GIDS

De complete gids voor penetratietesten

Soorten, kosten, het proces, een aanbieder kiezen en je organisatie voorbereiden. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij •

Wat is een penetratietest? 1

Soorten penetratietesten 2

Wanneer heb je een pentest nodig? 3

Het pentestproces in 5 stappen 4

Wat kost een pentest? En wat levert het op? 5

Een aanbieder kiezen 6

Veelgemaakte fouten 7

NIS2, DORA en compliance 8

Trends: PTaaS, AI en continue testing 9

Na de pentest: van rapport naar actie 10

Bronnenlijst •

Kerncijfers op een rij

De belangrijkste cijfers die laten zien waarom pentesting geen luxe is, maar een investering die zichzelf terugverdient.

EUR 5,9M
Gemiddelde kosten van een datalek in de Benelux
IBM Cost of a Data Breach 2024 [1]

60%
van datalekken door bekende, ongepatchte kwetsbaarheden
Automox [2]

194 dagen
gemiddelde tijd om een datalek te identificeren
IBM CODB 2024 [1]

27%
van Nederlandse bedrijven toetst ICT-beveiliging structureel
CBS Cybersecuritymonitor 2024 [3]

~8.000
Nederlandse organisaties vallen direct onder NIS2/ Cbw
Digitale Overheid [4]

300:1
ROI verhouding: pentest van EUR 30K vs. datalek van EUR 5,9M
DeepStrike / Shield7 [5]

74 dagen
gemiddelde tijd om een kritieke kwetsbaarheid te verhelpen
Edgescan 2024 [6]

20%
van alle datalekken begint met kwetsbaarheids-exploitatie
Verizon DBIR 2025 [7]

WAAROM DIT ERTOE DOET

Een aanvaller heeft gemiddeld 4 dagen nodig om een netwerk te penetreren. Organisaties doen er 74 dagen over om een kritieke kwetsbaarheid te patchen. Dat verschil van 70 dagen is precies het venster dat een pentest blootlegt.

1. Wat is een penetratietest?

Een penetratietest, of pentest, is een gecontroleerde cyberaanval op je eigen systemen. Een ethical hacker probeert actief kwetsbaarheden te vinden en te exploiteren, precies zoals een echte aanvaller dat zou doen, maar dan met jouw toestemming en binnen afgesproken kaders.

Het doel is niet alleen een lijst kwetsbaarheden opleveren. Een goede pentest laat zien wat een aanvaller daadwerkelijk kan bereiken: kan hij bij klantgegevens? Kan hij lateraal bewegen door je netwerk? Kan hij rechten escaleren naar domeinadmin? Die context maakt een pentest waardevol. Uit het Verizon DBIR 2025 blijkt dat 20% van alle datalekken begint met het exploiteren van een kwetsbaarheid [7], een stijging van 34% ten opzichte van het jaar ervoor.

> **Pentest vs. vulnerability scan**
>
> Een vulnerability scan is geautomatiseerd en zoekt naar bekende kwetsbaarheden. Een pentest gaat verder: een mens probeert actief binnen te dringen, combineert kwetsbaarheden en test wat een aanvaller werkelijk kan bereiken. Handmatige pentests vinden circa 20x meer unieke kwetsbaarheden dan automatische scans alleen [8].

Na de pentest ontvang je een rapport met alle bevindingen, inclusief risicoclassificatie (CVSS-scores), bewijs van exploitatie en concrete aanbevelingen. De meeste aanbieders bieden ook een hertest aan om te valideren dat je fixes werken. De gemiddelde tijd om serieuze bevindingen op te lossen is gedaald van 112 dagen in 2017 naar 37 dagen in 2024 [9].

