



5 BEST PRACTICES:

Die bestmögliche Vorbereitung Ihrer E-Commerce-Website auf ein erfolgreiches Feiertagsgeschäft

Exklusive Cloudflare-Daten vom Cyber Weekend 2019 mit bewährten Vorgehensweisen zur Verbesserung der Websiteperformance und -sicherheit – damit Ihre Website während und außerhalb des Feiertagsgeschäfts noch mehr Gewinn abwirft

Inhalts- verzeichnis

Neue Bedingungen für das Feiertagsgeschäft im Online-Handel	3
Best Practice 1: Kundenerfahrung insbesondere auf Mobilgeräten optimieren	5
Best Practice 2: Machen Sie Ihren Traffic-Anstieg am Cyber Weekend katastrophensicher.....	8
Best Practice 3: Stärken Sie Ihre Verteidigung gegen DDoS-Angriffe.....	12
Best Practice 4: Bot-basierte Kontoübernahmen verhindern.....	14
Best Practice 5: Schützen Sie Ihre Website, Ihre Kunden und Ihre Marke	16
Wie Cloudflare zu sorgenfreiem E-Commerce im Weihnachtsgeschäft beitragen kann	18
Quellen	19

Neue Bedingungen für das Feiertagsgeschäft im Online-Handel

Das Cyber Weekend 2019 hat mit Rekordumsätzen von über 28,4 Milliarden US-Dollar in den USA und bis zu 90 Milliarden US-Dollar weltweit den Online-Handel in Festtagslaune versetzt. ¹

An Herausforderungen herrschte allerdings auch kein Mangel. An diesem Cyber Weekend waren Online-Händler mit steigendem Wettbewerbsdruck, höheren Erwartungen der Verbraucher und wachsenden Sicherheitsanforderungen konfrontiert – was Sie bei Ihrer Planung für 2020 berücksichtigen sollten.

Eine Goldgrube wird mobil

Auf der einen Seite bieten allein Mobilgeräte bereits eine Fülle von Möglichkeiten.

An Thanksgiving entfielen 63 % des Website-Traffics und 45 % aller Käufe auf Mobilgeräte, gegenüber 24 % im Vorjahr.² Am Cyber Monday überschritten die Käufe per Smartphones erstmals die Marke von 3 Milliarden US-Dollar – eine beeindruckende Steigerung um 46 % verglichen mit 2018.³

Eine Wettbewerbslandschaft im rasanten Wandel

Trotz aller frohen Botschaften aus dem diesjährigen Feiertagsgeschäft entfiel 2019 immer noch fast die Hälfte aller E-Commerce-Einnahmen in den USA auf Amazon.

Und inzwischen ist Amazon auch nicht mehr allein. Im Jahr 2019 hat der chinesische E-Commerce-Riese Alibaba in nur 24 Stunden 38 Milliarden US-Dollar umgesetzt⁴ – und damit die Gesamteinnahmen der in den USA ansässigen Händler von Thanksgiving bis zum Cyber Monday weit in den Schatten gestellt.

Um sich gegen solche Konkurrenz zu behaupten, müssen Händler elegantes und müheloses Einkaufen ermöglichen, unterstützt durch optimal geschützte Cloud-, Handels- und Logistikfunktionen.

Weiter >>

2 x

Höhere Spitzen beim Website-Traffic während des Cyber Weekends 2019

↑ 12,2 %

Zunahme der Zahlungsinteraktionen für Online-Händler innerhalb des Cloudflare-Netzwerks, Black Friday 2019 vs. 2018

↑ 5,9 %

Zunahme der Zahlungsinteraktionen für Online-Händler innerhalb des Cloudflare-Netzwerks, Cyber Monday 2019 vs. 2018

Quelle: Cloudflare

Die zunehmende Bedrohung durch Cyberkriminalität

Leider sind die Händler nicht die einzigen, die während des Feiertagsgeschäfts die Kasse klingeln hören möchten. Cyberdiebe haben es darauf abgesehen, mit erbeuteten Anmeldeinformationen Kundenkonten für illegale Einkaufsbummel zu kapern.

In den USA übersteigen die Verluste aus Kontoübernahmen inzwischen 4 Milliarden US-Dollar pro Jahr.⁵ Weltweit könnte der Zahlungsbetrug im Jahr 2020 die Marke von 30 Milliarden Dollar sprengen.⁶ Hacker, die zur Erbeutung von Kreditkarteninformationen Malware in Websites einspeisen, dürften im laufenden Jahr eine große Bedrohung für den Einzelhandel sein.⁷

Bei der Abwehr kommt es aber auf das richtige Maß an. Der Anteil der Warenkorbabbrüche liegt ohnehin bereits bei mindestens 70 %. Daher müssen Händler neue Wege zur Stärkung ihrer Verteidigung finden, ohne die Hürden für den Kunden zu erhöhen.



Best Practices für ein erfolgreiches Feiertagsgeschäft

In diesem Bericht stellt Cloudflare Strategien vor, mit denen sich die Herausforderungen bei der Vorbereitung von E-Commerce-Websites auf wichtige Termine meistern lassen – sei es eine eintägige Verkaufsaktion oder das Feiertagsgeschäft.

Viele der verwertbaren Erkenntnisse in diesem E-Book basieren auf Cloudflare-Daten vom Black Friday bis zum Cyber Monday 2019, Branchentrends und den Erkenntnissen führender Online-Händler innerhalb des globalen Cloudflare-Netzwerks.

Um diese Best Practices zu ermitteln, hat Cloudflare vom 29. November bis Montag, den 2. Dezember 2019, den Datenverkehr auf E-Commerce-Websites gemessen, die über das HTTP Archive identifiziert und vom globalen Cloudflare-Netzwerk unterstützt wurden.

Unter Verwendung vollständig anonymisierter Daten aus diesen referenzierbaren Domains über das HTTP Archive untersuchten wir die täglichen Seitenaufrufe und die sich daraus

ergebenden Zahlungsinteraktionen sowie Cyberangriffe und andere Bedrohungen, die an den Einkaufstagen mit der größten Aktivität des Jahres innerhalb des Netzwerks identifiziert und bekämpft wurden.

Dadurch konnten wir Einblicke in die Faktoren gewinnen, die sich nachweislich am negativsten auf die Performance auswirken, sowie in die Abwehrstrategien, die sich für die Händler in unserem Netzwerk als wirksam erwiesen haben.

