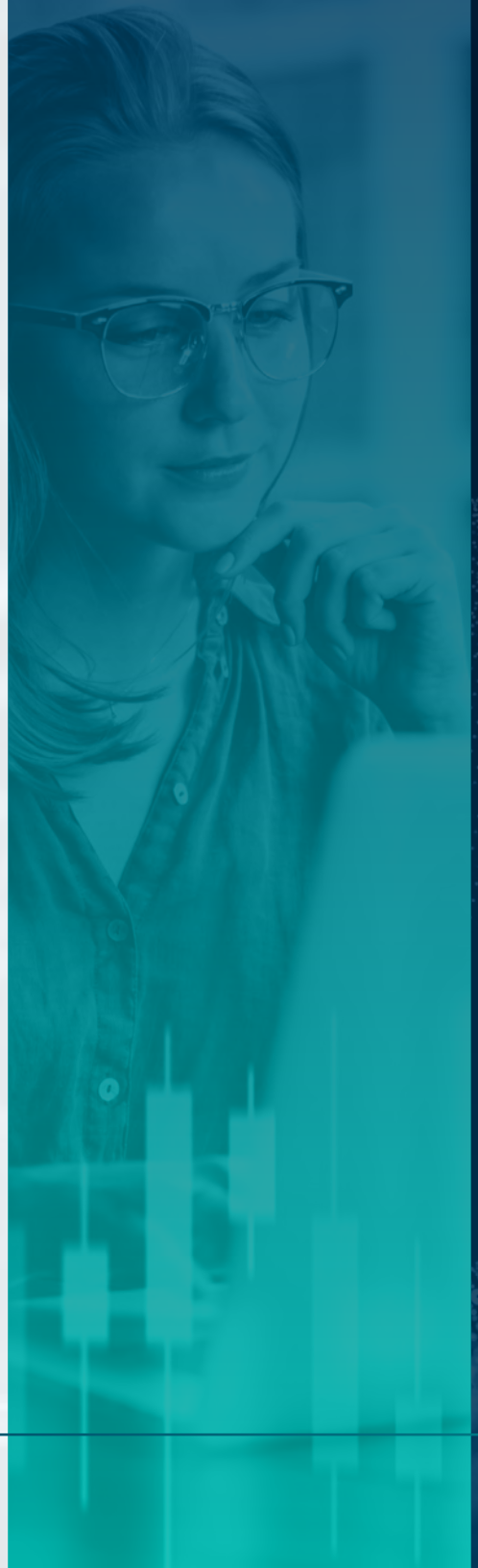
CSC



2023

BERICHT ZUR DOMAIN-SICHERHEIT

CSC war in den letzten vier Jahren führend bei der Berichterstattung über den Domain-Sicherheitsstatus der Forbes Global 2000-Unternehmen. 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 möchten das Bewusstsein für diese Bedrohungen schärfen und unsere Best Practices für die Domain-Sicherheit weitergeben.

Wir haben die Einführung von Domain-Sicherheitsmaßnahmen zur Eindämmung von Cyberrisiken im Domain-Ökosystem der Global 2000-Unternehmen, das außerhalb der Firewall eines Unternehmens liegt, sowie Vorfälle von potenziellem Online-Markenmissbrauch und Rechtsverletzungen durch Dritte analysiert.

ZUSAMMENFASSUNG DER WICHTIGSTEN ERGEBNISSE

43 % DER .AI-DOMAINS SIND DURCH DRITTEN REGISTRIERT

Unternehmen haben es entweder versäumt, ihre eigenen .AI-Domain-Namen zu registrieren, oder sie stellen jetzt fest, dass viele gewiefte Online-Betrüger diese Domains stattdessen erworben haben. Dies wird durch einen Anstieg der Domain-Dispute im Zusammenhang mit .AI-Endungen im Jahr 2023 um 350 % im Vergleich zum Vorjahr belegt.

21 % DER DNS-DATENSÄTZE AUS SUBDOMAINS VERWEISEN AUF INHALTE, DIE NICHT AUFGELÖST WERDEN KÖNNEN, SODASS UNTERNEHMEN ANFÄLLIG FÜR SUBDOMAIN-HIJACKING SIND

CSC hat mehr als 6 Millionen Domain Name System (DNS)-Datensätze aus unserer Datenbank analysiert und diese auf knapp über 440.000 DNS-Datensätze gefiltert. Dafür haben wir uns Einträge und CNAMEs angesehen, die auf Cloudinfrastrukturen verweisen. Hier könnte es potenziell zu Gefährdungen durch Subdomain-Hijacking kommen.

79 % DER REGISTRIERTEN DOMAINS, DIE DEN GLOBAL 2000-MARKEN ÄHNELN (HOMOGLYPHEN), SIND IM BESITZ VON DRITTEN

Von den 79 % der (gefälschten) Homoglyphen-Domains, die nicht den Global 2000-Markeninhabern gehören, verfügen 40 % über MX-Records, die bei zukünftigen Phishing-Angriffen verwendet werden könnten.

46 % DER UNTERNEHMEN, DIE MIT ENTERPRISE-CLASS-REGISTRAREN ARBEITEN, NUTZEN AUCH REGISTRY–LOCK

Ein Registry-Lock ermöglicht die durchgängige Sicherheit von Domain-Transaktionen, um menschliches Versagen und das Risiko durch Fremde zu minimieren. Es ist ein äußerst kostengünstiges Mittel, um Domains vor versehentlichen oder unbefugten Modifizierungen oder Löschungen zu schützen. Nur 7 % der Unternehmen, die mit Registraren für Verbraucher arbeiten, nutzen Registry-Lock. (Siehe Enterprise-Class-Registrare im Vergleich zu Registrare für Verbraucher.)

