



# Maßnahmen gegen **Cyberangriffe**



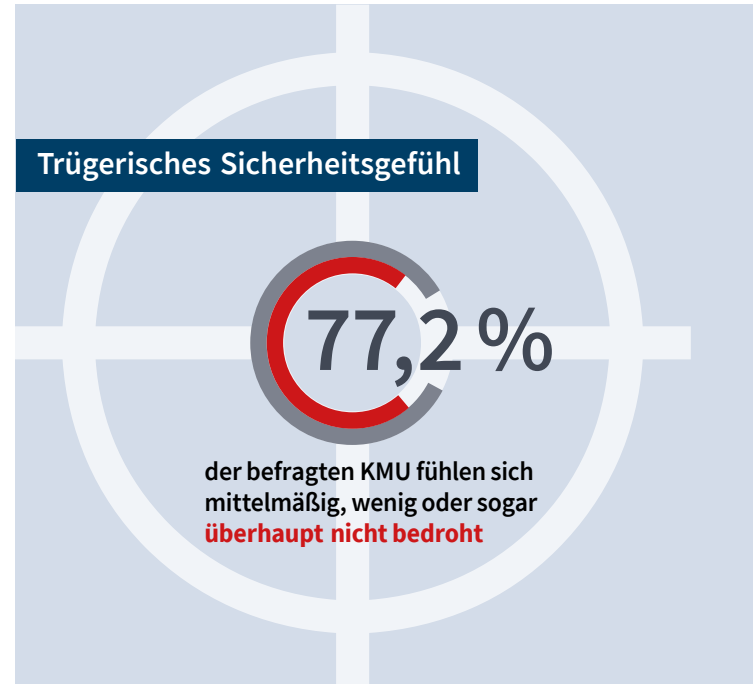
Sind kleine und mittelständische Unternehmen im Bereich IT-Sicherheit gut aufgestellt?

# Die aktuelle Bedrohungslage

## Wie gut sind KMU gegen Cyberkriminalität aufgestellt?

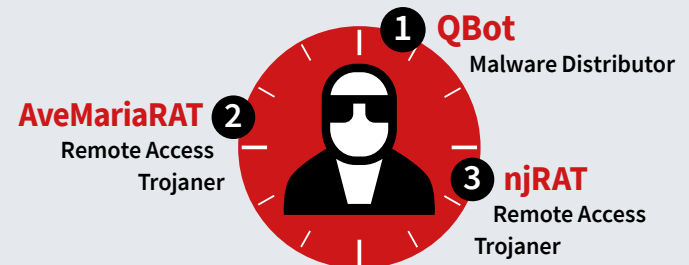
Kleinen und mittleren Unternehmen fehlt ein ausreichendes **Bewusstsein für Cybergefahren**. Sie sehen sich trotz der immens gestiegenen Bedrohungslage selbst nicht als interessante Ziele für Cyberkriminelle – Das zeigt eine aktuelle Umfrage der G DATA CyberDefense AG.

**Mehr als drei Viertel** der 193 befragten Unternehmen aus den Branchen Architektur- und Ingenieurbüros, Anwaltskanzleien, Steuerberater, Wirtschaftsprüfer sowie Finanzdienstleister fühlen sich von Cyberkriminellen nur mittelmäßig bis sehr wenig bedroht. Diese falsche Einschätzung ist fatal und führt dazu, dass sich die Unternehmen **unzureichend** gegen Angriffe schützen und sie IT-Sicherheitsvorfälle umso härter treffen.



Der Takedown von **Emotet** – von BSI-Präsident Arne Schönbohm als „König der Schadsoftware“ bezeichnet – führte insgesamt nicht zu einer Entspannung der Gefahrenlage. Im Gegenteil: Der inoffizielle Emotet-Nachfolger **QBot** war bei jeder vierten verhinderten Attacke beteiligt. Das zeigt, dass es für Unternehmen und auch speziell für KMU **keine Verschnaufpause** gibt.

