Der neue Cyber-Risiko-Score

DIE VERMESSUNG DER UNSICHERHEIT

Wissenschaftler der Westfälischen Hochschule Gelsenkirchen entwickeln ein transparentes Bewertungsmodell, das technische Schwachstellen mit dem Geschäftskontext von Unternehmen verknüpft. Der Score soll besonders kleinen und mittleren Unternehmen helfen, ihre Cyberrisiken zu quantifizieren und Investitionen zu priorisieren.

Die Ausgaben für IT-Sicherheit in Deutschland steigen kontinuierlich. Laut Bitkom beliefen sie sich 2024 auf 10,1 Milliarden Euro, für 2025 werden 11,1 Milliarden und für 2026 bereits 12,2 Milliarden Euro prognostiziert.[1] Doch ob diese Investitionen tatsächlich zu mehr Sicherheit führen, bleibt für viele Unternehmen unklar.

Zwar sind sich viele Firmen ihrer internen Risiken grundsätzlich bewusst, doch mangelt es häufig an einer präzisen Einschätzung und einem daraus resultierenden adäquaten Umgang. Gerade im Zeitalter des Homeoffice ist Konnektivität essenziell, birgt jedoch gleichzeitig neue Gefahrenpotenziale: Von außen erreichbare Dienste bieten Angriffsfläche für Angreifer, und oft haben kleine und mittlere Unternehmen (KMU) die eigenen Assets nicht im Blick.

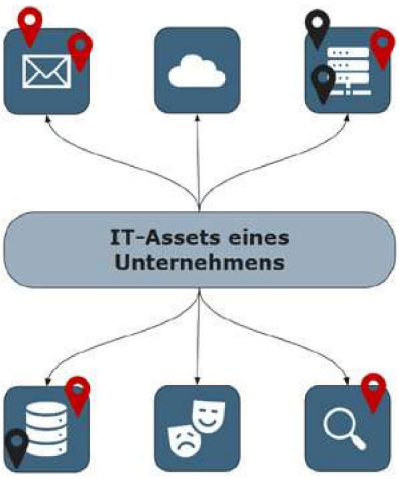

Abbildung 1: Mögliche Assets eines Unternehmens und ihre Schwachstellen, kategorisiert in CVEs und CWEs. (Bild: if(is))

Bild: whyframeshot - stock.adobe.com

Automatisierte Pentests und Schwachstellenscanner liefern zwar wertvolle Erkenntnisse über Sicherheitslücken und Fehlkonfigurationen. Doch lassen die Ergebnisse in puncto Vergleichbarkeit und konkreter Handlungsempfehlungen oft zu wünschen übrig. Zudem ist eine Diskrepanz innerhalb der Unternehmen festzustellen: Während das Management Kennzahlen für finanzielle Risikoabschätzungen und Investitionsentscheidungen benötigt, liefert die IT-Abteilung meist rein technische Berichte. Diese unterschiedlichen Perspektiven führen zu erheblichen Kommunikationsproblemen, obwohl beide Seiten dasselbe Ziel verfolgen: die Absicherung des Unternehmens.

