# BERICHT ZUR DOMAIN-SICHERHEIT

## FORBES GLOBAL 2000-UNTERNEHMEN

2021

# Kurzfassung

Vor dem Hintergrund zunehmender Cyber-Kriminalität haben Unternehmen in Jahr 2021 vermehrt Ransomware-Angriffe, E-Mail-Beeinträchtigungen (Business Email Compromise, BEC), Phishing-Angriffe, Angriffe auf die Lieferkette sowie Online-Marken- und Warenzeichenmissbrauch verzeichnet. Doch trotz des steigenden Cyber-Risikos im Bereich der Domains sind die Maßnahmen der Forbes Global 2000-Unternehmen zur Verbesserung der Domain-Sicherheit unverändert geblieben, wodurch diese Unternehmen einem noch größeren Risiko ausgesetzt sind.

## Domain-Sicherheit ist eine wichtige Komponente zur Abwehr von Cyber-Angriffen schon im Anfangsstadium, *d. h. sie ist die erste Verteidigungslinie.*

Laut CISA beginnen die meisten Cyber-Angriffe, z. B. Ransomware und BEC, mit Phishing. Obwohl Verluste durch Ransomware mittlerweile jährlich Milliardenbeträge übersteigen, gehen die meisten Maßnahmen zum Schutz vor Ransomware- Angriffe nicht in angemessener Weise die Phishing-Risiken in den frühen Phasen eines Ransomware-Angriffs an. Der Hauptgrund dafür ist, dass Domain-Sicherheitsmaßnahmen zum Schutz vor den häufigsten Phishing-Angriffen nicht vorhanden sind. Untersuchungen haben ergeben, dass Phishing-Angriffe am häufigsten durch folgende Angriffe erfolgen: Arglistige Domainregistrierungen, zum Verwechseln ähnliche Domains, kompromittierte Domains, Domain Hijacking oder Email-header-Spoofing.

## Cyber-Risiken für Domains verstehen

Die Nichtbeachtung der Domain-Sicherheit kann zu einem Risiko mit katastrophalen Auswirkungen werden. Ungeschützte Domains stellen eine erhebliche Bedrohung für Ihre Cybersicherheit, den Datenschutz, die Sicherheit der Verbraucher, das geistige Eigentum, die Lieferketten, den Umsatz und den Ruf dar.

CSC empfiehlt folgendes Rahmenkonzept gegen Cyber-Risiken und für eine bessere Domain-Sicherheit:

### RAHMENKONZEPT FÜR DOMAIN-SICHERHEIT

**Schutz vor verdächtigen und in böser Absicht registrierten Domains**

**Schutz gegen E-Mail-Header-Spoofing**

**Schutz vor Aktivitäten durch kompromittierte Domains**

### WICHTIGE RECHERCHE-ERGEBNISSE


**70 %** der Homoglyphen-Domains (Fuzzy Matches) – eine Taktik, die häufig beim Phishing und Markenmissbrauch eingesetzt wird – sind im Besitz von Dritten und bei Registraren für Verbraucher registriert. Von diesen Domain-Registrierungen wurden mehr als **60 %** in den letzten zwei Jahren registriert, was zeigt, dass dies eine rasch zunehmende Angriffsmethode ist.


**81 %** sind einem größeren Risiko von Domain- und DNS-Hijacking ausgesetzt, weil sie grundlegende Maßnahmen für die Domain-Sicherheit wie das Registry-Lock-Protokoll NICHT eingeführt haben.


**57 %** vertrauen Domain-Registraren für Verbraucher, die nur begrenzten Schutz vor Domain- und DNS-Hijacking, Distributed Denial of Service (DDoS), Man-in-the-Middle-Angriffen (MitM) oder DNS-Cache-Poisoning bieten.


Nur **50 %** nutzen DMARC-Einträge (Domain-based Message Authentication, Reporting and Conformance) als Methode zur Authentifizierung von E-Mails.

## Bedeutung der Domain-Sicherheit für die Abwehr gegen Phishing

Cyber-Angriffe aus jüngster Zeit zielten auf vernetzte Lieferketten in wichtigen Branchen und auf Softwareplattformen ab, bei denen eine Beeinträchtigung exponentielle Auswirkungen hat. Wegen der Verflechtung von Domains und DNS können die festgestellten Schwachstellen bei der Domain-Sicherheit und bei den Domain-Registraren zu einem weiteren Risiko für die Internet-Lieferkette führen. Proaktive, präventive Kontrollen können die zugrundeliegenden Domain-Assets sichern und vor den oben erwähnten Phishing-Angriffsmethoden schützen. Folgende Dinge sind unverzichtbar:

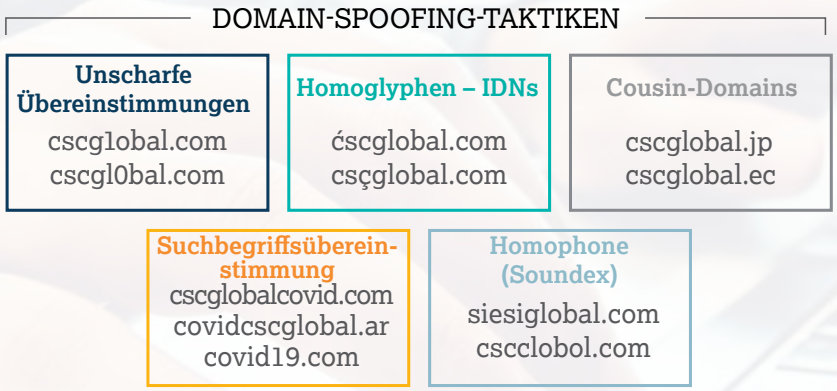
- **Domain-Registrar-Standards**, die über die Tücken aufklären, wenn große Unternehmen Registraren für Verbraucher vertrauen, und die Geschäftsverfahren verhindern, die für böswillige Zwecke wie Phishing und Markenmissbrauch genutzt werden.
- **Branchenweite Einführung von Maßnahmen zur Domain-Sicherheit** wie Registry-Locks für Domains, DMARC, DNS-Hosting-Redundanz, DNS-Sicherheitserweiterungen (DNSSEC) und CAA-Einträge (Certificate Authority Authorization).
- **Permanente rasche Erkennung und Deaktivierung verwirrend ähnlicher Domains**, die Marken imitieren und für Phishing und andere betrügerische Aktivitäten genutzt werden.

