CSC

Bericht zur Domainsicherheit 2024

EINFÜHRUNG

CSC war in den letzten fünf Jahren führend bei der Berichterstattung über den Domain-Sicherheitsstatus der Forbes Global-2000-Unternehmen. Wir analysieren die Einführung von Domain-Sicherheitsmaßnahmen zur Eindämmung von Cyberrisiken im Domain-Ökosystem der Global-2000-Unternehmen, die außerhalb der Firewall eines Unternehmens liegen, sowie Vorfälle von potenziellem Online-Markenmissbrauch und Rechtsverletzungen durch Dritte.

In diesem Jahr sehen wir, dass einige Unternehmen mehr Wert auf Sicherheit legen. Bei einem Teil der Unternehmen besteht jedoch immer noch ein erhebliches Sicherheitsrisiko. Wir wollen das Bewusstsein für diese Bedrohungen schärfen und unsere Best Practices für die Domain-Sicherheit weitergeben, um den Domain-Sicherheitsstatus aller Unternehmen zu verbessern.

CSC feiert den fünften Jahrestag seines jährlichen „Bericht zur Domainsicherheit“, und wir denken über unser kontinuierliches Engagement bei der Analyse der Domain-Sicherheitslage der Forbes Global-2000-Unternehmen nach. Auch in diesem Jahr, das mit dem 125-jährigen Bestehen von CSC zusammenfällt, wollen wir das Bewusstsein für Cyberrisiken außerhalb der Unternehmensgrenzen im digitalen Raum schärfen und auf die Notwendigkeit zuverlässiger Domain-Sicherheitsmaßnahmen hinweisen.

ZUSAMMENFASSUNG DER WICHTIGSTEN ERGEBNISSE

DIE BRANCHE FÜR MEDIZINISCHE GERÄTE UND GESUNDHEITSDIENSTLEISTUNGEN IST TROTZ ZUNEHMENDER CYBERANGRIFFE IM RANKING IN PUNCTO DOMAINSICHERHEIT ZURÜCKGEFALLEN

Die auffälligste Veränderung in Bezug auf die Domain-Sicherheit nach Branchen war in diesem Jahr bei Unternehmen aus dem Bereich Medizinische Geräte und Gesundheitsdienstleistungen zu beobachten, die um sieben Plätze von Platz 5 im Jahr 2023 auf Platz 12 im Jahr 2024 zurückfielen. Im Gegensatz dazu rückte der Sektor Technische Geräte und Ausrüstungen um acht Plätze von Platz 13 im Jahr 2023 auf Platz 5 im Jahr 2024 nach vorn.

80 % DER REGISTRIERTEN WEB-DOMAINS, DIE DEN GLOBAL-2000-MARKEN ÄHNELN (HOMOGLYPHEN), SIND IM BESITZ VON DRITTEN UND GEHÖREN NICHT ZU DIESER MARKE

Von den 80 % der Homoglyphen-Domains (ähnlich aussehende gefälschte Domains), die nicht den Global-2000-Markeninhabern gehören, verfügen 42 % über MX-Records (E-Mail-Austauschdatensätze), verglichen mit 40 % im Jahr 2023. Domains mit MX-Records können zum Versenden von Phishing-E-Mails oder zum Abfangen von E-Mails verwendet werden.

107 DER GLOBAL-2000-UNTERNEHMEN HABEN EINE DOMAIN-SICHERHEITSBEWERTUNG VON NULL

5 % der Global 2000-Unternehmen setzen keine der empfohlenen Maßnahmen zur Domainsicherheit ein und sind daher am stärksten gefährdet. Basierend auf unserer Analyse der Umsetzung wichtiger Domain-Sicherheitsmaßnahmen bedeutet eine Sicherheitsbewertung von Null, dass ein Unternehmen keine Maßnahmen ergriffen hat und somit dem höchsten Risiko für die Domainsicherheit ausgesetzt ist.

DIE NUTZUNG VON REGISTRY LOCK IST SEIT 2020 UM 7 PROZENTPUNKTE GESTIEGEN, ALLERDINGS IST DIE ANWENDUNG INSGESAMT MIT 24 % GERING

Registry Locks ermöglichen die durchgängige Sicherheit von Domaintransaktionen, um menschliches Versagen und das Risiko durch Dritte zu minimieren. Es ist ein äußerst kosteneffektives Mittel, um Domains vor versehentlichen oder unbefugten Änderungen oder Löschungen zu schützen.

DIE NUTZUNG VON DMARC IST SEIT 2020 UM 32 PROZENTPUNKTE GESTIEGEN

Im Jahr 2023 meldete die Anti-Phishing Working Group (APWG) einen Rekord von fast fünf Millionen registrierten Phishing-Angriffen, womit 2023 das Jahr mit den meisten Phishing-Angriffen war. Diese Zunahme der Angriffe hat dazu beigetragen, dass sich DMARC (Domain-based Message Authentication, Reporting and Conformance) durchgesetzt hat – ein E-Mail-Validierungssystem, das die E-Mail-Domain eines Unternehmens vor Spoofing und Phishing-Betrug schützen soll.

DIE EXTERNE ANGRIFFSFLÄCHE IST DAS EIGENTLICHE ÖKOSYSTEM DER DOMAIN

Während Cyberbedrohungen zunehmend KI-gestützt erfolgen, nehmen die Angriffe weiter zu. Daher ist die Domainsicherheit ein wichtiger Bestandteil der gesamten Cyber-Risikoevaluierung eines Unternehmens, die das Domain-Ökosystem eines Unternehmens als echte Schwachstelle für die in Abbildung 1 genannten Angriffe einbeziehen muss. Kompromittierte oder gekaperte legitime Domains oder böswillige Domainregistrierungen werden zur Ausführung aller in Abbildung 1 gezeigten Angriffe verwendet.

