgående accept. Handlingerne er meget drastiske, og vil kun blive anvendt i yderst kritiske situationer. Hvis de iværksættes uden kundes accept, skal det godkendes i IT Relation, af en ledelse der er bemyndiget til dette.

Handlingsplaner

Handlingsplaner adresserer konkrete hændelser og gør IT Relation i stand til at handle korrekt og hurtigt på en sikkerhedshændelse. IT Relations målsætning er at have handlingsplaner på de mest kendte og sandsynlige cyberangreb og katastrofe scenarier. Planerne skal løbende udvikles, testes, revideres og opdateres.
Handlingsplanerne er opbygget ud fra principperne:

1. Identificere en sikkerhedshændelse.
2. Stop skaden.
3. Analysere hændelsen.
4. Kommunikation.
5. Sikre beviser.
6. Registrering.
7. Evaluering.

Følgende kendte og sandsynlige scenarier er beskrevet i handlingsplanerne:

- ”Worm response”-procedure.
- ”Virus response”-procedure.
- Uautoriseret adgang.
- ”Ransomware”-udbrud.
- ”Denial of service/DDOS”.

Procedurer
Procedurer har til formål at kunne anvendes til at håndtere situationer. Procedurerne indeholder rollebeskrivelser, hvordan de iværksættes, kommunikation og en beskrivelse af faser gennem proceduren. Procedurerne har desuden til formål at gøre IT Relation mindre personafhængig, ved at flere personer ud fra proceduren kan udføre opgaven på den mest optimale måde.

Det er målet, at procedurer løbende forbedres ud fra evaluering samt tekniske og organisatoriske muligheder. Følgende procedurer indgår som vigtige elementer i beredskabsplanerne:

- Procedure for Situation Management.
- Procedure for styring af information internt og eksternt.
- Procedurer for styring af sikkerhedshændelser.

Test af beredskab

IT Relation foretager minimum én gang årligt test af beredskabsplanerne.

Test
Beredskabsplanen testes ved at samle repræsentater for de forskellige operationelle afdelinger, samt katestrofe ledelsen, og så afspilles en række scenarier af forskellige karakter og kritikalitet. En række af scenarierne er en del af det endelige nedbrud der kræver beredskabsledelsen aktiveres. Derefter testes beredskabsledelsen indtil de igen nedlægger beredskabet.

Ud fra scenariet gennemgås handlinger i beredskabsplanen, og det sikres, at alle har samme opfattelse af planens indhold.

Evaluering og forbedring

Under testen samt efterfølgende tages der noter om alt input til forbedring og justering. Ud fra inputtet besluttes, hvilke tilføjelser eller rettelser der skal foretages i beredskabsplanerne. Formålet med dette er, at beredskabsplanerne løbende gennemgår en forbedringscyklus og dermed forbedrer IT Relations evne til at håndtere katastrofesituationer.

Revision

IT Relation revideres én gang årligt af et eksternt IT-revisionsselskab. Revisionen omfatter blandt andet, at beredskabsplanerne er fornuftige ud fra kendt standard. Desuden revideres, at beredskabet er testet og evalueres som beskrevet.

Beredskab historik

Dato	Revision	Forfatter / ansvarlig	Resume
02-11-2018	1.0	Frank Bech Jensen	Dokument udarbejdet og reviewet.
23-09-2020	1.1	Bo Duholm Hansen	Opdateret dokumentet med IT Relations nyeste katastrofeplans tiltag
14-04-2021	1.2	Frank Bech Jensne	Opdateret og tilføjet kritiske handlingstrin for at imødegå alvorlige cybercrime hændelser.
10-05-2023	1.3	Bo Duholm Hansen	Opdateret skabelon, samt opdateret beredskabstesten.


TRelation®
Closer to Customers