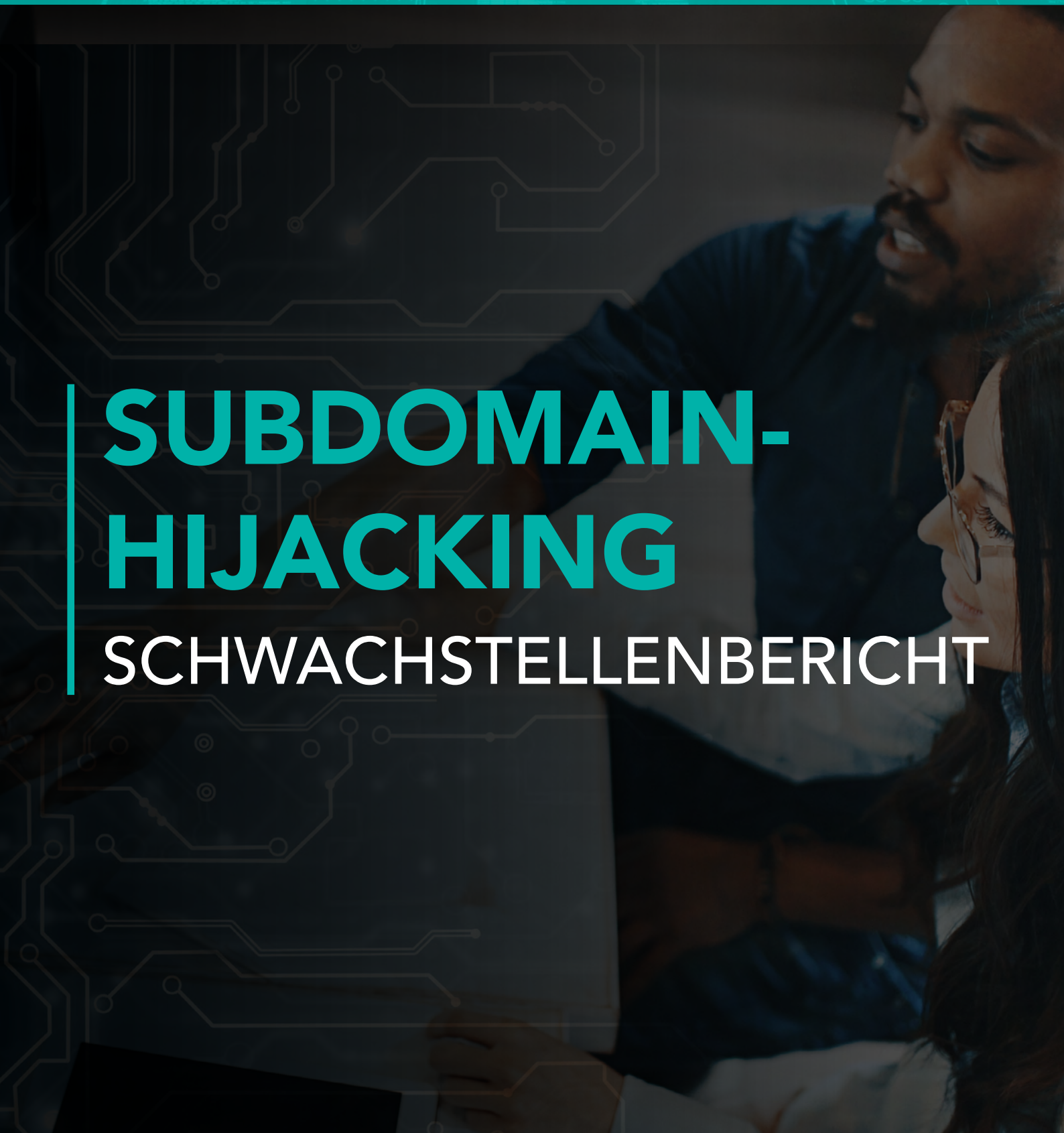


# SUBDOMAIN-HIJACKING

## SCHWACHSTELLENBERICHT

## KURZFASSUNG

Global agierende Unternehmen sind auf das Internet angewiesen. Das Internet ist für Websites, E-Mail, Authentifizierung, Voice over IP (VoIP) und vieles mehr, unverzichtbar. Als Teil der externen Angriffsfläche eines Unternehmens muss es kontinuierlich auf Angriffe und Betrug durch Cyberkriminalität überwacht werden. Das Domain Name System (DNS) ist im Grunde das Telefonbuch des Internets, und die Verwaltung von DNS-Einträgen ist eine der am schlechtesten bewältigten Aufgaben. Dies liegt an der mehr als 20-jährige Geschichte mit verschiedenen Eigentümern, Richtlinien und Anbietern für das DNS und natürlich an der damit verbundenen Scheu der Administratoren, etwas zu löschen, bei dem sie sich unsicher sind. