CIO CSO COMPUTERWOCHE VOICE OF DIGITAL

STUDIE

SECURITY AS A SERVICE 2023

DIE WICHTIGSTEN ERGEBNISSE PRÄSENTIERT VON

radware

Security Services erleichtern den Alltag

Liebe Leserinnen, liebe Leser,

vielen Dank für Ihr Interesse an den Ergebnissen unserer Studie „Security as a Service 2023“. An der Umfrage von CIO, CSO und COMPUTERWOCHE, die im Mai 2023 online durchgeführt wurde, haben sich insgesamt 373 Entscheiderinnen und Entscheider sowie aus Unternehmen der D-A-CH-Region beteiligt. Es handelt sich dabei um Verantwortliche aus allen (IT-Security-)relevanten Unternehmensbereichen, vom C-Level über die Fachbereiche bis hin zum IT-Bereich.

Die Studienergebnisse zeigen, dass es vor allem drei große technische Herausforderungen in Bezug auf IT-Sicherheit für die Unternehmen gibt: die wachsende Bedrohungslage durch immer komplexere Cyberangriffe, fehlende Informationen über den Wert von bedrohten Daten und Prozessen und die Absicherung von Cloud-Daten.

Um diesen Herausforderungen begegnen zu können, nehmen Unternehmen gerade in den Kernbereichen der Security zunehmen die Hilfe externer Dienstleister und Partner in Anspruch – es geht beispielsweise um die Überwachung von Security Policies, die Implementierung von sicherheitsfördernden Prozessen sowie von technischen Systemen und Software. Wichtig ist, dass diese Services alltagstauglich sind und die Unternehmen auch tatsächlich beispielsweise im Day-to-Day Betrieb ihrer IT-Security-Infrastruktur unterstützen können.

Je schneller der unmittelbare Mehrwert von Security Services ersichtlich wird, desto eher wächst das Vertrauen zu den Partnern. Es verwundert daher nicht, dass fast drei Viertel der von uns befragten Unternehmen ihre (mitunter eingekauften) Fähigkeiten zur Erkennung von Cyberrisiken und -angriffen sowie ihre Cyberabwehr mit den Schulnoten „gut“ oder sogar „sehr gut“ bewerten.

Die Kehrseite: Über 16 Prozent der Unternehmen geben an, dass es zwar Cybervorfälle gab, sie aber nicht genau wüssten, wie diese ausgesehen hätten. Drei Prozent der Befragten wissen zudem gar nicht, ob es in den vergangenen zwei Jahren einen Security Incident gegeben hat. Dazu kommt: Diejenigen, die Kenntnis von einem Vorfall haben, erlitten in fast 60 Prozent der Fälle einen nennenswerten Schaden.

Es entsteht mitunter der Eindruck, dass in vielen Unternehmen immer noch eher eine Scheinsicherheit als eine tatsächliche Sicherheit vorherrscht. Es gibt für die Security-Dienstleister also weiterhin reichlich Potenzial für neue Partnerschaften.

Wir freuen uns, Ihnen mit dem hier vorliegenden Whitepaper ausgewählte Ergebnisse unserer Studie präsentieren zu dürfen und wünschen eine spannende Lektüre.

Ihre Teams von Radware und der Marktforschung von CIO, CSO und COMPUTERWOCHE

Technische Antworten auf komplexe Cyberattacken sind gesucht

Als größte technische Herausforderung in der Security nennen 45 Prozent der Unternehmen die wachsende Bedrohung durch immer komplexere Cyberangriffe. Knapp dahinter liegen mit rund 45 Prozent die fehlenden Informationen über die bedrohten Daten und Prozesse. Die Absicherung der Daten in der Cloud liegt mit 43 Prozent der Nennungen auf dem dritten Platz.

Komplexität ist kein generelles technisches Problem, sondern wird eher bei der Bedrohungslage als Herausforderung angesehen. So nennen nur 17 Prozent die wachsende Komplexität im Identitäts- und Berechtigungsmanagement (IAM) als größte technische Herausforderung, und 23 Prozent entsprechend die Komplexität von IT-Infrastrukturen zum Beispiel durch Hybrid Clouds.

Demnach scheint für die Unternehmen die Komplexität in der Security selbst weniger eine Herausforderung zu sein als im Bereich der Cyberbedrohungen.