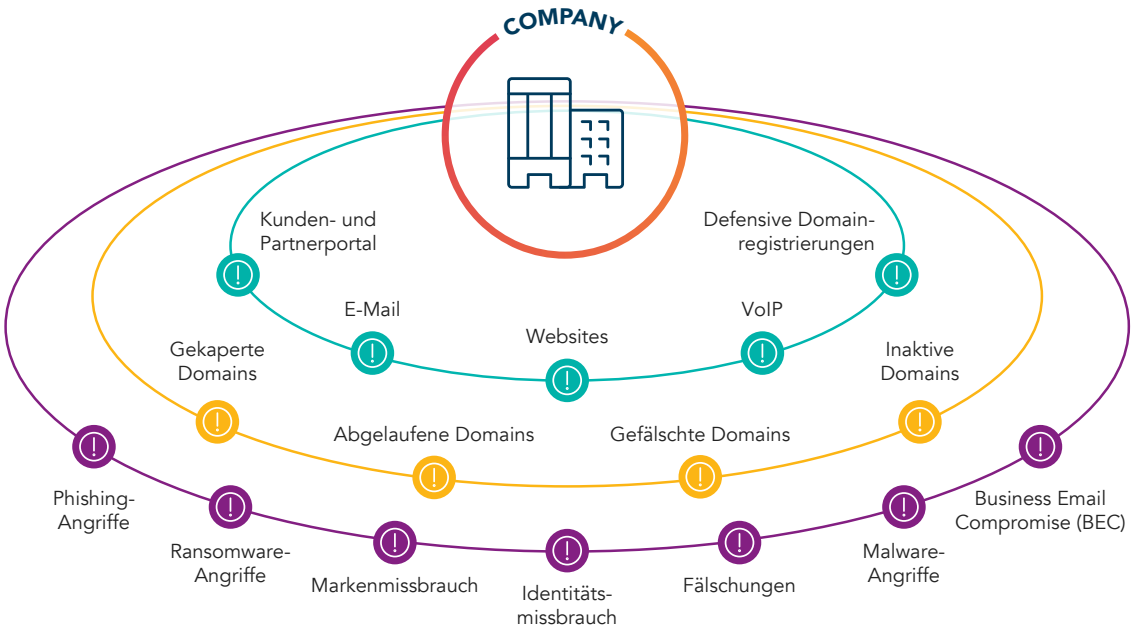
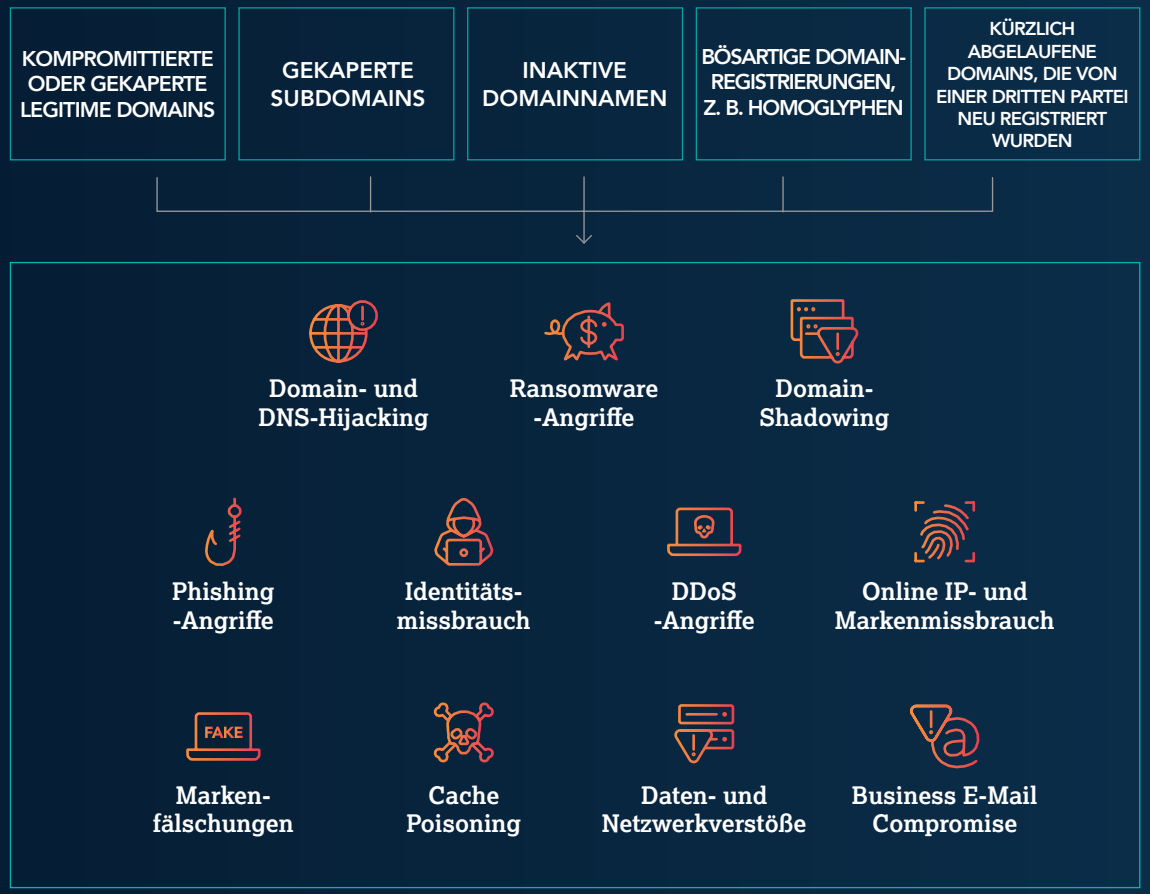


Abbildung 1: Die Galaxie des Domainnamen-Ökosystems

WAS IST DOMAINSICHERHEIT

Globale Unternehmen verlassen sich in allen Bereichen auf das Internet – für Websites, E-Mails, Authentifizierung, Voice-over-IP (VoIP), Kundenportale, Lieferantenanwendungen usw. Daher ist das Internet Teil der externen Angriffsfläche jedes Unternehmens und muss ständig auf Cyberkriminalität und Betrug überwacht werden. Angesichts der zunehmenden Cyberrisiken stehen Unternehmen und Cyberversicherer vor immer größeren Herausforderungen, diese Risiken zu quantifizieren und ihr Schadenspotenzial einzuschätzen. Dies bedeutet, dass Domainnamen entscheidende Elemente der Cybersicherheit eines Unternehmens sind, da das Internet und Domainnamen für die Geschäftsinfrastruktur und -kontinuität unerlässlich sind.



KOMPROMITTIERTE ODER GEKAPERTE LEGITIME DOMAINS

Jede ungesicherte Domain wird von Cyberkriminellen für ihre Zwecke missbraucht. Unternehmen sollten zum Schutz vor Hijacking einen mehrschichtigen „Defense in Depth“-Ansatz verfolgen.

