



Cybersicherheit in Unternehmen – Deutschland –

Unternehmerkunden-Studie 2022

Agenda und Rahmenbedingungen der Studie



ZIEL UND INHALT:

Cybersicherheit ist ein Thema, was immer mehr Unternehmen beschäftigt. Überall, wo Menschen Computer, Smartphones oder andere IT-Geräte benutzen, können Cyberattacken stattfinden.

Ziel dieser Studie ist es, Erkenntnisse darüber zu gewinnen, wie kleine und mittelständische Unternehmen mit dem Thema Cyberkriminalität umgehen.



TEILNEHMER:

Befragt wurden Unternehmen mit einem Jahresumsatz von bis zu 15 Millionen Euro – sowohl Commerzbank-Kunden als auch Kunden anderer Banken. Dazu zählen Freiberufler, Selbständige, Handwerker sowie kleinere und mittelständische Unternehmen.



UMFANG UND AUSWERTUNG:

Bundesweit wurden rund 2.500 Interviews mit Unternehmern* in einzelnen Regionen durchgeführt, davon **300 repräsentativ in Deutschland**.

Basierend auf einer Zufallsstichprobe ist die Befragung repräsentativ für die Region und wurde telefonisch vom Meinungsforschungsinstitut Ipsos durchgeführt.



ZEITRAUM:

Die Befragung fand zwischen dem 18. Juli und 10. August 2022 statt.

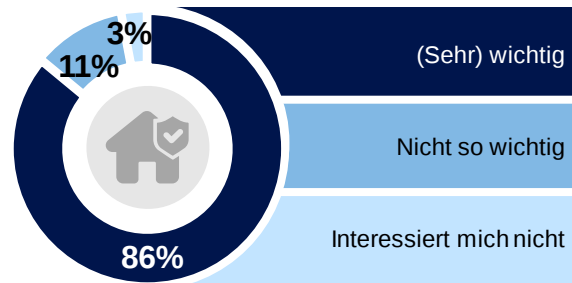
*) Mit dem Begriff Unternehmer sind in diesem Bericht Unternehmer m/w/d gemeint.



Unternehmen in Deutschland halten Cybersicherheit für äußerst wichtig und fühlen sich (sehr) gut aufgestellt

CYBERSICHERHEIT IST FÜR MEIN UNTERNEHMEN ...

DEUTSCHLAND



WIR SIND BEIM THEMA CYBERSICHERHEIT (SEHR) GUT AUFGESTELLT ...

91% → **ja**



Fragen: Wenn Sie jetzt einmal an Ihr Unternehmen denken, wie wichtig ist Ihnen das Thema Cybersicherheit? / Fühlen Sie sich mit Ihrem Unternehmen bei dem Thema Cybersicherheit gut aufgestellt? / Abweichungen zu 100%: Weiß nicht und k. A.



- > Für **86 Prozent** der Unternehmen in Deutschland ist das Thema **Cybersicherheit von großer Bedeutung**.
- > Gleichzeitig fühlen sich **91 Prozent** der Unternehmer in diesem Bereich **sehr gut bzw. gut aufgestellt**.
- > Lediglich **14 Prozent** halten das Thema **Cybersicherheit** für **irrelevant**.



Cybersicherheit ist bei mehr als der Hälfte der Unternehmen Chefsache

HAUPTSÄCHLICH ZUSTÄNDIG FÜR CYBERSICHERHEIT ...

DEUTSCHLAND



Frage: Wer in Ihrem Unternehmen ist für das Thema Cybersicherheit hauptsächlich zuständig? / Abweichungen zu 100%: Weiß nicht und k. A.



- > Beim Thema Cybersicherheit liegt die Verantwortung bei **54 Prozent** der Unternehmen in Deutschland hauptsächlich bei der **Geschäftsführung**.
- > **Knapp ein Fünftel** der Unternehmen in Deutschland nutzt vor allem die Kompetenz der **eigenen IT-Experten**.
- > **14 Prozent** greifen überwiegend auf **externe Mitarbeiter** zurück.

