GIDS

De complete gids voor vulnerability scanning

Scantypen, kosten, prioritering, selectiecriteria, NIS2 en CTEM. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Vulnerability scanning is de basis van proactieve beveiliging. Kwetsbaarheden worden sneller misbruikt dan ooit. Hieronder de feiten.

~6%

van alle gepubliceerde CVE's wordt daadwerkelijk geexploiteerd -- focus op wat ertoe doet

FIRST / EPSS Research [1]

EUR 270K

Gemiddelde schade per cyberincident voor MKB in Nederland

Verzekercyber.nl [2]

28%

van exploits verschijnt binnen 1 dag na publicatie van de kwetsbaarheid

Edgescan / Verizon DBIR [3]

$5,2B

Verwachte marktomvang Attack Surface Management (ASM) in 2030

Mordor Intelligence [4]

3× minder

breaches bij organisaties die CTEM (Continuous Threat Exposure Management) toepassen

Gartner [5]

43%

van het Nederlandse MKB had in 2024 te maken met een security-incident

CBS Cybersecuritymonitor 2024 [6]

NIS2

Art. 21: kwetsbaarheidsbeheer als verplichte beveiligingsmaatregel

NIS2-richtlijn Art. 21 [7]

60%

van kleine bedrijven gaat failliet binnen 6 maanden na een ernstige cyberaanval

Laurus Verzekeringen [8]

1. Wat is vulnerability scanning?

Vulnerability scanning is het geautomatiseerd doorzoeken van je IT-omgeving op bekende kwetsbaarheden -- zwakke plekken in software, configuraties en systemen die een aanvaller kan misbruiken.

Een scanner vergelijkt je systemen met databases van bekende kwetsbaarheden (CVE's) en rapporteert wat er openstaat, hoe ernstig het is en wat je eraan kunt doen. Het is geen aanval -- het is een gezondheidscheck van je digitale omgeving [9].

TYPEN VULNERABILITY SCANS

TYPE	WAT HET SCANT	WANNEER INZETTEN
Netwerkscan (extern)	Publiek bereikbare systemen: webservers, VPN, e-mail	Minimaal maandelijks -- dit is wat aanvallers als eerste zien
Netwerkscan (intern)	Interne netwerk: servers, werkstations, printers	Maandelijks -- detecteert lateral movement risico's
Webapplicatiescan	Websites en webapplicaties: SQL injection, XSS, OWASP Top 10	Na elke release en maandelijks voor productie
Cloudscan	Cloud-configuraties: AWS, Azure, M365, GCP	Continu -- misconfiguraties zijn de #1 oorzaak van cloud-incidenten
Authenticated scan	Scant met inloggegevens: ziet meer dan een externe aanvaller	Altijd prefereren boven unauthenticated -- 2--5x meer bevindingen
Unauthenticated scan	Scant zonder inloggegevens: simuleert een externe aanvaller	Baseline, maar onvoldoende als enige scantype

> **Authenticated vs unauthenticated**
>
> Een unauthenticated scan ziet alleen wat een buitenstaander ziet. Een authenticated scan logt in op systemen en detecteert 2--5x meer kwetsbaarheden, inclusief ontbrekende patches, verouderde software en configuratiefouten die van buitenaf onzichtbaar zijn [3].

2. Waarom is het belangrijk?

28% van exploits verschijnt binnen 1 dag na publicatie van een kwetsbaarheid. Het window of exploitation krimpt -- scannen is de enige manier om bij te blijven.

28% EXPLOITS BINNEN 1 DAG

Het Verizon DBIR en Edgescan tonen dat 28% van exploits voor bekende kwetsbaarheden beschikbaar is binnen 24 uur na publicatie [3]. Dit betekent dat je minder dan een dag hebt om te patchen voordat aanvallers actief zoeken naar kwetsbare systemen. Zonder scanning weet je niet welke systemen kwetsbaar zijn.

43% MKB GETROFFEN

Volgens de CBS Cybersecuritymonitor 2024 had 43% van het Nederlandse MKB in 2024 te maken met een security-incident [6]. Een groot deel hiervan was te voorkomen geweest met structureel vulnerability scanning en tijdig patchen. Het MKB wordt niet minder aangevallen dan enterprise -- het is een makkelijker doelwit.

