Ransomware tabletop

draaiboek voor de eerste oefening

Gebruik dit draaiboek om een compacte ransomware-oefening voor te bereiden. De nadruk ligt op besluiten, herstelvolgorde en communicatie, niet op gevaarlijke productie-tests.

Werk per sessie met één scenario, duidelijke rollen en maximaal vijf beslispunten. Noteer telkens wie beslist, welke informatie ontbreekt en welke actie na de oefening eigenaar krijgt.

1. **Kies drukpunt**
   Rollen, restore, communicatie, leveranciers of phishing.

2. **Zet rollen aan tafel**
   IT, directie, communicatie, privacy en leveranciers.

3. **Speel drie injects**
   Melding, escalatie, herstelkeuze.

4. **Leg besluiten vast**
   Niet alleen discussie, maar eigenaarschap.

5. **Plan opvolging**
   Maximaal vijf acties met eigenaar en datum.

Rollen aan tafel

Tabletop-oefening: wie zit aan tafel?

Een ransomware-aanval raakt de hele organisatie. Betrek de juiste rollen voor snelle besluiten en effectief herstel.

1 IT / Security

- Detectie en analyse van de aanval.
- Technische containment en isolatie.
- Back-ups en restore-strategie.
- Herstel van systemen en validatie.
- Technische impact inschatting.

2 Directie

- Strategische besluitvorming en prioriteiten stellen.
- Risico's afwegen (financieel, operationeel, reputationeel).
- Goedkeuren van herstelplan en benodigde middelen.
- Eindverantwoordelijkheid en stakeholders informeren.

3 Communicatie

- Interne communicatie naar medewerkers.
- Externe communicatie naar klanten, partners en media.
- Opstellen van kernboodschap en Q&A.
- Afstemming met directie en legal.

4 Privacy / Legal

- Beoordelen van privacy-incidenten en meldplicht.
- Juridische risico's en verplichtingen.
- Contact met toezichthouders indien nodig.
- Contractuele afspraken en aansprakelijkheid.

5 Leveranciers

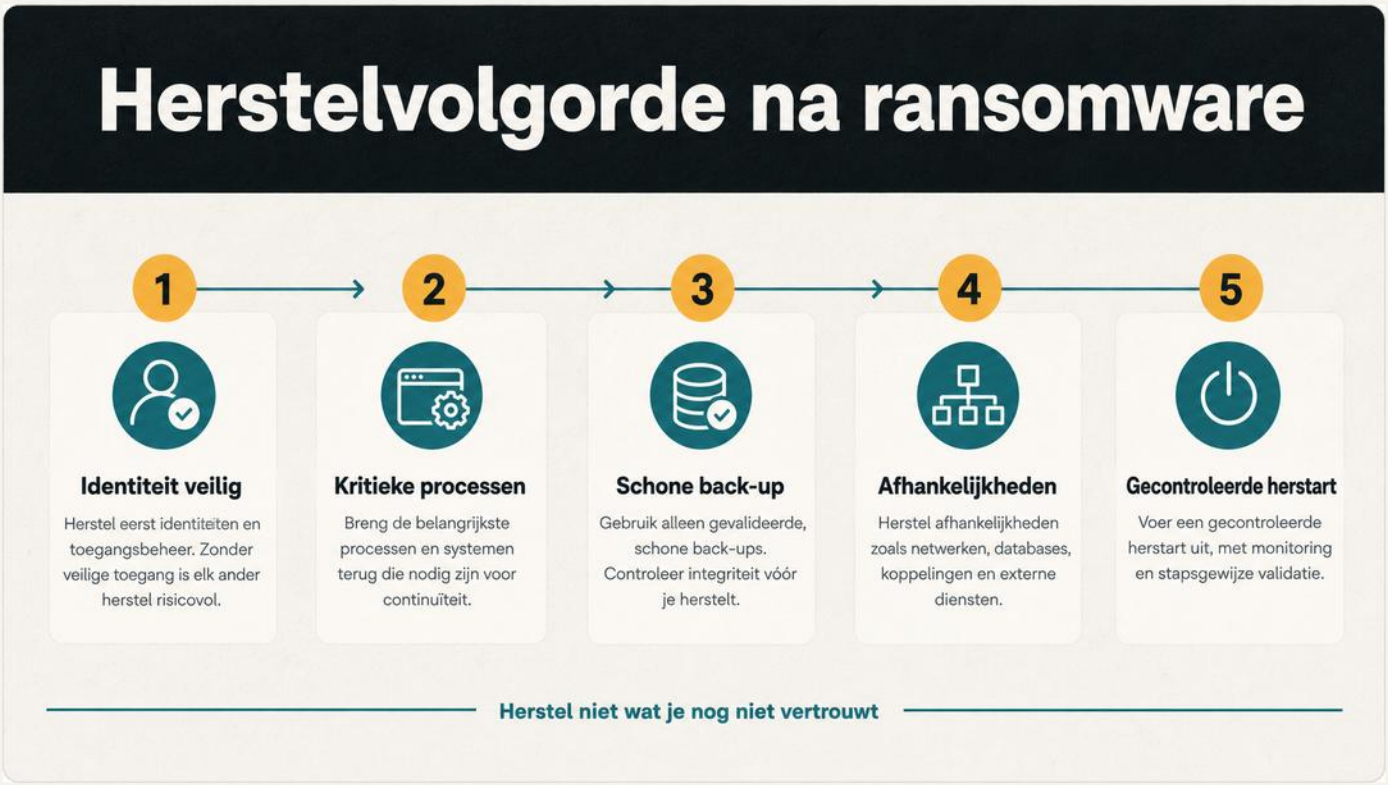
- Betrekken van kritieke leveranciers en partners.
- Afspraken over ondersteuning en responstijden.
- Toegang en informatie-uitwisseling coördineren.
- Evalueren van afhankelijkheden en alternatieven.