# Domain-Sicherheit:

## Auf die Global 2000-Unternehmen abzielende Aktivitäten verdächtiger oder in böser Absicht registrierter Domains

Wir haben Domainnamen identifiziert und analysiert, die Markennamen mit mehr als sechs Zeichen von Global 2000-Unternehmen enthalten und die nicht im Besitz der Marken selbst sind[1]. Ziel dieser verdächtigen oder in böser Absicht registrierten Domains ist es, das Vertrauen in die anvisierte Marke auszunutzen, um Phishing-Angriffe oder andere Formen von Online-Markenmissbrauch oder Urheberrechtsverletzungen zu starten, die zu Umsatzeinbußen, Traffic-Umleitung und einer Rufschädigung der Marke führen.

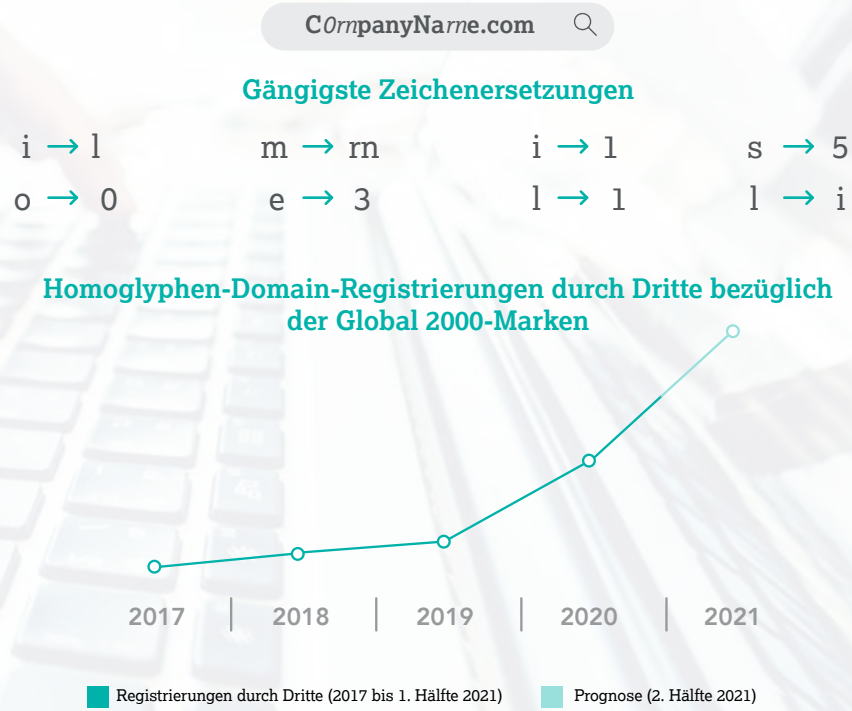
Es gibt unzählige Domain-Spoofing-Taktiken und -Möglichkeiten, die von Phishern und böswilligen Dritten genutzt werden können.




Wir haben uns entschieden, unsere Untersuchungen zur Domain-Sicherheit auf eine der vielen offenkundigen Taktiken zu konzentrieren, die mit bösartigen Domain-Registrierungsaktivitäten auf die Kernmarken der Global 2000-Unternehmen abzielen.

### Übliche Homoglyphen (so genannte Fuzzy Matches) in .COM-Domains

Da sie häufig für Phishing-Domains verwendet werden, haben wir bei unserer Analyse auch gängige Ersetzungen lateinischer Zeichen berücksichtigt, z. B. die Verwendung von C0rnpanyNarne.com, das wie CompanyName.com aussieht.




[1]Der Umfang der Untersuchung beschränkte sich auf die .COM-Erweiterungen, bei denen wir die meisten Registrierungen durch Dritte erwarteten. Um Falsch-Positiv-Befunde zu vermeiden, haben wir einen konservativen und aussagekräftigen Ansatz gewählt. Zudem haben wir Kernmarken mit sechs oder mehr Zeichen untersucht.

**70 %** der registrierten Domains, die den Global 2000-Marken ähnelten, waren im Fremdbesitz.

## Von den Domains im Besitz Fremder:

**60 %** wurden im Verlauf des Jahres 2020 bis zur Mitte des Jahres 2021 registriert. Unserer Prognose zufolge könnte dieser Anteil bis Ende 2021 auf **68 %** ansteigen.

**77 %** nutzten Domain-Privacy-Dienste oder verbergen auch WHOIS-Daten.

Dies zeigt, dass sie versuchen, die Eigentümerschaft und Identität zu verschleiern oder zu verbergen und damit möglicherweise unlautere Absichten verfolgen. Zum Vergleich: Legitime Global 2000-Marken nutzen nur in 25 % der Fälle Privacy-Dienste oder das Verbergen ihrer Daten.

**43 %** sind mit MX-Einträgen (E-Mail) konfiguriert.

Fast die Hälfte dieser Domains sind mit MX-Datensätzen konfiguriert, die zum Versenden von Phishing-E-Mails oder zum Abfangen von E-Mails verwendet werden können.

Unsere Analyse ergab, dass folgende Domain-Registrare am häufigsten in Verbindung mit verdächtigen oder böswilligen Registrierungen durch Fremde auftraten:

**GoDaddy.com, LLC** **Namecheap, Inc** **PDR, Ltd**

### Wie werden diese Domains von Dritten aktuell genutzt?

**56 %** verweisen auf Werbung, Pay-per-Click-Webinhalte oder werden für Domain-Parking genutzt.

Untersuchungen von Palo Alto zeigen, wie Pay-per-Click-Domains zur Verbreitung von Malware über diese Dienste genutzt werden. Cyber-Kriminelle können ruhende Domains als Strategie nutzen und sie genau dann aktivieren, wenn sie zum Angriff bereit sind.

**38 %** hatten inaktive Websites.

1/3 dieser Domains sind nicht mit Nameservern verbunden. Dies kann darauf hindeuten, dass der Domainname zu einem bestimmten Zeitpunkt gesperrt wurde.

Von den verbleibenden 2/3 haben **57 %** aktive MX-Einträge.

**6 %** verwiesen auf Markenimitationen und böswillige Inhalte, einschließlich Phishing und potenzielle Malware-Verbreitung.

Unerwünschte Inhalte können den Ruf einer Marke und das Vertrauen der Kunden schädigen. Das Risiko besteht darin, dass Nutzer auf Websites geraten, die böswillige Inhalte enthalten oder mit denen versucht wird, vertrauliche Informationen zu stehlen.

## Empfehlungen

Die Untersuchung dieser Domains im Fremdbesitz hat ergeben, dass viele von ihnen mit hoher Wahrscheinlichkeit als böswillige Domains für Cyber-Angriffe genutzt werden. Die Registranten verstecken sich in der Regel hinter Privacy-Diensten oder verborgenen WHOIS-Daten, um ihre Identität zu verschleiern. Sie registrieren Domains, die bekannten Marken zum Verwechseln ähnlich sehen, und wenden Taktiken an, die sie als seriös erscheinen lassen, um einen Endnutzer dazu zu verleiten, auf einen Link zu klicken oder einer Website zu vertrauen, die Markenrechte verletzt.