GEKAPERTE SUBDOMAINS

Ein Subdomain-Hijack ist ein Angriff, bei dem Cyberkriminelle die Kontrolle über eine legitime, nicht mehr genutzte Subdomain erlangen, um bösartige Inhalte zu hosten und Unternehmen mit Phishing- oder Malware-Angriffen anzugreifen. Dazu nutzen sie veraltete DNS-Einträge (Dangling DNS) aus, um auf ihre eigenen Inhalte zu verweisen.

INAKTIVE DOMAINNAMEN

Cyberkriminelle können markengeschützte Domains registrieren und so lange inaktiv halten, bis sie bereit sind, sie in einem Phishing- oder Malware-Angriff zu missbrauchen. Inaktive Domains werden zunächst oft nicht entdeckt , weil sie nicht sofort die Indikatoren einer für einen Angriff registrierten Domain aufweisen – z. B. einen aktiven MX-Record –, die normalerweise Alarm auslösen würden.

BÖSARTIGE DOMAINREGISTRIERUNGEN

Es gibt unzählige Domain-Spoofing-Permutationen und Homoglyphen, die von Phishern und böswilligen Dritten eingesetzt werden. Ziel dieser gefälschten Domainregistrierungen ist es, das Vertrauen der Verbraucher in die betreffende Marke auszunutzen, um überzeugende Phishing-Angriffe oder andere Formen des digitalen Markenmissbrauchs zu starten.

KÜRZLICH ABGELAUFENE MARKENDOMAINS, DIE VON EINER DRITTEN PARTEI NEU REGISTRIERT WURDEN

Unternehmen können sich aufgrund von Kostendruck dafür entscheiden, zuvor defensiv registrierte Domainnamen ablaufen zu lassen. Dies nutzen Cyberkriminelle aus und registrieren diese Domainnamen sofort zu böswilligen Zwecken neu. Sie sind ständig auf der Suche nach verfügbaren Markendomains, die sie für ihre Zwecke nutzen können.

ERGEBNISSE UND ANALYSE: UMSETZUNG VON MASSNAHMEN ZUR DOMAINSICHERHEIT BEI DEN GLOBAL 2000

In dieser Analyse untersuchte CSC die Umsetzung von fünf wichtigen Domain-Sicherheitsmaßnahmen – DMARC, DNS-Redundanz, Registry Locks, Certificate Authority Authorization (CAA) Records und DNS Security Extensions (DNSSEC) – innerhalb der Global-2000-Liste. Im Anschluss daran haben wir eine tiefgreifende Analyse der Akzeptanz in den verschiedenen Branchen und Regionen durchgeführt.

TRENDS BEI DER UMSETZUNG VON MASSNAHMEN ZUR DOMAINSICHERHEIT (2020-2024)

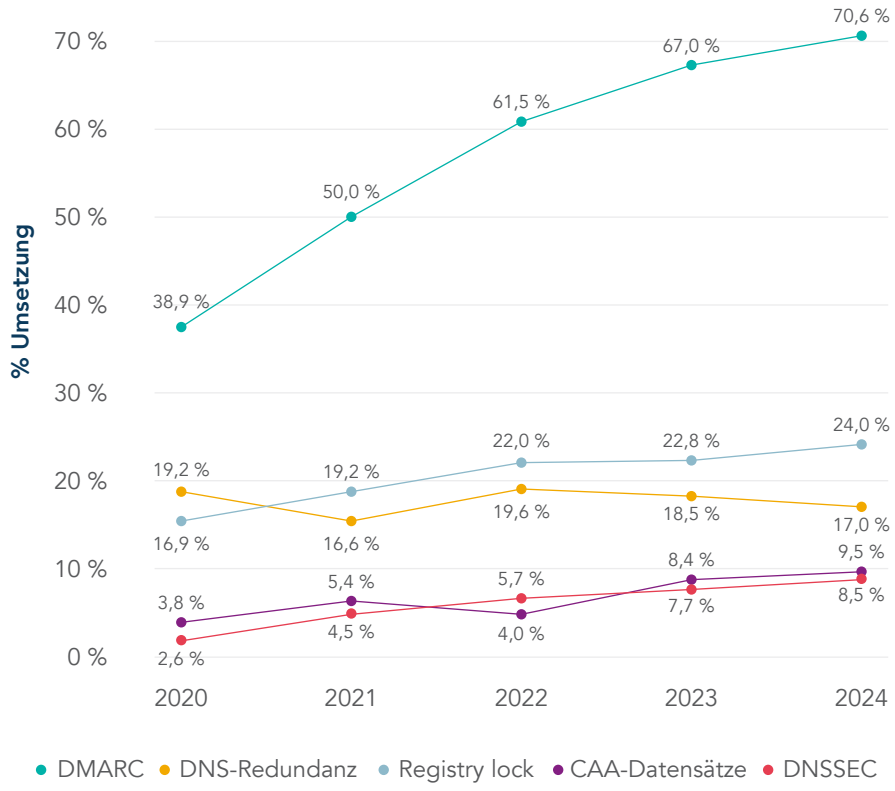


Abbildung 2: Umsetzung der fünf wichtigsten Domain-Sicherheitsmaßnahmen bei den Global 2000, 2020-2024

DMARC MIT DEM SCHNELLSTEN WACHSTUM

Angesichts der großen Zahl gemeldenter Phishing-Angriffe – einschließlich ihrer zunehmenden Größe und Komplexität – überrascht es nicht, dass die DMARC-Umsetzung schnell von 39 % im Jahr 2020 auf 71 % im Jahr 2024 gestiegen ist (Abbildung 3).