KERNBEGRIPPEN

- **Scope** - welke systemen worden getest en welke niet
- **Rules of engagement** - afspraken over wat de pentester wel en niet mag doen
- **CVSS** - Common Vulnerability Scoring System, de standaard voor risicoclassificatie (0-10)
- **PoC** - Proof of Concept, bewijs dat een kwetsbaarheid exploiteerbaar is
- **Hertest** - een tweede test om te valideren dat fixes werken
- **CCV Keurmerk** - Nederlands kwaliteitskeurmerk voor pentestbedrijven (gebaseerd op ISO/IEC 17065)

2. Soorten penetratietesten

Niet elke pentest is hetzelfde. De keuze hangt af van wat je wilt testen, hoeveel informatie de pentester vooraf krijgt, en hoe diepgaand de simulatie moet zijn.

OP BASIS VAN KENNIS

TYPE	INFORMATIE VOORAF	SIMULEERT
Black box	Geen - pentester weet niets	Externe aanvaller zonder voorkennis
Grey box	Beperkt - testaccounts, basis documentatie	Aanvaller met gestolen credentials of insider
White box	Volledig - broncode, architectuur, accounts	Diepgaande analyse, vindt meest mogelijke kwetsbaarheden

TIP

Begin met grey box als je voor het eerst een pentest laat uitvoeren. Je krijgt meer diepgang dan black box, zonder de kosten van een volledige white box analyse. Credential-gebaseerde aanvallen duren gemiddeld 292 dagen om te identificeren [1], wat grey box testen extra relevant maakt.

OP BASIS VAN DOELWIT

TYPE	FOCUS	GESCHIKT VOOR
Webapplicatie pentest	OWASP Top 10, business logic, authenticatie	Webapps, portalen, webshops
Netwerk pentest	Intern/extern netwerk, servers, firewalls	Kantoornetwerken, datacenters
API pentest	REST/GraphQL APIs, authenticatie, autorisatie	SaaS-platforms, mobiele backends
Mobile pentest	iOS/Android apps, lokale opslag, communicatie	Mobiele applicaties
Cloud pentest	AWS/Azure/GCP configuratie, IAM, storage	Cloudomgevingen

TYPE	FOCUS	GESCHIKT VOOR
Red team	Full-scope: technisch + social engineering + fysiek	Volwassen organisaties, TIBER-NL

Wat wordt het vaakst gevonden?

Broken Access Control is de meest voorkomende kwetsbaarheid in de OWASP Top 10. Security Misconfiguration is verantwoordelijk voor 20-30% van alle pentestbevindingen. SQL Injection maakt 19,47% uit van kritieke kwetsbaarheden in webapplicaties [6]. 63% van organisaties had in 2024 een API-beveiligingsincident [10].

3. Wanneer heb je een pentest nodig?

Een pentest is geen eenmalige exercitie. Er zijn concrete momenten waarop een test extra waardevol of zelfs verplicht is. Toch toetst slechts 27% van de Nederlandse bedrijven structureel hun ICT-beveiliging [3].

8 SIGNALEN DAT HET TIJD IS

1. **Je lanceert een nieuwe applicatie of platform** - test voor je live gaat, niet erna
2. **Je laatste pentest is langer dan 12 maanden geleden** - dreigingen veranderen continu
3. **Je hebt grote wijzigingen doorgevoerd** - migratie, nieuwe infrastructuur, grote releases
4. **Je moet voldoen aan NIS2, ISO 27001 of PCI DSS** - regelmatige tests zijn verplicht
5. **Klanten of partners vragen om bewijs** - steeds meer opdrachtgevers eisen pentestrapportages
6. **Je cyberverzekering vereist het** - veel verzekeraars geven korting bij aantoonbare testing
7. **Je hebt een security incident gehad** - test of de fix werkt en of er meer kwetsbaarheden zijn
8. **Je weet niet waar je risico's zitten** - een pentest geeft concreet inzicht

> **Hoe vaak testen Nederlandse bedrijven?**
>
> Bij grote bedrijven (250+ medewerkers) toetst 88% hun ICT-beveiliging structureel. Bij middelgrote bedrijven (50-250) is dat 73%, bij kleine bedrijven (10-50) slechts 47% [3]. Internationaal voert circa 40% van de organisaties kwartaal- of continue testen uit [8].

