GBB-Rating | JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN | Financial Accounting. | HEINRICH HEINE UNIVERSITÄT DÜSSELDORF

Cyber Security – Status quo und Herausforderungen

Ergebnisse GBB-Blitzumfrage, Februar 2019

Stefan Koll, Bernd Bretschneider | GBB-Rating Gesellschaft für Bonitätsbeurteilung mbH, Köln

Dr. Peter Kotzian, Prof. Dr. Barbara E. Weißenberger, Leonhard J. Lösse | Lehrstuhl für Betriebswirtschaftslehre, insbes. Accounting, Heinrich-Heine-Universität Düsseldorf

Prof. Dr. Corinna Ewelt-Knauer, Mohamed Amin Khaled | Lehrstuhl für Wirtschaftswissenschaften, insbes. Financial Accounting, Justus-Liebig-Universität Gießen

BUSINESS TALKS: MASTER THE LANGUAGE OF ACCOUNTING!
www.accounting.hhu.de

Cyber Security – Neue Herausforderungen

Im Zuge der digitalen Transformation verlagern sich immer mehr Geschäftsprozesse in den Online-Bereich. Gerade für Finanzdienstleister wurde das Thema Cyber Security zum neuen Aufgabenfeld und entwickelt sich zu einem wichtigen Erfolgsfaktor:

Wie gelingt es, Kommunikation mit Geschäftspartnern und Kunden sowie die Erbringung von Dienstleistungen und internen Prozessen gegen potentielle Risiken zu schützen, die aufgrund von Cyber-Kriminalität, d. h. von strafbarem Verhalten Dritter im Internet, entstehen?

Die hier vorgelegte Studie hat mittels einer Umfrage unter Finanzdienstleistern und Banken die aktuellen Einschätzungen zur Situation, den Herausforderungen und entstehenden Risiken, aber auch dem Umgang mit dem Thema Cyber-Security identifiziert.

Verwandte Themen aus früheren GBB-Blitzumfragen:
Chancen und Risiken von Big Data im digitalisierten Geschäftsumfeld | September 2017
Fintechs – Bedrohung oder Chance für die Geschäftsmodelle von Banken | April 2016
Die Banken und der digitale Strukturwandel | April 2014
(siehe auch https://www.gbb-rating.eu/de/presse/blitzumfrage/Seiten/default.aspx)

Cyber Security – Aktuelle Vorfälle und Entwicklungen vor dem Hintergrund der Umfrage

- **BaFin plant Cyber-Stresstests (2018):**
  Aus Sicht der BaFin kümmern sich deutsche Geldhäuser noch zu wenig um die IT-Sicherheitsrisiken. Die Aufsichtsbehörde will die IT-Sicherheitsvorkehrungen von Banken deshalb genauer prüfen. Gemeinsam mit der Deutschen Bundesbank wird an einer möglichen Implementierung von Cyber-Stresstests für den deutschen Finanzsektor gearbeitet. Insgesamt soll das Krisenmanagement verbessert werden.
- **EZB-Bankenaufsicht will IT-Risiken genauer prüfen (2018):**
  Die europäische Zentralbank warnt eindringlich vor den Folgen von Hackerangriffen im Finanzsektor und sieht die Möglichkeit, dass die nächste Finanzkrise durch eine Cyberattacke ausgelöst werden könnte. Derzeit seien die Verluste, die durch Hackerangriffe entstehen, meist kleiner als einzelne Kreditausfälle und würden deshalb häufig unterschätzt. Zukünftig könnten sie jedoch deutlich größere Schäden verursachen. Die EZB ist deshalb bestrebt die Banken hinsichtlich der bestehenden IT-Risiken zukünftig verstärkt zu prüfen.
- **Tiber-EU (2019) plant Cybertests:**
  Das European Framework for Threat Intelligence-based Ethical Red Teaming (Tiber-EU) der EZB soll Cybertests im Finanzwesen harmonisieren. Professionelle externe Dienstleister sollen die Hacks ausführen. Die Cybertests sollen von 2019 bis 2021 durchgeführt werden.
- **Cyberangriffe auf Politiker und Prominente (2019):**
  Der im Januar 2019 bekannt gewordene Hackerangriff auf Daten deutscher Politiker und Prominente zeigt, wie anfällig die digitale Gesellschaft ist und offenbart das steigende Bedrohungspotenzial. Die Bundesregierung wertete den Vorfall, im Rahmen dessen zahlreiche sensible Daten veröffentlicht wurden, als „schwerwiegenden Angriff“. Neben der Ankündigung eines neuen Frühwarnsystems zur Erkennung von Datenleaks wurde darüber hinaus die Bedeutung von Grundregeln im Rahmen der IT-Sicherheit unterstrichen (u. a. lange und komplexe Passwörter, zeitnahe Änderung von Passwörtern, Sicherung von Zugängen und Konten mittels Zwei-Faktor-Authentifizierung, Nutzung sicherer Messenger mit Ende-zu-Ende-Verschlüsselung).
- **Cyberangriffe auf den Bundestag (2018, 2015):**
  Massive Cyberangriffe auf das Datennetz des Bundestages wurden 2018 festgestellt. Bei dem Angriff auf den Bundestag 2015 hatten sich die Angreifer einen so weitreichenden Zugang verschafft, dass die Bundestags-IT ausgetauscht werden musste.

Hintergrund & Zielsetzung

Hintergrund

- Unter dem Begriff „Cyber Security“ werden sämtliche Aspekte der Sicherheit von Informationstechnik sowie darauf basierende Anwendungen, Prozesse, Kommunikation und verarbeitete Information subsumiert.
- Aufgrund der Digitalisierung und der zunehmenden Vernetzung von IT-Systemen wird nahezu jeder Bereich des unternehmerischen Handelns von digitalen Veränderungen berührt. Daraus resultieren jedoch erhöhte Sicherheitsrisiken und eine potentielle Bedrohung durch Cyberangriffe. Die Umsetzung von Maßnahmen, um den steigenden Anforderungen gerecht zu werden und eine angemessene IT-Sicherheit zu gewährleisten wird damit zum kritischen Erfolgsfaktor für die Unternehmen im Rahmen der Digitalisierung.
- Insbesondere Banken und Finanzdienstleister sind Cyber-Angriffen ausgesetzt. Angriffsziele können neben monetären Zielen auch Kundendaten sowie die Herbeiführung von Fehlfunktionen in Systemen sein. Bei Bekanntwerden entsprechender Angriffe ist damit oft ein erheblicher Reputationsschaden verbunden.

Zielsetzung

- Vor diesem Hintergrund bestand das Ziel der Umfrage darin, die Einschätzungen von Fach- und Führungskräften insbesondere im Banken- und Finanzdienstleistungssektor hinsichtlich des Status Quo von IT-Sicherheit, der vorhandenen Kompetenzen und verbundenen Herausforderungen zu erfassen. Ebenfalls wurden die bereitstehenden Ressourcen und Notfallmaßnahmen sowie die Entwicklung von Cyber-Vorfällen betrachtet.
- Hierzu wurde im Rahmen der Umfrage gemeinsam mit dem Lehrstuhl für Betriebswirtschaftslehre, insbesondere Accounting, an der Heinrich-Heine-Universität Düsseldorf und dem Lehrstuhl für Wirtschaftswissenschaften, insbesondere Financial Accounting an der Justus-Liebig-Universität Gießen ein strukturierter Online-Fragebogen entwickelt, der die relevanten Themenfelder zu Cyber Security adressiert.
- Die Ergebnisse dieser Umfrage erheben nicht den Anspruch repräsentativ zu sein. Sie werfen jedoch ein wichtiges Schlaglicht auf den Umgang mit Cyber Security und den damit einhergehenden Anforderungen.
- Wir bedanken uns bei allen Teilnehmern dieser Umfrage.

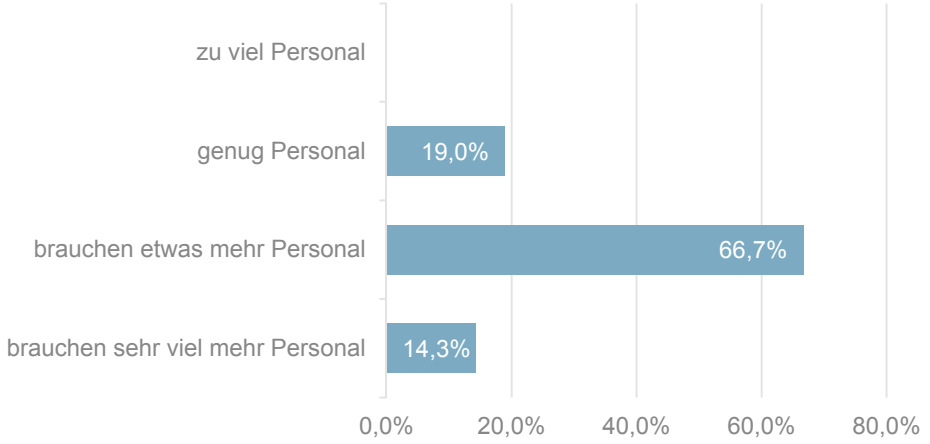
Kernergebnisse

1. Teilnehmer der Umfrage waren Fach- und Führungskräfte insbesondere aus dem Banken- und Finanzdienstleistungsbereich in Deutschland (Umfragedauer von März bis August 2018).
2. Kernthemen der Umfrage waren die Bereiche Ressourcen und Organisation von Cyber Security, Entwicklung und Art von Cyber-Kriminalitäts-Vorfällen sowie Maßnahmen im Rahmen von Cyber Security.
3. Hinsichtlich der personellen Ausstattung verfügen bislang nur wenige der befragten Unternehmen über ausreichende Kapazitäten in puncto Cyber Security. Der Ausbau der Kapazitäten soll primär durch Neueinstellungen sowie Fortbildung bestehender Mitarbeiter erfolgen.
4. Die Mehrheit der befragten Unternehmen verfügt bereits über Notfallpläne und führt Risikoanalysen für alle bzw. ausgewählte Geschäftsprozesse durch. Es verbleibt jedoch ein signifikanter Anteil der befragten Unternehmen, der über keine derartigen Risikovorsorgemaßnahmen verfügt und keine Notfallmechanismen implementiert hat.
5. Die Anzahl der IT-Sicherheitsvorfälle hat bei den befragten Unternehmen in 2017 tendenziell zugenommen. Die häufigsten Vorfälle waren Trickbetrug z. B. in Form von Fake-President-Attacken, Computersabotage (u. a. Datenverlust durch Ransomware) sowie der illegale Zugang Dritter auf Kundendaten durch Identitätsdiebstahl.
6. Als das größte Risiko, das sich aus Cyber-Angriffen ergibt, wird das Reputationsrisiko angesehen, noch vor dem Datenverlustrisiko.
7. Die größte Gefährdung für die Cyber Security wird in einem fahrlässigen Fehlverhalten der eigenen Mitarbeiter gesehen. Zusammen mit dem vom Kunden ausgehenden Risiko spielt der menschliche Faktor damit eine größere Rolle als gezielte Angriffe von außerhalb.
8. Automatisierte Sicherheitsupdates, Schulungen für Mitarbeiter und Mindestvorgaben für Passwörter werden als wichtige Maßnahmen zur Sicherstellung von Cyber Security eingeschätzt. Diese Maßnahmen greifen bekannte Probleme auf, die sich aus nachlässigem Verhalten von Mitarbeitern ergeben.
9. Die deutliche Mehrheit der Teilnehmer sieht durch den Eintritt neuer Wettbewerber in den Markt für digitale Finanzdienstleistungen (Fintechs) auch ein insgesamt höheres Anforderungsniveau an Cyber Security-Maßnahmen gegeben.

Status Quo: Ressourcen für IT-Sicherheit

Zur Sicherstellung von Cyber Security sind insbesondere IT-Experten von großer und weiter zunehmender Bedeutung.

Wie zufrieden sind Sie mit der personellen Ausstattung Ihres Unternehmens für die Aufgaben zur Sicherstellung von Cyber Security?

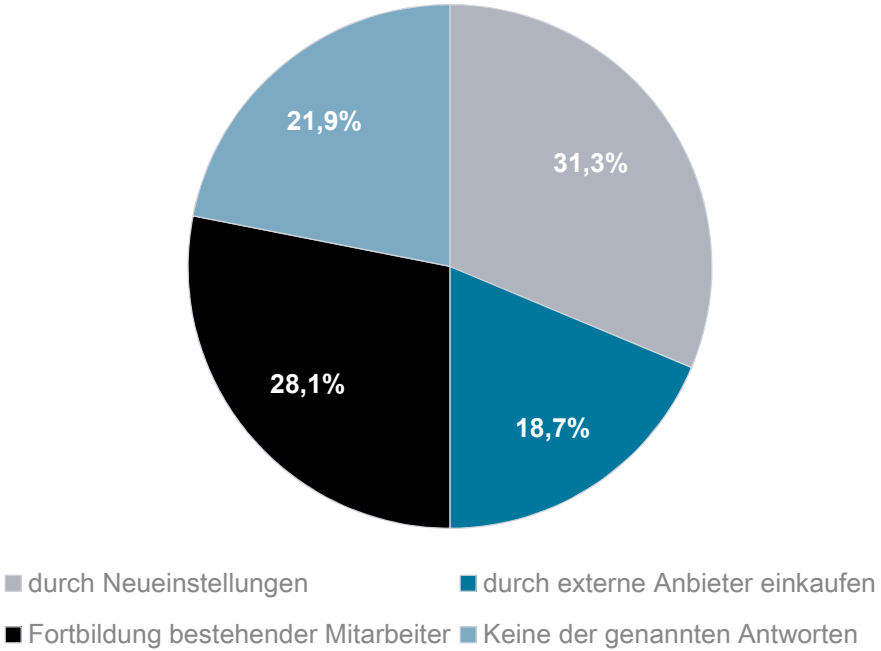


Angaben (oben und im Folgenden) in Prozent gültiger Fälle.

Bislang verfügen nur wenige Unternehmen über ausreichende personelle Kapazitäten in puncto Cyber Security.

Status Quo: Ressourcen für IT-Sicherheit

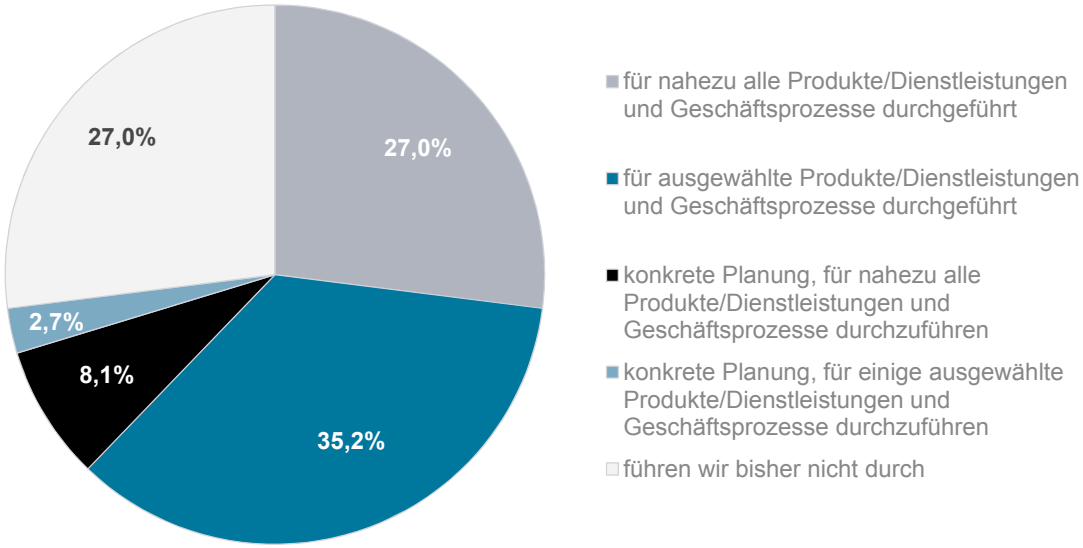
Ein Großteil der Unternehmen muss innerhalb der nächsten Jahre personelle Kapazitäten für Aufgaben zur Sicherstellung von Cyber Security ausbauen.
Nennen Sie die für Sie wichtigste Option.



Der Ausbau der personellen Kapazitäten soll primär durch Neueinstellungen sowie Fortbildung bestehender Mitarbeiter erfolgen. Der verbleibende Bedarf wird voraussichtlich durch externe Anbieter abgedeckt.

Organisation von Cyber Security

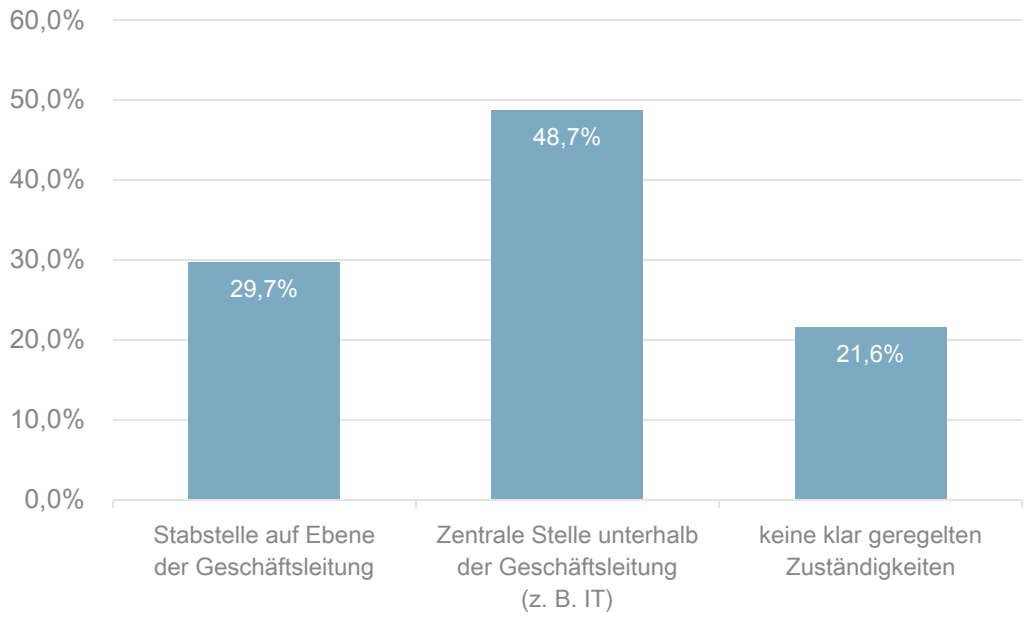
Sowohl Produkte und Dienstleistungen als auch Geschäftsprozesse unterliegen Cyber-Kriminalitätsrisiken (z. B. Fraud).
Führen Sie Risikoanalysen im Hinblick auf diese Risiken durch?



Mehrheitlich werden bei den Teilnehmern für alle bzw. ausgewählte Geschäfts-prozesse bereits jetzt Risikoanalysen durchgeführt. Immerhin rund ein Viertel führt dies für nahezu alle Produkte/Dienstleistungen und Prozesse durch. Es verbleibt jedoch ein Anteil von rund einem Viertel der Befragten, der noch keine solchen Risikoanalysen durchführt.

Organisation von Cyber Security

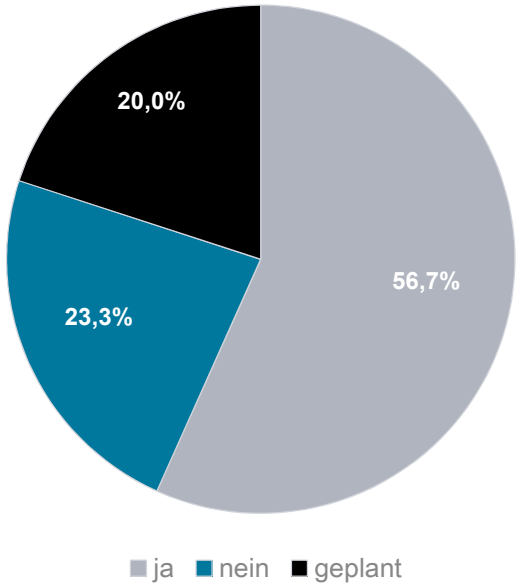
Im Umgang mit Cyber Security fällt eine Vielzahl von Aufgaben an.
Wie ist bei Ihnen der Umgang mit dem Thema Cyber Security organisiert?



In den meisten Unternehmen liegt die Verantwortung bei einer Stabsstelle oder einer zentralen Stelle unterhalb der Geschäftsleitung. Etwa ein Fünftel verfügt über keine klar geregelten Zuständigkeiten.

Organisation von Cyber Security

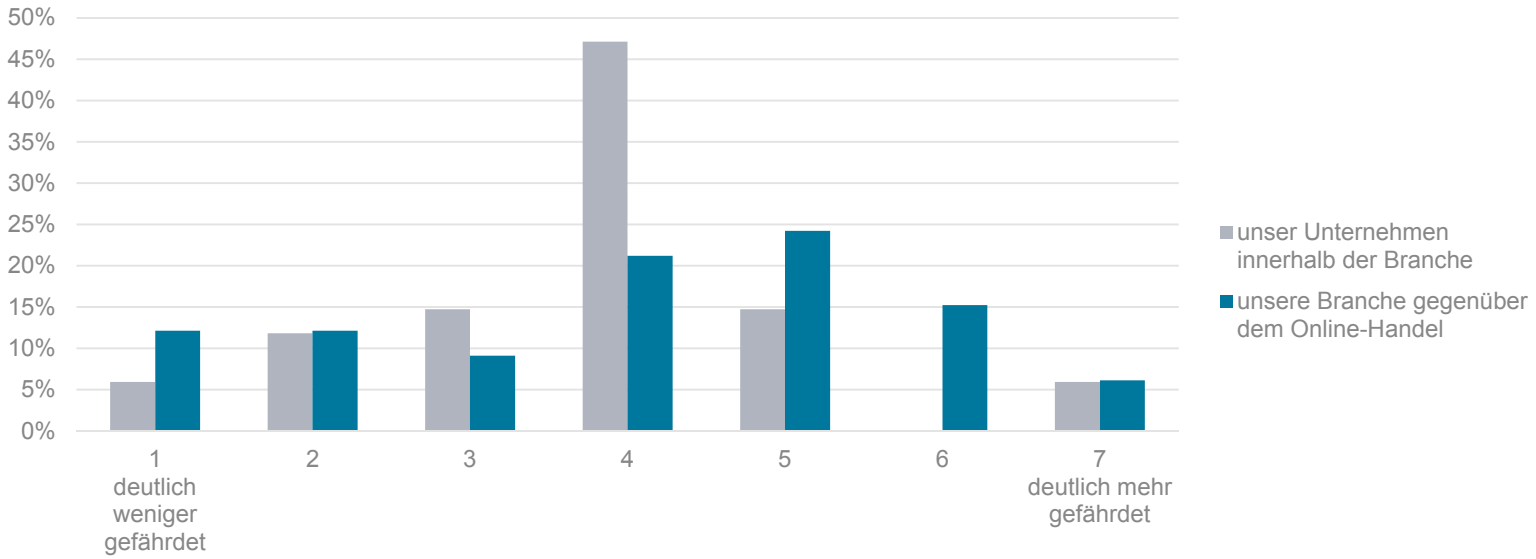
Cyber-Angriffe treten in der Regel ohne Vorwarnung auf und können Unternehmen völlig unerwartet treffen.
Gibt es in Ihrem Unternehmen einen Notfallplan für Cyber-Angriffe?



Die Mehrheit der befragten Unternehmen verfügt bereits über Notfallpläne, andere planen diese noch, ein hoher Anteil von Unternehmen ist für derartige Notfälle jedoch noch unvorbereitet.

Vorfälle von Cyber-Kriminalität

Für wie gefährdet halten Sie Ihr Unternehmen mit Blick auf Cyber-Kriminalität innerhalb Ihrer Branche? Wie schätzen Sie die Gefährdung Ihrer Branche durch Cyber-Kriminalität gegenüber dem Online-Handel ein?

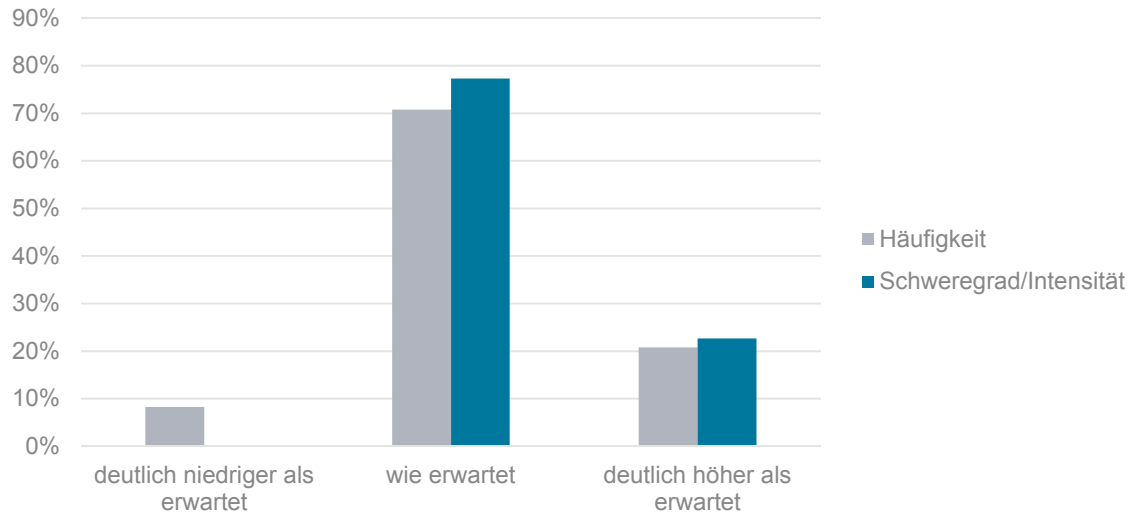


Verglichen mit Wettbewerbern aus der eigenen Branche sehen die befragten Unternehmen sich nicht deutlich gefährdeter oder weniger gefährdet. Verglichen mit Unternehmen aus dem Online-Handel wird die Gefährdung etwas höher gesehen.

Vorfälle von Cyber-Kriminalität

Unternehmen können immer wieder Ziel externer Angriffe aus dem Internet auf Informationstechnologien werden bzw. andere Probleme durch Cyber-Kriminalität erleben.

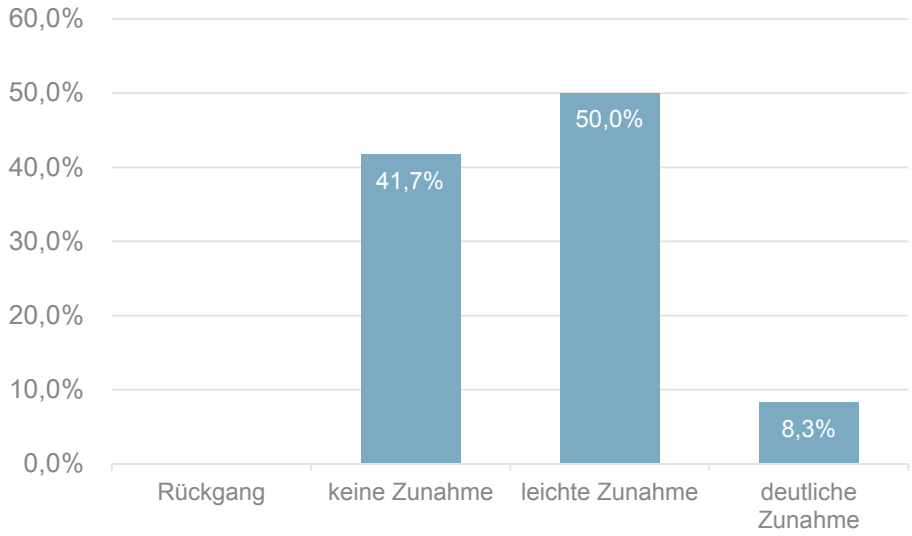
Wie beurteilen Sie die Häufigkeit bzw. den Schweregrad und die Intensität im letzten Jahr?



Der größte Teil der Befragten hat sowohl mit der tatsächlichen Anzahl von Problemen als auch deren Schweregrad bereits gerechnet. Etwa jedes fünfte Unternehmen hat einen oder beide Faktoren allerdings unterschätzt.

Vorfälle von Cyber-Kriminalität

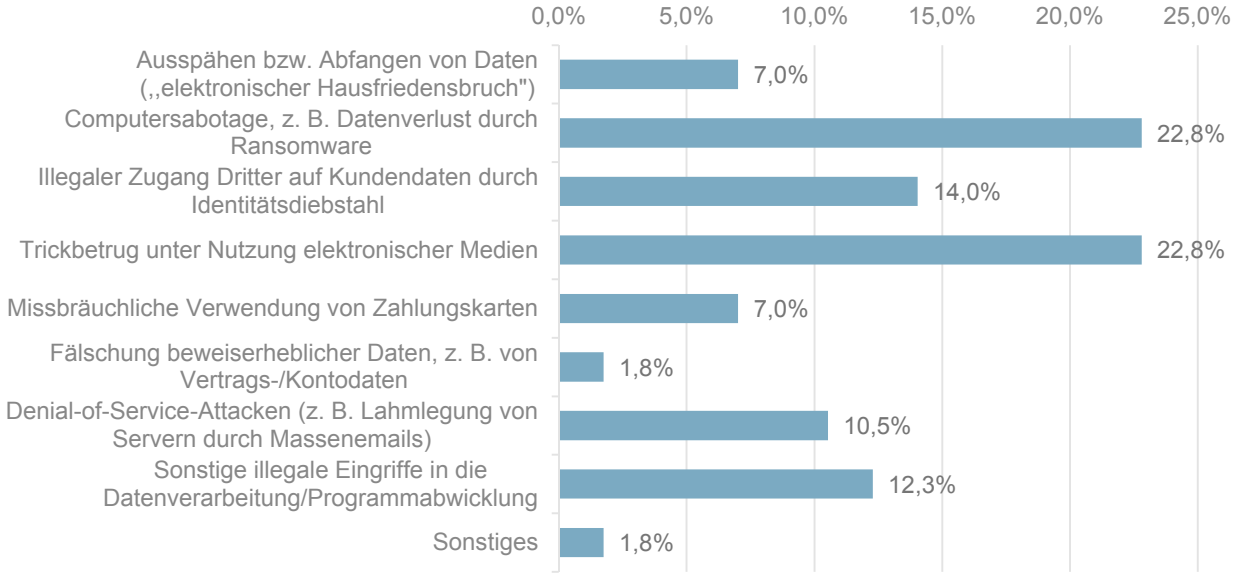
Haben Sie in Ihrem Unternehmen im Jahr 2017 einen Anstieg bei der Anzahl der IT-Sicherheitsvorfälle im Vergleich zum Vorjahr 2016 beobachtet (auch interne IT-Sicherheitsvorfälle)?



Die Anzahl der IT-Sicherheitsvorfälle hat 2017 gegenüber 2016 tendenziell zugenommen.

Vorfälle von Cyber-Kriminalität

Unternehmen werden mit einer großen Vielfalt an möglichen externen Cyber-Angriffen bzw. anderen Problemen durch Cyber-Kriminalität konfrontiert.
Welche Art hatten Sie im letzten Jahr? Nennen Sie die Ihrer Ansicht nach bis zu drei wichtigsten Vorfälle.

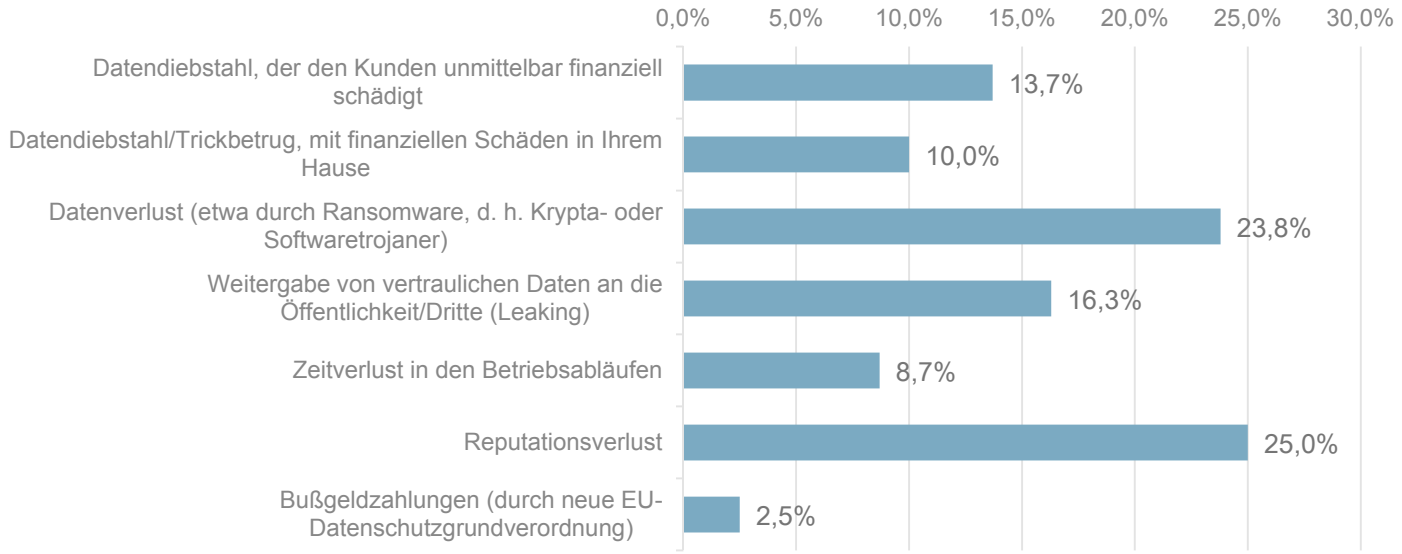


Angabe in Prozent der Nennungen, drei Nennungen möglich.

Die am wichtigsten eingeschätzten Vorfälle waren insbesondere Computersabotagen (z. B. Ransomware) und Trickbetrug z. B. in Form von Fake-President-Attacken.

Vorfälle von Cyber-Kriminalität

Was sind die größten Risiken, mit dem Sie bei Cyber-Angriffen konfrontiert werden?
Bitte nennen Sie die Ihrer Ansicht nach bis zu drei wichtigsten Risiken.

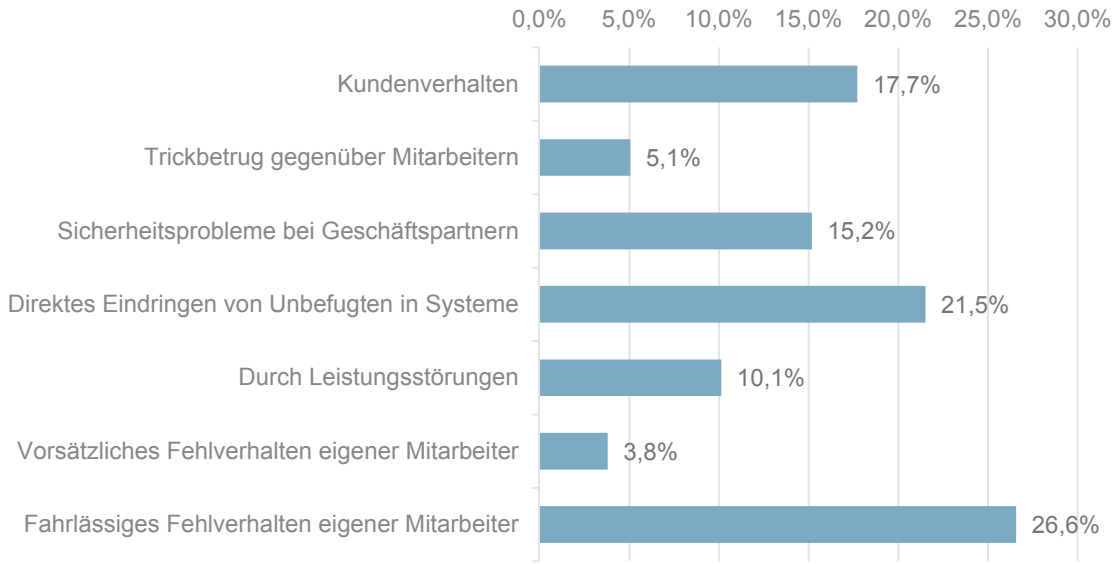


Angabe in Prozent der Nennungen, drei Nennungen möglich.

Die größten sich aus Cyber-Angriffen ergebenden Risiken werden in Reputationsverlusten sowie in einem Verlust von Daten gesehen.

Vorfälle von Cyber-Kriminalität

Durch welche Faktoren ist die Cyber Security in Ihrem Haus am stärksten gefährdet?
Nennen Sie die Ihrer Ansicht nach bis zu drei wichtigsten Faktoren.

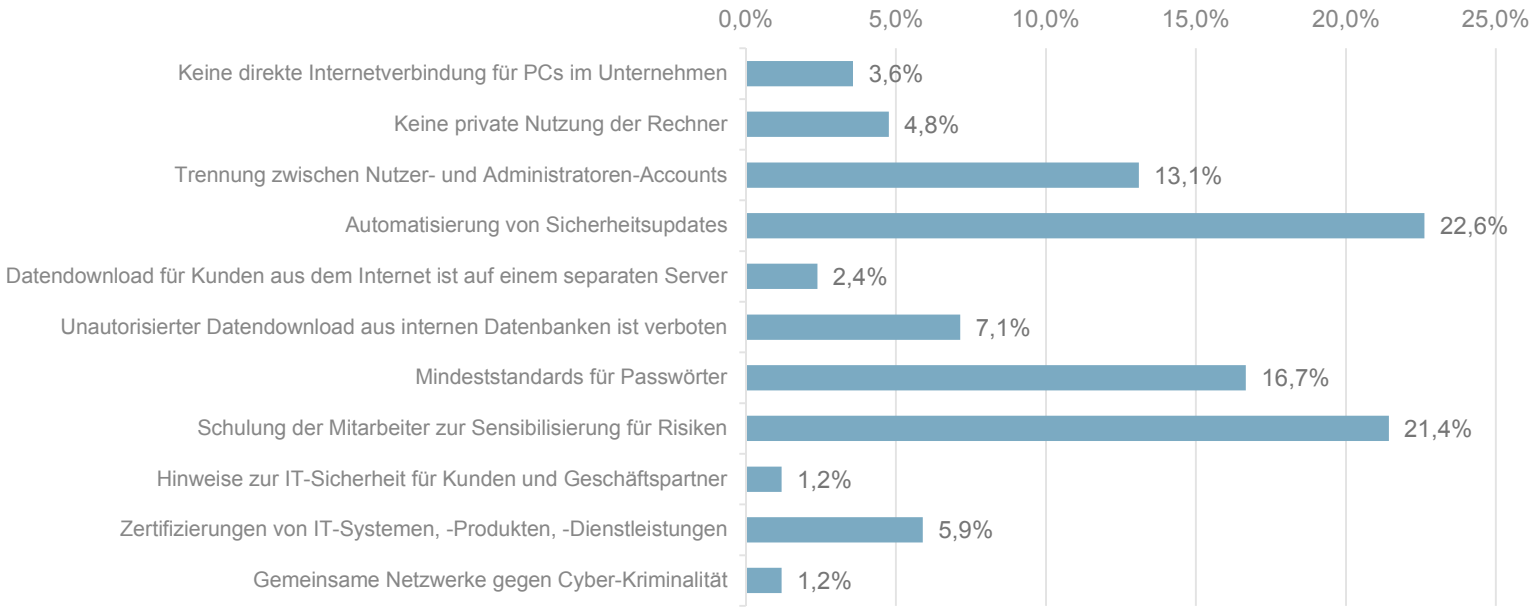


Angabe in Prozent der Nennungen, drei Nennungen möglich.

Die größte Gefährdung für die Cyber Security wird neben dem direkten Eindringen von Unbefugten in die Systeme des Unternehmens in einem fahrlässigen Fehlverhalten der eigenen Mitarbeiter gesehen. Zusammen mit dem vom Kunden ausgehenden Risiko spielt der menschliche Faktor damit eine größere Rolle als gezielte Angriffe von außerhalb.

Maßnahmen im Rahmen von Cyber-Security

Bitte nennen Sie bis zu drei besonders wichtige Maßnahmen, mit denen Sie Cyber Security in Ihrem Haus bereits sicherstellen.

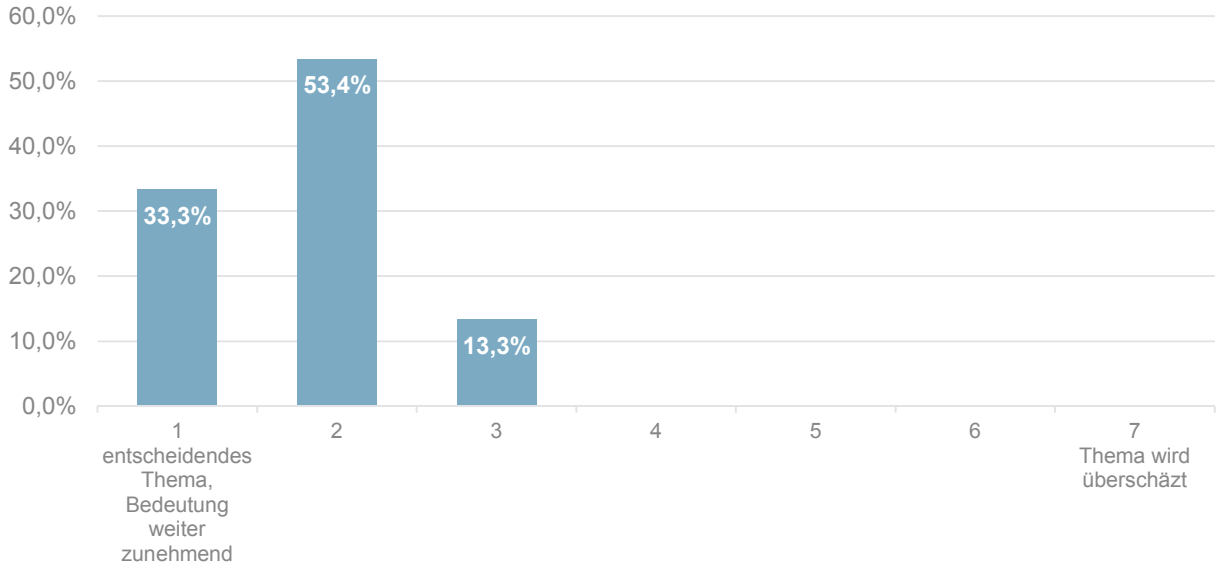


Angabe in Prozent der Nennungen, drei Nennungen möglich.

