CyberDirekt

Whitepaper Schwachstellenscans

Marktüberblick und Entscheidungshilfe

Was Schwachstellenscans im Rahmen der Cyber-Prävention leisten, wie sich einzelne Scan-Arten unterscheiden und wie Unternehmen den richtigen Anbieter finden können.

02 / 2026

CyberDirekt

Whitepaper Schwachstellenscans

1 Schwachstellenscans als zentraler Bestandteil moderner Cyber Sicherheitsstrategien

Angesichts der wachsenden Dynamik der Cyber-Bedrohungslandschaft können sich Unternehmen nicht mehr auf punktuelle Sicherheitsprüfungen verlassen. Neue Schwachstellen und Angriffsmethoden entstehen nahezu wöchentlich, wodurch ein kontinuierliches Monitoring der IT-Infrastruktur an Bedeutung gewinnt. **Schwachstellenscans** haben sich in diesem Umfeld als **zentraler Bestandteil moderner Cyber-Sicherheitsstrategien etabliert**. Sie ermöglichen es, potenzielle Einfallstore automatisiert zu identifizieren und Risiken zu priorisieren, bevor Angreifer sie ausnutzen.

Parallel dazu hat sich die **Technologie mittlerweile auch im Bereich der Cyberversicherung etabliert**. Wie die CyberDirekt Marktanalyse 2024 gezeigt hat, integrieren immer mehr Versicherer Schwachstellenscans in ihre Risikoprüfung, wobei vor allem neue Marktteilnehmer vermehrt auf Scan-Technologien setzen. Unternehmen profitieren dabei doppelt. Zum einen durch eine verbesserte Transparenz über den eigenen IT-Reifegrad und zum anderen durch die Möglichkeit, Schwachstellen gezielt zu beheben. Einige Versicherungsanbieter honorieren zudem gute Scan-Ergebnisse mit günstigeren Prämien oder besseren Versicherungsbedingungen.

Die am Markt erhältlichen Angebote für Schwachstellenscans unterscheiden sich allerdings im Umfang der enthaltenen Leistungen und durchgeführten Tests. Das Ziel dieses Whitepapers ist es, mehr Transparenz über die Leistungen und Merkmale von Schwachstellenscans zu schaffen. Dazu haben wir die **Angebote von elf führenden Anbietern von Schwachstellenscans analysiert** und ausgewertet, darunter sowohl große Cyberversicherer als auch spezialisierte Security-Rating-Dienste. Im Anschluss an die vergleichende Analyse liefern wir Ihnen eine praktische Liste an **Kriterien für die Auswahl eines geeigneten Anbieters**, wenn Sie einen Schwachstellenscan außerhalb einer Cyberversicherung beauftragen möchten.

2 Schwachstellenscans in der Übersicht: Umfang, Vorteile, Nachteile und Nutzen

Angesichts der wachsenden Zahl und Komplexität digitaler Angriffe können sich Unternehmen nicht mehr darauf verlassen, Bedrohungen erst im Schadensfall zu erkennen. Schwachstellenscans ermöglichen es, **Sicherheitslücken** in der eigenen IT-Infrastruktur **proaktiv zu identifizieren**, bevor sie von Angreifern ausgenutzt werden.

2.1 Was beinhalten Schwachstellenscans?

Moderne Schwachstellenscanner überprüfen eine Vielzahl technischer und sicherheitsrelevanter Aspekte. Sie beschränken sich nicht nur auf das einfache Aufspüren offener Ports, sondern bieten je nach Anbieter einen ganzheitlichen Außenblick auf die IT-Sicherheitslage: von technischen Schwachstellen über Konfigurationsfehler bis hin zu Leaks und Bedrohungsindikatoren. Typischerweise sind dabei die folgenden Kernkomponenten enthalten:

- **Netzwerk- und Port-Scans:** Externe Systeme werden auf offene Ports und aktive Dienste überprüft. Dabei wird erfasst, welche Software (inklusive Versionsstand) hinter einem Port betrieben wird, um bekannte Schwachstellen zu identifizieren. Befunde wie „Port 3389 (RDP) offen" gelten als potenzielle Risiken, da unnötig erreichbare Dienste Angriffsflächen bieten.
- **Überprüfung von Konfigurationen (TLS/SSL, Header etc.):** Viele Anbieter bewerten die Sicherheit von Web- und Mail-Diensten, etwa durch die Analyse der unterstützten TLS-/SSL-Protokolle, Cipher-Suites und Zertifikate. Auch HTTP-Sicherheitsheader sowie E-Mail-Standards wie SPF oder DKIM werden häufig überprüft. Abweichungen von Best Practices, wie z. B. abgelaufene Zertifikate oder unsichere Algorithmen, fließen als negative Befunde in die Bewertung ein.
- **Abgleich mit Schwachstellendatenbanken:** Das zentrale Element jedes Scans bildet der Vergleich erkannter Softwarestände mit bekannten Schwachstellen aus CVE-Datenbanken. Führende Anbieter greifen dabei auf umfangreiche, tagesaktuell gepflegte Wissensdatenbanken mit Millionen Einträgen zurück, um neu entdeckte Sicherheitslücken zeitnah zu erkennen.
- **Darknet- und Datenleck-Suche:** Einige Dienste erweitern den Scan um eine Überwachung des Darknets und anderer Quellen auf kompromittierte Unternehmensdaten. Wird beispielsweise festgestellt, dass Zugangsdaten von Mitarbeitenden in Leak-Datenbanken oder Untergrundforen auftauchen, erhält das Unternehmen eine Warnung, um Gegenmaßnahmen einzuleiten.
- **Malware- und Botnet-Indikatoren:** Fortgeschrittene Anbieter integrieren Threat-Intelligence-Daten, um zu prüfen, ob IP-Adressen oder Domains bereits in Spam-, Botnet- oder Ransomware-Indikatoren-Listen geführt werden. Teilweise werden eigene Honeypots oder Sensor-Netzwerke betrieben, um Aktivitäten von Angreifern zu erfassen und in die Risikoanalyse einfließen zu lassen.

2.2 Einsatz und Nutzen von Schwachstellenscans

Schwachstellenscans sind ein **zentrales Instrument des IT-Risikomanagements** und erfüllen mehrere strategische und operative Zwecke. Sie liefern nicht nur technische Befunde, sondern schaffen eine Grundlage für Priorisierung, Compliance, Bewertung und Sensibilisierung.

CyberDirekt

Strategische und operative Ziele von Schwachstellenscans

Risikopriorisierung

Durch die Bewertung identifizierter Schwachstellen nach Kritikalität können Unternehmen ihre Sicherheitsmaßnahmen gezielt auf die dringlichsten Risiken ausrichten und Ressourcen effizient einsetzen.

Compliance-Unterstützung

Viele regulatorische Rahmenwerke und Sicherheitsstandards schreiben regelmäßige Schwachstellenprüfungen vor. Scans helfen, diese Anforderungen nachweisbar zu erfüllen und die Audit-Readiness des Unternehmens sicherzustellen.

Risikoprüfung

Versicherer nutzen Scan-Ergebnisse als objektive Basis, um das Sicherheitsniveau und damit die Versicherbarkeizvon Antragstellern zu beurteilen und Risiken laufend zu überwachen.

Sensibilisierung und Awareness

Die Reports zeigen konkrete Schwachstellen und Handlungsbedarfe auf, sodass das Management entsprechend reagieren kann, und fördern das Sicherheitsbewusstsein im gesamten Unternehmen.

Quelle: CyberDirekt 2026

2.3 Verschiedene Scan-Arten im Überblick

Zur Beurteilung der IT-Sicherheitslage eines Unternehmens kommen unterschiedliche Arten von Scans zum Einsatz, die verschiedene Aspekte der Angriffsfläche abdecken. Die folgenden Beispiele zeigen **zentrale Scan-Typen**.

- **TLS/SSL-Scan**

  Ein TLS/SSL-Scan **überprüft die Sicherheit der verschlüsselten Verbindungen eines Unternehmens**, beispielsweise bei Web- oder Mailservern. Dabei wird geprüft, ob die eingesetzten Zertifikate gültig und vertrauenswürdig sind und ob moderne, sichere Verschlüsselungsprotokolle (z. B. TLS 1.2/1.3) verwendet werden. Das Ziel besteht darin, **veraltete oder unsichere Einstellungen zu erkennen**, die Angreifern den Zugriff auf vertrauliche Daten erleichtern könnten. Diese Art von Scan zeigt auf, ob die Kommunikation wirklich geschützt ist und gibt Hinweise, wie die Verschlüsselung verbessert werden kann.