## Die drei größten Malware-Gefahren



# Die aktuelle Bedrohungslage

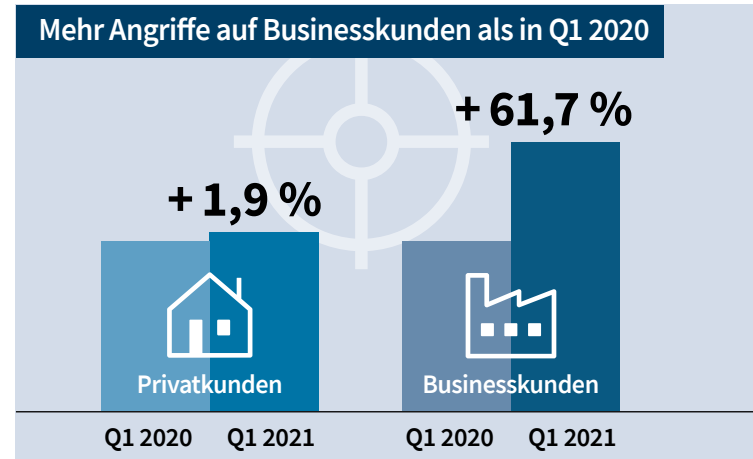
## Cyberkriminelle nehmen kleine und große Unternehmen ins Visier

Der **G DATA Bedrohungsreport** macht die alarmierende Bedrohungslage deutlich: Im ersten Quartal 2021 hat sich die Anzahl der **abgewehrten Angriffe** auf Unternehmen **um 62 % gesteigert** – im Vergleich zum Vorjahreszeitraum.

Generell greifen Cyberkriminelle sowohl kleine als auch mittelständische Firmen und Konzerne an, erpressen Lösegeld oder spähen besonders kritische Daten aus – um sie zu verkaufen oder für weitere Angriffe auszunutzen.

Die von G DATA befragten Unternehmen haben einen reichen Schatz an Daten, die nicht in die Hände von Dritten gelangen sollten. **Welche Maßnahmen** setzen die befragten Unternehmen aus den eingangs genannten Branchen um?

Wo lassen sich deutliche Unterschiede bei den einzelnen Wirtschaftszweigen erkennen und welche Rolle spielen **externe Dienstleister** bei der Absicherung?



## Große Kluft zwischen tatsächlicher und gefühlter Bedrohungslage bei KMU

Nur **ein Fünftel** der befragten KMU hat ein ausreichendes Bewusstsein für Cybergefahren, denn sie fühlen sich stark bis sehr stark von IT-Sicherheitsvorfällen bedroht. Die Mehrheit der Teilnehmer hat ein **unrealistisch positives** Bild der akuten Bedrohungslage.

Dieses falsche und trügerische Gefühl der Sicherheit führt dazu, dass die Cyberabwehr nicht umfassend aufgestellt ist. Die Folge: Nicht selten sind Schäden **existenzbedrohend**. Zu diesem Ergebnis kommt eine Umfrage des Bundesamtes für Sicherheit in der Informationstechnik im zweiten Halbjahr 2020 zur Lage der IT-Sicherheit im Homeoffice.

# Die Lage der IT-Sicherheit in KMU

KMU sind den Zahlen zufolge genauso stark durch Cybercrime bedroht wie große Unternehmen. Angreifer haben leichteres Spiel, wenn IT-Verantwortliche im KMU-Bereich nicht über das nötige Bewusstsein für die Risiken von Cyberattacken verfügen.

Die Einschätzung der Gefahrenlage weicht in der von G DATA erhobenen Umfrage am größten bei Rechtsanwälten, Steuerberatern sowie Wirtschafts-

prüfern ab. Ein Blick in die branchenspezifischen Ergebnisse zeigt, dass nahezu die Hälfte der Rechtsanwälte ein geringes Risiko für sich sehen, obwohl sie über viele vertrauliche Informationen von Mandanten und Gerichtsprozessen verfügen.

Steuerberater und Wirtschaftsprüfer sind dagegen besonders sensibel für Cybergefahren und sehen das höchste Bedrohungspotenzial unter den Befragten.

## Jedes KMU kennt IT-Sicherheitsvorfälle

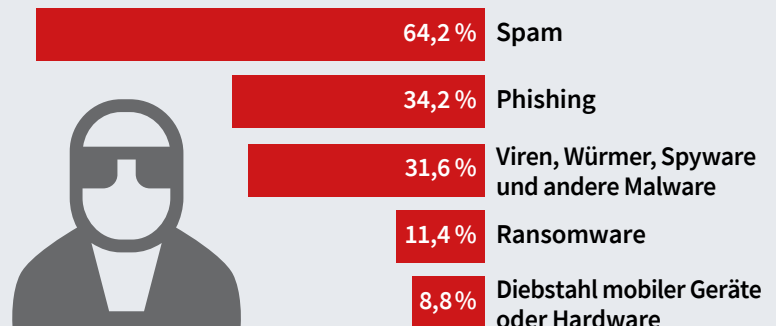
Die befragten KMU waren bereits von unterschiedlichen Vorfällen betroffen.

