



# BOARDROOM

## INSIDER COMMUNITY



# Schutz von Marke und Umsatz:

Reduzierung von Bots und  
Missbrauch während der gesamten  
Customer Journey

# Vorwort

**Haben Sie das Gefühl, dass Scraper in letzter Zeit zu einem großen Problem geworden sind? Dann haben Sie recht. Nach der Pandemie sind Scraper-Bots, die Einzelhändler im Visier haben, schwerer zu erkennen – und komplexer – geworden. Sie sammeln Daten, um sie auf Kosten Ihrer Marke auszunutzen und zu monetarisieren.**

Doch viele Führungskräfte sind sich der fatalen Auswirkungen von Scraper-Bots auf die Website-Performance, die Datensicherheit und den Umsatz des Unternehmens nicht bewusst oder unterschätzen sie. Während SEO-Scraper-Bots die Platzierung in Suchmaschinen verbessern können, werden Scraper-Bots mit schändlicheren Absichten eingesetzt, um Ihre Preise zu unterbieten, begrenzte Bestände zu verknappen und gefälschte Websites zu erstellen, um Kundeninformationen zu stehlen. Aus diesem Grund ist eine stärkere Sensibilisierung – und Zusammenarbeit zwischen den Teams für digitale Medien, Marketing, Betrug und Sicherheit – erforderlich, um nicht nur die Marke, sondern auch den Gewinn zu schützen.

In diesem Bericht wird erläutert, inwiefern viele Bereiche Ihres Einzelhandelsunternehmens profitieren werden, wenn Sie Scraper von Ihrer Website entfernen. Sie können sich nicht vor etwas schützen, das Sie nicht sehen können. Wenn Sie die Scraper losgeworden sind, sind Sie besser darauf vorbereitet, Ihr Umsatzpotenzial zu maximieren und den Kaufweg Ihrer Kunden zu optimieren.

**Susan McReynolds**

**Global Industry Strategist, Commerce, bei Akamai**



# Einführung

Bot-Angriffe auf Einzelhändler nehmen zu. Phishing-Kampagnen, die sich an Einzelhändler richten, ebenso. Insgesamt sind Scraping, Treue- und Zahlungskartenbetrug in der zweiten Jahreshälfte 2023 um über [700 %](#) angestiegen. 60 % der E-Commerce-Händler und 53 % der Einzelhändler verzeichneten einen [Anstieg](#) der Betrugsrate insgesamt. Digitale Kanäle waren für [52 %](#) der gesamten Betrugsverluste in der EMEA-Region verantwortlich und übertrafen damit erstmals physische Betrugsfälle, da digitale Transaktionen anonym sind.

Das Ergebnis? Im vergangenen Jahr stiegen die Verluste aus betrügerischen Einzelhandelsaktivitäten in der gesamten EMEA-Region an und beliefen sich in Großbritannien auf [11,3 Milliarden Pfund](#) und auf [15 Milliarden Euro](#) in Spanien. 94 % der Online-Shops in Deutschland waren von Betrug betroffen, wobei 20 % von ihnen Verluste von über 100.000 EUR erlitten.

Dies ist nicht nur ein Sicherheitsproblem, sondern eine Herausforderung für die IT, die CTOs und CIOs lösen müssen. Es handelt sich um ein Problem der Geschäftsoptimierung. Insbesondere für führende Marken- und Marketingfachleute im Einzelhandel kann Online-Missbrauch den Traffic rund um Produktdaten, Website und Interaktion verzerren und sich auf Strategie und Budgets sowie auf den hart erkämpften Ruf und das Vertrauen auswirken. Und die Auswirkungen auf das Wachstum können verheerend sein.

Dies ist eine unternehmenskritische Herausforderung, mit dem gleichen ultimativen Ziel, die Customer Journey zu verbessern und die Kundenbindung zu erhöhen. In diesem neuen Zeitalter des Online-Betrugs müssen Teams Silos auflösen und funktionsübergreifend an diesem Problem arbeiten.


