CSC

Bericht zur Domainsicherheit **2026**

Einführung

Zum sechsten Mal in Folge hat CSC den Status der Domainsicherheit untersucht und die Sicherheitslage der Forbes Global 2000-Unternehmen bewertet. Wir haben die Einführung von Maßnahmen zur Domainsicherheit analysiert, die zur Minderung von Cyberrisiken im Domain-Ökosystem der Global 2000-Unternehmen außerhalb der Firewall eines Unternehmens eingesetzt werden, sowie Vorfälle potenziellen Online-Markenmissbrauchs und Rechtsverletzungen durch Dritte.

In diesem Jahr haben wir die Domain-Sicherheitspraktiken von Global-2000-Unternehmen mit denen der Top-100-Unicorns der Welt verglichen. Obwohl es einige Ähnlichkeiten gibt, war eine unserer wichtigsten Fragen, ob diese neueren Unternehmen – viele davon aus den Bereichen Technologie und KI – eine strengere Domain-Sicherheitspolitik verfolgen. Dieser Bericht gibt Aufschluss über unsere Ergebnisse.

Angesichts der Zunahme von Cyberangriffen auf multinationale Unternehmen wie die Global 2000 setzt sich CSC weiterhin für ein stärkeres Bewusstsein für Domainsicherheit ein. Bedrohungen können von allen Bereichen der IT-Infrastruktur eines Unternehmens ausgehen, jedoch nutzen die meisten Angriffe einen Domainnamen, um in Systeme einzudringen. Eine solide Sicherheitsstrategie ist daher wichtiger denn je.

Zusammenfassung der wichtigsten Ergebnisse

Unicorns setzen wichtige Sicherheitsmaßnahmen für DNS-Einträge in hohem Maße um, vernachlässigen jedoch andere Bereiche, was mit zunehmendem Wachstum kritische Versäumnisse zur Folge haben könnte.

Bei Domain-Sicherheitsmaßnahmen, die auf DNS-Einträgen (Domain Name System) basieren, wie z. B. DMARC (Domain-based Message Authentication, Reporting and Conformance), SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DNSSEC (DNS Security Extensions) und CAA (Certificate Authority Authorization), haben wir eine höhere Akzeptanz bei Unicorns festgestellt, wobei bis zu 100 % SPF für ihre E-Mail-Authentifizierungsprotokolle verwenden. Allerdings nutzt nur 1 % DNS-Redundanz, und fast 90 % der Unicorns verwenden eine einzige Infrastruktur in der Cloud.

Fünf von acht Domain-Sicherheitsmaßnahmen wurden von Unicorns häufiger genutzt als von Global-2000-Unternehmen

Unicorns zeigten bei allen Maßnahmen im Zusammenhang mit DNS-Einträgen wie DMARC (96,0 % gegenüber 79,8 %), DNSSEC (16,8 % gegenüber 10,8 %) und CAA-Einträgen (33,0 % gegenüber 11,4 %) eine höhere Akzeptanz als Global-2000-Unternehmen. Dies deutet darauf hin, dass es sich bei den Teams, die die Domainnamen für Unicorns verwalten, wahrscheinlich um IT-Fachleute handelt, die über gute Kenntnisse der innerhalb des DNS verfügbaren Sicherheitsprotokolle verfügen, die für das Unternehmen keine hohen Kosten verursachen. Dies ist ein ermutigender Trend für Unternehmen, die (technologische) Innovationen vorantreiben, dem etablierte Unternehmen nacheifern könnten.

Die Diskrepanz bezüglich der Einführung von Registry Locks zwischen Global-2000-Unternehmen, die Registrare der Enterprise-Class nutzen, und solchen, die Registrare für Verbraucher nutzen, beträgt mehr als das Sechsfache

Registry Locks stellen eine der stärksten Abwehrmaßnahmen gegen Hijacking dar, da sie unbefugte Änderungen an Ihren Domains und DNS verhindern, selbst wenn Ihr Registrar-Konto kompromittiert wurde. Die meisten Registrare für Verbraucher können diesen Service aufgrund der dafür erforderlichen Ressourcen nicht anbieten. Dies zeigt sich auch in den Daten, wonach Unternehmen, die Registrare der Enterprise-Class nutzen, eine sechsmal höhere Akzeptanz und eine stärkere Sicherheitslage aufweisen. In unserem aktuellen Bericht „Die SSL-Landschaft“ haben wir außerdem festgestellt, dass 60 % der großen Unternehmen drei oder mehr SSL-Anbieter (Secure Sockets Layer) nutzen und damit ihr Risiko erhöhen. Anbieter der Enterprise-Class können Unternehmen eine bessere Kontrolle über ihre digitale Landschaft ermöglichen und sicherstellen, dass ihre Lieferkette ein vergleichbares hohes Sicherheitsniveau aufweist – denn wir haben gesehen, wie viel Schaden dies Unternehmen im vergangenen Jahr verursacht hat.[1]

Die APAC-Region verzeichnete zwischen 2024 und 2025 das größte Wachstum, liegt jedoch hinsichtlich der Gesamtakzeptanz weiterhin hinter EMEA und Amerika zurück

Wir beobachten eine deutliche Verbesserung der Akzeptanzraten bei Unternehmen in der APAC-Region im Vergleich zum Vorjahr. Hinsichtlich der tatsächlichen Akzeptanz liegt APAC jedoch weiterhin hinter anderen Regionen mit einem Abstand von mindestens 15 Prozentpunkten zurück.

Die Halbleiter- und Bankenbranche verzeichnen den deutlichsten Anstieg der Gesamtpunktzahl im letzten Jahr

Beide Branchen konnten ihre Platzierung im letzten Jahr um jeweils fünf Plätze verbessern. Das rasante Wachstum dieser beiden Branchen – bedingt durch den Vormarsch künstlicher Intelligenz (KI) und FinTech – in Verbindung mit strengeren Anforderungen an die Cybersicherheit könnten eine Erklärung für das verbesserte Sicherheitsniveau sein.

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 bösartige Domainregistrierungen werden zur Ausführung aller in Abbildung 1 gezeigten Angriffe verwendet.

