



En guide för ledningsgruppen

60 dagar till en cyberattack. Vad gör ni nu?

Tänk er att ni vet datumet. Om 60 dagar drabbas er organisation av en omfattande cyberattack, som slår ut systemen, riskerar att läcka information och får verksamheten att stå still. Vad gör ni med tiden fram till dess?

60

dagar att minska risken,
säkra återstarten och öva
tills det sitter.

Det här är en ledningsfråga

En attack stannar sällan vid IT. Den når leveranser, kunder och förtroende, och därför börjar arbetet i ledningsgruppen. Det är ni som avgör vad som måste fungera, vem som fattar besluten och vilka risker som tas först. Med de prioriteringarna på plats kan IT och säkerhet göra dem till skydd, upptäckt och återställning.



Vänta inte på dag 1.

Ingen vet när en attack kommer, och därför gör planen mest nytta om ni börjar redan nu. Ser ni tecken på intrång i dag går incidenthanteringen före allt annat.

DAG 1–14

Bestäm vem som leder.

Stäng de största luckorna.

De första två veckorna handlar om att ge arbetet riktning och ta bort de mest akuta riskerna. Det börjar med beslut som bara ledningen kan fatta och fortsätter där ett intrång skulle kosta mest.

● DAG 1–3 / LEDNINGENS BESLUT

01

Ge någon mandatet

Utse samordnare, incidentledare och ersättare, och ge dem rätt att kalla in stöd, flytta resurser och vid behov stoppa delar av driften.

02

Bestäm vad som måste fungera

Peka ut de processer, system och den information som verksamheten inte klarar sig utan, och bestäm hur länge var och en får ligga nere och hur mycket data ni har råd att förlora.

● DAG 4–14 / IT OCH SÄKERHET GENOMFÖR

Skydda inloggningarna

Inför flerfaktorsautentisering för e-post, fjärråtkomst och administratörskonton, helst en metod som står emot nätfiske, och stäng oanvända konton och behörigheter som ingen behöver.

Åtgärda kända svagheter

Börja med kritiska sårbarheter i internetexponerade system och stäng åtkomstvägar som inte behövs. Kontrollera sedan att uppdateringar och skydd faktiskt når alla enheter.

Se till att larmen når fram

Kontrollera att loggning och övervakning fungerar och att någon tar emot larmen, även kvällar och helger. Bestäm också när ett larm blir ledningens fråga.



Klart när:

Varje åtgärd har en ägare, ett datum och ett sätt att visa att den är gjord.

DAG 15–45

Säkra återstarten.

Öva innan det blir skarpt.

När de största luckorna är stängda flyttas fokus till det som avgör hur snabbt ni kommer tillbaka. En säkerhetskopia bevisar inte att ni kan starta om, och en incidentplan bevisar inte att någon kan använda den. Båda behöver provas, och det är nu ni har tid.

● DAG 15–30 / BYGG FÖRMÅGAN ATT FORTSÄTTA

Testa återställningen på riktigt

Återställ ett prioriterat system med tillhörande data i en avskild miljö, ta tid och kontrollera att allt fungerar efteråt. Se samtidigt till att säkerhetskopiorna inte går att ändra eller radera, med separata behörigheter och en kopia som är isolerad eller oföränderlig.

Planera för dagarna utan IT

Bestäm vilka delar av verksamheten som kan fortsätta manuellt och hur ni når varandra när ordinarie IT ligger nere, med kontaktlistor och en reservkanal som inte är beroende av den. Stäm också av med leverantörerna vad de åtar sig, hur de nås och vem som ansvarar för vad.

**Klart när:**

Ni vet hur lång tid återställningen tar, i vilken ordning systemen startas och hur de viktigaste processerna klarar sig utan IT.

● DAG 31–45 / ÖVA MED LEDNING OCH NYCKELPERSONER



E-post och affärssystemet ligger nere.
En angripare påstår sig ha stulit kunddata.
Vem gör vad den första timmen?

Nu prövas planen på dem som ska använda den. Samla ledningsgruppen och nyckelpersonerna kring scenariot och gå igenom vem som startar incidentplanen, vem som beslutar om att isolera system och kalla in extern hjälp, och vem som informerar medarbetare, kunder och andra berörda. Juridik och dataskydd bedömer under tiden vilka rapporteringskrav och tidsfrister som gäller för just er.

**Klart när:**

Varje lucka som övningen visade har en ägare och ett datum, och alla medarbetare vet hur de rapporterar något misstänkt.

DAG 46–60 OCH FRAMÅT

Visa att beredskapen håller.

Med fakta, inte känsla.

De sista veckorna samlar ni ihop arbetet i en gemensam genomgång av vad som fungerar och vad som återstår. Be om testresultat, inte lägesrapporter, så att ledningens beslut vilar på fakta.



Beredskap byggs tillsammans.

Ledning, IT, säkerhet, verksamhet och leverantörer behöver kunna sina roller och agera som ett lag, och övningen har visat hur långt ni har kommit.

FEM FRÅGOR LEDNINGEN SKA KUNNA SVARA JA PÅ

- 1 Vet vi vem som fattar besluten och tar emot larmen?
- 2 Vet vi vilka processer som ska startas först?
- 3 Har vi testat återställningen och mätt tiden?
- 4 Kan vi kommunicera när ordinarie IT ligger nere?
- 5 Har vi övat och stängt luckorna vi hittade?



Dag 60 är ingen slutpunkt.

Verksamheten förändras och hotbilden med den, så beredskapen behöver följa med. Bestäm vad som ska hända med de risker som återstår, vilka resurser arbetet får och när ni ses för nästa uppföljning, och fortsatt att testa och öva däremellan.

Var börjar ni?

Dizparc hjälper er att prioritera arbetet med cybersäkerhet och beredskap utifrån er verksamhet.

Läs mer på dizparc.se