112 UNTERNEHMEN HABEN EINEN DOMAIN-SICHERHEITS-SCORE VON **0 %**

6 % der Global 2000-Unternehmen setzen keine der empfohlenen Maßnahmen zur Domain-Sicherheit ein und sind daher am stärksten gefährdet. Basierend auf unserer Analyse der Einführung von wichtigen Domain-Sicherheitsmaßnahmen bedeutet ein Risikoniveau von 0 %, dass ein Unternehmen keine Maßnahmen ergriffen hat und damit dem höchsten Risiko für die Domainsicherheit ausgesetzt ist.

6 % DMARC-WACHSTUM UND DAS HÖCHSTE WACHSTUM DER LETZTEN VIER JAHRE

Die Einführung von DMARC (Domain-based Message Authentication, Reporting and Conformance) – ein E-Mail-Validierungssystem, das die E-Mail-Domain eines Unternehmens vor Spoofing und Phishing-Betrug schützen soll – ist seit 2020 um 28 % gestiegen.

2023 LIEFERT ÜBERZEUGENDE ARGUMENTE FÜR DOMAIN-SICHERHEIT

Während Cybersicherheit sich zunehmend auf KI stützt, nehmen die Angriffe weiter zu. Daher ist die Domain-Sicherheit ein wichtiger Bestandteil der gesamten Cyber-Risikoevaluierung eines Unternehmens. Die folgenden drei Domain-Sicherheitslücken werden genutzt, um alle unten aufgeführten Angriffe zu ermöglichen.

KOMPROMITTIERTE ODER GEHIJACKTE LEGITIME DOMAINS

BÖSARTIGE DOMAIN-REGISTRIERUNGEN, Z. B. HOMOGLYPHEN

GEHIJACKTE SUBDOMAINS

WAS IST DOMAIN-SICHERHEIT

Globale Unternehmen verlassen sich für alles auf das Internet – für Websites, E-Mails, Authentifizierung, Voice-over-IP (VoIP) und mehr. Daher ist das Internet Teil der externen Angriffsfläche jedes Unternehmens und muss kontinuierlich auf Cyberkriminalität und Betrug überwacht werden. Angesichts der zunehmenden Cyberrisiken stehen Unternehmen und Cyberversicherer vor immer größeren Herausforderungen, wenn es darum geht, die Risiken zu quantifizieren und ihre Schadensmöglichkeiten zu bewältigen. Gefühlt jeden Tag erfahren wir mehr über neue Entwicklungen in Bezug auf Angriffe auf die Lieferkette, Ransomware und Phishing-Angriffe und es wird immer komplizierter, die nötige Infrastruktur aufzubauen, um diese Angriffe abzuwehren.

CSC verwaltet die Domain-Sicherheit mit einem mehrschichtigen Ansatz und nutzt dazu eine proprietäre Technologie. In erster Linie geht es darum, die Online-Präsenz einer Marke zu sichern, indem das Domain-Portfolio – das durch Übernahmen aus mehreren Marken bestehen kann – und ein Online-DNS-Footprint gesichert werden. Zweitens überwachen und analysieren wir Bedrohungsvektoren, die auf Online-Marken abzielen, und gehen dagegen vor.

WAS IST SUBDOMAIN-HIJACKING?

Subdomain-Hijacking ist ein Angriff, bei dem Cyberkriminelle die Kontrolle über eine legitime Subdomain erlangen, die nicht mehr verwendet wird, und dort schädliche Inhalte hochladen, um Unternehmen mit Phishing- oder Malware-Kampagnen anzugreifen. Dazu nutzen sie vergessene DNS-Datensätze intelligent aus, um auf ihre eigenen Inhalte zu verweisen.

NEUE BEDROHUNG: SUBDOMAIN-HIJACKING

21 % der DNS-Datensätze aus aktiven Subdomains können nicht aufgelöst werden, sodass Unternehmen anfällig für Subdomain-Hijacking sind.

CSC hat mehr als 6 Millionen DNS-Datensätze aus unserer Datenbank analysiert. Dafür haben wir uns Einträge und CNAMEs angesehen haben, die auf Cloudinfrastrukturen verweisen, und konnten diese auf knapp über 440.000 aktive DNS-Datensätze filtern. Bei diesen Subdomains kann es zu Subdomain-Hijacking durch Kriminelle kommen. Wir haben diese Untersuchung durchgeführt, um den aktuellen Stand der Verwaltung von Subdomains bei Unternehmen zu verstehen und nachzuvollziehen, wie sich dies auf den allgemeinen Sicherheitsstatus des Unternehmens auswirkt.

SO ERKENNEN SIE SUBDOMAIN-HIJACKING FRÜHZEITIG

1. Führen Sie eine vollständige Prüfung der vorhandenen DNS-Zonendateien durch und prüfen Sie jeden Datensatz.
2. Identifizieren Sie die Domainnamen und die entsprechenden Subdomains, die aktiv sein sollten.
3. Sorgen Sie für eine kontinuierliche Überwachung durch regelmäßige Scans der aktiven DNS-Datensätze, um Statusänderungen zu erfassen und rund um die Uhr sofortige Warnungen an das SOC-Team zu generieren.
4. Ergreifen Sie sofort Durchsetzungsmaßnahmen gegen rechtswidrig geschaltete Webseiten und nutzen Sie Blockierungsfunktionen, um schädliche Online-Inhalte zu verhindern.

WIE KANN ES ZU SUBDOMAIN-HIJACKING KOMMEN, OHNE DASS IHRE LEGITIMEN SUBDOMAINS TATSÄCHLICH GEHACKT WERDEN?

Große Unternehmen mit unterschiedlichen Markenportfolios und internationalen Niederlassungen wissen oft nicht, wie groß ihr globaler digitaler Fußabdruck ist. Digitale Datensätze sammeln sich im Laufe der Zeit an, was die Aufrechterhaltung der Cyberhygiene zu einer echten Herausforderung macht. Unternehmen setzen beim Zugriff auf neue Technologien immer mehr auf Cloudanbieter, doch diese Zunahme der DNS-Datensätze – mehr denn je, und das bei zunehmend komplexeren Umgebungen – birgt für sie ein erhöhtes Risiko. Ohne einen Überblick über die digitalen Datensätze und eine tägliche Überwachung werden die digitalen Vermögenswerte von Unternehmen schnell unübersichtlich, was die Cyberhygiene komplexer macht und es Cyberkriminellen leicht macht, Schwachstellen auszunutzen.