WINDOW OF EXPLOITATION KRIMPT

De gemiddelde tijd tussen publicatie van een CVE en de eerste exploit daalt elk jaar. In 2020 was dit gemiddeld 42 dagen. In 2024 is dit gedaald naar minder dan 15 dagen, met 28% binnen 24 uur [3]. Jaarlijks of kwartaal scannen is niet meer voldoende -- maandelijks is het minimum, wekelijks is aanbevolen.

> **DE REALITEIT**
>
> Er worden jaarlijks 25.000+ nieuwe CVE's gepubliceerd. Slechts ~6% wordt daadwerkelijk geexploiteerd [1]. Maar die 6% veroorzaakt 100% van de schade. Vulnerability scanning in combinatie met risicoprioritering (EPSS, KEV) is de enige manier om te focussen op wat ertoe doet.

3. Hoe werkt het?

Vulnerability scanning is meer dan een knop indrukken. Het volledige proces omvat inventarisatie, scanning, triage, remediatie en verificatie.

HET SCANPROCES IN 5 STAPPEN

1 **Asset-inventarisatie**

VOORAF

Breng alle systemen in kaart: servers, werkstations, netwerkapparatuur, cloud-diensten, webapplicaties. Je kunt niet beveiligen wat je niet kent.

2 **Scanning**

GEAUTOMATISEERD

De scanner vergelijkt je systemen met CVE-databases en configuratie-benchmarks. Authenticated scans voor interne systemen, unauthenticated voor extern aanvalsvlak.

3 **Triage en prioritering**

NA ELKE SCAN

Niet elke kwetsbaarheid is even urgent. Prioriteer op basis van CVSS-score, EPSS-kans op exploitatie en opname in de KEV-catalogus (Known Exploited Vulnerabilities).

4 **Remediatie**

VOLGENS SLA

Patch of mitigeer kwetsbaarheden volgens prioriteit. Kritiek: binnen 24--48 uur. Hoog: binnen 7 dagen. Medium: binnen 30 dagen. Laag: volgende patchcyclus.

5 **Verificatiescan**

NA REMEDIATIE

Scan opnieuw om te bevestigen dat de kwetsbaarheid is verholpen. Zonder verificatie weet je niet of de patch effectief is.

AUTHENTICATED VS UNAUTHENTICATED

KENMERK	AUTHENTICATED	UNAUTHENTICATED
Wat het ziet	Alles: patches, configuratie, software-inventaris	Alleen wat extern zichtbaar is

KENMERK	AUTHENTICATED	UNAUTHENTICATED
Aantal bevindingen	2--5x meer dan unauthenticated	Beperkt tot extern aanvalsvlak
False positives	Lager -- kan verifieeeren of patches zijn geinstalleerd	Hoger -- kan niet verifieren
Setup	Vereist inloggegevens en configuratie	Geen setup nodig
Aanbeveling	Standaard voor alle interne scans	Alleen als aanvulling op authenticated

FREQUENTIE

TYPE OMGEVING	MINIMALE FREQUENTIE	AANBEVOLEN
Extern aanvalsvlak	Maandelijks	Wekelijks tot continu
Intern netwerk	Maandelijks	Wekelijks
Webapplicaties	Na elke release	Na elke release + maandelijks
Cloud-configuratie	Wekelijks	Continu
Na grote wijzigingen	Altijd	Altijd

TIP

Plan scans buiten kantooruren om impact op productiesystemen te minimaliseren. Authenticated scans op databases en kritieke servers kunnen performance beynvloeden -- test eerst in een acceptatieomgeving.

4. Wat kost het?

De kosten van vulnerability scanning varieren van EUR 2.000/jaar voor een klein MKB tot EUR 50.000+/jaar voor enterprise met managed service.

KOSTEN PER BEDRIJFSGROOTTE

ORGANISATIEGROOTTE	SELFSERVICE (EUR/JAAR)	MANAGED SERVICE (EUR/JAAR)
Micro (1--10 pers.)	1.500--3.000	3.000--6.000
Klein MKB (10--50 pers.)	2.500--6.000	5.000--12.000
Middelgroot MKB (50--100 pers.)	5.000--12.000	10.000--25.000
Groot MKB (100--250 pers.)	8.000--20.000	18.000--40.000
Enterprise (250+ pers.)	15.000--40.000	30.000--75.000+