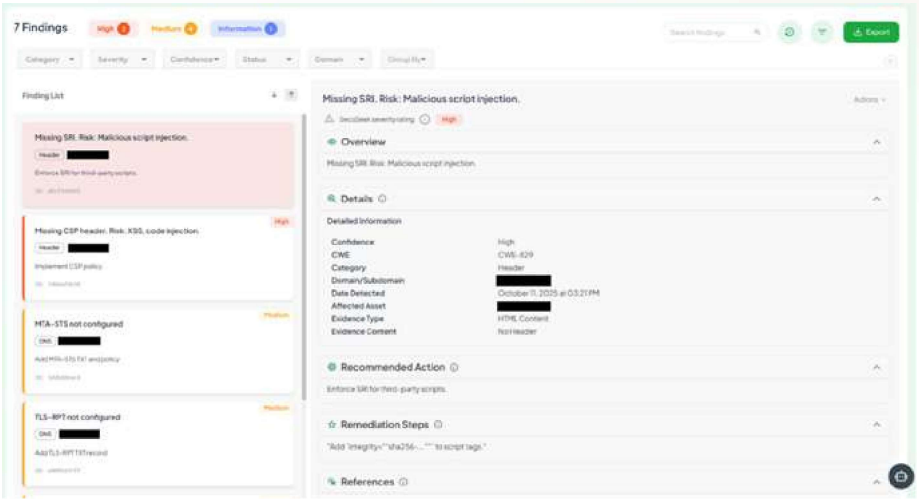

Abbildung 2: Beispiel eines Schwachstellen-Scans mit der Plattform SecuSeek (Bild: if(is)).

Um diese Lücke zu schließen, müssen technische Befunde in quantifizierbare Werte übersetzt werden. Die Bewertung der IT-Sicherheitslage ist kein neues Konzept, doch bestehenden Modellen mangelt es häufig an Transparenz und Verhältnismäßigkeit. Viele Bewertungssysteme agieren als proprietäre „Blackboxen" oder ignorieren den Geschäftskontext und damit kritische Ankerpunkte des Unternehmens. Aspekte wie ein funktionierendes Notfallmanagement oder klare Hierarchien werden häufig nicht ausreichend berücksichtigt. Zudem wirken langwierige Audits und Zertifizierungen durch ihren hohen Aufwand oft eher abschreckend als motivierend.

An dieser Stelle setzt der Cyber-Risiko-Score (CRS) an. Ziel ist ein kontextsensitiver, objektiver Bewertungsmaßstab, der nicht nur transparent und verständlich ist, sondern auch eine faire Vergleichbarkeit innerhalb von Branchen ermöglicht. Doch warum reichen die bisherigen Ansätze nicht aus?

SCHWÄCHEN UND BLINDE FLECKEN

Eine zentrale Schwäche vieler aktueller Risikomanagement-Tools ist ihre Unvollständigkeit. Wesentliche Aspekte einer ganzheitlichen Bewertung bleiben oft außen vor – etwa die wirtschaftliche Bewertung von Assets oder eine systematische Risikoevaluierung. Auch die Konsistenz der Ergebnisse lässt zu wünschen übrig: Zwischen qualitativen und quantitativen Ansätzen klafft eine deutliche Lücke.[2]

Hinzu kommt: Quantitative Methoden, die das gesamte Ausmaß eines Risikos abbilden könnten, fehlen häufig. Die exakte Verortung von Schwachstellen oder Fehlkonfigurationen ist jedoch entscheidend. Ein weiteres Problemfeld ist die Diskrepanz zwischen den Perspektiven von Softwareentwicklung und Unternehmensmanagement. Die Abhängigkeiten beider Bereiche sind bislang kaum erforscht.[3] IT-Sicherheitsaspekte werden im Managementalltag oft zugunsten anderer Entscheidungen vernachlässigt – ein wiederkehrendes Phänomen, das bereits in früheren Studien diskutiert wurde.[4]

Kritik gibt es auch an sogenannten Punktlösungen: Isolierte IT-Sicherheitsmaßnahmen ignorieren den Gesamtaufwand und die Anpassungsfähigkeit der Angreifer. Für eine fundierte Bewertung müssen jedoch auch Implementierungskosten und operative Kompromisse einbezogen werden. Unternehmensziele und Umsatz sind die eigentlichen Treiber – ein Risk-Assessment muss diese Faktoren berücksichtigen.[5]

Ein weiteres Thema ist die Detektion von Angriffen und Schäden, die auf fehlende oder fehlerhafte IT-Sicherheitsmechanismen zurückgehen. Neben technischen Faktoren spielt hier der „Human Factor" eine zentrale Rolle. Ein Bewertungsmodell sollte daher auch die Art und Weise der Detektion widerspiegeln.[6]

Die Fachliteratur betont immer wieder: Der menschliche Faktor und die Interaktion der Nutzer mit dem Netzwerk sind entscheidend. Gängige Bewertungsmethoden vernachlässigen diesen Aspekt häufig, obwohl Nutzerverhalten Risiken sowohl verursachen als auch mindern kann.[7]