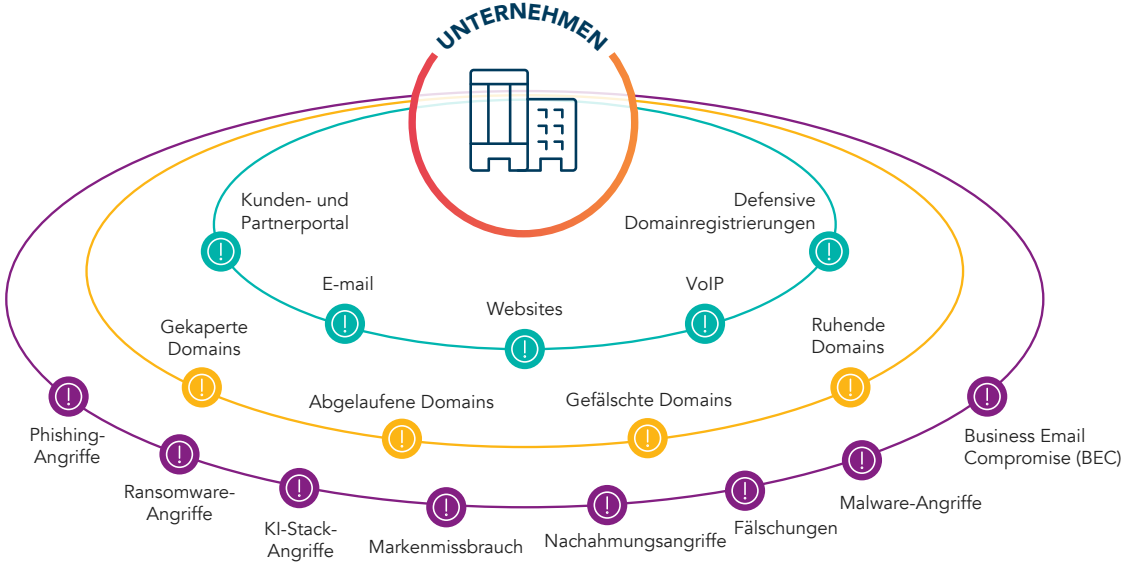


Abbildung 1: Die Galaxie des Domainnamen-Ökosystems

Was ist Domainsicherheit

Globale Unternehmen verlassen sich in allen Bereichen auf das Internet – für Websites, E-Mails, Authentifizierung, Voice-over-IP (VoIP), Kundenportale, Lieferantenanwendungen und die gesamte Lieferkette. Das Internet ist 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. 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-Kampagnen 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. Ruhende Domains entgehen oft der ersten Erkennung, da sie nicht sofort Anzeichen dafür aufweisen, dass sie für einen Angriff registriert wurden – z. B. einen aktiven MX-Eintrag (E-Mail), der normalerweise Alarm auslösen würde.

→ Bösartige Domainregistrierungen

Es gibt unzählige Domain-Spoofing-Permutationen und Homoglyphen, die von Phishern und böswilligen Dritten eingesetzt werden. Der Zweck dieser gefälschten Domainregistrierungen besteht darin, 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 Dritten 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 Global-2000-Unternehmen

In dieser Analyse untersuchte CSC die Umsetzung von fünf wichtigen Domain-Sicherheitsmaßnahmen innerhalb der Global-2000-Liste: DMARC, DNS-Redundanz, Registry Locks, CAA-Einträge und DNSSEC. 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 (2020–2025)

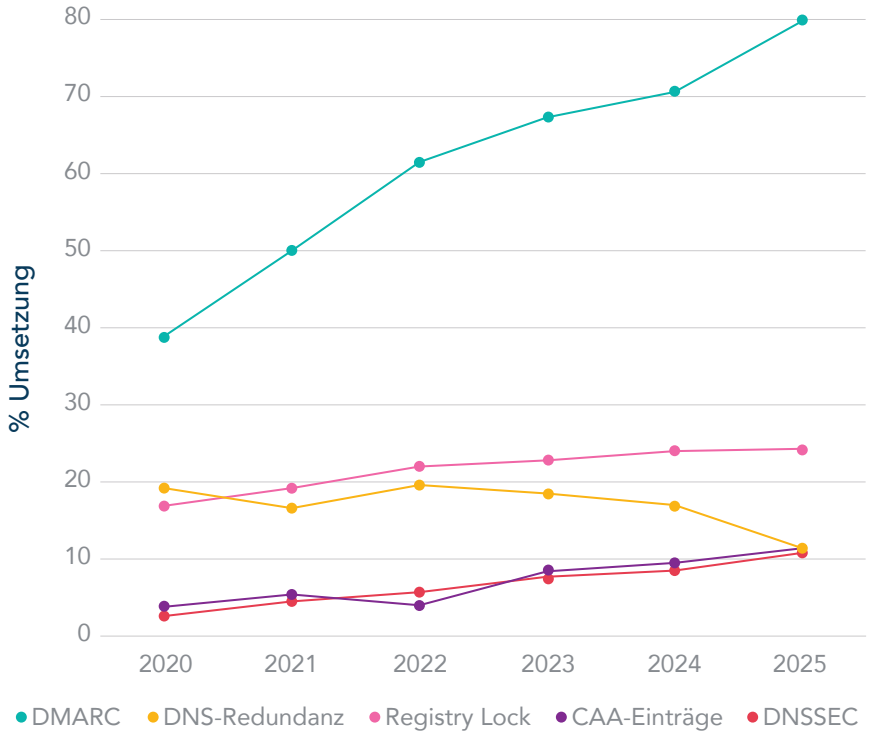


Abbildung 2: Umsetzung der fünf wichtigsten Domain-Sicherheitsmaßnahmen bei den Global 2000, 2020–2025

DMARC weist das schnellste Wachstum auf

Angesichts der großen Zahl gemeldeter Phishing-Angriffe – einschließlich ihres zunehmenden Umfangs und Komplexität – überrascht es nicht, dass die DMARC-Umsetzung schnell von 39 % im Jahr 2020 auf 80 % im Jahr 2025 gestiegen ist (Abbildung 3). Wir haben auch einen Anstieg der DMARC-Akzeptanz aufgrund des Inkrafttretens von NIS2 im Oktober 2024 beobachtet, wodurch die Cybersicherheit für Unternehmen, die in der Europäischen Union tätig sind, stärker in den Vordergrund rückt. Von den verbleibenden 20 %, die bei der Umsetzung noch hinterherhinken, stammen 85 % aus dem asiatisch-pazifischen Raum und aus allen Branchen, was mit unseren Beobachtungen zur regionalen Einführung übereinstimmt.