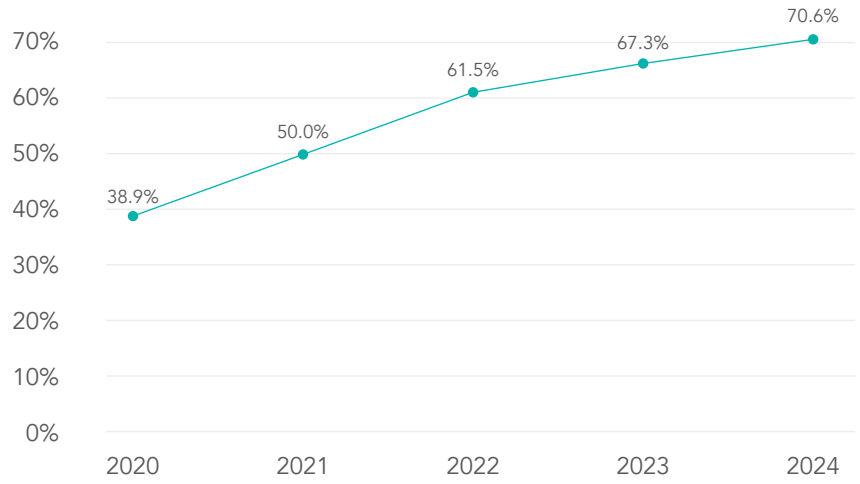


Abbildung 3: DMARC-Akzeptanzraten 2020-2024

Ein weiterer Faktor für die steigende Verbreitung von DMARC könnte die zunehmende Einführung von Markenindikatoren zur Identifizierung von Nachrichten (BIMI) in E-Mail-Clients sein, die die Anzeige von Markenlogos in authentifizierten E-Mails ermöglichen. DMARC ist eine Sicherheitsvoraussetzung für die Einrichtung von BIMI und beide arbeiten zusammen, um die Authentizität der Identität eines Unternehmens in einer E-Mail-Domain zu überprüfen.

STETIGE, ABER LANGSAME ZUNAHME BEI DER NUTZUNG VON REGISTRY LOCKS

Die Akzeptanzraten von Registry Locks stiegen von 17 % der Unternehmen im Jahr 2020 auf 24 % im Jahr 2024. Wir haben außerdem festgestellt, dass Unternehmen, die Enterprise-Class-Registrare nutzen, mit 45 % im Jahr 2024 auch häufiger Registry Lock einsetzen. Angesichts des wachsenden Drucks, die Cybersicherheit zu erhöhen, bieten immer mehr Registrierungsstellen Sperren für ihre Domänenerweiterungen an, um die Transaktionssicherheit von End-to-End-Domänennamen zu gewährleisten und so menschliche Fehler und das Risiko Dritter zu verringern.

Da sich das Domain-Portfolio eines Unternehmens ständig ändert, verwendet CSC einen prädiktiven Modellierungsalgorithmus, der mehr als 20 Attribute eines Domainnamens bewertet, um festzustellen, ob diese Domain geschäftskritische Aufgaben für den Betrieb Ihres Unternehmens und Ihre Marke online erfüllt, und empfiehlt wichtige Domains, die gesperrt werden sollten.

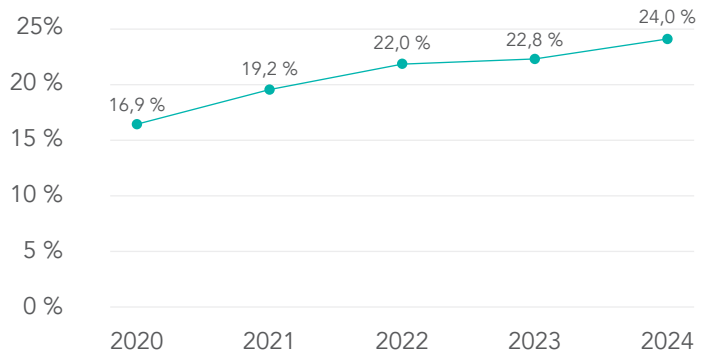


Abbildung 4: Registry Lock-Akzeptanzraten 2020-2024

SICHERHEITSMASSNAHMEN WIE DNS-REDUNDANZ, DNSSEC UND CAA-DATENSÄTZE

Der Prozentsatz der Unternehmen, die DNSSEC einsetzen, ist zwar immer noch gering, hat sich aber in den letzten fünf Jahren von 3 % im Jahr 2020 auf 9 % im Jahr 2024 verdreifacht. DNSSEC gewährleistet die Authentifizierung und Datenintegrität von DNS-Anfragen und -Antworten, was wiederum Cyberkriminelle daran hindert, den Internetverkehr auf bösartige Websites, wie z. B. Phishing-Websites, umzuleiten.

Überraschenderweise ist die DNS-Redundanz in diesem Jahr erneut um 1 % gesunken, so dass der Prozentsatz der Unternehmen, die der DNS-Redundanz Priorität einräumen, in diesem Jahr niedriger ist als im Jahr 2020. DNS-Redundanz ist eine kritische Komponente in der Kerninfrastruktur jedes Unternehmens. Wir stellen fest, dass die Implementierung dieser Sicherheitsmaßnahme abnimmt, was darauf zurückzuführen sein könnte, dass Unternehmen steigende Kosten und eine höhere Ressourcenzuweisung planen müssen.