Die Quantifizierung von Risiken bleibt eine Herausforderung. Bei der Übertragung qualitativer Aussagen gehen oft wichtige Informationen verloren. Hinzu kommen ökonomische Hürden: Investitionen in Cybersicherheit bringen selten einen unmittelbaren Return on Investment (ROI). Gerade kleine und mittlere Unternehmen mit begrenztem Budget benötigen daher Scores mit konkreten Handlungsempfehlungen, um fundierte Entscheidungen treffen zu können.[8]

CYBER-RISIKO-CHECK DES BSI

Ein praktisches Beispiel für standardisierte Risikobewertung ist der Cyber-Risiko-Check des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dieser IT-Sicherheitscheck für KMU basiert auf der DIN SPEC 27076, die das BSI gemeinsam mit 20 Partnern entwickelt hat. Mithilfe eines kurzen Interviews mit 27 Anforderungen wird die IT-Sicherheit eines Unternehmens geprüft. Die Teilnehmer erhalten anschließend Handlungsempfehlungen für nicht erfüllte Anforderungen. Damit schafft der Check eine strukturierte IT-Sicherheitsbewertung und bietet zugleich konkrete, leicht umsetzbare Verbesserungsimpulse, die auf die Bedürfnisse von KMU abgestimmt sind.[9]

Die Ergebnisse sind ernüchternd: Laut BSI-Lagebericht 2025 sind die meisten KMU nicht ausreichend gegen Cyberbedrohungen geschützt. Lediglich rund 56 Prozent der überprüften Unternehmen erfüllen die Anforderungen des Cyber-Risiko-Checks.[10]

Die anonymisierten Ergebnisse dieser Checks dienen als Datenquelle für die Validierung und Weiterentwicklung des hier vorgestellten Cyber-Risiko-Scores.

DER CYBER-RISIKO-SCORE

Das Kernkonzept des CRS ist eine hybride Heuristik, die auf den fundamentalen Prinzipien der Risikobewertung basiert.[11] Anstatt sich auf die bloße Identifizierung technischer Schwachstellen zu beschränken, integriert der CRS diese in den übergeordneten Geschäftskontext des Unternehmens. Das Ziel besteht darin, komplexe Datenpunkte zu einer einzigen, intuitiven Kennzahl zusammenzufassen, die auf einer Skala von 0 (minimales Risiko) bis 10 (kritisches Risiko) dargestellt wird. Diese Zahl dient nicht der Panikmache, sondern ist eine objektive Grundlage für die Priorisierung von Ressourcen.

Der CRS wird aus zwei Hauptkomponenten berechnet: der Eintrittswahrscheinlichkeit (Likelihood) und dem Schadensausmaß (Impact), moduliert durch die organisatorische Reife des Unternehmens.

Die Likelihood-Bewertung im CRS stellt eine Abkehr vom Dogma dar, dass ein hoher CVSS-Score automatisch ein hohes Risiko bedeutet. Ein CVSS-Score von 9.8 beschreibt lediglich den technischen Schweregrad einer Lücke, ignoriert aber zwei entscheidende Fragen: Wird diese Lücke tatsächlich angegriffen? Und wie wichtig ist das betroffene IT-System für das Unternehmen?

Die Likelihood-Heuristik beantwortet diese Fragen durch eine zweistufige Kontextualisierung:

1. **Interne Kontextualisierung (Asset-Kritikalität)**
   Nicht jedes IT-System hat die gleiche Priorität. Eine Schwachstelle auf einem isolierten Testsystem stellt ein vernachlässigbares Risiko dar, während dieselbe Schwachstelle auf dem zentralen Enterprise-Resource-Planning-(ERP)-Server oder dem Domain-Controller existenzbedrohend sein kann. Der CRS führt daher den Faktor der „Kontext-Schwere" ein. Bei der Berechnung wird der technische Roh-Score eines Befunds mit einem festgelegten Kritikalitätsfaktor multipliziert. Dies gewährleistet, dass das Modell „business-aware" agiert und Risiken dort priorisiert, wo die Wertschöpfung des Unternehmens stattfindet.