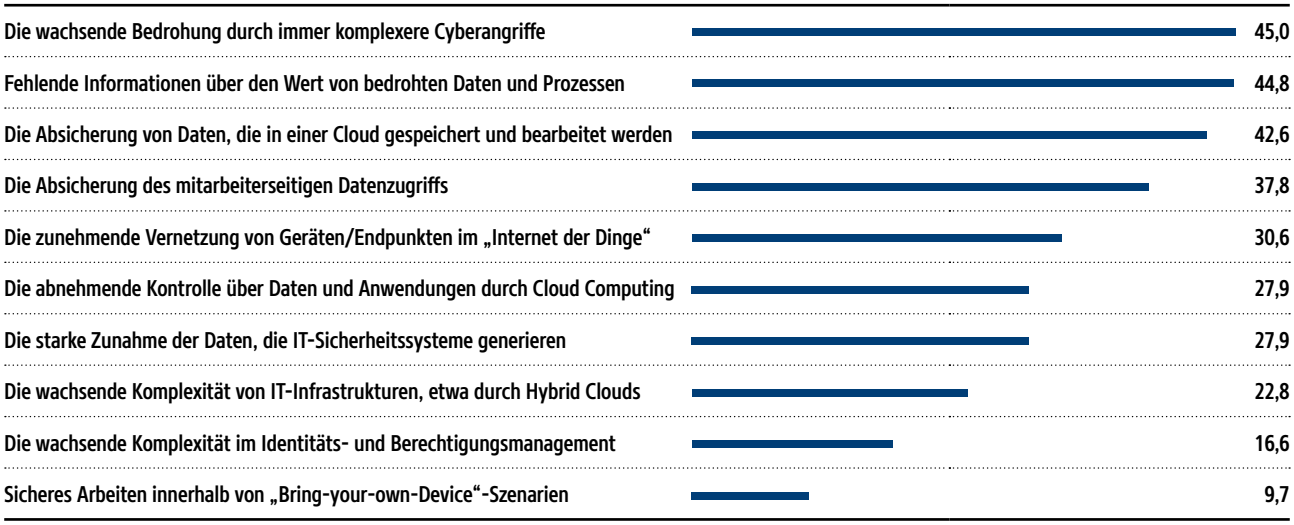
Die komplexen Cyberattacken nennen die Unternehmen mit 500 bis 999 Beschäftigten besonders häufig (48 Prozent), kleinere Unternehmen mit weniger als 500 Beschäftigten sind nur noch zu 41 Prozent dieser Meinung.

KRITIS-Betreiber sind wegen der komplexen Cyberattacken etwas weniger besorgt (43 Prozent der Nennungen) als Organisationen, die nicht zu KRITIS gerechnet werden (46 Prozent).

In Geschäftsführung und Vorstand gelten bei 61 Prozent die wachsenden Bedrohungen durch immer komplexere Cyberangriffe als zentrale Herausforderung, im C-Level des IT-Bereichs sagen dies immer noch 50 Prozent der Befragten. In der Stufe darunter, der IT-Leitung, sinkt der Anteil derer, die die Komplexität der Cyberattacken als besonderes Problem für die technische Security sehen, auf 31 Prozent.

Was sind in Ihren Augen für die Unternehmen die größten technischen Herausforderungen in Bezug auf IT-Security?

Angaben in Prozent. Mehrfachnennungen möglich. Dargestellt sind die Top-10-Antworten. Basis: n = 373