**[Susan McReynolds, Global Industry Strategist, Commerce, bei Akamai](#), erklärt: „Um die Customer Journey, Ihre Gewinne, die Marke und den Umsatz zu schützen, müssen alle Beteiligten die Auswirkungen während der gesamten Auftragsabwicklung verstehen.“**

Dieser Bericht enthält folgende Informationen:

- Wie sich digitale Bedrohungen im Einzelhandel in Folge der Pandemie verändert haben
- Warum Einzelhändler jetzt handeln müssen
- Aktuelle und neue Betrugstrends
- Ihre Auswirkungen auf Marke und Umsatz
- Wie diese Herausforderungen bewältigt werden können



# Abschnitt 1: Wie sich Bots verändert haben – und warum dies so wichtig ist

 Während der COVID-19-Pandemie führte die zunehmende Abhängigkeit von digitalen Plattformen (sowohl aus der Sicht der Unternehmen als auch der Verbraucher) zu einer Vielzahl neuer Schwachstellen, die die Betrugslandschaft im Einzelhandel grundlegend verändert haben. Wie? Angreifer haben es immer auf Geld abgesehen. Und während der Pandemie fanden Sie dies, mehr als je zuvor, im Internet.

Die noch nie dagewesene Nachfrage nach bestimmten Produkten wie Toilettenpapier, Desinfektionsmitteln, Babynahrung und Trainingsgeräten für zu Hause eröffnete Bot-Betreibern lukrative Möglichkeiten, diese Bedingungen auszunutzen. [Scraper-Bots](#) horten beispielsweise stark nachgefragte Artikel, um sie dann zu überhöhten Preisen weiterzuverkaufen. Dabei profitieren sie von Engpässen und der hohen Nachfrage der Verbraucher.

Bis zu diesem Zeitpunkt verursachten Scraper-Bots keinen größeren Schaden und waren ziemlich leicht zu erkennen. Dadurch konnten sie mit herkömmlichen Sicherheitstools einfacher bekämpft werden. Aber da sie der erste Schritt bei einem Angriff zum Horten von Beständen waren und dieses Horten so rentabel war, entschieden sich Bot-Betreiber, erhebliche Ressourcen zu investieren, um Scraper schwerer erkennbar zu machen.

Gleichzeitig schufen Fortschritte im Bereich maschinelles Lernen und KI perfekte Bedingungen für Angreifer, um ihr Ziel zu erreichen. Außerdem wurde die Fähigkeit verbessert, mehrere Angriffe gleichzeitig zu starten und dabei ausgeklügelte Techniken zum Erschweren der Erkennbarkeit wie rotierende IP-Adressen und Proxys einzusetzen, um herkömmliche Bot-Erkennungssysteme zu umgehen. [Richard Meeus, Director of Security Technology and Strategy EMEA bei Akamai](#), erläutert: **„Bots werden immer intelligenter. Sie können einen Menschen genau nachahmen und sich ein- und ausklinken, bevor man etwas davon mitbekommt. Dadurch sind sie schwerer zu erkennen und zu bekämpfen. Außerdem greifen sie in großen Mengen und aus Tausenden von verschiedenen Orten an. Kein Einzelhändler ist dagegen gewappnet.“**

Der durch die Pandemie verursachte astronomische Anstieg der Online-Transaktionen (der Anteil der weltweiten Online-Einzelhandelsverkäufe am Gesamtumsatz des Einzelhandels stieg 2020 durchschnittlich von 16 % auf [19 %](#)) führte auch zu einer Zunahme direkter Betrugsarten wie z. B. Kontoübernahmen (Account Takeover, ATO) und Phishing-Angriffe zum Diebstahl vertraulicher Daten. Einzelhändler hatten Schwierigkeiten, legitime Kundeninteraktionen von schädlichen Bot-Aktivitäten zu unterscheiden – und Cyberkriminelle nutzten diese Schwächen im Technologie-Stack des Einzelhandels aus.

Leider bleiben diese Anfälligkeiten bis heute bestehen. Einzelhändlern fällt es schwer, mit der Entwicklung des digitalen Betrugs und Missbrauchs Schritt zu halten, die schneller fortschreitet als je zuvor. Und angesichts des Wachstums des globalen E-Commerce – etwa 22 % des weltweiten Einzelhandelsumsatzes im Jahr 2024, der bis 2026 voraussichtlich auf [27 %](#) ansteigen wird – liegt es in der Verantwortung der Einzelhändler, die wachsende Zahl legitimer Online-Kunden zu schützen.

