BERICHT

Deutschlands Top-100-Unternehmen:

Bericht zu Cybersicherheitsbedrohungen

SecurityScorecard

Einleitung

Dieser Bericht analysiert die Cybersicherheit der 100 größten deutschen Unternehmen (nach Marktkapitalisierung).

Bislang müssen Unternehmen Sicherheitsvorfälle nur in wenigen Fällen melden, wodurch Regierungsvertretern, Politikern und Investoren oft wichtige Informationen zu Cybersicherheitsvorfällen fehlen. Ähnlich wie Kreditbewertungen zur Standardisierung im Finanzwesen sollten Unternehmen auch einen allgemeingültigen Rahmen zur Bewertung von Cybersicherheitsrisiken erhalten.

Um es auf den Punkt zu bringen: Autos haben Tachometer, in Arztpraxen gibt es Waagen – doch bei der Cybersicherheit befinden sich Unternehmen und öffentliche Einrichtungen im „Dauer-Blindflug".

SecurityScorecard-Bewertungen haben eine allgemeine Aussagekraft über die Cybersicherheit. Vergleichbar mit der Ermittlung von Kredit-Scores in der Finanzwelt berechnet SecurityScorecard eine punktebasierte Bewertung zur Quantifizierung des Cybersicherheitsrisikos im gesamten digitalen Ökosystem.
Mithilfe des weltgrößten proprietären Datenbestands zu Risiken und Bedrohungen hat SecurityScorecard 15.000 bisherige Sicherheitsvorfälle analysiert, um deren zugrunde liegenden Cybersicherheitsprobleme zu identifizieren.

Bei Unternehmen mit einem A-Rating ist ein Cybersicherheitsvorfall

13-MAL UNWAHRSCHEINLICHER

als bei Firmen mit einem F-Rating.

Wichtigste Ergebnisse:

Die 100 größten deutschen Unternehmen wurden nach kritischen Cybersicherheitsfaktoren wie Netzwerksicherheit, Malware-Infektionen, Endpunktsicherheit, Patching-Kadenz, Anwendungssicherheit und DNS-Status bewertet. Nach einer umfassenden Analyse der Angriffsfläche und gemeldeten Sicherheitsvorfälle kommt SecurityScorecard zu folgenden Ergebnissen:

1. **94 %** hatten einen Sicherheitsvorfall in ihrem Third-Party-Ökosystem.
2. **95 %** hatten einen Sicherheitsvorfall in ihrem Fourth-Party-Ökosystem.
3. **20 %** erreichen ein A-Rating und hatten keine Sicherheitsvorfälle im Vorjahr.
4. **34 %** der Unternehmen werden mit einem C-Rating oder schlechter eingestuft.
5. **8 %** hatten im letzten Jahr einen Sicherheitsvorfall.
6. Schlusslicht ist der Kommunikationssektor mit einem C-Rating (oder schlechter) für **57 %** der Unternehmen.
7. Das stärkste Sicherheitsprofil hat die deutsche Versorgungswirtschaft: Nur **17 %** dieser Unternehmen haben ein C-Rating oder eine schlechtere Bewertung erhalten.

Ergebnisse

Gesamtbewertung

1. **21 %** mit A-Rating
2. **44 %** mit B-Rating
3. **30 %** mit C-Rating
4. **2 %** mit D-Rating
5. **2 %** mit F-Rating

Rating	Sicherheitsvorfall Wahrscheinlichkeit
A	1-fach
B	2,9-fach
C	5,4-fach
D	9,2-fach
F	13,8-fach

Im Durchschnitt kostet eine Datenpanne weltweit 4,5 Mio. USD.

IBM Security: „Cost of Data Breach Report 2023".

Branchen-übersicht

Cyberrisiken in der Lieferkette

Ist ein direkter Angriff auf ein Unternehmen nicht möglich, rücken die Lieferanten und Partner eines Unternehmens ins Visier von Cyberkriminellen. Wie frühere SecurityScorecard-Studien zeigen, haben 98 % der Unternehmen einen Drittanbieter, bei dem es einen Sicherheitsvorfall gab. Und die schlechtesten Sicherheitsbewertungen findet man in den Branchen, die allein wegen ihrer unzähligen Third-Party-, Fourth-Party- und weiteren Anbietern die komplexesten Angriffsflächen aufweisen.

„Das Ökosystem von Lieferanten ist ein äußerst attraktives Ziel für Ransomware-Angreifer. Die Third-Party-Opfer erfahren oft erst durch die Lösegeldforderung von einem Vorfall. So haben die Angreifer genug Zeit, unbemerkt Hunderte von Unternehmen zu infiltrieren."