Unter den Top drei über alle Branchen hinweg befinden sich **Spam, Phishing** sowie **Viren, Würmer und andere Schadprogramme**. Das ist nicht verwunderlich, denn die meisten Cyberangriffe beginnen mit einer E-Mail an eine Mitarbeiterin oder einen Mitarbeiter.

Diese Nachrichten enthalten oft einen schädlichen Dateianhang oder einen Link zu einer Webseite, über die Schadcode ausgeliefert oder vertrauliche Daten abgefischt werden.

Oft reicht **ein falscher Klick** eines Mitarbeitenden aus und die Cyberattacke beginnt. Häufig wird über diesen Weg **Ransomware** verbreitet, über die Kriminelle Dateien, Computer oder sogar ganze Netzwerke verschlüsseln, um **Lösegeld** für die Wiederfreigabe zu erpressen. Mit diesen besonders perfiden Angriffen hatte bereits jedes zehnte KMU (11,4 %) zu kämpfen.

### Die Top-5 der gemeldeten IT Security Vorfälle



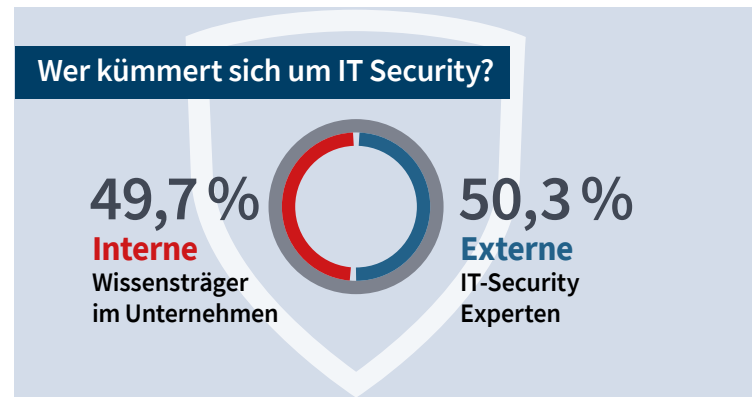
# Die Lage der IT-Sicherheit in KMU

**Steuerberater** liegen bei der Angabe von IT-Sicherheitsvorfällen über dem Durchschnitt der Befragten und sind mit mehr als 20 % am stärksten von Ransomware betroffen. Sie sind deutlich stärker mit von Kunden eingesandten Dateien konfrontiert als die anderen befragten Branchen – das könnte die erhöhte Anfälligkeit für Ransomware erklären.

Dagegen geben mehr als ein Viertel der **Rechtsanwälte** an, von IT-Sicherheitsvorfällen bisher nicht betroffen zu sein. Fraglich ist hier, ob Rechtsanwälte wirklich weniger betroffen sind oder die Angriffe nur weniger sichtbar sind und nicht erkannt werden.

## Interne Maßnahmen zur Verbesserung der IT-Sicherheit sind rudimentär

Bei der Hälfte der befragten Unternehmen wird das Wissen über IT-Security durch die Mitarbeitenden aufgebaut, die andere Hälfte der Teilnehmer vertraut auf externe Spezialisten. Das macht deutlich: **Rund die Hälfte der KMU** trauen sich zu, IT-Security-Themen selbst zu bewältigen und fühlen sich ausreichend durch Fachpresse (51 %), Veranstaltungen (40 %) und Fortbildungen (39 %) informiert.



Angesichts der **Komplexität** von IT-Sicherheit kann man hier aber in Zweifel ziehen, ob KMU auch die Sachkenntnis für die Umsetzung besitzen und ihre IT-Sicherheit alleine auf ein sicheres Fundament stellen können.

Bei den eingesetzten Maßnahmen ist in den befragten KMU ein deutlicher Nachholbedarf erkennbar: Fast **87 %** der Unternehmen haben eine **Endpoint Protection** im Einsatz, nutzen eine **Firewall (68 %)** und kümmern sich um die **E-Mail-Sicherheit** und **Backups** (jeweils knapp **zwei Drittel**).