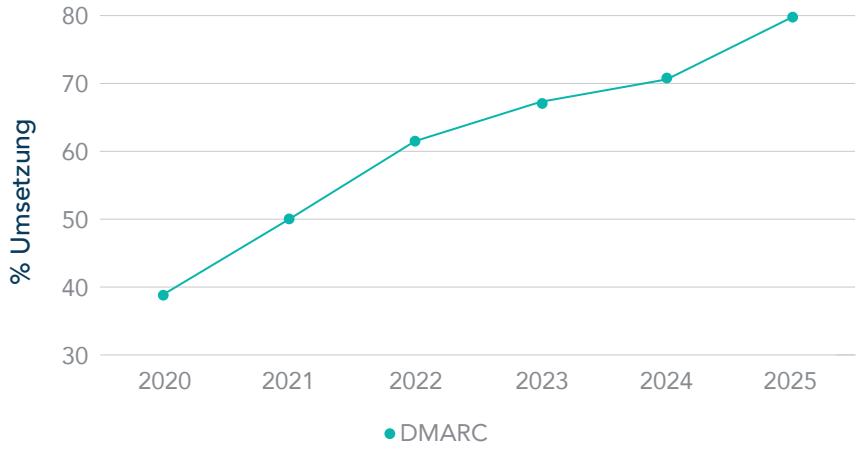


Abbildung 3: DMARC-Akzeptanzraten 2020-2025

Was ist NIS2?

Die Richtlinie 2 zur Sicherung von Netz- und Informationssystemen (NIS2) ist das neue Cybersicherheitsgesetz der Europäischen Union – Richtlinie (EU) 2022/2555 –, das am 14. Dezember 2022 verabschiedet wurde. Sie stellt strengere Anforderungen als frühere Richtlinien, um ein höheres gemeinsames Niveau der Cybersicherheit in allen EU-Mitgliedstaaten zu gewährleisten. Darin werden Verpflichtungen insbesondere für kritische Einrichtungen gemäß der Richtlinie über die Resilienz kritischer Einrichtungen (CER) – Richtlinie (EU) 2022/2557 – dargelegt, darunter Organisationen in den Bereichen Energie, Verkehr, Gesundheitswesen, Bankwesen, Finanzmarketinginfrastruktur, digitale Infrastruktur und öffentliche Verwaltung. Diese Organisationen müssen konkrete Maßnahmen ergreifen, um Cyberrisiken zu bewältigen, Systeme zu schützen, unverzüglich auf Vorfälle zu reagieren und nationale Cybersicherheitsstrategien einzuhalten. Die Meldung von Vorfällen ist obligatorisch, während der Austausch von Bedrohungsinformationen gefördert wird. Die Regulierungsbehörden sind außerdem befugt, Organisationen zu prüfen, die Einhaltung der Vorschriften durchzusetzen und bei Verstößen Geldbußen zu verhängen.

Dieser Fokus auf Cybersicherheit auf nationaler Ebene wird durch ähnliche Maßnahmen von Regierungen auf der ganzen Welt ergänzt, die ebenfalls ähnliche Richtlinien für kritische Branchen in ihren jeweiligen Ländern verabschiedet haben. In Australien beispielsweise umfasst die australische Cybersicherheitsstrategie 2023-2030 ein neues Cybersicherheitsgesetz 2024 und Änderungen des Gesetzes über die Sicherheit kritischer Infrastrukturen (SOCI Act), das Mindeststandards für die Sicherheit vorschreibt, eine Meldepflicht einführt und Regeln und Verpflichtungen im Bereich Risikomanagement und Datensicherheit klarstellt. Unternehmen, die international tätig sind, sind gefragt, ihre Sicherheitspraktiken an diese steigenden globalen Standards anzupassen.

Rückgang der DNS-Redundanz

Die DNS-Redundanz ist im Vergleich zum Vorjahr leicht zurückgegangen. Dies ist zum Teil auf eine Änderung der Methodik von CSC im letzten Jahr zurückzuführen, aber auch in den zugrunde liegenden Daten ist ein leichter Rückgang zu verzeichnen. Dies hat zu einer prozentualen Veränderung von insgesamt 6 % gegenüber dem Vorjahr geführt, wobei Unternehmen der DNS-Redundanz Priorität einräumen. 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. Viele Unternehmen setzen außerdem auf eine einzige Infrastruktur in der Cloud, um Kosten zu sparen, die Skalierbarkeit zu verbessern, den Datenzugriff zu erleichtern und weitere Vorteile zu erzielen. Einerseits bietet die Cloud ein global verteiltes System, aber es bestehen immer noch die gleichen potenziellen Risiken, wenn Teilbereiche des Systems offline gehen. Die einzige Möglichkeit, Risiken im Zusammenhang mit dem DNS wirklich zu mindern, besteht darin, zwei robuste, unabhängige Netzwerke für Redundanz (doppelte Infrastruktur) einzurichten.

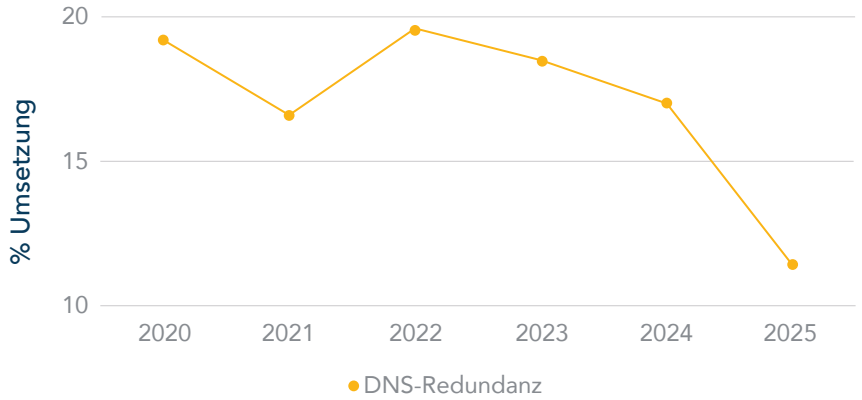


Abbildung 4: DNS-Redundanz-Akzeptanzraten 2020–2025

Sehen Sie sich unser Webinar an und erfahren Sie, warum sich das DNS zum größten Single Point of Failure im heutigen digitalen Ökosystem entwickelt hat.

Sicherheitsmaßnahmen wie Registry Lock, DNSSEC und CAA-Einträge haben stetig, wenngleich langsam zugenommen

Die Akzeptanz von Registry Lock stieg bis 2025 geringfügig auf 24 %. Wir haben außerdem beobachtet, dass Unternehmen, die Registrare der Enterprise-Class nutzen, mit 53 % im Jahr 2025 auch häufiger Registry Lock einsetzen. Angesichts des wachsenden Drucks, die Cybersicherheit zu erhöhen, bieten immer mehr Registrierungsstellen Sperren für ihre Domainerweiterungen an, um die Transaktionssicherheit von End-to-End-Domainnamen zu gewährleisten und so menschliche Fehler sowie Risiken durch Dritte zu verringern.