2. **Externe Bedrohungsanalyse (Threat Intelligence)**
   Die bloße Existenz einer Lücke stellt noch keinen Angriff dar. Um die Wahrscheinlichkeit eines Angriffs zu bewerten, integriert der CRS moderne Threat-Intelligence-Metriken:

   - **EPSS (Exploit Prediction Scoring System):** Dieser Wert gibt die statistische Wahrscheinlichkeit an, mit der eine Schwachstelle innerhalb der nächsten 30 Tage aktiv ausgenutzt wird.[12] Eine Lücke mit einem EPSS-Wert von 95 Prozent wird im Modell deutlich höher gewichtet als eine theoretische Lücke mit 0,1 Prozent, auch wenn beide denselben CVSS-Wert aufweisen.

   - **CISA KEV (Known Exploited Vulnerabilities):** Das Modell ist mit einem „Not-Aus-Schalter" ausgestattet. Wird eine

Common Vulnerabilities and Exposures (CVE) im Katalog der Cybersecurity and Infrastructure Security Agency (CISA) für aktiv ausgenutzte Schwachstellen gefunden, wird der Likelihood-Score – unabhängig von anderen Faktoren – auf das Maximum gesetzt. Dies reflektiert die Realität, dass bei einer aktiv ausgenutzten Lücke die Zeit für probabilistische Abwägungen vorbei ist; hier herrscht akuter Handlungsbedarf.

Die finale Berechnung der Likelihood erfolgt über eine gewichtete Formel, die entweder der internen Relevanz (Kontext-Schwere) den Vorrang gibt, oder die externe Bedrohungslage (EPSS) höher bewertet (siehe Abbildung 3).

$$LIKELIHOOD = \max\left(\frac{Crit_x \cdot CVSS_x}{Crit_{max} \cdot 10} \cdot v + EPSS_x \cdot (1 - v)\right)$$

Abbildung 3: Berechnung des Likelihood-Scores mittels CVSS, EPSS und dem Kritikalitätsfaktor (Bild: if(is))

RELATIVER IMPACT STATT ABSOLUTER EURO-BETRÄGE

Die zweite Säule des CRS ist der Impact-Score. Die Bewertung des Schadensausmaßes für KMUs stellt eine Herausforderung dar, da die Relation von entscheidender Bedeutung ist. Ein Schadensfall in Höhe von 500.000 Euro wird von einem Konzern als „Cost of doing business" verbucht, während er für ein kleines mittelständisches Unternehmen die Insolvenz bedeuten kann. Absolute Euro-Beträge sind daher als Risikometrik ungeeignet, um Dringlichkeit vergleichbar zu machen.

Der CRS löst dies durch das Konzept des „relativen Impacts" auf. Die Heuristik folgt dabei einem dreistufigen Prozess:

1. **Basis-Schaden:** Zunächst wird auf Basis von Branchen-Reports (zum Beispiel für das Gesundheitswesen, die Fertigungsindustrie oder den Finanzsektor) oder Daten von Versicherern ein durchschnittlicher monetärer Schaden durch Cybervorfälle ermittelt. Dies dient als statistischer Anker.

2. **Modulation:** Dieser Wert wird durch die individuelle Resilienz des Unternehmens angepasst.

3. **Relativierung:** Die Verhältnissetzung zum Jahresumsatz des Unternehmens ist von entscheidender Bedeutung. Das Modell quantifiziert, welchen Prozentsatz des Jahresumsatzes potenzielle Vorfälle gefährden.

Im Anschluss wird diese prozentuale Belastung über eine Normierungsfunktion auf einer Skala von 0 bis 10 abgebildet. Das Modell definiert Schwellenwerte für die „Schmerzgrenze". Ein Schaden, der mehr als 20 Prozent oder in aggressiveren Modellen 50 Prozent des Jahresumsatzes entspricht, wird als existenziell (Impact-Score 10) eingestuft. Das gewährleistet, dass der CRS für ein 5-Millionen-Euro-Unternehmen genauso präzise funktioniert wie für ein 500-Millionen-Euro-Unternehmen. Das Risiko wird für die Geschäftsführung durch die direkte Kopplung an die finanzielle Leistungsfähigkeit spürbar.

