

example.com

SCAN-ZEITPUNKT 21.09.2026, 08:00	UMFANG Passiv und aktiv (mit Portprüfung) + OpenVAS	GEPRÜFTE HOSTS 8	QUELLEN crt.sh, certspotter
-------------------------------------	--	---------------------	--------------------------------

EXPOSURE-SCORE

36 / 100



Durchschnittliche Priorität aller Befunde, 0 bis 100. Je niedriger, desto besser.

BEFUNDE: 10

0 KRITISCH	3 HOCH	3 MITTEL	4 NIEDRIG
---------------	-----------	-------------	--------------

Das Wichtigste in Kürze

Diese Befunde sollten Sie zuerst angehen. Sie verbinden hohen Schweregrad mit der Bedeutung des betroffenen Systems.

PRIÖ	SCHWEREGRAD	BEFUND UND EMPFEHLUNG
61	HOCH	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	HOCH	vpn.example.com RDP aus dem Internet erreichbar (Port 3389) → Port in der Firewall schließen oder auf bekannte IP-Adressen beschränken.
56	HOCH	shop.example.com Verwaltungsoberfläche öffentlich erreichbar (phpMyAdmin) → Nur über VPN oder eine IP-Freigabeliste erreichbar machen.
34	MITTEL	dev.example.com Entwicklungs- oder Testsystem öffentlich erreichbar → Hinter Anmeldung, VPN oder IP-Freigabe legen, nicht mehr benötigte Systeme abschalten.
34	MITTEL	mail.example.com TLS-Zertifikat läuft in 9 Tagen ab → Zertifikat erneuern und prüfen, ob die automatische Verlängerung funktioniert.

Alle Befunde nach Host

example.com

PRIORITÄT	SCHWEREGRAD	BEFUND UND EMPFEHLUNG
24	NIEDRIG	DMARC steht auf p=none, gefälschte Mails werden nicht abgewiesen → Nach Auswertung der Berichte auf p=quarantine oder p=reject erhöhen.

www.example.com

PRIORITÄT	SCHWEREGRAD	BEFUND UND EMPFEHLUNG
24	NIEDRIG	Softwareversion im Header Server sichtbar (Apache/2.4.49) → Versionsangabe im Webserver abschalten (z. B. server_tokens off, ServerTokens Prod).
20	NIEDRIG	Content-Security-Policy fehlt → Eine Content-Security-Policy festlegen, die nur benötigte Quellen erlaubt.

shop.example.com

PRIORITÄT	SCHWEREGRAD	BEFUND UND EMPFEHLUNG
56	HOCH	Verwaltungsoberfläche öffentlich erreichbar (phpMyAdmin) → Nur über VPN oder eine IP-Freigabeliste erreichbar machen.
32	MITTEL	HSTS-Header fehlt → Header Strict-Transport-Security: max-age=31536000; includeSubDomains setzen.

mail.example.com

PRIORITÄT	SCHWEREGRAD	BEFUND UND EMPFEHLUNG
34	MITTEL	TLS-Zertifikat läuft in 9 Tagen ab → Zertifikat erneuern und prüfen, ob die automatische Verlängerung funktioniert.

vpn.example.com

PRIORITÄT	SCHWEREGRAD	BEFUND UND EMPFEHLUNG
61	HOCH	OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	HOCH	RDP aus dem Internet erreichbar (Port 3389) → Port in der Firewall schließen oder auf bekannte IP-Adressen beschränken.

dev.example.com

PRIO SCHWEREGRAD BEFUND UND EMPFEHLUNG

34	MITTEL	Entwicklungs- oder Testsystem öffentlich erreichbar → Hinter Anmeldung, VPN oder IP-Freigabe legen, nicht mehr benötigte Systeme abschalten.
----	--------	---

portal.example.com

PRIO SCHWEREGRAD BEFUND UND EMPFEHLUNG

17	NIEDRIG	X-Content-Type-Options fehlt → X-Content-Type-Options: nosniff setzen.
----	---------	---

Ohne Befunde

cdn.example.com

Methode und Grenzen

Subdomains stammen aus öffentlichen Zertifikatslogs (Certificate Transparency). Geprüft wurden nur Hosts, die sich per DNS auflösen lassen.

Pro Host wurden das TLS-Zertifikat, die Weiterleitung von HTTP auf HTTPS, die Sicherheits-Header der Startseite und erkennbare Verwaltungsoberflächen geprüft, für die Hauptdomain zusätzlich SPF und DMARC.

Ein passiver Scan prüft keine offenen Ports und dringt nicht in Anwendungen ein. Er zeigt, was von außen ohne Zugangsdaten sichtbar ist.

Der Bericht ist eine Momentaufnahme zum angegebenen Zeitpunkt. Die Priorität ist eine Einschätzung und ersetzt keinen Penetrationstest.

Zusätzlich wurde mit OpenVAS (Greenbone) ein aktiver Schwachstellenscan der öffentlichen Adressen durchgeführt. Grundlage ist der nachgewiesene Besitz der Domain. Übernommen wurden nur Befunde mit einer Erkennungsqualität von mindestens 70 Prozent.

Nächste Schritte

Wir besprechen den Bericht gern mit Ihnen und zeigen, wie veyrisk Ihre Angriffsfläche laufend überwacht, statt nur einmal hinzusehen.

KONTAKT

neonotu GmbH
Edelsbergstraße 8, 80686 München
+49 89 2000 7975 0 · contact@veyrisk.com