9 wichtige Trends im Bereich Cybersicherheit für 2024



1. CTEM (Continuous Threat Exposure Management)





- 3. Management von Cybersicherheitsrisiken durch Dritte
 - 4. Datenschutzorientierte Entkopplung von Anwendungen
 - 5. Generative KI

6. Programme für Sicherheits-

verhalten

und -kultur

und Daten

9. Umschulung im Bereich Cybersicherheit

101100 010110



7. Cybersicherheit-UDIVIS

8. Sich entwickelnde Betriebsmodelle für Cybersicherheit

Widerstandsfähigkeit 1. CTEM (Continuous Threat

Exposure Management)

Optimierung für

wurde insbesondere durch die beschleunigte Einführung von SaaS, die Ausweitung digitaler Lieferketten, die verstärkte Präsenz von Unternehmen in den sozialen Medien, die Entwicklung kundenspezifischer Anwendungen, die Telearbeit und die internetbasierte Kundeninteraktion angetrieben.

Die Angriffsflächen von Unternehmen sind in den

letzten Jahren enorm gewachsen. Dieses Wachstum



heitswerts von IAM

2. Erhöhung des Cybersicher-

Haftungsausschluss: Die Trends sind nicht nach ihrer Wichtigkeit geordnet.

Die Rolle des IAM (Identity- und Access-Management) in der Cybersicherheit wird immer

wichtiger. Seit 2023 ist IAM das zweithäufigste Diskussionsthema von SRM-Führungskräften (Security and Risk Management), die Gartners Kundenanfrageservice nutzen.





heitsrisiken durch Dritte Die Unvermeidbarkeit von Cybersicherheitsvorfällen bei Dritten zwingt SRM-Führungskräfte dazu,

3. Management von Cybersicher-

zu konzentrieren und von vorgelagerten Due-Diligence-Aktivitäten abzurücken.

sich stärker auf resilienzorientierte Investitionen



und Daten Multinationale Unternehmen, die sich jahrzehntelang auf Single-Tenant-Anwendungen verlassen haben, sehen sich mit wachsenden Compliance-Anforderungen und

Entkopplung von Anwendungen

4. Datenschutzorientierte

dem Risiko von Geschäftsdisruptionen konfrontiert. Dies ist auf die zunehmenden länderspezifischen Datenschutz- und Lokalisierungsanforderungen zurückzuführen, die zu einer erzwungenen Fragmentierung von Unternehmensanwendungsarchitekturen und Datenlokalisierungspraktiken



SRM-Führungskräfte können den Ruf und die Leistung

Optimierung für Leistung

der Sicherheitsabteilung verbessern, indem sie GenAl (generative KI) in proaktiver Zusammenarbeit mit Stakeholdern einsetzen. Dies wird dazu beitragen, die

5. Generative KI

Grundlagen für eine ethische, sichere und geschützte Nutzung dieser disruptiven Technologie zu schaffen.





SBCPs (Security Behavior and Culture Programs) verfolgen einen unternehmensweiten Ansatz zur Minimierung von Cybersicherheitsvorfällen im Zusammenhang mit dem Verhalten von Mitarbeitenden.

Ein stärkerer Fokus auf die menschlichen Elemente

Sicherheitsverhalten und -kultur

6. Programme für

von SBCPs zeigt sich weiterhin vielversprechend, um die Auswirkungen von unsicherem Mitarbeiterverhalten zu minimieren.



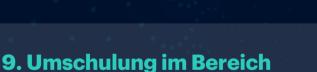
erzielten Schutzniveau ziehen können.

ODMs (Outcome-Driven Metrics) der Cybersicherheit sind operative Metriken mit besonderen Eigenschaften,

mit denen die Stakeholder der Cybersicherheit eine

Cybersicherheit und dem durch diese Investitionen

gerade Linie zwischen den Investitionen in die





Dies stellt herkömmliche Betriebsmodelle für die Cybersicherheit infrage. SRM-Führungskräfte passen ihre Betriebsmodelle an die Geschäftsanforderungen an.

IT-Abteilungen auf die Geschäftsbereiche.

8. Sich entwickelnde Betriebs-

Der Erwerb, die Entwicklung und die Bereitstellung

von Technologie verlagert sich von den zentralen

modelle für Cybersicherheit



viele Führungskräfte in der Cybersicherheit stellen weiterhin Personal basierend auf veralteten Rollen und Fähigkeiten ein. SRM-Führungskräfte müssen ihren Teams neue Kompetenzen beibringen, indem

Die Fähigkeiten, die Cybersicherheitsteams

benötigen, verändern sich derzeit drastisch, doch

Cybersicherheit

sie vorhandene Talente umschulen und neue Talente mit neuen Profilen einstellen.





Ressourcen und Tools für Führungskräfte im Bereich Cybersicherheit:

Umsetzbare, objektive Insights

Leadership-Vision für Führungs-Die neuen Technologien und kräfte im Bereich Sicherheit und Trends im Bereich Sicherheit Risikomanagement im Jahr 2024 tur 2024 von Gartner

Jetzt herunterladen

Prioritäten für das Jahr 2024.

Entdecken Sie die 3 wichtigsten strategischen

Positionieren Sie Ihr Unternehmen für den Erfolg. Entdecken Sie diese zusätzlichen, ergänzenden

Webinar

Roadmap IT-Roadmap für

Jetzt ansehen

Cybersicherheit Erstellen Sie eine belastbare, skalierbare und agile Cybersicherheitsstrategie.

Identifizieren Sie die neuen Technologien, die die

Sicherheitslandschaft revolutionieren werden.

Wie wir helfen

Quelle: Gartner

E-Book

Wie Gartner mit CISOs zusammenarbeitet

Finden Sie heraus, wie wir Ihnen die Erkenntnisse, die Beratung und die Tools

bieten können, die Sie zur Erfüllung Ihrer geschäftskritischen Prioritäten benötigen. Mehr erfahren



Jetzt herunterladen

Bereits Kunde?

Erhalten Sie über Ihr Kundenportal Zugang zu weiteren Ressourcen. Anmelden

Erfahren Sie mehr über Gartner für Führungskräfte im Bereich Cybersicherheit

© 2024 Gartner, Inc. und/oder deren Tochterunternehmen. Alle Rechte vorbehalten. CM_GTS_2771860

Folgen Sie uns auf LinkedIn

Kunde werden