PRIJSMODELLEN

MODEL	HOE HET WERKT	GESCHIKT VOOR
Per IP-adres	Vast bedrag per gescand IP-adres	Kleine omgevingen met weinig externe systemen
Per asset	Vast bedrag per gescand apparaat/systeem	Voorspelbare omgevingen
Flat fee / tier	Vast maandbedrag op basis van organisatiegrootte	Meest voorspelbaar, aanbevolen voor MKB
Per scan	Betaal per uitgevoerde scan	Incidenteel scannen (niet aanbevolen als structureel)

VERBORGEN KOSTEN

- **Remediatie** -- scanning vindt kwetsbaarheden, maar fixen kost tijd en geld. Reken op 2--4 uur per kritieke kwetsbaarheid
- **Authenticated scan setup** -- configuratie van scanaccounts, firewall-regels en credentials management
- **False positive triage** -- zonder expert-triage besteed je uren aan het beoordelen van niet-bestaande kwetsbaarheden
- **Rapportage en compliance** -- sommige platformen rekenen extra voor NIS2-compliance rapportages

- **Extra scantypen** -- webapplicatie- en cloudscans zijn vaak aparte modules met eigen licentiekosten

> **ROI-berekening**
>
> Een MKB-investering van EUR 8.000/jaar in vulnerability scanning vs. gemiddelde schade van EUR 270.000 per incident [2]. Als scanning de kans op een incident met 30% verlaagt (conservatief -- kwetsbaarheden zijn bij 60% van breaches de initiiele aanvalsvector [10]), is de besparing EUR 81.000 in verwachte schade per jaar.

5. Waar moet je op letten?

Niet elke vulnerability scanning oplossing is gelijk. Deze selectiecriteria helpen je de juiste keuze te maken.

SELECTIECRITERIA

CRITERIUM	WAAROM BELANGRIJK
Cloud-native	Geen on-premise hardware nodig, schaalt mee met je omgeving, automatische updates van CVE-database [4]
EPSS-integratie	Exploit Prediction Scoring System: berekent de kans dat een kwetsbaarheid daadwerkelijk wordt misbruikt. Voorkomt dat je 25.000 CVE's handmatig moet prioriteren [1]
Authenticated scanning	Detecteert 2--5x meer kwetsbaarheden dan unauthenticated. Is een must voor intern scannen
Rapportage op management-niveau	Technische rapporten voor IT, executive summaries voor directie, compliance-overzichten voor auditors
NIS2-compliance mapping	Automatische mapping van bevindingen naar NIS2 Art. 21 maatregelen
Patch management integratie	Directe koppeling met je patchsysteem zodat gevonden kwetsbaarheden automatisch in de patch-pipeline terechtkomen
Multi-omgeving	Ondersteunt netwerk, web, cloud en containers vanuit een platform
SLA voor CVE-database updates	Hoe snel worden nieuwe CVE's opgenomen? Binnen 24 uur is de norm
False positive rate	Hoge false positive rates leiden tot alert fatigue. Vraag naar benchmarks en triage-services
API en integraties	Koppeling met SIEM, ticketsysteem en CI/CD pipeline voor geautomatiseerde workflows

10 VRAGEN AAN JE LEVERANCIER

1. Ondersteunen jullie authenticated scanning voor alle OS-types?
2. Hoe snel worden nieuwe CVE's opgenomen in de scandatabase?

3. Bieden jullie EPSS-gebaseerde prioritering?
4. Wat is de gemiddelde false positive rate na triage?
5. Ondersteunen jullie cloud-configuratiescans (AWS, Azure, M365)?
6. Hoe integreren jullie met onze patch management tooling?
7. Bieden jullie NIS2-compliance rapportages?
8. Wat is inbegrepen bij "managed" -- alleen scanning of ook triage en advies?
9. Hoe werkt het prijsmodel bij groei van het aantal assets?
10. Kunnen we scan-resultaten exporteren naar ons SIEM of ticketsysteem via API?

> **LET OP: SCANNING ZONDER OPVOLGING**
>
> Een scan die 200 kwetsbaarheden vindt maar niet leidt tot actie, creert een vals gevoel van veiligheid. Zorg dat je de capaciteit hebt om bevindingen op te volgen -- intern of via een managed service die triage en remediatie-advies biedt.

6. Veelgemaakte fouten

Deze acht valkuilen ondermijnen de effectiviteit van je vulnerability management programma.

1. Scannen zonder opvolging

De meest voorkomende fout: regelmatig scannen maar niets doen met de resultaten. Een kwetsbaarheidsrapport dat in een la belandt, beschermt niemand. Koppel elke scan aan een remediatieproces met duidelijke eigenaren en deadlines [9].