## Abschnitt 2: Wie schädliche Aktivitäten den Umsatz im Einzelhandel senken und das Vertrauen der Verbraucher untergraben

Angriffe auf Einzelhändler wirken sich grundlegend auf das Geschäftsergebnis aus. Eine kürzlich durchgeführte [Studie](#) ergab, dass den Händlern **für jeden Betrug in Höhe von 1 US-Dollar Kosten von durchschnittlich 3 US-Dollar entstehen**. Die jüngsten [Zahlen](#) aus dem Jahr 2023 zeigen, dass die Gesamtkosten für Betrug im E-Commerce weltweit **48 Milliarden US-Dollar übersteigen**. Im Jahr 2022 waren es noch **41 Milliarden US-Dollar**. Die kumulierten [Verluste](#) im Zusammenhang mit Online-Zahlungsbetrug werden weltweit auf über **343 Milliarden US-Dollar** ansteigen. Diese Summe entspricht mehr als dem Dreifachen des Nettoeinkommens von Apple im Jahr 2023.



Und das sind nur die offensichtlichen finanziellen Auswirkungen – der Verlust von Wettbewerbsvorteilen, die Schwächung des Markenwerts, der Loyalität und des Vertrauens sind noch nicht eingerechnet (und wohl wesentlich kostspieliger). Wie und wo manifestiert sich das im Unternehmen?

### Die Rolle von Scraping bei der Untergrabung von Preisstrategien und Exklusivität

Scraping – das Auslesen von Daten auf Websites durch automatisierte Bots – stellt eine erhebliche Bedrohung für die Marken, Preisstrategien und die Produktexklusivität der Einzelhändler dar. Viele Einzelhandelsunternehmen wissen nicht einmal, dass sie ein Scraping-Problem haben – oder noch schlimmer, sie wissen nicht, welche Auswirkungen diese Art von Aktivität auf das Unternehmen hat.

## Hier sind sechs Möglichkeiten, wie Scraping Ihrem Unternehmen schaden kann:

### 1. Preisüberwachung und Preisunterbietung

Wettbewerber können mit Scraping-Bots die Preisinformationen eines Einzelhändlers kontinuierlich überwachen. Mit diesen Daten können sie die Preise des Einzelhändlers unterbieten. Dann ist es schwierig, einen Wettbewerbsvorteil aufrechtzuerhalten oder dynamische Preisstrategien effektiv umzusetzen.

### 2. Wettbewerbsnachteile

Durch die Analyse von Preis-, Produkt- und Bestandsdaten gewinnen Wettbewerber wertvolle Einblicke in die Strategien eines Einzelhändlers und können dann ihre eigene Taktik entsprechend anpassen und sich einen unfairen Vorteil verschaffen. Die Ausgangsbedingungen sind nicht mehr gleich.

### 3. Verlust von Exklusivität und Markenwert

Sie wissen, wieviel Blut, Schweiß und Tränen Ihr Marketingteam in die Erstellung von Produktbildern und -beschreibungen investiert hat. Scraping-Bots können diese und andere proprietäre Inhalte von der Website eines Einzelhändlers extrahieren. Diese gestohlenen Inhalte können dann verwendet werden, um gefälschte oder unbefugte Angebote auf Marktplätzen Dritter oder sogar auf ähnlich aussehenden Websites zu erstellen, wodurch Exklusivität und Markenwert untergraben werden.

Auf einer höheren Ebene stellt dies ein Problem für die Markenidentifizierung dar. Nicht alle, aber viele Verkäufer sind bösartig. Sie richten diese Seiten nur ein, um Kreditkarteninformationen zu stehlen. Und Ihr Kunde kennt den Unterschied nicht.

### 4. Bestandsmanipulation

Bots können Echtzeitdaten zum Bestand auswerten und Kauflimits oder Warteschlangensysteme umgehen, was

ihnen einen unfairen Vorteil gegenüber menschlichen Kunden verschafft.

Wie bereits erwähnt, ermöglicht dies Wiederverkäufern oder Scalpern, limitierte oder stark gehypte Artikel wie PlayStations, Kosmetikmarken oder Schuhe zu horten, sodass legitime Kunden keine Käufe tätigen können. Selbst wenn sie es können, werden viele dieser Wiederverkäufer den Preis um das Dreifache oder mehr erhöhen, was zu Verärgerung treuer Kunden führt.

### 5. Ungenaue Lagerbestände

Bots, die große Mengen von Produkten horten oder kaufen, können die Lagerbestände schnell aufbrauchen, was zu Fehlmengen (und enttäuschten Kunden) führt. Dies hat weitere negative Auswirkungen auf die Umsatzprognosen.

### 6. Verzerrte Marketingmetriken

Diese Bots verhalten sich wie Menschen – und Ihre Analysen spiegeln sie als solche wider, sodass Ihre Marketingdaten verzerrt werden. Bei einem Kunden von Akamai waren 90 % des Traffics Bots, was sich erheblich auf die Marketingkampagnen und die Cloudkosten auswirkte.