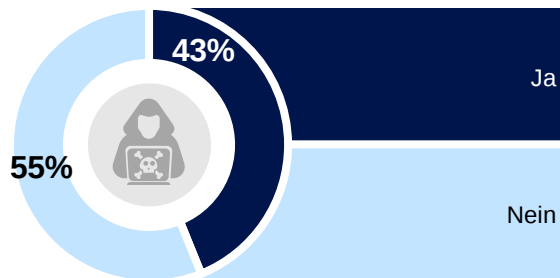


EIGENE ERFAHRUNGEN MIT CYBERKRIMINALITÄT

Zwei von fünf Unternehmen in Deutschland wurden bereits Opfer eines Cyberangriffs

MEIN UNTERNEHMEN WURDE SCHON EINMAL ANGEGRIFFEN ...

DEUTSCHLAND



- > **43 Prozent** der Unternehmen in Deutschland wurden bereits Opfer eines Cyberangriffs.
- > **55 Prozent** der Unternehmen in Deutschland sind von Cyberkriminalität bisher **verschont** geblieben.



Frage: Ist Ihr Unternehmen schon einmal durch irgendeine Form von Cyberkriminalität angegriffen bzw. beeinträchtigt worden? / Abweichungen zu 100%: Weiß nicht und k. A. bzw. durch Rundungen



EIGENE ERFAHRUNGEN MIT CYBERKRIMINALITÄT

Drei von fünf betroffenen Unternehmen in Deutschland erhielten Phishing-Mails

FORMEN DER CYBERKRIMINALITÄT ...

DEUTSCHLAND

Datendiebstahl per gefälschter E-Mails (Phishing-Mails)	62%
Vertrauenserschleichung, um an sensible Daten zu kommen	34%
Identitätsdiebstahl (z.B. Diebstahl von Login-Daten, Passwörtern etc.)	20%
Cybererpressung / Zugriff auf eigene Daten gesperrt (Freigabe bei Lösegeld)	19%
Datendiebstahl durch Schadsoftware	18%
Datendiebstahl per SMS (Smishing)	12%
Umleitung von Zahlungsströmen auf Fremdkonten	11%
Datendiebstahl per Fernwartungssoftware	8%
Provozierte Serverüberlastung	6%
Datendiebstahl per QR-Code	5%



- > Bei **62 Prozent** der Unternehmen, die Opfer eines Cyberangriffs wurden, waren **Phishing-Mails** die Ursache.
- > Bei **einem Drittel** der Unternehmen haben Externe versucht, sich das Vertrauen von Mitarbeitern zu erschleichen, um an **sensible Daten** zu kommen.
- > Jeweils **ein Fünftel** der Unternehmen wurde mit einem **Identitätsdiebstahl** der Daten beraubt oder mit einer **Lösegeldforderung** konfrontiert.



Frage: Welche Form von Cyberkriminalität war es? (Mehrfachnennungen möglich)

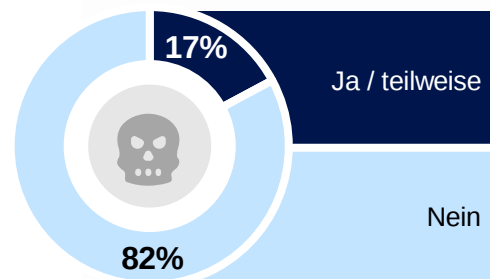


ENTSTANDENE SCHÄDEN

Die Cyberangriffe haben bei jedem sechsten betroffenen Unternehmen einen Schaden hinterlassen

MEINEM UNTERNEHMEN IST EIN SCHADEN ENTSTANDEN ...

DEUTSCHLAND



WENN JA / TEILWEISE, WAR DER SCHADEN FOLGENDER ART...



Finanzieller Schaden



Imageschaden / Vertrauensverlust



Verlust von Kundendaten



Verlust von Kunden



Firmenspionage



- > **17 Prozent** der Unternehmen in Deutschland, die bereits angegriffen wurden, beklagen **Schäden** durch Cyberkriminalität.
- > Die Folgen von Cyberattacken reichen von **finanziellen Schäden, Imageverlust, Verlust von Kundendaten und Kunden** bis hin zur **Firmenspionage**.



Fragen: Ist Ihrem Unternehmen dadurch irgendein Schaden entstanden? / Welche Art Schaden ist in Ihrem Unternehmen entstanden? (Mehrfachnennungen möglich) / Abweichungen zu 100%: Weiß nicht und k. A. bzw. durch Rundungen



ENTSTANDENE SCHÄDEN

Aufmerksame Mitarbeiter und Sicherheits-Software helfen entscheidend bei der Abwehr von Cyberangriffen

SCHADEN KONNTE ABGEWENDET WERDEN DURCH ...