> **HET VENSTER VAN KWETSBAARHEID**
>
> Een aanvaller heeft gemiddeld 4 dagen nodig om een netwerk te penetreren. Organisaties doen er gemiddeld 74 dagen over om een kritieke kwetsbaarheid te patchen [6]. Die 70 dagen verschil is je risicovenster.

4. Het pentestproces in 5 stappen

Een professionele pentest volgt een gestructureerd proces. Hier is wat je kunt verwachten van intake tot hertest.

1 Scopebepaling en intake

1-2 DAGEN

Samen bepalen jullie welke systemen getest worden, welke aanvalsmethoden zijn toegestaan (rules of engagement), en wat de doelstellingen zijn. Dit wordt vastgelegd in een scope-document met NDA.

2 Reconnaissance

2-3 DAGEN

De pentester verzamelt informatie over je systemen: open poorten, services, technologieen, publiek beschikbare informatie. Bij grey/white box wordt dit aangevuld met de verstrekte documentatie.

3 Actieve testing en exploitatie

3-10 DAGEN

De daadwerkelijke aanvalspogingen. De pentester zoekt en exploiteert kwetsbaarheden: SQL injection, XSS, privilege escalation, laterale beweging. Alles wordt gedocumenteerd met bewijs. Gemiddeld vindt een pentest 12 kwetsbaarheden, waarvan 16% als High of Critical [11].

4 Rapportage

2-3 DAGEN

Alle bevindingen worden vastgelegd in een rapport met: managementsamenvatting, technische details per kwetsbaarheid, CVSS-scores, reproductiestappen en concrete aanbevelingen.

5 Presentatie en hertest

1-2 DAGEN

De pentester presenteert de bevindingen aan je team. Na het doorvoeren van fixes wordt een hertest uitgevoerd. 15-20% van initieel hoog-risico bevindingen is nog steeds exploiteerbaar bij de eerste hertest [12].

TOTALE DOORLOOPTIJD

Een standaard pentest duurt **2-4 weken** van intake tot hertest. Complexe trajecten (meerdere systemen, red team) kunnen 4-8 weken duren.

5. Wat kost een pentest? En wat levert het op?

Pentestprijzen varieren op basis van scope, complexiteit en type test. Hieronder realistische prijsindicaties voor de Nederlandse markt [13].

TYPE	SCOPE	PRIJSINDICATIE (NL)
Quick pentest	Beperkte scope, snelle scan + handmatig	EUR 2.800 - 5.500
Webapplicatie pentest	Enkele applicatie, OWASP Top 10	EUR 3.500 - 20.000+ [13]
Netwerk pentest	Extern + intern netwerk	EUR 4.500 - 12.000
API pentest	REST/GraphQL endpoints	EUR 3.000 - 7.500
Mobile pentest	iOS of Android + backend	EUR 5.000 - 15.000
Multi-scope pentest	Meerdere apps + API's + netwerk	EUR 8.000 - 20.000
Red team assessment	Full-scope inclusief social engineering	EUR 25.000 - 60.000+

WAT BEPAALT DE PRIJS?

- **Aantal systemen en applicaties** - meer scope = meer testdagen
- **Type test** - black box kost meer tijd dan grey/white box
- **Complexiteit** - een microservices-architectuur is complexer dan een enkele webapp
- **Urgentie** - spoedopdrachten kosten meer
- **Hertest** - inbegrepen of apart geprijsd
- **Certificeringen pentester** - OSCP/GPEN testers zijn duurder maar beter gekwalificeerd
- **Dagtarief** - senior pentesters rekenen EUR 800 - 1.400 per dag [13]

DE ROI VAN PENTESTING

> **Een pentest kost EUR 5.000 - 20.000. Een datalek kost gemiddeld EUR 5,9 miljoen in de Benelux.**
>
> Dat is een ROI-verhouding van meer dan 300:1. Organisaties met volwassen pentesting-programma's ervaren 75% minder beveiligingsincidenten en besparen gemiddeld USD 2,2 miljoen per jaar [5]. Uitgebreide pentesting-programma's leveren een ROI van 510% tot 1.266%.

