GIDS

De complete gids voor cybersecurity crisisoefeningen

Tabletop exercises, kosten, NIS2/DORA-vereisten, scenario's en selectiecriteria. Voor MKB-organisaties die hun crisisrespons willen testen.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Oefenen op cyberincidenten is niet optioneel meer. De regelgeving verplicht het en de praktijk bewijst de waarde.

48 uur
Gemiddelde detectie- en containmenttijd bij organisaties die regelmatig oefenen
Eye Security 2026 [1]

121+
Unieke ransomware-incidenten in Nederland in 2024
NCSC Cybersecuritybeeld 2025 [2]

81,1%
Van cybercrime-incidenten in de EU betreft ransomware
ENISA Threat Landscape 2025 [3]

5 dagen
Mediaan doorlooptijd van inbraak tot ransomware-uitvoering (2025)
DeepStrike/diverse bronnen [4]

USD 4,44M
Gemiddelde kosten per datalek wereldwijd
IBM Cost of Data Breach 2025 [5]

64%
Van ransomware-slachtoffers betaalt geen losgeld (was 50% twee jaar eerder)
Verizon DBIR 2025 [6]

~10.000
Nederlandse bedrijven die onder de Cyberbeveiligingswet (NIS2) gaan vallen
Digitale Overheid [7]

21 dagen
Gemiddelde hersteltijd na een ransomware-aanval
Cigent/diverse bronnen [4]

1. Wat is een cybersecurity crisisoefening?

Een cybersecurity crisisoefening is een gesimuleerd incident waarbij je team oefent met de respons op een cyberaanval, zonder dat er daadwerkelijke systemen worden geraakt.

Bij een tabletop exercise zitten IT, management, communicatie en soms juridische medewerkers aan tafel. Ze krijgen een scenario voorgelegd en moeten in real-time beslissingen nemen [8]. Het doel is niet om fouten te bestraffen, maar om knelpunten te ontdekken en procedures te verbeteren.

Het NCSC omschrijft een cyberoefening als "een gesimuleerde gebeurtenis die het mogelijk maakt om de respons op een cyberaanval binnen je organisatie te verbeteren" [9].

> **Verschil met penetratietesten:** Een pentest test je technische beveiliging. Een crisisoefening test je organisatorische respons -- besluitvorming, communicatie, escalatie en samenwerking onder druk.

2. Waarom is het belangrijk?

Organisaties die regelmatig oefenen reageren sneller, communiceren beter en lijden minder schade bij echte incidenten.

De mediaan doorlooptijd van inbraak tot ransomware-uitvoering is gedaald tot 5 dagen in 2025 [4]. Dat betekent dat je organisatie binnen 5 dagen moet detecteren, beslissen en handelen om erger te voorkomen. Zonder oefening is dat een illusie.

CONCRETE VOORDELEN

- **Snellere besluitvorming** -- organisaties die oefenen nemen snellere en zekerdere beslissingen tijdens echte incidenten [10]
- **Lagere kosten** -- snellere containment correleert direct met minder dataverlies en lagere financiele impact [10]
- **Compliance** -- NIS2 en DORA vereisen regulier testen van incidentrespons [10]
- **Betere communicatie** -- wie belt wie? Wat melden we extern? Oefenen maakt dit concreet
- **Identificatie van gaten** -- ontdek welke procedures ontbreken voordat het ertoe doet

> **ROI:** Containment binnen 31 dagen kost gemiddeld USD 10,6 miljoen. Bij meer dan 91 dagen loopt dit op tot USD 18,7 miljoen [11]. Elke dag die je wint door te oefenen bespaart geld.

3. Hoe werkt het? Het oefenproces

Van voorbereiding tot follow-up: zo verloopt een cybersecurity crisisoefening.

1 Doelstelling en scope bepalen

1-2 WEKEN

Wat wil je testen? Incident response plan, communicatieprocessen, besluitvorming onder druk? Wie moeten deelnemen?

2 Scenario ontwikkelen

1-2 WEKEN

Een realistisch scenario wordt opgesteld, afgestemd op je sector en dreigingsprofiel. Injecties (nieuwe informatie tijdens de oefening) worden voorbereid.

3 De oefening uitvoeren

HALVE TOT HELE DAG

Deelnemers worden geconfronteerd met het scenario. De facilitator stuurt, geeft injecties en observeert. Alles wordt gedocumenteerd.

4 Hot wash (directe evaluatie)

30-60 MINUTEN

Direct na de oefening: wat ging goed? Wat niet? Eerste indrukken worden vastgelegd terwijl alles nog vers is.

5 Rapportage en verbeterplan

1-2 WEKEN

Een gedetailleerd rapport met bevindingen, aanbevelingen en een concreet actieplan. Het incident response plan wordt bijgewerkt.

TIP

Plan de eerstvolgende oefening al voor je de rapportage van de vorige hebt afgerond. Regelmatig oefenen (minimaal 1x per jaar, bij voorkeur 2x) is veel waardevoller dan een eenmalige oefening.