Christine Ross, Product Marketing Director bei Akamai, erläutert: „Kunden haben berichtet, dass ein Produkt ständig auf ihrer Website angeklickt wird. Sie gingen davon aus, dass das Produkt einfach beliebt sei. Tatsächlich aber steckten Bots dahinter und keine Kunden. Um der Nachfrage gerecht werden zu können, kauften sie mehr von diesem Produkt. In Wirklichkeit wurde es aber nicht gekauft. Die Seite wurde nicht von echten Menschen aufgerufen. Dies wirkte sich auf wichtige Entscheidungen zur Optimierung des Lagerbestands und der Websites aus. Und wenn Sie die Bot-Daten nicht herausfiltern können, optimieren Sie manchmal für die Bots und nicht für die Verbraucher. Dies kann den ROI im Marketing zunichtemachen und das Unternehmenswachstum behindern.“



## **Verminderte Website-Performance und ihre Auswirkungen auf die Nutzerinteraktion**

Ein weiterer Bereich, der stark betroffen ist, ist die Performance der Website – dem Fenster eines Einzelhändlers in die Welt. Bots, die Scraping durchführen oder Inventar horten, können die Website-Infrastruktur eines Einzelhändlers überlasten, was zu langsameren Ladezeiten, höheren Serverkosten und sogar zu Website-Ausfällen führt. Diese Verschlechterung der Performance wirkt sich direkt auf die Interaktion mit den Nutzern aus, da Kunden, die mit langsamen Seitenladezeiten oder Ausfallzeiten konfrontiert sind, die Website wahrscheinlich verlassen und sich möglicherweise der Konkurrenz zuwenden.

Angesichts der Tatsache, dass die durchschnittlichen Seitenaufrufe pro Kaufsitzung im Jahr 2023 mehr als 20 Seiten betrafen, was die Notwendigkeit von mehr Seiten und Inhalten für die Konvertierung verdeutlicht, wird eine leistungsfähige Website umso wichtiger. Die Frustration der Nutzer mit Websites im Einzelhandel ist real und weit verbreitet: [40 %](#) der Einkaufserlebnisse sind betroffen. Dies steht in direktem Zusammenhang mit der Konversion – und kostet Einzelhändler fast 0,60 US-Dollar pro Besuch an verschwendeten Ausgaben.

Ein schlechtes Nutzererlebnis ist auch Gift für die Kundenbindung. Wiederkehrende Kunden bedeuten einen viermal höheren Absatz als neue Kunden und kommen seltener über bezahlte Kanäle. Wenn Sie ein Marketingleiter sind, der mit einem knappen Budget zu kämpfen hat, ist dies ein wichtiger Punkt.

## **Kompromittierte Konten und die damit verbundenen Finanz- und Reputationskosten**

Botgesteuerte Credential-Stuffing-Angriffe und Phishing-Kampagnen können zu kompromittierten Kundenkonten führen, die besonders schädlich sind. Diese gestohlenen Anmeldedaten können dann für Kontoübernahmen, Identitätsdiebstahl oder sogar Datenschutzverletzungen verwendet werden – all dies betrifft die Finanzen und Sicherheit der Kunden, und die Schuld liegt ganz klar bei Ihnen.

Aus der Sicht eines Einzelhändlers kann der unbefugte Kontozugriff sofort zu betrügerischen Bestellungen und Rückbuchungen, zum Diebstahl von Treuepunkten, zum Missbrauch von Gutscheinen/Werbeaktionen, zum Wiederverkauf von Konten und CVV-Validierungsangriffen führen – um nur einige Beispiele zu nennen. Zu den langfristigen Folgen der Kontoübernahme gehören der Ersatz von Kundenvermögen, potenzielle Geldstrafen, ein vermindertes Markenvertrauen, erhöhte Kosten für Betrugsuntersuchungen und Burnout in Betrugs-, Sicherheits- und Marketingteams.

Bei Datenschutzverletzungen fallen unter anderem finanzielle Kosten für die Behebung an:



### **Erhöhte Betriebskosten**

(z. B. Sicherheit, Compliance oder sogar, wie bei [Neiman Marcus](#) im Jahr 2021, die Einrichtung eines speziellen Callcenters, um entsprechende Kundenbeschwerden zu melden).



### **Erstattungen und Kreditüberwachung**

für betroffene Kunden (ein Beispiel hierfür ist Hudson Bay, das 2018 Services zum Identitätsschutz von Kunden anbot).



