GIDS

De complete gids voor patch & vulnerability management

Kwetsbaarheden detecteren, patches beheren, compliance aantonen. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De feiten die de urgentie onderbouwen.

50.000+
CVEs gepubliceerd in 2025 -- circa 130 nieuwe kwetsbaarheden per dag
DeepStrike [1]

20%
van datalekken begint met exploitatie van kwetsbaarheden
Verizon DBIR 2025 [2]

33%
van kritieke kwetsbaarheden blijft langer dan 180 dagen ongepatcht
Diverse bronnen [3]

55 dgn
mediaan tijd dat kritieke CISA KEV-kwetsbaarheden ongepatcht blijven na fix
Maze / CISA [4]

EUR 4,88M
gemiddelde kosten van een datalek in 2024 -- 10% stijging t.o.v. vorig jaar
IBM Cost of Data Breach [5]

38%
van gerapporteerde kwetsbaarheden in 2025 is High of Critical (CVSS >= 7)
DeepStrike [1]

32%
van geexploiteerde kwetsbaarheden in H1 2025 betrof zero-day of 1-day exploits
DeepStrike [1]

Q2 2026
verwachte inwerkingtreding Cyberbeveiligingswet -- patchbeleid wordt wettelijke eis
Digitale Overheid [6]

1. Wat is patch & vulnerability management?

Patch & vulnerability management is het gestructureerde proces van het identificeren, classificeren, prioriteren en verhelpen van kwetsbaarheden in software, systemen en firmware.

Het omvat twee samenhangende disciplines: vulnerability management (continu scannen en prioriteren) en patch management (het gestructureerd testen en uitrollen van updates). Samen vormen ze de basis van preventieve cybersecurity. Zonder dit proces is elke andere beveiligingsmaatregel als een slot op een deur die openstaat [1].

KERNFUNCTIES

- **Vulnerability scanning** -- Geautomatiseerd scannen van netwerken, endpoints en applicaties op bekende kwetsbaarheden
- **Risico-gebaseerde prioritering** -- Niet alleen CVSS-score, maar ook exploitability en business impact
- **Patch deployment** -- Geautomatiseerd testen en uitrollen van updates over endpoints en servers
- **Third-party patching** -- Niet alleen het besturingssysteem, ook applicaties zoals browsers, PDF-readers en Java
- **Compliance-rapportages** -- Dashboards en rapporten voor NIS2, ISO 27001 en audits

2. Waarom is het belangrijk?

Kwetsbaarheden worden sneller geexploiteerd dan ooit. Zonder gestructureerd patchbeheer loop je achter de feiten aan.

In 2025 werden meer dan 50.000 CVEs gepubliceerd -- circa 130 per dag [1]. Vulnerability exploitation was de initiële toegangsmethode in 20% van alle datalekken [2]. De gemiddelde tijd tot exploitatie is inmiddels negatief: aanvallers exploiteren kwetsbaarheden vaker voordat patches beschikbaar zijn [1].

Het NCSC publiceert dagelijks Security Advisories en benadrukt dat normale patches binnen 30 dagen geinstalleerd moeten worden, en kritieke patches binnen 48-72 uur [7]. In de praktijk blijft 33% van kritieke kwetsbaarheden langer dan 180 dagen ongepatcht [3].

> **DE KOSTEN VAN NIET-PATCHEN**
>
> Een gemiddeld datalek kost USD 4,88 miljoen [5]. Voor Nederlands MKB liggen de kosten per cyberincident tussen EUR 20.000 en EUR 200.000 [8]. VPN-appliances van Fortinet en Ivanti behoren tot de meest geexploiteerde systemen -- allemaal door bekende, patchbare kwetsbaarheden [9].

3. Hoe werkt het? Het proces

Kwetsbaarhedenbeheer is een cyclisch proces. Het NCSC beschrijft vijf fasen: beoordelen, prioriteren, behandelen, evalueren, verbeteren.