$$IMPACT = f\left(\frac{Schaden_{Branche}}{Jahresumsatz}\right)$$

Abbildung 4: Berechnung des Impact-Scores, indem der durchschnittliche Branchenschaden nach einem Cyberangriff durch den jeweiligen Jahresumsatz dividiert wird (Bild: if(is))

Ein rein technischer Scan kann die organisatorische Verteidigungsfähigkeit eines Unternehmens nicht adäquat abbilden. Der Nutzer ist sich der Existenz des offenen Ports bewusst, hat jedoch keine Kenntnis darüber, dass dieser von einem Administrator überwacht wird. Er erkennt die veraltete Software, nicht jedoch den Notfallplan, der im Fall eines Ausfalls greift. Um diese Blindheit zu überwinden, integriert der CRS die Ergebnisse des BSI CyberRisikoChecks.

Im CRS dienen diese Ergebnisse als mathematische „Modulatoren", die die technischen Scores verstärken oder abschwächen:

- **Impact-Modulation (Fokus: reaktive Maßnahmen):** Fragencluster zu den Themen Notfallmanagement und Datensicherung (Backups) beeinflussen den Impact-Score. Ein Unternehmen mit einem hohen Reifegrad (etwa etablierte und getestete Notfallpläne) erhält einen Bonus-Faktor, der den angenommenen monetären Schaden reduziert. Die zugrunde liegende Logik ist, dass eine vorbereitete Partei eine schnellere Wiederherstellung der Online-Verfügbarkeit, einen geringeren Umsatzverlust und eine Minimierung von Reputationsschäden und Bußgeldern erfährt. Im Gegenzug wird ein Unternehmen ohne Notfallkonzept mit einem Malus-Faktor belegt. Im Ernstfall kann Chaos zu erheblichen Kosten führen.

- **Likelihood-Modulation (Fokus: präventive Maßnahmen):** Fragencluster zu den Themen Patchmanagement, Mitarbeitersensibilisierung und Zugriffssteuerung wirken sich auf den Likelihood-Score aus. Selbst wenn technische Schwachstellen existieren, reduziert ein gut durchdachter Prozess die Wahrscheinlichkeit einer erfolgreichen Ausnutzung erheblich. Ein funktionierendes Patchmanagement ist essenziell, um das Zeitfenster für Angreifer zu schließen. Geschulte Mitarbeiterinnen und Mitarbeiter erkennen Phishingmails, bevor Malware ausgeführt wird. Auch hier wird proaktives Verhalten direkt in der Score-Berechnung belohnt.

Durch diese Integration wird der CRS zu einem ganzheitlichen Instrument. Er bestraft nicht nur technisches Versagen, sondern belohnt Investitionen in organisatorische Sicherheit. Unternehmen können ihren Score also nicht nur durch teure Hardware, sondern auch durch optimierte Prozesse („Hausaufgaben machen") aktiv verbessern.

HYBRIDE FORMEL VERHINDERT RISIKO-VERWÄSSERUNG

Die letzte Meile der Heuristik besteht in der Synthese von Impact und Likelihood zum finalen Cyber-Risiko-Score. Das Modell vermeidet den Fehler einfacher Durchschnittsberechnungen, die extreme Risiken oft verwässern („hoher Impact + niedrige Likelihood = mittleres Risiko"; eine oft trügerische Sicherheit).

Stattdessen nutzt der CRS eine hybride Formel, die zwei mathematische Prinzipien vereint (siehe Abbildung 5):

1. **Das geometrische Mittel:** Dies veranschaulicht die multiplikative Natur von Risiken. Es wird betont, dass ein signifikantes Risiko nur entsteht, wenn beide Faktoren

vorhanden sind. Wenn einer der Faktoren den Wert Null erreicht, bricht das Risiko zusammen, was der logischen Definition von Risiko entspricht.