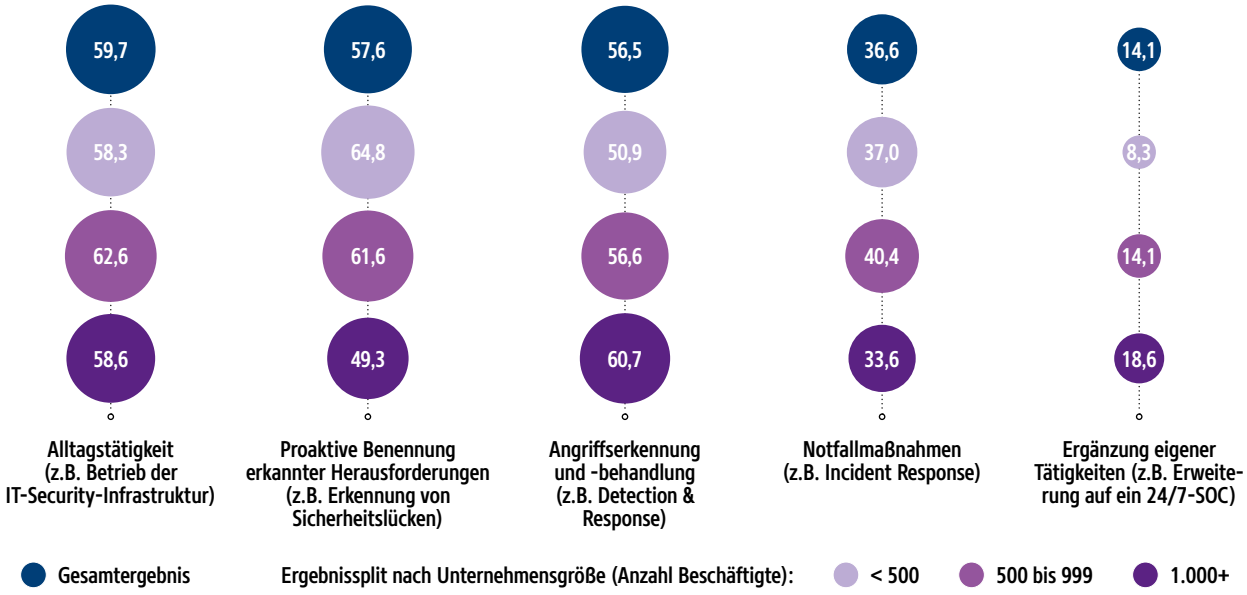
2

Security-Dienstleistungen müssen alltagstauglich sein

Den größten Mehrwert bieten Security-Dienstleistungen, wenn sie bei der Alltagstätigkeit eines Unternehmens helfen – das sagen 60 Prozent der Befragten. 58 Prozent erkennen in der proaktiven Benennung erkannter Herausforderungen einen solchen Mehrwert, zum Beispiel durch das Aufspüren von Sicherheitslücken. Weniger gefragt ist die Erweiterung bestehender Security-Funktionen.

In welchem Bereich bietet ein IT-Security-Dienstleister / MSSP Ihrem Unternehmen den größten Mehrwert?

Angaben in Prozent. Mehrfachnennungen möglich. Fünf vorgegebene Antworten. Filter: Unternehmen, die mit mindestens einem IT-Security-Dienstleister / MSSP zusammenarbeiten. Basis: n = 347



So ist die Ergänzung eigener Security-Tätigkeiten nur für 14 Prozent ein besonders großer Mehrwert, zum Beispiel die Erweiterung des eigenen SOC-Betriebs auf ein 24x7-SOC (24 Stunden, 7 Tage die Woche). Erstaunlich ist zudem, dass Unterstützung bei Notfallmaßnahmen (Incident Response) nur von 37 Prozent der Befragten als sehr großer Mehrwert von Security Services gesehen wird. Angriffserkennung und -behandlung nennen indes 57 Prozent der Unternehmen auf die Frage nach dem größten Mehrwert von Security-Dienstleistungen.

Die Ergänzung eigener Security-Funktionen erkennen größere Unternehmen eher als Nutzen von Security-Dienstleistungen an: So sehen nur acht Prozent der kleineren Unternehmen mit weniger als 500 Beschäftigten hierin den größten Mehrwert, bei 500 bis 999 Beschäftigten sind es 14 Prozent, bei den größeren mit mehr als 1.000 Beschäftigten 19 Prozent.