Cyberkriminelle durchsuchen Infrastrukturen wie die Cloud und öffentlich zugängliche Dienste. Dazu gehört die Suche nach DNS-Zoneneinträgen, die auf Webservices verweisen, die nicht mehr von einer Marke verwendet werden. Indem sie Inhalte auf Cloudanbietern hosten, die keine Verifizierungsprüfungen durchführen, können Kriminelle eine zuvor genutzte Zone als Ziel anfordern und Webnutzer auf diese Subdomains umleiten. Diese sind dann mit eigenen unrechtmäßigen Inhalten versehen. All dies funktioniert, ohne dabei in die Infrastruktur eines Unternehmens oder das Servicekonto eines Drittanbieters einzudringen. ZDNet berichtete, dass es bei Microsoft® zu Subdomain-Hijacking kam, bei dem Kriminelle auf den Subdomains des Unternehmens Poker-Casinos anzeigten.

Diese Anhäufung inaktiver Zonen, die nicht auf Inhalte verweisen, wird als „dangling DNS" (wörtl. „hängendes DNS") bezeichnet, und setzt Unternehmen dem Risiko von Subdomain-Hijacking aus.

Dies ermöglicht weitere Cyberangriffe auf Marken, wie beispielsweise Phishing- und Malware-Angriffe, die zu Einnahmeverlusten, Datenextraktion, Verlust des Kundenvertrauens und Reputationsschäden führen können. Laut einer Studie des in Wien ansässigen IT-Sicherheitsberatungsunternehmens Certitude Consulting, die kürzlich in Security Week veröffentlicht wurde, sind Tausende von Unternehmen anfällig für diese Angriffe.

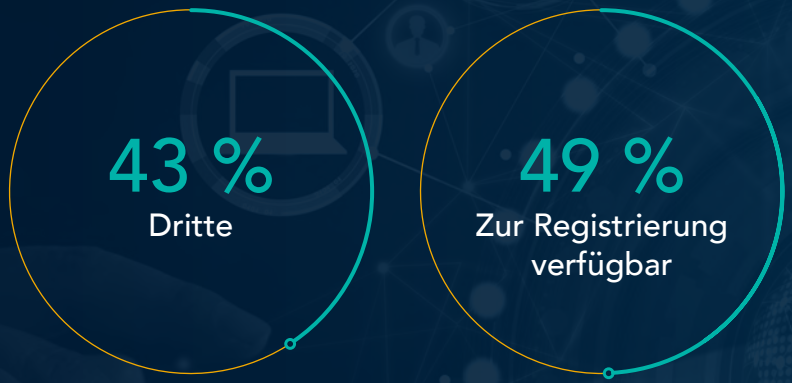
Die Verwaltung von DNS-Datensätzen muss fester Bestandteil der Cyberhygiene sein. Seit mehr als 20 Jahren sind Unternehmen dem Risiko schlechter Verwaltung ausgesetzt, da sie unterschiedliche Inhaber, Richtlinien und Anbieter für die Verwaltung von DNS beschäftigen. Das Ganze wird bei Fusionen und Übernahmen noch komplizierter. Darüber hinaus besteht eine generelle Angst davor, etwas zu löschen, das Inhaber nicht eindeutig zuordnen können.

Subdomain-Hijacking ist eine von vielen Bedrohungen für die Domain-Sicherheit, die heute bestehen, einschließlich Domain- und DNS-Hijacking, Domain Shadowing und Cache Poisoning. Diese Bedrohungen ermöglichen oft noch gefährlichere Phishing- und Ransomware-Angriffe, Business Email Compromise (BEC) oder Datenextraktion.

Lesen Sie unseren Bericht zu Subdomain-Hijacking-Schwachstellen oder wenden Sie sich an CSC, um mehr zu erfahren

43 % DER .AI-DOMAINS SIND DURCH DRITTEN REGISTRIERT

Unternehmen haben es entweder versäumt, ihre eigenen .AI-Domain-Namen zu registrieren, oder sie stellen jetzt fest, dass viele gewiefte Online-Betrüger diese Domains stattdessen erworben haben.



Die technologische Landschaft hat sich mit der Verbreitung von Technologien der künstlichen Intelligenz (KI) erheblich verändert. Diese Verschiebung zeigt sich in dem bemerkenswerten Anstieg der Registrierung von .AI-Domains, der die weit verbreitete Annahme und Begeisterung für KI widerspiegelt. CSC ist an der Spitze dieses Trends und berät seine Kunden proaktiv über die Bedeutung einer Registrierungs- und Durchsetzungsstrategie für .AI-Domains[1].

Darüber hinaus ist im Jahr 2023 ein deutlicher Anstieg der Domain-Dispute im Zusammenhang mit .AI-Endungen zu verzeichnen. Stand September 2023 ist ein deutlicher Anstieg gegenüber den Vorjahren zu verzeichnen. Dieser Anstieg von 350 % gegenüber dem Vorjahr und die Tatsache, dass die Gesamtzahl der Fälle bereits die Gesamtzahl der vorangegangenen vier Jahre übersteigt, unterstreicht die wachsende Notwendigkeit von Wachsamkeit und Vorschriften[2].