2. **Die Maximum-Funktion:** Dieser sogenannte „Dominanz-Term" stellt sicher, dass ein Extremwert in einer Dimension nicht ignoriert werden kann. Ein existenzbedrohender Impact (Score 10) führt auch bei geringer Wahrscheinlichkeit zu einem erhöhten Alarmzustand, ebenso wie eine akute Angriffswelle (Likelihood 10), die auch bei moderatem Schaden ernst genommen werden muss.

$$CRS = f_{max}\left(\sqrt{IMPACT \cdot LIKELIHOOD}\right)$$

Abbildung 5: Finale Berechnung des Cyber-Risiko-Scores mittels geometrisches Mittel und einer Maximum-Funktion (Bild: if(is))

Die Auswertung umfasst jedoch nicht nur die Zahl. Der CRS nutzt die im Prozess gesammelten Daten – besonders die Kontextschwere der einzelnen Assets –, um einen priorisierten Handlungsplan zu generieren. Das Bewertungssystem identifiziert nicht nur das Problem, sondern simuliert auch die Lösung: „Wenn Sie Maßnahme A auf Server B umsetzen, sinkt Ihr Score voraussichtlich um 1,2 Punkte."

Dadurch wird die IT-Sicherheit von einer unübersichtlichen technischen Herausforderung in eine steuerbare Managementaufgabe transformiert. Der CRS liefert Transparenz durch Methodik, Relevanz durch Kontext und Handlungsfähigkeit durch Priorisierung. In einer Zeit, in der die Frage nicht mehr „ob", sondern „wann" ein Angriff erfolgt, ist diese Klarheit der wertvollste Schutzschild, den ein Unternehmen haben kann.

DATENBESCHAFFUNG ALS ZENTRALE HERAUSFORDERUNG

Die Entwicklung eines öffentlichen Scoring-Modells ist mit zahlreichen Herausforderungen verbunden. Derzeit basiert der Cyberrisiko-Score auf öffentlich verfügbaren Daten, wie der Anzahl und den Kosten von Cybersicherheitsvorfällen je Unternehmensbranche. Diese Grundlage ist jedoch begrenzt und eignet sich vorerst nur für interne Evaluationen der Heuristik. Für den produktiven Einsatz sind hochwertige Unternehmensdaten in großer Menge erforderlich.

Die Beschaffung der Daten stellt sowohl organisatorisch als auch methodisch eine Herausforderung dar. Sicherheitsrelevante Unternehmensdaten sind häufig vertraulich, nicht standardisiert oder regulatorisch eingeschränkt zugänglich, was eine systematische Sammlung erschwert. Gleichzeitig besteht die Herausforderung, ausreichend große Datenmengen pro Branche zu erhalten, um robuste und generalisierbare Scoring- und Lernmodelle zu ermöglichen.

Neben der Qualität spielt auch die Herkunft dieser Daten eine zentrale Rolle. Um einen Bias zu vermeiden, ist es ratsam, die erhobenen Daten diversifiziert in einer hohen Anzahl pro Branche und aus geografisch verteilten Regionen zu beziehen. Dies ist besonders dann relevant, wenn die Daten aus öffentlichen Quellen stammen, da diese häufig nur von US-Unternehmen bereitgestellt werden. Einseitige Datenquellen können das Modell verzerren und zu einer Über- oder Unterbewertung bestimmter Branchen oder Regionen führen, obwohl die Risiken global unterschiedlich ausgeprägt sind. Ebenso ist darauf zu achten, dass die verschiedenen Unternehmensgrößen, Digitalisierungsgrade und regionale Bedrohungsprofile ausreichend repräsentiert sind, um systematische Verzerrungen zu vermeiden.

Ein Bias entsteht unter anderem durch die selektive Datengrundlage, wenn etwa Unternehmen mit bestimmten IT-Sicherheitsniveaus über- oder unterrepräsentiert sind. Dies könnte etwa der Fall sein, wenn nur besonders gut abgesicherte oder ausschließlich stark betroffene Organisationen Daten bereitstellen würden. Ohne geeignete Maßnahmen zur Diversifizierung besteht das Risiko, dass das Modell branchenspezifische Risiken nicht objektiv lernt.

