eco IT-SICHERHEITSUMFRAGE 2023

VERBAND DER INTERNETWIRTSCHAFT

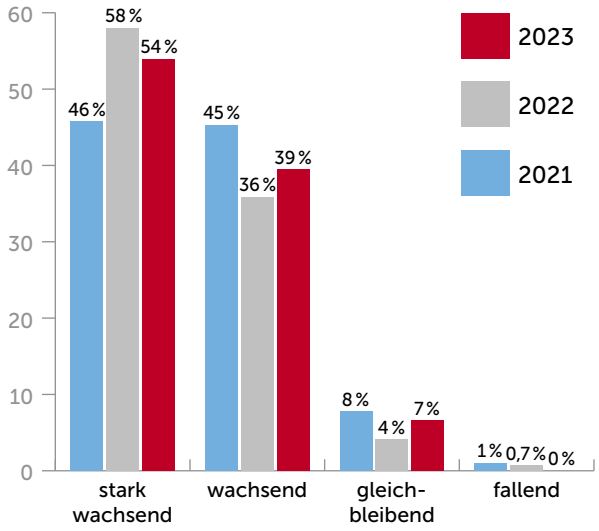
Inhalt

Bereits seit 2014 begleitet Oliver Dehning als Leiter die Kompetenzgruppe Sicherheit des eco – Verbands der Internetwirtschaft e.V.

Einleitung

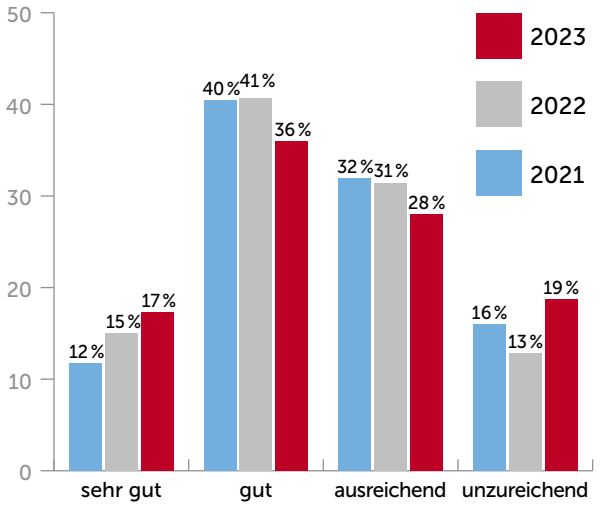
Die eco Kompetenzgruppe Sicherheit hat mit der IT-Sicherheitsumfrage 2023 eine umfassende Analyse der IT-Sicherheit in Deutschland veröffentlicht. Die Kompetenzgruppe beschäftigt sich seit über zehn Jahren mit der Sicherheit von (IT-)Infrastrukturen der Internetwirtschaft. Im Zentrum stehen Fragen zur personellen und organisatorischen Sicherheit, zum Schutz von IT-Systemen (Server & Netzwerke), der Sicherheit mobiler Kommunikationstechnik (Tablets, Smartphones, WLAN) bis hin zu Fragen des Sicherheitsmanagements und der Mitarbeitersensibilisierung. Die jährliche Umfrage geht stets auch auf aktuelle Themen ein und untersuchte beispielsweise die Auswirkungen der Corona-Pandemie und des Ukraine-Krieges auf die IT-Sicherheitslage. Der Zeitraum für die Erhebung der Daten der IT-Sicherheitsumfrage 2023 lag im Jahr 2022 von September bis Dezember. Befragt wurden über 100 Expert:innen für IT-Sicherheit im Rahmen von Online- und Live-Events.

ABB. 1 Einschätzung der Bedrohungslage bei der Internet-Sicherheit



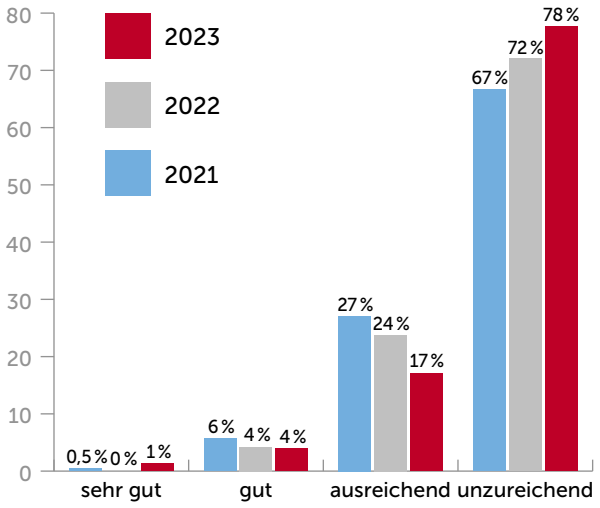
Quelle: eco e.V.

ABB. 2 Absicherung meines Unternehmens gegen Cybercrime



Quelle: eco e.V.

ABB. 3 Schutz der deutschen Wirtschaft gegen Cybercrime



Quelle: eco e.V.

Allgemeine Lage

Auch im Jahr 2022 schätzen mehr als 90 % der befragten IT-Expert:innen die allgemeine Bedrohungslage als hoch, beziehungsweise als sehr hoch ein. Nur etwa 7 % der Befragten gehen von einer gleichbleibenden Bedrohungslage aus. Von einer sinkenden Bedrohungslage geht Ende 2022 niemand mehr aus.

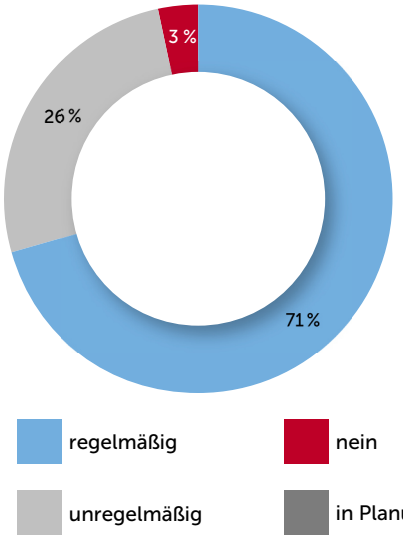
Dabei sagen viele Expert:innen, dass ihr eigenes Unternehmen im Kampf gegen Cybervorfälle erheblich besser aufgestellt ist als die deutsche Wirtschaft im Allgemeinen. Beurteilten im Jahr 2020 noch runde 12 % der Befragten ihr Unternehmen als „sehr gut" im Kampf gegen Cybercrime aufgestellt, so sind es Ende 2022 bereits über 17 %, die ihr Unternehmen als optimal gewappnet ansehen. Ein Großteil der Befragten stimmt der Aussage zu, die deutsche Wirtschaft sei IT-sicherheitstechnisch insgesamt unzureichend aufgestellt. Die Beurteilung der Lage hat sich über die Jahre sogar verschärft. Beurteilten im Jahr 2021 noch 66 % die Bemühungen der Wirtschaft als „unzureichend", so sind es Ende 2022 schon 77 % der befragten Expert:innen, die zu diesem düsteren Ergebnis kommen.

Bedrohungslage wird noch immer unterschätzt

„Die Diskrepanz bei der Beurteilung der eigenen Sicherheitslage und der Sicherheitslage in Deutschland allgemein zeigt, wie schwer es selbst Expert:innen fällt, die Bedrohung richtig einzuschätzen", sagt Oliver Dehning, Leiter der Kompetenzgruppe Sicherheit im eco – Verband der Internetwirtschaft e. V. „Grade viele Mittelständler stehen im Fokus international agierender Cybercrime-Netzwerke und sind sich dessen nicht bewusst."

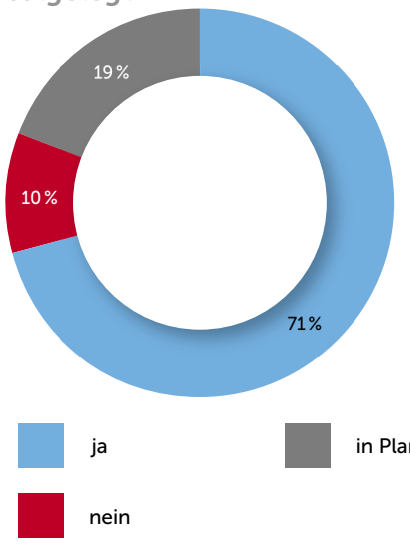
Die meisten Verantwortlichen suchen nach Wegen, sich auf einen Fall der Fälle vorzubereiten und ihre Mitarbeiter zu sensibilisieren.

ABB. 4 Schulen und sensibilisieren Sie Ihre Mitarbeiter zu Cybercrime?



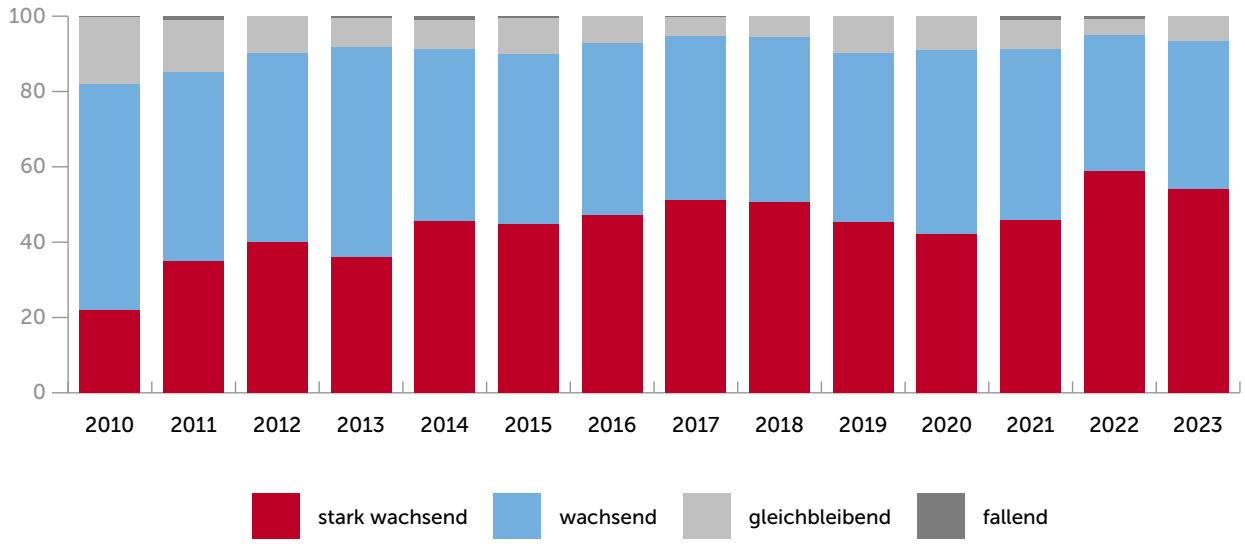
Quelle: eco e.V.

ABB. 4 Hat Ihr Unternehmen für den Fall eines Cybercrime-Vorfalls interne Prozesse bzw. einen Notfallplan festgelegt?



Quelle: eco e.V.

ABB. 6 Ich schätze die allgemeine Bedrohungslage bei der Internetsicherheit wie folgt ein



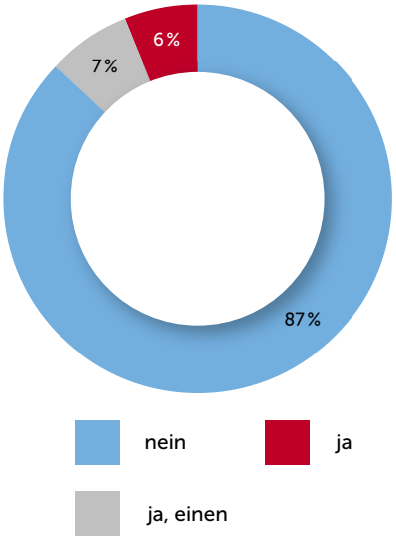
Quelle: eco e.V.

So geben 70 % der Teilnehmenden an, regelmäßige Mitarbeiterschulungen durchzuführen, nur 3 % sehen von dieser Maßnahme ab.

Neben kontinuierlichen Mitarbeiterschulungen zur Steigerung der Awareness im Bereich Sicherheit und Phishing gehört die Notfallplanung für die befragten Unternehmen aktuell zu den Top-Sicherheitsthemen. Mehr als 70 % haben definierte interne Prozesse, um einen Cyberangriff abzuwehren und bereits festgelegte Notfallpläne – fast 20 % planen dies für die Zukunft.

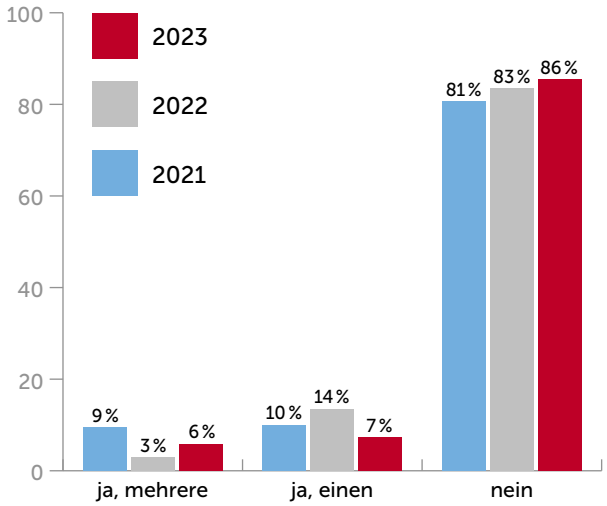
Betrachten wir die Antworten der Umfrageteilnehmer seit 2010, so sehen wir, dass die Bedrohungslage insgesamt als wachsend

ABB. 7 Sicherheitsvorfall im letzten Jahr?