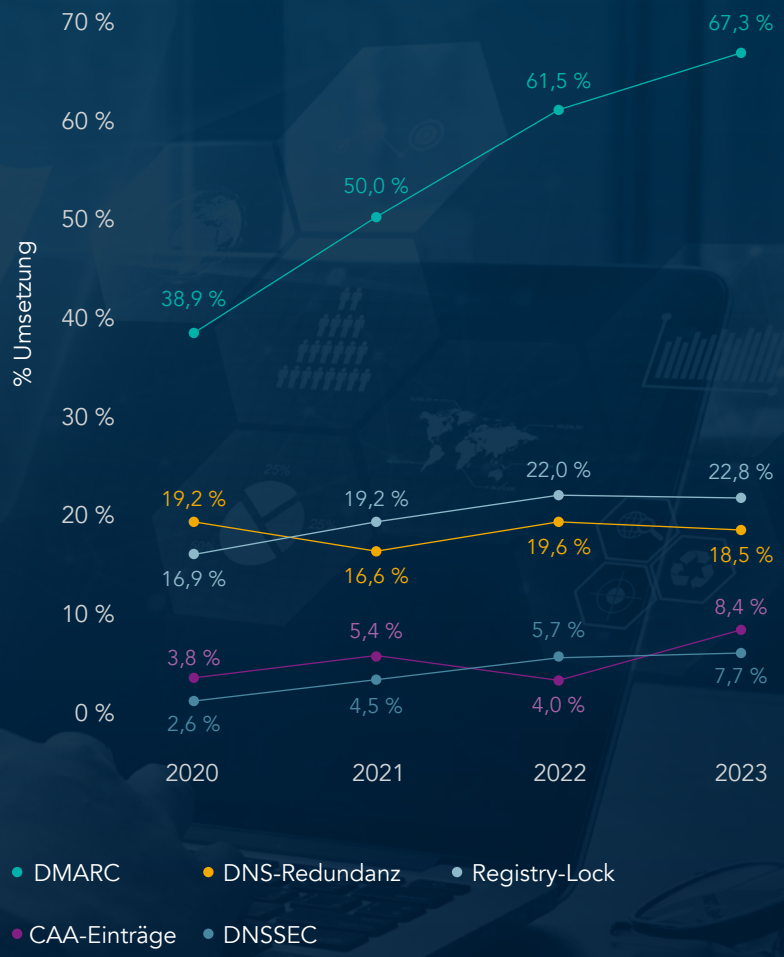
Insgesamt sind 43 % der Global 2000-Unternehmen von Registrierungen und Rechtsverletzungen durch Dritte betroffen. Von den Unternehmen mit Markendomains, die für .AI registriert sind, befinden sich 84 % im Besitz von Dritten. 49 % sind frei verfügbar. Bestimmte Branchen wie das Bankwesen, diversifizierte Finanzunternehmen sowie IT-Software und -Services verzeichnen den höchsten Prozentsatz an vergebenen .AI-Domains.

Die Regierungen verschärfen die Vorschriften für KI-Tools, und die Unternehmen entwickeln weiterhin KI-Systeme und -Prozesse und führen sie ein. Dieser Trend deutet darauf hin, dass die Nachfrage nach .AI-Domains wahrscheinlich weiter steigen wird. Darüber hinaus bedeutet die jüngste Entscheidung von Google®, .AI-Domains als generische Top-Level-Domains und nicht als Ländercode zu behandeln, eine Anerkennung der globalen Relevanz von KI[3].

Die Zunahme der .AI-Domain-Registrierungen ist bezeichnend für die gesamte Technologielandschaft. Mit der zunehmenden Durchdringung der verschiedenen Aspekte des täglichen Lebens durch KI müssen die damit verbundenen Aufgaben und Herausforderungen mit Sorgfalt und Weitsicht angegangen werden.

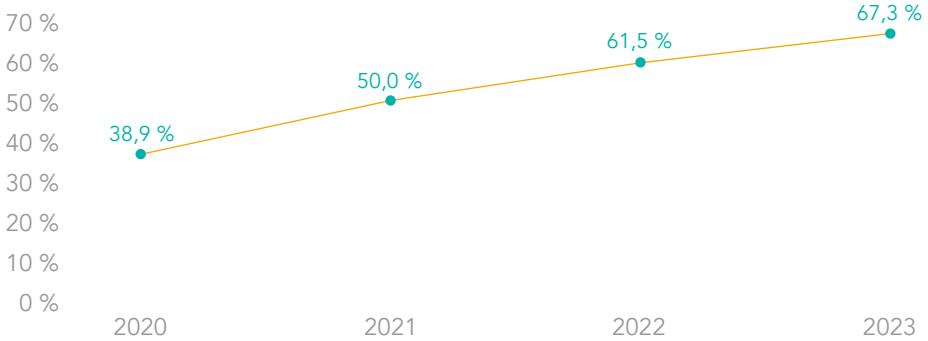
In diesem Jahr sind Domain-Streitigkeiten im Zusammenhang mit .AI-Erweiterungen um 350 % gestiegen.

TRENDS BEI DER UMSETZUNG VON MASSNAHMEN ZUR DOMAIN-SICHERHEIT (2020–2023)



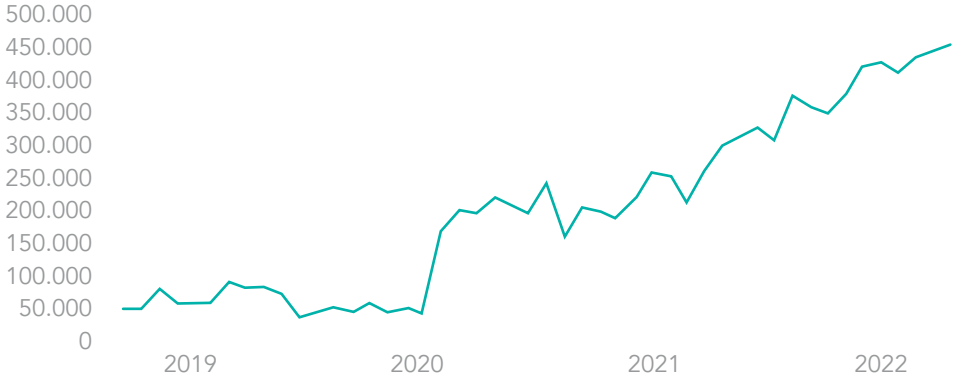
DMARC MIT DEM SCHNELLSTEN WACHSTUM

In Anbetracht der vielen gemeldeten Phishing-Angriffe – einschließlich ihres zunehmenden Umfangs und ihrer Komplexität – ist es keine Überraschung, dass die Nutzung von DMARC recht schnell von 39 % im Jahr 2020 auf 67 % im Jahr 2023 gestiegen ist.



