TRUST IN GERMAN SICHERHEIT

G DATA Business IT-Security Barometer

Wie steht es um die IT-Sicherheit im deutschen Mittelstand?

G DATA CyberDefense AG | Oktober 2017

Einleitung

Cyberkriminalität ist für Unternehmen in Deutschland zu einem echten Problem geworden - täglich haben es die IT-Verantwortlichen mit Schadprogrammen, wie WannaCry, Locky und anderen Online-Angriffen, zu tun. Die G DATA Sicherheitsexperten zählten alleine für das erste Halbjahr 2017 fast 4,9 Millionen neue Computerschädlinge – und das mit steigender Tendenz. Am Jahresende könnte mit insgesamt fast zehn Millionen neuer Schadprogramme ein neuer Negativ-Höchststand erreicht sein. Dabei sind die Auswirkungen durch die Malware-Flut für Unternehmen oft fatal. Laut Bitkom entsteht deutschen Unternehmen durch Malware und Online-Attacken, und damit verbundenen Datendiebstahl, Erpressung und Sabotage, jedes Jahr ein Schaden von 55 Milliarden Euro.

Besonders im Fokus der Täter stehen mittelständische Firmen, die als Innovationsmotor der deutschen Wirtschaft über die Landesgrenzen hinaus bekannt sind. Diese Unternehmen sind wachstumsstark und mit ihren Produkten und Dienstleistungen sehr erfolgreich. Patente für Neuentwicklungen spielen hier eine sehr große Rolle. Umfassender Schutz und eine durchdachte IT-Security-Strategie sind daher nötig, um IT-Systeme und Geschäftsdaten zu schützen und Folgen wie finanzielle Verluste bis hin zum Ruin zu verhindern.

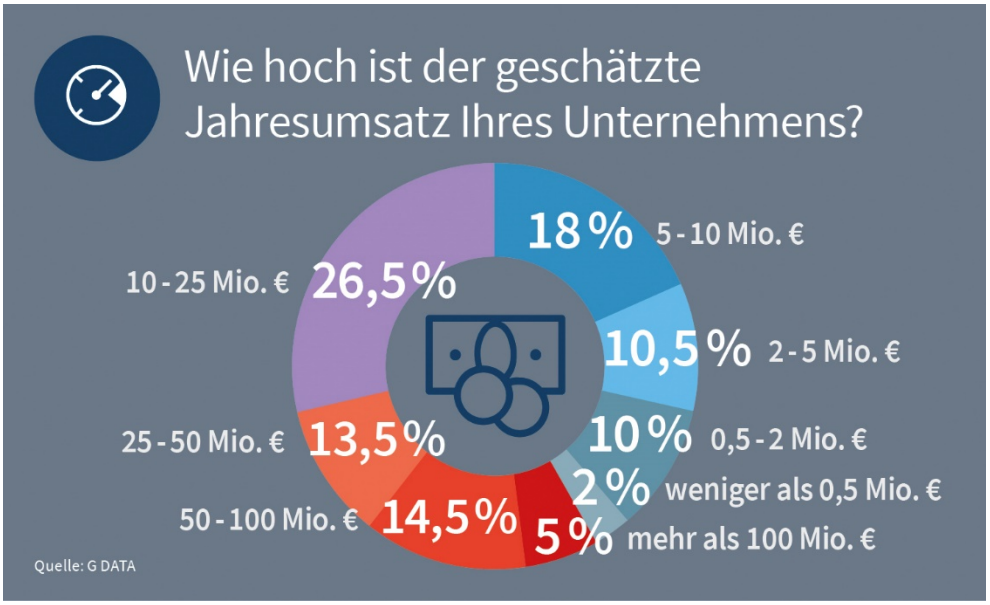
Das G DATA Business IT-Security Barometer widmet sich daher der IT-Sicherheit in mittelständischen Unternehmen und beleuchtet dabei die Bereiche IT-Bedrohungslage, Schutzmaßnahmen, Umsetzung der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) und die Wichtigkeit der Datenverarbeitung durch IT-Security-Anbieter in Deutschland.

Methodik der Studie

Für das G DATA Business IT-Security Barometer – „Wie steht es um die IT-Sicherheit im deutschen Mittelstand?“ wurden branchenübergreifend 200 mittelständische Unternehmen aus ganz Deutschland befragt.

Die teilnehmenden Firmen hatten 50 bis 500 Mitarbeiter. Zu Beginn des Fragebogens wurde dieser Aspekt als Eingangskriterium befragt, um sicherzustellen, dass nur diese Mittelständler das Panel beantworten.

Außerdem wurde darauf geachtet, dass die Teilnehmer aus einem IT-affinen Bereich innerhalb der Firma kamen, um die Fragen beantworten zu können.

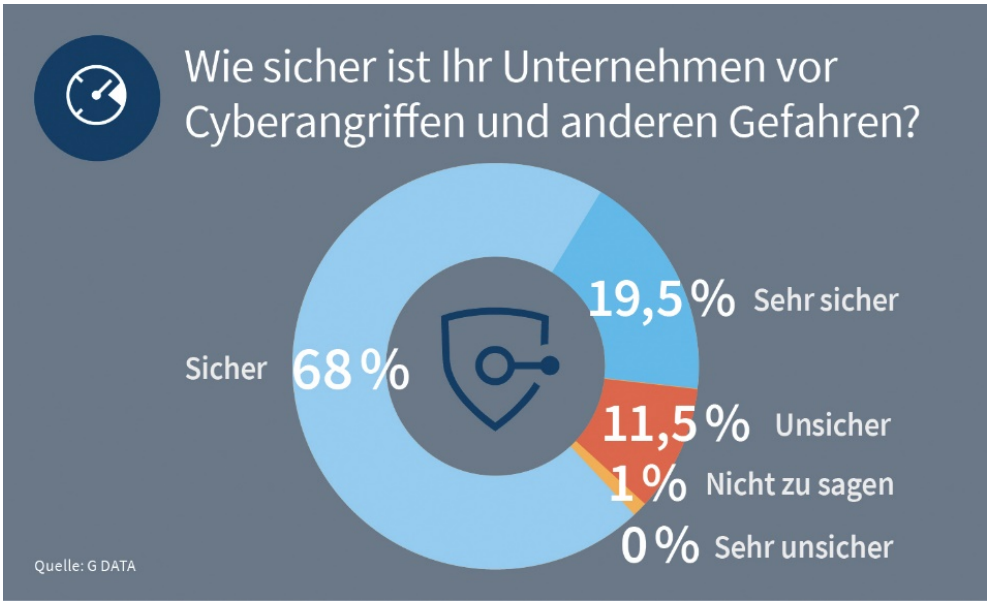


Die Umfrage wurde von OmniQuest GmbH im Auftrag der G DATA CyberDefense AG von Ende August bis Anfang September 2017 durchgeführt.