Da sich das Domainportfolio eines Unternehmens ständig ändert, verwendet CSC einen prädiktiven Modellierungsalgorithmus, der mehr als 20 Attribute eines Domainnamens bewertet, um festzustellen, ob dieser Name geschäftskritische Aufgaben für den Betrieb Ihres Unternehmens und Ihre Marke online erfüllt, und empfiehlt wichtige Domains, die gesperrt werden sollten. Im Zuge des Aufstiegs der KI setzen wir uns weiterhin für eine starke Domainsicherheit als Vertrauenssignal ein. Dies ist besonders relevant, da die KI-Stacks von Unternehmen, die Anwendungsprogrammierschnittstellen (APIs) und Plugins verwenden, für ihre Funktion auf Domains und DNS angewiesen sind.

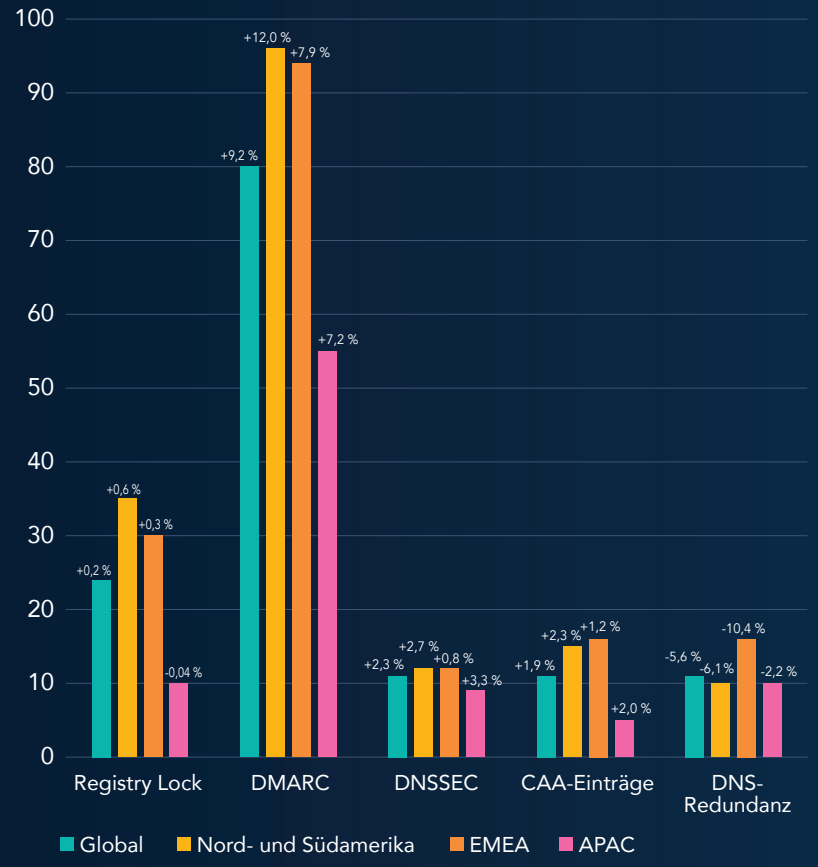
Der Anteil der Unternehmen, die DNSSEC einsetzen, ist zwar immer noch gering, hat sich aber in den letzten sechs Jahren auf 11 % im Jahr 2025 vervierfacht. DNSSEC gewährleistet die Authentifizierung und Datenintegrität von DNS-Anfragen und -Antworten, was wiederum Cyberkriminelle daran hindert, den Internetverkehr auf bösartige Websites, wie z. B. Phishing-Websites, umzuleiten. In einigen Ländern liegt die Akzeptanz von DNSSEC bei mehr als 67 %. In großen Unternehmen ist sie jedoch nach wie vor geringer. Dies ist zum Teil darauf zurückzuführen, dass Aktualisierungsprozesse in einer komplexeren Organisationsstruktur aufwändiger sind, aber dennoch handelt es sich um eine Sicherheitsmaßnahme, die alle kritischen Domains umsetzen sollten.

Schließlich stieg die Verwendung von CAA-Datensätzen im Jahr 2025 wieder auf 11 %. CAA-Einträge ermöglichen es Unternehmen, bestimmte Zertifizierungsstellen (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. Ein weiterer Vorteil von CAA-Einträgen besteht darin, dass Unternehmen die Einhaltung von Vorschriften durchsetzen können, sodass Mitarbeiter und Mitarbeiterinnen nur autorisierte Anbieter nutzen. In unserem aktuellen Bericht „Die SSL-Landschaft“ haben wir festgestellt, dass über 60 % der großen Unternehmen mehr als drei Anbieter nutzen, eines von ihnen nutzt sogar 13 Anbieter. Aus dem Bericht geht auch hervor, dass die von betrügerischen Websites am meisten genutzten Anbieter auch diejenigen sind, die insgesamt am häufigsten genutzt werden. Eine genauere Überprüfung des SSL-Managements ist erforderlich, zumal KI-Stacks ebenfalls immer autonomer werden.

Domain-Sicherheitsmaßnahmen

Nach Region

Die APAC-Region verzeichnete zwischen 2024 und 2025 das größte Wachstum bei der Umsetzung von Domain-Sicherheitsmaßnahmen, liegt jedoch hinsichtlich der Gesamtakzeptanz weiterhin hinter EMEA und Amerika zurück.



+/- % Veränderung gegenüber dem Vorjahr

Abbildung 5: Einführung von Domainsicherheit nach Region

Nach Branche

IT-Software und -Dienstleistungen sind auch 2025 die Branche mit der besten Performance.

Branchenklassifizierung	Ranking 2025	Ranking 2024
Halbleiter	6	11
Bankwesen	11	16
Hardware und technische Ausrüstung	13	5
Luft- und Raumfahrt und Verteidigung	16	8

Die am besten abschneidenden Branchen sind nach wie vor diejenigen, die für ihren Geschäftsbetrieb stark auf das Internet angewiesen sind, wie z. B. IT-Software und -Dienstleistungen sowie Medien. Auch das Bankwesen und die Halbleiterindustrie konnten ihr Ranking im letzten Jahr weiter verbessern. Das rasante Wachstum dieser beiden Branchen – bedingt durch den Vormarsch künstlicher Intelligenz (KI) und FinTech – in Verbindung mit strengeren Anforderungen an die Cybersicherheit könnten eine Erklärung für das verbesserte Sicherheitsniveau sein. Zu den am schlechtesten abschneidenden Branchen zählen weiterhin das Baugewerbe, der Bergbau und die Versorgungswirtschaft. Bemerkenswert ist, dass viele der Branchen mit niedrigem Ranking auch als kritische Branchen eingestuft werden, insbesondere in der NIS2-Richtlinie. Dies könnte bedeuten, dass diese Branchen im kommenden Jahr ihre Domainsicherheit ernster nehmen werden, insbesondere angesichts der zunehmenden Angriffe auf diese Branchen.

↑ DIE FÜNF AM BESTEN ABSCHNEIDENDEN BRANCHEN

- IT-Software und -Dienstleistungen
- Medien
- Einzelhandel
- Unternehmensdienstleistungen und Geschäftsbedarf
- Telekommunikationsdienste

↓ DIE FÜNF AM SCHLECHTESTEN ABSCHNEIDENDEN BRANCHEN

- Bauwesen
- Werkstoffe
- Lebensmittelmärkte
- Versorgungsunternehmen
- Nahrungsmittel, Getränke und Tabakwaren

Domain-Sicherheitsmaßnahmen 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 Domainregistrars 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. Um mehr darüber zu erfahren, wie die Verwendung eines Enterprise-Class-Registrars dazu beitragen kann, Domain-Hijacking, Dangling DNS und Domain-Identitätswechsel zu verhindern, laden Sie unsere „Checkliste zur Domainsicherheit“ herunter.

Registrare für Verbraucher

Ein Registrar für Verbraucher ist auf Domain-Dienste, Websites und E-Mail für Privatpersonen, Unternehmer und Kleinunternehmen, die gerade am Anfang stehen, ausgerichtet. Viele bieten keine Domain-Sicherheitsdienste an, wodurch die Akzeptanzrate ebenfalls geringer ist.

Unternehmen, die auf Enterprise-Class-Fähigkeiten setzen, haben eine höhere Einführungsrate von Domain-Sicherheitsmaßnahmen

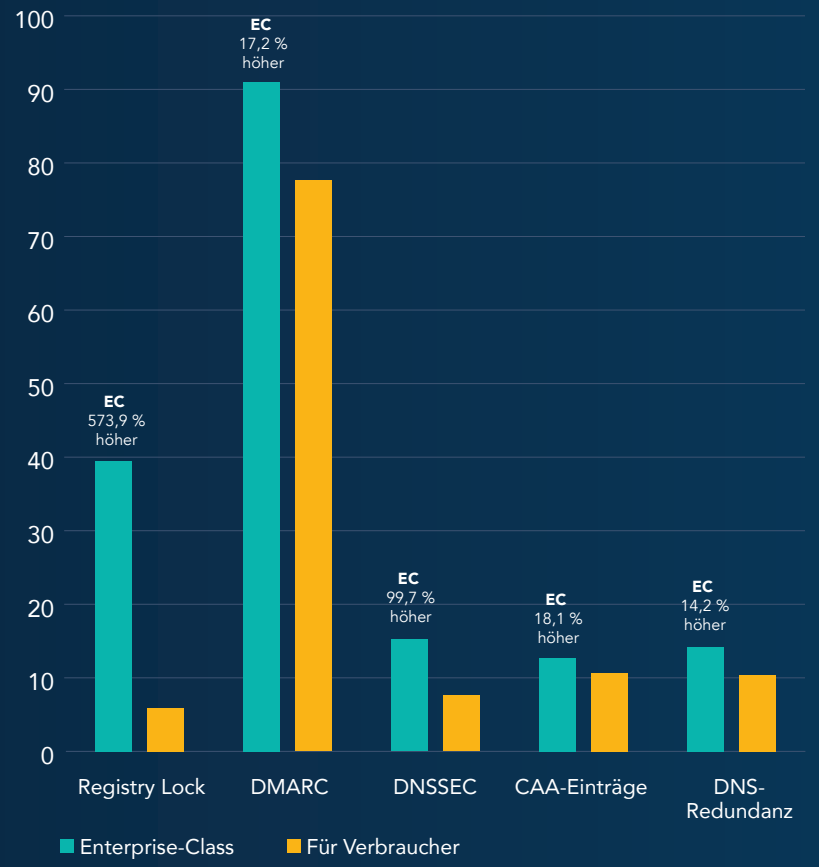


Abbildung 6: Reifegrad der Sicherheitsmaßnahmen – Enterprise-Class-Registrare (EC) im Vergleich zu Registraren für Verbraucher (CG)

Domain-Sicherheitsstatus

Ausgehend von der Wichtigkeit von acht grundlegenden Sicherheitsmaßnahmen, die wir nach der Domainsicherheitsrisikostufe 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:

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

Domainsicherheitsrisikostufen

Anzahl der Unternehmen

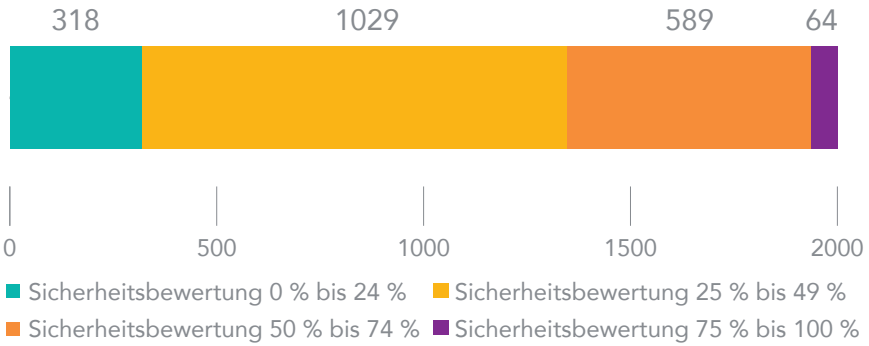


Abbildung 7: Domainsicherheitsbewertungen und zugehörige Domainsicherheitsrisikostufen von Global-2000-Unternehmen

67 % aller Global-2000-Unternehmen haben weniger als die Hälfte der empfohlenen Sicherheitsmaßnahmen umgesetzt.

↑ DIE UNTERNEHMEN MIT DEN BESTEN WERTEN

Wie bereits im Vorjahresbericht gibt es nur ein Unternehmen, das eine Punktzahl von 100 % erreicht hat. Nur acht Unternehmen erreichen eine Punktzahl von sieben von acht, ein Drittel weniger als im Vorjahr.

↓ DIE UNTERNEHMEN MIT DEN SCHLECHTESTEN WERTEN

87 Unternehmen haben eine Domain-Sicherheitsbewertung von Null – eine Verbesserung gegenüber den 107 Unternehmen des Vorjahres. Diese Unternehmen stammen hauptsächlich aus der Asien-Pazifik-Region (APAC), die 87 % der Unternehmen in dieser Gruppe stellt.

Verdächtige oder bösartige Domain-Aktivitäten, die auf die Global 2000 abzielen

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.

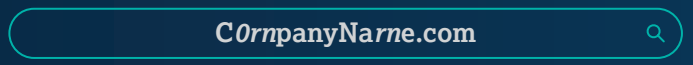
WIR KONZENTRIEREN UNS ABSICHTLICH AUF GÄNGIGE HOMOGLYPHEN, DA SIE ZU DEN GEFÄHRLICHSTEN ANGRIFFSMETHODEN VON BEDROHUNGSAKTEUREN ZÄHLEN

Domain-Spoofing-Taktiken

Abbildung 8: übliche Domain-Spoofing-Taktiken

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.



Zu den gängigsten Zeichenersetzungen gehören folgende:

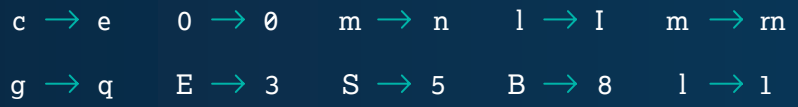


Abbildung 9: übliche Homoglyphen (Fuzzy-Matches) in .COM-Domains

88 % DER HOMOGLYPHEN-DOMAINS SIND IM BESITZ VON DRITTEN

Bei den Domains im Besitz von Dritten wurde Folgendes festgestellt:

40% verfügen im Jahr 2025 über MX-Einträge, verglichen mit 42 % im Jahr 2024. Domains mit MX-Records können zum Versenden von Phishing-E-Mails oder zum Abfangen von E-Mails verwendet werden. Dies ist ein wichtiger Grund für die zunehmende Anzahl von DMARC-Einträgen.

WIE WERDEN DRITTANBIETER-DOMAINS EINGESETZT?

40% verweisen auf Werbung, Pay-per-Click-Anzeigen oder werden für Domain-Parking genutzt.

39% haben inaktive Websites.

32% aller inaktiven Domains verfügen über aktive E-Mail-Einträge, was bedeutet, dass selbst Domains, die nicht zu Live-Inhalten führen, weiterhin für E-Mail-Aktivitäten genutzt werden können.

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

19% führen zu einer aktiven Website, die nicht mit dem Markeninhaber verbunden ist.

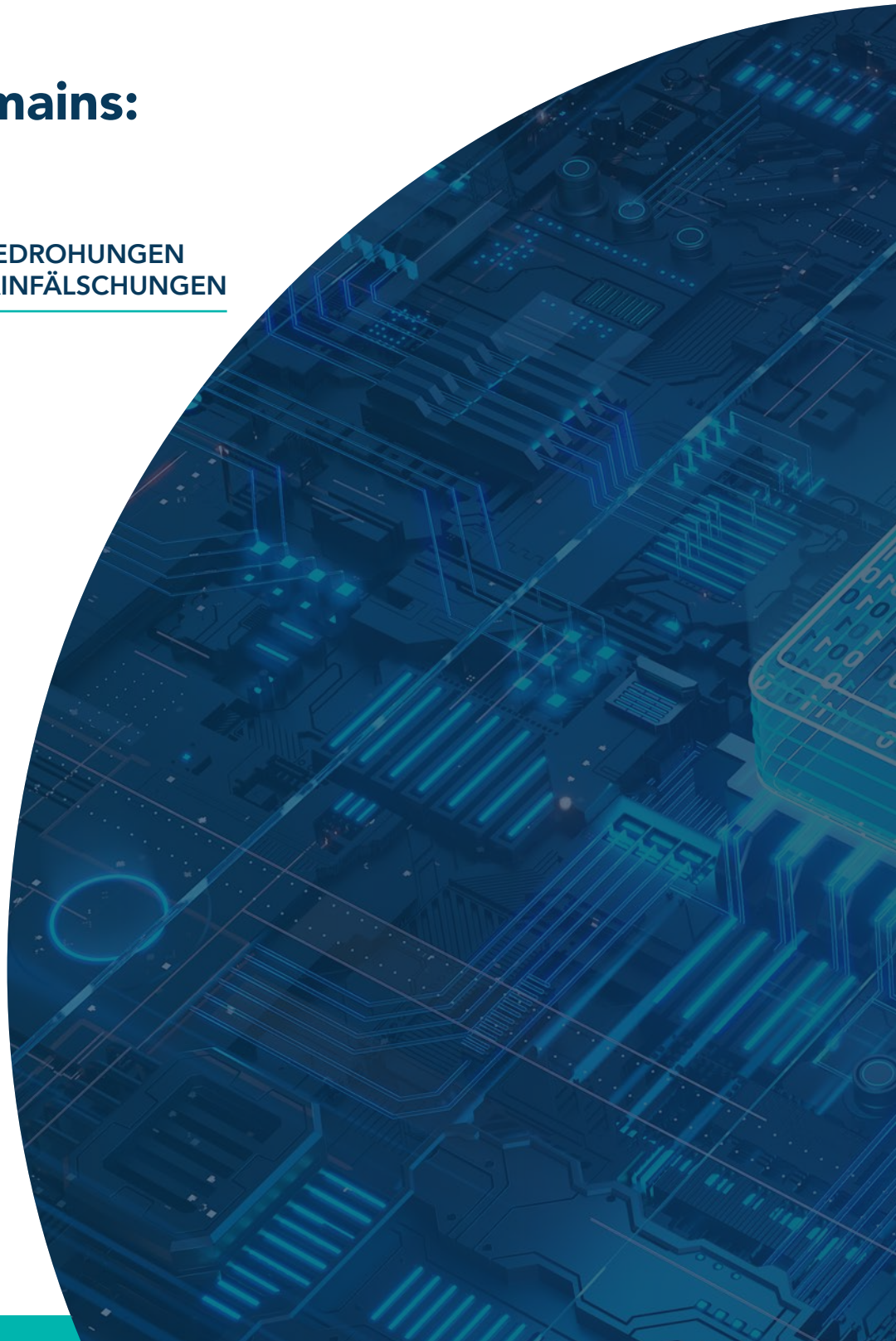
Unternehmen sollten sich auch der Verwendung ruhender Domains bewusst sein, bei denen Dritte Massenregistrierungen vornehmen und die Namen manchmal über einen langen Zeitraum ruhen lassen. Wie aus den Ergebnissen hervorgeht, sind 32 % der Drittanbieter-Domains inaktiv, enthalten jedoch MX-Einträge, die leicht aktiviert werden können.