Die jüngsten Zahlen der APWG zeigen, dass 2022 ein Rekordjahr bei Phishing war, in dem über 4,7 Millionen Angriffe protokolliert wurden, und BEC-Angriffe im 4. Quartal 2022 durchschnittlich 132.559 US-Dollar Schaden verursachten. Seit Anfang 2019 ist die Zahl der Phishing-Angriffe um mehr als 150 % pro Jahr gestiegen, wobei in den letzten Jahren pro Quartal mehr als eine Million Phishing-Angriffe stattfanden, die jeden Monat auf etwa 600 verschiedene Marken abzielten.

GESAMTZAHL EINDEUTIGER PHISHING-ANGRIFFE PRO MONAT (APWG)



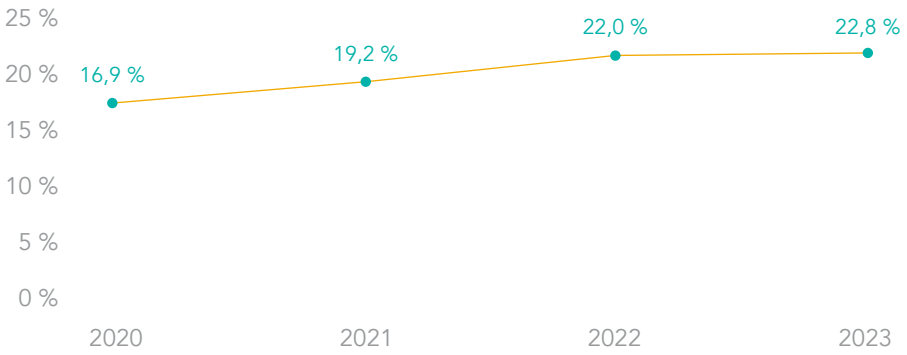
Ein weiterer Faktor für die steigende Verbreitung von DMARC ist die zunehmende Einführung von Markenindikatoren zur Identifizierung von Nachrichten (BIMI) in E-Mail-Clients, die die Anzeige von Markenlogos in authentifizierten E-Mails ermöglichen. DMARC ist eine Sicherheitsvoraussetzung für die Einrichtung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

LEICHTE ZUNAHME VON REGISTRY-LOCK, ABER WEITERHIN HOHES RISIKO FÜR DIE GLOBAL-2000-UNTERNEHMEN

Der Prozentsatz der Unternehmen, die Registry-Lock aktiviert haben, ist von 17 % im Jahr 2020 auf 23 % im Jahr 2023 gestiegen. Wir haben außerdem festgestellt, dass 46 % der Unternehmen, die mit Enterprise-Class-Registraren arbeiten, auch Registry-Lock nutzen. Angesichts der zunehmenden Forderungen von Regierungsbehörden, die Cybersicherheit zu erhöhen und die Risiken des DNS-Missbrauchs zu beseitigen, sowie als Reaktion auf Vorschriften und den Druck aus der Branche bieten immer mehr Registrierungsbehörden Sperren für ihre Domain-Endungen an. Ein Registry-Lock ermöglicht die durchgängige Sicherheit von Domain-Transaktionen, um menschliches Versagen und das Risiko durch Fremde zu minimieren. Es ist ein äußerst kostengünstiges Mittel, um Domains vor versehentlichen oder unbefugten Modifizierungen oder Löschungen zu schützen. Einige Domains bleiben jedoch möglicherweise entsperrt, da nicht jede Registrierungsbehörde weltweit Sperrdienste anbietet.