Wie steht es um die IT-Sicherheit im deutschen Mittelstand? – Die Ergebnisse

Unternehmen fühlen sich sicher vor Online-Kriminalität

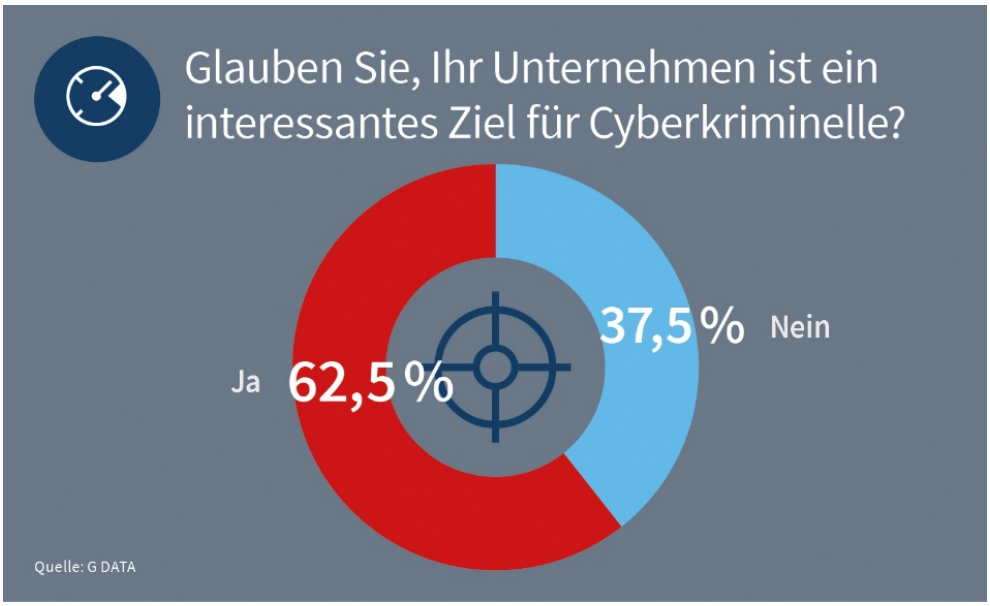
Fast neun von zehn Unternehmen fühlen sich in puncto Cyberbedrohungen sicher oder sogar sehr sicher. Es ist anzunehmen, dass diese glauben, gut gegen Online-Attacken gerüstet zu sein. Unsicher fühlen sich dagegen nur annähernd 12 Prozent der Teilnehmer. Die am häufigsten gewählte Antwort von den Mittelständlern, in Relation mit dem erzielten Jahresumsatz, ist mit 68 Prozent „sicher“. Der Maximal-Peak zeichnete sich mit rund 86 Prozent bei Unternehmen mit einem Jahresumsatz von 5 bis 10 Millionen ab, während der Minimalwert von etwa 44 Prozent bei Unternehmen mit einem Jahresumsatz von 25 bis 50 Millionen erreicht wurde. Aus diesem Segment fühlt sich ein Drittel unsicher oder kann die gefühlte Sicherheitslage nicht einschätzen. Diese Firmen könnten bereits Opfer von Cyberkriminellen und deren Attacken gewesen sein und sind daher eher vorsichtig bei der Einschätzung.



Wie sicher ist Ihr Unternehmen aktuell in Hinblick auf Cyberangriffe und andere Gefahren aus dem Internet?												
		Mitarbeiter im Unternehmen			Jahresumsatz des Unternehmens							
	Total	50 - 99	100 - 249	250 - 500	Bis zu 500.000 €	500.000 € bis 2 Mio. €	2 Mio. € bis 5 Mio €	5 Mio. € bis 10 Mio. €	10 Mio. € bis 25 Mio. €	25 Mio. € bis 50 Mio. €	50 Mio. € bis 100 Mio. €	Mehr als 100 Mio. €
Sehr sicher	19,5%	9,8%	21,8%	23,9%	0%	20%	19%	13,9%	30,2%	22,2%	10,3%	10%
Sicher	68%	80,4%	66,7%	60,6%	100%	65%	76,2%	86,1%	62,3%	44,4%	72,4%	60%
Unsicher	11,5%	9,8%	9,0%	15,5%	0%	15%	0%	0%	7,5%	29,6%	17,2%	30%
Sehr unsicher	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Nicht einschätzbar	1,0%	0%	2,6%	0%	0%	0%	5%	0%	0%	3,7%	0%	0%

Daten bei Mittelständler als Ziel von Cyberkriminellen

Grundsätzlich ist jede Firma ein interessantes Ziel für die Täter, weil jedes Unternehmen mit Daten arbeitet, die entwendet und weiterverkauft werden können. Jeder sechste Mittelständler sieht genau diese Gefahr und geht davon aus, ein interessantes Ziel darzustellen. Diese Ansicht verstärkt sich mit zunehmender Mitarbeiterzahl: Fast sieben von zehn Firmen mit 250 bis 500 Beschäftigten glauben daran, dass ihr Unternehmen ein interessantes Ziel für Cyberkriminelle ist.



In puncto Jahresumsatz ergibt sich das Bild, dass Unternehmen mit Einnahmen von bis zu zwei Millionen Euro nicht glauben, für die Kriminellen interessant zu sein. Erst bei den Firmen mit einem höheren Umsatz fühlt sich die Mehrheit der Mittelständler im kriminellen Fadenkreuz.

Glauben Sie, dass Ihr Unternehmen ein interessantes Ziel für Cyberkriminelle ist?												
		Mitarbeiter im Unternehmen			Jahresumsatz des Unternehmens							
	Total	50 - 99	100 - 249	250 - 500	Bis zu 500.000 €	500.000 € bis 2 Mio. €	2 Mio. € bis 5 Mio €	5 Mio. € bis 10 Mio. €	10 Mio. € bis 25 Mio. €	25 Mio. € bis 50 Mio. €	50 Mio. € bis 100 Mio. €	Mehr als 100 Mio. €
Ja	62,5%	52,9%	62,8%	69%	25%	40%	52,4%	69,4%	62,3%	74,1%	69%	70%
Nein	37,5%	47,1%	37,2%	31%	75%	60%	47,6%	30,6%	37,7%	25,9%	31,0%	30%

Um herauszufinden, warum sich mittelständische Firmen als potentielle Opfer von Cyberkriminalität sehen oder nicht, fragt das G DATA Business IT-Security Barometer nach den Gründen für diese Sichtweise. Die Teilnehmer konnten dabei frei und ungestützt antworten, was sie als Ursache ansehen. Die Ergebnisse wurden sinnvoll zusammengefasst. Dabei sehen die meisten Mittelständer, die ihr Unternehmen im Fokus der Täter sehen, ihre Daten als Objekt der kriminellen Begierde. Informationen aus Firmen, wie Kundendatenbanken oder Konstruktionspläne, sind für Cyberkriminelle ein äußerst begehrtes Diebesgut. Neben der Absicht Sabotage zu betreiben, gehört der Diebstahl dieser lukrativen Daten zu den meisten verfolgten Absichten der Täter – aus Sicht der Mittelständler.

Darüber hinaus geben andere Unternehmen an, aufgrund der betriebenen Forschung und Entwicklung oder des Geschäftsfeldes beziehungsweise der Branche interessant zu sein. Es ist davon auszugehen, dass einzelne Unternehmen oder ganze Wirtschaftszweige für Cyberkriminelle besonders interessante Angriffsziele darstellen, dazu gehören beispielweise die Akteure, die zur kritischen Infrastruktur zählen. Weitere Gründe sind unter anderem der geschäftliche Erfolg oder die Schadenswirkung durch Angriffe, zum Beispiel durch Störungen in den Betriebsabläufen.

Dagegen sehen die meisten Teilnehmer des G DATA Business IT-Security Barometers, die ihr Unternehmen als uninteressant für Cyberkriminelle ansehen, dass das Geschäftsfeld oder die Branche nicht anziehend genug oder die Daten nicht von Belange für die Täter sind. Die Größe und Bekanntheit der Firma sind die zweite Top-Antwort dieser Mittelständler. Diese Ansicht könnte für diese Unternehmen fatale Auswirkungen haben, falls aufgrund dieser Ansicht die IT-Systeme nicht gut genug gegen Online-Attacken abgesichert sind. Wie eingangs schon beschrieben, stellen per se alle Unternehmen für die Täter ein interessantes Angriffsziel dar und Daten sind dabei ein wichtiger Anreiz. Alle Unternehmen verfügen über abgreifbare Informationen alleine schon deshalb, weil die Datenverarbeitung heute IT-gestützt ist. Davon abgesehen können die Angreifer auch andere Ziele

verfolgen, zum Beispiel Sabotage oder die Verschlüsselung von Daten bis hin zu ganzen Computern in Verbindung mit der Erpressung von Lösegeld mit einem Ransomware-Schädling. Hierbei hat das Tätigkeitsfeld oder die Branche keinen Belang für die Täter.

Ransomware – jedes dritte Unternehmen war bereits betroffen

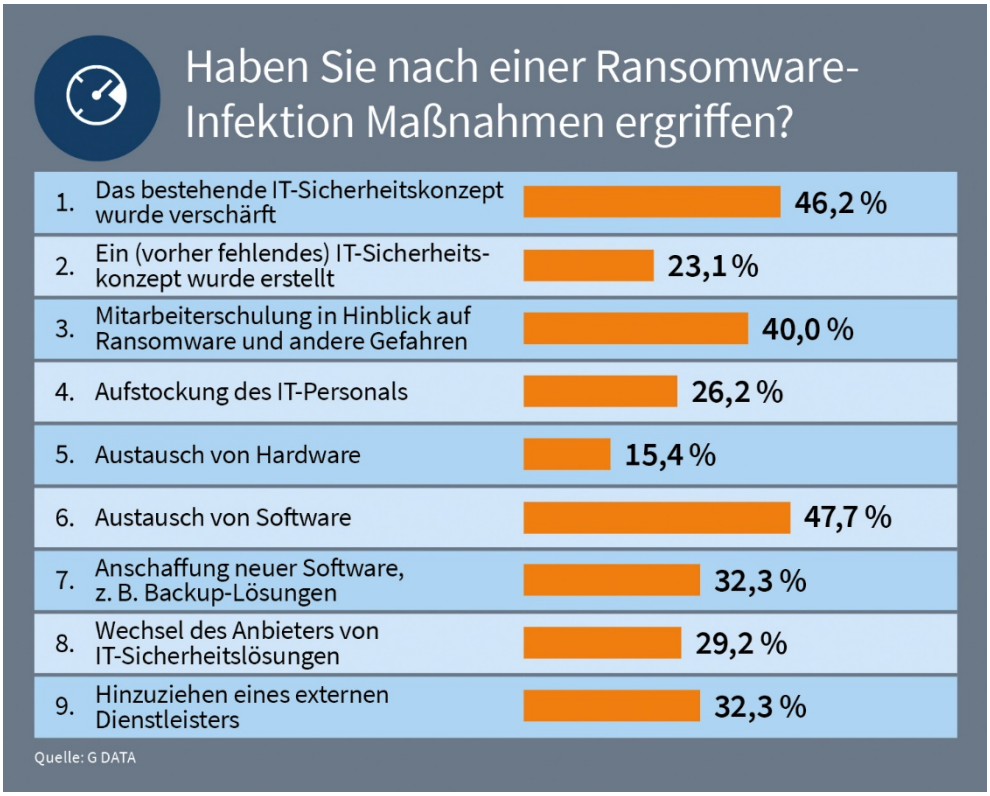
Locky, Petna oder WannaCry sind Ransomware-Schädlinge, die in den letzten Monaten in den Medien sehr präsent waren. Computer wurden massenweise verschlüsselt und Lösegeld von den betroffenen Nutzern erpresst. Die Ransowmare WannaCry schaffte es unter anderem die Deutsche Bahn, den Logistiker FedEx und zahlreiche Parkscheinautomaten lahm zu legen.

Die Mehrheit der Mittelständler – mehr als zwei Drittel – in dieser Studie waren noch nie Opfer einer Infektion mit diesem Schadprogrammtyp, sodass davon ausgegangen werden kann, dass sie hier effektiv abgesichert waren. Mehr als 22 Prozent hatte bereits mit einer Ransomware-Infektion zu kämpfen, aber nur eines von zehn Unternehmen hatte es mehrmals getroffen.

Bei den Ergebnissen fällt auch hier auf, dass die Gefahr, von den heimtückischen Schadprogrammen angegriffen zu werden, mit der Anzahl der Mitarbeiter im Unternehmen steigt: Mit 30 Prozent an einmaligen erfolgreichen Attacken mit Erpressertrojanern haben die Firmen mit mehr als 100 Millionen Euro Jahresumsatz den höchsten Anteil der Betroffenen.

War Ihr Unternehmen bereits ein Opfer von Ransomware?												
		Mitarbeiter im Unternehmen			Jahresumsatz des Unternehmens							
	Total	50 - 99	100 - 249	250 - 500	Bis zu 500.000 €	500.000 € bis 2 Mio. €	2 Mio. € bis 5 Mio €	5 Mio. € bis 10 Mio. €	10 Mio. € bis 25 Mio. €	25 Mio. € bis 50 Mio. €	50 Mio. € bis 100 Mio. €	Mehr als 100 Mio. €
Ja, mehrmals	10%	5,9%	9%	14,1%	0%	15%	9,5%	5,6%	17%	11,1%	3,4%	0%
Ja, einmal	23%	13,7%	26,9%	23,9%	25%	15%	28,6%	27,8%	20,8%	22,2%	17,2%	30%
Nein	67,5%	80,4%	64,1%	62%	75%	70%	61,9%	66,7%	62,3%	66,7%	79,3%	70%

Alle Teilnehmer, die angaben, bereits ein Opfer von erfolgreichen Ransomware-Attacken geworden zu sein, wurden nach möglichen Änderungen in der IT-Sicherheitsstrategie als Reaktion für die Infektion befragt.



Dabei haben die meisten auf den Vorfall mit dem Austausch von Softwarelösungen reagiert oder das bestehende IT-Sicherheitskonzept verschärft, um weitere erfolgreiche Angriffe zukünftig zu verhindern. Auf Platz drei steht die Schulung der eigenen Mitarbeiter in Hinblick auf Ransomware und andere Online-Gefahren. Mitarbeiter können Cyberkriminellen unbewusst eine Tür zu den IT-Systemen des Unternehmens öffnen, wenn sie beispielsweise auf erhaltene E-Mails mit infizierten Dateianhang klicken oder sie den eingefügten Link in der Nachricht anwählen. Der oftmals in Szenarien erwähnte USB-Stick auf dem Parkplatz, der ohne vorherige Virenprüfung in den USB-Port des Rechners gesteckt und ausgelesen wird, ist ein weiteres Beispiel dafür, wie Offline-Angriffe möglich sind. Dabei passieren diese Vorfälle oft, weil Mitarbeiter nicht ausreichend über solche Gefahren und Szenarien aufgeklärt sind. Bei Firmen mit 50 bis 100 Millionen Euro Jahresumsatz sind Mitarbeiterschulungen sogar auf Platz 1, genauso wie bei kleinen Mittelständlern mit 50 bis 99 Angestellten.

Haben Sie nach einer Ransomware-Infektion Änderungen vorgenommen oder besondere Maßnahmen ergriffen? (Mehrfachnennung möglich)												
		Mitarbeiter im Unternehmen			Jahresumsatz des Unternehmens							
	Total	50 - 99	100 - 249	250 - 500	Bis zu 500.000 €	500.000 € bis 2 Mio. €	2 Mio. € bis 5 Mio €	5 Mio. € bis 10 Mio. €	10 Mio. € bis 25 Mio. €	25 Mio. € bis 50 Mio. €	50 Mio. € bis 100 Mio. €	Mehr als 100 Mio. €
Bestehendes IT-Sicherheitskonzept wurde verschärft	46,2%	60,0%	39,3%	48,1%	100%	50%	25%	25%	55%	55,6%	50%	67%
Ein IT-Sicherheitskonzept wurde erstellt	23,1%	20%	25%	22,2%	0%	33,3%	25%	8,3%	25%	44,4%	16,7%	0%
Mitarbeiterschulung in puncto IT-Security	40%	60%	32,1%	40,7%	100%	33,3%	12,5%	25%	50%	44,4%	66,7%	33,3%
Aufstockung IT-Personal	26,2%	10%	25%	33,3%	0%	33,3%	37,5%	25%	20%	33,3%	16,7%	33,3%
Austausch von Hardware	15,4%	10%	7,1%	25,9%	0%	0%	12,5%	8,3%	25%	22,2%	16,7%	0,0%
Austausch von Software	47,7%	40%	53,6%	44,4%	0%	16,7%	37,5%	58,3%	60%	66,7%	33,3%	0,0%
Anschaffung neuer Lösungen (z.B. Backup)	32,3%	10%	21,4%	51,9%	0%	50%	25,0%	8,3%	25%	77,8%	33,3%	33,3%
Wechsel IT-Security-Anbieter	29,2%	20%	21,4%	40,7%	0%	16,7%	37,5%	25%	25%	33,3%	33,3%	66,7%
Hinzuziehen eines Dienstleisters	32,3%	40%	28,6%	33,3%	0%	33,3%	50%	41,7%	20%	33,3%	33,3%	33,3%
Andere Maßnahmen	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Nichts	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Security Software als häufigste Maßnahme zum Schutz gegen Online-Kriminelle

Im G DATA Business IT-Security Barometer wurden die teilnehmenden mittelständischen Unternehmen dazu befragt, welche Maßnahmen sie ergreifen, um sich gegen Online-Attacken zu schützen. Dabei war eine Mehrfachnennung möglich. Wenig überraschend ist, dass der Einsatz einer Virenschutzsoftware mit mehr als 56 Prozent die Top-Antwort ist - unabhängig von der Anzahl der Beschäftigten. In puncto Jahresumsatz ist das Bild nicht mehr so einheitlich: Bei den Unternehmen mit einem Umsatz zwischen 5 und 25 Millionen Euro rangiert diese Antwortmöglichkeit nur auf Platz drei. Hier ist die am ehesten ergriffene Maßnahme die IT-Security Schulung für Mitarbeiter

(Mittelständler mit Jahreseinnahmen zwischen fünf und zehn Millionen Euro) beziehungsweise regelmäßige Backups. Die Erstellung eines IT-Sicherheitskonzeptes, verbunden mit der Definition der besonders sensiblen und schützenswerten Bereichen, ist das wichtigste Mittel in der Abwehr von Cyberbedrohungen für Firmen mit Bruttoeinnahmen von 50 bis 100 Millionen Euro im Jahr. Hier kommt der Virenschutz auf den zweiten Platz.

Im Allgemeinen ist das Erstellen von regelmäßigen Systemabbildern und Datensicherungen die am zweit häufigsten gewählte Maßnahme, gefolgt von IT-Sicherheitsschulungen für Mitarbeiter mit einem Wert von 50 Prozent auf Platz drei.

Welche Maßnahmen ergreifen Sie, um Ihr Unternehmen vor Online-Bedrohungen abzusichern? (Mehrfachnennung möglich)												
		Mitarbeiter im Unternehmen			Jahresumsatz des Unternehmens							
	Total	50 - 99	100 - 249	250 - 500	Bis zu 500.000 €	500.000 € bis 2 Mio. €	2 Mio. € bis 5 Mio €	5 Mio. € bis 10 Mio. €	10 Mio. € bis 25 Mio. €	25 Mio. € bis 50 Mio. €	50 Mio. € bis 100 Mio. €	Mehr als 100 Mio. €
Einsatz Virenschutzlösung	56,5%	56,9%	53,8%	59,2%	50%	60%	52,4%	36,1%	56,6%	66,7%	72,4%	60%
Installation Software-Updates	43,5%	37,3%	41%	50,7%	25%	40%	38,1%	25%	45,3%	51,9%	62,1%	50%
Richtlinien oder Verbot für Nutzung privater Mitarbeiter-Mobilgeräte	37,5%	37,3%	33,3%	42,3%	25%	15%	33,3%	41,7%	37,7%	51,9%	41,4%	30%
Mobile Device Mangement	19%	13,7%	11,5%	31%	0%	15%	19%	11,1%	15,1%	29,6%	24,1%	40%
Regeln für Nutzung von PC, Internet und Geräten	42,5%	39,2%	39,7%	47,9%	50%	25%	52,4%	36,1%	34%	66,7%	44,8%	50%
Einsatz Monitoring Software	31%	21,6%	26,9%	42,3%	0%	25%	33,3%	16,7%	32,1%	40,7%	44,8%	30%
Definition von Vertraulichkeitsstufen für Daten	26,5%	17,6%	30,8%	28,2%	0%	10%	28,6%	25%	22,6%	40,7%	34,5%	30%
Regelmäßige Backups	51,5%	47,1%	50%	56,3%	50%	45%	38,1%	33,3%	60,4%	59,3%	69%	40%
Erstellung IT-Sicherheitskonzept	42,0%	25,5%	37,2%	59,2%	25%	30%	38,1%	19,4%	37,7%	55,6%	75,9%	50%
Erstellung Notfallplan	35,5%	31,4%	35,9%	38%	25%	30%	23,8%	25%	32,1%	51,9%	58,6%	20%
Mitarbeiterschulungen in puncto IT-Security	50%	51%	51,3%	47,9%	25%	30%	32,8%	50%	58,6%	59,3%	62,1%	50%
Bennung IT-Sicherheits-Beauftragter	34,5%	29,4%	34,6%	38%	50%	25%	28,6%	25,0%	39,6%	40,7%	41,4%	30%
Andere Maßnahmen	1%	0%	0%	1,4%	0%	0%	0%	0%	0%	0%	0%	0%
Nichts	2%	5,9%	0%	1,4%	25%	0%	0%	8%	0%	0%	0%	0%

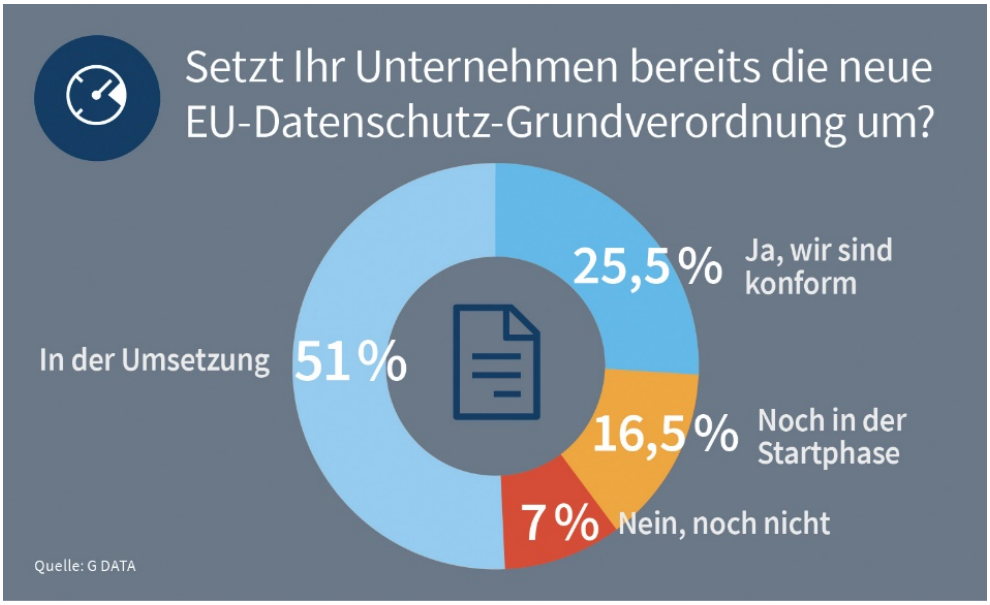
EU-Datenschutz-Grundverordnung: Die meisten Mittelständler stecken gerade in der Umsetzung

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) tritt am 25. Mai 2018 in Kraft und soll personenbezogene Daten besser und einheitlich in Europa schützen[1]. Daten verarbeitet jedes Unternehmen, weshalb von den Regelungen auch Jedes betroffen ist. Das neue Regelwerk stellt dabei viele Firmen vor eine große Herausforderung, aber spätestens jetzt müssen die erforderlichen Maßnahmen geplant und dann umgesetzt werden. Kommt es zu einer Verletzung des neuen Rechts, drohen empfindliche Strafen: Bis zu 4 Prozent des Jahresumsatzes des auffällig gewordenen Unternehmens.