Wir empfehlen Unternehmen die Einrichtung eines robusten Domain-, Internet- und Phishing-Überwachungsprogramms, das auch Möglichkeiten zur Löschung bietet. Außerdem sollten Unternehmen eine sichere Strategie für ein umfassendes Domain-Management entwickeln. Dessen Aufgaben sind die Registrierung exakter Übereinstimmungen und der Schutz gegen eine Vielzahl von Domain-Spoofing-Taktiken, wie Homoglyphen, Fuzzy Matches und Cousin-Domains. Auch die Registrierung neuer generischer Top-Level-Domains (gTLDs) und länderspezifischer Domain-Erweiterungen für die Länder, in denen die Unternehmen Geschäfte tätigen, sowie für andere Hochrisiko-Länder gehört dazu.

# Analyse der Domain-Sicherheit

## Aufstellung der Forbes Global 2000-Unternehmen in Bezug auf Domain-Sicherheit

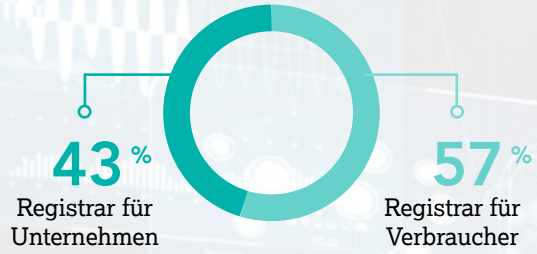
Die Erkenntnisse, die in diesem Bericht mitgeteilt werden, basieren ausschließlich auf öffentlich zugänglichen Datensätzen. Sie alle sind Cyber-Kriminellen und staatlich geförderten Akteuren leicht zugänglich und erleichtern DNS-Angriffe und Domainnamen-Hijacking. Daher möchten wir das Bewusstsein für diese Bedrohungen schärfen und unsere bewährten Verfahren für die Domain-Sicherheit weitergeben, um die Domain-Sicherheitslage aller Unternehmen zu verbessern. Bei dieser Untersuchung betrachtete CSC die Akzeptanz der Maßnahmen zur Domain-Sicherheit bei Unternehmen der Global 2000-Liste. Danach wurden Branchengruppen und Regionen näher unter die Lupe genommen.

In unserem diesjährigen Bericht haben wir auch den Trend bei der Einführung von Maßnahmen zur Domain-Sicherheit unter Beachtung der Art der genutzten Domain-Registrare untersucht. Bei allen Sicherheitsmaßnahmen haben wir festgestellt, dass diese bei Unternehmen, die Registrare für Unternehmen nutzen, in größerem Umfang eingeführt wurden als bei Unternehmen, die auf Registrare für Verbraucher setzen. Dies gilt insbesondere für die Einführung von Registry-Locks, da die meisten Registrare für Verbraucher solche Registry-Locks nicht unterstützen.

**Im Durchschnitt ist der Grad der Einführung von Maßnahmen zur Domain-Sicherheit bei Registraren für Unternehmen doppelt so hoch wie bei Registraren für Verbraucher.**

Unsere Beobachtungen beziehen sich auf Unternehmen, die in der Global 2000-Liste enthalten sind. Da jedes Jahr neue Unternehmen in die Liste aufgenommen werden, unterscheiden sich die untersuchten Unternehmen 2020 geringfügig von denen des Vorjahres.

# Domain-Registrare




## ERGEBNISSE

57 % der Global 2000-Unternehmen – die größten börsennotierten Unternehmen der Welt – nutzen keine Registrare für Unternehmen. Die Verwaltung des gesamten Domainnamenportfolios durch einen namhaften Registrar für Unternehmen (Enterprise-Class-Registrar) im Gegensatz zu einem Registrar für Verbraucher (Retail-Registrar) ermöglicht die Einführung von Standards und bewährten Verfahren für die Domain-Sicherheit.

## SCHLÜSSELMERKMALE EINES REGISTRARS FÜR UNTERNEHMEN:

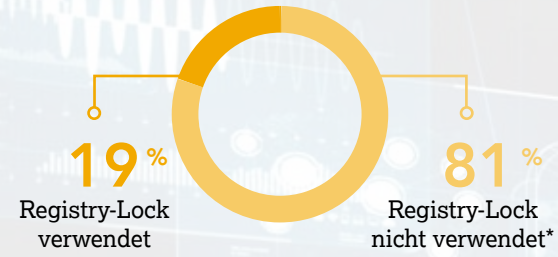
- ☑ Unternehmensweite Skalierung und Expertise mit einem unternehmenseigenen DNS und einem Angebot zur Zertifikatsverwaltung
- ☑ Cybersicherheit und Urheberrechtsschutz stehen im Mittelpunkt

  Folgendes wird nicht angeboten:
  - Domain-Dienste über Retail-Websites oder Wiederverkäufer
  - Pay-per-Click-, Domain-Spinning- und Domain-Auktionsdienste, die die Verletzung von geistigem Eigentum und Markenrechten erleichtern
- ☑ Hervorhebung der Domain-Sicherheit durch erweiterte Dienste wie Domain-Registry-Lock, DMARC, DNSSEC, CAA-Einträge und DNS-Hosting-Redundanz
- ☑ Bereitstellung von Support rund um die Uhr (24 x 7 x 365), weltweit und vor Ort mit Domain-Registrierung auf der ganzen Welt
- ☑ Implementierung von KYC-Methoden (Know Your Customer, KCY) zur Gewinnung und Validierung von Kundeninteraktionen
- ☑ Globale Akkreditierung durch die Internet Corporation for Assigned Names and Numbers (ICANN) und Registrys
- ☑ Möglichkeiten zur Domain-, Marken- und Betrugsüberwachung sowie zur Durchsetzung und Löschung
- ☑ Angebot von kostenlosen Beratungsdienstleistungen und -Tools (z. B. CSC Security Center℠), die das Domain-Management und die Domain-Sicherheit zusammen mit Markenschutz und Betrugsabwehr erleichtern
- ☑ Nutzung der besten operativen Verfahren und Kontrollen, wie z. B. die Anordnung von schriftlichen Anträgen, die Durchführung von Schulungen zum Thema Cybersicherheit und die Ergreifung von Datenschutzmaßnahmen
- ☑ erstklassige Geschäftsverfahren mit Sicherheit als Schwerpunkt, z. B. ISO 27001-zertifizierte Rechenzentren, SOC 2-Konformität und Penetrations- und Schwachstellentests durch Drittanbieter

## ⓘ BEDROHUNG

In der Vergangenheit waren Registrare für Verbraucher häufig das Ziel von Cyber-Angriffen. Eine überwältigende Anzahl ermöglicht Markenmissbrauch und Betrug. (Gründe für die Nutzung eines Registrars für Unternehmen sind oben beschrieben.)