Durch die Kombination unserer Ergebnisse mit einer Trendforschungsübersicht aus Drittquellen konnten wir unsere Analyse in einen breiteren Kontext stellen. Aus den Ergebnissen haben wir 5 Best Practices für ein erfolgreiches Online-Feiertagsgeschäft im Jahr 2020 und darüber hinaus entwickelt.

ÜBER CLOUDFLARE

Cloudflare ist ein führender Spezialist in Sachen Sicherheit, Performance und Störungsfreiheit mit dem erklärten Ziel, das Internet besser zu machen.

Unsere integrierte Cloud-Plattform, die das Vertrauen von über 25 Millionen Internetwebsites genießt, hilft Marken und Händlern, die Performance ihrer Websites zu verbessern und gleichzeitig Kundendaten und Transaktionen zu schützen.

- Über 190 Städte und mehr als 90 Länder umfassendes Netzwerk
- 99 % der Internetbenutzer in Industrieländern werden innerhalb von 100 Millisekunden erreicht
- Täglich durchschnittlich 50 Milliarden Cyber-Bedrohungen im 4. Quartal 2019 blockiert
- 35 Tbit/s Gesamtnetzwerkcapazität



BEST PRACTICE 1

Kundenerfahrung insbesondere auf Mobilgeräten optimieren



Laut PwC shoppen 54 % der Käufer in der Feiertagszeit lieber bequem über ihr Smartphone, ihren Computer und sogar über einen Sprachassistenten wie Alexa, als ein Geschäft aufzusuchen.⁸

Im Jahr 2019 wurde fast die Hälfte aller Online-Verkäufe während des Feiertagsgeschäfts über Mobilgeräte abgewickelt. Am Black Friday wurden nicht weniger als 64 % aller Zahlungstransaktionen über ein Mobilgerät eingeleitet.⁹ Im Jahr 2021 könnten bis zu 72,9 % aller Online-Käufe auf diesem Weg getätigt werden.¹⁰

Kurz gesagt: Mobilgeräte sind zum wichtigsten Motor für E-Commerce-Wachstum geworden. Aber Vorsicht: Da immer mehr Verbraucher (und Wettbewerber im Einzelhandel) auf Mobilgeräte setzen, wird die Kundenerfahrung über die Gewinner und Verlierer im E-Commerce entscheiden. Mit den folgenden Maßnahmen können Sie die Möglichkeiten des mobilen Verkaufskanals voll ausschöpfen.

Weiter >>

► Weniger Latenz, mehr Konversionen

Für mobile Kunden bestimmt der visuelle Inhalt das Einkaufserlebnis, genau wie auf dem Desktop. Scharfe Produktbilder, 3D-Darstellungen, stabile Produktvideos und Aufsehen erregende visuelle Handelsfeatures wie VR- und AR-Simulationen können dazu beitragen, das Interesse zu wecken und das Kaufvertrauen zu stärken. Sie können auch zu einem Anstieg der Warenkorbwerte um 60–70 % führen.¹¹ Eine hohe Latenz hingegen kann Ihr Geschäft deutlich beeinträchtigen.



Eine Reihe von Faktoren dämpft das Kundeninteresse an visuellen Inhalten und Handelsfeatures erheblich, entweder durch erhöhte Latenzzeiten oder andere Performanceprobleme. Um die Vorteile von visuellen Inhalten und Handelsfeatures bestmöglich auszuschöpfen, sollten Händler Folgendes berücksichtigen:

- ▶ Optimieren Sie Gerätetypen und Netzwerkkonnektivität, um Performanceeinbußen zu minimieren
- ▶ Vermeiden Sie das Einbetten von Videodateien in Formaten wie MP4 und MOV, da diese zu längeren Ladezeiten führen
- ▶ Setzen Sie Content Delivery Networks mit erweiterten Komprimierungs- und Cache-Funktionen ein

“ Wir registrieren größere Flexibilität und höhere Reaktionsfähigkeit beim Support, aber auch höhere Einsatzfähigkeit ...
Unsere Homepage lädt viel schneller.“

Karan Tewari Manager, Platform Engineering

falabella

(FALLSTUDIE LESEN)

Weiter >>

► Den richtigen Mittelweg zwischen dynamischen Features und Performance-Anforderungen finden

Dynamische Webseiten und KI-gestützte Features, die relevante Seiteninhalte und vorausschauende Produktempfehlungen präsentieren, spielen für den Erfolg von E-Commerce-Websites eine immer wichtigere Rolle. Sie verbessern nicht nur das Käuferlebnis, sondern tragen auch zu höheren Konversionsraten, stärkerer Markentreue und der Steigerung des Customer Lifetime Value bei.



Wenn Händler allerdings auf eine Personalisierung der gesamten Website setzen, sollten sie sich der damit verbundenen Auswirkungen auf die Performance bewusst sein. Seiten, die umfangreiches JavaScript oder dynamische Seiten-Assets benötigen, laden u. U. länger als vergleichbare Seiten mit statischen Bildern und ohne Personalisierung.

► Geschwindigkeit und SEO optimieren

Ob es sich um die Suche nach neuen Produkten oder um einen Kauf per Mobilgerät handelt, die sofortige Zufriedenstellung ist das A und O. Das bedeutet, dass die Händler es ihren Kunden so leicht wie möglich machen müssen, ihre Produkte über die organische Suche zu finden.



Der Mobile First Index von Google misst, wie gut Ihre Website auf Mobilgeräten funktioniert. Dies wirkt sich darauf aus, an welcher Stelle Ihr Shop in den Suchergebnissen erscheint, auch in Desktop-Versionen.

Um das Kundenerlebnis zu verbessern und gleichzeitig das aktuelle Suchmaschinenranking zu erhalten oder zu verbessern, empfehlen wir Händlern Folgendes:

- Erstellen Sie reaktionsfähige Websites mit Seiten und Bildern, die sich automatisch an die Bildschirmgröße anpassen
- Führen Sie mithilfe gängiger Online-Tools Performance-Tests zur Optimierung der Ladegeschwindigkeit von visuellen Inhalten
- Setzen Sie Google AMP zur Verkürzung der Seitenladedauer und zur Verbesserung der mobilen Nutzererfahrung ein

“Bei der Kundenkonversion spielt Geschwindigkeit eine enorm wichtige Rolle. Damit das Geschäft weiter wachsen kann, gehört es zu den Hauptzielen unseres Teams, die Geschwindigkeit und Reaktionsfähigkeit unserer Websites sicherzustellen. Mithilfe von Cloudflare ist uns das – und noch vieles mehr – gelungen.“

Andy Dean Technical Operations Manager

ALLSAINTS

(Fallstudie lesen)

BEST PRACTICE 2

Traffic-Anstieg am Cyber Weekend gegen Störungen absichern

Der Traffic für E-Commerce-Websites innerhalb des globalen Cloudflare-Netzwerks ist während des Cyber Weekends um mehr als 200 % angestiegen und hat am Black Friday mit 21,5 Millionen Seitenaufrufen seinen Höhepunkt erreicht, verglichen mit 11,3 Millionen durchschnittlichen täglichen Seitenaufrufen zu Beginn des Monats. Am Cyber Monday ging der Traffic nur leicht auf 18 Millionen Seitenaufrufe zurück.

