IFCR
INSTITUT FOR CYBER RISK

Guide til udarbejdelse af IT-beredskabsplan

Marts 2022

Styrk din virksomheds parathed og evne til at styre en krisesituation

Danske virksomheder udsættes hver dag for hackerangreb. Trusselsbilledet er højt, og antallet af angreb er stigende.Det handler ikke længere om, hvorvidt virksomheder rammes, men mere om hvornår og hvor hårdt de bliver ramt.

Derfor gælder det om at være godt forberedt, når cyberangrebet rammer. Her er IT-beredskabsplanen et nøgleværktøj. Med en god beredskabsplan er virksomheden klar til at navigere mens angrebet står på - og det kan være guld værd.

Din IT-beredskabsplan er dit planlægningsværktøj til håndtering af hackerangreb og nedbrud, så du igennem planlægning kan komme tilbage til normal drift igen hurtigst muligt.

Formålet er at styrke jeres virksomheds parathed og evner til at styre en krisesituation. Vi (Institut For Cyber Risk) har udviklet denne guide, så du nemt kan komme i gang med at udvikle en IT-beredskabsplan på en overskuelig måde.

Sådan kommer du godt i gang med at udforme en IT-beredskabsplan
Denne guide er udarbejdet for små og mellemstore virksomheder med eller uden egen it-drift, og guiden indeholder en "drejebog" over de elementer, som en IT-beredskabsplan bør indeholde, og som vi (Institut For Cyber Risk) anbefaler, at du følger.

Start med en analyse af forretningen, så I kan fokusere beredskabsinvesteringen på det, der virkelig betyder noget. Sørg for at folk med dyb indsigt i økonomi og forretningsprocesser deltager (CEO, CFO, proces-ejere/forretningsprofiler, CTO/IT-chef, jura og presseafdeling).

Når "kronjuvelerne" – de forretningsprocesser som virksomheden ikke kan overleve uden - er fundet, så kan I gå videre med at analysere i to spor; et i forretningen og et, der er IT-relateret. For forretningen er opgaven at finde måder at arbejde i nøddrift – pen og papir hvis det giver mening – indtil IT er retableret. IT-mæssigt er opgaven at finde ud af hvilke systemer og services, der understøtter hver proces, og det skal ske i samarbejde mellem de udførende og IT-afdelingen.
Når de kritiske IT-systemer, services og leverandører er kendt, kan I fokusere indsatsen på at beskytte dem.

Det kræver dels kontrakt- og leverandørstyring for de eksterne dele, dels tekniske planer for jeres interne dele.

Derudover skal I have selve jeres responsplan klar, når krisen rammer. Der skal være en velbeskrevet beredskabsorganisation og klare rammer for folk, så man kender sin rolle og ansvar, når det brænder på. Der skal være en tydelig måde at gå fra normaldrift/normal incident-håndtering til aktivt beredskab, og det er en fordel, hvis I kan støtte jer til procedurer, som I anvender i normaldrift.

Træf designbeslutninger på oplyst grundlag

Kend forretningens hjerteblod. Udfør en konsekvensanalyse for forretningen, for at afdække:

1. Hvad der er de kritiske forretningsprocesser/kronjuveler.
2. Hvilke muligheder der er for at drive processerne videre uden IT-understøttelse (forretningsprocedurer for at være i nøddrift).
3.. Hvor hurtigt forretningen bukker under, hvis en proces ikke virker samt estimat af tabt fortjeneste over tid (eks. 1 dag, 3 dage, en uge, en måned).
4. Hvor meget data, der kan tåles at miste (typisk afgørende for hvor ofte der skal tages backup).
5. Hvilke IT-systemer, der understøtter hver proces.

For hvert IT-system er der nu afdækket krav til/behov for beredskab i form af, hvor meget data kan man tåle at miste og hvor hurtigt skal systemet være retableret).

Definér ansvar og ejerskab i beredskabsorganisationen. Det vil sige; hvem gør hvad under et cyberangreb, men det er samtidig en støtte til uddelegering af opgaven med at udarbejde de forskellige dele af beredskabet

1. Hvem kan tage finansielle beslutninger?
2. Hvem leder organisationen under krisen?
3. Hvem leder beredskabsindsatsen?
4. Hvem udformer og ejer forretnings-nødprocedurer?
5. Hvem kommunikerer med interessenter og presse, og hvordan?
6. Hvem kommunikerer med leverandører, og hvordan?

Få styr på service-/driftsleverandører og leverandørkontrakter (Ekstern):

1. Afklar hvilke service-/driftsleverandører, der understøtter de kritiske forretningsprocesser – dvs. hvem leverer de eksterne services, der direkte eller indirekte indgår i arbejdsgangene.
2.. Vurdér om kontrakterne er dækkende i forhold til de krav/behov, der er. Hvis ikke så kender I nu en svaghed i jeres beredskab, som I kan gøre noget ved, og I ved fra konsekvensanalysen hvad konsekvensen kan være – så er det nemmere at vurdere, hvor meget det giver mening at investere i en ændring af kontrakten.

Afklar og dokumentér hvordan interne IT-systemer retableres (Intern):

1. Listen af IT-systemer, der understøtter kritiske forretningsprocesser, har I beskrevet. Dette skal nedbrydes til IT-komponenter, og det er typisk IT-afdelingen, der har den viden.
2.. Dokumentér hvilke afhængigheder, der er til reetablering, herunder:
   - Installationsprocedurer,
   - Hardware- og software-genanskaffelse, software repositories,
   - Sikker/duplikeret/off-site backup og
   - Alternativ lokation/hosting provider.
3. Beskriv teknisk procedure for retablering, herunder hvordan det testes, at systemet er fuldt retableret og virker for forretningen.
4. Vurdér og/eller test om retablering kan ske, og data kan retableres. Hvis ikke så kender I nu en svaghed i jeres beredskab, som I kan gøre noget ved, og I ved fra konkvensen er konsekvensanalysen – så er det nemmere at vurdere, hvor meget man bør investere i at gøre de kritiske IT-komponenter/-systemer mere robuste.

