BEDEUTUNG DER DOMAIN-SICHERHEIT BEI LIEFERENGPÄSSEN

cscdbs.com/de

Kurzfassung

Neue Untersuchungen von CSC zeigen, dass Betrüger die Knappheit an Babynahrung im Jahr 2022 ausnutzten, um Verbraucher mit gefälschten Marken-Domains zu täuschen. Wesentliche Ergebnisse zeigen einen Anstieg der Domain-Registrierungen im Zusammenhang mit Babynahrung, die vertrauenswürdige Marken ausnutzen, um Verbraucher von authentischen Websites und Apps weg zu lenken. **84 %** dieser seit 2021 erstellten Web-Domains sind gefälscht, d. h. sie gehören nicht dem Markeninhaber, sondern Drittparteien. Dies kann für die Verbraucher in Bezug auf Produktsicherheit, Phishing-Angriffe, finanzielle Notlagen und Datenverluste ein echtes Problem darstellen – und auch für die Unternehmen, die Inhaber dieser Marken sind. Gefälschte Domains dieser Art wurden nicht nur am Markt für Babynahrung, sondern auch in der Halbleiterindustrie registriert, um Chip-Hersteller zu imitieren. **95 %** der seit 2021 erstellten registrierten Marken-Domains sind im Besitz von Drittparteien, die nicht der Markeninhaber sind.

Schließlich mangelt es einer beträchtlichen Anzahl von Unternehmen an Domain-Sicherheitshygiene, wodurch sie sich selbst einem größeren Domain-Sicherheitsrisiko aussetzen und das Ausmaß des Problems in allen kritischen Infrastruktursektoren deutlich wird. Domain-Sicherheitshygiene kann ein Unternehmen widerstandsfähiger gegen Risiken machen, die im Falle eines groß angelegten Angriffs auf einen Cloud-Anbieter oder einen Domain-Registrar (z. B. DNS-Hijacking oder DDoS-Angriff) oder bei Social-Engineering- oder Phishing-Angriffen bestehen.

Verbindung zwischen Domain-Sicherheit und Lieferkette

In den letzten zwei Jahren waren wir alle mit Lieferengpässen bei Artikeln konfrontiert, von denen wir uns vorher nicht vorstellen konnten, dass sie knapp werden könnten. Führungskräfte in den Unternehmen fragen sich: „Was sollten wir wissen, wissen es aber nicht?“ Es gibt einen bedeutenden Risikofaktor für Unternehmen, der nach wie vor unbemerkt bleibt – die Sicherheit der Registrierung von Marken-Webdomains.

Wie wir bei den jüngsten Angriffen auf die Lieferkette, z. B. bei **Colonial Pipeline** und **JBS Foods**, gesehen haben, hat ein Angriff auf ein Unternehmen über einen einzelnen Angriffspunkt das Potenzial, ein ganzes Netzwerk verbundener Unternehmen und Produkte, Partner, Lieferanten und Kunden zu beeinträchtigen – und kann dem Angreifer exponentielle Gewinne einbringen. Da Domains und das DNS miteinander verbunden sind, kann sich eine einzige Sicherheitsverletzung bei einem Domain-Registrar oder einem Cloud-Anbieter oder ein Phishing-Angriff unter Verwendung einer gefälschten Domain über die Internet-Lieferkette hinaus auf die Produkt- und Infrastrukturlieferketten auswirken.

Online-Betrug beinhaltet gefälschte Domain-Registrierungen und Angriffe auf Cloud-Anbieter, Domain-Registrare und DNS-Hosting-Anbieter.

Beispiel:

Die Knappheit an Babynahrung ist ein Problem für Marken außerhalb des Internets, das durch Cybersicherheitsrisiken vergrößert wird.