## Registry-Lock




### Nutzung nach Art des Registrars

52 % der Unternehmen, die mit einem Registrar für Unternehmen zusammenarbeiten, verwenden Registry-Lock

4 % der Unternehmen, die mit einem Registrar für Verbraucher zusammenarbeiten, nutzen Registry-Lock

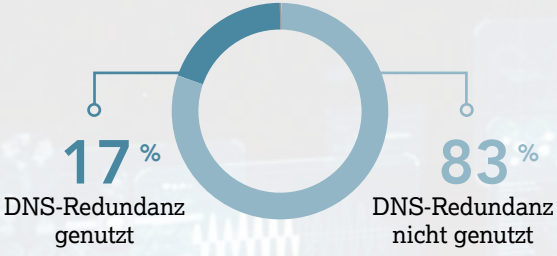
### ERGEBNISSE

Alarmierend ist, dass nur 19 % Registry-Lock als Schutzmaßnahme einsetzen, was signalisiert, dass vier von fünf Global 2000-Unternehmen in Bezug auf die Domain-Sicherheit stark gefährdet sind. Angesichts der anhaltenden DNS-Hijacking-Risiken für globale Unternehmen wird diese Kontrolle von den Global 2000-Unternehmen nur in sehr geringem Maße angewendet. Unter den 43 % der Global 2000-Unternehmen, die Registrare für Unternehmen nutzen, ist der Anteil der Unternehmen, die Registry-Locks einsetzen, mit 52 % höher als bei den Unternehmen, die Registrare für Verbraucher nutzen, denn hier liegt der Anteil nur bei 4 %. Dies deutet darauf hin, dass die Art des Registrars einen Einfluss auf die Einführung von Sicherheitskontrollen für Domains hat.

### BEDROHUNG

Ein Registry-Lock ermöglicht die durchgängige Sicherheit von Domainnamen-Transaktionen, um menschliches Versagen und das Risiko durch Fremde zu minimieren. Sie ist ein äußerst kostengünstiges Mittel, um Domainnamen vor versehentlichen oder unbefugten Änderungen oder Löschungen zu schützen. Ungesicherte Domains sind anfällig für Social-Engineering-Taktiken, die zu nicht autorisierten DNS-Änderungen und Domainnamen-Hijacking führen können. *Außerdem bleiben möglicherweise einige Domains ungesperrt, da nicht alle Registrys auf der ganzen Welt Sperrdienste anbieten.

## DNS-Redundanz




### Nutzung nach Art des Registrars

20 % der Unternehmen, die mit einem Registrar für Unternehmen zusammenarbeiten, haben DNS-Redundanz realisiert

13 % der Unternehmen, die mit einem Registrar für Verbraucher zusammenarbeiten, haben DNS-Redundanz realisiert

### ERGEBNISSE

Nur 17 % der Global 2000-Unternehmen verfügen über DNS-Redundanz für ihre wichtigste Domain (Secondary-DNS). Mehr als 80 % haben kein Secondary-DNS, das Bedrohungen eindämmen würde. Sie gehen damit das Risiko kostspieliger Vorfälle ein, wenn Mitarbeiter oder Kunden auch nur für ein paar Minuten nicht auf ihre Websites zugreifen oder dort Transaktionen durchführen können.

### BEDROHUNG

Fehlende DNS-Redundanz birgt potenzielle Sicherheitsbedrohungen wie geringe Resilienz bei DDoS-Angriffen sowie Ausfallzeiten. Diese Angriffe überfluten Netzwerke, Dienste oder Anwendungen und verhindern, dass echte Kundenanfragen durchkommen, was zu Umsatzeinbußen und geschmälertem Ansehen führt.

## DNSSEC


### Nutzung nach Art des Registrars

7 % der Unternehmen, die mit einem Registrar für Unternehmen zusammenarbeiten, verwenden DNSSEC

3 % der Unternehmen, die mit einem Registrar für Verbraucher zusammenarbeiten, nutzen DNSSEC

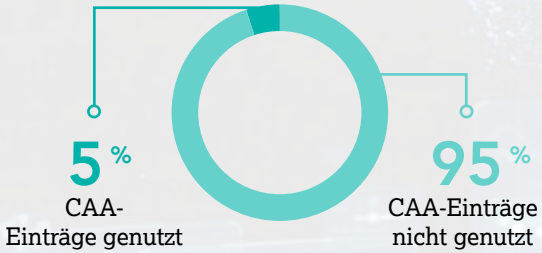
### ERGEBNISSE

DNSSEC (Domain Name System Security Extensions) ist eine weitere Methode, um eine authentifizierte Kommunikation zwischen DNS-Servern zu ermöglichen. Mit nur 5 % ist DNSSEC nur in sehr geringem Maße eingeführt. DNSSEC verhindert Angriffe über DNS-Cache-Poisoning. Das bedeutet, dass 95 % aller Global 2000-Unternehmen anfällig für einen Cache-Poisoning-Angriff sind.

### BEDROHUNG

Die Nichtbereitstellung von DNSSEC – eines der kostengünstigsten Sicherheitsprotokolle – führt zu Schwachstellen im DNS. Das könnte auch dazu führen, dass ein Angreifer jeden Schritt des DNS-Lookup-Prozesses an sich reißt. Dadurch können Hacker die Kontrolle über eine Internet-Browsing-Sitzung übernehmen und Benutzer auf irreführende Websites umleiten.