Automatisierte Updates und Schulungen für Mitarbeiter werden als wichtige Maßnahmen eingeschätzt. Beides, wie auch Vorgaben für Passwörter, greift bekannte Probleme auf, die sich aus nachlässigem Verhalten von Mitarbeitern ergeben. Gemeinsame Netzwerke gegen Cyber-Kriminalität spielen nur eine untergeordnete Rolle.

Maßnahmen im Rahmen von Cyber-Security

Unabhängig von der Sichtweise Ihres Unternehmens:
Wie beurteilen Sie persönlich die Relevanz von Cyber Security für Ihr Unternehmen für die nächsten drei bis fünf Jahre?

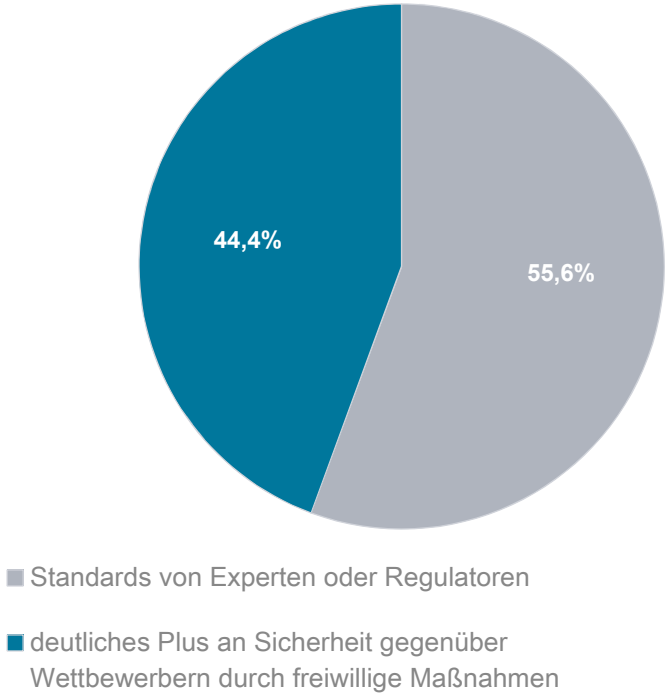


Angaben in Prozent gültiger Fälle.

Cyber Security wird von allen Befragten als relevant bzw. sehr relevant eingeschätzt. Im Gegensatz zu vielen anderen Themen aus dem Bereich Digitalisierung geht niemand davon aus, es sei ein überschätztes Thema. Die Bereitschaft für eine weitere Sensibilisierung für dieses Thema sollte insofern gegeben sein.

Maßnahmen im Rahmen von Cyber-Security

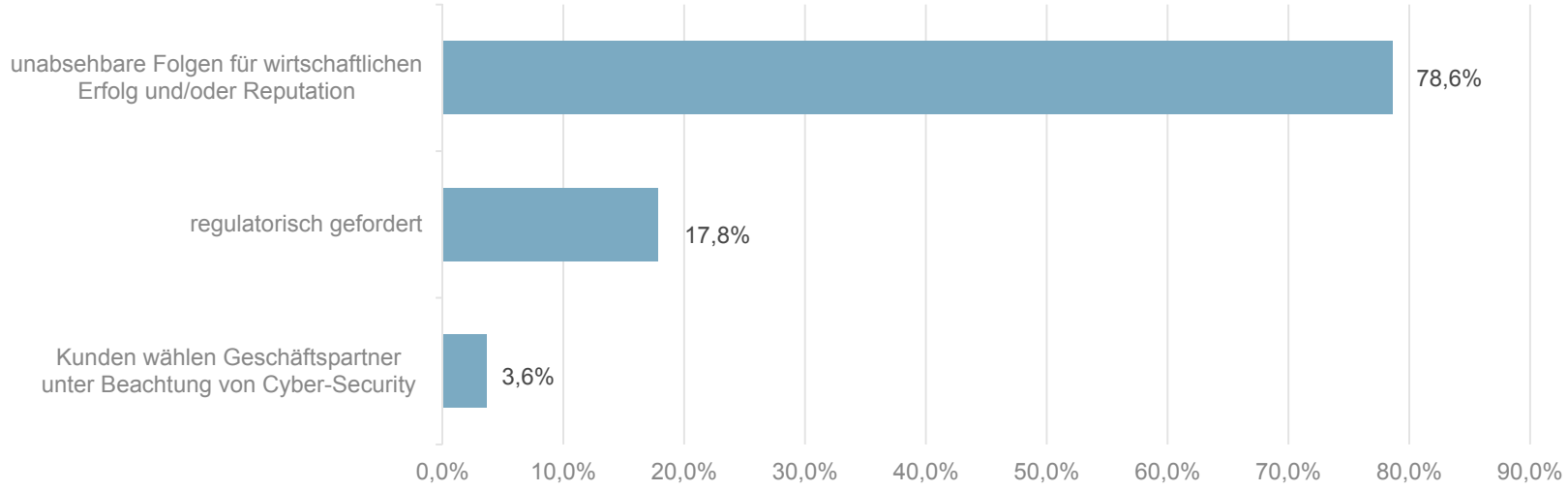
Was sind die wichtigsten Orientierungspunkte für Ihre Maßnahmen zum Thema Cyber Security?



Unternehmen orientieren sich in ihren Maßnahmen sowohl an regulatorischen Standards als auch daran, durch zusätzliche freiwillige Maßnahmen die Cyber Security sicherer zu gestalten als mögliche Wettbewerber.

Maßnahmen im Rahmen von Cyber-Security

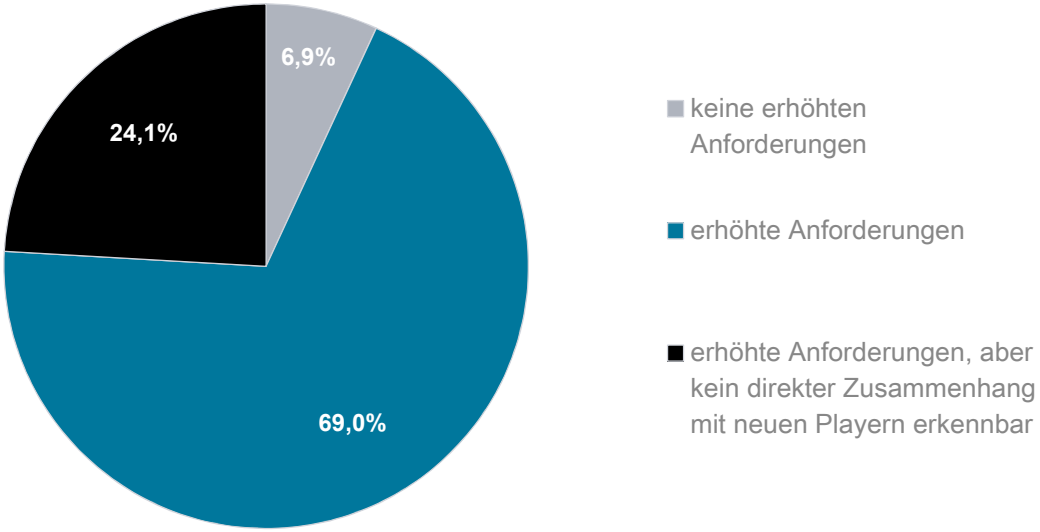
Welcher der folgenden Faktoren ist der Haupttreiber für Ihre Aktivitäten im Bereich Cyber Security?