DEUTSCHLAND



Frage: Durch wen oder was konnte der Angriff abgewehrt bzw. der Verlust ausgeglichen werden?
(Mehrfachnennungen möglich)



- > **Aufmerksame Geschäftsführer oder Mitarbeiter** konnten bei **knapp drei Viertel** der Unternehmen in Deutschland, die schon einmal einen Angriff abwehren konnten, einen Cyberangriff verhindern.
- > **Drei von fünf** Unternehmen haben den Schaden durch den Einsatz einer **Sicherheits-Software** abgewendet.
- > Bei **38 Prozent** dieser Unternehmen hat **die Aufmerksamkeit und das schnelle Handeln externer Dienstleister bzw. externer Mitarbeiter** den Schaden vereitelt.

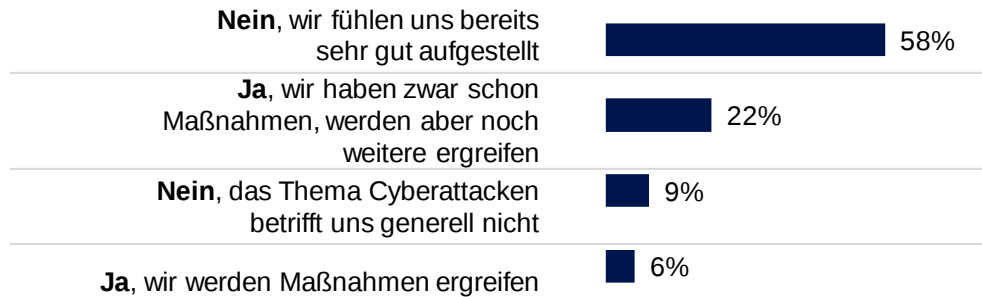


ZUKÜNFTIGE SCHUTZMAßNAHMEN

Unternehmen fühlen sich gegen Cyberangriffe gewappnet und planen keine weiteren Maßnahmen

WIR PLANEN MAßNAHMEN GEGEN CYBERANGRIFFE ...

DEUTSCHLAND



ZEITRAUM FÜR SCHUTZMAßNAHMEN GEGEN CYBERKRIMINALITÄT

Unternehmen, die (weitere) Schutzmaßnahmen ergreifen wollen

DEUTSCHLAND



■ innerhalb der nächsten 6 Monate ■ innerhalb des nächsten Jahres ■ Innerhalb der nächsten 3 Jahre oder später



- > **58 Prozent** aller Unternehmen in Deutschland fühlen sich gegen Cyberangriffe bereits **gut aufgestellt** und sehen **keine Notwendigkeit, weitere Maßnahmen zu ergreifen**.
- > **Gut ein Fünftel** hat **bereits Maßnahmen ergriffen**, will sich aber **künftig noch besser schützen**.
- > **42 Prozent** der Unternehmen, die **weitere Schutzmaßnahmen planen**, sehen diese für die **kommenden sechs Monate** vor.



Fragen: Planen Sie Maßnahmen im Unternehmen, um vor Cyberattacken geschützt zu sein? / In welchem Zeitraum möchten Sie diese Maßnahmen umsetzen? / Abweichungen zu 100%: Weiß nicht und k. A.