## CAA-Einträge




### Nutzung nach Art des Registrars

8 % der Unternehmen, die mit einem Registrar für Unternehmen zusammenarbeiten, verwenden CAA-Einträge

4 % der Unternehmen, die mit einem Registrar für Verbraucher zusammenarbeiten, nutzen CAA-Einträge

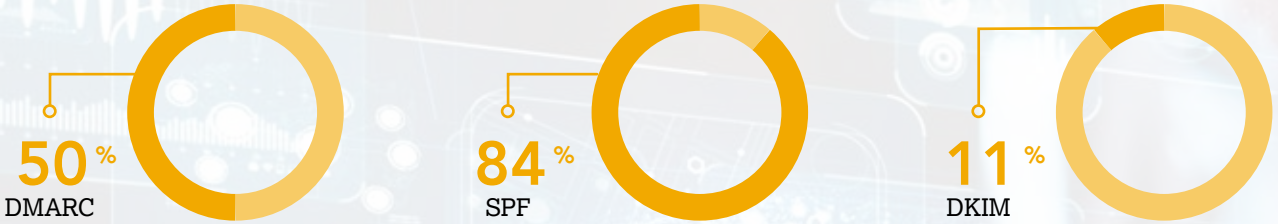
### ERGEBNISSE

Nur 5 % der Global 2000-Unternehmen nutzen CAA-Einträge (Certificate Authority Authorization, CAA). Mit CAA-Einträgen kann ein Unternehmen eine bestimmte Zertifizierungsstelle (Certificate Authority, CA) als alleinigen Aussteller von Zertifikaten für seine Domains benennen. Wenn ein Cyber-Krimineller nicht die ernannte Zertifizierungsstelle nutzt, um ein neues Zertifikat zu erhalten, schlägt seine Anfrage fehl, und Sie erhalten eine Warnung, dass jemand versucht hat, ein neues Zertifikat außerhalb Ihrer CAA-Richtlinie anzufordern. Sie haben damit ein großartiges Instrument zur Einhaltung von Vorschriften (Compliance) und auch eine hervorragende Sicherheitsschicht.

### BEDROHUNG

Nachdem Cyber-Kriminelle Zugang zu einem Domainnamen erhalten, haben sie in vielen Fällen Zugang zu ausgestellten digitalen Zertifikaten. Durch das Hinzufügen von CAA-Einträgen wird sichergestellt, dass nur der von Ihnen gewählte Provider ein Zertifikat für Ihre Domainnamen ausstellen kann. Dies ist eine wesentliche technische Schutzmaßnahme, die die Durchsetzung von Richtlinien und die Abwehr von Cyber-Bedrohungen wie HTTPS-Phishing von entführten Subdomains ermöglicht.

# E-Mail-Authentifizierung




## Nutzung nach Art des Registrars

70 % der Unternehmen, die mit einem Registrar für Unternehmen zusammenarbeiten, verwenden DMARC

44 % der Unternehmen, die mit einem Registrar für Verbraucher zusammenarbeiten, nutzen DMARC

## ERGEBNISSE

Die Nutzung von DMARC (Domain-based Message Authentication, Reporting and Conformance) liegt bei den Global 2000-Unternehmen inzwischen bei 50 %. DMARC ist ein E-Mail-Validierungssystem, das entwickelt wurde, um die E-Mail-Domain eines Unternehmens vor der Verwendung für E-Mail-Spoofing, Phishing-Betrug und andere Cyber-Kriminalität zu schützen. DMARC sorgt im Wesentlichen für E-Mail-Authentifizierung auf die gleiche Weise wie DNSSEC auf der DNS-Ebene. Wir wissen auch, dass selbst bei vorhandenen DMARC-Einträgen das Fehlen einer DMARC-Ablehnungsrichtlinie immer noch ein Phishing-Risiko darstellt.

## BEDROHUNG

Es ist sehr einfach, E-Mails zu fälschen und sie so aussehen zu lassen, als kämen sie von einer seriösen Quelle, obwohl sie es in Wirklichkeit nicht sind. Die Authentifizierung des E-Mail-Kanals mit DMARC, SPF oder DKIM minimiert das Auftreten von E-Mail-Spoofing und potenziellem Phishing.

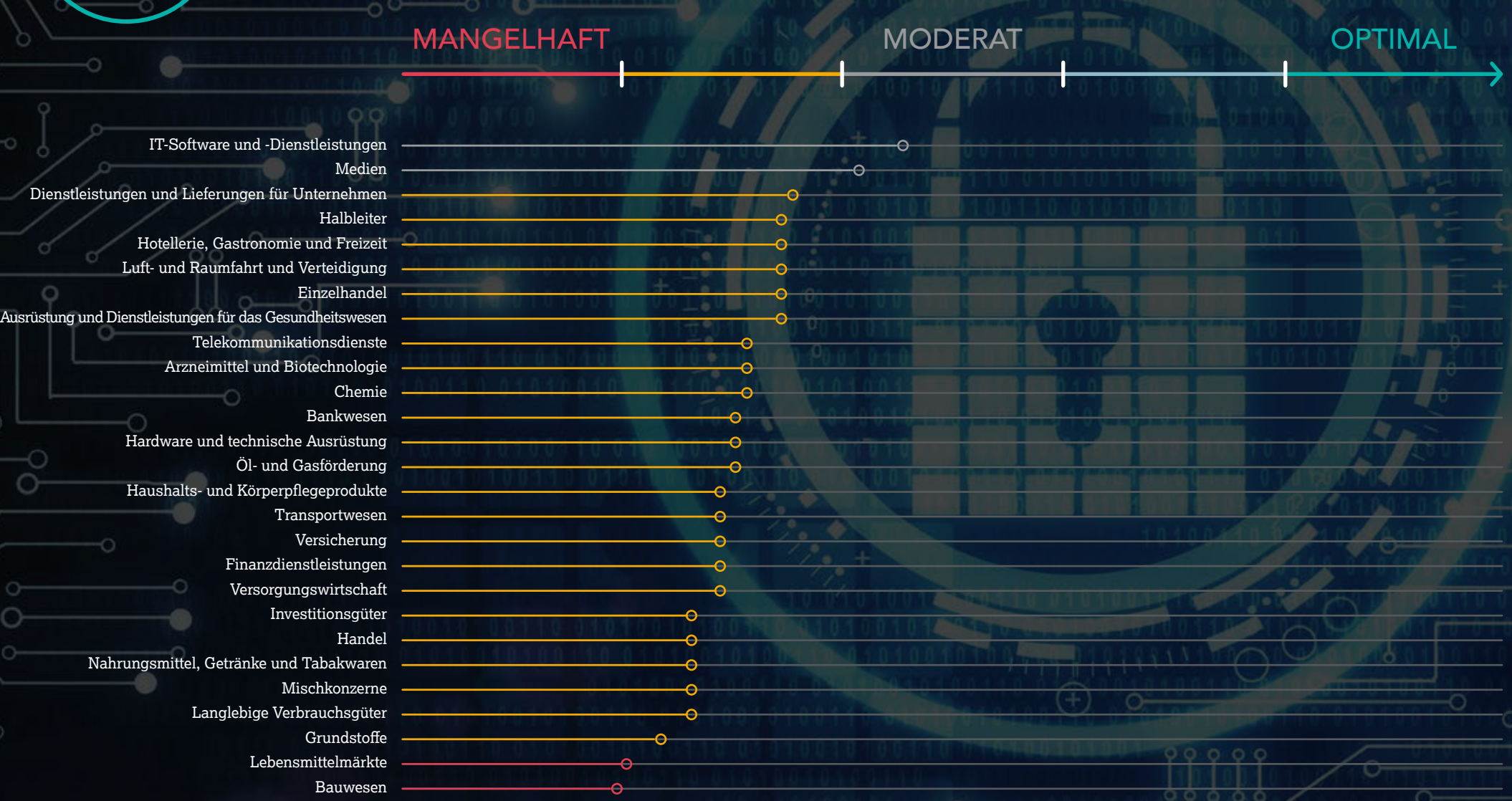
# Akzeptanz von Domain-Sicherheitsmaßnahmen nach Branchengruppen