Quelle: eco e.V.

ABB. 8 Gab es im letzten Jahr einen gravierenden Sicherheitsvorfall in Ihrem Unternehmen?



Quelle: eco e.V.

eingeschätzt wird. So steigerte sich die Einschätzung der Expert:innen, die 2010 die Bedrohungslage noch zu 22 % als „stark wachsend" und zu 60 % als „wachsend" eingestuft hatten über die Jahre: Zu 53 % „stark wachsend" respektive 39 % als „wachsend".

Trotz dieser Einschätzung gab es in der befragten Gruppe nur relativ wenige Cyber-Sicherheitsvorfälle. So gaben nur 13 % an, einen (7 %) oder mehrere (6 %) gravierende Sicherheitsvorfälle im letzten Jahr verzeichnet zu haben.

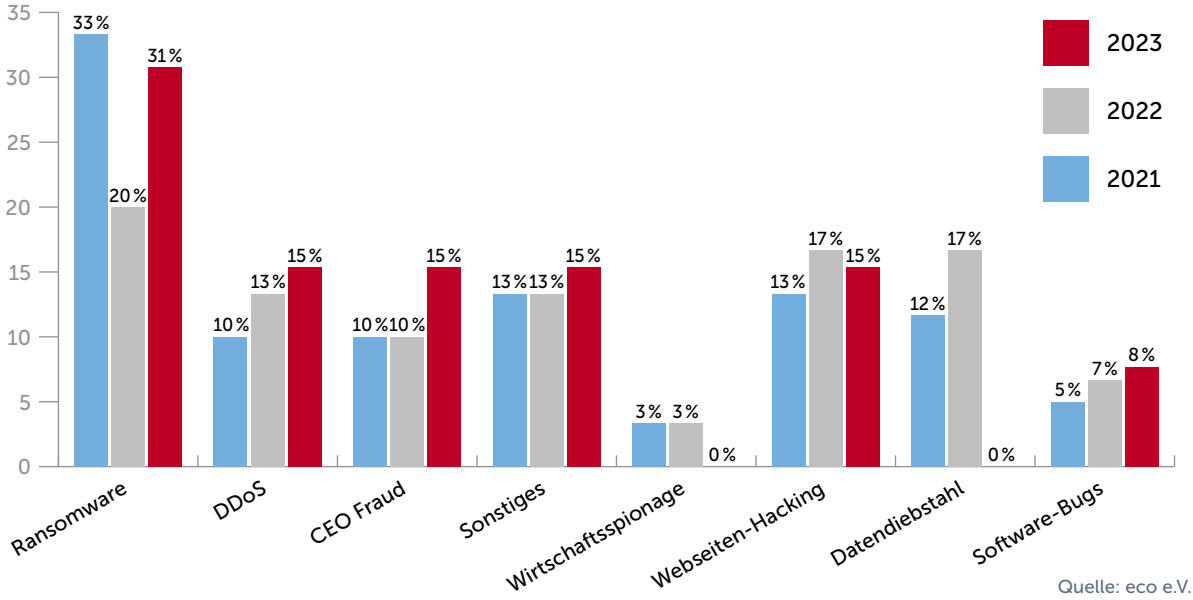
Im Vergleich zu den beiden vorhergehenden Jahren ist dies ein leicht rückläufiger Wert, wie die Abbildung 8 zeigt.

Am häufigsten kam bei Angriffen gegen Unternehmen Ransomware zum Einsatz, DDoS Angriffe und CEO Fraud halten sich mit rund 10 - 15 % der verzeichneten Angriffsarten im Mittelfeld der letzten drei Jahre. Ein wichtiges Thema ist und bleibt Datendiebstahl, auch wenn dies in der Umfrage 2023 nicht genannt wurde. Hier spielt eventuell das Thema „Ransomware" mit ein, da sich Ransomware-Angriffe nicht mehr nur mit einer Verschlüsselung von Systemen und Daten begnügen, sondern auch im Hintergrund unternehmenswichtige Daten kopieren und an die Kriminellen übermitteln, um weitere Erpressungen zu starten.

Die wirtschaftlichen Schäden eines Angriffs zu bewerten fällt schwer, meist sind die Antworten der Unternehmen in diesem Bereich sehr ausweichend oder bleiben völlig aus. Bei den von uns befragten Unternehmen kam es nach einem Angriff zu 90 % auch zu einem Schaden. In zwei von drei Fällen war der Schaden nur leicht, bei 22 % stellte sich der Schaden als erheblich für das Unternehmen dar.