Die Studie zeigt, dass die Hälfte der Mittelständler gerade dabei ist, die erforderlichen Punkte umzusetzen, ein Viertel gibt an, sogar schon der EU-DSGVO vollständig zu entsprechen. Nur sieben Prozent der teilnehmen Firmen haben sich mit dem Thema noch gar nicht beschäftigt. Dieser Anteil ist bei den Unternehmen mit Einnahmen von bis zu einer halben Millionen Euro mit einem Viertel am größten, im Vergleich zu den anderen Umsatzstufen. Gleichzeitig ist bei diesen Firmen der

[1] G DATA stellt für Firmen ein Whitepaper „Die neue EU-Datenschutz-Grundverordnung – Was Unternehmen jetzt wissen müssen“ kostenlos im Internet zur Verfügung.

Anteil derer, die gerade an der Umsetzung arbeiten, mit ebenfalls 25 Prozent am niedrigsten. Trotzdem zeigt auch der Blick auf die Jahreseinnahmen und die Mitarbeiterzahlen, dass die meisten Unternehmen bald der EU-DSGVO entsprechen werden und so auch den Termin des Inkrafttretens im kommenden Jahr halten werden können. Dabei haben die Mittelständler mit einem Jahresumsatz zwischen 10 und 25 Millionen Euro im Vergleich zu den anderen klar die Nase vorn: Hier sind neun von zehn Firmen entweder bereits EU-DSGVO-konform oder stehen durch die Umsetzung kurz davor.

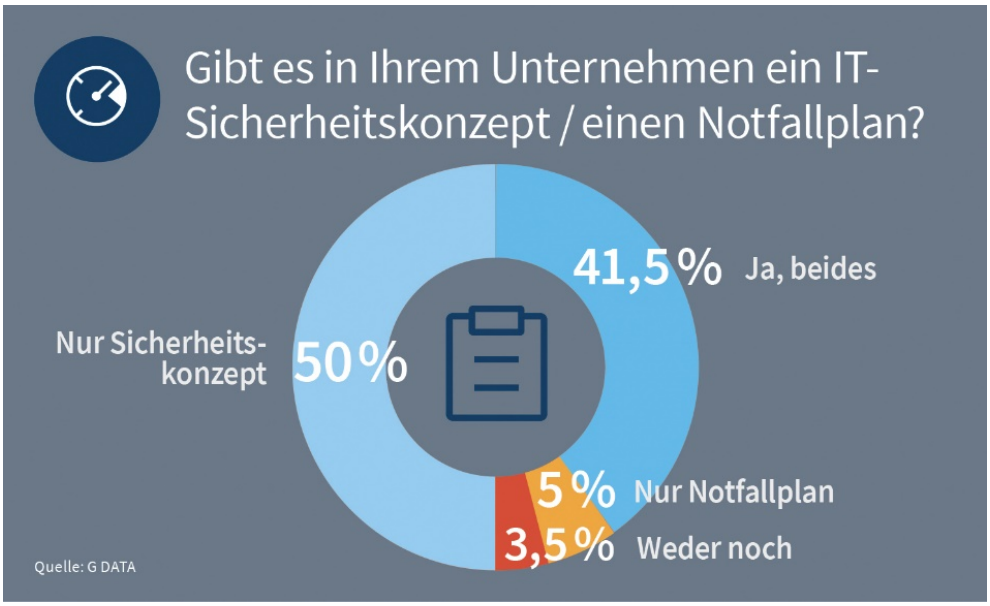


Haben Sie bereits alle erforderlichen Maßnahmen zur Umsetzung und Einhaltung der neuen EU-Datenschutz-Grundverordnung umgesetzt?												
		Mitarbeiter im Unternehmen			Jahresumsatz des Unternehmens							
	Total	50 - 99	100 - 249	250 - 500	Bis zu 500.000 €	500.000 € bis 2 Mio. €	2 Mio. € bis 5 Mio €	5 Mio. € bis 10 Mio. €	10 Mio. € bis 25 Mio. €	25 Mio. € bis 50 Mio. €	50 Mio. € bis 100 Mio. €	Mehr als 100 Mio. €
Ja, das Unternehmen ist bereits EU-DSGVO-konform	25,5%	17,6%	26,9%	29,6%	25%	25%	19%	25%	28,3%	29,7%	27,6%	10%
Wir setzen aktuell die erforderlichen Maßnahmen um	51%	56,9%	48,7%	49,3%	25%	45%	52,4%	52,8%	62,3%	37%	51,7%	40%
Wir sind hier noch am Anfang	16,5%	13,7%	19,2%	15,5%	25%	10%	19%	13,9%	7,5%	33,3%	17,3%	30%
Nein, unser Unternehmen ist noch nicht DSGVO-konform und wir haben noch nicht damit beschäftigt	7%	11,8%	5,1%	5,6%	25%	20%	9,6%	8,3%	1,9%	0%	3,4%	20%

Die Ergebnisse zeigen, dass dieser Prozess für mittelständische Unternehmen sehr umfangreich und anspruchsvoll ist, aber so viel Druck durch die drohenden Strafen erzeugt wird, dass das Thema eine hohe Priorität besitzt.

IT-Sicherheitskonzepte sind weit verbreitet, Notfallpläne weniger

Ein umfassendes und ausgefeiltes IT-Sicherheitskonzept ist der Grundpfeiler bei der Abwehr von Schadprogrammen und anderen Online-Attacken; davon sind auch die meisten Unternehmen in dieser Studie überzeugt: 91 Prozent verfügen über einen Fahrplan - wenn die Ergebnisse für die Antwortmöglichkeiten „Wir haben ein IT-Sicherheitskonzept und einen Notfallplan definiert“ und „Wir haben nur ein generelles IT-Sicherheitskonzept“ zusammengezählt werden. Bei Mittelständlern, die im Jahr zwischen 10 und 50 Millionen Euro verdienen, werden hier sogar 100 Prozent erreicht.



Auf einen Notfall sind dagegen noch längst nicht so viele mittelständische Firmen im G DATA Business IT Security Barometer mit einen speziellen Plan vorbereitet. Dies kann im Ernstfall zu größeren Schäden und auch zeitlichen Verzögerungen in der Reaktion auf die Vorfälle bedeuten, weil zunächst nicht klar ist, was zu tun ist. Im Allgemeinen verfügt fast die Hälfte der Mittelständler über ein solches Notfallprozedere. Auffällig ist aber, dass je mehr Mitarbeiter in einem Unternehmen arbeiten, desto eher ist ein Notfallplan verfügbar: Fast sechs von zehn Mittelständler mit 250 bis 500 Angestellten hat Notfallprozedere in der Schublade, im Vergleich dazu haben aber nur drei von zehn Firmen mit 50 bis 99 Mitarbeitern für den Notfall vorgesorgt. Dies spiegelt sich auch teilweise wieder, wenn nach Jahreseinnahmen unterschieden wird. Firmen mit mehr als 100 Millionen Umsatz haben zu 60 Prozent einen Notfallplan parat. Dagegen haben die Firmen mit der geringsten Umsatz-Kategorie in diesem Panel nur zu 25 Prozent eine definierte Vorgehensweise für den Fall von erfolgreichen Angriffen.