LET OP

Een pentest onder EUR 2.500 is een red flag. Voor dat bedrag krijg je waarschijnlijk alleen een geautomatiseerde scan met een rapport eromheen, geen echte handmatige pentest door een ervaren specialist.

6. Een aanbieder kiezen

De kwaliteit van een pentest staat of valt met de aanbieder. Nederland heeft een volwassen markt met gespecialiseerde partijen en een eigen kwaliteitskeurmerk.

CERTIFICERINGEN DIE ERTOE DOEN

CERTIFICERING	FOCUS	NIVEAU
CCV Keurmerk Pentesten	Nederlands kwaliteitskeurmerk (ISO/IEC 17065)	Nationaal erkend [14]
CREST	Internationaal erkend voor pentestbedrijven	Hoog, wereldwijd gerespecteerd
OSCP	Praktijkgerichte penetratietest	De standaard voor individuele pentesters
GPEN	Netwerk penetratietest (SANS/GIAC)	Hoog, gerespecteerd
CEH	Ethical hacking (EC-Council)	Instap, theoretisch
OSWE	Web application security expert	Geavanceerd, webapp-specifiek

CCV KEURMERK

Het CCV Keurmerk Pentesten vereist dat medewerkers een VOG overleggen (niet ouder dan 3 jaar), dat het bedrijf een kwaliteitsmanagementsysteem hanteert, en dat een onafhankelijke certificeringsinstantie de kwaliteit beoordeelt [14]. Vraag je aanbieder of zij dit keurmerk hebben.

10 VRAGEN VOOR JE AANBIEDER

1. Hebben jullie het CCV Keurmerk Pentesten of CREST-accreditatie?
2. Welke certificeringen hebben jullie pentesters individueel (OSCP, GPEN)?
3. Kunnen jullie een geanonimiseerd voorbeeldrapport delen?
4. Is een hertest inbegrepen in de prijs?
5. Welke methodologie volgen jullie (OWASP, PTES, OSSTMM)?
6. Hebben jullie ervaring in mijn specifieke sector?
7. Hoe communiceren jullie tijdens de test bij kritieke bevindingen?
8. Wat is de doorlooptijd van intake tot rapport?
9. Bieden jullie ondersteuning bij het verhelpen van bevindingen?

10. Zijn jullie verzekerd voor eventuele schade tijdens de test?

De juiste pentesting partner vinden?

Nederland kent tientallen gespecialiseerde pentestbedrijven. De keuze hangt af van je sector, het type test en je budget. Via IBgids.nl word je vrijblijvend gematcht met aanbieders die passen bij jouw situatie.

7. Veelgemaakte fouten

Deze fouten zien we regelmatig bij organisaties die een pentest laten uitvoeren. Voorkom ze.

1. Te beperkte scope kiezen om kosten te besparen

Alleen de website testen terwijl de echte risico's in het interne netwerk of de API's zitten geeft een vals gevoel van veiligheid. 63% van organisaties had in 2024 een API-beveiligingsincident [10]. Laat een risicoanalyse uitvoeren voordat je de scope bepaalt.

2. Geen hertest plannen na het fixen

Na het fixen van kwetsbaarheden wordt niet gevalideerd of de fixes werken. 15-20% van hoog-risico bevindingen is nog steeds exploiteerbaar bij de eerste hertest [12]. Neem altijd een hertest op in je contract.

3. De pentest als eindstation zien

Een pentest is een momentopname. 65% van organisaties had herhaalde kritieke bevindingen in opeenvolgende jaarlijkse pentests [12]. Maak een verbeterplan met deadlines en eigenaren.

4. Alleen op prijs selecteren

De goedkoopste aanbieder levert vaak een geautomatiseerde scan af als "pentest". Kijk naar certificeringen (CCV Keurmerk, CREST), ervaring en rapportkwaliteit.