– Ryan Sherstobitoff, Senior Vice President of Threat Research and Intelligence

Kommunikationsbranche

Unternehmen im Kommunikationssektor schnitten bei der Sicherheitsbewertung insgesamt am schlechtesten ab: 57 % erhielten ein C-Rating oder eine noch schlechtere Einstufung. Da die Kommunikationsbranche Telekommunikations-, Internet- und Cloud-Anbieter umfasst, hat sie es mit einer ungewöhnlich komplexen Angriffsfläche zu tun.

Diese Branche ist auf weitläufige Drittanbieter-, Partner- und ISP-Netzwerke angewiesen. In anderen Worten: Der Kommunikationssektor unterliegt schon deshalb einem höheren Third-Party-Risiko, weil es mehr Drittanbieter gibt.

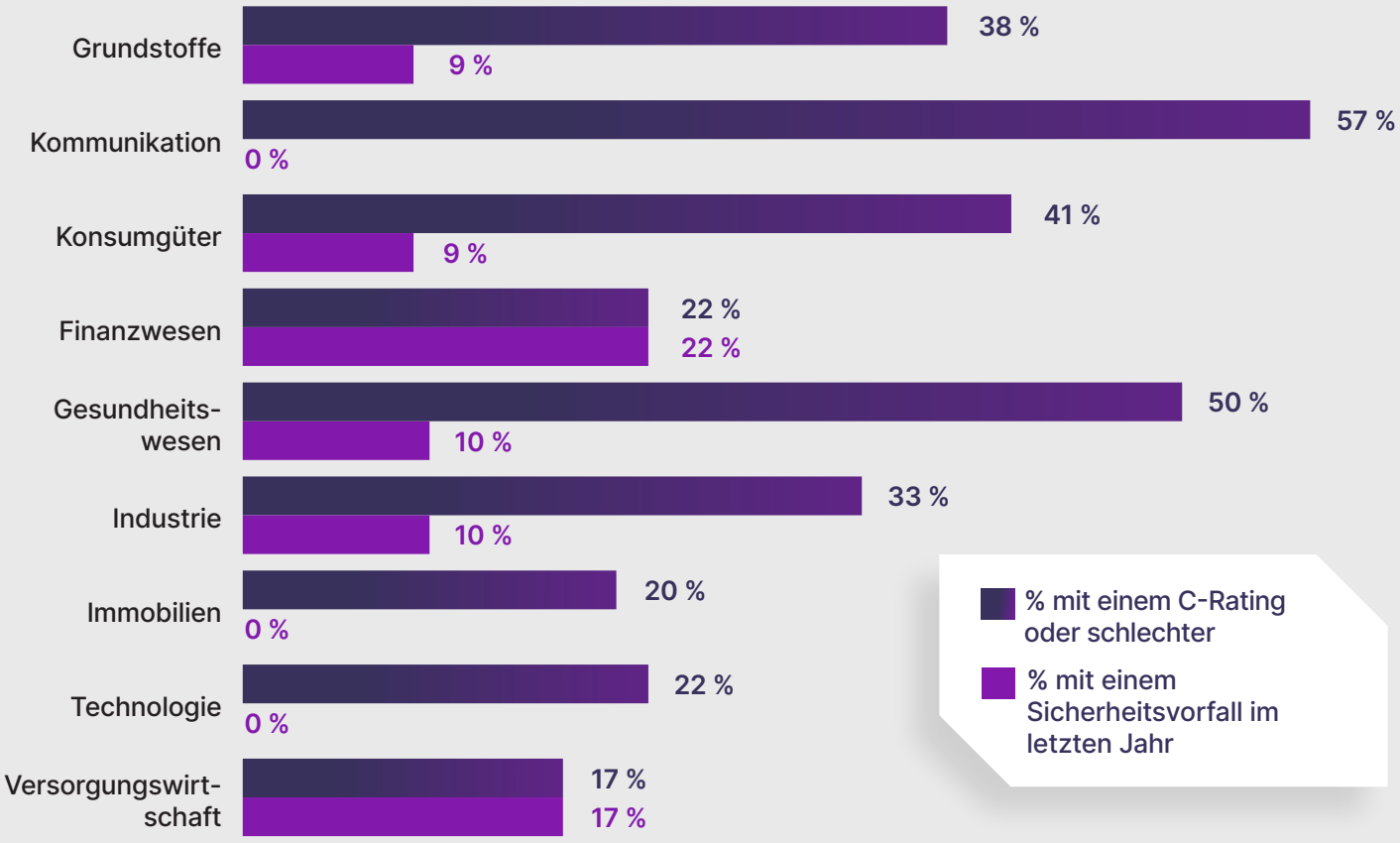
Gesundheitswesen

Der deutsche Gesundheitssektor landet bei der Gesamtbewertung auf dem vorletzten Platz: 50 % erhalten ein C-Rating oder darunter. Ähnlich wie in der Kommunikationsbranche gibt es auch im Gesundheitswesen zahlreiche unterschiedliche und sehr spezielle Geschäftsbeziehungen zu Drittanbietern, wodurch mehr Third-Party-Sicherheitsvorfälle möglich (und wahrscheinlich) werden.

Versorgungswirtschaft

Wie bereits erwähnt, ist die Versorgungswirtschaft in Deutschland die robusteste Branche. Nur 17 % der Versorgungsunternehmen weisen ein Rating von C oder eine schlechtere Bewertung auf. Die zweitstärkste Cybersicherheit hat der Immobiliensektor: Hier schneiden lediglich 20 % der Unternehmen mit einem C-Rating oder noch schlechter ab.

Bewertungen nach Sektoren



Bewertung nach Ländern

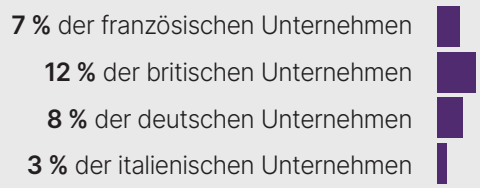