# Die Lage der IT-Sicherheit in KMU

Alarmierend ist hier, dass **13 %** der befragten KMU nach eigenen Angaben **keine Endpoint Protection** im Einsatz haben und somit nicht durch eine Sicherheitslösung geschützt sind. Dabei gibt es auf dem Markt Security Software, die auch für Kleinstunternehmen handzuhaben ist oder bei der sie ihre IT-Sicherheit von extern managen lassen können – bei einem geringen Budgeteinsatz.

Für welche Option sich KMU auch immer entscheiden, eine Sicherheitslösung ist grundlegend für die Abwehr von Cyberbedrohungen, sollte aber durch weitere Maßnahmen sinnvoll ergänzt werden. Lediglich **weniger als die Hälfte** der Umfrageteilnehmer nutzen eine **sichere VPN-Verbindung** und nur knapp **40 %** der KMU installieren **Updates und Patches** der genutzten Programme, um Sicherheitslücken zu schließen.

Erfolgt ein Angriff, werden genau diese Schwachstellen in Betriebssystemen und Anwendungen ausgenutzt. Die Implementierung der bereitstehenden Patches ist eine einfache und lohnenswerte Maßnahme, die umgehend für mehr Sicherheit sorgt.

## Alarmierende Defizite



Dass nur **sechs von zehn** Unternehmen **Backups** haben, ist eine von vielen Erklärungen für die schwerwiegenden Folgen, wenn ein Angriff erfolgreich ist und die Daten verloren sind. Fatal ist zudem, wenn zum Beispiel vertrauliche Steuerdaten von Privatpersonen bzw. Firmen oder Informationen über Strafprozesse in die Hände Dritter gelängen.

# Die Lage der IT-Sicherheit in KMU

## Was verhindert eine umfassende IT-Sicherheit in KMU?

Fehlendes Bewusstsein und der Mangel an nötigen Ressourcen stehen den befragten Unternehmen massiv im Weg, ihre IT-Systeme umfassend zu schützen. Rund ein Viertel der befragten KMU geben als Grund an, dass ihr Unternehmen kein interessantes Angriffsziel für Cyberkriminelle sei.

Hier offenbart sich klar ein mangelndes Bewusstsein für die vorhandenen Gefahren.

Aber auch andere Gründe wie Zeit-, Budget- und Personalmangel hindern KMU daran, sich besser aufzustellen. Zeitmangel ist das am häufigsten genannte Argument gegen mehr IT-Sicherheit.

Hier wird deutlich, dass Rechtsanwälte, Steuerberater, Architekten, Wirtschaftsprüfer oder aber Finanzdienstleister mit ihrem Kerngeschäft genug beschäftigt sind. Sie haben schlicht **keine Zeit für IT-Sicherheit**. Das fehlende Budget verschärft das Problem und ist insofern fatal, als dass die Bewältigung eines erfolgreichen Angriffs um einiges kostspieliger ist als die Investition in IT-Sicherheit.



**Zeitmangel** für das Thema IT Security



Zu wenig **Budget** zur Verfügung



Bedrohung wird **nicht wahrgenommen**



Zu wenig **Fachpersonal** für IT-Bereich

Mehr als ein Viertel der Wirtschaftsprüfer geben an, auf **kostenlose** Sicherheitslösungen zu setzen und nutzen damit Software, die eigentlich für **Heimanwender** gedacht ist. Unternehmen sollten aber auf eine bedarfsgerechte und umfassende **Businesslösung** setzen, die auch einen hohen Anspruch an das Thema **Datenschutz** hat.

# Die Lage der IT-Sicherheit in KMU

Wichtig ist auch die Möglichkeit eines zentralen Managements aller Clients, damit die Schutzwirkung aller Komponenten der Sicherheitslösung auch sichergestellt werden kann. Der sehr begrenzte oder nicht deutschsprachige Support bei kostenfreien Produkten kann dann zum Problem werden, wenn Schwierigkeiten mit dem Programm auftreten, die selbst nicht gelöst werden können.

## KMU profitieren vom Fachwissen der Dienstleister

Die  **Hälfte** der befragten Unternehmen setzt auf die Unterstützung von Systemhäusern und Dienstleistern bei der IT-Sicherheit. Bei vier von zehn KMU (41 %) übernehmen sie sogar die komplette IT und damit auch IT-Security.

Bei 40 % stehen IT-Experten für Fragen zur IT-Sicherheit zur Verfügung.

9 % der Umfrageteilnehmer haben Anbieter beauftragt, die sie durch regelmäßige Reports und Empfehlungen zur Verbesserung der Cybersicherheit unterstützen.