Die neue Untersuchung von CSC zeigt, dass das Risiko für Unternehmen und Verbraucher bei Lieferengpässen steigt

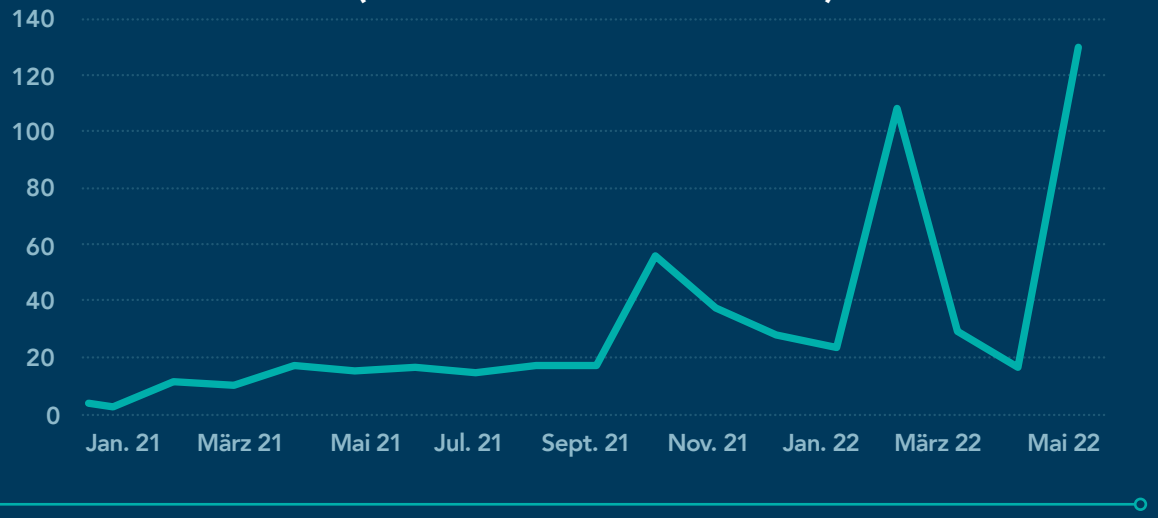
Gefälschte Domains stehen im Mittelpunkt des Betrugs im Internet, was zu Einnahmeverlusten, Reputationsschäden, Problemen mit der Verbrauchersicherheit und zusätzlichen Problemen mit der Cybersicherheit für Markeninhaber führen kann. CSC hat beobachtet, dass bei globalen und gesellschaftlichen Ereignissen, wie z. B. Lieferengpässen, mehr Domain-Registrierungen erfolgen, mit denen versucht wird, aus dem Ereignis Kapital zu schlagen. Im Januar 2022 veröffentlichte CSC **eine Untersuchung über den Anstieg betrügerischer COVID-bezogener Domains**, mit denen Cyber-Kriminelle Marken mit Impfstoffbezug und von Gesundheitsorganisationen für betrügerische Zwecke nutzen.

Das Forschungsteam von CSC untersuchte Web-Domains, die die wichtigsten Markennamen für Babynahrung und Halbleiter enthalten. In Einklang mit früheren Studien wurde festgestellt, dass die Registrierung gefälschter Domains zwischen 2021 und Mai 2022 zunahm.

Wichtige Ergebnisse: Engpass bei Babynahrung

CSC überprüfte Domains, die die fünf wichtigsten Markennamen für Babynahrung und andere relevante Suchbegriffe wie Babymilch, Muttermilchersatz und Babynahrung enthielten.

Monatliche Anzahl der Registrierungen von Drittparteien-Domains mit Bezug zu Babynahrung (Marken und Schlüsselwörter)



84 %

der Domains sind im Besitz von Drittparteien*

**Wir definieren Drittparteien-Domains als Domains, die nicht im Besitz der Markeninhaber und gefälscht sind.*

93 % nutzten Domain-Privacy-Dienste oder verbargen auch WHOIS-Daten.

Dies zeigt, dass sie versuchen, die Eigentümerschaft und Identität zu verschleiern oder zu verbergen, und damit möglicherweise unlautere Absichten verfolgen.

26 % sind mit MX-Records (E-Mail) konfiguriert.

Domains mit MX-Records können zum Versenden von Phishing-E-Mails oder zum Abfangen von E-Mails verwendet werden.