In unserer stark vernetzten digitalen Welt überschreitet die Cybersicherheit nationale Grenzen und unternehmenseigene Netzwerke. Folglich ist die Cybersicherheit eine globale Herausforderung. Entsprechend wichtig sind der Informationsaustausch und die Zusammenarbeit zwischen Regierungen, Branchen und Unternehmen zur Gewährleistung unserer kollektiven Cyberresilienz.

Obwohl sich diese Analyse auf deutsche Unternehmen konzentriert, wurden auch vergleichbare Daten von führenden Unternehmen aus Italien, Frankreich und Großbritannien herangezogen. Demnach haben britische Unternehmen die stärkste Cybersicherheit, von denen nur 24 % ein C-Rating oder eine schlechtere Bewertung erhielten – wohingegen 34 % der deutschen, 40 % der französischen und 41 % der italienischen Firmen bei der Sicherheit in der C-Klasse oder darunter spielen.

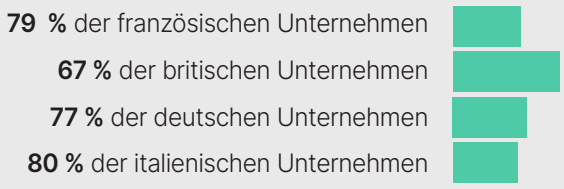
Verglichen mit Großbritannien, Deutschland und Italien belegt Frankreich den unrühmlichen 1. Platz bei Datenpannen durch Third- und Fourth-Anbieter (98 % bzw. 100 %).

Benchmarking

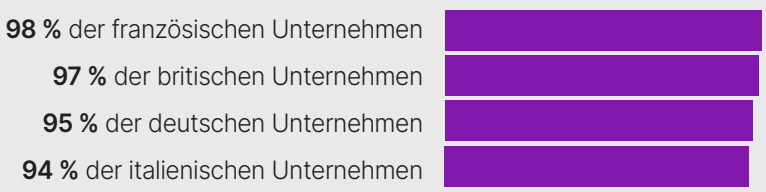
Unternehmen mit Sicherheitsvorfällen im letzten Jahr



Unternehmen mit A-Rating ohne Sicherheitsvorfälle im letzten Jahr



Unternehmen mit Sicherheitsvorfällen in Third-Party-Ökosystemen



„Das Third-Party-Risikomanagement ist eine zentrale Komponente jedes robusten Cybersicherheitsprogramms und die in diesem Bericht untersuchten Unternehmen würden davon profitieren, wenn sie dem Priorität einräumten. Die Branchen und Unternehmen in Deutschland (und in Europa insgesamt) müssen jetzt mehr tun, um für die Umsetzung des DORA [Digital Operational Resilience Act] bis Januar 2025 sowie der NIS2-Richtlinie bereit zu sein.