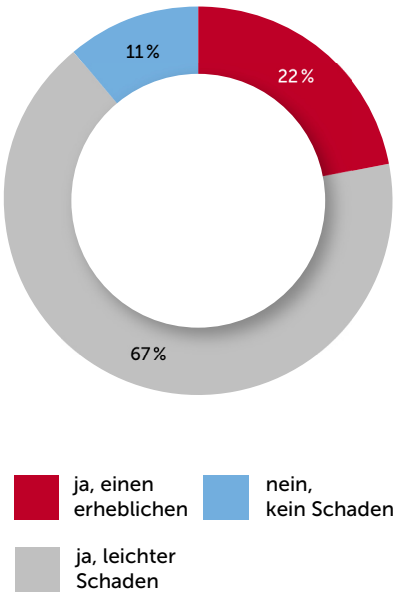
Die Hälfte der befragten Gruppe – überwiegend IT-affine Unternehmen – löste die Probleme im Zusammenhang mit Cyberangriffen intern. Externe Hilfe wurde nur in 10 % der Fälle in Anspruch genommen. Im Falle eines Cybercrime Vorfalls ist ein entschlossenes und schnelles Handeln erforderlich. Betroffene Unternehmen sollten nicht zögern, sich frühzeitig Hilfe von Spezialisten zu sichern und auch die Behörden zu informieren, die Sie unterstützen können.

ABB. 9 Angriffe im Bereich



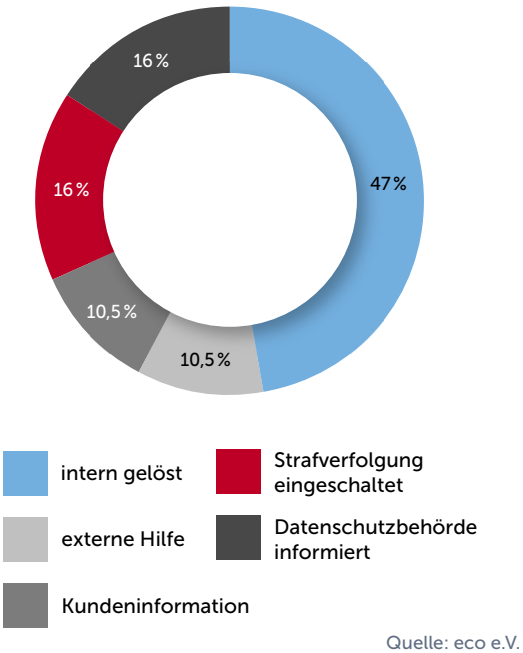
Quelle: eco e.V.

ABB. 10 Gab es einen wirtschaftlichen Schaden?



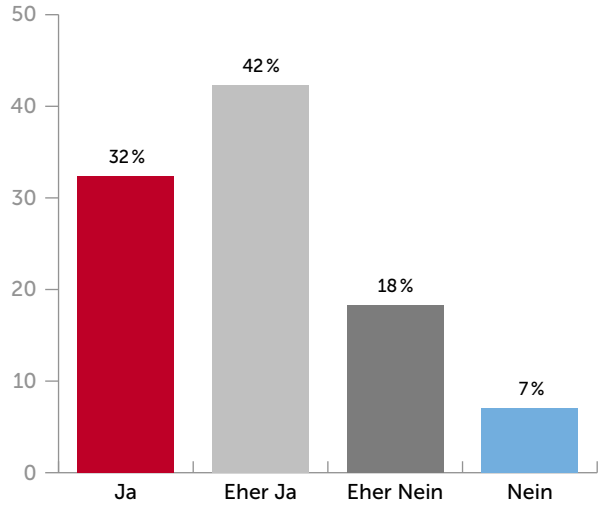
Quelle: eco e.V.

ABB. 11 Wie hat Ihr Unternehmen reagiert?



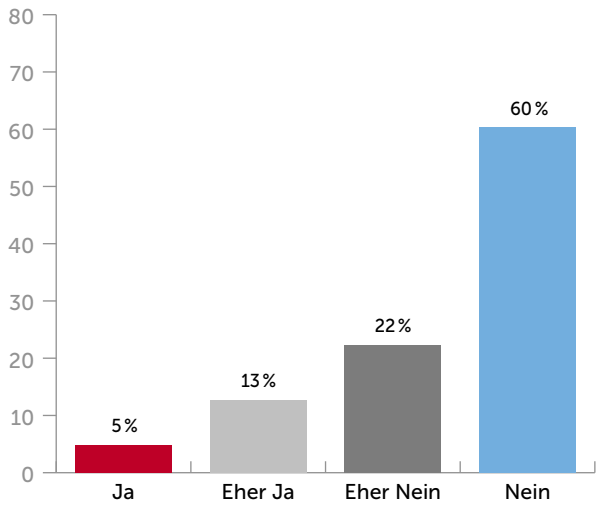
Quelle: eco e.V.