In der Untersuchung wurden folgende Domain-Registrare am häufigsten mit der Registrierung gefälschter Domains in Verbindung gebracht:

- GoDaddy.com, LLC
- Sav.com, LLC
- Chengdu West Dimension Digital Technology Co., Ltd

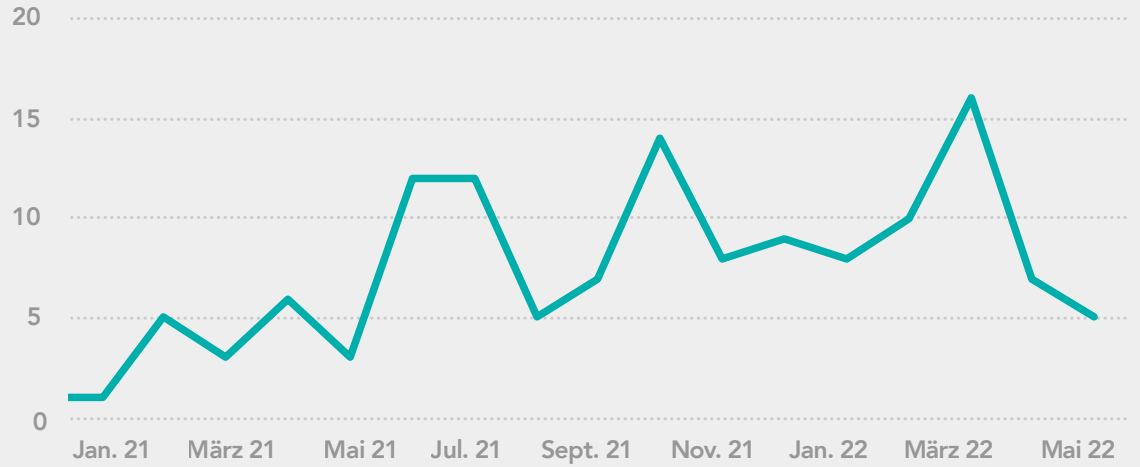
Folgende DNS-Hosting-Domains wurden in der Untersuchung am häufigsten mit der Registrierung gefälschter Domains in Verbindung gebracht:

- domaincontrol.com (Anbieter: GoDaddy)
- bodis.com (Anbieter: Bodis)
- registrar-servers.com (Anbieter: NameCheap)

Wichtige Ergebnisse: Halbleiterknappheit

CSC untersuchte Domains, die die sechs wichtigsten Halbleiter-Markennamen oder andere relevante Suchbegriffe wie Halbleiter- und Elektronik-Chip enthielten.

Monatliche Anzahl der Registrierungen von Drittparteien-Domains mit Bezug zu Halbleiter-Chips (Marken und Schlüsselwörter)



95 %

der Domains sind im Besitz von Drittparteien*

**Wir definieren Drittparteien-Domains als Domains, die nicht im Besitz der Markeninhaber und gefälscht sind.*

79 % **nutzten Domain-Privacy-Dienste oder verbargen auch WHOIS-Daten.**

Dies zeigt, dass sie versuchen, die Eigentümerschaft und Identität zu verschleiern oder zu verbergen, und damit möglicherweise unlautere Absichten verfolgen.

44 % **sind mit MX-Records (E-Mail) konfiguriert.**

Domains mit MX-Records können zum Versenden von Phishing-E-Mails oder zum Abfangen von E-Mails verwendet werden.

In der Untersuchung wurden folgende Domain-Registrare am häufigsten mit der Registrierung gefälschter Domains in Verbindung gebracht:

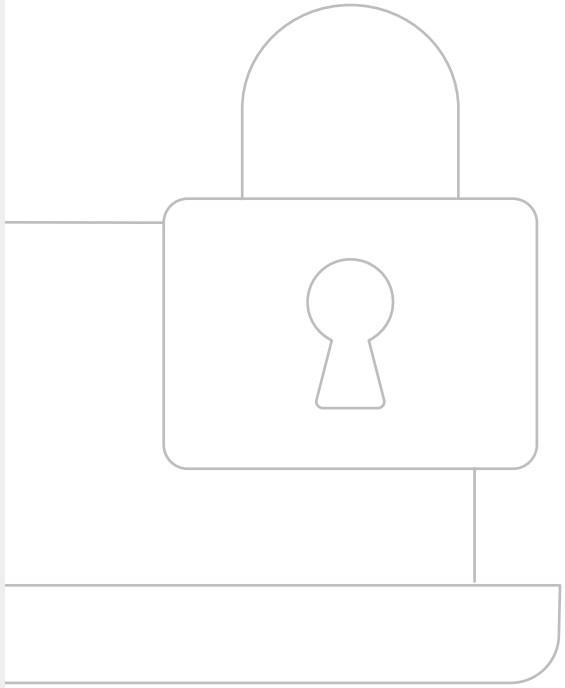
- GoDaddy.com, LLC
- Namecheap Inc.
- Dynadot LLC