Aktivitäten bzgl. Cyber Security werden vor allem durch die nicht absehbaren Folgen in puncto Reputation sowie wirtschaftlicher Erfolg getrieben.

Maßnahmen im Rahmen von Cyber-Security

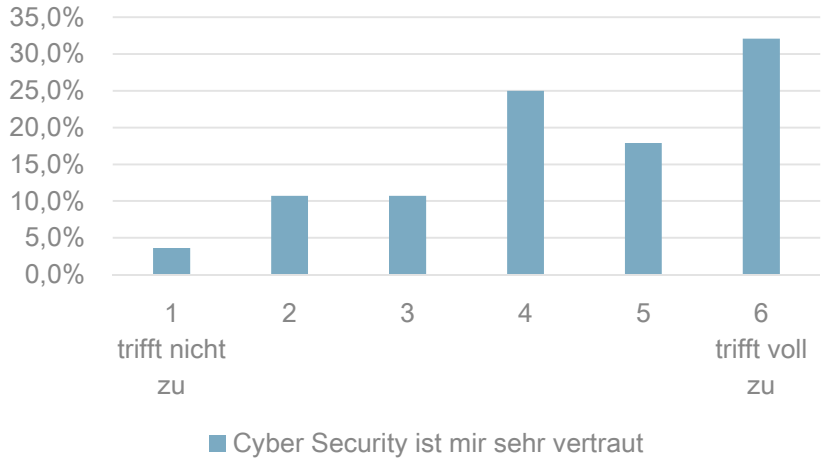
In den letzten Jahren sind zahlreiche neue Player in den Markt für digitale Finanzdienstleistungen eingetreten (sogenannte Fintechs).
Ergeben sich durch die neuen Player und die eingegangenen Kooperationen erhöhte Anforderungen hinsichtlich der Cyber Security von Banken und anderen Finanzdienstleistern?

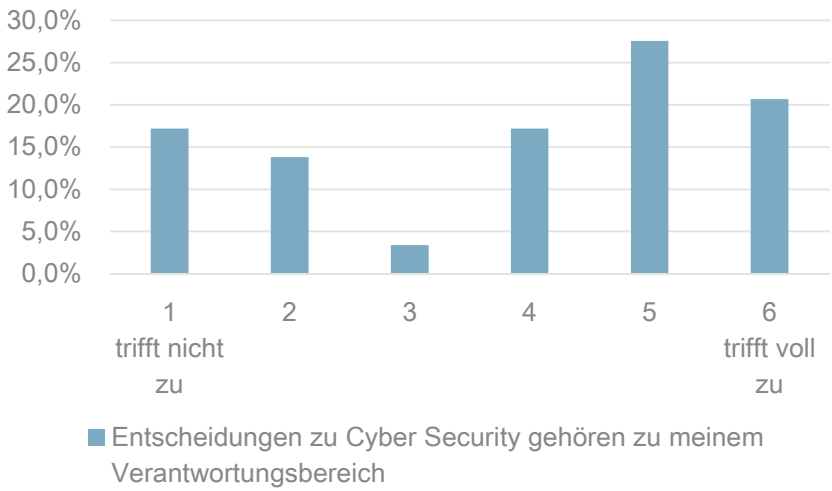


Tendenziell wird eine Erhöhung von Anforderungen durch neue Player gesehen, die bereits von ihrem Geschäftsmodell her ein Produkt der Digitalisierung sind und sich von Anfang an mit der Thematik befassen mussten.

Über die Teilnehmer der Studie

Wie vertraut sind die Teilnehmer der Studie mit der Cyber Security Thematik und gehört diese zu ihrem Verantwortungsbereich?



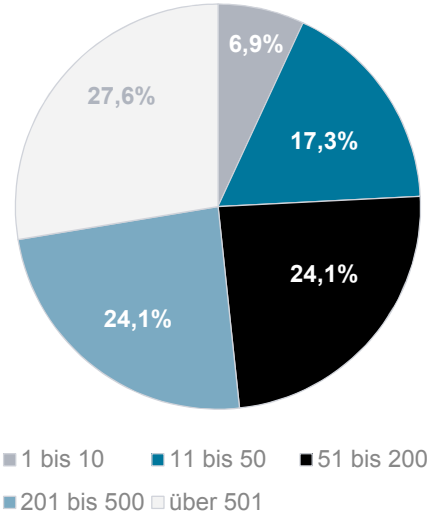


Cyber Security ist den Teilnehmern insgesamt ein vertrautes Thema.

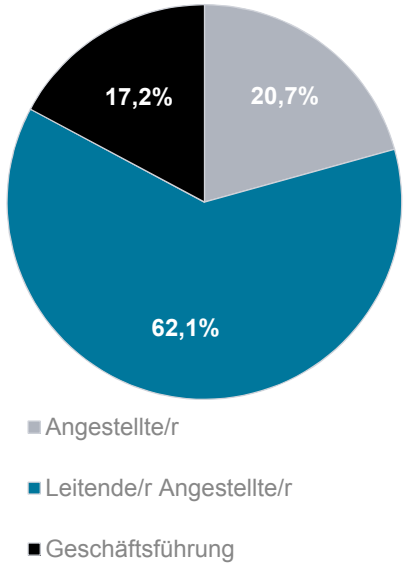
Über die Teilnehmer der Studie

Kontaktiert wurden 243 Personen. Teilgenommen haben davon 46 (19%).

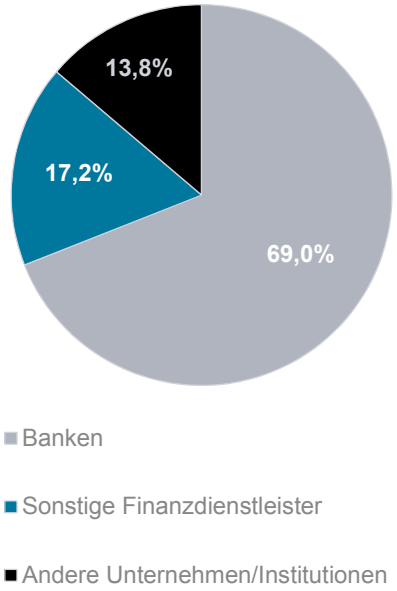
Unternehmensgröße (Mitarbeiterzahl)



Position im Unternehmen



Branche



Kontakt

Bernd Bretschneider, Stefan Koll
GBB-Rating
Gesellschaft für Bonitätsbeurteilung mbH
Kattenbug 1
50667 Köln
Fon +49 221 912897-222
Fax +49 221 912897-270
E-Mail S.Koll@gbb-rating.eu
Web www.gbb-rating.eu

Prof. Dr. Barbara E. Weißenberger
Heinrich-Heine-Universität Düsseldorf
Lehrstuhl für BWL, insb. Accounting
Universitätsstraße 1
40225 Düsseldorf
Barbara.Weissenberger@hhu.de
Tel: +49 (0) 211 81-11839 (Sekr.)

Prof. Dr. Corinna Ewelt-Knauer,
Justus-Liebig-Universität Gießen
Professur für Financial Accounting
Licher Straße 62
35394 Gießen
Corinna.Ewelt-Knauer@wirtschaft.uni-giessen.de
Tel: 0641 / 99 225 81 (Sekr.)