- **Darknet-Scan**

  Ein Darknet-Scan (auch bekannt als Dark Web Scan) **sucht in den verborgenen Bereichen des Internets nach gestohlenen oder geleakten Unternehmensdaten**. Dafür werden spezialisierte Crawler und Datenbanken eingesetzt, die in Untergrundforen, auf Marktplätzen und Leak-Seiten nach bestimmten Schlüsselbegriffen suchen. Dazu gehören typischerweise Firmennamen, Domainnamen, E-Mail-Adressen der Mitarbeitenden oder Kundendatenbanken. Wird etwas gefunden, erhält das Unternehmen eine Warnmeldung. Der Darknet-Scan ist daher ein **wichtiges Frühwarnsystem**, um Datenlecks außerhalb der eigenen Systeme zu entdecken und geeignete Gegenmaßnahmen einzuleiten.

- **Data Leak Scan**

  Ein Data Leak Scan **sucht nach ungewollt veröffentlichten Unternehmensdaten, sowohl im offenen Internet als auch im Darknet**. Er erkennt zum Beispiel Dokumente, Quellcode oder Zugangsdaten, die versehentlich öffentlich zugänglich gemacht oder in Datenbanken früherer Hacks auftauchen. Dadurch hilft ein solcher Scan, Datenpannen frühzeitig zu entdecken und einen möglichen Informationsabfluss außerhalb des Unternehmensnetzwerks sichtbar zu machen und schnell zu beheben. Da immer mehr Unternehmen ihre Daten in Cloud-Diensten und externen Plattformen speichern, ist diese Art von Scan eine **wichtige Ergänzung zum internen Schwachstellenmanagement.**

2.4 Vor- und Nachteile von Schwachstellenscans

Schwachstellenscans bieten Unternehmen einen wichtigen Sicherheitsvorteil, indem sie IT-Risiken automatisiert und frühzeitig sichtbar machen. Trotz ihrer Effizienz und breiten Anwendbarkeit haben sie jedoch auch methodische und praktische Grenzen.

Vorteile von Schwachstellenscans	Nachteile und Grenzen
Frühwarnsystem: Proaktive Erkennung von Sicherheitslücken, bevor Angreifer sie ausnutzen können.	False Positives: Automatisierte Scans können Fehlalarme erzeugen und manuelle Nachprüfung erfordern.
Automatisiert und kosteneffizient: Schnelle, flächendeckende Analysen ohne hohen Personalaufwand.	Keine Prüfung hinsichtlich Ausnutzbarkeit: Scans erkennen Schwachstellen, bewerten aber nicht, ob sie tatsächlich ausnutzbar sind.
Risikotransparenz: Ergebnisse liefern Prioritäten (z. B. nach CVSS-Schweregrad) und ermöglichen gezieltes Risikomanagement.	Manuelle Nacharbeit: Umsetzung der Maßnahmen (z. B. Patching, Anpassung von Konfigurationen) erfordert personelle Ressourcen.
Nicht-invasiv: Durchführung ohne Eingriff in laufende Systeme und daher keine Beeinträchtigung des Betriebs.	Begrenzte Abdeckung: Erkennt nur bekannte Schwachstellen, während Zero-Day-Lücken bei rein automatisierten Ansätzen oft unentdeckt bleiben.

Quelle: CyberDirekt 2026

3 Vergleichende Analyse: Gemeinsamkeiten und Unterschiede zwischen den Anbietern

Im Folgenden widmen wir uns dem **Vergleich von elf führenden Anbietern von Schwachstellenscans**. Die wichtigsten Vergleichspunkte sind Scan-Arten, Häufigkeit, Aufbereitung der Berichte, abgedeckte technische Merkmale sowie Auffälligkeiten im Angebot.

3.1 Scan-Arten und Leistungsumfang

Alle untersuchten Anbieter führen **externe Schwachstellenscans** der IT-Infrastruktur durch, in der Regel aus der Perspektive eines potenziellen Angreifers (sog. “outside-in”-Ansatz). Ebenfalls bei allen elf Anbietern inkludiert ist ein **Port- und Service-Scan**, bei dem automatisiert offene Ports identifiziert und die darauf betriebenen Dienste erkannt werden. Neun von elf Anbietern führen außerdem einen Abgleich mit bekannten Schwachstellen durch.

Gemeinsamkeiten im Leistungsumfang grundlegender Scans

CyberDirekt

Alle Anbieter führen externe Schwachstellenscans aus der Perspektive eines potenziellen Angreifers durch.

Port- und Service-Scans sind bei allen Anbietern Bestandteil des Schwachstellenscans.

Neun von elf Anbietern gleichen zusätzlich die Ergebnisse mit bekannten Schwachstellen ab.

Quelle: CyberDirekt 2026

Unterschiede zwischen den Anbietern zeigen sich vor allem **hinsichtlich ergänzender Scan-Arten**, die über diesen Basisumfang hinausgehen. Hier hat unsere Analyse unter anderem die folgenden Differenzen gezeigt.