Laut Cloudflare-Daten stieg die Anzahl der Zahlungsinteraktionen am Black Friday im Vergleich zum Vorjahr um 12,2 %, während die Zahlungsinteraktionen am Cyber Monday um fast 6 % zunahm. Die Zahlungsinteraktionen bilden die Häufigkeit ab, mit der Nutzer auf Checkout-Seiten und Warenkörbe geklickt haben. Sie werden verwendet, um die Kaufabsicht zu messen. Ob diese Transaktionen auch wirklich abgeschlossen wurden oder wie viel der Kunde gezahlt hat, verraten sie jedoch nicht.

Was die Zahlen aussagen

Vergleicht man diese Seitenaufrufe und Zahlungsinteraktionen mit öffentlich gemeldeten Umsatzzahlen im Einzelhandel, ergeben sich einige interessante Muster. Am Black Friday wurde die höchste Zahl von Online-Käufern verzeichnet, die insgesamt 7,4 Milliarden US-Dollar ausgaben.¹⁵ Am Cyber Monday gab eine kleinere Zahl an

Online-Käufern insgesamt 9,4 Milliarden Dollar aus:¹⁶ 2 Milliarden Dollar mehr, obwohl insgesamt weniger Transaktionen abgewickelt wurden. Offenbar werden also am Black Friday vor allem enorme Mengen umgesetzt, während am Cyber Monday bevorzugt höherpreisige Artikel erstanden werden.



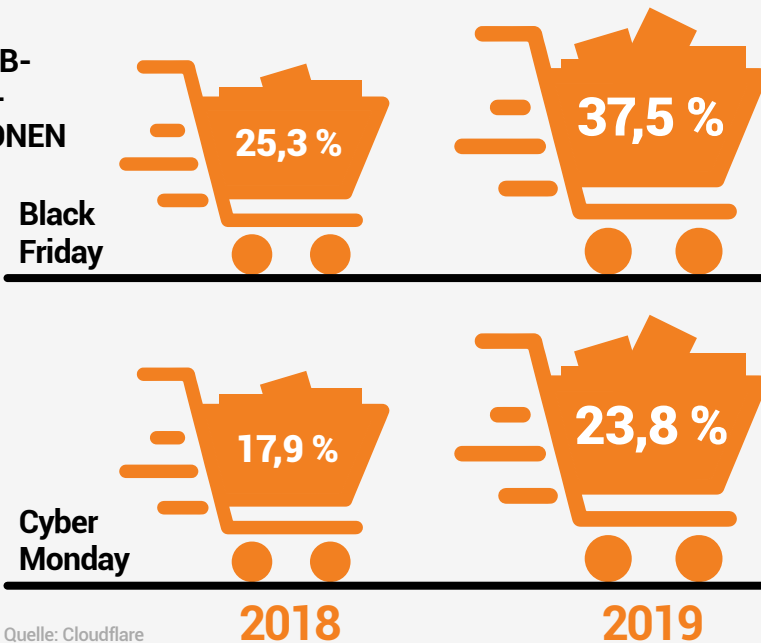
Jeder Ausfall einer Website ist eine Chance für eine andere

Diese Umsätze waren durchaus nicht gleichmäßig verteilt: Berichten zufolge gab es bei einer Reihe von Händlern Website-, Mobil- und App-Pannen, die sie Millionenbeträge kosteten. Tatsächlich musste ein großer Markeneinzelhändler eine Ausfallzeit von nicht weniger als 12 Stunden verkraften, die ihn an Thanksgiving möglicherweise 40 % seiner digitalen Verkäufe gekostet hat.¹⁷

Viele Websites waren jedoch während dieses für das Feiertagsgeschäft wichtigen Wochenendes online und funktionierten einwandfrei. Wir möchten Ihnen nun einige der umsichtigen Maßnahmen vorstellen, mit denen diese Händler und andere Marktführer die Verfügbarkeit während solcher Spitzenverkaufszeiten maximieren.

Weiter >>

WARENKORB-ZAHLUNGS-INTERAKTIONEN



Quelle: Cloudflare

► Vorausschauende Planung

Wenn Websites das mit dem Cyber Weekend verbundene erhöhte Traffic- und Transaktionsaufkommen nicht bewältigen können, werden wankelmütige Kunden ohne zu zögern auf andere Seiten abwandern. Vorausgesetzt, sie können überhaupt auf Ihre Seite zugreifen.

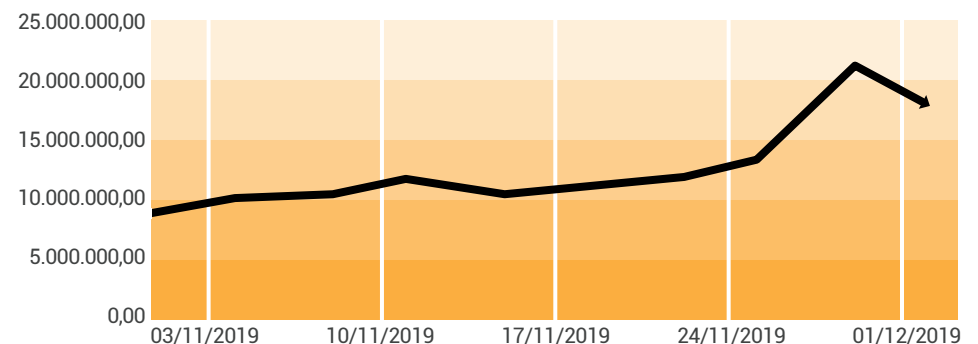


Um Ausfallzeiten und die damit verbundenen negativen Auswirkungen auf Ihren Umsatz und Ruf zu vermeiden, sollten Sie vorausschauend planen. Beginnen Sie mit der Erstellung einer Prognose Ihres Kapazitätsbedarfs auf Grundlage des Traffic- und Absatzwachstums für jedes der letzten drei bis fünf Jahre. Führen Sie dann Lasttests für interne und externe Systeme mit mindestens 200 % der von Ihnen geschätzten Spitzenbelastung durch.

