



**TechData**

RECOMMENDATION

according to  
ISO/IEC 27001  
BSI Grundschrift

# Risiken erkennen ...

... aus der Perspektive  
eines Angreifers.

Sensibilisieren Sie Ihre Kunden,  
zeigen Sie die aktuelle Bedrohungslage  
auf und ergreifen Sie Maßnahmen.

# Tech Data Cyber Scoring

## Stellen Sie sich den Herausforderungen

Laut Bitkom entstand 2019 ein wirtschaftlicher Schaden von mehr als 100 Milliarden Euro in Deutschland. Drei von vier Unternehmen wurden Opfer von Sabotage, Datendiebstahl oder Spionage. Aktuell entstehen tagtäglich 350.000 neue Schadprogramme und potenziell unerwünschte Anwendungen. Kleine und mittelständische Unternehmen stehen im Zugzwang. Der Bedarf und Wunsch nach einer betriebsunterbrechungsfreien IT mit Rundumschutz nimmt mit jedem bekannten Vorfall zu. Größter Bedarf und Wunsch von allen, Partnern und Kunden ist es, die IT-Risiken richtig einzuschätzen sowie Empfehlungen zur Verbesserung der Gefährdungssituation zu haben. Genau hier setzt das Cyber Scoring von Tech Data an.

## Bieten Sie Hackern keine Angriffsflächen

Richtig gelesen. Das Tech Data Cyber Scoring nutzt das Framework und öffentlich zugängliche Daten von intelligenten Open-Source-Werkzeugen und -Techniken (OSINT) zur Erfassung von Informationen, wie sie auch Angreifer einsetzen. Somit findet die Einschätzung aus der Sicht eines Angreifers statt. Verwundbare, aus der Ferne ausnutzbare oder falsch konfigurierte Systeme werden entdeckt. Das Besondere, mit dem Cyber Scoring haben Sie einen Management-Report zur Hand, der Ihnen gleichzeitig als **Dokumentation und Wirksamkeitsüberprüfung** dient (DSGVO-konform).

## Schützen Sie Ihre Kunden und machen Sie IT-Sicherheit messbar

Das Tech Data Cyber Scoring versetzt Sie in die Lage, einen aktuellen, neutralen Einblick in die Cyber Security Readiness Ihrer Kunden zu erhalten. Die daraus gewonnenen Daten werden analysiert, und die Erkenntnisse werden als Management- oder Spezialistenbericht kategorisiert und aufbereitet. Im Ergebnis erhalten Sie das aktuelle Gesamtrisiko sowie Handlungsempfehlungen.

## Risikoeinschätzung in acht Kategorien





## In vier Phasen zur geprüften Sicherheit

### 1. Aufklärung

Die Aufklärungsphase dient dazu, anhand der angegebenen Domain herauszufinden, welche Systeme, Netzwerke und vereinzelnde Endpoints zu dem Unternehmen gehören. Hierzu gehören auch die Domainn die unter der Verantwortung des Unternehmens stehen.

### 2. Identifizierung

Die identifizierten Systeme werden untersucht. Dabei werden für alle sicherheitsrelevanten Domains bzw. IP-Adressen aktuelle und öffentlich zugängliche Daten erhoben. Für einige Datenkategorien liegen auch historische Werte von früher öffentlich verfügbaren Daten vor.

**Gesamtbewertung** – Bewertung der Cyber-Sicherheitsrisiken eines Unternehmens auf Basis von ausserhalb des Unternehmens wahrnehmbaren technischen Gegebenheiten.



**Konkrete Gefährdungslage** – Bewertung aller Indizien, die auf einem laufenden Angriff oder eine akute Angriffsmöglichkeit hindeuten.



**Reputation im Cyberraum** – Bewertung der Reputation des Unternehmens im Internet.



**Mitarbeiterverhalten im Cyberspace** – Bewertung aller Indizien, wie vorsichtig die Mitarbeiter des Unternehmens im Internet auftreten.



**Organisations- & Prozessrisiken** – Bewertung aller Indizien, die mit den Betriebs-, Wartungs- und Sicherheitsprozessen in Zusammenhang stehen.



**Länderrisiken** – Bewertung der Risiken, die durch Präsenz in verschiedenen Jurisdikationen und Kulturkreisen entstehen.



**Vertrauenswürdige Verschlüsselung** – Bewertung der korrekten Konfiguration der SSL/TLS Verschlüsselungstechnologien



**Konfiguration der Webserver** – Bewertung aller sichtbaren Konfigurationseigenschaften aller Internetseiten und Webapplikation



**Angriffsfläche im Internet** – Bewertung der offenen Ports, die für das gesamte Internet erreichbar sind.



### 3. Bewertung

Die Identifizierungsphase oft mehrere Tausend Ergebnisse. Der zu Grunde liegende Algorithmus analysiert diese Werte, fasst diese in acht Kategorien zusammen und bewertet sie nach ihrer Auswirkung.

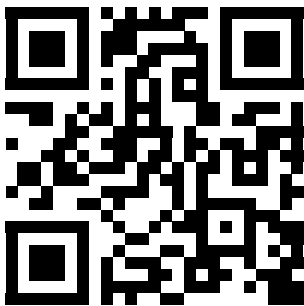
### 4. Ergebnis

Die Reports helfen Ihnen beim Bewerten der besonders kritischen Schwachstellen. Der Management-Report lässt sich ohne Zustimmung erheben. Validierte Benchmarks dienen Ihnen zur Priorisierung der Maßnahmen und Erstellung einer Roadmap für Ihre Kunden.

## Schützen Sie Ihre Kunden!

1. Erhalten Sie als Partner von Tech Data Ihr eigenes Scoring. Wir bewerten das Gesamtrisiko Ihres Unternehmens und geben Ihnen damit einen ersten Einblick in den Ablauf des Scorings.
2. Integrieren Sie das Scoring in Ihr Geschäftsmodell.
3. Generieren Sie durch gezielte Sensibilisierung wiederkehrende Einnahmen.

Wir sind für Sie da! BU-Security@techdata.com  
oder 089 4700 3222.



**Ihr schneller Weg  
zum Cyber Scoring.**

**[de.techdata.com/cyber-scoring](https://de.techdata.com/cyber-scoring)**



*Security Solutions*

[de.techdata.com](https://de.techdata.com)

[BU-Security@techdata.com](mailto:BU-Security@techdata.com)