Verfügen Sie über ein IT-Sicherheitskonzept und einen Notfallplan für den Fall von Angriffen?												
		Mitarbeiter im Unternehmen			Jahresumsatz des Unternehmens							
	Total	50 - 99	100 - 249	250 - 500	Bis zu 500.000 €	500.000 € bis 2 Mio. €	2 Mio. € bis 5 Mio €	5 Mio. € bis 10 Mio. €	10 Mio. € bis 25 Mio. €	25 Mio. € bis 50 Mio. €	50 Mio. € bis 100 Mio. €	Mehr als 100 Mio. €
Wir haben ein IT-Sicherheitskonzept und einen Notfallplan	41,5%	31,4%	39,7%	50,7%	25%	35%	23,8%	36,1%	45,3%	51,9%	51,7%	40%
Wir haben nur ein IT-Sicherheitskonzept	50%	56,9%	53,8%	40,8%	50%	55%	57,1%	50%	54,7%	44,4%	41,4%	40%
Wir haben nur einen Notfallplan	5%	3,9%	3,8%	7,0%	0%	5%	4,8%	11,1%	0%	0%	6,9%	20%
Wir haben nichts von beiden	3,5%	7,8%	2,6%	1,4%	25%	5%	14,3%	2,8%	0%	3,7%	0%	0%

Erfreulicherweise ist der Anteil der Befragten, die weder einen Notfallplan, noch ein IT-Sicherheitskonzept haben, sehr gering. Im Allgemeinen sind es lediglich knapp vier Prozent. Dabei zeigt sich auch hier ein Trend in Verbindung mit den Mitarbeiterzahlen: Je mehr Angestellte ein Mittelständler in dieser Studie hat, desto seltener existieren weder ein Notfallprozedere, noch ein Absicherungsplan. Vorbildlich erscheinen auch die Firmen mit einem Jahresgewinn zwischen 10 und 25 und mit mehr als 50 Millionen, hier hat kein Teilnehmer die Antwortmöglichkeit „Wir haben nichts von beiden“ gewählt.

Die Studie zeigt an dieser Stelle, dass die Notwendigkeit von IT-Sicherheitskonzepten im Mittelstand angekommen ist. Hierbei können externe IT-Security-Dienstleister[2] helfen. Sie definieren die besonders schützenswerten Geschäftsbereiche und IT-Systeme und stellen ein Konzept sowie einen Notfallplan für den Ernstfall auf.

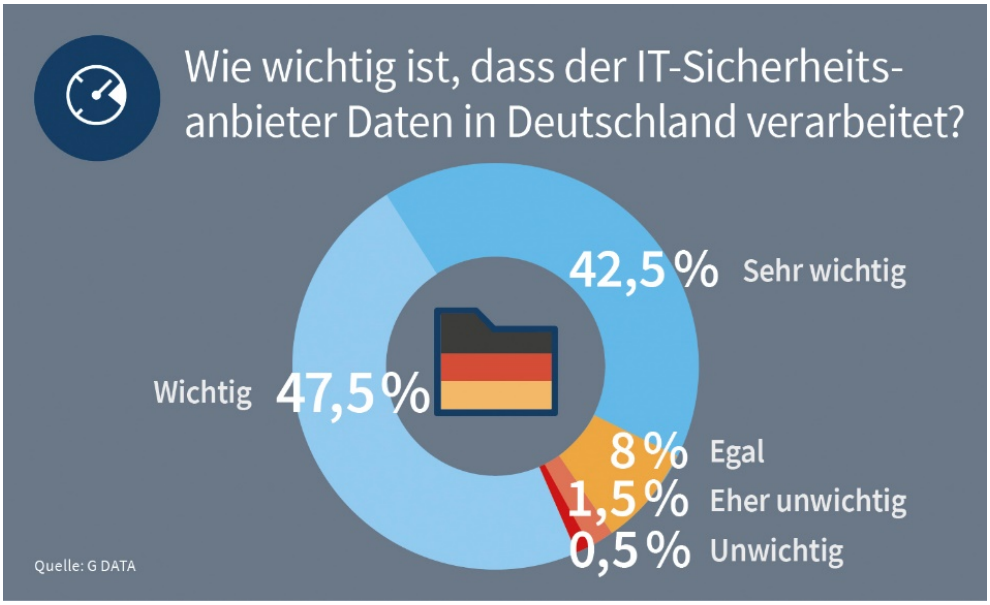
Die Daten sollen in Deutschland bleiben

Die Sensibilität für die Frage „was geschieht mit meinen Daten“ hat spätestens seit den Enthüllungen des Whistleblowers Edward Snowden und dem daraus resultierenden NSA-Skandal stark zugenommen. Auch bei dem jüngst ausgesprochenen Verbot für die US-amerikanischen Behörden Sicherheitslösungen der Firma Kaspersky einzusetzen, handelt es sich um einen Misstrauensbeweis - wobei es solches Misstrauen in Europa auch gegenüber amerikanischen IT Security-Unternehmen gibt.

Denn neben der Schutzwirkung der Lösungen geht vielen dabei um den Ausschluss von Backdoors für Behörden, Geheimdienste und andere staatliche Akteure, es geht auch darum, wo die durch die

[2] Ein Beispiel für einen IT-Security-Dienstleister ist die G DATA Advanced Analytics. Das Unternehmen bietet ein umfangreiches Dienstleistungsportfolio, wie persönliche Beratung, Mitarbeiterschulungen, Incident Response, Penetrationstests oder Malware-Analysen. Mehr unter www.gdata-advancedanalytics.de

Nutzung der Software entstandenen Daten verarbeitet werden und ob diese ausreichend geschützt sind.[3]



Das G DATA Business IT-Security Barometer hat daher gefragt, wie wichtig es den mittelständischen Unternehmen ist, dass die Verarbeitung der durch den IT-Sicherheitsanbieter erhobenen Daten, darunter Informationen zu Schadprogrammen oder gemeldeten verdächtigen Aktivitäten auf dem Computer, ausschließlich in Deutschland stattfindet. Das Ergebnis: neun von zehn Firmen finden diesen Aspekt wichtig bzw. sehr wichtig, nur für zehn Prozent der Teilnehmer hat dies keine Belang. Den höchsten Wert erreicht die Gruppe der Mittelständler mit Einnahmen von fünf bis zehn Millionen Euro im Jahr, hier liegt der Spitzenwert bei über 94 Prozent. Im Vergleich der Mitarbeiterzahlen kommen die Firmen mit 250 bis 500 Angestellten mit 93 Prozent auf den höchsten Anteil der Befürworter. Die Ergebnisse zeigen, dass es Unternehmenskunden nicht egal ist, was mit ihren Daten passiert und diese mehrheitlich auf die deutschen Datenschutzgesetze und deutsche Anbieter vertrauen.