[Weiter >>](#)

TÄGLICHE SEITENAUFRUFE BEI HÄNDLERN INNERHALB DES GLOBALEN CLOUDFLARE-NETZWERKS, 1. Nov. bis 1. Dez. 2019

Quelle: Cloudflare



► Verbessern Sie Ihre Infrastruktur

Ausfallzeiten bedeuten nicht nur, dass Ihre Website oder App vollständig offline geht. Möglicherweise fehlen auch Seitenelemente oder es kommt beim Bezahlvorgang zu Problemen oder Ausfällen. Wenn Käufer Transaktionen abrechnen, kann das zu jährlichen Umsatzverlusten von bis zu 4 Billionen US-Dollar weltweit beitragen.¹⁸ Wie soll da bei Kunden oder Händlern Feiertagslaune aufkommen?



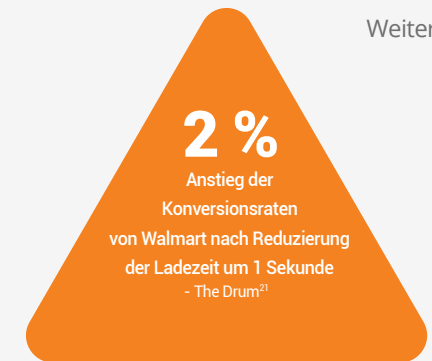
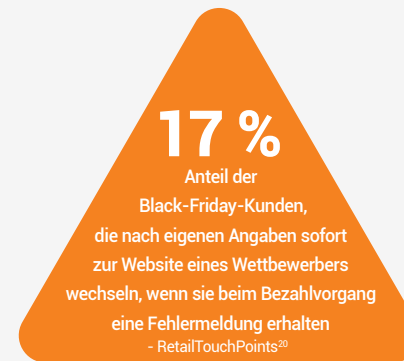
Unabhängig davon, ob Sie Server vor Ort oder in der Cloud hosten, stellen Sie sicher, dass diese die von Ihnen prognostizierte Arbeitslast auch bewältigen können. Falls Ihre Website ausfällt, müssen Sie auch dafür

gesorgt haben, dass ein Failover zu einer alternativen Seite durchgeführt werden kann. Ihr Hosting-Provider sollte Ihnen Optionen für eine Colocation-Migration von Websites bei Katastrophen oder Ausfällen bieten.

- Testen Sie die Performance für Anwendungen von Drittanbietern, die API-Verkehr auf Ihre Website leiten
- Bewältigen Sie Traffic-Spitzen mit einer Durchsatzratenbegrenzung, um eine Überlastung der Infrastruktur zu verhindern

- Verteilen Sie bei einem Serverausfall den Datenverkehr auf mehrere Seiten
- Führen Sie eine Zustandsüberwachung ein, um zu verhindern, dass der Datenverkehr zu einem ausgefallenen Server geleitet wird

Weiter >>



“Der Black Friday ist jedes Jahr einer der wichtigsten Tage für unsere Händler und 2019 hat alles bisher Dagewesene in den Schatten gestellt. Dank der Unterstützung von Cloudflare konnten wir die Nachfrage bewältigen und weltweit blitzschnell auf Käufer reagieren.“

Charles Ng Production Engineering Manager

► Erhöhen Sie auch die Cyber-Sicherheit

Vom Black Friday bis zum Cyber Monday 2019 hat sich Cloudflare allein in den USA 189 Millionen Cyber-Bedrohungen von Online-Händlern angenommen. Tatsächlich stellten die USA bei der Zahl der Angriffe die meisten anderen Regionen



in den Schatten, wobei Deutschland mit 118 Millionen bekämpften Bedrohungen die zweithöchste Angriffszahl weltweit verzeichnete. Zum Vergleich: In Großbritannien wurden 27 Millionen Bedrohungen bekämpft.

Wie die Daten zeigen, konzentrierten sich die Cyber-Bedrohungen am Cyber Weekend stark auf größere Volkswirtschaften, in denen im Dezember bedeutende kulturelle oder religiöse Feste begangen werden.

Auf den folgenden Seiten werden wir uns mit einigen der häufigsten Angriffsweisen beschäftigen, die Sicherheit, Performance und Verfügbarkeit einer Website erheblich beeinträchtigen können. Außerdem werden wir wichtige Strategien zu ihrer Bekämpfung vorstellen.

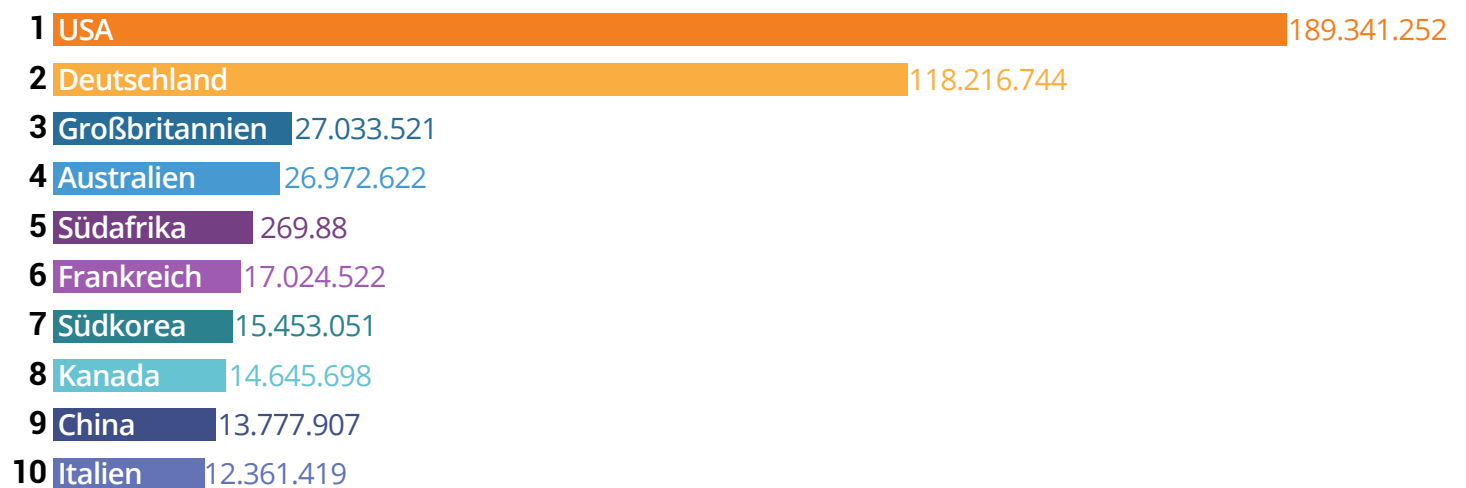
Über 189 Mio. Cyber-Bedrohungen für US-Online-Händler
Black Friday bis Cyber Monday 2019