„Der europaweite Anstieg der Datenpannen zeigt, dass deutsche Unternehmen das Third-Party-Risikomanagement (TPRM) nicht nur in ihr Security-Programm, sondern auch in den Lieferantenauswahl-Prozess integrieren müssen.

SecurityScorecard kann dabei mit Bewertungen zur Beurteilung potenzieller Anbieter und dem Monitoring bestehender Lieferanten helfen, um diese in die Verantwortung zu nehmen.“

– Thomas de Raaf, Senior Field Sales Director, DACH

Lieferkettenrisiken gehen über Drittanbieter hinaus

Zwar werden in der Lieferkette normalerweise die Third-Party-Anbieter am stärksten überprüft, doch auch Fourth-Party-Anbieter stellen ein erhebliches Risiko dar.

Wie dieser Bericht zeigt, gab es im Third-Party-Ökosystem von 94 % der Unternehmen einen Sicherheitsvorfall. Weitere Analysen offenbaren zudem bei 95 % der größten deutschen Unternehmen eine Kompromittierung im Fourth-Party-Ökosystem. Das unterstreicht, wie wichtig die Identifizierung und Bewertung des Sicherheitsprofils aller weiteren nachrangigen Anbieter im digitalen Ökosystem eines Unternehmens ist.

Sind ein Third- oder Fourth-Party-Anbieter von einer Kompromittierung betroffen, kann dies auf einen Schlag eine große Zahl seiner Kunden oder sogar deren Kunden in Mitleidenschaft ziehen: Der MOVEit-Exploit wurde z. B. im Frühjahr 2023 entdeckt und Unternehmen haben immer noch mit den Folgen dieser Schwachstelle zu kämpfen, die voraussichtlich Kosten von mindestens 65 Milliarden US-Dollar verursachen dürfte.

Weitere Einblicke in die Marktkapitalisierung

Ein womöglich widersprüchliches Ergebnis unserer Analyse ist, dass die 25 Unternehmen mit der höchsten Marktkapitalisierung beim Rating am schlechtesten abschneiden (44 % mit C-Ratings oder darunter), während von den 25 Unternehmen am unteren Ende der Skala lediglich 28 % ein C-Rating erhielten. Dies zeigt, dass jedes Unternehmen – unabhängig von Größe, Branche, Umsatz oder Marktkapitalisierung – zum Ziel von Cyberkriminellen werden kann, wenn es an einer starken Cyberabwehr mangelt.

Weltweit scheint es zudem einen Zusammenhang zwischen der Cyberrisiko-Exposition eines Landes und seinem Bruttoinlandsprodukt (BIP) zu geben. Im Januar präsentierte SecurityScorecard auf der Jahrestagung des Weltwirtschaftsforums in Davos die Cyber Resilience Scorecard, wonach der wirtschaftliche Wohlstand eines Landes eng mit seiner Fähigkeit zusammenhängt, mit einer komplexen Cyberbedrohungslage zurechtzukommen.

Nach dem Bericht weisen der Nahe Osten, Nordamerika, der Pazifikraum sowie Nord-, West- und Mitteleuropa die höchsten Sicherheitsbewertungen weltweit auf. Mit anderen Worten: Regionen mit einem höheren Pro-Kopf-BIP haben tendenziell eine bessere Cybersicherheitshygiene und ein geringeres Cyberrisiko. Mit einem der höchsten Pro-Kopf-BIP in Europa dürfte Deutschland vermutlich bessere Voraussetzungen mitbringen, in eine belastbare, sichere Infrastruktur zu investieren sowie aktive Security-Programme zu implementieren und aufrechtzuerhalten, um sich ständig weiterentwickelnden Cyberbedrohungen wirkungsvoll zu erwehren. In wohlhabenderen Ländern wie Deutschland dürfte auch mehr lizenzierte Software verwendet werden, die mit Security-Patches auf dem neuesten Sicherheitsstand gehalten wird.

Der Schutz kritischer Infrastrukturen ist entscheidend

Rund 40 % der Unternehmen in diesem Bericht stammen aus kritischen Sektoren, konkret: Energiewirtschaft, Telekommunikation, Transport, Industrie und Gesundheitswesen. Damit eine Gesellschaft reibungslos funktioniert, muss sich die Bevölkerung darauf verlassen können, dass staatliche Dienstleistungen und Einrichtungen sicher sind. Unternehmen in diesen Sektoren dürften daher von den folgenden Empfehlungen profitieren. Weitere Hinweise und Best Practices finden Sie im SecurityScorecard Report 2023 „Addressing the Trust Deficit in Critical Infrastructure“, der die Schaffung von Vertrauen in kritische Infrastrukturen thematisiert.