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

REGISTRY-LOCK

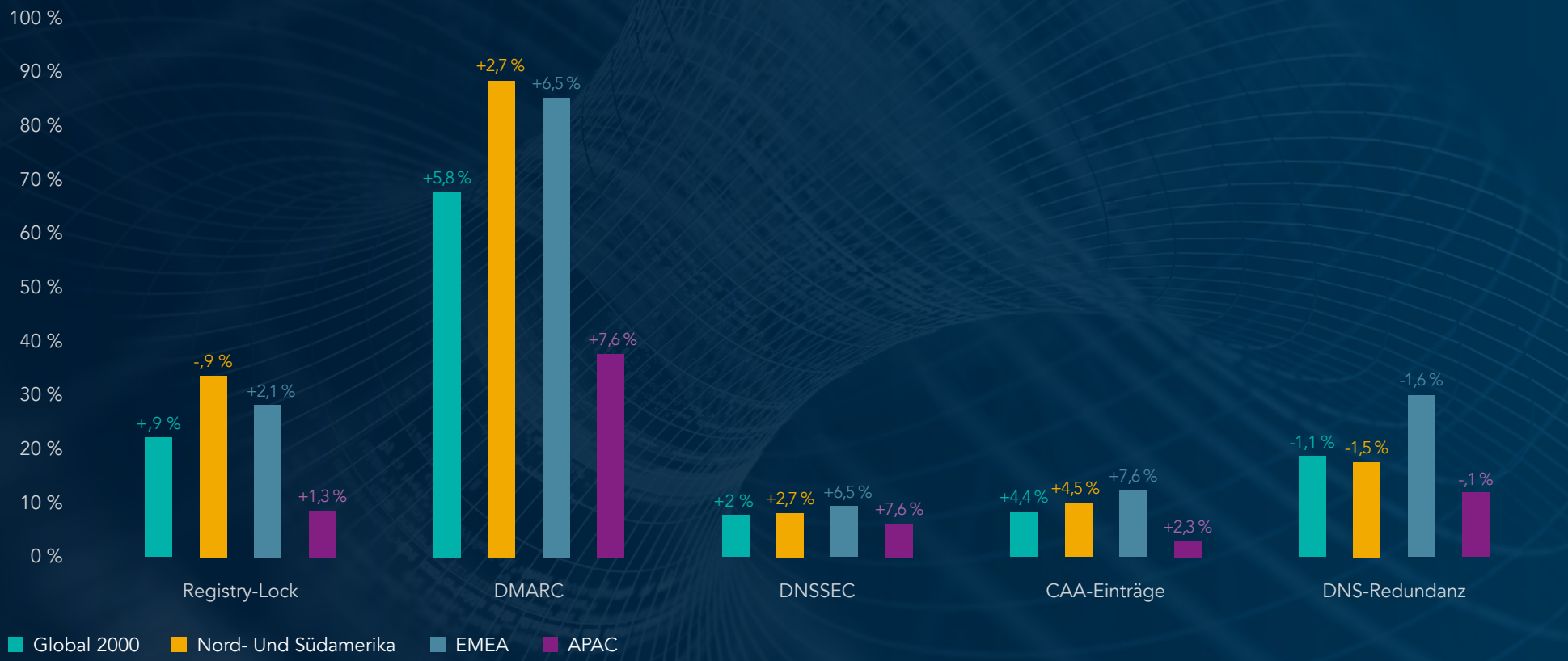


SICHERHEITSMASSNAHMEN WIE DNS-REDUNDANZ, DNSSEC UND CAA-DATENSÄTZE WAREN INKONSISTENT

Der Prozentsatz der Unternehmen, die DNSSEC (Domain Name System Security Extensions) einsetzen, hat sich in den letzten drei Jahren von 3 % im Jahr 2020 auf 8 % im Jahr 2023 mehr als verdoppelt. Überraschenderweise ist die DNS-Redundanz im Vergleich zum Vorjahr um 1 % auf 19 % gesunken, obwohl immer mehr Regierungsbehörden eine Ausfallsicherheit des DNS fordern. DNS-Redundanz ist eine kritische Komponente in der Kerninfrastruktur eines jeden Unternehmens. Wir stellen fest, dass die Implementierung dieser Sicherheitsmaßnahme abnimmt, was darauf zurückzuführen sein könnte, dass die Unternehmen steigende Kosten und Ressourcen einplanen müssen.

Schließlich hat sich die Nutzung von CAA-Einträgen (Certification Authority Authorization) in diesem Jahr erheblich erhöht, und zwar von 3,8 % im Jahr 2020 auf 8,4 % im Jahr 2023. 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 benannte Zertifizierungsstelle verwenden, um ein neues Zertifikat zu erhalten: Ihre Anfrage schlägt fehl und das Unternehmen erhält eine Warnung. Viele Unternehmen nutzen diese Sicherheitskontrolle jedoch immer noch nicht in vollem Umfang, da es für sie oft schwierig ist, sich mit den Anforderungen zurechtzufinden, insbesondere wenn sie mehrere Anbieter für ihre Domains, DNS und SSL (Secure Sockets Layer) verwenden.

DOMAIN-SICHERHEITSMASSNAHMEN 2023 NACH REGION



+/- % Veränderung gegenüber dem Vorjahr

DOMAIN-SICHERHEITSMASSNAHMEN 2023 NACH REGISTRAR-TYP

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

Registrare für Verbraucher:

Ein Registrar für Verbraucher ist auf Domain-Services, Websites und E-Mail für die private Nutzung sowie Unternehmer und Kleinunternehmen, die gerade am Anfang stehen, spezialisiert.

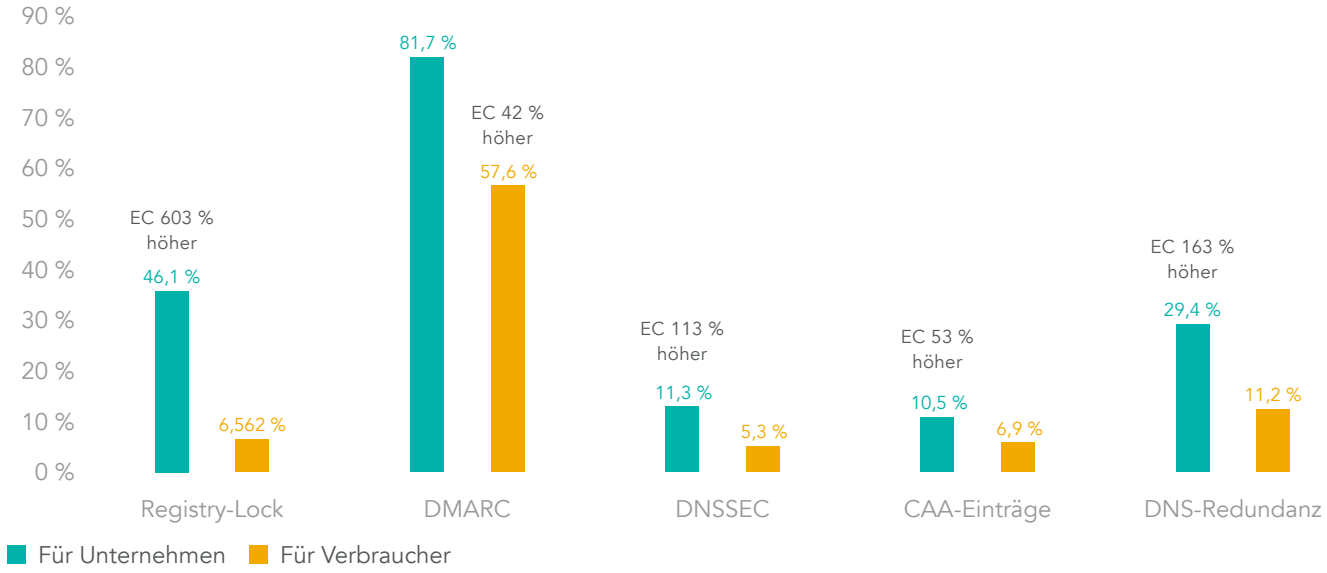
Enterprise-Class-Registrare:

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.