- **TLS/SSL- und Konfigurations-Checks:** Sechs von elf Anbietern prüfen explizit die Sicherheit von Verschlüsselungszertifikaten und -einstellungen.
- **Darknet- und Leak-Monitoring:** Etwas mehr als die Hälfte (sechs von elf) der Anbieter bietet zusätzlich einen Darknet-Scan bzw. Data Leak Scan an. Ein Versicherer nennt dabei ausdrücklich ein „Dark Web Monitoring" (kontinuierliche Überwachung des Darknets) als festen Bestandteil seines Programms.
- **Benchmarking und Peer-Vergleich:** Etwa ein Drittel (vier von elf) der Anbieter ergänzen ihre Scan-Ergebnisse um Branchenbenchmarks, sodass Kunden ihr Sicherheitsniveau im Vergleich zu ähnlichen Unternehmen einordnen können.
- **Manuelle Prüfungen:** Fast alle Anbieter setzen auf vollautomatisierte Verfahren ohne individuellen Test durch einen Security-Analysten. Menschliche Expertise wird nur vereinzelt in die Scans eingebunden. So bietet beispielsweise ein Anbieter seine automatisierten Schwachstellenscans ergänzt mit manuellen Penetrationstests und OSINT-Recherche als Premium-Service an.

Deutliche Unterschiede bei ergänzenden Scan-Arten

CyberDirekt

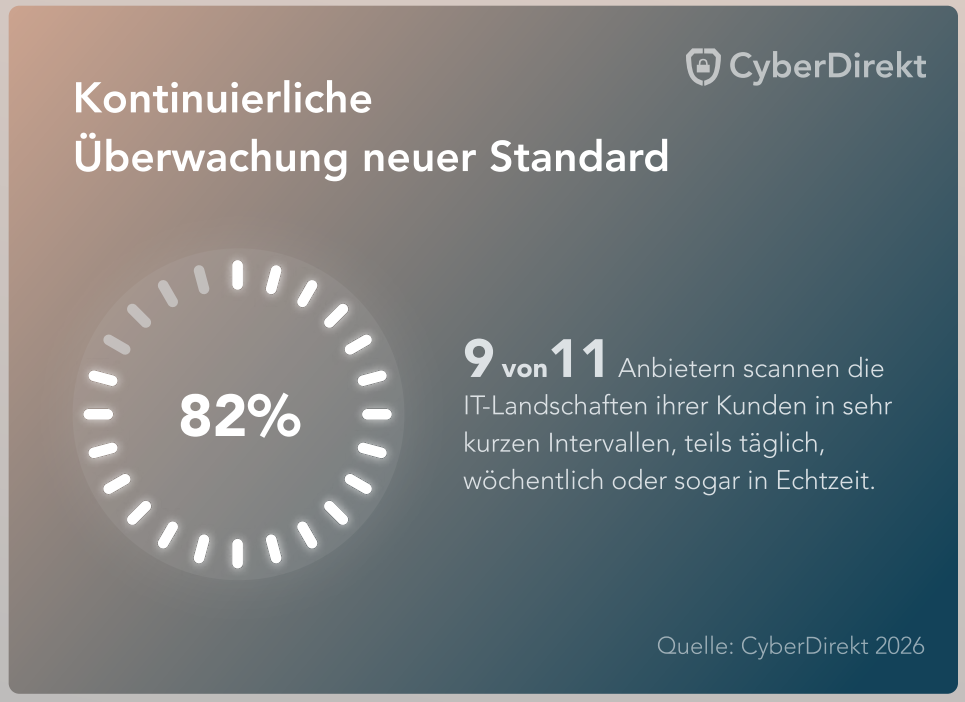
Rund **55%** der Anbieter prüfen gezielt die Sicherheit von Verschlüsselungszertifikaten und -einstellungen.

Ebenfalls etwa **55%** der Anbieter bieten ein Darknet- bzw. Data-Leak-Scanning an.

Etwa **36%** der Anbieter ergänzen ihre Ergebnisse um Branchenbenchmarks.

Quelle: CyberDirekt 2026

3.2 Monitoring und Tiefe des Scans



Unsere Analyse hat gezeigt, dass **kontinuierliche Überwachung** nach dem Motto “Kontinuierlich statt punktuell” **mittlerweile Standard** ist. Neun von elf Anbietern führen Scans in sehr kurzen Intervallen durch, teils täglich, wöchentlich oder sogar in Echtzeit.