2. Vulnerability management als project

Een eenmalige scan is een momentopname. Nieuwe kwetsbaarheden verschijnen dagelijks. Vulnerability management is een doorlopend proces, geen project. Organisaties die het als project behandelen, vervallen na de eerste scan weer in de oude situatie [5].

3. Alleen extern scannen

Externe scans tonen wat een aanvaller van buitenaf ziet. Maar de meeste schade ontstaat na initiele toegang -- via lateral movement, privilege escalation en toegang tot interne systemen. Interne scans met authenticated credentials zijn minstens zo belangrijk als externe scans.

4. Geen asset-inventaris

Je kunt niet scannen wat je niet kent. Schaduw-IT, vergeten testservers, oude webapplicaties -- dit zijn de systemen die het eerst worden gecompromitteerd. Begin elke vulnerability management cyclus met een actuele asset-inventaris [4].

5. CVSS als enige prioriteringscriterium

CVSS meet de technische ernst van een kwetsbaarheid, niet de kans op exploitatie. Een CVSS 9.8 kwetsbaarheid die in de praktijk niet wordt misbruikt, is minder urgent dan een CVSS 7.0 die actief wordt geexploiteerd. Combineer CVSS met EPSS (exploitatiekans) en de KEV-catalogus (bevestigde exploitatie) voor een realistischer beeld [1].

6. Patch management niet geintegreerd

Vulnerability scanning en patch management zijn twee kanten van dezelfde medaille. Als je scansysteem niet automatisch kwetsbaarheden doorstuurt naar je patchsysteem, ontstaan er handmatige tussenstappen die vertragen en foutgevoelig zijn.

7. Compliance als doel in plaats van middel

Scannen omdat de auditor het vraagt, niet omdat je wilt weten of je kwetsbaar bent. Het resultaat: een minimale scan op het minimale aantal systemen, net genoeg om het vinkje te zetten. Dit beschermt tegen auditors, niet tegen aanvallers [7].

8. Geen communicatie met management

Als management niet weet welke risico's er zijn, worden er geen middelen vrijgemaakt voor remediatie. Vertaal technische bevindingen naar bedrijfsrisico's: "We hebben 12 kritieke kwetsbaarheden op systemen die klantdata verwerken. Zonder patch lopen we EUR X risico." Dat is een taal die budget vrijmaakt.

7. Compliance: NIS2

De Cyberbeveiligingswet (NIS2-implementatie) maakt kwetsbaarheidsbeheer wettelijk verplicht voor ~10.000 Nederlandse organisaties.

ART. 21 LID 2: KWETSBAARHEIDSBEHEER

NIS2 Artikel 21, lid 2 verplicht essentiele en belangrijke entiteiten tot het nemen van maatregelen voor "beveiliging bij de verwerving, ontwikkeling en het onderhoud van netwerk- en informatiesystemen, met inbegrip van de respons op en de bekendmaking van kwetsbaarheden". Vulnerability scanning is de directe invulling van deze verplichting [7].

CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet -- de Nederlandse implementatie van NIS2 -- treedt naar verwachting in Q2 2026 in werking. De wet vertaalt de Europese eisen naar Nederlandse wetgeving en stelt concrete handhavingsmechanismen vast. Kwetsbaarheidsbeheer wordt een aantoonbare verplichting [11].

BOETES EN BESTUURDERSAANSPRAKELIJKHEID

TYPE ENTITEIT	MAXIMALE BOETE
Essentiele entiteiten	EUR 10.000.000 of 2% van de wereldwijde jaaromzet
Belangrijke entiteiten	EUR 7.000.000 of 1,4% van de jaaromzet

NIS2 introduceert bestuurdersaansprakelijkheid: bestuurders kunnen persoonlijk aansprakelijk worden gesteld als de organisatie niet aan de zorgplicht voldoet. Dit geldt expliciet voor het niet implementeren van kwetsbaarheidsbeheer [11].

TIP

Gebruik je vulnerability scanning rapportages als bewijs bij NIS2-audits. Een dashboard dat aantoont dat je structureel scant, prioriteert op basis van risico en kwetsbaarheden tijdig verhelpt, is het sterkste compliance-bewijs dat je kunt leveren.