### **Gerichtsgebühren und Abrechnungen**

Nach einem [Verstoß](#) gegen den Schutz von Zahlungskarteninformationen im Jahr 2013 musste der Einzelhandelsriese Target eine Reihe von Klagen im Gesamtwert von fast [300 Millionen US-Dollar](#) beilegen. Die Auswirkungen auf das Wachstum waren gravierend: Die Gewinne von Target gingen im vierten Quartal des Jahres im Vergleich zum Vorjahr um fast 50 % zurück, und der Aktienkurs fiel über die nächsten zwei Monate um 9 %.



### **Bußgelder und Ermittlungen**

Im Fall von Target leitete das Justizministerium eine Untersuchung ein. Als bei [Dixons Carphone](#) 2018 die Daten von 14 Millionen Kunden kompromittiert wurden, verhängte das Information Commissioner's Office die Höchststrafe von 500.000 britischen Pfund.





Die Reputationskosten von kompromittierten Konten und Verstößen beeinflussen auch das Gesamtwachstum. 54 % der Kunden geben an, dass sie zu einer anderen Marke wechseln würden, wenn bei der verwendeten Marke eine Datenschutzverletzung auftritt. Börsennotierte Unternehmen erleiden nach einem Verstoß einen durchschnittlichen Kursverlust von [3,5 %](#). Im Falle von Dixons Carphone führten rückläufige Gewinne zur Schließung von 100 Carphone Warehouse-Filialen innerhalb


eines Jahres und zum vollständigen Ende der Marke Carphone Warehouse bis 2020.

Kompromittierte Konten sind ein wichtiger Faktor für Kundenwahrnehmung, Vertrauen und Loyalität, die Marken- und Marketingverantwortliche erreichen wollen. So lag beispielsweise die Verbraucherwahrnehmung von Target vor dem Vorfall bei [20,7](#) im Brand Index Buzz Rating und sank im Jahr darauf auf ein Tief von 9,4. Fünf Jahre später lag die Zahl bei 17,3 und verdeutlichte die ungeheuren Anstrengungen, um ihr Ansehen bei den Verbrauchern wiederzuerlangen. In der heutigen vernetzten, von sozialen Medien gesättigten Umgebung kann die Markenwahrnehmung innerhalb von Minuten entschieden werden.

Das veränderte Verbraucherverhalten in Verbindung mit der Krise der Lebenshaltungskosten hat auch die Loyalität der Verbraucher erschüttert. Vertrauen, ein Tor zur Loyalität, ist der Schlüssel, um die nächste Generation von Verbrauchern zu gewinnen und nachhaltiges Geschäftswachstum zu fördern. Millennials und die Generation Z haben das [geringste Markenvertrauen](#). Vielleicht ist dies auf die Tatsache zurückzuführen, dass etwa [20 %](#) der Befragten von einer Kompromittierung ihrer Daten in der Vergangenheit wissen (im Vergleich zu 2 % der Gen X und 10 % der Babyboomer).

Daher erfordert diese Vertrauensbildung schnelle, reibungslose und betrugssichere Erlebnisse. Käufer sind bereit, bei einem Händler, dem sie vertrauen, 46 % mehr zu zahlen. Was ist der größte Faktor, um dieses Vertrauen zu gewinnen? Ein sicherer Bestellprozess und der Schutz personenbezogener Daten. Laut einer globalen [Studie](#) aus dem Jahr 2023 geben fast 90 % der Verbraucher an, dass dies für Einzelhändler von entscheidender Bedeutung ist, um dieses Ziel zu erreichen. Auch der gute Ruf der Marke steht mit 76 % ganz oben auf der Liste.

# Fazit: Bekämpfung von Bots und Missbrauch durch organisatorische Ausrichtung

 Angesichts der zunehmenden Verbreitung dieser schädlichen Technologien kann sich dies wie eine weitere riesige Herausforderung anfühlen, die es zu bewältigen gilt. Das muss aber nicht sein. Die gute Nachricht ist, dass es effektive Möglichkeiten gibt, Ihre Marke in Ihrer Kontrolle zu behalten und Ihre Customer Journey zu verbessern. Aber wo sollen Sie anfangen?