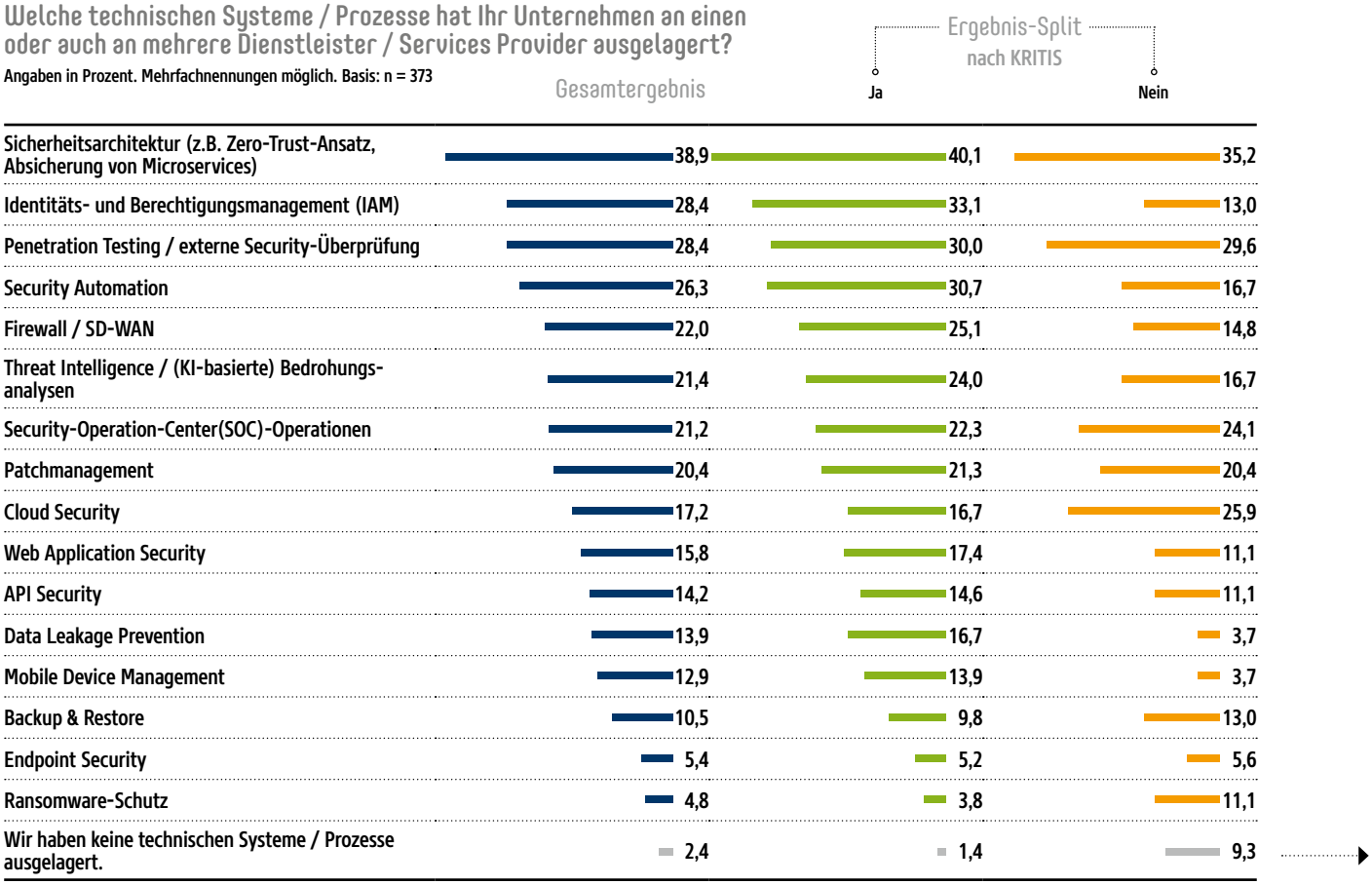
Für KRITIS-Betreiber ist diese Ergänzung der eigenen Security-Funktionen mit 14 Prozent der Nennungen weniger wichtig als im Nicht-KRITIS-Bereich mit 18 Prozent.

CIOs und IT-Leitungen ist dagegen die Angriffserkennung und Angriffsabwehr weitaus wichtiger als eine Unterstützung im Arbeitsalltag. So sehen 66 Prozent der CIOs Services für Detection and Response als den größten Mehrwert von Security Services, in den IT-Leitungen denken immer noch 62 Prozent so.

3

Welche technischen Systeme / Prozesse hat Ihr Unternehmen an einen oder auch an mehrere Dienstleister / Services Provider ausgelagert?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 373



Dienstleister überwachen Richtlinien und erstellen Sicherheitsarchitekturen

Fast vier von zehn Unternehmen nutzen Dienstleister für die Überwachung von Security Policies, die Implementierung von sicherheitsfördernden Prozessen sowie von technischen Systemen und Software. Die häufigste technische Aufgabe für Dienstleister ist der Aufbau einer Sicherheitsarchitektur wie Zero Trust.