ABB. 12 Hat die Pandemie die Cyberbedrohungslage verschärft?



Quelle: eco e.V.

ABB. 13 Mehr Cyberangriffe durch Homeoffice?



Quelle: eco e.V.

Aktuelle Themen

Die abgefragten Themen der IT-Sicherheitsumfrage bleiben über die Jahre stabil, um eine Vergleichbarkeit zu gewährleisten. Allerdings nehmen die Studienautoren wichtige Ereignisse zum Anlass, um den Fragenkatalog zu erweitern und um den sich ändernden politischen und gesellschaftlichen Bedingungen gerecht zu werden.

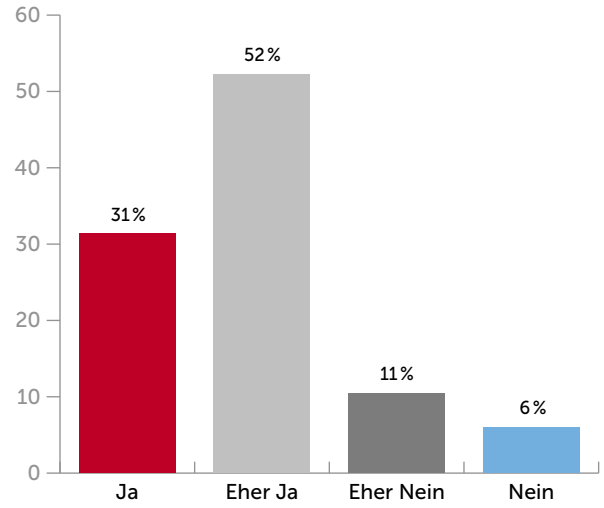
Ein solches einschneidendes Ereignis ist die Corona Pandemie, welche einen starken Wandel der Arbeitsmethoden zu Folge hatte. Präsenzarbeit wurde stark eingeschränkt und neue Möglichkeiten des mobilen Arbeitens getestet. Daraus entstanden neue Herausforderungen, die Systeme der Mitarbeiter auch im Home-Office und im mobilen Einsatz abzusichern.

Drei von vier (75 %) der befragten Unternehmen gab an, dass die Pandemie die Cyberbedrohungslage eindeutig verschärft hat. Nur rund jeder und jede Vierte ist der Ansicht, dass die Bedrohung sich pandemiebedingt nicht geändert hat.

Dem gegenüber sagt die Mehrzahl der Unternehmen, es sei durch den vermehrten Anteil von Home-Office und mobilem Arbeiten nicht zu erfolgreichen Cyberangriffen auf ihr Unternehmen gekommen.

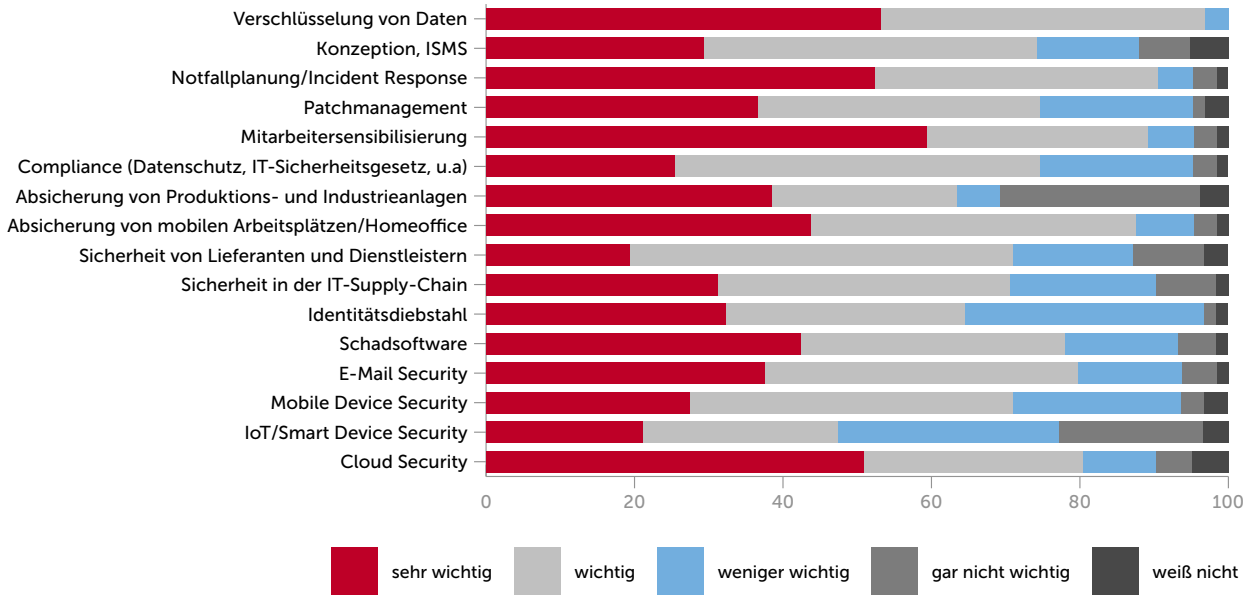
Die große Mehrheit der Experten denkt, dass der Angriffskrieg gegen die Ukraine die Bedrohungslage massiv verschärft hat. Rund 84 % der Befragten sehen eine Verschärfung der Lage, hier herrscht eine große Unsicherheit vor staatlich gesteuerten Ransomware Gruppen.