Um die Heuristik zu evaluieren und stetig zu verbessern, ist der Cyber-Risiko-Score darauf angewiesen, dass sich zahlreiche Unternehmen aktiv testen lassen, um eine ausreichende Datengrundlage aufzubauen.

Die zuvor beschriebene Heuristik bildet ein unmittelbar einsetzbares Fundament für den Cyber-Risiko-Score. Die wahre Stärke und der langfristige strategische Wert des CRS liegen jedoch in seiner Weiterentwicklung zu einem prädiktiven, selbstlernenden Analysemodell. Regelbasierte Scoring-Logiken ermöglichen heute bereits eine transparente und deterministische Bewertung von IT-Sicherheitsmängeln. Der Nutzen dieses Modells steigt jedoch exponentiell an, sobald es zusätzlich prädiktive Muster, Risikodynamiken und latente Zusammenhänge erkennen kann, die heuristisch nicht explizit modelliert wurden. Die größte Herausforderung für ein prädiktives Sicherheitsmodell ist die Verfügbarkeit von Trainingsdaten. Besonders im Kontext der Cybersicherheit sind geeignete Datensätze oft fragmentiert, sensibel oder gar nicht in ausreichender Tiefe öffentlich verfügbar, obwohl sie für die Modellgüte entscheidend wären.

Das langfristige Ziel besteht darin, das regelbasierte Modul mithilfe von ausreichend gesammelten Trainingsdaten durch ein trainiertes

Bild: Deemerwha studio – stock.adobe.com

Machine-Learning-(ML)-Modell zu ersetzen. Um dieses Ziel datenschutzkonform und skalierbar zu erreichen, bietet sich der Einsatz von Federated Learning an. Das zukünftige Machine-Learning-Modell wird dezentral innerhalb der IT-Umgebungen teilnehmender Organisationen trainiert, ohne dass sicherheitskritische Rohdaten zentral gesammelt oder übertragen werden müssen. Federated Learning schafft damit eine strategische Grundlage, um den Cyber-Risiko-Score langfristig zu einem selbstlernenden, prädiktiven und anonym datenoptimierten Sicherheitsmodell weiterzuentwickeln.

FAZIT

Cyberrisiko-Scoring-Modelle sind keine neue Entwicklung. Große Unternehmen nutzen bereits eigene Modelle, um ihre IT-Sicherheit messbar zu machen. Für die meisten anderen Organisationen bleibt diese Möglichkeit jedoch verschlossen: Die existierenden Modelle sind unternehmensspezifisch zugeschnitten und nicht öffentlich zugänglich.

Der Cyber-Risiko-Score soll hier Abhilfe schaffen: Auch kleinen und mittelständischen Unternehmen soll es möglich sein, ihre IT-Sicherheit einfach zu messen. Der Fokus liegt deshalb bewusst auf einer nicht-invasiven, leicht umsetzbaren Bewertung, die bestehende IT-Prozesse nicht stört.

Der entwickelte Score dient als Metrik zur Vergleichbarkeit der IT-Sicherheit unterschiedlicher Unternehmen. Voraussetzung ist die Standardisierung des Scoring-Modells. Nur durch einheitliche Bewertungslogiken, Mängelkategorien und Gewichtungen entsteht eine faire, nachvollziehbare und sektorübergreifende Vergleichbarkeit.

Eine Standardisierung des Cyber-Risiko-Score wäre zudem ein Schritt zur Stärkung der deutschen IT-Sicherheits-Souveränität – viele Frameworks und darauf aufbauende Modelle stammen aus den USA. Ein offener, standardisierter deutscher Score kann langfristig ein interoperables Ökosystem ermöglichen, in dem Sicherheitsbenchmarks, Branchenanalysen und ML-basierte Risiko-Prognosen auf einer gemeinsamen Methodik aufbauen – statt auf proprietären Insellösungen.