Folgende DNS-Hosting-Domains wurden in der Untersuchung am häufigsten mit der Registrierung gefälschter Domains in Verbindung gebracht:

- domaincontrol.com (Anbieter: GoDaddy)
- registrar-servers.com (Anbieter: NameCheap)
- hichina.com (Anbieter: Alibaba)

Domain-Sicherheit und Cyber-Hygiene

Bei der Domain-Sicherheit ist es nicht nur wichtig, Ihr Unternehmen vor Registrierungen gefälschter Domains zu schützen, sondern auch proaktiv zu handeln und wichtige Sicherheitskontrollen als Teil der **Domain-Sicherheitshygiene** einzusetzen. CSC empfiehlt einen **DiD-Ansatz (Defense in Depth)**, der die folgenden hochentwickelten Sicherheitsmaßnahmen umfasst:



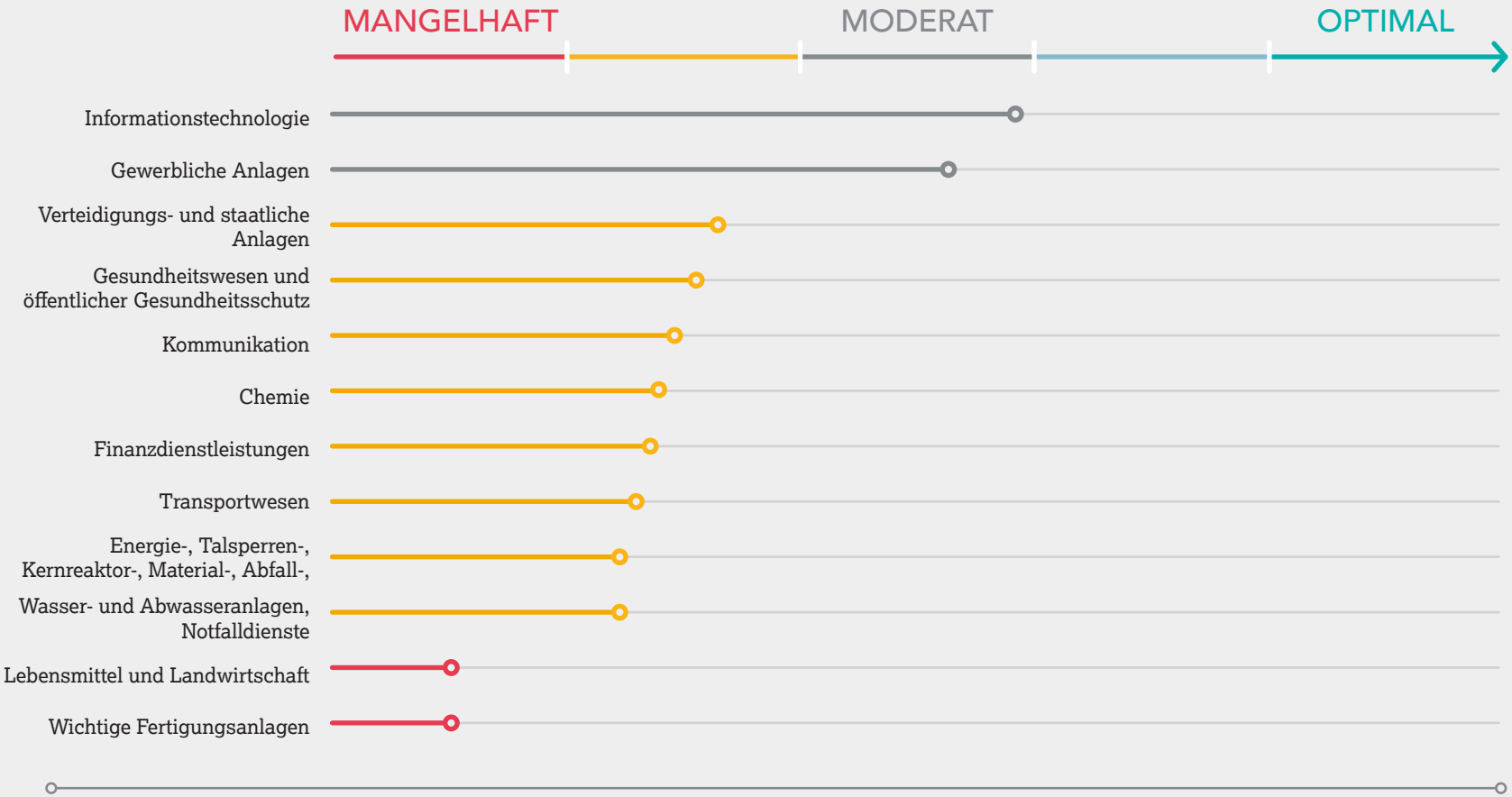
Maßnahmen von CSC zur Domain-Sicherheitshygiene