5. Het team niet informeren

Als je SOC-team niet weet dat er een pentest loopt, gaan ze de pentester blokkeren of in paniek raken over de alerts. Informeer de juiste mensen vooraf.

6. Bevindingen niet structureel oppakken

Circa 50% van ontdekte kwetsbaarheden blijft onhersteld. 32% van kritieke kwetsbaarheden is na 180 dagen nog niet opgelost [12]. Wijs een eigenaar toe aan elke bevinding en rapporteer maandelijks over voortgang.

8. NIS2, DORA en compliance

Regelmatige pentests zijn niet langer een nice-to-have. Onder meerdere regelgevingen zijn ze verplicht, met stevige boetes bij niet-naleving.

NIS2 / CYBERBEVEILIGINGSWET

NIS2 Artikel 21 vereist dat organisaties in essentiele en belangrijke sectoren regelmatige security audits en penetratietesten uitvoeren. De Cyberbeveiligingswet (Cbw) wordt in Nederland verwacht in Q2 2026 en raakt circa 8.000 organisaties direct, plus naar schatting 50.000 toeleveranciers indirect [4].

BOETES NIS2

Essentiele entiteiten: tot EUR 10.000.000 of 2% van de wereldwijde jaaromzet. **Belangrijke entiteiten:** tot EUR 7.000.000 of 1,4% van de wereldwijde jaaromzet. Bij herhaalde overtredingen kan persoonlijke aansprakelijkheid van bestuurders volgen [15].

DORA

DORA (van kracht sinds januari 2025) verplicht Threat-Led Penetration Testing (TLPT) voor systeemrelevante financiele instellingen. Dit gaat verder dan een standaard pentest en volgt het TIBER-NL kader.

ISO 27001 EN PCI DSS

ISO 27001 Annex A Control 8.8 vereist systematische identificatie en management van technische kwetsbaarheden. **PCI DSS** verplicht organisaties die creditcardgegevens verwerken om jaarlijks een penetratietest te laten uitvoeren.

WAT MOET JE AANTONEN?

- Dat je regelmatig (minimaal jaarlijks) penetratietesten uitvoert
- Dat bevindingen worden opgelost binnen een redelijke termijn
- Dat je een hertest uitvoert om te valideren dat fixes werken
- Dat je het proces documenteert en beschikbaar hebt voor audits
- Dat je pentester gekwalificeerd is (CCV Keurmerk of equivalent)

9. Trends: PTaaS, AI en continue testing

De pentesting-markt verandert snel. Drie ontwikkelingen die je als inkoper moet kennen.

PTAAS: PENTEST AS A SERVICE

Bij PTaaS krijg je geen eenmalig rapport, maar doorlopende toegang tot een platform met real-time dashboards, ticketing-integratie en automatische hertests na patches. Meer dan 70% van bedrijven gebruikt al PTaaS of een vergelijkbaar model [16]. De globale PTaaS-markt groeit met 22,4% per jaar naar USD 5,99 miljard in 2033.

WANNEER PTAAS OVERWEGEN?

Als je regelmatig wijzigingen doorvoert (agile/DevOps), als je meerdere applicaties hebt die continu getest moeten worden, of als je verplicht bent tot frequente compliance-rapportages.

AI IN PENTESTING

AI-tools reduceren testtijd met tot 30% en geautomatiseerd pentesting steeg 2,5x in 2024 [8]. 70% van security researchers gebruikt AI-tools in hun workflow. Maar: handmatige pentests vinden circa 20x meer unieke kwetsbaarheden dan automatische scans alleen. AI versnelt, maar vervangt de menselijke pentester niet.

CONTINUE TESTING VS. POINT-IN-TIME

Organisaties die overstappen naar kwartaal-testen zien 42% minder onopgeloste kwetsbaarheden binnen 6 maanden [17]. De trend verschuift van jaarlijkse "compliance-tests" naar continue beveiliging. Een combinatie van pentest + bug bounty vindt 3-5x meer high-impact kwetsbaarheden [18].