Empfehlungen

Für viele deutsche Unternehmen sollte die Verbesserung der Cybersicherheitshygiene hohe Priorität haben. Obwohl die Mehrheit bei der Cybersicherheit relativ gut abschneidet, waren fast alle Unternehmen von Sicherheitsvorfällen bei Third- und Fourth-Anbietern betroffen. Zur Risikominimierung und Verbesserung des allgemeinen Cybersicherheitsprofils empfiehlt SecurityScorecard folgende Maßnahmen:

Schwerpunkt auf Anwendungs- und Netzwerksicherheit: Alle Unternehmen sollten die Verbesserung der Anwendungs- und Netzwerksicherheit priorisieren. Diese beiden Aspekte sind für den Schutz vor unterschiedlichsten Cyberbedrohungen von grundlegender Bedeutung.

Unternehmen mit hohem Risiko: In den 34 % der Unternehmen mit einem Cybersicherheitsrating von C (oder schlechter) besteht dringender Handlungsbedarf. Neben der Stärkung der Anwendungs- und Netzwerksicherheit sollten diese Hochrisiko-Unternehmen besonders auf Folgendes achten:

DNS-STATUS: Sicherstellung des Status und der Integrität der Domain-Name-System-Konfigurationen (DNS). Fehlkonfigurationen dieser kritischen Komponente können zu Schwachstellen führen.

ENDPUNKTSICHERHEIT: Stärkung der Sicherheit aller Endpunkte, einschließlich Laptops, Desktops, Mobil- und mitarbeitereigene Geräte (BYOD, Bring Your Own Device). Das Identifizieren und Beheben von Schwachstellen bei diesen Endpunkten ist von entscheidender Bedeutung.

PATCHING-KADENZ: Festlegung einer einheitlichen, zeitnahen Patching-Kadenz für Systeme, Software und Hardware. Regelmäßige Updates tragen dazu bei, bekannte Schwachstellen zu beheben.

Neben der Kenntnis der eigenen Sicherheitsbewertung sollten alle Unternehmen auch die Faktoren kennen, die diese beeinflussen. Jedes Unternehmen kann einen detaillierten Bericht zu seiner Bewertung kostenlos von SecurityScorecard erhalten.

Fazit

Vertrauen und Transparenz sind in der Cybersicherheit extrem wichtig. Dennoch fällt vielen Unternehmen die Selbsteinschätzung ihrer Cybersicherheit schwer. Unsere Analyse der nach Marktkapitalisierung größten deutschen Unternehmen unterstreicht die entscheidende Bedeutung dieser Grundsätze.

Die Bewertung der Cybersicherheit ist ein ständiger Prozess. Sicherheitsbewertungen liefern Cybersecurity-Verantwortlichen die nötigen Erkenntnisse, um fundierte Entscheidungen zu treffen, das Sicherheitsprofil zu stärken und eskalierenden Risiken durch bessere Zusammenarbeit zu begegnen.

Angesichts der sich ständig verändernden und sich entwickelnden Bedrohungslage stellen Security-Ratings und Lösungen für das Third-Party-Monitoring ein proaktives Engagement für die Cybersicherheit dar. Wir sind davon überzeugt, dass jedes bei dieser Analyse berücksichtigte Unternehmen seine Cybersicherheit verbessern und zu insgesamt mehr Sicherheit sowie einer besseren Zusammenarbeit in Sicherheitsfragen beitragen kann.

Methodik

Eine dynamische Bedrohungslage erfordert eine Risikobewertung in Echtzeit. Auch muss die Bewertung von Cyberrisiken auf Grundlage aktueller Daten erfolgen. SecurityScorecard erhebt nicht invasiv umfassende Daten zur Cybersicherheitsleistung von Unternehmen auf der ganzen Welt, um deren Cyberabwehr zu beurteilen. Wir erstellen eine Gesamtbewertung mit einem Rating von A bis F basierend auf zehn Faktoren, die einen Sicherheitsvorfall wahrscheinlich machen.

Analyse-Zeitraum:
Der Bericht gibt Auskunft über das Cybersicherheitsprofil der 100 größten Unternehmen in Deutschland nach Marktkapitalisierung im Zeitraum vom 13. März 2023 bis 13. März 2024.

Anhang

Was sind Sicherheitsbewertungen?

