GIDS

De complete gids voor incident response voorbereiding

IR-plannen, playbooks, tabletop exercises, retainers en NIS2-meldprocedures.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Voorbereiding bepaalt de uitkomst bij een cyberincident.

58%
lagere breachkosten met IR-team en getest plan
IBM 2024 [1]

USD 3,26M
breachkosten met voorbereiding vs USD 5,29M zonder
IBM [1]

24 uur
maximale termijn eerste NIS2-incidentmelding
NCSC [2]

61 dgn
kortere breach-levenscyclus bij interne detectie
IBM [1]

59%
van organisaties getroffen door ransomware in 2024
Diverse [3]

EUR 50K--200K
kosten ransomware-incident Nederlands MKB
VerzkerCyber [4]

75%
heeft IR-plan, slechts 63% test het regelmatig
IBM [1]

76%
minder kans op ernstig incident bij structurele investering
Diverse NL [5]

1. Wat is IR voorbereiding?

Incident Response Voorbereiding omvat alle activiteiten om voorbereid te zijn op cyberincidenten -- voordat ze plaatsvinden.

Dit is anders dan IR Services (response tijdens een incident). IR Voorbereiding richt zich op: IR-plan schrijven, playbooks ontwikkelen, tabletop exercises, IR retainer afsluiten en meldprocedures testen.

ZES COMPONENTEN

- **IR Plan** -- Procedures, rollen, communicatieprotocollen
- **Playbooks** -- Per scenario (ransomware, phishing, DDoS)
- **Tabletop Exercises** -- Simulaties met alle stakeholders
- **IR Retainer** -- Contract met externe IR-experts
- **Forensic Readiness** -- Logging en bewijsbewaring
- **Meldprocedures** -- NIS2 (24u) en AVG (72u)

2. Waarom is het belangrijk?

58% lagere breachkosten en 61 dagen snellere detectie door voorbereiding.

Organisaties met getest IR-plan: USD 3,26M per breach. Zonder: USD 5,29M [1]. Verschil: USD 2,03 miljoen. Onder NIS2 moeten incidenten binnen 24 uur gemeld worden [2]. Zonder voorbereide procedures is die deadline niet haalbaar.

3. Het voorbereidingsproces

1 **Risicoanalyse**

WEEK 1--2

Identificeer scenario's: ransomware, datadiefstal, phishing, DDoS, insider threat.

2 **IR Plan en playbooks**

WEEK 2--4

Schrijf plan (rollen, communicatie, escalatie) en playbooks per scenario. Maak offline kopie.

3 **Meldprocedures**

WEEK 3--4

NIS2 (24u/72u/1 maand) en AVG (72u AP). Registreer op mijn.ncsc.nl.

4 **Tabletop exercise**

WEEK 5--6

Simulatie met management, IT, juridisch, communicatie. Evalueer en pas plan aan.

5 **IR Retainer**

WEEK 6--8

Sluit retainer af voor 24/7 beschikbaarheid. Controleer logging en bewijsbewaring.

4. Wat kost het?

TIER	WAT JE KRIJGT	PRIJSINDICATIE
Basis	IR Plan + playbooks (eenmalig)	EUR 3.000--8.000
Standaard	Plan + tabletop + IR retainer	EUR 8.000--20.000/jaar
Premium	Alles + meerdere exercises + forensic readiness	EUR 20.000--50.000/jaar

5. Selectiecriteria

- **Sectorervaring** -- Elk type incident vraagt andere expertise
- **24/7 beschikbaarheid** -- Gegarandeerde responstijd
- **Juridische kennis** -- NIS2, AVG, aansprakelijkheid
- **Forensic capabilities** -- Bewijsmateriaal veiligstellen
- **Playbook-kwaliteit** -- Concreet, niet generiek

6. Veelgemaakte fouten

1. Plan in de la leggen

Niet getest = waardeloos. Minimaal jaarlijks een tabletop exercise.

2. Alleen IT betrekken

IR raakt juridisch, communicatie, HR en management.

3. Geen offline kopie

Bij ransomware is het digitale plan onbereikbaar. Print het uit.

4. Meldprocedures niet oefenen

24-uur NIS2-melding vereist voorbereiding.

7. NIS2 meldplicht

TERMIJN	WAT	DETAILS
24 uur	Early warning	Eerste melding CSIRT via mijn.ncsc.nl [2]
72 uur	Incidentmelding	Technische en organisatorische details
1 maand	Eindrapport	Analyse, impact, maatregelen

8. Verschil met verwante oplossingen

KENMERK	IR VOORBEREIDING	IR SERVICES	SOC/SIEM
Wanneer	Voor incident	Tijdens incident	Continu
Doel	Plannen, oefenen	Stoppen, herstellen	Detecteren
Output	Plannen, exercises	Forensisch rapport	Alerts

9. Trends 2025--2026

1. NIS2-gedreven vraag

Meldplicht dwingt tot formele IR-voorbereiding.

2. Cyberverzekeraars eisen IR-plan

Getest plan als acceptatie-eis.

3. AI-ondersteunde IR

Snellere triage en communicatie met AI.

10. Aan de slag

Heb je een IR-plan? Is het getest? Als het antwoord "nee" of "meer dan een jaar geleden" is, begin nu.

Bronnenlijst

[1] **IBM** -- Cost of Data Breach 2024. ibm.com/reports/data-breach

[2] **NCSC** -- Meldplicht. ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor/meldplicht

[3] **Diverse** -- Ransomware stats 2024

[4] **VerzkerCyber** -- Kosten. verzekercyber.nl/wat-zijn-de-gemiddelde-kosten-van-een-cyberaanval/

[5] **Diverse NL** -- Cybersecurity investment

[6] **PreparedEx** -- Tabletop cost. preparedex.com/the-real-cost-of-a-tabletop-exercise-what-goes-into-creating-a-successful-one/

[7] **NCSC** -- Incident melden. ncsc.nl/contact/contactformulieren/incident-melden

[8] **CertificeringsAdvies** -- NIS2. certificeringsadvies.nl/nis2-meldplicht-bij-incidenten-wat-is-een-significant-incident-en-hoe-richt-je-je-incidentresponse-in/

[9] **NFIR** -- IR Retainer. nfir.nl/en/ir-retainer/

[10] **PwC** -- IR Retainer. pwc.nl/en/topics/digital/cybersecurity-privacy/cloud-incident-readiness/incident-response-retainer-services.html

[11] **Bureau Veritas** -- IRRA. cybersecurity.bureauveritas.com/services/integrated-approach/incident-response-pro/forensic-incident-readiness-assessment-fira

[12] **Sygnia** -- Tabletop. sygnia.co/blog/incident-response-tabletop-exercise/

[13] **CISA** -- Tabletop. cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

[14] **Digitale Overheid** -- Cbw. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[15] **NTNT** -- Kosten MKB. ntnt.nl/wat-kost-goede-cybersecurity-voor-een-mkb/