Unterstützung beim Aufbau einer Sicherheitsarchitektur wie dem Zero-Trust-Modell oder der Absicherung von Microservices ist besonders gefragt – nahezu unabhängig von der Anzahl der Mitarbeiterinnen und Mitarbeiter im Unternehmen.

KRITIS-Betreiber nutzen diese Dienstleistung in 40 Prozent, andere Organisationen dagegen in 35 Prozent der Fälle. Noch deutlichere Unterschiede bei der Nutzung von Dienstleistungen im technischen Bereich gibt es bei Identity- und Access-Management-Lösungen: Hier greifen 33 Prozent der KRITIS-Betreiber zu, aber nur 13 Prozent der Nicht-KRITIS-Organisationen.

Umgekehrt ist es die Cloud-Sicherheit, bei der KRITIS-Betreiber nur in 17 Prozent der Fälle Dienstleister nutzen, während andere Organisationen dies zu 26 Prozent tun.

Dienstleistungen im Bereich Monitoring von Security Policies oder die Implementierung von Software sind bei KRITIS-Betreibern in 43 Prozent der Fälle im Einsatz (gegenüber anderen Unternehmen mit 28 bzw. 30 Prozent).

Die Analyse von Vorfällen ist mit 20 Prozent der Antworten weniger oft in den Händen von Dienstleistern. Ransomware-Schutz beziehen nur fünf Prozent von einem Dienstleister, obwohl die vielen Vorfälle auf einen höheren Bedarf an Unterstützung hindeuten.

3

Welche technischen Systeme / Prozesse hat Ihr Unternehmen an einen oder auch an mehrere Dienstleister / Services Provider ausgelagert?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 373

Ergebnis-Split nach Unternehmensgröße (Anzahl Beschäftigte)

	< 500	500 – 999	1.000 +
Sicherheitsarchitektur (z.B. Zero-Trust-Ansatz, Absicherung von Microservices)	38,8	38,5	39,2
Identitäts- und Berechtigungsmanagement (IAM)	28,1	30,8	27,0
Penetration Testing / externe Security-Überprüfung	22,3	35,6	28,4
Security Automation	25,6	29,8	24,3
Firewall / SD-WAN	19,0	29,8	18,9
Threat Intelligence / (KI-basierte) Bedrohungs-analysen	25,6	19,2	19,6
Security-Operation-Center(SOC)-Operationen	24,8	17,3	20,9
Patchmanagement	19,0	20,2	21,6
Cloud Security	11,6	17,3	21,6
Web Application Security	7,4	27,9	14,2
API Security	9,9	18,3	14,9
Data Leakage Prevention	14,9	15,4	12,2
Mobile Device Management	14,0	16,3	9,5
Backup & Restore	8,3	10,6	12,2
Endpoint Security	3,3	6,7	6,1
Ransomware-Schutz	0,8	7,7	6,1
Wir haben keine technischen Systeme / Prozesse ausgelagert.	4,1	1,9	1,4

Welche Security-Themen hat Ihr Unternehmen an einen oder auch an mehrere Dienstleister / Services Provider ausgelagert?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 373

Überwachung von Security Policies	39,1
Implementierung von sicherheitsfördernden Prozessen in einzelnen Abteilungen	39,1
Implementierung von technischen Systemen / Software	38,6
Evaluation von Security-Lösungen	32,2
Erstellung von Security Policies	31,1
Network Security	27,1
Analyse von Bedrohungen	23,1
Analyse von Angriffen / forensische Maßnahmen	20,4
Data Leakage Prevention	13,9
Andere IT-Security-Themen	0,5
Wir haben keine Security-Themen ausgelagert.	3,2
Weiß nicht	3,5

4

Mehr Scheinsicherheit als Sicherheit: Interne Sicht ist getrübt

73 Prozent der Unternehmen halten ihre Fähigkeiten zur Erkennung von Cyberrisiken und Cyberangriffen für „gut“ oder „sehr gut“, ebenso ihre Cyberabwehr. Gleichzeitig sagen 19 Prozent, dass sie nicht wissen, ob es einen Cybervorfall gegeben hat, oder sie können die Vorfälle nicht einordnen. Kam es zu einem Vorfall, erlitten 59 Prozent einen nennenswerten Schaden.