Einige Branchen sind durch COVID-19 stärker ins Rampenlicht gerückt. Das sind die Branchen Ausrüstung und Dienstleistungen für das Gesundheitswesen, Arzneimittel und Biotechnologie, Chemie sowie Haushalts- und Körperpflegeprodukte. Der gestiegene Bedarf in all diesen Branchen in den letzten anderthalb Jahren haben sie zu wichtigen Zielen für Cyber-Kriminelle gemacht. Daher ist es höchst beunruhigend, dass diese Branchen in Bezug auf Risikominderungsmaßnahmen immer noch im mittleren oder unteren Bereich der Skala liegen. In diesen vier Branchen ist die Akzeptanz von DNSSEC äußerst gering, in den Branchen Ausrüstung und Dienstleistungen für das Gesundheitswesen sowie Haushalts- und Körperpflegeprodukte liegt sie sogar bei 0 %. Auch die Akzeptanz von CAA-Einträgen ist sehr gering, was bedeutet, dass digitale Zertifikate mit dem Anschein von Seriosität für gefährdete Domains bestehen könnten, ohne dass die Marke davon Kenntnis hat. Außerdem setzt im Durchschnitt nur eines von vier Unternehmen in diesen Branchen Registry-Locks ein, die das Hijacking von Domainnamen und unbefugte Änderungen am DNS verhindern. Doch vielleicht ist die geringe Akzeptanz dieser drei Protokolle nicht überraschend, wenn man bedenkt, dass 32 bis 48 % der Unternehmen in diesen Branchen Registrare für Verbraucher nutzen, die DNSSEC, Registry-Locks oder CAA-Einträge standardmäßig nicht anbieten. Sie könnten also zusätzlich von der Zusammenarbeit mit einem Domain-Registrar für Unternehmen profitieren.

Auch die Öl- und Gasindustrie steht in letzter Zeit im Rampenlicht, insbesondere seit dem Ransomware-Angriff auf das US-Energieunternehmen Colonial Pipelines, der die Abschaltung von 5.500 Meilen seiner über Bundesstaaten verlaufenden Kraftstoffpipeline erzwang. „Der Vorfall ist eine der bisher schädlichsten Lösegeldaktionen im Online-Bereich und hat die Aufmerksamkeit darauf gelenkt, wie anfällig die Energieinfrastruktur der USA für Hacker ist“, kommentierte Reuters. Unternehmen in der Öl- und Gasindustrie sollten dies ernsthaft zur Kenntnis nehmen, zumal unsere Statistiken zeigen, dass die Öl- und Gasindustrie innerhalb der Global 2000-Unternehmen in punkto Risikominderung eher schlecht abschneidet. Gerade einmal 4 % der Unternehmen in dieser Branche nutzen DNSSEC und nur 10 % nutzen Registry-Lock.

Der Bankensektor ist nach wie vor uneinheitlich, was die Einführung von Maßnahmen zur Domain- und DNS-Sicherheit betrifft. Für eine Branche, die wohl das Hauptziel für Phishing-Angriffe darstellt, ist die Akzeptanz von DMARC, dem E-Mail-Authentifizierungsprotokoll, mit 49,7 % immer noch besorgniserregend niedrig.

# Bewertung der Risikominderung



# Empfehlungen

Domain-Sicherheit ist das fehlende Glied bei den meisten Strategien zur Cybersicherheit.  Erstklassige Sicherheitsmaßnahmen für Domains können dazu beitragen, Phishing-, BEC- und Ransomware-Angriffe bereits im Anfangsstadium zu verhindern. Viele Branchenexperten haben betont, dass es sehr wichtig ist, eine strenge Cyber-Hygiene aufrechtzuerhalten. Domain-Sicherheit ist ein Paradebeispiel für Defizite bei Unternehmen. Domain-Sicherheit spielt eine präventive Rolle gegen Phishing-Angriffe, was dann auch BEC-Angriffe, Identitätsdiebstahl, Ransomware-Angriffe und viele andere Bedrohungen verhindern würde.

Sämtliche Unternehmen in allen Branchen – und insbesondere diejenigen, die aufgrund von COVID-19 jetzt noch stärker gefährdet sind – sollten einen mehrschichtigen Ansatz für die Domain-Sicherheit verfolgen, der mit der Zusammenarbeit mit einem Enterprise-Class-Provider beginnt. CSC empfiehlt vier Schlüsselstrategien:

- **Anwendung** eines Ansatzes der tief gestaffelten Verteidigung für das Domain-Management
- **Überprüfung** der Geschäftsverfahren des Domain-Registrars dahingehend, dass sie nicht zu Betrug und Markenmissbrauch beitragen
- **Ständige Überwachung** des Domain-Raums und der wichtigsten digitalen Kanäle wie Marktplätze, Apps, soziale Medien und E-Mail auf Markenmissbrauch, Rechtsverletzungen, Phishing und Betrug
- **Nutzung** der Durchsetzung im globalen Maßstab, z. B. durch Löschungen und moderne Techniken bei der Internet-Sperrung

## ANWENDUNG EINES ANSATZES DER TIEF GESTAFFELTEN VERTEIDIGUNG FÜR DAS DOMAIN-MANAGEMENT

- Eliminierung des Risikos durch Fremde durch Bewertung der Sicherheit, Technologie und der Prozesse Ihres Domain-Registrars zusammen mit Ihrem DNS-Management-Provider
- Schutz wichtiger Domainnamen, des DNS und digitaler Zertifikate durch folgende Maßnahmen:
  - Implementierung der Zwei-Faktor-Authentifizierung
  - Überwachung der DNS-Aktivitäten
  - Verwendung von Sicherheitsmaßnahmen wie Domain-Registry-Locks, DNSSEC, DMARC, CAA-Einträge und Redundanz beim DNS-Hosting

## ÜBERPRÜFUNG DER GESCHÄFTSVERFAHREN DES DOMAIN-REGISTRARS DAHINGEHEND, DASS SIE NICHT ZU BETRUG UND MARKENMISSBRAUCH BEITRAGEN