1 Inventarisatie en scanning

WEEK 1--2

Scan je volledige IT-omgeving: servers, endpoints, netwerkapparatuur en applicaties. Gebruik een vulnerability scanner die zowel agent-based als agentless kan werken.

2 Prioritering

DOORLOPEND

Prioriteer op basis van risico, niet alleen CVSS-score. Kijk naar exploitability (is er een exploit beschikbaar?), business impact en bereikbaarheid van het systeem.

3 Patching en remediation

DOORLOPEND

Rol patches uit via een geautomatiseerd platform. Test eerst in een staging-omgeving. Kritieke patches binnen 48-72 uur, normale patches binnen 30 dagen [7].

4 Verificatie

NA ELKE PATCHRONDE

Scan opnieuw om te verifiëren dat patches succesvol zijn toegepast. Documenteer uitzonderingen en compenserende maatregelen voor systemen die niet gepatcht kunnen worden.

5 Rapportage en verbetering

MAANDELIJKS

Rapporteer KPIs: patch compliance rate, Mean Time to Patch, aantal openstaande kritieke kwetsbaarheden. Gebruik deze data om het proces te verbeteren.

4. Wat kost het?

De investering in patch & vulnerability management varieert van EUR 2.000 per jaar (basis scanning) tot EUR 40.000+ per jaar (volledig managed).

TIER	WAT JE KRIJGT	PRIJSINDICATIE	GESCHIKT VOOR
Basis	Vulnerability scanning, basisrapportages	EUR 2.000--5.000/jaar	MKB tot 50 assets
Standaard	Scanning + patch management, third-party patching, compliance-rapportages	EUR 5.000--15.000/jaar	MKB 50--250 endpoints
Premium	Volledig managed: scanning, patching, prioritering, rapportage, 24/7 monitoring	EUR 15.000--40.000/jaar	MKB 250+ endpoints

5. Waar moet je op letten bij de selectie?

Niet elke oplossing biedt dezelfde breedte en diepte. Hier zijn de criteria die ertoe doen.

- **Breedte van scanning** -- OS, applicaties, netwerk, containers, cloud
- **Third-party patching** -- Niet alleen Windows Updates maar ook browsers, Java, Adobe, etc.
- **Risico-gebaseerde prioritering** -- Exploitability en business context, niet alleen CVSS
- **Automatiseringsgraad** -- Automatische patch deployment met rollback-mogelijkheid
- **Integratie met SIEM/SOAR** -- Geautomatiseerde workflows en ticketing
- **Compliance-rapportages** -- NIS2, ISO 27001, SOC 2 ready reports

6. Veelgemaakte fouten

De meeste patchproblemen zijn organisatorisch, niet technisch.

1. Alleen scannen zonder prioriteren

Honderden kwetsbaarheden zonder duidelijke actievolgorde leidt tot analysis paralysis. Focus op de 5-10 kwetsbaarheden met het hoogste werkelijke risico.

2. Patchen uitstellen vanwege angst voor downtime

Het risico van niet-patchen is bijna altijd groter dan het risico van de patch zelf. Test patches in staging en plan maintenance windows.

3. Third-party applicaties vergeten

75%+ van kwetsbaarheden zit in applicaties, niet in het besturingssysteem. Browsers, PDF-readers en Java moeten ook gepatcht worden.

4. Geen exception management

Systemen die niet gepatcht kunnen worden (legacy, OT) moeten compenserende maatregelen krijgen: netwerksegmentatie, virtual patching, extra monitoring.

7. Compliance: NIS2 en regelgeving

Kwetsbaarhedenbeheer valt expliciet onder de zorgplicht van de Cyberbeveiligingswet (NIS2).

Het NCSC beschrijft kwetsbaarhedenbeheer als een cyclisch proces in vijf fasen en biedt een toolbox voor implementatie [7]. De NORA-standaarden voor de overheid benoemen patchmanagement als vereist beheerproces. ISO 27001 Annex A.12.6 vereist formeel beheer van technische kwetsbaarheden.