Die Mehrheit der Unternehmen hält sich in allen abgefragten Security-Bereichen für „gut“ oder „sehr gut“ aufgestellt. Für die Erkennung von Cyberangriffen sagen dies 74 Prozent der großen Unternehmen mit mehr als 1.000 Beschäftigten, 77 Prozent der Unternehmen mit 500 bis 999 Beschäftigten und immer noch 69 Prozent der kleineren Unternehmen mit weniger als 500 Beschäftigten.

Unternehmen, die nach dem IT-Sicherheitsgesetz respektive der Verordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI-Gesetz) zu den Betreibern Kritischer Infrastrukturen gehören – fortan KRITIS-Betreiber genannt –, sind bei der Erkennung von Cyberattacken noch zuversichtlicher: Hier sagen 79 Prozent, sie wären darin „gut“ oder „sehr gut“, im Vergleich zu 60 Prozent bei Organisationen, die nicht selbst unter die KRITIS-Verordnung fallen.

Bemerkenswert ist, dass insbesondere der C-Level im IT-Bereich und die IT-Leitung sehr positiv über die eigenen Security-Fähigkeiten denken. Im Fall der Erkennung von Cyberattacken sind es jeweils 81 Prozent der Befragten. Weitaus weniger optimistisch sind die Fachbereiche mit einem Anteil von 50 Prozent der Antworten und die Geschäftsführung mit 66 Prozent.

Selbst nach einem erlittenen großen Schaden gehen immer noch 80 Prozent der betroffenen Unternehmen davon aus, dass ihre Erkennung und Abwehr von Cyberangriffen „gut“ oder „sehr gut“ sei. Verursacht werden die Schäden in erster Linie durch nachlässige Beschäftigte (37 Prozent) und finanziell getriebene Cyberattacken (35 Prozent).

Unternehmen, die nicht zu den KRITIS-Betreibern zählen, sagen sogar zu 19 Prozent, dass es keine Cybervorfälle gab. Diejenigen indes, bei denen ein Vorfall aufgetreten ist respektive entdeckt wurde, sagen nur noch zu sechs Prozent, sie hätten keinen Schaden erlitten.

Wie gut ist Ihr Unternehmen in den aufgeführten einzelnen IT-Security-Bereichen aufgestellt?

Angaben in Prozent. Abgefragt wurde auf einer Schulnotenskala, dargestellt sind die konsolidierten Werte für die Noten „Sehr gut“ und „Gut“.
Basis: n = 369

Gesamtergebnis

72,9

Ergebnis-Split nach ...

Unternehmensgröße (Anzahl Beschäftigte)

- 68,9 — < 500
- 76,7 — 500 – 999
- 73,5 — 1.000 +

Einordnung Infrastruktur

- 79,0 — KRITIS-Betreiber
- 60,4 — Nicht-kritische Infrastruktur

Funktion im Unternehmen

- 65,7 — Geschäftsführung / Vorstand / COO / CFO
- 81,1 — CIO / IT-Vorstand / CDO / CTO / Technik-Vorstand / CSO / CISO
- 81,3 — IT-Leitung, IT-Security-Verantwortliche & IT-Admins
- 50,0 — Fachbereiche (z.B. HR, Einkauf)

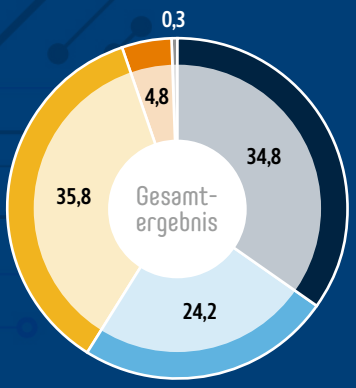
In welche der folgenden vorgegebenen Kategorien fallen die Cybervorfälle, mit denen Ihr Unternehmen in den letzten zwei Jahren konfrontiert war?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 373

Risikopotenzial durch Nachlässigkeit interner Mitarbeitender	36,7
Finanziell getriebene Cyberangriffe (z.B. Ransomware, Crypto-Mining)	35,1
Zugriff auf Daten durch staatliche Geheimdienste	25,5
Angriffe aus der Supply Chain / von Partnern	21,2
Industriespionage	20,1
Angriffe auf die Supply Chain	19,6
Datendiebstahl / Sabotage durch eigene (ehemalige) Mitarbeitende	19,3
Diebstahl digitaler Identitäten / Diebstahl von Zugangsdaten	10,5
Es gab Cybervorfälle, ich kann sie jedoch nicht zuordnen.	16,4
Es gab keine Cybervorfälle	8,8
Weiß nicht, ob es Cybervorfälle gab	2,7

Gab es einen nennenswerten Schaden durch die Cybervorfälle?