Die folgenden Probleme treten häufig bei Domain-Registraren für Verbraucher auf:

- Betrieb von Domain-Märkten, in denen Domainnamen, die Marken enthalten, erfasst, versteigert und an den Meistbietenden verkauft werden
- Domainnamen-Spinning und Befürwortung der Registrierung von Domainnamen, die Marken enthalten
- Monetarisierung von Domainnamen, die Marken enthalten, über Pay-per-Click-Websites
- Häufig auftretende Verstöße, die zu DNS-Angriffen, Phishing und BEC führen

## STÄNDIGE ÜBERWACHUNG DES DOMAIN-RAUMS UND DER WICHTIGSTEN DIGITALEN KANÄLE WIE MARKTPLÄTZE, APPS, SOZIALE MEDIEN UND E-MAIL AUF MARKENMISSBRAUCH, RECHTSVERLETZUNGEN, PHISHING UND BETRUG

- Nutzung der Phishing-Überwachung und eines Netzwerks von Browsern, Partnern, ISPs und SIEMs zur Betrugsabwehr
- Identifizierung von Domain- und DNS-Spoofing-Taktiken wie Homoglyphen (Fuzzy Matches und IDNs), Cousin-Domains, Keyword Match und Homophone
- Identifizierung von Warenzeichen- und Urheberrechtsmissbrauch in Webinhalten
- Schutz der Marken vor Missbrauch auf Online-Marktplätzen durch Marktplatzüberwachung
- Verfolgung aller Erwähnungen von Marken über relevante Social-Media-Kanäle
- Überwachung der großen App Stores
- Suche nach Werbung, die potenzielle Kunden von der Nutzung Ihrer Online-Assets abhält und Ihre Marke schädigt

## NUTZUNG DER DURCHSETZUNG IM GLOBALEN MASSSTAB, Z. B. DURCH LÖSCHUNGEN UND MODERNE TECHNIKEN BEI DER INTERNET-SPERRUNG

- Nutzung einer Kombination von Maßnahmen zur Durchsetzung bei Urheberrechtsverletzungen und Betrug:
  - Zu den vorrangigen Durchsetzungsmaßnahmen gehören die Streichung von Marktplätzen, die Sperrung von Social-Media-Seiten, die Streichung von mobilen Apps, Unterlassungsaufforderungen, die Entfernung betrügerischer Inhalte und die vollständige Eindämmung von Bedrohungsvektoren
  - Zweitrangige Durchsetzungsmaßnahmen beinhalten u. a. die Sperrung von Domains auf Registrarebene, die Sperrung von Domains mit ungültigen WHOIS-Einträgen und Warnungen vor Betrug
  - Drittrangige Durchsetzungsmaßnahmen umfassen u. a. Verfahren gemäß der Uniform Domain-Name Dispute-Resolution Policy (UDRP) und der Uniform Rapid Suspension (URS), Domainerwerb, eingehende Untersuchungen und Testkäufe
- Nutzung einer Reihe von technischen und rechtlichen Ansätzen für die Durchsetzung, wobei von Fall zu Fall der am besten geeignete Ansatz zu wählen ist

# Branchenakzeptanz nach Sicherheitsmaßnahme

HOHE AKZEPTANZ  GERINGE AKZEPTANZ

## Registrar für Unternehmen


| | |
|---|---|
| Hotellerie, Gastronomie und Freizeit | 75 % |
| Haushalts- und Körperpflegeprodukte | 68 % |
| Dienstleistungen und Lieferungen für Unternehmen | 65 % |
| Medien | 64 % |
| IT-Software und -Dienstleistungen | 61 % |
| Chemie | 57 % |
| Einzelhandel | 56 % |
| Arzneimittel und Biotechnologie | 56 % |
| Luft- und Raumfahrt und Verteidigung | 54 % |
| Halbleiter | 53 % |
| Ausrüstung und Dienstleistungen für das Gesundheitswesen | 52 % |
| Investitionsgüter | 47 % |
| Transportwesen | 47 % |
| Nahrungsmittel, Getränke und Tabakwaren | 47 % |
| Langlebige Verbrauchsgüter | 46 % |
| Versicherung | 45 % |
| Hardware und technische Ausrüstung | 42 % |
| Bankwesen | 38 % |
| Mischkonzerne | 38 % |
| Telekommunikationsdienste | 36 % |
| Handel | 35 % |
| Finanzdienstleistungen | 35 % |
| Versorgungswirtschaft | 35 % |
| Öl- und Gasförderung | 28 % |
| Bauwesen | 24 % |
| Grundstoffe | 22 % |
| Lebensmittelmärkte | 22 % |

## Registry-Lock


| | |
|---|---|
| IT-Software und -Dienstleistungen | 48 % |
| Medien | 40 % |
| Luft- und Raumfahrt und Verteidigung | 33 % |
| Dienstleistungen und Lieferungen für Unternehmen | 33 % |
| Halbleiter | 28 % |
| Telekommunikationsdienste | 28 % |
| Einzelhandel | 27 % |
| Chemie | 27 % |
| Arzneimittel und Biotechnologie | 27 % |
| Ausrüstung und Dienstleistungen für das Gesundheitswesen | 25 % |
| Langlebige Verbrauchsgüter | 24 % |
| Investitionsgüter | 23 % |
| Hotellerie, Gastronomie und Freizeit | 21 % |
| Haushalts- und Körperpflegeprodukte | 21 % |
| Finanzdienstleistungen | 20 % |
| Transportwesen | 19 % |
| Hardware und technische Ausrüstung | 19 % |
| Versicherung | 18 % |
| Nahrungsmittel, Getränke und Tabakwaren | 16 % |
| Bankwesen | 14 % |
| Mischkonzerne | 13 % |
| Versorgungswirtschaft | 11 % |
| Öl- und Gasförderung | 10 % |
| Grundstoffe | 9 % |
| Lebensmittelmärkte | 6 % |
| Bauwesen | 6 % |
| Handel | 3 % |