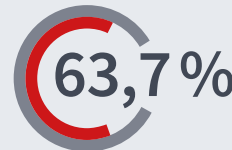
Mit **68 %** liegen **Steuerberater** bei dem Einbezug von **externen IT-Spezialisten** ganz vorne.

**Rechtsanwälte und Wirtschaftsprüfer** wiederum legen den Schwerpunkt auf **interne Wissensträger** und vertrauen zu **60 %** auf das Wissen und die Fähigkeiten ihrer Mitarbeitenden.

Ob Mitarbeitende allgemein überhaupt die Möglichkeiten haben, sich intensiv mit IT-Sicherheit auseinanderzusetzen, ist sehr fraglich.

Die Gründe für die **Beauftragung eines externen Dienstleisters** liegen für **64 %** der befragten KMU auf der Hand: Die Hilfestellung durch **ausgewiesene Experten**, die durch ihr Fachwissen unterstützen.

Für die  **Hälfte** der Befragten ist zudem eine möglichst hohe **Zeitersparnis** und die Arbeitserleichterung entscheidend dafür, einen Dienstleister zu beauftragen.



(Umfrage-Durchschnitt)  
Steuerkanzleien: 78,6 %  
Finanzdienstleister: 51,9 %



(Umfrage-Durchschnitt)  
Architekten/Ingenieure: 58 %  
Wirtschaftsprüfer: 33,3 %



# Die Lage der IT-Sicherheit in KMU

Bei den befragten Unternehmen der unterschiedlichen Branchen sind die Beweggründe, einen externen IT-Security-Dienstleister zu beauftragen, unterschiedlich stark gewichtet und weichen von den Gesamtergebnissen ab:

Steuerberater geben mit nahezu 80 % an, dass das Fachwissen der Experten der entscheidende Grund für die Beauftragung eines Dienstleisters ist. Für Architekten, Wirtschaftsprüfer und Finanzdienstleister ist es außerdem überdurchschnittlich wichtig, Einblicke in die

Vorgänge der IT-Sicherheit zu erhalten.

Architekten wiederum legen deutlich über Durchschnitt Wert darauf, dass sich die Securitylösung in der Cloud befindet. Dies könnte damit zusammenhängen, dass Architekten traditionell mit großen Datenmengen hantieren und einen regen Austausch mit beteiligten Projektpartnern wie Kunden, Baufirmen und Ämtern pflegen.

Cloudbasierte Lösungen erleichtern die Zusammenarbeit in diesem Kontext enorm – wenn sie sicher konfiguriert sind.

## Fazit: KMU wiegen sich bei IT-Sicherheit in falscher Sicherheit und haben akuten Nachholbedarf

Insgesamt zeigt sich, dass die befragten KMU ein **mangelndes Bewusstsein** für Cybergefahren haben und sich der Illusion hingeben, kein Opfer eines Cyberangriffs zu werden.

Daher verwundert es nicht, dass immer noch **jedes zehnte** Unternehmen **keinen basalen Schutz** einer Sicherheitslösung in Anspruch nimmt und damit grob fahrlässig handelt.

Es ist nur eine **Frage der Zeit**, bis ein Angriff erfolgreich ist. Dabei gibt es längst Securitysoftware auf dem Markt, die den Bedürfnissen von KMU entsprechen:

**Umfassender und unkomplizierter Schutz vor Cyberbedrohungen** – auch als gemanagte Lösung und das verbunden mit geringen Kosten.