Angaben in Prozent. Filter: Unternehmen, in denen es in den vergangenen zwei Jahren einen Cybervorfall gab.
Basis: n = 330



- Ja, es gab einen essenziell großen Schaden
- Ja, es gab einen großen Schaden
- Nein, der Schaden hielt sich noch im Rahmen
- Nein, kein Schaden
- Weiß nicht

Radware 360 Cloud-Anwendungsschutz

Sichern Sie Ihre Apps, gewinnen Sie die Kontrolle zurück, aktivieren Sie Ihr Unternehmen

Radware ist ein führender Anbieter von Sicherheitslösungen für Unternehmen jeder Größe. Das Unternehmen ist spezialisiert auf DDoS-Schutz, Cloud Application Protection, Bot Protection, API Management und Application Delivery. Radware wurde von führenden Analystenfirmen wie IDC, Forrester, Gartner und anderen als Branchenführer anerkannt und hat mehrere Auszeichnungen erhalten, darunter „Leader in DDoS Protection“, „Leader in ADC and Application Delivery“, „Leader in Bot Protection“ und „Visionary in WAF Security“. Mit einem Kundenstamm, der einige der größten Unternehmen der Welt umfasst, und strategischen Partnerschaften mit Branchenführern wie Cisco, Check Point, AWS, Microsoft Azure und Nokia ist Radware bestens gerüstet, um Ihr Unternehmen vor verschiedenen Cyber-Bedrohungen zu schützen. Wenn Sie mehr über die Produkte und Dienstleistungen von Radware erfahren möchten, besuchen Sie unsere Website **https://de.radware.com**

Studiensteckbrief

Herausgeber ..... CIO, CSO und COMPUTERWOCHE

Studienpartner ..... Radware GmbH

Grundgesamtheiten ..... Oberste (IT-)Verantwortliche in Unternehmen der DACH-Region: Beteiligte an strategischen (IT-)Entscheidungsprozessen im C-Level-Bereich und in den Fachbereichen (LoBs); Entscheidungsbefugte sowie Experten und Expertinnen aus dem IT-(Security)-Bereich

Teilnehmergenerierung ..... Persönliche E-Mail-Einladung über die exklusive Unternehmensdatenbank von CIO, CSO und COMPUTERWOCHE sowie – zur Erfüllung von Quotenvorgaben – über externe Online-Access-Panels

Gesamtstichprobe ..... 373 abgeschlossene und qualifizierte Interviews

Untersuchungszeitraum ..... 23. bis 30. Mai 2023

Methode ..... Online-Umfrage (CAWI)

Fragebogenentwicklung und Durchführung ..... Custom Research Team von CIO, CSO und COMPUTERWOCHE in Abstimmung mit den Studienpartnern

---

Impressum

Studienkonzept / Fragebogenentwicklung:
Simon Hülsbömer,
Matthias Teichmann

Endredaktion / CvD Studienberichtsband:
Armin Rozsa,
Matthias Teichmann

Analysen / Kommentierungen:
Oliver Schonschek, Bad Ems

Hosting / Koordination Feldarbeit:
Armin Rozsa

Studienpartner:

Radware GmbH
Robert-Bosch-Str.
11a – 2nd floor
63225 Langen
Telefon: +49-6103-70657-0
E-Mail: info_de@radware.com
Website: https://de.radware.com

Artdirector & Grafik:
Daniela Petrini, Reutte

Umschlaggestaltung unter Verwendung eines Farbfotos von © freepik.com/slidesgo

Lektorat:
Elke Reinhold, München

Ansprechpartner:
Matthias Teichmann
matthias.teichmann@foundryco.com

Herausgeber:

Foundry
(formerly IDG Communications)

Anschrift:
IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 München
Telefon: +49 89 36086 0
Fax: +49 89 36086 118

Vertretungsberechtigter:
Jonas Triebel, Geschäftsführer

Registergericht:
Amtsgericht München, HRB 99110

Umsatzsteueridentifikationsnummer:
DE 811 257 834

Weitere Informationen unter:
www.foundryco.com