Über 442 Mio. Cyber-Bedrohungen von Online-Händlern in den 10 am stärksten angegriffenen Ländern
Black Friday bis Cyber Monday 2019

DIE 10 AM STÄRKSTEN VON CYBER-BEDROHUNGEN BETROFFENEN LÄNDER

Black Friday bis Cyber Monday 2019

Quelle: Cloudflare



BEST PRACTICE 3

Abwehr von DDoS-Angriffen stärken

Zu einer effektiven Absicherung gehört die Vorbereitung auf einen Ansturm von DDoS-Angriffen (Distributed Denial-of-Service) durch böswillige Akteure, die versuchen, Ihre Hosting-Server offline zu bringen, indem sie sie mit Traffic von gefährdeten Geräten und Netzwerken überfluten. Im Jahr 2019 hat das globale Cloudflare-Netzwerk zwischen dem Black Friday und dem Cyber Monday zehn große DDoS-Angriffe registriert und bekämpft. Der größte dieser Angriffe erreichte bei 1,27 TB pro Sekunde seinen Höhepunkt und dauerte knapp 48 Minuten.

Ganz gleich, ob es bei solchen Angriffen darum geht, Konversionen zu verhindern, Käufer zu Wettbewerbern umzuleiten, Ihre Website zu erpressen, den Diebstahl von Kundendaten zu verschleiern oder einfach nur Ihre Marke zu schädigen – die Kunden werden die Schuld in jedem Fall bei Ihnen suchen. Um solche Situationen möglichst zu vermeiden, sollten Händler bei der Entwicklung ihrer Verteidigungsstrategie folgende Punkte berücksichtigen.

► Bereiten Sie sich auf 5G-gestützte Angriffe vor

Die höheren Geschwindigkeiten und geringeren Latenzzeiten von 5G sind ein Segen für Händler, die neue Dienste und Website-Features einführen wollen. Da durch 5G aber immer mehr Verbrauchergeräte miteinander vernetzt werden können, werden unter anderem Cyberkriminelle, skrupellose Wettbewerber und Hacktivisten versuchen, die schlechten oder oft nicht vorhandenen Sicherheitskontrollen vieler neuer Smart Devices auszunutzen.



Die schwindelerregende Menge an Traffic, die Bedrohungsakteure durch gefährdete, an das 5G-Netz angeschlossene Geräte erzeugen können, kann schnell zu einer Erschöpfung der Ressourcen innerhalb der Seiteninfrastrukturen führen und IT-Teams dazu zwingen, übermäßig viel Kapazität bereitzustellen.²² Diese Überlegungen sollten in die Prognosen zum Traffic während des Feiertagsgeschäfts einfließen.

[Weiter >>](#)

► Unterschätzen Sie die kleineren Angriffe nicht!

Branchenweiten Schätzungen zufolge spielt DDoS bei bis zu 33 % aller Cyberangriffe auf Online- und Mobilhändler eine Rolle.²³



Häufig sind diese auf der Anwendungsschicht (Schicht 7) stattfindenden Angriffe mit niedriger Geschwindigkeit genau darauf ausgelegt, unter dem Radar zu bleiben. Sie zielen auf ein oder mehrere Service-Gateways und Anwendungsebenen ab, sodass sie insgesamt weniger Traffic benötigen, um Ihre Website auszuschalten.

Doch selbst wenn der E-Commerce-Sektor das Risiko von Angriffen mit besonders hoher Bandbreite berücksichtigen muss, liegen bis zu drei Viertel der DDoS-Angriffe bei 5 Gigabit pro Sekunde (Gbit/s) oder weniger.²⁴

► Wechseln Sie zu Cloud-basierter DDoS-Abwehr

Eine Strategie zur Bekämpfung dieser Bedrohungen besteht darin, die Investitionen in Ihre bestehende Infrastruktur zu erweitern, um die durch DDoS-Angriffe verursachte Auslastung zu bewältigen.



Händler werden aber wahrscheinlich feststellen, dass traditionelle DDoS-Lösungen sich nicht ohne weiteres an die wachsende Komplexität der Angriffsmethoden anpassen können und nutzlos sind, wenn Angriffe die Netzwerkkapazität eines Unternehmens übersteigen.

Wir haben eine bessere Idee: Führen Sie eine skalierbare, Cloud-basierte Abwehrlösung ein, um Bedrohungen durch DDoS-Angriffe jeder Größenordnung und Komplexität zu

neutralisieren. Wenn Sie Ihren Shop in Betrieb halten und sich nicht den Unmut Ihrer Kunden zuziehen wollen, sollten Sie Lösungen in Betracht ziehen, die Folgendes bieten:

- Bereitstellung von Diensten am Netzwerkrand für maximale Flexibilität bei der Eindämmung sich schnell entwickelnder Bedrohungsarten
- Unbegrenzte und zeitlich unbeschränkte Abwehr, damit Ihre Website immer gegen DDoS-Angriffe jeder Art und Komplexität gewappnet ist
- Nutzung von Bedrohungsinformationen aus der ganzen Welt zum Schutz vor den ausgefeiltesten Angriffen
- Nahtlose Integration mit anderen Sicherheits-, Performance- und Analytics-Lösungen und bestehenden Geschäftsprozessen

“Mithilfe von Cloudflare erreicht unser Online-Shop seine Höchstleistung – die optimale Lösung für Website-Sicherheit und -Performance.“

Sam Wolf Gründer und CEO



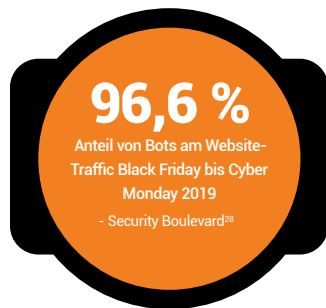
BEST PRACTICE 4

Bot-basierte Kontoübernahmen verhindern

Credential Stuffing hat im Online-Handel am Cyber Weekend Hochkonjunktur. Im Jahr 2019 starteten Cyberkriminelle eine Rekordzahl von Bot-Angriffen, bei denen sie gestohlene Anmeldeinformationen nutzten, um Kundenkonten für illegale Einkaufsumbummel zu missbrauchen.