DOMAINREGISTRARE, BEI DENEN ES DIE MEISTEN GEFÄLSCHTEN DOMAINREGISTRIERUNGEN IM BESITZ VON DRITTEN GIBT

- GoDaddy®
- Namecheap™
- Network Solutions

Verdächtige und bösartige Domains: Auf wen wird abgezielt?

BRANCHE	ANTEIL DER BEDROHUNGEN DURCH DOMAINFÄLSCHUNGEN
Bankwesen	16,3 %
IT-Software und -Dienstleistungen	6,6 %
Finanzdienstleistungen	5,8 %
Versorgungsunternehmen	5,4 %
Versicherung	5,4 %
Bauwesen	5,2 %
Öl- und Gasförderung	5,1 %
Unternehmensdienstleistungen und Geschäftsbedarf	4,3 %
Investitionsgüter	4,3 %
Transportwesen	4,3 %
Langlebige Verbrauchsgüter	4,0 %
Einzelhandel	3,6 %
Hardware und technische Ausrüstung	3,6 %
Werkstoffe	3,5 %
Nahrungsmittel, Getränke und Tabakwaren	2,8 %
Telekommunikationsdienste	2,7 %
Arzneimittel und Biotechnologie	2,4 %
Ausstattung und Dienstleistungen im Gesundheitswesen	2,4 %
Halbleiter	2,3 %
Luft- und Raumfahrt und Verteidigung	1,9 %
Handel	1,7 %
Chemikalien	1,7 %
Lebensmittelmärkte	1,5 %
Hotellerie, Gastronomie und Freizeit	1,3 %
Haushalts- und Körperpflegeprodukte	1,0 %
Medien	0,9 %



Einblicke in die Domainsicherheit: Sind Unicorn-Unternehmen die vorbildlichen Verfechter der Domainsicherheit?

Dieses Jahr hat sich CSC vorgenommen, die Global-2000-Unternehmen – von denen viele in traditionsreichen Branchen tätig sind – mit den 100 führenden Unicorn-Unternehmen zu vergleichen. Die Mehrheit der 100 führenden Unicorn-Unternehmen sind IT-Unternehmen, von denen viele in der KI-Branche tätig sind. Der Einfachheit halber haben wir bei diesen Unternehmen dieselben Domain-Sicherheitsmerkmale untersucht wie bei den Global-2000-Unternehmen. Unser Hauptziel bei der Analyse war es, festzustellen, ob kleinere Start-up-Unternehmen besser auf Domain-Sicherheitsrisiken eingestellt sind und Sicherheitsmaßnahmen besser umsetzen können als größere etablierte Unternehmen. Viele der Unicorn-Unternehmen aus der KI-Branche sind sich der Notwendigkeit von Sicherheitsprotokollen rund um die kritische Infrastruktur von Domains und DNS bewusst und weisen in einigen Bereichen eine hohe Akzeptanz auf, in anderen hingegen Defizite. Darüber hinaus trägt der KI-Stack, den viele dieser Unternehmen aufbauen, zu den breiteren Risiken in der Lieferkette der Unternehmen bei, die sie einsetzen.

Was sind Unicorns?

Ein Unicorn ist ein Unternehmen in Privatbesitz mit einer Bewertung von über 1 Milliarde US-Dollar. Es handelt sich in der Regel um Start-ups oder relativ junge Unternehmen, die in ihrer Branche oft wegweisend sind.

Highlights

Abbildung 10: Umsetzung von Maßnahmen zur Domainsicherheit – 100 Unicorns im Vergleich zu Global-2000-Unternehmen

Im Vergleich zu den Global 2000 erreichen die Unicorns bei acht Domainsicherheitsattributen in fünf Kategorien eine höhere Punktzahl. Besonders gut schneiden sie in den Bereichen E-Mail-Sicherheit, da sie SPF, DKIM und DMARC häufiger einsetzen, sowie DNSSEC und CAA-Einträgen ab. Sie alle haben gemeinsam, dass sie über DNS-Einträge verwaltet werden. Dies deutet darauf hin, dass es sich bei den Teams, die die Domainnamen für Unicorns verwalten, wahrscheinlich um IT-Fachleute handelt, die über gute Kenntnisse der innerhalb des DNS verfügbaren Sicherheitsprotokolle verfügen, die für das Unternehmen keine hohen Kosten verursachen.

Bei den Global-2000-Unternehmen haben diejenigen ein höheres Sicherheitsniveau, die einen Registrar der Enterprise-Class nutzen. Warum ist das wichtig? Enterprise-Class-Registrare verfügen über solide Sicherheitsmaßnahmen, wie z. B. die Schulung von Mitarbeitern und Mitarbeiterinnen in Bezug auf Social Engineering und Zwei-Faktor-Authentifizierung. Unternehmen, die Verbraucher-Registrare nutzen, mussten Erfahrungen mit „Doppelgänger-Domains“ machen, bei denen Konten gehackt und Subdomains auf legitimen Domainnamen eingerichtet wurden.

Zudem wurden Registry Locks seltener genutzt, was darauf zurückzuführen ist, dass viele Registrare für Verbraucher diesen Dienst nicht anbieten. Da Global-2000-Unternehmen Registrare der Enterprise-Class nutzen, ist die Chance größer, dass sie Registry Locks einsetzen.

Da sich Unicorns noch in der Entwicklungsphase befinden und sich auf das Marktwachstum konzentrieren, spielt die Wahl des Registrars für sie möglicherweise eine untergeordnete Rolle, oder sie kennen die Unterschiede zwischen Registraren nicht und wissen nicht, wie sich dies auf ihren Sicherheitsstatus auswirkt. Die Art des Registrars wirkt sich direkt auf die Einführung von Registry Locks und die Sicherheit aus, denn diese Sperrmechanismen werden von Registraren für Verbraucher nicht unterstützt. Daher sind Unicorns anfällig für Angriffe wie DNS-Hijacking, Domain-Hijacking, E-Mail-Spoofing und vieles mehr, wenn ihr Registrar ohne zusätzliche Sicherheitsebenen leichter angreifbar ist. Selbst mit einem starken IT-Team und soliden DNS-Grundlagen könnten Unicorns, wenn sie ihre Geschäftstätigkeit mit größeren, komplexeren Domainportfolios ausweiten, einem großen Risiko ausgesetzt sein, wenn die Sicherheit ihrer Domains in den Händen ihres Domainregistrars liegt, da sich jeder Vorfall oder jede Ausfallzeit direkt auf die meisten dieser online tätigen Unternehmen auswirkt.