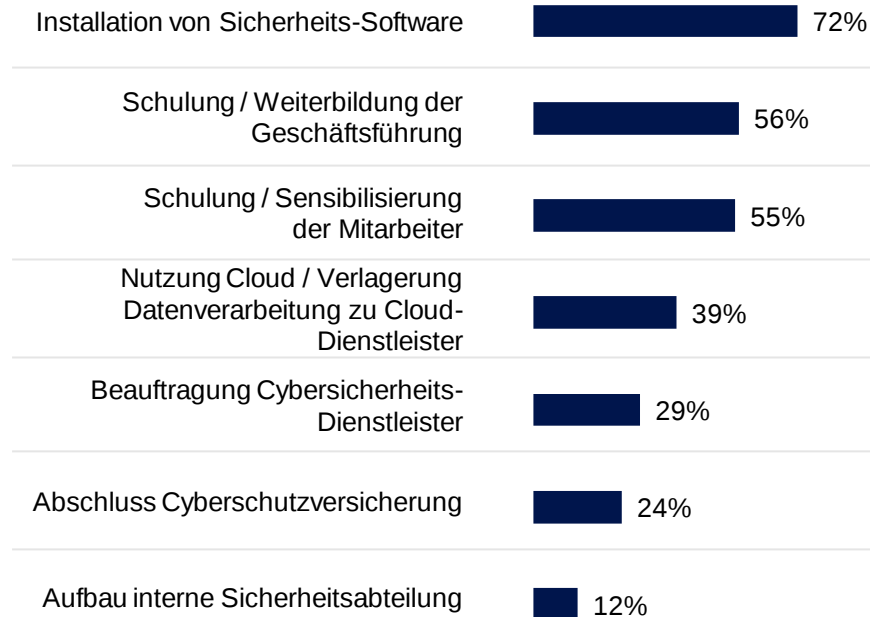


Sicherheits-Software und die eigene Weiterbildung bieten den besten Schutz

GEPLANTE BZW. INSTALLIERTE SCHUTZMAßNAHMEN ...

Unternehmen, die (weitere) Schutzmaßnahmen ergreifen (wollen)

DEUTSCHLAND



Frage: Welche Maßnahmen haben Sie bereits installiert bzw. welche Maßnahmen planen Sie für die Zukunft, um vor Cyberattacken geschützt zu sein? (Mehrfachnennungen möglich)



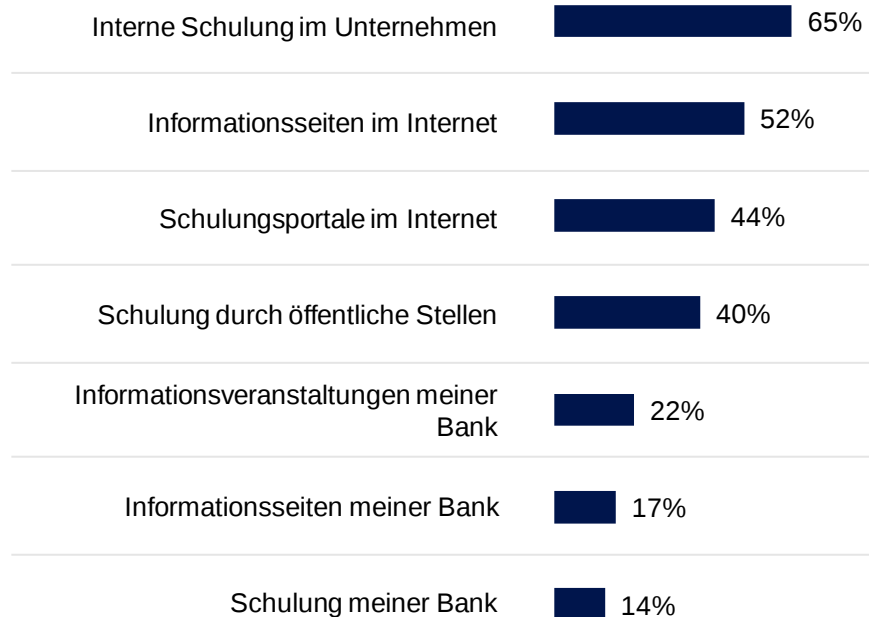
- > **72 Prozent** der Unternehmen vertrauen auf die **Installation von Sicherheits-Software**.
- > Daneben ist das Thema **Weiterbildung** der beste Schutz. In Deutschland setzen **56 Prozent** der Unternehmen auf die **Schulung und Weiterbildung der Geschäftsführung**.
- > **55 Prozent** der Unternehmen in Deutschland halten die **Schulung und Sensibilisierung der Mitarbeiter** für wichtig.



Unternehmen sensibilisieren Mitarbeiter primär durch interne Schulungen

SENSIBILISIERUNG DER MITARBEITER DURCH ...