Wie wichtig ist Ihnen, dass ein IT-Sicherheitsanbieter erhobene Daten ausschließlich in Deutschland verarbeitet und nicht im Ausland?												
		Mitarbeiter im Unternehmen			Jahresumsatz des Unternehmens							
	Total	50 - 99	100 - 249	250 - 500	Bis zu 500.000 €	500.000 € bis 2 Mio. €	2 Mio. € bis 5 Mio €	5 Mio. € bis 10 Mio. €	10 Mio. € bis 25 Mio. €	25 Mio. € bis 50 Mio. €	50 Mio. € bis 100 Mio. €	Mehr als 100 Mio. €
Sehr wichtig	42,5%	43,1%	37,2%	47,9%	25%	35%	38,1%	30,6%	34,0%	66,7%	55,2%	60%
Wichtig	47,5%	39,2%	55,1%	45,1%	50%	45%	42,9%	63,9%	60,4%	25,9%	37,9%	20%
Weder wichtig, noch unwichtig	8%	13,7%	7,7%	4,2%	25%	15%	19%	3%	3,8%	3,7%	6,9%	20%
Eher unwichtig	1,5%	2%	0%	2,8%	0%	5%	0%	0%	1,9%	0%	0%	0%
Unwichtig	0,5%	2%	0%	0%	0%	0%	0%	2,8%	0%	0%	0%	0%

[3] G DATA bekennt sich dazu, keine Hintertüren für Geheimdienste oder andere Ermittlungsbehörden in seine Sicherheitslösungen einzubauen. Darüber hinaus garantiert der IT-Security-Herstellern seinen Kunden, dass alle Daten in Deutschland verbleiben und sicher sind vor dem Zugriff Dritter.

Fazit

Das G DATA Business IT-Security Barometer – „Wie steht es um die IT-Sicherheit im deutschen Mittelstand“ kommt zum Schluss, dass die Absicherung vor Cyberbedrohungen in den Unternehmen im Allgemeinen einen hohen Stellenwert hat. Allerdings zeigt sich, dass insbesondere größere Mittelständler vorsichtiger und realistischer sind. Kleinere Unternehmen in dieser Umfrage haben hier an manchen Stellen einen Nachholbedarf, zum Beispiel wenn es um die Frage geht, ob die Firma im Fadenkreuz der Kriminellen steht und damit verbundenen Gründe, warum das eigene Unternehmen uninteressant für Angreifer ist. Hier könnte es zu unzureichenden Abwehrmaßnahmen kommen, sodass diese Mittelständler zu leichten Zielen für Cyberattacken werden.

Erfreulicherweise ist der Faktor Mensch im Mittelstand zum großen Teil bei der Abwehrstrategie berücksichtigt, um Anwenderfehler nicht zu Angriffsvektoren eskalieren zu lassen. Ansonsten basieren viele Abwehrkonzepte erwartungsgemäß auf einem Virenschutz und regelmäßigen Backups. Diese scheinen dazu zu führen, dass viele Unternehmen im G DATA Business IT-Security Barometer noch keine Schäden durch Ransomware zu verzeichnen hatten, falls dies aber der Fall war, wurden Maßnahmen ergriffen, um die Abwehrstrategie nachzubessern.

Als überraschend erwies sich, dass die Wenigsten über einen Notfallplan für den Fall von erfolgreichen Angriffen verfügen – hier besteht bei einigen Mittelständlern noch Nachholbedarf. Dagegen scheint sich aber die Implementation eines umfangreichen IT-Sicherheitskonzept im Mittelstand weitgehend durchgesetzt zu haben, wodurch ein umfassender IT-Schutz überhaupt erst möglich wird.

Ein besonders wichtiges Thema für den deutschen Mittelstand ist die Frage, wo die vom IT-Sicherheitsanbieter erhobenen und verarbeiteten Daten verbleiben. Die deutliche Mehrheit der deutschen Mittelständler empfindet es als wichtig oder sehr wichtig, dass diese in Deutschland bleiben und entscheidet sich hiermit für den deutschen Datenschutz und vertrauensvolle Anbieter.

Über G DATA

IT Security wurde in Deutschland erfunden: Die G DATA CyberDefense AG gilt als Erfinder des AntiVirus. Das 1985 in Bochum gegründete Unternehmen hat vor mehr als 30 Jahren das erste Programm gegen Computerviren entwickelt. Heute gehört G DATA zu den weltweit führenden Anbietern von IT-Security-Lösungen.

Testergebnisse beweisen: IT Security „Made in Germany“ schützt Internetnutzer am besten. Seit 2005 testet die Stiftung Warentest Internet Security-Produkte. In allen zehn Tests, die von 2005 bis 2017 durchgeführt wurden, erreichte G DATA die beste Virenerkennung. In Vergleichstests von AV-TEST demonstriert G DATA regelmäßig beste Ergebnisse bei der Erkennung von Computerschädlingen. Auch international wurde G DATA Internet Security von unabhängigen Verbrauchermagazinen als bestes Internetsicherheitspaket ausgezeichnet – u. a. in Australien, Belgien, Frankreich, Italien, den Niederlanden, Österreich, Spanien und den USA.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G DATA Security-Lösungen sind weltweit in mehr als 90 Ländern erhältlich.

G DATA ist Lösungspartner der Microsoft Cloud Deutschland und ist als einziger Antiviren-Hersteller mit einer speziell auf die Azure-Architektur abgestimmten Managed Endpoint Security vertreten. Weitere Informationen zum Unternehmen und zu G DATA Security-Lösungen finden Sie unter www.gdata.de.