Mehrere **Cyberversicherer** bieten **sogar ein 24/7-Monitoring** mit Warnmeldungen bei neu entdeckten Schwachstellen an. Keiner der Anbieter verlässt sich auf Einzel-Scans.

In Bezug auf die **Scan-Tiefe** zeigen sich Unterschiede. Manche Anbieter führen nur externe, nicht authentifizierte Scans durch, die aus Angreifersicht arbeiten. Einige, vor allem **Versicherer mit Kundenportalen**, ermöglichen **zusätzlich interne Scans** oder den Einsatz von Agenten. Alle Lösungen erkennen gängige Schwachstellen wie offene Ports, veraltete Software oder fehlende Patches. Zwei Anbieter gehen außerdem darüber hinaus und erfassen zusätzlich Cloud-Storage-Leaks (z. B. ungesicherte S3-Buckets).

Insgesamt zeigen jedoch **alle Anbieter eine solide Grundabdeckung**. Unterschiede bestehen vor allem in den Zusatzfunktionen und der Aufbereitung der Reports.

3.3 Verständlichkeit der Scan-Berichte

Da die Zielgruppe der Scan-Berichte in der Regel Entscheider ohne tiefes technisches Wissen sind, legen fast alle Anbieter Wert auf eine verständliche Aufbereitung der Ergebnisse. Rund drei Viertel (8 von 11) der Anbieter liefern eine **managementgerechte Ergebnisdarstellung mit Ampelfarben, Scores oder klaren Handlungsempfehlungen in Alltagssprache**.

- Fünf von elf Anbietern stellen zusätzlich eine **Executive Summary** bereit, die technische Risiken in Business-Sprache übersetzt.
- Viele Reports nutzen grafische Risk Scores, Balken und Charts zur Veranschaulichung.
- **Klare Handlungsempfehlungen** (z. B. „Konfiguration anpassen“) sind nahezu überall vorhanden. Insbesondere Versicherer verknüpfen die Ergebnisse mit Unterstützungs- oder Folgedienstleistungen, um die erkannten Sicherheitslücken oder Schwachstellen zu beheben.
- Die Berichte sind **mehrheitlich C-Level-tauglich**, da Fachbegriffe erklärt oder in konkrete Risiken übersetzt werden.
- Nur reine Tech-Rating-Plattformen liefern vereinzelt noch Rohdaten ohne vereinfachte Darstellung, obwohl auch hier **erklärende Tooltips und FAQs** vorhanden sind, die bei der Auswertung unterstützen.

3.4 Technische Abdeckung der Scans und besondere Auffälligkeiten

Bei den technischen Features decken die Anbieter einen großen gemeinsamen Nenner ab, doch es gibt auch Ausreißer nach oben. **Alle analysierten Dienste erfassen grundlegende technische Aspekte** wie offene Ports, bekannte Software-Schwachstellen sowie potenziell unsichere Konfigurationen.

Abweichungen zeigen sich vor allem **im Umfang der abgedeckten Risikokategorien**. Während zwei der spezialisierten Rating-Anbieter mehr als 20 bis 25 Kategorien parallel analysieren (darunter Web-Applikationssicherheit, Patchmanagement und Malware-Indikatoren), fokussieren sich **Versicherungsanbieter tendenziell stärker auf unmittelbar ausnutzbare Schwachstellen** (z. B. Ports, Vulnerabilities oder Leaks) und weniger auf abstrakte Bewertungsmetriken.

3.4.1 Besondere Stärken und Differenzierungsmerkmale

Einige Anbieter positionieren sich mit spezifischen Alleinstellungsmerkmalen innerhalb des Marktes.

- Ein Scan-Dienst hebt seine besonders **hohe Präzision ohne False Positives** hervor, die durch einen vollständig technischen, stark automatisierten Prüfansatz erreicht werden soll.
- Ein weiterer Anbieter **integriert Threat-Intelligence-Daten** zu aktuellen Angriffsmustern, wodurch Erkenntnisse über aktive Hacker-Gruppierungen und Exploit-Trends unmittelbar in die Risikobewertung einfließen.
- Ein dritter Anbieter betreibt ein **globales Sensornetzwerk mit eigenen Honeypots**, das eine frühzeitige Erkennung neuer Bedrohungen ermöglicht. Kunden werden beispielsweise proaktiv informiert, wenn im Darknet verstärkt über Schwachstellen in von ihnen eingesetzter Software diskutiert wird.