Dokumentér planen

Dokumentér beredskabsplanen – gå i gang med at formulere den endelige it-beredskabsplan:

1. Første del af planen beskriver, hvordan beredskabet er skruet sammen, herunder:
   - Introduktion med definition af scope (lokationer, systemer, processer som er omfattet af it-beredskabet) og tærsklen for hvornår noget er et minor-/major-incident, der håndteres i normaldrift, og hvornår det er en krise, der håndteres af beredskabsorganisationen.
   - Roller og ansvar som I har defineret i analysefasen skal dokumenteres og even tuelt udbygges med flere operationelle roller. Hvis roller og ansvar divergerer fra den daglige linjeledelse, så skal beredskabsorganisationens struktur naturligvis dokumenteres.
   - kontaktinformationer til interne og eksterne interessenter udarbejdes.
   - Eskalationsprocedure dokumenteres (hvordan kommer man fra en almindelig driftshændelse til at aktivere beredskabet, tid og omfang af hændelsen?)
   - Samspil med andre planer (eksempelvis eksisterende Incident Management, Presseberedskab, HR-procedurer) og ITs standard drift-/installationsprocedurer dokumenteres.
2. Anden del af planen beskriver, hvordan man agerer i krisesituationen (handlingsplaner), herunder:
   - Aktivering – hvordan startes beredskabet, hvordan informeres beredskabsorganisationen/tilkaldes folk?
   - Rolleinstrukser/action-cards for beredskabsledelsen:
     1. Vurdering af situationen og plan for handlinger.
     2. Intern/ekstern kommunikationsstyring.
     3. Prioritering af indsats, iværksættelse af retableringsprocedurer.
3. Bilag med retableringsprocedurer (hvordan kommer man tilbage til operationel drift).

Træning

Vedligehold beredskabsplanen:

1. Distribuér planen til de relevante nøglepersoner, som er defineret under roller og ansvar (beredskabsorganisationen). Sørg for at den er tilgængelig, selv hvis IT-systemerne bryder ned – men stadig på en sikker måde. Husk bare at jo flere steder der gemmes en kopi, jo sværere er den at holde ajour.
2. Gentag konsekvensanalysen årligt så forretningsbehovet er kendt, selv om forretningen ændrer sig.
3. **Træning og afprøvning.** Test planen årligt med alle relevante nøglepersoner, som er en del af IT-beredskabet (minimum skrivebordsøvelse).
   Træning skal være motiverende så sørg for en passende sværhedsgrad. At finde fejl og mangler kan gøres til en succesoplevelse med den rette tilgang. Start gerne med en helt simpel workshop som første test hvor deltagerne kan diskutere, hvordan de ville agere og vurdere, om planen giver mening for dem. Ret planen til og gentag umiddelbart efter med et mere realistisk scenarie og en egentlig skrivebordsøvelse hvor I simulerer et angreb, eks.ransomware. Med stigende modenhed kan I invitere leverandører med og udføre egentlige reetableringsøvelser, hvor systemer lukkes ned.
   Det I gerne vil opnå er:
   - At sikre at planens tekniske procedurer fungerer (kan man faktisk genskabe IT systemer som beskrevet, og er det de rette systemer, der er dækket?)
   - At sikre at beredskabsorganisationen fungerer (er rollerne velbeskrevet og fungerer kommunikationen?)
   - At sikre at udpegede folk reagerer hensigtsmæssigt i situationen. Dette er til dels træning og kendskab til rollen, men også et spørgsmål om personlighed – folk reagerer forskelligt i en ekstrem stresssituation, og det kan føre til uventede gnidninger i beredskabsorganisationen.
4. Opdatér planen i forhold til mangler og uhensigtsmæssigheder, der bliver fundet under træningen.

Med en god beredskabsplan er virksomheden klar til at navigere mens angrebet står på - og det kan være guld værd!

Friha Akhtar
Partner, Senior Security Sales Advisor
Email: fak@ifcr.dk
Mobil: +45 28 58 02 55

Rune Fog Hansen
Senior Security Advisor- Team GRC
Email: rha@ifcr.dk
Mobil: +45 52 15 01 87

Institut For Cyber Risk
Nærum Hovedgade 10A
2850 Nærum

Besøg os på www.ifcr.dk

IFCR
INSTITUT FOR CYBER RISK

Med mere end 90 års samlet erfaring inden for cyber risk, hvoraf mere end de seneste 20 år er fra Deloitte Risk Advisory, bygger Institut for Cyber Risk (IFCR) på et solidt fundament. Vi har en dyb forståelse for cyber risk i et forretningsperspektiv og besidder solide kompetencer inden for både cyber risk, sikkerhedstest, informationssikkerhed, GDPR, Cyber Awareness, ISO og meget andet. IFCR-teamet har stor erfaring med at servicere både private og offentlige organisationer, og udgangspunktet er altid "størst værdi for pengene".

Institut for Cyber Risk tilbyder kun de services, hvor vores faglige kompetencer vejer tungest. Som organisation kan I derfor være 100 procent sikre på, at alle opgaver bliver udført af medarbejdere med de bedste kompetencer, den største omhu og den største professionalisme hver gang.