8. Scanning vs pentest vs bug bounty

Vulnerability scanning, penetration testing en bug bounty programma's vullen elkaar aan. Hieronder de afbakening.

KENMERK	VULNERABILITY SCANNING	PENETRATION TESTING	BUG BOUNTY
Aanpak	Volledig geautomatiseerd	Handmatig + geautomatiseerd door specialisten	Crowdsourced: onafhankelijke onderzoekers
Doel	Bekende kwetsbaarheden identificeren	Kwetsbaarheden exploiteren en impact aantonen	Onbekende kwetsbaarheden vinden
Scope	Breed: alle systemen	Diep: specifieke systemen of scenario's	Open: alles wat in scope is gedefinieerd
Frequentie	Continu tot wekelijks	Jaarlijks tot halfjaarlijks	Continu (doorlopend programma)
Output	CVE-lijst met CVSS/ EPSS-scores	Exploitatiebewijs met impactanalyse	Individuele kwetsbaarheidsrapporten
False positives	Relatief hoog (5--20%)	Laag (handmatig geverifieerd)	Laag (bewezen door onderzoeker)
Kosten MKB	EUR 5.000--15.000/jaar	EUR 5.000--50.000 per test	EUR 500--10.000 per bounty

MATURITEITSMODEL: DRIE FASES

FASE	WAT JE DOET	WANNEER
1. Basis	Geautomatiseerde vulnerability scanning (extern + intern, authenticated)	Nu starten -- dit is de minimale baseline
2. Verdieping	Jaarlijkse penetration test op kritieke systemen + doorlopende scanning	Als scanning structureel draait en remediatie op orde is
3. Volwassen	Bug bounty programma + continue scanning + periodieke pentests + CTEM	Enterprise-niveau: maximale dekking van bekende en onbekende kwetsbaarheden

Begin met scanning, niet met pentesting

Een penetration test op een omgeving die vol staat met bekende, ongepatchte kwetsbaarheden is verspild geld -- de pentester vindt dezelfde kwetsbaarheden die een scanner in 30 minuten had gevonden. Zorg eerst dat je scanning en patching op orde zijn. Pas dan heeft een pentest meerwaarde: het vindt kwetsbaarheden die een scanner mist [9].

9. Trends

Vier ontwikkelingen die vulnerability scanning de komende jaren veranderen.

1. CTEM: Continuous Threat Exposure Management

Gartner introduceert CTEM als opvolger van traditioneel vulnerability management. CTEM gaat verder dan scannen: het combineert vulnerability scanning, attack surface management, threat intelligence en business context tot een doorlopend programma dat risico's prioriteert op basis van daadwerkelijke dreiging. Organisaties die CTEM toepassen, ervaren 3x minder breaches [5].

2. Attack Surface Management (ASM)

ASM breidt vulnerability scanning uit naar het volledige externe aanvalsvlak: vergeten subdomeinen, schaduw-IT, cloud-diensten die niet in je inventaris staan. De ASM-markt groeit naar $5,2 miljard in 2030 [4]. ASM detecteert wat je niet wist dat je had -- en dat is vaak het zwakste punt.

3. AI-powered scanning en prioritering

AI versnelt de triage van scanresultaten: automatische false positive reductie, contextbewuste prioritering en voorspellende analyse van welke kwetsbaarheden het eerst worden misbruikt. De combinatie van CVSS + EPSS + KEV + AI maakt het mogelijk om van 25.000 CVE's per jaar te focussen op de 50 die er echt toe doen [1].

4. CVSS + EPSS + KEV: drielaags prioritering

De industrie beweegt weg van CVSS als enige prioriteringscriterium. De nieuwe standaard is een drielaags model:

- **CVSS** -- Technische ernst van de kwetsbaarheid (hoe erg kan het zijn?)
- **EPSS** -- Kans op exploitatie binnen 30 dagen (hoe waarschijnlijk is het?)
- **KEV** -- Bevestigde actieve exploitatie (wordt het nu misbruikt?)

Dit drielaags model reduceert het aantal "kritieke" kwetsbaarheden van duizenden naar tientallen -- beheersbaar voor elk MKB [1].

WAT BETEKENT DIT VOOR JOU?

Vulnerability scanning evolueert van een periodieke scan naar een doorlopend programma dat je aanvalsvlak continu in kaart brengt en risico's prioriteert op basis van echte dreigingsdata. Begin met basis vulnerability scanning en groei naar CTEM als je maturiteit toeneemt.