Domain-Sicherheitsmaßnahme	Zweck
DNS-Hosting-Redundanz	Schützt vor Ausfallzeiten und DDoS-Angriffen.
Domain Name System Security Extensions (DNSSEC)	Verhindert, dass Hacker die Kontrolle über eine Internet-Browsing-Sitzung übernehmen, mit dem Ziel, die Nutzer auf betrügerische Websites umzuleiten.
Sender Policy Framework (SPF)	E-Mail-Authentifizierungsstandards, die Spam, Spoofing und Phishing verhindern.
Domain-based Message Authentication, Reporting and Conformance (DMARC)	
DomainKeys Identified Mail (DKIM)	
MultiLock	Kombiniert Sperren auf Registrierungsbehörden- und Registrar-Ebene sowie eine WHOIS-Sperre, um unbefugte Änderungen von DNS-Einträgen und Domain-Hijacking zu verhindern.
Certification-Authority-Autorisierungs-Einträge (CAA-Einträge)	Stellt sicher, dass nur autorisierte Zertifizierungsbehörden ein Zertifikat ausgeben können.
Verwendung eines Enterprise-Class-Registrars	Ein solcher Registrar ist spezialisiert auf die Zusammenarbeit mit Unternehmen, die erweiterte Geschäftspraktiken, Fähigkeiten, Fachwissen und Supportpersonal in Bezug auf Domain- und DNS-Verwaltung sowie Sicherheit, Markenschutz und Betrugsabwehr, Daten-Governance sowie Cybersicherheit benötigen.

Betrachtung des Gesamtbildes in kritischen Branchen

Anhand unserer Daten aus dem **Bericht zur Domain-Sicherheit** haben wir uns die Global Forbes 2000-Unternehmen angesehen und die zugrunde liegenden Industriesektoren einem der 16 **CISA-Sektoren für kritische Infrastrukturen zugeordnet**. Anschließend haben wir die acht auf der vorherigen Seite genannten Signale für die Domain-Sicherheitshygiene beobachtet, um die Akzeptanz von Domain-Sicherheitsmaßnahmen in diesen kritischen Infrastruktursektoren einzustufen.

Bewertung der Risikominderung



Diese neuesten Ergebnisse verdeutlichen das größere Problem, mit dem zum Beispiel die Halbleiter- und Babynahrungsbranche, die kritische verarbeitende Industrie sowie die Lebensmittel- und Agrarbranche konfrontiert sind, und zeigen, dass die Situation bezüglich Domain-Sicherheit nach wie vor schlecht ist und sich kaum verbessert hat.

Der CSC-Bericht zur Domain-Sicherheit Domain Security Report: Forbes Global 2000 enthält eine eingehendere Analyse des Domain-Sicherheitsstatus in den kritischsten Wirtschaftszweigen rund um den Globus.

81 % sind einem größeren Risiko für das Domain- und DNS-Hijacking ausgesetzt, weil sie grundlegende Maßnahmen für die Domain-Sicherheit wie Registry-Lock für Domains 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.

50 % nutzen DMARC-Einträge zur E-Mail-Authentifizierung.

Risiken führen zu Notmaßnahmen und erfordern Maßnahmen

Käufer von knappen Waren setzen alles daran, einen Weg zu finden, um das zu kaufen, was sie brauchen. Marken und die Domain-Branche müssen wachsam sein und sicherstellen, dass die Verbraucher sichere und autorisierte Domains besuchen. Ein schwacher Domain-Sicherheitsstatus ist keine neue Herausforderung, aber er wird immer mehr zu einem zentralen Thema, das eine stärkere strategische Berücksichtigung erfordert. Unternehmen müssen das Internet durchforsten, um alles ausfindig zu machen und zu beseitigen, was ihre Marke verwässern oder schädigen könnte und den Endverbraucher auf einen Pfad zu betrügerischen Aktivitäten führt. Diese Risiken sind vermeidbar, und es muss Schluss damit sein, dass der Verbraucher auf der Suche nach dem, was er braucht, im Internet surft, nur um dann von einem Cyber-Kriminellen erwischt zu werden. Bessere Domain-Sicherheitsmaßnahmen müssen eingeführt werden, und die Wirtschaft muss umfassende Domain-Sicherheitsstandards akzeptieren und übernehmen.