HOHE AKZEPTANZ  GERINGE AKZEPTANZ

## DNS-Redundanz


| | |
|---|---|
| Transportwesen | 28 % |
| Öl- und Gasförderung | 25 % |
| Bankwesen | 23 % |
| IT-Software und -Dienstleistungen | 23 % |
| Luft- und Raumfahrt und Verteidigung | 21 % |
| Handel | 21 % |
| Telekommunikationsdienste | 20 % |
| Chemie | 20 % |
| Halbleiter | 19 % |
| Versicherung | 19 % |
| Einzelhandel | 18 % |
| Finanzdienstleistungen | 17 % |
| Hotellerie, Gastronomie und Freizeit | 17 % |
| Lebensmittelmärkte | 16 % |
| Investitionsgüter | 14 % |
| Langlebige Verbrauchsgüter | 13 % |
| Grundstoffe | 12 % |
| Dienstleistungen und Lieferungen für Unternehmen | 12 % |
| Medien | 12 % |
| Haushalts- und Körperpflegeprodukte | 12 % |
| Versorgungswirtschaft | 11 % |
| Arzneimittel und Biotechnologie | 11 % |
| Nahrungsmittel, Getränke und Tabakwaren | 10 % |
| Bauwesen | 9 % |
| Mischkonzerne | 9 % |
| Hardware und technische Ausrüstung | 8 % |
| Ausrüstung und Dienstleistungen für das Gesundheitswesen | 7 % |

## DNSSEC


| | |
|---|---|
| IT-Software und -Dienstleistungen | 14 % |
| Luft- und Raumfahrt und Verteidigung | 13 % |
| Medien | 12 % |
| Bankwesen | 9 % |
| Halbleiter | 9 % |
| Finanzdienstleistungen | 6 % |
| Versorgungswirtschaft | 6 % |
| Dienstleistungen und Lieferungen für Unternehmen | 6 % |
| Versicherung | 4 % |
| Telekommunikationsdienste | 4 % |
| Öl- und Gasförderung | 4 % |
| Investitionsgüter | 4 % |
| Langlebige Verbrauchsgüter | 3 % |
| Handel | 3 % |
| Arzneimittel und Biotechnologie | 3 % |
| Bauwesen | 2 % |
| Chemie | 2 % |
| Hardware und technische Ausrüstung | 2 % |
| Hotellerie, Gastronomie und Freizeit | 0 % |
| Ausrüstung und Dienstleistungen für das Gesundheitswesen | 0 % |
| Einzelhandel | 0 % |
| Transportwesen | 0 % |
| Haushalts- und Körperpflegeprodukte | 0 % |
| Nahrungsmittel, Getränke und Tabakwaren | 0 % |
| Mischkonzerne | 0 % |
| Grundstoffe | 0 % |
| Lebensmittelmärkte | 0 % |

HOHE AKZEPTANZ  GERINGE AKZEPTANZ

## CAA-Einträge


| | |
|---|---|
| Medien | 16 % |
| IT-Software und -Dienstleistungen | 13 % |
| Öl- und Gasförderung | 13 % |
| Bankwesen | 9 % |
| Dienstleistungen und Lieferungen für Unternehmen | 8 % |
| Telekommunikationsdienste | 8 % |
| Mischkonzerne | 6 % |
| Versorgungswirtschaft | 6 % |
| Finanzdienstleistungen | 6 % |
| Chemie | 5 % |
| Hardware und technische Ausrüstung | 5 % |
| Ausrüstung und Dienstleistungen für das Gesundheitswesen | 5 % |
| Hotellerie, Gastronomie und Freizeit | 4 % |
| Transportwesen | 4 % |
| Versicherung | 4 % |
| Grundstoffe | 3 % |
| Einzelhandel | 3 % |
| Arzneimittel und Biotechnologie | 3 % |
| Langlebige Verbrauchsgüter | 2 % |
| Investitionsgüter | 2 % |
| Bauwesen | 1 % |
| Nahrungsmittel, Getränke und Tabakwaren | 1 % |
| Halbleiter | 0 % |
| Luft- und Raumfahrt und Verteidigung | 0 % |
| Haushalts- und Körperpflegeprodukte | 0 % |
| Handel | 0 % |
| Lebensmittelmärkte | 0 % |

## DMARC


| | |
|---|---|
| IT-Software und -Dienstleistungen | 74 % |
| Ausrüstung und Dienstleistungen für das Gesundheitswesen | 73 % |
| Halbleiter | 72 % |
| Medien | 64 % |
| Hotellerie, Gastronomie und Freizeit | 63 % |
| Einzelhandel | 60 % |
| Arzneimittel und Biotechnologie | 60 % |
| Öl- und Gasförderung | 59 % |
| Mischkonzerne | 56 % |
| Telekommunikationsdienste | 56 % |
| Hardware und technische Ausrüstung | 56 % |
| Nahrungsmittel, Getränke und Tabakwaren | 54 % |
| Versorgungswirtschaft | 54 % |
| Dienstleistungen und Lieferungen für Unternehmen | 53 % |
| Luft- und Raumfahrt und Verteidigung | 50 % |
| Bankwesen | 50 % |
| Grundstoffe | 47 % |
| Haushalts- und Körperpflegeprodukte | 47 % |
| Transportwesen | 46 % |
| Versicherung | 46 % |
| Finanzdienstleistungen | 43 % |
| Handel | 41 % |
| Chemie | 41 % |
| Langlebige Verbrauchsgüter | 38 % |
| Lebensmittelmärkte | 38 % |
| Investitionsgüter | 37 % |
| Bauwesen | 28 % |

**CSC** ist vertrauenswürdiger Anbieter erster Wahl für die Forbes Global 2000-Unternehmen und die 100 Best Global Brands® in den Bereichen Domainverwaltung, Domain Name System (DNS), Digital Certificate Management sowie digitaler Marken- und Betrugsschutz. Angesichts der Tatsache, dass weltweit tätige Unternehmen in erheblichem Maße in ihre Sicherheitsvorkehrungen investieren, kann CSC ihnen dabei helfen, bekannte Sicherheitslücken zu erkennen und ihre Domainnamen, DNS und digitalen Zertifikate zu sichern. Durch Nutzung firmeneigener Sicherheitslösungen schützt CSC Unternehmen vor Cyber-Bedrohungen gegen ihre Online-Assets und hilft ihnen, verheerende Umsatzeinbußen, Rufschädigung ihrer Marken oder erhebliche Geldbußen durch Richtlinien wie der DSGVO zu vermeiden. Wir bieten auch Online-Markenschutz – eine Kombination aus Online-Markenüberwachung und Durchsetzungsmaßnahmen – und verfolgen dabei einen ganzheitlichen Ansatz zum Schutz digitaler Assets, zusammen mit Betrugsschutzdiensten zur Bekämpfung von Phishing.


## Recherche und Editorial von CSC

**Vincent D'Angelo,** Global Director, Corporate Development and Strategic Alliances

**Stephanie Mitchell,** Manager, Marketing

**Quinn Taggart,** Senior Advisor, Global Brand Security

**Letitia Thian,** Manager, Marketing

**Sue Watts,** Global Leader, Marketing


cscdbs.com/de




DBS09172021