SecurityScorecard bietet Unternehmen einen umfassenden Überblick über das Sicherheitsprofil von Unternehmen, einschließlich der Third- und Fourth-Party-Risiken.

Diese Sicherheitsbewertungen sind vollständig nachweisbar und beruhen auf einer fundierten, transparenten Beobachtung mit Security-Scans des gesamten IPv4-Adressraums. In Korrelation mit Daten über Sicherheitsvorfälle liefern die SecurityScorecard-Faktoren Erkenntnisse, die Unternehmen wichtige Bereiche aufzeigen, um ihre Risiko-Exposition zu verringern. Die Bewertung basiert auf folgenden zehn Faktoren:

Netzwerksicherheit: Überprüfung auf offene Ports (wie SMB und RDP), unsichere oder falsch konfigurierte SSL-Zertifikate sowie Datenbank- und IoT-Schwachstellen

DNS-Status: Überprüfung auf Fehlkonfigurationen (wie Open Resolver) und empfohlene Konfigurationen für DNSSEC, SPF, DKIM und DMARC

Patching-Kadenz: Ermittlung der Update-Häufigkeit für identifizierte Dienste, Software und Hardware eines Unternehmens

Endpunktsicherheit: Ermittlung der Versionen und Anfälligkeit von Laptops, Desktop-Rechnern, Mobil- und BYOD-Geräten, die auf die Netzwerke eines Unternehmens zugreifen

IP-Reputation: Signalerfassung durch das Sinkhole-System von SecurityScorecard, das weltweit Millionen Malware-Signale von Command-and-Control-Infrastrukturen (C2) verarbeitet, die von Angreifern kontrolliert werden, einschließlich Zuordnung der identifizierten kompromittierten IP-Adressen zu den betroffenen Unternehmen

Hacker-Chatter: Beobachtung der Hacker-Untergrundszene und Darknet-Webseiten, die sich mit angegriffenen Unternehmen und IP-Adressen beschäftigen

Informationslecks: kompromittierte Anmeldedaten aus Datenpannen oder Datenlecks, Keylogger-Dumps, Pastebin-Dumps, Datenbank-Dumps und anderen Informations-Repositories

Social Engineering: Messung der Nutzung von Unternehmenskonten für soziale Netzwerke, Finanzkonten und Marketinglisten

Cubit Scores: Ermittlung kritischer Sicherheits- und Konfigurationsprobleme (wie exponierte Systemsteuerungen auf Administratorebene) durch Berechnung mit dem proprietären Bedrohungsalgorithmus von SecurityScorecard

Erfahren Sie mehr und erstellen Sie Ihr kostenloses Konto unter SecurityScorecard.com

ÜBER SECURITYSCORECARD

SecurityScorecard wird von führenden Investoren finanziert, darunter Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV und Riverwood Capital. Mit der ständigen Sicherheitsbewertung von über 12 Millionen Unternehmen ist SecurityScorecard der weltweit führende Anbieter von Cybersecurity-Ratings und Einstufungen der Reaktionsfähigkeit und Resilienz von Unternehmen.

SecurityScorecard wurde 2013 von den Sicherheits- und Risikoexperten Dr. Aleksandr Yampolskiy und Sam Kassoumeh gegründet. Über 25.000 Unternehmen und Einrichtungen nutzen die patentierte Bewertungstechnologie von SecurityScorecard für das Unternehmens- und Third-Party-Risikomanagement, Vorstandsberichte, Due-Diligence-Prozesse, den Abschluss von Cyberversicherungen und die Regulierungsaufsicht.

SecurityScorecard trägt zu mehr Sicherheit in der Welt bei und unterstützt Unternehmen, ein besseres Verständnis von Cyberrisiken zu gewinnen und die Stärkung der eigenen Cybersicherheit auf allen Unternehmensebenen sowie bei Lieferanten zu thematisieren und zu verbessern. SecurityScorecard hat die Auszeichnung „Federal Risk and Authorization Management Program (FedRAMP) Ready“ erhalten – eine Bestätigung der robusten Sicherheitsstandards des Unternehmens zum Schutz von Kundeninformationen. Außerdem wird SecurityScorecard von der US-Behörde für Cyber- und Infrastruktursicherheit CISA als kostenloses Cybertool und kostenloser Cyberservice genannt. Jedes Unternehmen und jede Einrichtung kann bei SecurityScorecard ein vertrauenswürdiges, transparentes Instant Rating durchführen lassen. Für weitere Informationen besuchen Sie securityscorecard.com oder vernetzen Sie sich mit uns auf LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io