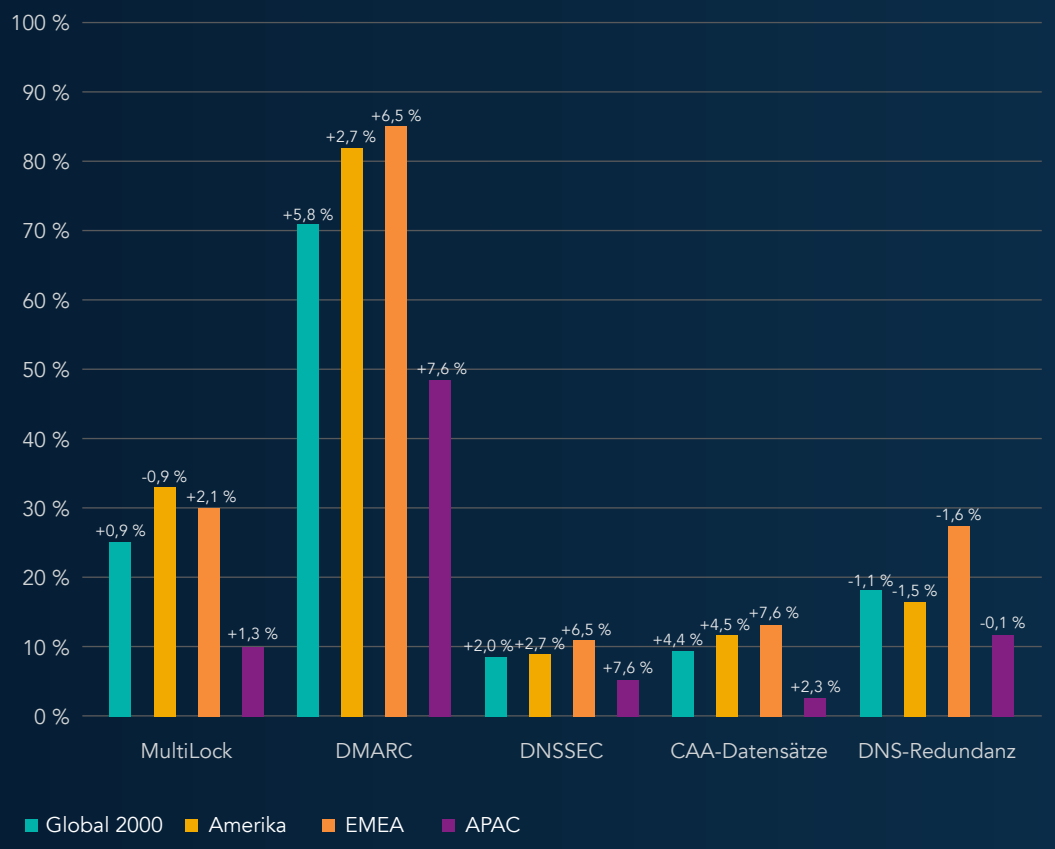
Schließlich stieg die Verwendung von CAA-Datensätzen von 4 % im Jahr 2020 auf 10 % im Jahr 2024. CAA-Einträge ermöglichen es Unternehmen, eine bestimmte Zertifizierungsstelle (CA) als einzigen Aussteller von digitalen Zertifikaten für die Domains ihres Unternehmens zu benennen. Dies verhindert, dass Cyberkriminelle eine nicht autorisierte Zertifizierungsstelle verwenden, um ein neues digitales Zertifikat zu erhalten, da ihre Anfrage fehlschlägt und das Unternehmen eine Warnung erhält.

Wir haben außerdem festgestellt, dass Unternehmen, die Enterprise-Class-Registrare nutzen, mit 45 % im Jahr 2024 auch häufiger Registry Lock einsetzen.

DOMAIN-SICHERHEITSMASSNAHMEN 2024

NACH REGION

Die EMEA-Region verzeichnete zwischen 2023 und 2024 das größte Wachstum bei der Umsetzung von Domain-Sicherheitsmaßnahmen.



+/- % Veränderung gegenüber dem Vorjahr

Abbildung 5: Einführung von Domainsicherheit nach Region

NACH BRANCHE

Gesundheitswesen fällt im Ranking 2024 um sieben Plätze zurück.

Branchenklassifizierung	Rang 2024	Rang 2023
Technische Geräte und Ausrüstungen	5	13 ↑
Medizinische Geräte und Gesundheits-dienstleistungen	12	5 ↓

Unter den 26 Forbes Global-2000-Branchen rutschte **Medizinische Geräte und Gesundheitsdienstleistungen** um sieben Plätze ab und ist unter den fünf besten Branchen nicht mehr vertreten. Der Absturz im Ranking von Platz 5 im Jahr 2023 auf Platz 12 im Jahr 2024 steht in krassem Gegensatz zum deutlichen Anstieg der Cyberangriffe auf Krankenhäuser und Gesundheitssysteme in diesem Jahr, zumal der Gesundheitssektor nun das häufigste Ziel von Ransomware-Angriffen ist.[1] Bereits 2024 hat der Gesundheitssektor 280 Cybervorfälle gemeldet. Das sind „24 % aller Cybervorfälle in den Vereinigten Staaten im Jahr 2024, womit der Gesundheitssektor vor allen anderen Branchen liegt.“[2]

Der Sektor Technische Geräte und Ausrüstungen rückte um acht Plätze auf Platz 5 nach vorn. Für Technologieunternehmen ist eine Platzierung unter den ersten fünf zweifellos von Vorteil. Ihr Wachstum könnte auf die Sicherheitsmaßnahmen zurückzuführen sein, die diese Unternehmen eingeführt haben, seit mit Solar Winds im Jahr 2020 größere Angriffe auf die Lieferkette begannen.

↑ DIE FÜNF AM BESTEN ABSCHNEIDENDEN BRANCHEN

- Unternehmensdienstleistungen und Geschäftsbedarf
- IT-Software und -Dienstleistungen
- Medien
- Einzelhandel
- Hardware und technische Ausrüstung

↓ DIE FÜNF AM SCHLECHTESTEN ABSCHNEIDENDEN BRANCHEN

- Bauwesen
- Nahrungsmittel, Getränke und Tabakwaren
- Lebensmittelmärkte
- Werkstoffe
- Öl- und Gasförderung

DOMAIN-SICHERHEITSMASSNAHMEN 2024 NACH REGISTRAR-TYP

Für diesen Bericht haben wir den Trend bei der Einführung von Domainsicherheit je nach Art des von den Global-2000-Unternehmen genutzten Domain-Registrars analysiert.

Viele Unternehmen befinden sich in dem Irrglauben, dass alle Registrare gleich sind. Falsches Vertrauen in Verbraucherregistrare, die möglicherweise der Domainsicherheit keine Priorität einräumen oder diese überhaupt nicht anbieten, kann sich negativ auf den allgemeinen Sicherheitsstatus eines Unternehmens auswirken. Dies gilt insbesondere für die Einführung von Registry Locks, da die meisten Verbraucherregistrare diese nicht unterstützen.

ENTERPRISE-CLASS-REGISTRARE:

Ein Enterprise-Class-Registrar legt den Fokus hingegen auf die Arbeit mit Unternehmen und Markeninhabern, die erweiterte Geschäftspraktiken und Funktionen, Expertise und personelle Unterstützung für die Domain- und DNS-Verwaltung sowie Sicherheit, Markenschutz, Betrugsabwehr, Daten-Governance und Cybersicherheit benötigen.

REGISTRARE FÜR VERBRAUCHER:

Ein Registrar für Verbraucher ist auf Domain-Dienste, Websites und E-Mail für Privatpersonen, Unternehmer und Kleinunternehmen, die gerade am anfangen, ausgerichtet.