4. Wat kost het?

De kosten variëren sterk afhankelijk van complexiteit, aantal deelnemers en of je externe begeleiding inhuurt.

TYPE OEFENING	KOSTEN	TOELICHTING
Zelf-georganiseerd (gratis materiaal)	EUR 0-1.000	NCSC/DTC oefenmateriaal + eigen facilitatie [9][12]
Basis tabletop (halve dag)	EUR 3.000-7.500	1 scenario, externe facilitator, 5-10 deelnemers
Standaard tabletop (hele dag)	EUR 7.500-15.000	2-3 scenario's, voorbereiding + debriefing + rapport
Uitgebreide oefening	EUR 15.000-30.000	Maatwerk, meerdere teams, gedetailleerde rapportage
Enterprise/multi-site	EUR 30.000-50.000+ [13]	Meerdere locaties, volledige crisis-simulatie

JAARLIJKS BUDGET (MKB)

COMPONENT	KOSTEN PER JAAR
1-2 extern begeleide oefeningen	EUR 7.500-30.000
Interne voorbereidingstijd	EUR 3.000-6.000
Follow-up trainingen	EUR 2.000-5.000
Totaal	**EUR 12.500-41.000**

TIP

Het Digital Trust Center biedt gratis oefenmateriaal voor MKB [12]. SURF heeft kant-en-klare tabletop scenario's beschikbaar [14]. Start hier als je budget beperkt is.

5. Waar moet je op letten bij de keuze?

Een goede facilitator maakt het verschil tussen een nuttige oefening en een verspilde middag.

1. Relevante scenario's

Het scenario moet passen bij je sector, bedrijfsgrootte en dreigingsprofiel. Een ransomware-scenario is relevant voor bijna iedereen, maar de details moeten kloppen.

2. Ervaring van de facilitator

Een goede facilitator creëert realistische druk zonder deelnemers te overrompelen. Ervaring met soortgelijke organisaties is een pre.

3. Kwaliteit van de debriefing

De waarde zit in de nabespreking en het rapport. Vraag naar voorbeelden van eerdere rapportages.

10 VRAGEN VOOR JE AANBIEDER

1. Welke scenario's gebruiken jullie en zijn die afgestemd op onze sector?
2. Hoeveel crisisoefeningen begeleiden jullie per jaar?
3. Hoe ziet de voorbereiding eruit en wat verwachten jullie van ons?
4. Wie faciliteert de oefening en wat is diens achtergrond?
5. Hoe worden lessen vastgelegd en opgenomen in een verbeterplan?
6. Kunnen jullie meerdere scenario-niveaus aanbieden (beginner tot gevorderd)?
7. Is er follow-up ondersteuning na de oefening?
8. Hoe verhoudt de oefening zich tot NIS2/DORA-vereisten?
9. Kunnen jullie ook het management/bestuur betrekken?
10. Wat zijn de kosten voor een herhaaloefening later dit jaar?

> **RED FLAGS**
>
> Wees alert als een aanbieder: alleen standaard-scenario's gebruikt zonder aanpassing, geen debriefing of rapport levert, geen ervaring heeft met jouw sector, geen NIS2-kennis heeft, of de oefening behandelt als een test in plaats van een leermoment.

6. Veelgemaakte fouten

Deze fouten ondermijnen de waarde van een crisisoefening.

1. Te technisch

De oefening richt zich alleen op IT, terwijl crisismanagement ook communicatie, juridisch, HR en management omvat. Betrek het volledige crisisteam.

2. Onrealistisch scenario

Een scenario dat te ver van je dagelijkse realiteit staat levert geen bruikbare inzichten. Een ransomware-aanval op je eigen systemen is relevanter dan een state-sponsored APT.

3. Geen follow-up

Lessen die niet worden omgezet in verbeteracties zijn verloren moeite. Plan concrete verbeteringen met deadlines en verantwoordelijken.

4. Te weinig deelnemers

Als alleen IT meedoet, mis je de communicatie- en managementcomponent. Directie, communicatie en juridisch horen erbij.

5. Blame culture

Als fouten worden bestraft, leren deelnemers niets. Creëer een veilige omgeving waar fouten leermomenten zijn.

6. Eenmalig oefenen

Een jaarlijkse oefening is het absolute minimum. Kwartaalijkse micro-oefeningen (15-30 minuten) houden de kennis vers.

7. NIS2, DORA en regelgeving

Zowel NIS2 als DORA stellen concrete eisen aan het testen van je cyberweerbaarheid.

NIS2 / CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet mandateert "robuuste cybersecuritymaatregelen, inclusief incident handling en crisis management" [10]. Regulier testen en evalueren van deze capaciteiten is vereist. Bestuurders zijn persoonlijk aansprakelijk [15].

Boetes: tot EUR 10 miljoen of 2% van de wereldwijde omzet voor essentiele entiteiten [15].

DORA (FINANCIELE SECTOR)

DORA is van kracht sinds 17 januari 2025 en vereist stress testing, tabletop exercises en cyberaanval-simulaties [16]. Threat-led penetration testing (TLPT) is verplicht voor significante financiele entiteiten. De wet geldt voor 20 typen financiele entiteiten en hun ICT-dienstverleners.