Zudem stärkt Standardisierung die digitale Resilienz des Mittelstands, erleichtert Audit-Prozesse, verbessert die Messbarkeit von Security-Investitionen und schafft die Grundlage für vertrauenswürdige und anonymisierte Lernarchitekturen. ■

Literatur

[1] *Statista, „Ausgaben für IT-Sicherheit in Deutschland bis 2026", Statista, 28. November 2025. https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/*

[2] *I. D. Sánchez-García, J. Mejía und T. S. F. Gilabert, „Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation", Applied Sciences, Bd. 13, Nr. 1, S. 395, Dez. 2022, doi: 10.3390/app13010395. https://doi.org/10.3390/app13010395*

[3] *M. Ekstedt, Z. Afzal, P. Mukherjee, S. Hacks und R. Lagerström, „Yet another cybersecurity risk assessment framework", International Journal Of Information Security, Bd. 22, Nr. 6, S. 1713–1729, Juli 2023, doi: 10.1007/s10207-023-00713-y. https://doi.org/10.1007/s10207-023-00713-y*

[4] *P. Katsumata, J. Hemenway and W. Gavins, „Cybersecurity risk management," 2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, San Jose, CA, USA, 2010, pp. 890-895, doi: 10.1109/MILCOM.2010.5680181. https://ieeexplore.ieee.org/document/5680181*

[5] *J. Hughes und G. Cybenko, „Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity", Technology Innovation Management Review, Bd. 3, S. 15–24, Aug. 2013, doi: 10.22215/timreview/712. https://www.researchgate.net/publication/326311568_Quantitative_Metrics_and_Risk_Assessment_The_Three_Tenets_Model_of_Cybersecurity*

[6] *Ö. Söner, G. Kayisoglu, P. Bolat und K. Tam, „Cybersecurity risk assessment of VDR", Journal Of Navigation, Bd. 76, Nr. 1, S. 20–37, Jan. 2023, doi: 10.1017/s0373463322000595. https://www.cambridge.org/core/journals/journal-of-navigation/article/abs/cybersecurity-risk-assessment-of-vdr/8C1F2DEA2F6FA516526B8804C5B07DBC*

[7] *Z. M. King, D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman und C. Sample, „Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment", Frontiers in Psychology, Bd. 9, S. 39, Feb. 2018, doi: 10.3389/fpsyg.2018.00039. https://doi.org/10.3389/fpsyg.2018.00039*

[8] *A. Fielder, S. König, E. Panaousis, S. Schauer und S. Rass, „Risk assessment uncertainties in cybersecurity investments", Games, Bd. 9, Nr. 2, S. 34, Juni 2018, doi: 10.3390/g9020034. https://doi.org/10.3390/g9020034*

[9] *„CyberRisikoCheck", Bundesamt für Sicherheit in der Informationstechnik (Zugriff am: 18.01.2026). https://www.bsi.bund.de/dok/crc*

[10] *„IT-Sicherheit auch für KMU", BSI Lagebericht 2025 (Zugriff am: 18.01.2026). https://medien.bsi.bund.de/lagebericht/de/it-sicherheit-fuer-kmus/*

[11] *„4.3 Risiken bewerten", Bundesamt für Sicherheit in der Informationstechnik (Zugriff am: 18.01.2026). https://www.bsi.bund.de/dok/6611132*

[12] *„What is EPSS (Exploit Prediction Scoring System)?", Bitsight, 30. September 2025 (Zugriff am: 18.01.2026). https://www.bitsight.com/glossary/epss-exploit-prediction-scoring-system#:~:text=Exploit%20Prediction%20Scoring%20System%20(EPSS)%20is%20a,pose%20the%20greatest%20threat%20to%20their%20organizations*

[13] *„Known Exploited Vulnerabilities Catalog", Cybersecurity and Infrastructure Security Agency (Zugriff am: 18.01.2026). https://www.cisa.gov/known-exploited-vulnerabilities-catalog*

MERT AYAS
studiert den Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Ganzheitliche und einheitliche Risikobewertung der Unternehmens-IT – Cyber-Risiko-Score".

FERHAN KESICI
studiert den Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Ganzheitliche und einheitliche Risikobewertung der Unternehmens-IT – Cyber-Risiko-Score".

DENNIS STROZ
studiert den Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Ganzheitliche und einheitliche Risikobewertung der Unternehmens-IT – Cyber-Risiko-Score".

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.