Stappenplan: Cyber Recovery Readiness

7 stappen om je voorbereiding op herstel te toetsen

Een cyberaanval. Je systemen vallen uit, maar je back-ups zijn beschikbaar en de herstelsoftware staat klaar. Toch weet je daarmee nog niet wanneer kritieke bedrijfsprocessen weer operationeel zijn. Misschien ontbreekt de toegang tot je back-upomgeving of steunt je herstelplan op dezelfde architectuur die is getroffen. Of je merkt dat een technisch geslaagde restore onvoldoende is om een bedrijfsproces te hervatten.

Doorloop onderstaande stappen voor één kritische procesketen. Maak per stap zichtbaar wat goed geregeld is, wat aannemelijk is en wat je ook echt hebt getest. Je kunt dit stappenplan als gespreksopener gebruiken in je organisatie als het gaat om cyberrecovery.

#1 Leg vast wat 'weer operationeel zijn' betekent

De omgeving herstellen is een te ruim vertrekpunt. Kies een bedrijfsproces en beschrijf de minimale werking die nodig is. Moeten medewerkers alleen klantgegevens kunnen raadplegen, of ook transacties verwerken? Welke tijdelijke werkwijze is voor jouw organisatie acceptabel?

Koppel de maximaal te verdragen uitval en het toegestane dataverlies daaraan. Breng vervolgens alle benodigde applicaties, gegevens en externe diensten in kaart. Zo voorkom je dat een applicatie prioriteit krijgt terwijl een noodzakelijke koppeling ontbreekt.

Maak concreet: wanneer verklaart de procesverantwoordelijke dat dit proces weer operationeel mag zijn?

#2 Zoek de afhankelijkheden die herstel blokkeren

Een applicatie kan afhankelijk zijn van identiteitsbeheer, DNS, netwerkverbindingen, certificaten en opslag. Die voorzieningen kunnen op hun beurt weer van elkaar afhankelijk zijn.

Loop de herstelvolgorde daarom vanaf een onbeschikbare omgeving door:

- Leidinggevenden werken aan richting en verantwoordelijkheden.
- IT kijkt naar de inrichting en het beheer.

Teken deze afhankelijkheden uit en toets hoe je de eerste voorzieningen beschikbaar krijgt. Een lijst met servers vertelt je nog niet hoe je kunt beginnen.

Maak concreet: welke afhankelijkheid moet je eerst doorbreken voordat echt herstel mogelijk is?

#3 Test toegang zonder je dagelijkse voorzieningen

Een noodaccount helpt alleen als het ook werkt wanneer de gebruikelijke inlogroute uitvalt.

- Controleer daarom de volledige toegangsketen: account, wachtwoord, MFA (multifactorauthenticatie), benodigde apparatuur en bereikbaarheid van je beheeromgeving.
- Neem ook decryptiesleutels, configuraties, licentiegegevens en herstelprocedures mee.
- Bewaar noodzakelijke informatie beschermd en bereikbaar buiten de getroffen omgeving.
- Laat een bevoegde collega de toegang daadwerkelijk testen zonder de eigen laptop of centrale wachtwoordvoorziening.

Maak concreet: wat kun je nog benaderen als je reguliere werkplek en inlogvoorzieningen onbruikbaar zijn?

#4 Bereid besluiten voor die onderzoek vereisen

Tijdens een aanval weet je niet meteen welke systemen betrouwbaar zijn. Leg vooraf vast wie:

- Het onderzoek leidt (intern of ook externe partijen?);
- Herstel voorbereidt;
- Toestemming geeft voor het opnieuw verbinden van systemen.

Bepaal welke informatie die besluiten ondersteunt. Denk aan alle getroffen onderdelen, aanwijzingen voor achtergebleven toegang en de betrouwbaarheid van mogelijke herstelpunten. Je onderzoek en de herstelvoorbereiding kunnen parallel aan elkaar lopen. Voorkom dat teams daarbij bewijsmateriaal overschrijven of een omgeving opnieuw blootstellen aan het gevaar.

Maak concreet: welke bevindingen moeten beschikbaar zijn om verantwoord door te kunnen gaan?

#5 Toets zowel de back-up als de bestemming

Een back-up van vóór de zichtbare verstoring kan alsnog besmet zijn. En betrouwbare data terugzetten op een getroffen systeem kan de aanval opnieuw ruimte geven...

- Bereid daarom voor hoe specialisten herstelpunten onderzoeken en hoe je de herstelomgeving opbouwt en controleert.

- Neem ook misbruikte accounts en kwetsbaarheden mee. Alleen bestanden terugzetten verwijdert de oorspronkelijke toegangsroute niet.
- Beschrijf welke controles nodig zijn voordat systemen opnieuw verbinding krijgen met andere delen van je omgeving.

Maak concreet: waarop baseer je het vertrouwen in de data én de omgeving waarin je data herstelt?

#6 Valideer de procesketen en de gegevens

Een draaiende server is geen bewijs dat het werk hervat kan worden. Laat applicatiebeheerders en procesverantwoordelijken controleren of gegevens compleet zijn, koppelingen functioneren en een representatieve handeling uitvoerbaar is.

Let ook op werk dat tijdens de uitval doorging. Handmatige registraties of transacties in andere systemen moeten mogelijk worden samengevoegd met teruggezette data. Zonder die afstemming kunnen gegevens ontbreken of dubbel worden verwerkt.

Maak concreet: welke functionele controle bewijst dat het proces weer klopt?

#7 Meet de hele oefening en test de knelpunten opnieuw

- Start de tijdmeting bij het incidentscenario.
- Registreer afzonderlijk de tijd voor besluitvorming, onderzoek, toegang, technische voorbereiding, het terugzetten van data en functionele validatie.
- Sommige activiteiten lopen parallel aan elkaar. Zoek uit waar wachten de voortgang blokkeert.
- Combineer een tabletop met technische hersteltests. Gebruik daarvoor alleen middelen die in het scenario beschikbaar blijven.
- Geef tekortkomingen een eigenaar en hertest de aanpassingen.

Maak concreet: welk knelpunt bepaalt je totale hersteltijd, en is dat inmiddels opgelost?

Is jouw organisatie voorbereid op herstel na een cyberaanval?

Bespreek de uitkomsten van dit stappenplan met onze specialisten. Binnen de Bechtle-groep ondersteunen we organisaties bij vraagstukken rondom cyber recovery, herstelprocessen en dataprotectie. We bespreken graag vrijblijvend de mogelijkheden.

Neem contact op