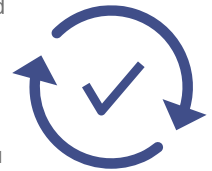
Bei einigen Händlern machten schädliche Bots unmittelbar vor dem Cyber Weekend bis zu 97 % des Site-Traffics aus.²⁵ Am Black Friday und am Cyber Monday handelte es sich bei zwei Dritteln des gesamten Traffics auf den Anmeldeseiten um Bot-basierte Kontoübernahmeversuche.²⁶

Die Gründe liegen auf der Hand. Laut eMarketer werden mit den in den Kundenprofilen gespeicherten Kreditkartendaten im Jahr 2020 weltweit Online-Einkäufe mit einem Wert von mehr als 26 Billionen US-Dollar im Einzelhandel abgewickelt werden.²⁷ Da aufgrund großer Datenlecks gestohlene Anmeldedaten immer günstiger werden, werden Online-Händler auch in Zukunft das Ziel Nummer eins für Credential-Stuffing-Bot-Angriffe bleiben, die auf illegale Einkäufe abzielen. Aber Sie können sich wehren.



►Führen Sie CAPTCHAs ein.

Die Bot-Angriffe während des Feiertagsgeschäfts sind zunehmend auch darauf ausgerichtet, sich den Hauptgewinn zu sichern: Geschenkgutscheine.



Cyberdiebe setzen Bots über Kontoübernahmen oder Gastkäufer-Anmeldungen ein, um Geschenkgutscheine mit gestohlenen Codes schnell zu validieren und sie dann entweder auf dem Schwarzmarkt zu verkaufen oder in betrügerischer Absicht Artikel zu erwerben, die sie dann online weiterverkaufen können.

Die Einführung von CAPTCHAs bei der Anmeldung kann helfen, Bot-basierte Kontoübernahmen und illegale Gastkäufer-Anmeldungen zu blockieren. Diese CAPTCHAs tauchen in Form von Fragen auf Seiten auf, auf denen Händler Bot-Traffic befürchten. Sie helfen dabei, zu ermitteln, ob es sich bei dem Nutzer um einen Menschen oder um einen Bot handelt.

Weiter >>

► Legen Sie eine Durchsatzratenbegrenzung fest

Die Durchsatzratenbegrenzung kann dabei helfen, Web Scraping zu verhindern. Ein echter Nutzer wird wahrscheinlich nicht innerhalb weniger Minuten oder Sekunden Inhalte von mehreren hundert Seiten abfragen. Bei einem solchen „Nutzer“ handelt es sich sehr wahrscheinlich um einen Bot. Im Jahr 2019 setzte Cloudflare bei der Bekämpfung von knapp 6 % aller erkannten Angriffe auf Online-Händler in den USA vom Black Friday bis zum Cyber Monday die Durchsatzratenbegrenzung ein.



► Nutzen Sie einen Bot-Management-Dienst

Damit Sicherheitsmaßnahmen wie CAPTCHA die Kundenerfahrung so wenig wie möglich beeinträchtigen, ist es außerdem ratsam, einen Bot-Management-Dienst einzurichten. Diese Cloud-basierten Dienste spüren mithilfe von fortgeschrittenem Machine Learning schädliche Bots auf und blockieren ihre Anmeldeversuche, ohne zusätzliche Hürden für die Nutzer zu schaffen. Um die besten Ergebnisse zu erzielen, sollten Sie sich für Lösungen entscheiden, die Folgendes tun:



- Sich nicht auf die Suche nach einer großen Anzahl von Zugriffsversuchen zu einem beliebigen Zeitpunkt beschränken
- Fortgeschrittenere, niederschwellige und langsam verlaufende Bot-Angriffe, die menschliches Verhalten besser nachahmen, erkennen und unterbinden
- Globale Netzwerke für Bedrohungsinformationen nutzen, damit Angriffe auf einen Händler von allen anderen erkannt und blockiert werden

Dieser eine Schritt kann sich das ganze Jahr über auszahlen. Nach Angaben von Forschern könnten Online-Händler im Jahr 2019 bis zu 10 Milliarden US-Dollar durch Bot-Angriffe eingebüßt haben, entweder durch entgangene Verkäufe, vergeudete Arbeitsstunden oder Kunden, die eine Website verlassen haben, nachdem diese nicht mehr funktionierte oder einige ihrer Funktionen nicht mehr verfügbar waren.³² Umsichtige Händler, die Bot-Management-Dienste einsetzen, werden diese Art von Verlusten im laufenden Jahr vermeiden.

“ Ich habe großes Vertrauen darin, dass Cloudflare Bedrohungen identifizieren kann. Das Unternehmen bewältigt vielfältigen Internet-Traffic in großem Umfang und kann diese Daten einsetzen, um selbst die komplexesten DDoS-Angriffe und böswillige Bot-Angriffe zu erkennen und zu bekämpfen.

Aaron Suggs Director of Engineering

Glossier.

(Fallstudie lesen)

BEST PRACTICE 5

Ihren Shop, Ihre Kunden und Ihre Marke schützen

Vor dem Cyber Weekend darf auf keiner Checkliste die Bewertung der Sicherheit von Websites, Anwendungen von Drittanbietern und Webdiensten wie APIs fehlen.

Neben dem Schutz vor Datenlecks sollte man auch weiteren Schwachstellen Rechnung tragen und sich unter anderem auf Cross-Site-Scripting-Angriffe (XSS) vorbereiten. Diese ermöglichen es Hackern, sich als Kunden auszugeben oder diese zur Preisgabe personenbezogener Daten zu verleiten. Ein weiteres Angriffswerkzeug ist SQL-Injection (SQLi), das auf die Bearbeitung von Suchanfragen durch Datenbanken abzielt, um Produktkataloge oder Preise zu manipulieren und gegebenenfalls betrügerische Käufe abzuschließen.

Vor dem Feiertagsgeschäft im Jahr 2019 waren Online-Händler in den USA und Großbritannien von diesen und anderen Angriffsformen betroffen.

Abgesehen von den unmittelbaren finanziellen Verlusten fällt solchen Vorfällen häufig zuerst die Markentreue zum Opfer. Fast ein Drittel (32 %) der Kunden gibt an, dass sie nicht länger bei einem Händler einkaufen würden, wenn dort ihre personenbezogenen Daten gestohlen werden.³³

► Rüsten Sie sich für den Kampf

Aufgrund der globalen Struktur des Internets sind die Käufer Angriffen ausgesetzt, die von verschiedenen Standorten aus gestartet werden und hinsichtlich Ausmaß und Komplexität variieren.