Boetes onder de Cyberbeveiligingswet: tot EUR 10 miljoen of 2% mondiale jaaromzet voor essentiele entiteiten. Kwetsbaarheden in VPN-appliances en netwerkapparatuur zijn een belangrijke meldcategorie bij het NCSC.

8. Verschil met verwante oplossingen

Patch management is niet hetzelfde als vulnerability management, en geen van beide vervangt een pentest.

KENMERK	VULNERABILITY MANAGEMENT	PATCH MANAGEMENT	PENTEST
Doel	Kwetsbaarheden detecteren en prioriteren	Patches testen en uitrollen	Kwetsbaarheden actief exploiteren
Frequentie	Continu (dagelijks/wekelijks)	Continu (dagelijks/ wekelijks)	Periodiek (jaarlijks/ kwartaal)
Scope	Alle bekende CVEs	Beschikbare patches	Gerichte exploitatie
Output	Prioriteitenlijst	Gepatcte systemen	Exploitatierapport

9. Trends 2025--2026

1. AI-gedreven prioritering

Machine learning voorspelt welke kwetsbaarheden daadwerkelijk geexploiteerd zullen worden, zodat je niet alles tegelijk hoeft te patchen.

2. Continuous Threat Exposure Management (CTEM)

Van periodiek scannen naar continue blootstelling-analyse: real-time inzicht in je aanvalsoppervlak.

3. Virtual patching

WAF- en IPS-regels als tijdelijke mitigatie wanneer patchen niet direct mogelijk is, met name voor legacy systemen.

10. Aan de slag

Start met een vulnerability scan van je huidige omgeving. Veel aanbieders bieden een gratis initiële scan aan.

Breng in kaart hoeveel assets je hebt, welke kritiek zijn voor je bedrijfsvoering, en wat je huidige patchstatus is. Bepaal of je self-service wilt of een managed service. De investering is bescheiden vergeleken met de kosten van een incident door een bekende kwetsbaarheid.

Bronnenlijst

[1] **DeepStrike** -- Vulnerability Statistics 2025. deepstrike.io/blog/vulnerability-statistics-2025

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

[3] **Edgescan** -- Vulnerability Statistics Report 2025. info.edgescan.com/hubfs/23DOWNLOADABLE%20CONTENT/Vulnerability%20Statistics%20Reports/Edgescan_VulnerabilityStatsReport_2025.pdf

[4] **Maze** -- 2025: The Year Vulnerabilities Broke Every Record. mazehq.com/blog/2025-wrapped-the-year-vulnerabilities-broke-every-record

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

[6] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2-richtlijn). digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[7] **NCSC** -- Kwetsbaarhedenbeheer. ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren/kwetsbaarhedenbeheer

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

[9] **CISA** -- Fortinet Advisory. cisa.gov/news-events/alerts/2025/04/11/fortinet-releases-advisory-new-post-exploitation-technique-known-vulnerabilities

[10] **NCSC** -- Security Advisories. ncsc.nl/dienstverlening/security-advisories

[11] **NCSC** -- Basisprincipe 3. ncsc.nl/wat-kun-je-zelf-doen/basisprincipes/bescherm-systemen-applicaties-en-apparaten

[12] **Mordor Intelligence** -- Security & Vulnerability Management Market. mordorintelligence.com/industry-reports/security-and-vulnerability-management-market

[13] **MarketsandMarkets** -- Vulnerability Management Market. marketsandmarkets.com/Market-Reports/security-vulnerability-management-market-204180861.html

[14] **CBS** -- Cybersecuritymonitor 2024. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[15] **Rapid7** -- 2024 Threat Landscape Statistics. rapid7.com/blog/post/2024/12/16/2024-threat-landscape-statistics-ransomware-activity-vulnerability-exploits-and-attack-trends/