Marken haben erhebliche Investitionen in die digitale Transformation, den Markenschutz und die Minderung von Cybersicherheitsrisiken getätigt. Doch die daraus resultierenden systemischen Risiken bei Domains und innerhalb des DNS führen zu Schwachstellen in der Lieferkette, Phishing, Betrug (d. h. Ransomware und Business Email Compromise), Markenmissbrauch sowie Fälschungen. Unternehmen, die kritische Infrastrukturen versorgen, müssen verstärkt ihre Möglichkeiten zur Verbesserung ihres Sicherheitsstatus ausschöpfen. Domain-Sicherheit ist ein Teil davon und ein systemisches Geschäftsrisiko.

Darüber hinaus sollte auch die Cyber-Versicherungsbranche diese Risiken bewerten. Die Prämien für Cyber-Versicherungen und das Risikoübernahmeverfahren ändern sich für viele Unternehmen, da die Versicherer beginnen, neue Metriken zu berücksichtigen, die die Versicherungspolice beeinflussen können. Ein schwacher Domain-Sicherheitsstatus, der sich in diesen Metriken widerspiegelt, könnte für diese Unternehmen langfristige Folgen haben. Untätigkeit ist keine Option, wenn es um die Domain-Sicherheit geht. CSC sieht einen dringenden Bedarf an umfassenderen Domain-Sicherheitsstandards sowie an Richtlinien oder Vorschriften für die täglichen Aktivitäten und Verhaltensweisen im DNS.

Mehr darüber, wie Sie den Schutz Ihres Unternehmens gewährleisten können, erfahren Sie hier:

EMPFEHLUNGEN ZUR DOMAIN-SICHERHEIT IN UNSEREM BLOG-BEITRAG ZUR LIEFERKETTE

CSC ist für die Unternehmen im Forbes Global 2000 und 100 Best Global Brands® in den Bereichen Unternehmens-Domains, Domain Name System (DNS), Verwaltung digitaler Zertifikate sowie Schutz digitaler Marken und Betrugsschutz der bevorzugte Anbieter. Angesichts der Tatsache, dass weltweit tätige Unternehmen in erheblichem Maße in ihren Sicherheitsstatus investieren, kann CSC ihnen dabei helfen, bekannte Sicherheitslücken in der Cybersicherheit zu verstehen und ihre digitalen Online-Vermögenswerte und Marken zu schützen. Durch den Einsatz von CSCs firmeneigener Technologie können Unternehmen ihren Sicherheitsstatus verbessern, um sich vor Cyber-Bedrohungen zu schützen, die auf ihre Online-Vermögenswerte und den Ruf ihrer Marke abzielen. So können sie verheerende Umsatzeinbußen und erhebliche finanzielle Strafen aufgrund von Richtlinien wie der Datenschutzgrundverordnung (DSGVO) vermeiden. CSC bietet auch Online-Markenschutz – eine Kombination aus Online-Markenüberwachung und Durchsetzungsmaßnahmen – und verfolgt dabei einen ganzheitlichen Ansatz zum Schutz digitaler Vermögenswerte, zusammen mit Anti-Fraud-Dienstleistungen zur Bekämpfung von Phishing. CSC hat seinen Hauptsitz seit 1899 in Wilmington, Delaware, USA, und verfügt über Niederlassungen in den Vereinigten Staaten, Kanada, Europa und im asiatisch-pazifischen Raum. CSC ist ein globales Unternehmen, das überall dort tätig werden kann, wo unsere Kunden sind – und das erreichen wir, indem wir Experten in jedem Geschäftsbereich beschäftigen, den wir bedienen. Besuchen Sie **cscdbs.com/de**.

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

Quinn Taggart, Senior Advisor, Global Brand Security

Sue Watts, Global Leader, Marketing

David Barnett, Head of Consultancy, Brand Monitoring

cscdbs.com/de

DBS07062022