Um diesen Bedrohungen wirklich einen Riegel vorschieben zu können, müssen Sie Ihren Online-Shop, Anwendungen von Drittanbietern und Webdienste wie APIs vor häufigen Schwachstellen – etwa im Hinblick auf SQLi- und XSS-Angriffe – sowie vor Datenlecks schützen. Auf der nächsten Seite erfahren Sie, was zu jedem ernstzunehmenden Schlachtplan gehören sollte.

[Weiter >>](#)

8,7 % Anteil der Angriffe auf Online-Händler mit Cross-Site Scripting (XSS)
- Total Retail³⁴

8,2 % Anteil der Angriffe auf Online-Händler mit SQL-Injection (SQLi)
- Total Retail³⁵

► Setzen Sie eine Web Application Firewall ein

Die Bekämpfung von Angriffen mit SQL-Injection und Cross-Site-Scripting ist nicht besonders



schwierig. Aber bei den vielen Details, die mit dem Betrieb einer stabilen E-Commerce-Site verbunden sind, lassen sich Fehler nicht ausschließen und Hacker können jederzeit erfinderische neue Zero-Day-Angriffe starten, um diese Schwachstellen auszunutzen.³⁶

Folglich ist eine Web Application Firewall (WAF) für eine Präsenz auf den digitalen Kanälen unerlässlich. WAFs erkennen und blockieren XSS- und SQLi-Angriffe und sind für die Einhaltung des PCI-DSS erforderlich, um Zahlungsdaten und andere personenbezogene Kundendaten zu schützen. Sie filtern außerdem Schadcode heraus und bieten umfassende Sicherheit gegen Malware und Hackerangriffe auf eingebettete Webanwendungen.

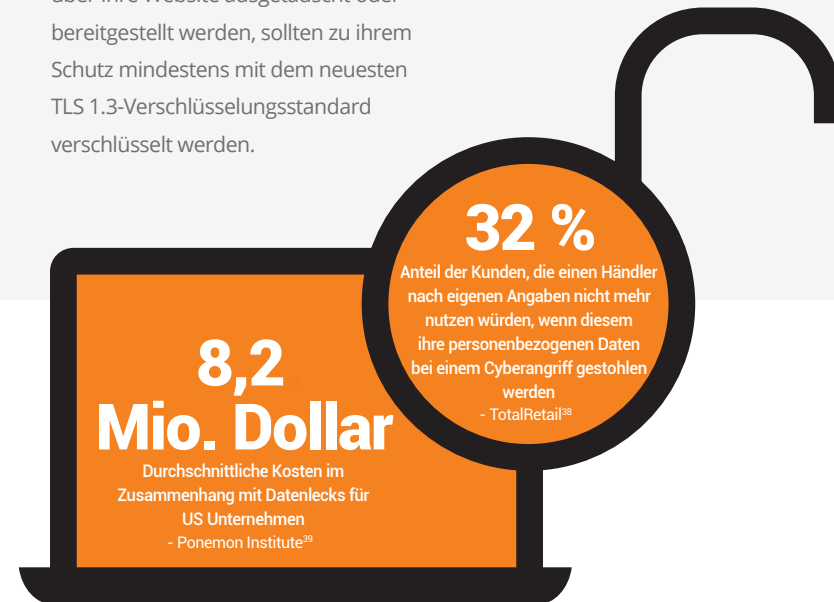
► Verschlüsseln Sie *alle* Ihre Daten

Im Online- und Mobile-Handel werden hochsensible Nutzerdaten gespeichert, etwa



Kreditkarten- und andere personenbezogene Informationen. Das macht sie zu einem Hauptziel für Hacker. Alle Daten, die über Ihre Website ausgetauscht oder bereitgestellt werden, sollten zu ihrem Schutz mindestens mit dem neuesten TLS 1.3-Verschlüsselungsstandard verschlüsselt werden.

TLS 1.3 erhöht nicht nur die Sicherheit Ihrer verschlüsselten Verbindungen, sondern reduziert auch die Latenzzeit und optimiert die Performance. Das ist wichtig für Händler, die pro Millisekunde, die sie hinter ihren Konkurrenten zurückbleiben, jährlich Einbußen von bis zu 4 Millionen US-Dollar haben können.³⁷



Wie Cloudflare zu sorgenfreiem E-Commerce während des Feiertagsgeschäfts beitragen kann

Angesichts der Herausforderungen, die mit der Vorbereitung Ihrer E-Commerce-Website auf ein erfolgreiches Cyber Weekend einhergehen, kann man leicht den Mut verlieren. Aber Cloudflare steht Ihnen zur Seite.

Unsere integrierte Cloud-Plattform, die das Vertrauen von über 20 Millionen Internetwebsites genießt, hilft Marken und Händlern, die Performance ihrer Websites zu verbessern und gleichzeitig Kundendaten und Transaktionen zu schützen – während des Feiertagsgeschäfts ebenso wie an jedem anderen Tag im Jahr. Unsere Dienste und Lösungen können den Online- und Mobile-Handel in den folgenden Bereichen unterstützen:

Verbesserung der Kundenerfahrung für mehr Konversionen

- CDN
- Argo Smart Routing
- Größenanpassung und Optimierung von Bildern
- Video-Streaming
- Schnellere Abrufbarkeit von Webcontent
- AMP-Support

Sicherstellung der Verfügbarkeit und Ausfallsicherheit des Webshops

- Lastverteilung
- Verwalteter DNS-Service
- DDoS-Abwehr
- Virtuelles Backbone
- Durchsatzratenbegrenzung

Schutz von Kundendaten und Transaktionen

- Bot-Management
- Web Application Firewall
- TLS 1.3

Einsatz von vernetzter Intelligenz und maschinellem Lernen

Mit Cloudflare erhöht sich durch einen Angriff in Sydney Ihre Sicherheit in Berlin. Ein Unterseekabel wird durchtrennt? Ihre Kunden werden automatisch umgeleitet – ohne dass es in Ihrem Shop zu Ausfallzeiten kommt. Das globale Netzwerk von Cloudflare analysiert den Datenverkehr von über 20 Millionen Internetwebsites weltweit, der mehr als 1 Milliarde eindeutige IP-Adressen pro Tag umfasst, um Ihren E-Commerce-Website in Betrieb zu halten.