## Strategien zum Schutz Ihrer Marke – und Ihres Geschäftsergebnisses

In der Regel konzentrieren sich verschiedene Teams auf den Schutz verschiedener Ergebnisse: Das Sicherheitsteam schützt Daten, das Marketingteam schützt Umsätze, das IT-Team schützt vor Ausfällen, das CX-Team schützt den Kaufweg des Kunden. Diese Teams müssen jedoch mehrere Herausforderungen bewältigen:

- *Kommunizieren sie auf derselben Seite über gemeinsame Geschäftsergebnisse und -ziele?*
- *Können sie folgende Frage beantworten: „Sind die Stakeholder auf die technischen Anforderungen und Tools zum Schutz der Kundendaten, der Marke und des Umsatzes abgestimmt?“*

Meist stellen wir fest, dass die Antwort „nein“ lautet. Dies ist aber von entscheidender Bedeutung. Weitere wichtige Fragen, die diese Teams gemeinsam beantworten müssen, sind:

- *Welche Ergebnisse wollen wir erreichen (z. B. Schutz von Umsätzen, Kundendaten, Kaufweg, Betrug)?*
- *Benötigen wir eine oder mehrere Lösungen, um verschiedene Herausforderungen und Anwendungsfälle von Stakeholdern zu lösen?*
- *Gibt es eine Kluft zwischen dem Käufer der Lösung und dem, der sie tatsächlich verwendet?*
- *Worin besteht der Erfolg? Haben wir klar definierte KPIs?*
- *Was sind wir bereit zu tolerieren/welche Kompromisse müssen getroffen werden, um die Sicherheit mit der Optimierung des Kaufwegs in Einklang zu bringen?*
- *Schützen wir unser gesamtes Vermögen (Website, mobile App, APIs und Infrastruktur)?*
- *Wie gehen wir mit der gewünschten, unerwünschten und unscharfen Grenze zwischen den beiden um?*

 **Jedes Team muss diese Punkte verstehen und ein gemeinsames Ziel haben, das die Ausrichtung und das Handeln fördert, um optimale Ergebnisse für das Unternehmen zu erzielen.**

Der Betrug im Einzelhandel nimmt rasant zu und hat weitreichende Auswirkungen auf die Einzelhändler. Wie bereits erläutert, gehen die Verluste über direkt zu erkennenden Posten wie Bußgelder, Abrechnungen oder Gerichtsgebühren hinaus. Sie wirken sich direkt auf das ultimative Ziel des Einzelhändlers aus, den Umsatz durch Marken- und Kundentreue zu steigern. Marke und Loyalität hängen von Vertrauen und Kundenerlebnis ab – Faktoren, die durch betrügerische Aktivitäten im Handumdrehen verloren gehen.

Die Zunahme des Missbrauchs in Verbindung mit einer schwierigen Kauflandschaft und dem stetigen Anstieg der Online-Verkäufe machen es für Einzelhändler wichtiger denn je, fortschrittliche Sicherheitsmaßnahmen zum Schutz ihrer Marke und ihrer Kunden zu priorisieren und in diese zu investieren. Das bedeutet, dass Geschäftsbereiche zusammenarbeiten müssen, um die Auswirkungen schädlicher Angriffe zu verstehen und gemeinsam zu nutzen, da sie nicht mehr nur den Sicherheits- und IT-Teams vorbehalten sind.

Wenn Sie Unterstützung benötigen, [wenden Sie sich an das Akamai-Team](#), oder erfahren Sie mehr über [Lösungen für Einzelhandel, Reisen und Gastgewerbe](#). Akamai [unterstützt globale Einzelhändler und Marken](#) wie [Lufthansa](#), die [Wagner eCommerce Group](#), [Panasonic](#) und [TOUS](#) seit mehr als 25 Jahren dabei, sichere und ansprechende Online-Erlebnisse zu bieten.



## Über Akamai

Akamai unterstützt und schützt das digitale Leben. Führende Unternehmen weltweit setzen bei der Erstellung, Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai. So unterstützen wir täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. [Akamai Connected Cloud](#), eine stark verteilte Edge- und Cloud-Plattform, bringt Anwendungen und Erlebnisse näher an die Nutzer und hält Bedrohungen fern. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter [akamai.com](#) und [akamai.com/blog](#) oder folgen Sie Akamai Technologies auf [X](#) (ehemals Twitter) und [LinkedIn](#).



**Dieses Whitepaper wurde in Zusammenarbeit mit Retail Gazette, der größten B2B-Publikation Großbritanniens, veröffentlicht.**

Besuchen Sie [www.retailgazette.co.uk](#), und schließen Sie sich 300.000 weiteren monatlichen Nutzern an, die kostenlos auf die neuesten Nachrichten, Interviews, Analysen, ausführlichen Berichte und Whitepaper zugreifen können.

