Ransomware-oefening scorecard

5 controles voordat je team onder druk moet herstellen

Gebruik deze scorecard om snel te zien of je ransomware-oefening verder moet gaan dan een technische test. De beste oefening maakt beslissingen zichtbaar: wie alarmeert, wie beslist, welke back-up is betrouwbaar, wat zeggen we extern en wanneer starten we systemen veilig opnieuw?

Scoreer elk punt van 0 tot 1

- Detectie: herkennen we snel genoeg dat dit ransomware kan zijn?
- Rollen: weet iedereen wie beslist, communiceert en uitvoert?
- Back-up: is herstel getest, gescheiden en haalbaar binnen de afgesproken tijd?
- Communicatie: kunnen we intern, extern en richting klanten rustig communiceren?
- Herstart: weten we welke systemen eerst terug mogen en wie dat vrijgeeft?

Werkblad voor je oefening

Vul dit vóór de oefening in. Houd het concreet: namen, systemen, tijdvensters en beslismomenten. Een score zonder vervolgactie is geen voorbereiding.

1. Detectie

Welke signalen zien we? Wie mag escaleren? Wanneer noemen we het een incident?

2. Rollen

Wie is incident lead, technisch lead, communicatie, directie, juridisch/privacy en leveranciercontact?

3. Back-up

Welke herstelbron gebruiken we eerst? Is die offline/gescheiden getest? Wat is de verwachte hersteltijd?

4. Communicatie

Welke boodschap gaat naar medewerkers, klanten, leveranciers en eventueel toezichthouder? Wie keurt die goed?

5. Herstart

Welke systemen komen als eerste terug? Welke controle is nodig voordat gebruikers weer toegang krijgen?

Na de score: wat doe je?

Score 4-5

Plan een scenario-oefening met directie, IT, communicatie en privacy/juridisch. Test vooral overdracht en herstartvolgorde.

Score 2-3

Maak eerst één verbeterlijst: rollen, back-upbewijs, contactlijst en beslisboom. Oefen daarna opnieuw met één realistisch scenario.

Score 0-1

Begin niet met een grote simulatie. Breng systemen, herstelbronnen en contactroutes eerst in kaart, anders test je vooral chaos.

Gebruik dit als startpunt

Een goede ransomware-oefening test geen paniek, maar beslissingen. Herhaal de score na elke verbetering en bewaar de acties bij je incidentresponsplan.