DEUTSCHLAND



Frage: Welche Möglichkeiten nutzen Sie bzw. wollen Sie nutzen, um Ihre Mitarbeiter zum Thema Cybersicherheit zu sensibilisieren bzw. um sich selbst weiterzubilden? (Mehrfachnennungen möglich)



- > **Zwei Drittel** der Unternehmen mit Schulungsbedarf bieten bereits **interne Schulungen im eigenen Unternehmen** an oder planen, diese auszuweiten.
- > **Gut die Hälfte** der Unternehmen mit Schulungsbedarf informiert sich zum Thema Cybersicherheit im **Internet**.
- > **44 Prozent** der Unternehmen in Deutschland nutzen **Schulungsportale im Internet**.

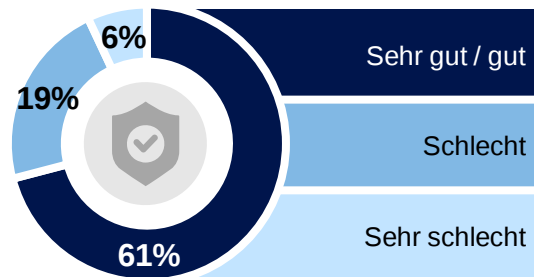


ZUKÜNFTIGE SCHUTZMAßNAHMEN

Drei von fünf Unternehmen fühlen sich von ihrer Bank zu Cybersicherheit sehr gut oder gut informiert

UNTERSTÜTZUNG DURCH DIE BANK BEIM THEMA CYBERSICHERHEIT

DEUTSCHLAND



> **61 Prozent** der Unternehmen in Deutschland fühlen sich von ihrer Bank **sehr gut bzw. gut unterstützt und informiert**.



Frage: Wie gut fühlen Sie sich durch Ihre Bank zum Thema Cybersicherheit unterstützt und informiert? / Abweichungen zu 100%: Weiß nicht und k. A.

Die wichtigsten Erkenntnisse im Überblick



BEDEUTUNG VON CYBERSICHERHEIT

- ▶ Unternehmen in Deutschland halten Cybersicherheit für äußerst wichtig und fühlen sich gleichzeitig (sehr) gut aufgestellt.
- ▶ Cybersicherheit ist bei mehr als der Hälfte der Unternehmen Chefsache.
- ▶ Auch die Kompetenz der eigenen IT-Experten sowie externe Mitarbeiter werden von Unternehmen in Deutschland genutzt.



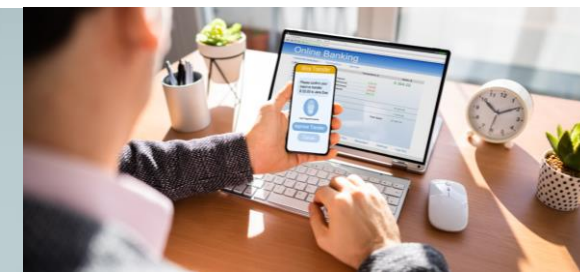
EIGENE ERFAHRUNGEN MIT CYBERKRIMINALITÄT

- ▶ Zwei von fünf Unternehmen in Deutschland wurden bereits Opfer eines Cyberangriffs.
- ▶ Drei von fünf betroffenen Unternehmen in Deutschland erhielten Phishing-Mails.
- ▶ Bei einem Drittel der Unternehmen haben Externe versucht, sich das Vertrauen von Mitarbeitern zu erschleichen, um an sensible Daten zu kommen.



ENTSTANDENE SCHÄDEN

- ▶ Die Cyberangriffe haben bei jedem sechsten betroffenen Unternehmen einen Schaden hinterlassen.
- ▶ Die Folgen reichen von finanziellen Schäden, Imageverlust, Verlust von Kundendaten und Kunden bis hin zur Firmenspionage.
- ▶ Aufmerksame Mitarbeiter und Sicherheits-Software helfen entscheidend bei der Abwehr von Cyberangriffen.



ZUKÜNFTIGE SCHUTZMAßNAHMEN

- ▶ Drei von fünf Unternehmen in Deutschland fühlen sich gegen Cyberangriffe gut gewappnet, knapp ein Fünftel plant noch weitere Schutzmaßnahmen.
- ▶ Sicherheits-Software und die Schulung der Geschäftsführung sowie der Mitarbeiter bieten den besten Schutz.
- ▶ Drei von fünf Unternehmen in Deutschland fühlen sich von ihrer Bank zu Cybersicherheit sehr gut oder gut informiert.



COMMERZBANK