10. Na de pentest: van rapport naar actie

Het rapport is pas het begin. Wat je erna doet bepaalt de waarde van de investering. Circa 50% van ontdekte kwetsbaarheden blijft onhersteld [12]. Zo voorkom je dat.

BEVINDINGEN PRIORITEREN

Niet alles hoeft direct gefixt. Prioriteer op basis van CVSS-score, exploiteerbaarheid en business impact:

CVSS-SCORE	ERNST	ACTIE	BENCHMARK REMEDIATIETIJD
9.0 – 10.0	Kritiek	Direct aanpakken	Mediaan: 15 dagen [6]
7.0 – 8.9	Hoog	Binnen 2 weken	Mediaan: 37 dagen [9]
4.0 – 6.9	Medium	Binnen 30 dagen	Mediaan: 54-74 dagen [6]
0.1 – 3.9	Laag	Planmatig oppakken	Variabel

VERBETERPLAN MAKEN

Maak voor elke bevinding een ticket met eigenaar en deadline. Bespreek de bevindingen met je hele IT-team. Slechts 57% van organisaties lost minstens 90% van serieuze bevindingen op, terwijl 15% minder dan 10% oplost [9].

HERTEST EN STRUCTUREEL VERBETEREN

Laat na het doorvoeren van fixes een hertest uitvoeren. Gebruik de bevindingen om je ontwikkelprocessen te verbeteren. Als dezelfde type kwetsbaarheid steeds terugkomt, investeer dan in training, code review, of security tooling in je CI/CD pipeline.

Bronnenlijst

[1] **IBM Cost of a Data Breach 2024** - Kosten, detectietijd, Benelux-specifieke data. newsroom.ibm.com

[2] **Automox** - Bad Cyber Hygiene: 60% datalekken door ongepatchte kwetsbaarheden. automox.com

[3] **CBS Cybersecuritymonitor 2024** - ICT-beveiligingsmaatregelen Nederlandse bedrijven. cbs.nl

[4] **Digitale Overheid / NCSC** - Cyberbeveiligingswet, scope ~8.000 organisaties. digitaleoverheid.nl

[5] **DeepStrike / Shield7** - ROI-analyse pentesting: 300:1 tot 1.266%. deepstrike.io + shield7.com

[6] **Edgescan Vulnerability Statistics 2024** - MTTR per kwetsbaarheidstype. edgescan.com/stats-report

[7] **Verizon DBIR 2025** - 22.052 incidenten, 20% via kwetsbaarheids-exploitatie. verizon.com/business/resources/reports/dbir

[8] **DeepStrike 2025** - Penetration Testing Statistics, AI-trends, testfrequentie. deepstrike.io

[9] **Cobalt State of Pentesting 2024** - MTTR, resolutiepercentages, 10-jarige trend. resource.cobalt.io

[10] **OWASP Foundation** - Top 10 Web Application Security Risks. owasp.org

[11] **HackerOne** - Gemiddeld 12 kwetsbaarheden per pentest. hackerone.com

[12] **DeepStrike / Indusface 2025** - Hertest-statistieken, remediatiepercentages. deepstrike.io + indusface.com

[13] **Sectricity / Tozetta / Security.Rocks** - Nederlandse pentestprijzen 2025-2026. sectricity.com + tozetta.com

[14] **Het CCV** - Keurmerk Pentesten (ISO/IEC 17065). hetccv.nl

[15] **NIS2 Directive EU / PwC NL** - Boetestructuur en persoonlijke aansprakelijkheid. nis2directive.eu + pwc.nl

[16] **MarketsandMarkets / Grand View Research** - PTaaS marktomvang. marketsandmarkets.com

[17] **Pentera State of Pentesting 2025** - Budget en effectiviteit. pentera.io

[18] **HackerOne / Bugcrowd** - Pentest vs. Bug Bounty vergelijking. hackerone.com + bugcrowd.com

Deze gids is samengesteld door IBgids.nl op basis van openbare bronnen en marktonderzoek. Alle genoemde prijzen zijn indicatief en gebaseerd op de Nederlandse markt (peildatum: maart 2026).