Viele Unternehmen befinden sich in dem Irrglauben, dass alle Registrare gleich sind. Falsches Vertrauen in Registrare für Verbraucher, die möglicherweise nicht auf Domain-Sicherheit ausgelegt sind, kann sich negativ auf den allgemeinen Sicherheitsstatus eines Unternehmens auswirken. Dies gilt insbesondere für die Einführung von Registry-Locks, da die meisten Registrare für Verbraucher diese nicht unterstützen.

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

Reifegrad der Sicherheitsmaßnahmen, Enterprise-Class-Registrare (EC) im Vergleich zu Registrare für Verbraucher (CG)



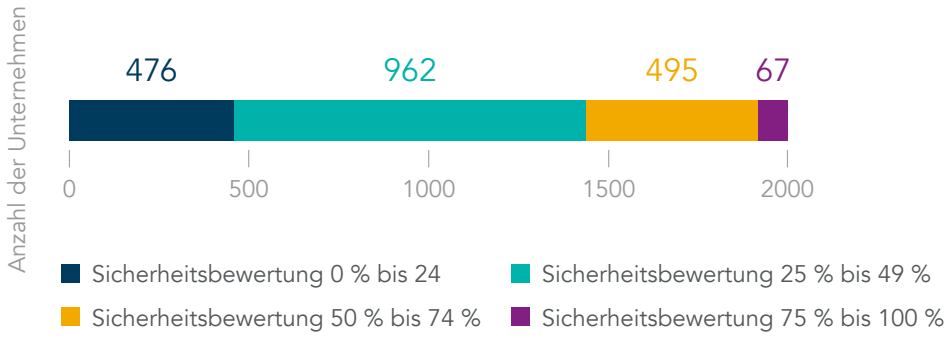
DOMAIN-SICHERHEITSSTATUS INSGESAMT

Anhand der Wichtigkeit von acht grundlegenden Sicherheitsmaßnahmen, die wir nach der Risikostufe der Domain-Sicherheit 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
- CAA-Einträge
- DNS-Redundanz
- DNSSEC
- Sender policy framework (SPF)
- DomainKeys identified mail (DKIM)
- DMARC

RISIKOSTUFEN DER DOMAIN-SICHERHEIT VON GLOBAL 2000-UNTERNEHMEN



72 % aller Unternehmen haben weniger als die Hälfte der Sicherheitsmaßnahmen umgesetzt

DIE FÜNF AM BESTEN ABSCHNEIDENDEN BRANCHEN

- IT-Software und -Dienstleistungen
- Medien
- Dienstleistungen und Lieferungen für Geschäftsleute
- Hotellerie, Gastronomie und Freizeit
- Ausstattung und Dienstleistungen im Gesundheitswesen

DIE UNTERNEHMEN MIT DEN BESTEN WERTEN

- Nur zwei Unternehmen erzielten mit 100 % umgesetzten Maßnahmen zur Domain-Sicherheit die höchste Sicherheitsbewertung.

DIE FÜNF AM SCHLECHTESTEN ABSCHNEIDENDEN BRANCHEN

- Versorgungsunternehmen
- Handel
- Lebensmittelmärkte
- Bauwesen
- Werkstoffe

DIE UNTERNEHMEN MIT DEN SCHLECHTESTEN WERTEN

- 112 Unternehmen haben eine Domain-Sicherheitsbewertung von null.
- Diese Unternehmen stammen hauptsächlich aus der Asien-Pazifik-Region (APAC), die 87 % der Unternehmen in dieser Gruppe stellt.

AUF GLOBAL 2000-UNTERNEHMEN ABZIELENDE VERDÄCHTIGE ODER BÖSARTIGE DOMAIN-AKTIVITÄTEN

Wir haben Domains identifiziert und analysiert, die Markennamen mit mehr als sechs Zeichen von Global 2000-Unternehmen enthalten, aber nicht im Besitz der Markeninhaber selbst sind. Ziel dieser gefälschten Domain-Registrierungen ist es, das Vertrauen in die anvisierten Marken auszunutzen, um Phishing-Angriffe, andere Formen des digitalen Markenmissbrauchs oder Verletzungen des geistigen Eigentums zu starten, die zu Umsatzeinbußen, Traffic-Umleitungen und einer Beeinträchtigung des Markenrufs führen.

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

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
Homophones (Soundex)	siesiglobal.com | cscclobol.com

Übliche Homoglyphen (sog. 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

i → l	m → rn	i → l	s → 5	o → 0
e → 3	l → 1	l → i	w → vv	

MEHR ALS 79 % DER HOMOGLYPHEN-DOMAINS SIND IM BESITZ VON DRITTEN

Bei den Domains im Besitz von Dritten wurde Folgendes festgestellt:

87 % verschleierten 2023 ihre WHOIS bzw. Eigentümerangaben im Vergleich zu 82 % im Jahr 2022. Dieser Anstieg könnte absichtlich oder aufgrund von Anforderungen durch Datenschutzrichtlinien wie der Datenschutzgrundverordnung (DSGVO) erfolgt sein. Versuche, die Identität und den Besitz zu verschleiern oder zu verbergen, insbesondere bei Domains von Dritten, deuten jedoch auf eine Registrierung mit böswilligen Absichten hin.

40 % haben 2023 MX Records. 2022 lag dieser Anteil bei 48 %. Domains mit MX-Records können zum Versenden von Phishing-E-Mails oder zum Abfangen von E-Mails verwendet werden.

WIE WERDEN DOMAINS DURCH DRITTE GENUTZT?

36 % verweisen auf Werbung, Pay-per-Click-Webinhalte oder werden für Domain-Parking genutzt.

49 % hatten inaktive Webseiten.

1 % verweist auf bösartige Inhalte, die den Ruf einer Marke und das Vertrauen der Kunden schädigen können.

14 % führen zu einer aktiven Webseite, die nicht mit dem Markeninhaber verbunden ist.