UNTERNEHMEN, DIE AUF ENTERPRISE-CLASS-FÄHIGKEITEN SETZEN, HABEN EINE HÖHERE EINFÜHRUNGSRATE VON DOMAIN-SICHERHEITSMASSNAHMEN

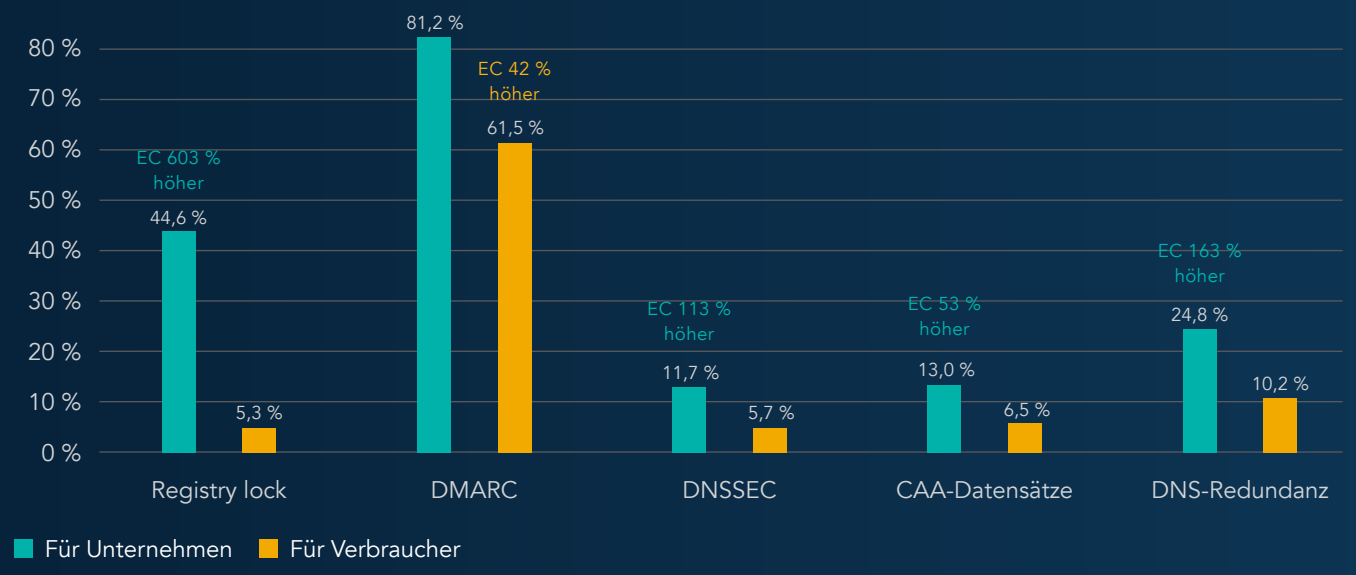


Abbildung 6: Reifegrad der Sicherheitsmaßnahmen – Enterprise-Class-Registrare (EC) im Vergleich zu Registraren für Verbraucher (CG)

DOMAIN-SICHERHEITSSTATUS

Ausgehend von der Wichtigkeit von acht grundlegenden Sicherheitsmaßnahmen, die wir nach der Risikostufe der Domainsicherheit eines Unternehmens gruppiert haben, hat CSC einen Durchschnittswert für jedes Unternehmen ermittelt. Dieser Durchschnittswert ergibt die Sicherheitsbewertung des Unternehmens, wobei ein höherer Wert für einen besseren Sicherheitsstatus steht, das Unternehmen also einem geringeren Risiko von Domain-Sicherheitsbedrohungen ausgesetzt ist.

WICHTIGE DOMAIN-SICHERHEITSMASSNAHMEN:

- Enterprise-Class-Registrar
- Registry Lock (MultiLock)
- CAA-Datensätze
- DNS-Redundanz
- DNSSEC
- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- DMARC

RISIKOSTUFEN DER DOMAINSICHERHEIT

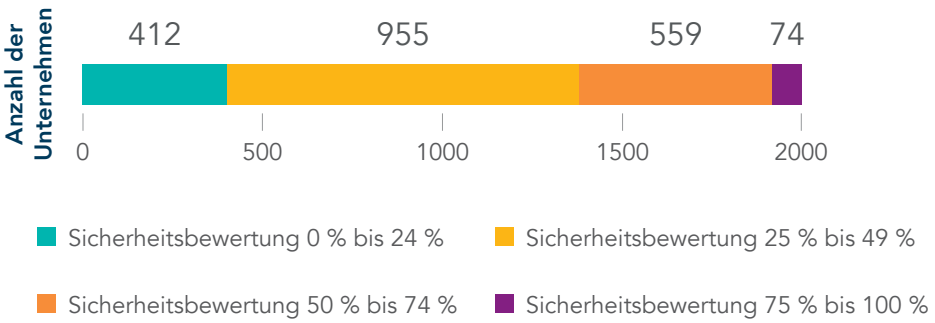


Abbildung 7: Domain-Sicherheitsbewertungen und zugehörige Risikostufen der Domainsicherheit von Global-2000-Unternehmen

68 % aller Global-2000-Unternehmen haben weniger als die Hälfte der empfohlenen Sicherheitsmaßnahmen umgesetzt.

DIE UNTERNEHMEN MIT DEN BESTEN WERTEN

Es gibt nur ein Unternehmen, das eine Bewertung von 100 % hat und auch im letzten Jahr eine Bewertung von 100 % hatte. Es gibt 12 Unternehmen, die eine Bewertung von 7 von 8 erreicht haben.

DIE UNTERNEHMEN MIT DEN SCHLECHTESTEN WERTEN

107 Unternehmen haben eine Domain-Sicherheitsbewertung von Null. Diese Unternehmen stammen hauptsächlich aus dem asiatisch-pazifischen-Raum (APAC), der 87 % der Unternehmen in dieser Gruppe ausmacht.

AUF GLOBAL-2000-UNTERNEHMEN ABZIELENDE VERDÄCHTIGE ODER BÖSARTIGE DOMAINAKTIVITÄTEN

Wir haben Domains identifiziert und analysiert, die Markennamen mit mehr als sechs Zeichen von Global-2000-Unternehmen enthalten, aber nicht im Besitz der Marken selbst sind. Ziel dieser Domainregistrierungen durch Dritte ist es, das Vertrauen in die anvisierten Marken auszunutzen, um Phishing-Angriffe, andere Formen des digitalen Markenmissbrauchs oder Verletzungen des geistigen Eigentums einzuleiten. Die Folge sind Umsatzeinbußen, die Umleitung von Datenverkehr und eine Beeinträchtigung des Markenrufs der betroffenen Marke.