3.4.2 Schwächen und Lücken in den analysierten Angeboten

Obwohl in den öffentlich zugänglichen Informationen kaum offensiv kommunizierte Schwächen erkennbar sind, zeigen sich **Unterschiede zwischen den Anbietern hinsichtlich ihres Leistungsportfolios**. Zwei der untersuchten Versicherer ergänzen ihre Scan-Dienste beispielsweise um zusätzliche IT-Sicherheitsservices wie Phishing-Trainings oder Notfall-Hotlines

Weitere **Unterschiede bestehen in der Risikodarstellung**. Während die reinen Rating-Anbieter (drei von elf) primär einen numerischen Score bereitstellen, setzen **versicherungsorientierte Dienste** auf konkrete **Handlungsempfehlungen und Warnmeldungen**. In einigen Fällen werden beide Formate kombiniert. Fachlich wird empfohlen, für operative Entscheidungen vorrangig die konkreten Befunde heranzuziehen, da die Berechnungsmethoden der Scores zwischen den Anbietern variieren, beispielsweise hinsichtlich der Einbeziehung von Darknet-Analysen.

Leichte **Schwächen** sind, wenn überhaupt, **im Bereich der Leak- und Darknet-Überwachung** erkennbar. Während mehr als die Hälfte der Anbieter hier über eigene Lösungen verfügt, verzichten einige klassische Versicherer auf eigenständige Darknet-Scans und konzentrieren sich auf die Analyse der internen IT-Oberfläche des Unternehmens. Diese Lücken werden teilweise durch Partnerschaften mit spezialisierten Rating-Diensten kompensiert, deren Daten im Hintergrund in die Bewertung einfließen.

3.5 Zusammenfassende Bewertung

Insgesamt zeigt sich ein weitgehend homogenes Leistungsniveau im Bereich des technischen Schwachstellen-Scannings. **Neun von elf Anbietern decken ein vergleichbares Fundament ab**, das die Analyse von Netzwerk-, System- und Web-Schwachstellen umfasst. Sechs Anbieter erweitern dieses Basisspektrum durch ergänzende Module wie Threat-Intelligence-Integration und Leak-Erkennung.

Die **Unterschiede zwischen den Anbietern liegen im Detail**. Insbesondere darin, ob und in welchem Umfang Darknet-Daten in die Bewertung einfließen und ob das Ergebnis als reiner Scan-Report oder im Rahmen eines umfassenderen Servicepakets mit Beratung und Handlungsempfehlungen bereitgestellt wird.

Übergreifend ist ein klarer Trend erkennbar. Die Angebote entwickeln sich hin zu einer **höheren technischen Tiefe, stärkerer Automatisierung** und einer engeren Integration in das übergeordnete Cyber-Risk-Management der Kunden.

4 Schwachstellenscans außerhalb der Cyberversicherung: Kriterien für die Anbieterauswahl

Wie aus den Ergebnissen der Analyse hervorgeht, verfügen die meisten Scan-Anbieter über eine weitgehend ähnliche technische Basis und unterscheiden sich vor allem in Zusatzfunktionen, Serviceumfang und Ergebnisaufbereitung. **Für Unternehmen und Makler** wird daher entscheidend sein, welcher Anbieter den größten **praktischen und wirtschaftlichen Mehrwert** bietet.

Wer Schwachstellenscans außerhalb einer Cyberversicherung beauftragt, sollte neben Preis-Leistung, Datenqualität und Verständlichkeit der Ergebnisse auch auf den technischen Umfang, die Aktualität der Scan-Engine, den Unterstützungsservice sowie die Integration in bestehende Sicherheitsprozesse achten. Nachfolgend finden Sie eine Liste an Kriterien, auf die Makler und Unternehmen bei der **Auswahl eines geeigneten Scan-Anbieters** achten sollten.

1. Welche Arten von Schwachstellen werden abgedeckt?

Prüfen Sie, ob der Anbieter neben klassischen Netzwerk- und Server-Scans **auch Webanwendungen, Cloud-Umgebungen und mobile Geräte** berücksichtigt. Achten Sie außerdem darauf, ob auch Fehlkonfigurationen (z. B. SSL, Firewalls, unsichere Protokolle) erkannt werden.

2. Wie aktuell ist die Schwachstellendatenbank des Anbieters?

Die Scan-Engine sollte kontinuierlich mit den neuesten CVEs und Bedrohungsinformationen versorgt werden. Idealerweise pflegt der Anbieter eine umfangreiche Wissensdatenbank, die **mehrmals täglich um neue Prüfmechanismen erweitert** wird. Fragen Sie, ob auch **Zero-Day-Exploits** und externe Threat-Intelligence-Feeds (z. B. aus Darknet-Quellen) einbezogen werden.