“ Cloudflare sorgt dafür, dass wir online bleiben, bietet unseren Endnutzern eine schnellere Website und schützt die sensiblen Daten unserer Kunden.“

Steven Ou Gründer und CTO

TOUCH OF MODERN

(FALLSTUDIE LESEN)

Bereiten Sie sich jetzt auf das Cyber Weekend vor – es dauert nur fünf Minuten

Finden Sie heraus, wie leicht Sie das Angebot von Cloudflare nutzen können, um sich innerhalb von nur fünf Minuten für Ihr nächstes Verkaufsevent oder das gesamte Feiertagsgeschäft zu rüsten.

cloudflare.com/ecommerce

Quellen

- ¹ [Adobe Digital Insights „2019 Holiday Shopping Trends“, 1. Nov. 2019 – 31. Dez. 2019](#)
- ² [Levy, Nat, „Holiday e-commerce spending already hitting records as Amazon and others gear up for peak shopping season“, GeekWire, 29. November 2019](#)
- ³ [Perez, Sarah; Lunden, Ingrid „Cyber Monday totaled \\$9.4 billion in online sales, smartphones accounted for a record \\$3 Billion“, Techcrunch, 3. Dezember 2019](#)
- ⁴ [Pham, Sherisse, „Singles Day sales for Alibaba top \\$38 billion, breaking last year’s record“, CNN, 12. November 2019](#)
- ⁵ [Groenfeldt, Tom, „Credit Card Fraud is Down, But Account Fraud That Directly Hurts Consumers Remains High“, Forbes, 18. März 2019](#)
- ⁶ [Nilson Report, „Payment Card Fraud Losses Reach \\$27.85 billion“, 21. November 2019](#)
- ⁷ [Lerner, Dov, „The Holidays Are a Prime Time for Cybercrime“, Total Retail, 15. November 2019](#)
- ⁸ [PwC, 2019 Holiday Outlook](#)
- ⁹ [LexisNexis Risk Solutions, „Bots on Mobile Devices Fuel Holiday Shopping Cyberattacks“, 16. Dez. 2019](#)
- ¹⁰ [Statistica, „Global Mobile Retail Commerce Sales Share 2016-2021“, 7. Oktober 2019](#)
- ¹¹ [PYMNTS.com, „Look at the Pretty Pictures: Behind Visual Commerce’s Rise“, 12. November 2019](#)
- ¹² [Yahoo! Finance, „Personalization Drives 5X Conversion Rates During Black Friday and Cyber Monday“, 9. Dezember 2019](#)
- ¹³ [Kapur, Ajay, „Site speed is the new competitive battleground in ecommerce“, DigitalCommerce360, 16. April 2019](#)
- ¹⁴ [Think With Google, „The 3 areas brands should invest in to improve consumer experiences on mobile“](#)
- ¹⁵ [Liao, Shannon, „Black Friday pulls in a record \\$7.4 billion in online sales as many turn to mobile orders“, CNN Business, 1. Dezember 2019](#)
- ¹⁶ [Lucas, Amelia, „Cyber Monday online sales hit record \\$9.4 billion, boosted by late-night spending spree, Adobe says“, CNBC, 3. Dezember 2019](#)
- ¹⁷ [Crets, Stephanie, „Site glitches and downtime plague retailers during Cyber 5“, DigitalCommerce360, 4. Dezember 2019](#)
- ¹⁸ [Pioryshkina, Kate, „5 Steps to Creating the Perfect Mobile Checkout“, Destination CRM, 18. September 2019](#)
- ¹⁹ [Taylor, Glenn, „Costco Thanksgiving Day Site Outages Cost an Estimated \\$11 Million“, Retail TouchPoints, 2. Dezember 2019](#)
- ²⁰ [Taylor, Glenn, „Costco Thanksgiving Day Site Outages Cost an Estimated \\$11 Million“, Retail TouchPoints, 2. Dezember 2019](#)
- ²¹ [Solanki, Ricky, „Why a slow website is killing your conversions“, The Drum, 28. August 2019](#)
- ²² [HelpNetSecurity, „Most decision makers expect 5G to impact their cybersecurity strategy“, 29. Oktober 2019](#)
- ²³ [Reynolds, Roy, „DDoS Attacks on Retailers are Getting Sneaky— it’s Time to Rethink Your Denial of Service Protection“, Premier Construction News, Oktober 2019](#)
- ²⁴ [Reynolds, Roy, „DDoS Attacks on Retailers are Getting Sneaky— it’s Time to Rethink Your Denial of Service Protection“, Premier Construction News, Oktober 2019](#)
- ²⁵ [Popken, Ben, „Grinch bots’ are here to ruin your holiday shopping“, NBC News, 30. November 2019](#)
- ²⁶ [Thatha Pavan, „Nearly Two-Thirds of Traffic Was Bad Bots on Login Pages of E-Commerce Firms this Holiday Season“, Retail IT Insights, 16. Dezember 2019](#)
- ²⁷ [EMarketer, „Global Ecommerce 2019“](#)
- ²⁸ [Thatha, Pavan, „Nearly Two-Thirds of Holiday E-Commerce Traffic Was Bad Bots“, Security Boulevard, 17. Dezember 2019](#)
- ²⁹ [PYMNTS.com, „Grinch Bots’ Ramp Up Cybercrime During Holidays“, 2. Dezember 2019](#)
- ³⁰ [Popken, Ben, „Grinch bots’ are here to ruin your holiday shopping“, NBC News, 30. November 2019](#)
- ³¹ [Groenfeldt, Tom, „Credit Card Fraud is Down, But Account Fraud That Directly Hurts Consumers Remains High“, Forbes, 18. März 2019](#)
- ³² [Wodinsky, Shoshana, „Bots Will Cost Ecommerce Sites \\$10 Billion in 2019“, Adweek, 26. November 2019](#)
- ³³ [Keenan, Joe, „Macy’s Suffers Online Magecart Card-Skimming Attack, Data Breach“, My Total Retail, 19. November 2019](#)
- ³⁴ [Lackey, Zane, „It’s the Most Wonderful Time of the Year ... for Hackers“, Total Retail, 9. Dezember 2019](#)
- ³⁵ [Lackey, Zane, „It’s the Most Wonderful Time of the Year ... for Hackers“, Total Retail, 9. Dezember 2019](#)
- ³⁶ [Porup, J.M., „What is Cross-Site Scripting \(XSS\)? Low-Hanging Fruit for Both Attackers and Defenders“, CSO, 19. April 2018](#)
- ³⁷ [Eianav, Yoav, „Amazon Found Every 100ms of Latency Cost Them 1% of Sales“](#)
- ³⁸ [Lackey, Zane, „It’s the Most Wonderful Time of the Year ... for Hackers“, Total Retail, 9. Dezember 2019](#)
- ³⁹ [Ponemon Institute, „2019 Cost of a Data Breach Report“](#)