KI und Technologie dominieren

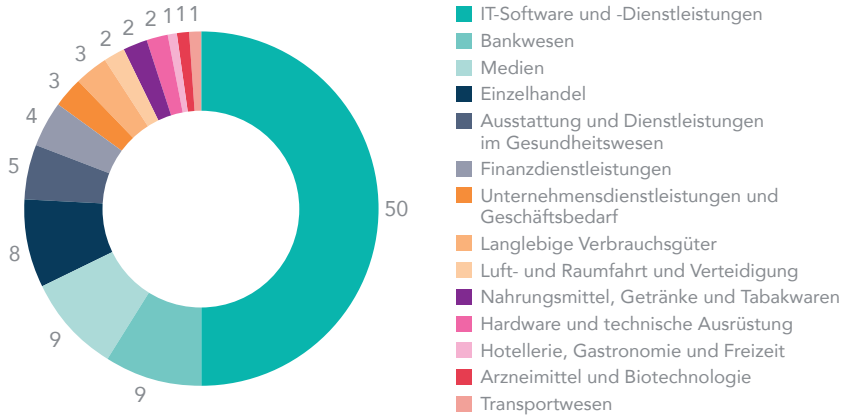


Abbildung 11: Branchenverteilung unter 100 Unicorns

Die Hälfte der Unternehmen unter den 100 Top-Unicorns gehören zur IT-Branche, gefolgt vom Bankwesen, das an zweiter Stelle steht. Bei vielen IT-Dienstleistern handelt es sich um reine KI-Unternehmen, und bei den meisten Bankunternehmen handelt es sich um FinTech-Start-ups, die beide stark auf das Internet angewiesen sind, um ihr Geschäft voranzutreiben.

Wer ist am sichersten?

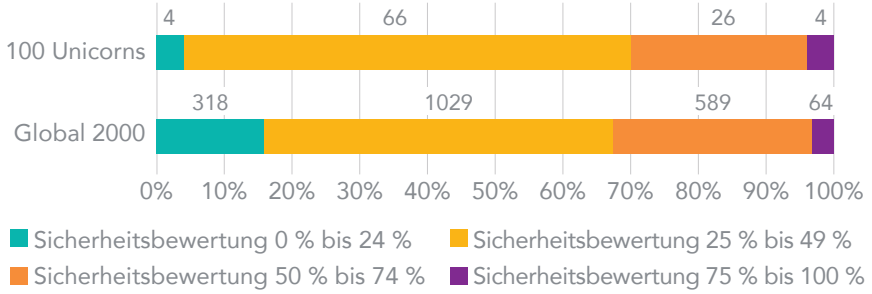


Abbildung 12: Levels der Domain-Sicherheit – 100 Unicorns im Vergleich zu Global-2000-Unternehmen

Ein Vergleich der Domain-Risikowerte der Global 2000 mit denen der Unicorns bringt keine wesentlichen Unterschiede zutage. Es ist offensichtlich, dass weniger Unicorns (4 %) im niedrigen Wertebereich liegen, verglichen mit 15 % der Global 2000. Allerdings sind deutlich mehr Unicorns im mittleren Bereich vertreten, was zeigt, dass sie bestimmte Elemente wie E-Mail-Sicherheit ernst nehmen, aber einige der fortschrittlicheren Sicherheitsprotokolle wie Registry Locks und DNS-Redundanz vernachlässigen.

Fazit

Unternehmen investieren weiterhin schrittweise in die Verbesserung der Sicherheit ihrer Domains, aber bei den größten Unternehmen der Welt gibt es noch viel Nachholbedarf. Wir glauben, dass staatliche Maßnahmen mit Gesetzen wie NIS2 dazu beitragen werden, diese Veränderungen schneller voranzutreiben, zumal wir eine anhaltende Zunahme von Cyberangriffen auf multinationale Unternehmen beobachten.

Unicorns haben schnell Domain-Sicherheitsprotokolle rund um die DNS-Sicherheit eingeführt, was häufig auf kleinere, flexiblere IT-Abteilungen zurückzuführen ist, die in der Lage sind, schnelle Entscheidungen zu treffen, ohne die Komplexität eines weltweit aufgestellten Unternehmens bewältigen zu müssen. Dennoch sind sie in Bezug auf DNS-Redundanz, Registry Locks und Enterprise-Class-Registrare eher im Rückstand. Dies kann sich jedoch mit fortschreitender Reife des Unternehmens und immer fortschrittlicheren Anbietern ändern. Mit der Zeit werden die Unicorns dafür sorgen müssen, dass sowohl ihre eigene Domainsicherheit als auch die ihrer Lieferkette und der Lieferkette, deren Bestandteil sie sind, gestärkt wird. Möglicherweise bedarf es eines größeren Vorfalls oder eines staatlichen Eingriffs, um die Dringlichkeit des Themas zu verdeutlichen – auch wenn KI, die Branche, in der viele Unicorns tätig sind, weiter an Bedeutung gewinnt und unterstreicht, wie wichtig die Sicherheit für das Wachstum ihrer Unternehmen ist.

Wenn ein Unternehmen seine Domainsicherheit vernachlässigt, 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.

Wenn Unternehmen die Sicherheit ihrer Domains nicht ernst nehmen, kann dies den Missbrauch durch Dritte zur Folge haben. Angesichts sich ständig verändernder geopolitischer Systeme, immer raffinierterer böswilliger Akteure und der Einführung von KI in böswilligen Cyberkampagnen müssen wir alle gemeinsam dafür sorgen, dass wir zu schwer angreifbaren Zielen werden.

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 zur 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 in puncto Cybersicherheit zu verstehen und ihre digitalen Online-Vermögenswerte 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-Vermögenswerte 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 und kann überall dort tätig sein, wo unsere Kunden und Kundinnen sind. Dies erreichen wir, indem wir in jedem Geschäftsbereich, den wir bedienen, Experten und Expertinnen beschäftigen.

Kontaktieren Sie uns

cscdbs.com/de

[1]cnbc.com/2025/09/21/what-we-know-about-the-cyberattack-that-hit-major-european-airports.html