Oefen besluiten, niet alleen techniek

Oefenvragen

- Wie neemt het eerste besluit als informatie onvolledig is?
- Welke afhankelijkheid vertraagt herstel of communicatie?
- Welke afspraak moet na de oefening direct worden aangepast?

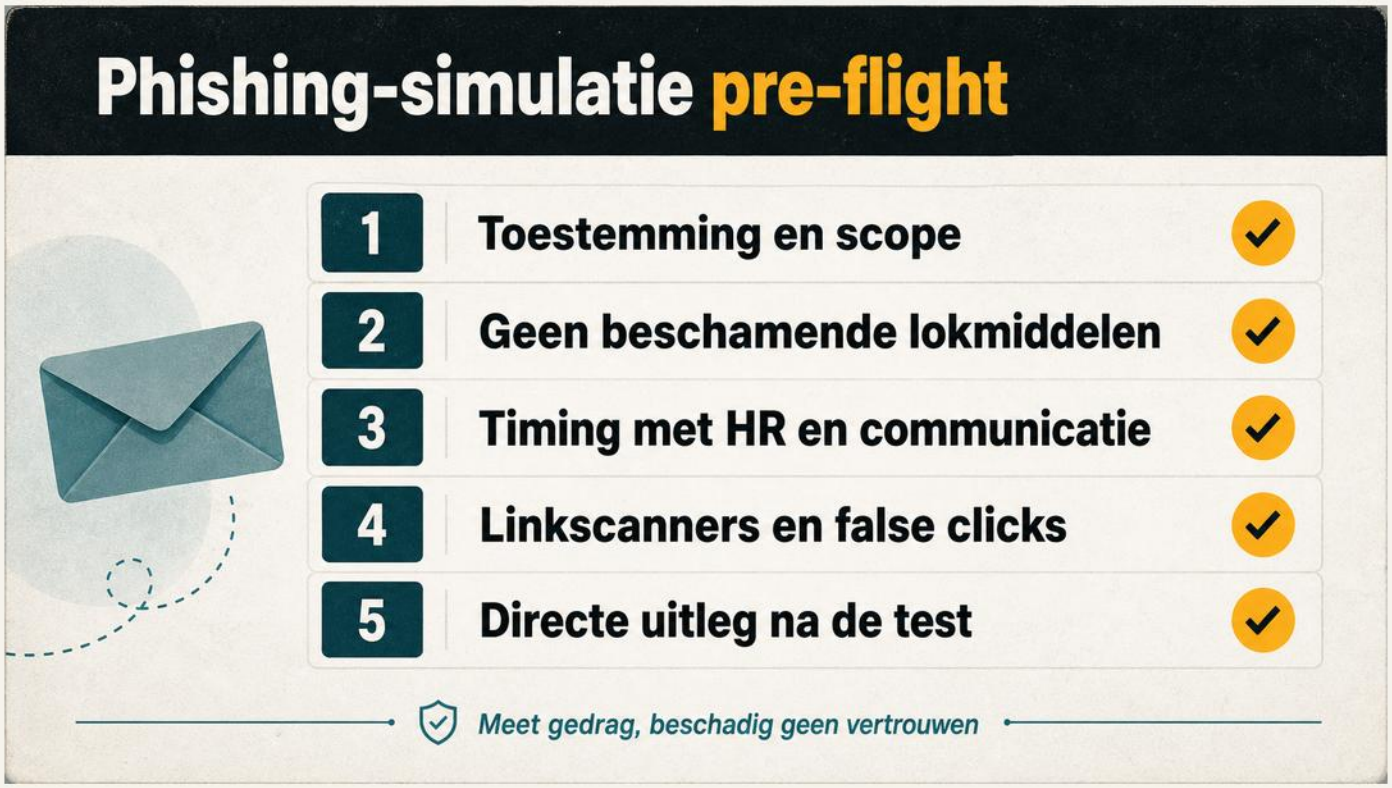
Herstelvolgorde



Oefenvragen

- Wie neemt het eerste besluit als informatie onvolledig is?
- Welke afhankelijkheid vertraagt herstel of communicatie?
- Welke afspraak moet na de oefening direct worden aangepast?

Phishing pre-flight



Oefenvragen

- Wie neemt het eerste besluit als informatie onvolledig is?
- Welke afhankelijkheid vertraagt herstel of communicatie?
- Welke afspraak moet na de oefening direct worden aangepast?

Oefenlog

Vul dit na de sessie in en koppel het aan je incidentresponsplan.

Belangrijkste besluit dat bleef hangen

Informatie die ontbrak

Systeem of afhankelijkheid die herstel vertraagde

Boodschap die nog niet klaar was

Actie, eigenaar en datum