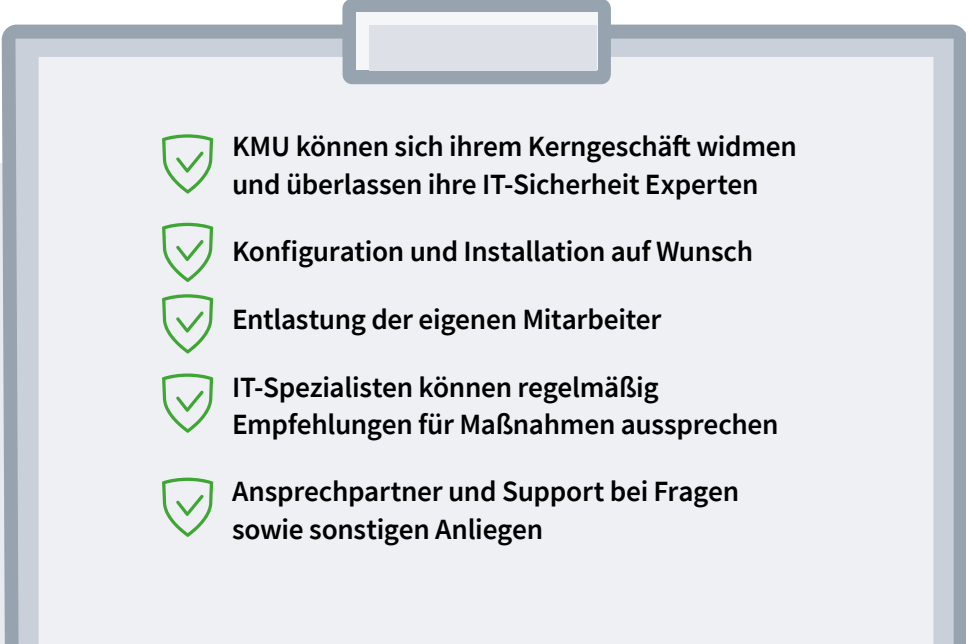







# Externe Dienstleister

Viele KMU setzen bei IT-Sicherheit auf externe Dienstleister, um Unterstützung durch Experten zu bekommen. Allerdings gibt rund die Hälfte der Umfrageteilnehmer ihre IT-Sicherheit nicht in fremde Hände und versucht, dieses Thema selbst zu managen. Es reicht nicht, nur gut informiert zu bleiben. Insbesondere die Umsetzung von individuell auf das Unternehmen hin zugeschnittenen IT-Sicherheitsmaßnahmen spielt eine entscheidende Rolle. Weitere Hindernisse für eine umfassende und bedarfsgerechte IT-Security im KMU-Segment sind Budget- und Ressourcenprobleme.

Werden externe IT-Security-Spezialisten beauftragt, überlassen vier von zehn KMU dem Dienstleister ihre komplette Cybersicherheit, was gerade für diese Unternehmen sehr sinnvoll ist, um sich voll und ganz dem Kerngeschäft widmen zu können. Der Dienstleister sollte jedoch in Hinblick auf die Kompetenzen im Sicherheitsbereich sorgfältig ausgewählt werden. Auch hierzu ist ein Bewusstsein für Cybergefahren die Grundlage, denn ohne ein realistisches Bewusstsein für die Gefahrenlage ist IT-Sicherheit nicht bedarfsgerecht möglich.

## Checkliste: Die Vorteile von externen Dienstleistern

- 
-  **KMU können sich ihrem Kerngeschäft widmen und überlassen ihre IT-Sicherheit Experten**
  -  **Konfiguration und Installation auf Wunsch**
  -  **Entlastung der eigenen Mitarbeiter**
  -  **IT-Spezialisten können regelmäßig Empfehlungen für Maßnahmen aussprechen**
  -  **Ansprechpartner und Support bei Fragen sowie sonstigen Anliegen**

## Über die Umfrage

Für die Umfrage befragten techconsult und Heise im Auftrag von G DATA CyberDefense AG insgesamt **193 kleine und mittelständische Unternehmen** aus den Bereichen Architekten (Baubranche), Rechtsanwälte, Steuerberater, Wirtschaftsprüfer und Finanzdienstleister. Die befragten KMU haben bis zu fünfzig Computer im Einsatz.

## Über die G DATA CyberDefense AG

Mit umfassenden Cyber-Defense-Dienstleistungen macht der **Erfinder des AntiVirus** Unternehmen verteidigungsfähig gegen Cybercrime. Mehr als 500 Mitarbeiter sorgen für die digitale Sicherheit von Unternehmen und Anwendern. Forschung und Entwicklung erfolgen in Deutschland. G DATA schützt mit NextGen-KI-Technologien, Endpoint Protection, bietet Penetrationstests und Incident Response bis zu Awarenesstrainings, um Unternehmen wirksam zu verteidigen. Speziell für kleine Unternehmen bietet der Cyber-Defense-Hersteller mit **G DATA 365 Essentials** eine Managed-Securitylösung an. Zudem wurde G DATA zum „**IT-Champion**“ gekürt und ist damit das vertrauenswürdigste IT-Security-Unternehmen Deutschlands.



[gdata.de/business](https://gdata.de/business)

[kontakt@gdata.de](mailto:kontakt@gdata.de) | +49 234 9762-170



TRUST IN  
GERMAN  
SICHERHEIT