Mit der kürzlichen Einführung von Threads von Instagram im Juli 2023 bekommen Marken bereits die Auswirkungen von Domain-Registrierungen durch Dritte zu spüren, von denen einige zur Vortäuschung von Zugehörigkeit, Logomissbrauch, Markennachahmung und mehr verwendet werden.

Mehr erfahren: Neue CSC-Studie zeigt, dass die Einführung von Threads durch Instagram bereits ein wachsendes Ziel für Betrug und Markenmissbrauch ist

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

Branche	Anteil der Bedrohungen durch Domain-Fälschungen
Bankwesen	13,1 %
Bauwesen	5,4 %
Öl- und Gasförderung	4,5 %
Finanzdienstleistungen	4,2 %
Werkstoffe	4,2 %
IT-Software und -Dienstleistungen	4,1 %
Versorgungsunternehmen	3,6 %
Dienstleistungen und Lieferungen für Geschäftsleute	3,5 %
Versicherung	3,5 %
Investitionsgüter	3,4 %
Langlebige Verbrauchsgüter	3,3 %
Einzelhandel	3,2 %
Chemikalien	2,8 %
Arzneimittel und Biotechnologie	2,6 %
Transportwesen	2,4 %
Hardware und technische Ausrüstung	2,2 %
Nahrungsmittel, Getränke und Tabakwaren	2,1 %
Telekommunikationsdienste	1,9 %
Ausstattung und Dienstleistungen im Gesundheitswesen	1,9 %
Halbleiter	1,7 %
Hotellerie, Gastronomie und Freizeit	1,2 %
Luft- und Raumfahrt und Verteidigung	1,1 %
Haushalts- und Körperpflegeprodukte	1,0 %
Handel	0,9 %
Medien	0,9 %
Lebensmittelmärkte	0,8 %

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

- GoDaddy®
- Namecheap™
- Network Solutions

FAZIT

Wenn sich ein Unternehmen nicht um die Domain-Sicherheit kümmert, kann das katastrophale Folgen haben. 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.

Unsere Untersuchungen zeigen, dass 43 % der mit Global 2000-Unternehmen in Verbindung stehenden .AI-Domains durch Dritten registriert sind. Wie der Anstieg der Domain-Dispute im Zusammenhang mit .AI-Endungen im Jahr 2023 um 350 % im Vergleich zum Vorjahr zeigt, müssen Unternehmen, die ihre .AI-Domains nicht gesichert haben, nun feststellen, dass viele gewiefte Online-Betrüger diese Domains stattdessen erworben haben.

Zur Ergänzung strategischer Domain-Registrierungen müssen Unternehmen die Domain-Sicherheit anhand eines mehrschichtigen Sicherheitsmodells in einem Zero-Trust-Framework anwenden, um verlässliche Unternehmenssicherheit mit möglichst geringem Risiko für das Unternehmen zu schaffen. Eine Partnerschaft mit einem Enterprise-Class-Registrar ist nicht nur notwendig, um Einblick in exponierte Bereiche (einschließlich Domain-Namen und DNS) zu erhalten und Bedrohungsvektoren analysieren zu können, die auf die Online-Präsenz eines Unternehmens abzielen, sondern auch die Ressourcen für Gegen- und Durchsetzungsmaßnahmen zu gewinnen.

Sehen Sie sich die Liste der defensiven und proaktiven Sicherheitsmaßnahmen von CSC an, um Ihre Domains und Marken mit einem mehrschichtigen, tief greifenden Ansatz zur Domain-Sicherheit zu schützen.

Laden Sie unsere Checkliste für Domain-Sicherheit herunter.

ÜBER DIE DOMAINSEC-PLATTFORM VON CSC

Die 3D Domain Security and Enforcement-Lösung von CSC basiert auf der leistungsstarken DomainSec℠-Plattform. DomainSec ist eine SaaS-Plattform (Software as a Service) für Cybersicherheit. Sie wurde von CSC entwickelt und ist die erste vollumfängliche Lösung für den Schutz und die Verteidigung der Domain-Ökosysteme von Marken. Mithilfe der firmeneigenen geschützten MLDS-Technologie (Machine Learning Deep Search) und einer Kombination aus maschinellem Lernen, künstlicher Intelligenz und Clustering-Technologie erkennt sie Frühindikatoren für eine Gefährdung.

DomainSec vereint die Domain-Verwaltung und -Sicherheit von CSC mit Lösungen zum Marken- und Betrugsschutz in einer Plattform. Dadurch können wir einen wesentlich besseren Schutz bieten und Unternehmen dabei helfen, ihr Zero-Trust-Sicherheitsmodell zu optimieren und viel mehr als nur bloße Schutzparameter anzuwenden.

CSC ist der bevorzugte Sicherheitsanbieter 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. Weltweit tätige Unternehmen investieren derzeit in erheblichem Maße in ihren Sicherheitsstatus. CSC kann ihnen dabei helfen, bekannte Sicherheitslücken in der Cybersicherheit zu verstehen und zu erkennen, wie diese mit ihrem Zero-Trust-Modell zusammenhängen. 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.

[1]CSC-Blog: „AI-zeit bereit? Eine Domain, die Sie in Ihr Portfolio aufnehmen sollten, bevor es jemand anderes tut" cscdbs.com/blog/ai-you-ready-a-domain-to-add-to-your-portfoliobefore-someone-else-does/

[2]DNDisputes.com: „KI: Fälle von Domain-Namensstreitigkeiten bei AI-Endungen" dndisputes.com/case/domain/extension/ai /

[3]Search Engine Land: „Google behandelt .AI-Domains jetzt als generische Top-Level-Domains" searchengineland.com/google-now-treats-ai-domains-as-generic-top-level-domains-427770

Copyright ©2023 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. Bitte wenden Sie sich an Ihren Rechts- oder Finanzberater, um herauszufinden, inwiefern diese Informationen auf Sie zutreffen.

CSC10112023