10. Aan de slag

Je weet nu wat vulnerability scanning is, wat het kost, hoe je het opzet en waar je op moet letten. Tijd om te handelen.

DRIE STAPPEN OM TE STARTEN

1 **Bepaal je situatie**

Heb je een actuele asset-inventaris? Scan je al structureel? Heb je een patchproces? Val je onder NIS2? Als je geen van deze vragen met "ja" kunt beantwoorden, begin dan met een externe scan als baseline.

2 **Vergelijk oplossingen**

Gebruik de 10 vragen uit hoofdstuk 5 om minimaal 3 aanbieders te vergelijken. Let op authenticated scanning, EPSS-integratie, rapportage en patch management koppeling.

3 **Start klein, schaal op**

Begin met externe en interne netwerkscan (authenticated). Voeg webapplicatie- en cloudscans toe na de eerste cyclus. Bouw naar een volledig vulnerability management programma met doorlopende scanning, triage en remediatie.

Bronnenlijst

[1] **FIRST / EPSS** -- Exploit Prediction Scoring System: ~6% van CVE's wordt geexploiteerd. first.org/epss/

[2] **Verzekercyber.nl** -- Gemiddelde schade MKB per cyberincident: EUR 270K. verzekercyber.nl/wat-kost-een-cyberverzekering/

[3] **Edgescan / Verizon DBIR** -- 28% van exploits binnen 1 dag na publicatie. edgescan.com/resources/vulnerability-stats-report/

[4] **Mordor Intelligence** -- Attack Surface Management markt: $5,2B in 2030. mordorintelligence.com/industry-reports/attack-surface-management-market

[5] **Gartner** -- CTEM: organisaties die het toepassen ervaren 3x minder breaches. gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

[6] **CBS** -- Cybersecuritymonitor 2024: 43% MKB incident. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[7] **NIS2-richtlijn** -- Art. 21 lid 2: kwetsbaarheidsbeheer als verplichte maatregel. eur-lex.europa.eu/eli/dir/2022/2555/oj

[8] **Laurus Verzekeringen** -- 60% failliet binnen 6 maanden na ernstige cyberaanval. laurusverzekeringen.nl/cyberverzekeringen-onmisbaar/

[9] **NCSC** -- Basismaatregelen cyberbeveiliging: kwetsbaarheidsbeheer. ncsc.nl/onderwerpen/basismaatregelen

[10] **Verizon** -- Data Breach Investigations Report 2025: vulnerability exploitation als aanvalsvector. verizon.com/business/resources/reports/dbir/

[11] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2): bestuurdersaansprakelijkheid. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[12] **ENISA** -- Good Practices for Vulnerability Disclosure. enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

[13] **Digital Trust Center** -- Kwetsbaarheden in software: herkennen en verhelpen. digitaltrustcenter.nl/informatie-advies/kwetsbaarheden-in-software

[14] **CISA** -- Known Exploited Vulnerabilities Catalog (KEV). cisa.gov/known-exploited-vulnerabilities-catalog

[15] **NIST** -- National Vulnerability Database (NVD): 25.000+ CVE's per jaar. nvd.nist.gov/

[16] **OWASP** -- OWASP Top 10 2021: meest voorkomende webapplicatie-kwetsbaarheden. owasp.org/www-project-top-ten/

[17] **NCSC** -- Cyberbeveiligingswet: veelgestelde vragen en boetestructuur. ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/

[18] **Forrester** -- The State of Vulnerability Risk Management 2024. forrester.com/report/the-state-of-vulnerability-risk-management

[19] **Mandiant / Google Cloud** -- M-Trends 2025: time to exploit daalt verder. mandiant.com/m-trends

[20] **Fox-IT / NCC Group** -- Vulnerability management als doorlopend proces. fox-it.com/vulnerability-management/

[21] **Vodafone Business** -- 77% MKB cybercrime in afgelopen 2 jaar. vodafone.nl/zakelijk/inspiratie/mkb-doelwit-cybercrime-onderzoeken

[22] **IBM** -- Cost of a Data Breach Report 2024: vulnerability exploitation lifecycle. ibm.com/reports/data-breach

Deze gids is samengesteld door IBgids.nl op basis van openbare bronnen en marktonderzoek. Alle genoemde prijzen zijn indicatief (peildatum: maart 2026). IBgids.nl is een onafhankelijk platform en geen leverancier of adviseur.