3. In welchem Intervall und Umfang erfolgen die Scans?

Erkundigen Sie sich, ob die **Scans kontinuierlich, regelmäßig (täglich, wöchentlich) oder nur on-demand durchgeführt** werden. Ein professioneller Anbieter sollte automatische Rescans nach Behebung von Schwachstellen ermöglichen und optional ein kontinuierliches Monitoring bieten. Ein Scan nach wesentlichen Systemänderungen sollte jederzeit möglich sein.

4. Wie werden die Ergebnisse des Scans aufbereitet?

Bitten Sie um **Musterberichte oder Demo-Dashboards,** um die Qualität der Ergebnisdarstellung zu prüfen. Achten Sie darauf, dass die **Reports auch für Nicht-Techniker verständlich** sind. Ein guter Bericht priorisiert Risiken und erläutert in verständlicher Sprache, welche Maßnahmen erforderlich sind, anstatt nur technische Codes auszugeben.

5. Gibt es einen Gesamt-Risikoscore?

Einige Anbieter stellen zusätzlich einen Gesamtscore (z. B. 0–100 oder ähnlich einer Bonitätsskala) bereit, der das Sicherheitsniveau zusammenfasst. Klären Sie, **auf welcher Grundlage dieser Wert berechnet wird** und welche Faktoren in die Bewertung einfließen.

6. Wie hoch ist die erwartete Genauigkeit (False-Positive-Rate)?

Erkunden Sie sich, **wie häufig Fehlalarme auftreten und wie viel manuelle Nacharbeit** dadurch erforderlich ist. Seriöse Anbieter geben offen zu, dass bestimmte Befunde überprüft werden müssen, und stellen gegebenenfalls Filter- oder Validierungstools bereit, um die Ergebnisqualität zu verbessern.

7. Werden auch Leaks und externe Bedrohungen überwacht?

Prüfen Sie, ob ein **Darknet-Monitoring oder Leak-Scanning** Teil des Angebots ist. Wichtig ist, welche Arten von Datenlecks erfasst werden, wie zum Beispiel kompromittierte Zugangsdaten, personenbezogene Informationen oder Kreditkartendaten.

8. Wie sicher ist der Scanvorgang?

Klären Sie, ob der Anbieter passive bzw. externe Prüfungen durchführt oder ob aktive Exploit-Tests Teil des Scans sind. Auch wenn Tests wie Port-Scans und Banner-Grabbing in der Regel **keine Auswirkungen auf die gescannten Systeme** haben, sollten Sie sich diesbezüglich rückversichern. Seriöse Anbieter setzen auf Mechanismen zur Lastbegrenzung und vermeiden riskante Verfahren, die zu Ausfällen führen könnten.

9. Welche Ressourcen oder Vorbereitungen sind nötig?

Ermitteln Sie, ob alle zu prüfenden **IPs bzw. Hosts manuell übermittelt** werden müssen oder ob der Scanner automatisch weitere verbundene Assets entdeckt (sog. Asset Discovery). Fragen Sie auch nach, ob **interne Sensoren oder Agenten installiert** werden müssen oder ob der Scan vollständig extern erfolgt. Manche Anbieter, insbesondere Versicherer, führen ausschließlich externe Scans durch (auf Basis der angegebenen Domain). Andere Anbieter stellen bei Bedarf zusätzliche Programme oder Geräte bereit, um auch interne Systeme im Unternehmensnetzwerk genauer zu prüfen.

10. Wie häufig und in welcher Form werden Warnungen versendet?

Fragen Sie, ob **Echtzeit-Benachrichtigungen bei kritischen Funden** bereitgestellt werden oder ob lediglich regelmäßige Reports verfügbar sind. Optimalerweise bietet der Anbieter ein Dashboard mit Live-Updates und zusätzlichen E-Mail-Alerts bei Hochrisiko-Funden. Prüfen Sie, ob der Schweregrad, ab dem eine Sofort-Benachrichtigung getriggert wird, individuell eingestellt werden kann.

11. Welche Unterstützung gibt es bei der Interpretation und Behebung?

Bringen Sie in Erfahrung, ob der Anbieter **lediglich die Ergebnisse liefert oder auch beratende Unterstützung bietet**. Viele Anbieter, insbesondere Cyberversicherer, stellen Teams bereit, die bei der Interpretation der Ergebnisse und bei der Umsetzung von Gegenmaßnahmen helfen. Erkundigen Sie sich nach Support-Optionen (z. B. 24/7-Erreichbarkeit, dedizierte Ansprechpartner) sowie nach möglichen SLAs für Reaktionszeiten auf Support-Anfragen.