ABB. 14 Hat der Krieg gegen die Ukraine die Bedrohungslage verschärft?



Quelle: eco e.V.

ABB. 15 Sicherheitsthemen 2023



Quelle: eco e.V.

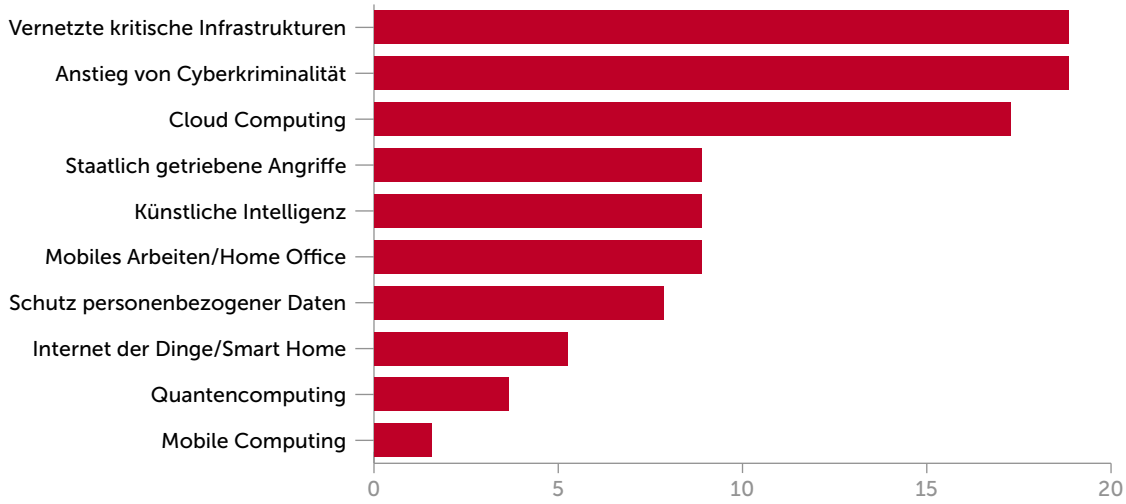
Sicherheitsthemen 2022

Mitarbeitersensibilisierung und Notfallplanung belegen die Spitzenplätze in den Sicherheitsthemen der Umfrage zur IT-Sicherheit 2023. Dicht gefolgt vom Thema Cloud-Security und Verschlüsselung von Daten. Dies spiegelt sich auch in den Antworten auf die Frage „Was sind die Treiber für Veränderungen in der IT-Sicherheit im Jahr 2022/2023" wider.

Der Anstieg von Cyberkriminalität, besonders im Bereich Ransomware und CEO Fraud (vgl. Abbildung 9) und die immer stärkere Vernetzung kritischer Infrastrukturen bilden den Antrieb für Veränderungen im Bereich der Cyber-Sicherheitsbemühungen.