Es gibt unzählige Domain-Spoofing-Taktiken und Permutationen, die von Phishern und böswilligen Dritten eingesetzt werden.

WIR KONZENTRIEREN UNS ABSICHTLICH AUF GÄNGIGE HOMOGLYPHEN, DA SIE ZU DEN GEFÄHRLICHSTEN ANGRIFFSMETHODEN VON BEDROHUNGSAKTEUREN ZÄHLEN

DOMAIN-SPOOFING-TAKTIKEN DOMAINS

Fuzzy Matches	cscg1obal.com | cscgl0bal.com
Homoglyphen – Internationalisierte Domains (IDNs)	ćscglobal.com | csçglobal.com
Cousin-Domains	cscglobal.jp | cscglobal.ec
Schlüsselwort-Übereinstimmung	cscglobalcovid.com | covidcscglobal.ar | covid19.com
Homophone (Soundex)	siesiglobal.com | cscclobol.com

Abbildung 8: übliche Domain-Spoofing-Taktiken

COMMON HOMOGLYPHS (FUZZY MATCHES) IN .COM DOMAINS

Da sie häufig in 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.

C0rnpanyNarne.com

Gängigste Zeichenersetzungen

c → e	0 → 0	m → n	l → I	m → rn
g → q	E → 3	S → 5	B → 8	l → 1

Abbildung 9: Übliche Homoglyphen (sog. Fuzzy Matches) in .COM-Domains

80 % DER HOMOGLYPHEN-DOMAINS SIND IM BESITZ VON DRITTEN.

Bei den Domains im Besitz von Dritten wurde Folgendes festgestellt:

42% haben 2024 MX-Records. 2023 lag dieser Anteil bei 40 %. Domains mit MX-Records können zum Versenden von Phishing-E-Mails oder zum Abfangen von E-Mails verwendet werden.

WIE WERDEN DRITTEN-DOMAINS EINGESETZT?

48% verweisen auf Werbung, Pay-per-Click-Webinhalte oder werden für Domain-Parking genutzt.

33% haben inaktive Websites.

2% verweisen auf bösartige Inhalte, die den Ruf einer Marke und das Vertrauen der Kunden schädigen können.

17% führen zu einer aktiven Website, die nicht mit dem Markeninhaber verbunden ist.

DOMAIN-REGISTRARE, BEI DENEN ES DIE MEISTEN GEFÄLSCHTEN DOMAINREGISTRIERUNGEN IM BESITZ VON DRITTEN GIBT

- GoDaddy®
- Namecheap™
- Network Solutions

VERDÄCHTIGE UND IN BÖSER ABSICHT REGISTRIERTE DOMAINS: AUF WEN WIRD ABGEZIELT?

BRANCHE	ANTEIL DER BEDROHUNGEN DURCH DOMAINFÄLSCHUNGEN
Bankwesen	19,9 %
Finanzdienstleistungen	7,2 %
IT-Software und -Dienstleistungen	7,2 %
Bauwesen	6,4 %
Versicherung	6,3 %
Öl- und Gasförderung	6,2 %
Versorgungsunternehmen	6,1 %
Investitionsgüter	5,5 %
Langlebige Verbrauchsgüter	5,3 %
Unternehmensdienstleistungen und Geschäftsbedarf	5,0 %
Transportwesen	4,9 %
Werkstoffe	4,7 %
Einzelhandel	4,6 %
Hardware und technische Ausrüstung	4,2 %
Arzneimittel und Biotechnologie	3,5 %
Nahrungsmittel, Getränke und Tabakwaren	3,4 %
Ausstattung und Dienstleistungen im Gesundheitswesen	3,4 %
Telekommunikationsdienste	3,0 %
Halbleiter	2,9 %
Chemikalien	2,6 %
Luft- und Raumfahrt und Verteidigung	2,0 %
Hotellerie, Gastronomie und Freizeit	1,7 %
Haushalts- und Körperpflegeprodukte	1,7 %
Lebensmittelmärkte	1,5 %
Handel	1,2 %
Medien	1,1 %

EINBLICKE IN DIE DOMAINSICHERHEIT: WAS UNS DIE FLUT NEUER DOMAINS WÄHREND DER OLYMPISCHEN SPIELE 2024 GELEHRT HAT

Ebenso wie andere globale Großveranstaltungen waren auch die Olympischen Spiele in Paris im Juli 2024 einer Reihe von digitalen Bedrohungen durch Betrüger ausgesetzt, die versuchten, die globale Reichweite der Spiele durch gefälschte Produkte, gefälschte Tickets, betrügerische Streaming-Websites und Phishing-Angriffe auszunutzen. Um diese Bedrohungen zu bekämpfen, sollte die Überwachung globaler Ökosysteme von Domains – wie gefälschter, abgelaufener, neu registrierter oder reaktivierter Domains – für jedes Unternehmen und jede Marke im Rahmen seiner Sicherheits- und Online-Markenschutz-Strategie Priorität haben. Unternehmen sollten besonders auf **inaktive Domains** achten – solche, die zwar noch nicht missbräuchlich eingesetzt werden, aber Anzeichen einer sich entwickelnden Angriffsinfrastruktur aufweisen.

HIGHLIGHTS

Bei unseren Recherchen haben wir 8.857 eindeutige Domainnamen Dritter identifiziert, die den Begriff „Olympia“ oder verwandte Schlüsselbegriffe wie „Paris 2024“ enthielten (siehe Abbildung 10). Wir haben die Domainaktivitäten, einschließlich Neuregistrierungen, Löschungen und erneuter Registrierungen, im Zeitraum vom 1. August 2023 bis zum 13. August 2024 untersucht. Wie aus Abbildung 10 hervorgeht, haben wir einen besonders starken Anstieg der Neuregistrierungsaktivitäten beobachtet, der mit dem Beginn der Olympischen Spiele am 26. Juli und deren Ende am 13. August zusammenfiel. Unter den noch registrierten Domains waren 49 % inaktiv und verfügten über keine aktive Website. Von diesen Domains verfügten jedoch 25 % über einen MX-Record und 8 % über ein mit der Domain verknüpftes SSL-Zertifikat.