12. Ist eine Integration in bestehende Prozesse und Tools möglich?

Klären Sie, ob der Anbieter Schnittstellen (APIs) oder Integrationen zu gängigen Systemen wie **Ticket-Systemen oder SIEM-Tools** anbietet, um das Schwachstellenmanagement und die Nachverfolgung zu erleichtern.

13. Verfügt der Anbieter über branchenspezifische Erfahrung oder Referenzen?

Erkundigen Sie sich nach Erfahrungen in Ihrer Branche sowie nach nachweisbaren **Erfolgsgeschichten oder Referenzkunden**, um die Praxistauglichkeit der Lösung für Ihr Unternehmen bzw. Ihren Kunden besser einschätzen zu können.

14. Wie gestaltet sich das Preismodell?

Vergleichen Sie, ob die **Kosten nach Anzahl der IPs/Domains, Unternehmensgröße oder pauschal pro Jahr** berechnet werden. Achten Sie darauf, ob Zusatzleistungen wie Darknet-Scanning oder Beratungs-Services im Preis enthalten sind oder separat berechnet werden.

Wichtig ist, die Anbieter gezielt mit den oben genannten Fragen zu konfrontieren. Ein **seriöser Dienstleister wird transparente und nachvollziehbare Antworten geben**. Auf diese Weise lässt sich strukturiert beurteilen, welcher Schwachstellenscan-Service am besten zu den Anforderungen des Unternehmens passt.

5 Zusammenfassung und Ausblick

Die Analyse zeigt, dass **externe Schwachstellenscans bei allen betrachteten Anbietern zum festen Leistungsumfang** gehören, auch wenn die konkrete Beschreibung und Transparenz variieren. TLS/SSL-Prüfungen werden insbesondere von spezialisierten Rating-Plattformen als eigenständige Bewertungsfaktoren ausgewiesen, während klassische Versicherer diese Aspekte in der Regel im Rahmen ihres allgemeinen Vulnerability-Scannings abdecken.

Darknet- und Leak-Monitoring sind bei mehreren Anbietern Bestandteil des Scan-Umfangs, werden jedoch unterschiedlich deutlich kommuniziert. Während spezialisierte Anbieter diese Funktion explizit benennen, bleibt sie bei einigen Versicherern nur indirekt über Methodik- oder Portfolioangaben erkennbar.

In Bezug auf die Scan-Frequenz dominiert ein kontinuierlicher oder nahezu Echtzeit-orientierter Ansatz. Die meisten Anbieter führen **fortlaufende Scans** durch **oder** verfügen über ein **permanentes Monitoring** mit kurzen Reaktionszeiten. Einzelne Dienste setzen auf wöchentliche Prüfintervalle, wodurch ein grundsätzlich hoher Aktualitätsgrad über alle Anbieter hinweg gewährleistet ist.

Schwachstellenscans werden **auch künftig ein zentrales Element der Cyber-Abwehr** bleiben und in den kommenden Jahren weiter an Bedeutung gewinnen. Angesichts der zunehmenden Dynamik neuer Schwachstellen, der beschleunigten Angriffsketten und der wachsenden regulatorischen Anforderungen ist zu erwarten, dass eine kontinuierliche Überwachung der IT-Infrastruktur sowohl in Unternehmen als auch in der Risikoprüfung von Versicherern zum Standard werden wird.

Gleichzeitig zeigt sich, dass die Wirksamkeit der Scans künftig stärker von ihrer **Einbindung in ganzheitliche Sicherheitsprozesse** abhängen wird. Um die aktuell bestehenden Grenzen und Einschränkungen (z. B. hinsichtlich False Positives, manueller Nacharbeit und fehlender Bewertung der tatsächlichen Ausnutzbarkeit der Schwachstellen) zu überwinden, müssen automatisierte Scans zunehmend **mit Threat Intelligence, Penetrationstests und aktivem Patchmanagement kombiniert** werden. Der Mehrwert dürfte daher künftig weniger in der reinen Identifikation von Schwachstellen liegen, sondern in der kontextualisierten Bewertung, Priorisierung und Behebung von Risiken.

Autoren:
Tobias Fröhlich, Leiter Cyber Security, RapidResponse GmbH
Johannes Kral, Radaktion, CyberDirekt GmbH

CyberDirekt GmbH
Köpenicker Str. 154 A
10997 Berlin

info@cyberdirekt.de
www.cyberdirekt.de

CyberDirekt