GRATIS OVERHEIDSONDERSTEUNING

- **NCSC**: oefenmateriaal en begeleiding voor alle organisaties [9]
- **Digital Trust Center**: gratis oefenprogramma voor MKB [12]
- **SURF**: kant-en-klare tabletop scenario's en handleidingen [14]
- **Overheidsbrede Cyberoefening**: jaarlijkse livestream-oefening [9]

8. Tabletop vs. functionele vs. full-scale oefening

Kies het juiste type oefening voor je doelstelling en volwassenheidsniveau.

TYPE	WAT	KOSTEN	GESCHIKT VOOR
Tabletop (discussie)	Scenario-bespreking aan tafel	EUR 3.000-15.000	Alle organisaties, beginners
Functioneel	Oefening met echte systemen en processen	EUR 15.000-30.000	Organisaties met bestaand IRP
Full-scale	Volledige simulatie met alle teams	EUR 30.000-50.000+	Grote organisaties, gevorderd
Walk-through	Stapsgewijs doorlopen van het IRP	EUR 1.000-5.000	Alle organisaties, start

TIP

Begin met een walk-through van je incident response plan, gevolgd door een tabletop exercise. Bouw pas na 2-3 succesvolle tabletops op naar functionele of full-scale oefeningen.

9. Trends 2025-2026

Het oefenlandschap verandert door regelgeving, AI en nieuwe dreigingen.

1. NIS2-gedreven adoptie

Met de inwerkingtreding van de Cyberbeveiligingswet in Q2 2026 wordt een piek verwacht in de vraag naar crisisoefeningen, vooral bij organisaties die voor het eerst onder de wet vallen [7].

2. AI-scenario's

Deepfake CEO-fraude, AI-gegenereerde phishing en shadow AI als aanvalsvector worden steeds relevantere scenario's voor oefeningen.

3. Boardroom exercises

NIS2 legt persoonlijke aansprakelijkheid bij bestuurders. Specifieke oefeningen voor directie en commissarissen worden steeds gebruikelijker [10].

4. Supply chain oefeningen

Met 30% van datalekken via derden [6] ontstaan multi-organisatie oefeningen met leveranciers en partners.

10. Aan de slag

Klaar om je crisisrespons te testen? Begin hier.

1. **Check je incident response plan** -- heb je er een? Is het actueel?
2. **Start gratis** -- gebruik NCSC/DTC oefenmateriaal voor een eerste walk-through
3. **Plan een tabletop** -- boek een extern begeleide oefening met een relevant scenario
4. **Betrek de directie** -- crisismanagement is geen IT-feestje
5. **Plan de volgende** -- maak oefenen een terugkerend onderdeel van je security-programma

Bronnenlijst

[1] **Eye Security** -- The State of Incident Response 2026. eye.security/blog/the-state-of-incident-response-2026-insights-from-630-investigations

[2] **NCSC** -- Cybersecuritybeeld 2025. ncsc.nl/nieuws/cybersecuritybeeld-2025-dreigingen-divers-en-onvoorspelbaar-digitale-basishygiene-op-orde-blijft

[3] **ENISA** -- Threat Landscape 2025. enisa.europa.eu/publications/enisa-threat-landscape-2025

[4] **DeepStrike** -- Ransomware Statistics 2026. deepstrike.io/blog/ransomware-statistics-2025

[5] **IBM** -- Cost of a Data Breach Report 2025. ibm.com/reports/data-breach

[6] **Verizon** -- 2025 Data Breach Investigations Report. verizon.com/business/resources/reports/dbir/

[7] **Digitale Overheid** -- Cyberbeveiligingswet. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[8] **Neo Security** -- Crisis-oefening tabletop simulatie. neosecurity.nl/tabletop-exercises

[9] **NCSC** -- Oefen en bereid je voor op een cyberincident. ncsc.nl/oefenen/oefen-en-bereid-je-voor-op-een-cyberincident

[10] **Kudelski Security** -- Tabletop Exercises Boardroom Imperative. kudelskisecurity.com/modern-ciso-blog/why-tabletop-exercises-are-becoming-a-boardroom-imperative

[11] **Ponemon/DTEX** -- 2025 Cost of Insider Risks. ponemon.dtexsystems.com/

[12] **Digital Trust Center** -- Oefen en bereid je voor. digitaltrustcenter.nl/oefen

[13] **CM-Alliance** -- Cyber Crisis Tabletop Exercises Pricing. cm-alliance.com/cyber-tabletop-exercises-pricing

[14] **SURF SEC** -- Kant-en-klare tabletop oefening cybercrisis. sec.surf.nl/kant-en-klare-tabletop-oefening-cybercrisis/

[15] **Nieuwhuisconsult** -- Boetes NIS2. nieuwhuisconsult.nl/nieuws/wat-zijn-de-boetes-bij-niet-naleving-van-nis-2

[16] **ESMA** -- Digital Operational Resilience Act. esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

[17] **CBS** -- Cybersecuritymonitor 2024. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true