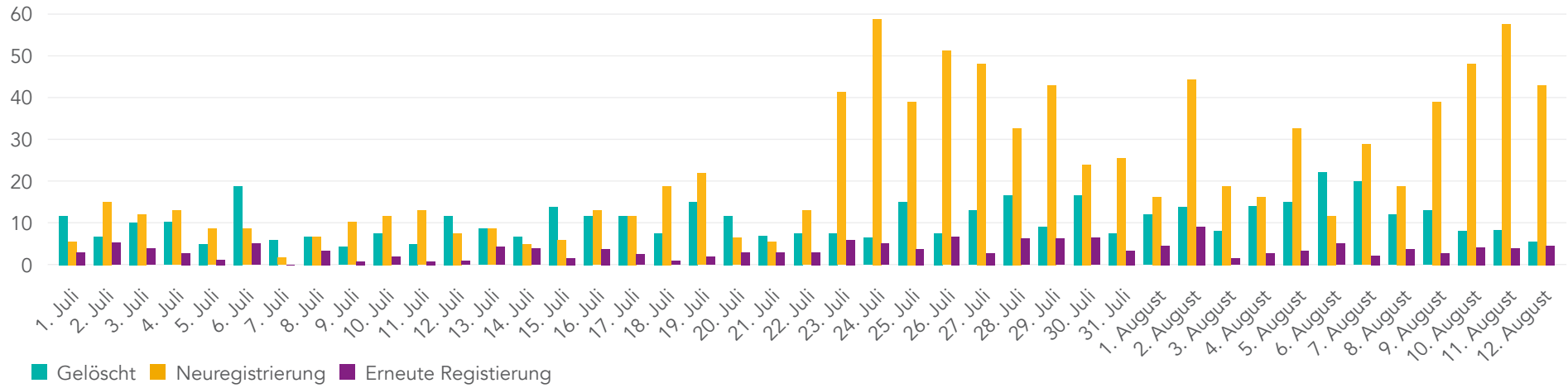


Abbildung 10: Verlauf der Domainregistrierung zwischen dem 1. Juli 2024 und dem 1. August 2024 (60 Tage)

WICHTIGSTE ERKENNTNIS

Eine kontinuierliche Echtzeit-Überwachung dieser Domains ist unbedingt erforderlich, da inaktive Domains jederzeit für Cyberangriffe missbraucht werden können. Indem Unternehmen böswillig genutzte Domainnamen verfolgen, können sie potenzielle Risikofaktoren besser erkennen, bevor sie aktiviert werden.

CONCLUSION

Wenn sich ein Unternehmen nicht um die Domainsicherheit kümmert, kann das katastrophale Folgen haben. Ungeschützte Domains stellen eine erhebliche Bedrohung für die Cybersicherheit eines Unternehmens, den Datenschutz, die Sicherheit der Verbraucher, das geistige Eigentum, die Lieferketten, den Umsatz und den Ruf dar.

Unternehmen sollten, sofern sie dies nicht bereits tun, das gesamte globale Domainnamen-Ökosystem einschließlich der generischen Top-Level-Domains und der länderspezifischen Top-Level-Domains überprüfen. Fortschrittliche Überwachungsdienste wie die 3D Domain Security and Enforcement Solution von CSC können eine breitere Palette von Domain-Variationen erkennen, die über exakte Übereinstimmungen, Wildcards und Tippfehler hinausgehen. Darüber hinaus müssen Unternehmen mit einem Anbieter zusammenarbeiten, der in der Lage ist, verschiedene Bedrohungen wie z. B. Phishing-Websites, Malware-Downloader, Typosquatting-Domains, betrügerische Suchmaschinenoptimierungsseiten sowie Social-Media-Portale, mobile App-Stores und Marktplätze, die gefälschte Produkte verkaufen, zu blockieren.

Sehen Sie sich die Liste der defensiven und proaktiven Sicherheitsmaßnahmen von CSC an, um Ihre Domains und Marken mit einem mehrschichtigen „Defense in Depth“-Ansatz zur Domainsicherheit zu schützen.

Laden Sie unsere Checkliste für Domainsicherheit herunter.

CSC ist der vertrauenswürdige Anbieter von Sicherheit und Threat Intelligence der Wahl für Unternehmen im Forbes Global 2000 und für die 100 Best Global Brands (Interbrand®) mit Schwerpunkten in den Bereichen Domainsicherheit und -management sowie digitalem Markenschutz und Betrugssicherung. Angesichts der erheblichen Investitionen, die globale Unternehmen in ihre Sicherheitsposition tätigen, kann unsere Plattform DomainSec℠ ihnen helfen, bestehende Versäumnisse bei der Cybersicherheit zu verstehen und ihre digitalen Online-Assets und -Marken zu schützen. Durch den Einsatz der firmeneigenen Technologie von CSC können Unternehmen ihren Sicherheitsstatus verbessern, um sich vor Cyberbedrohungen zu schützen, die auf ihre Online-Assets und den Ruf ihrer Marke abzielen. So können sie verheerende Umsatzeinbußen vermeiden. CSC bietet darüber hinaus Online-Markenschutz – eine Kombination aus Online-Markenüberwachung und Durchsetzungsmaßnahmen – einschließlich einer mehrdimensionalen Übersicht über verschiedene Bedrohungen außerhalb der Firewall, die bestimmte Domains ins Visier nehmen. Unsere Lösungen werden ergänzt durch Betrugspräventionsdienste, die Phishing bereits in der Frühphase des Angriffs bekämpfen. 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 in der Lage ist, überall dort tätig zu sein, wo unsere Kunden sind – und das erreichen wir, indem wir Experten in jedem Geschäftsbereich beschäftigen, den wir bedienen.

Kontaktieren sie uns

cscdbs.com/de

Copyright ©2024 Corporation Service Company. Alle Rechte vorbehalten.

CSC ist eine Dienstleistungsgesellschaft und bietet keinerlei rechtliche oder finanzielle Beratung an. Die hier aufgeführten Materialien dienen ausschließlich Informationszwecken. Wenden Sie sich an Ihren Rechts- oder Finanzberater, um zu ermitteln, inwiefern diese Informationen auf Sie zutreffen.

[1] npr.org/sections/shots-health-news/2024/09/17/nx-s1-5111590/cyberattacks-ransomware-health-care-federal-response

[2] tebra.com/theintake/practice-operations/medical-news/the-major-cyberattacks-that-have-affected-healthcare-systems-in-2024

DBS10232024