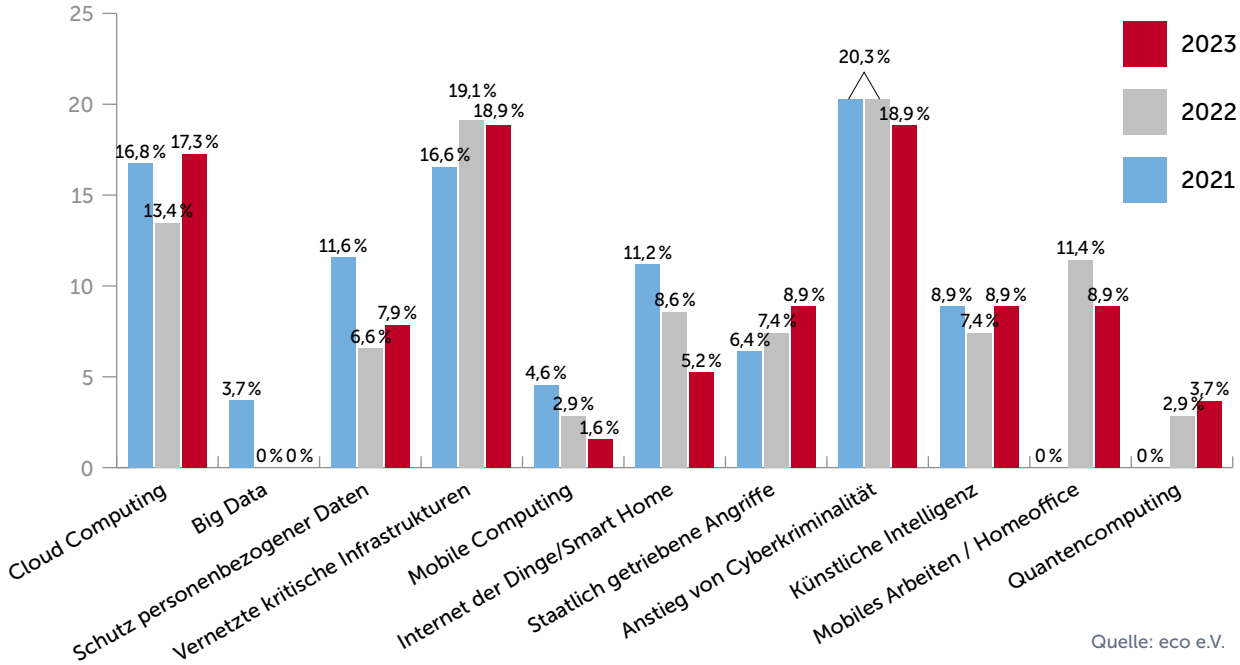
Auch der Schutz der Mitarbeiter beim mobilen Arbeiten und im Home-Office wurde im Laufe der Jahre immer wichtiger, hier sehen sich die befragten Unternehmen sicherheitstechnisch bereits auf einem hohen Niveau.

ABB. 16 Treiber für Veränderungen in der IT-Sicherheit



Quelle: eco e.V.

ABB. 17 Treiber für Veränderungen, 2021 bis 2023



Quelle: eco e.V.

Insgesamt zeigt die Studie: Die IT-Sicherheitslage bleibt weiterhin angespannt. Organisierte Cyberkriminalität, aber auch staatliche Akteure nutzen den Cyberraum immer häufiger gezielt für Angriffe auf Unternehmen, sowie auf öffentliche Infrastrukturen. Nie war es daher wichtiger, Cybersicherheit jederzeit mitzudenken. Cybersicherheit sollte Chefsache sein und bei allen unternehmerischen Entscheidungen mitgedacht werden.

Ihre Ansprechpartner bei eco zum Thema Security:

Markus Schaffrin

Geschäftsbereichsleiter Mitglieder Services
eco - Verband der Internetwirtschaft e.V.
Büro Köln
Lichtstraße 43h
50825 Köln
Telefon:+49 (221) 7000 48 – 170
E-Mail: markus.schaffrin@eco.de

Michael Weirich

Projekt Manager IT-Sicherheit
eco - Verband der Internetwirtschaft e.V.
Büro Köln
Lichtstraße 43h
50825 Köln
Telefon:+49 (221) 7000 48 – 193
Mobil: +49(0)171 – 554 0303
E-Mail: michael.weirich@eco.de

Fabian Landa

Junior Projektmanager Digitalisierung & Cybersecurity
eco - Verband der Internetwirtschaft e.V.
Büro Köln
Lichtstraße 43h
50825 Köln
Telefon: +49 (221) 700 048 - 295
Mobil: +49(0)151 – 2382 7038
E-Mail: fabian.landa@eco.de

eco IT-SICHERHEITSUMFRAGE 2023

eco –Verband der Internetwirtschaft e.V.
Lichtstraße 43h, 50825 Köln
fon +49(0)221/700048-0
fax +49(0)221/700048-111
info@eco.de
www.eco.de

VERBAND DER INTERNETWIRTSCHAFT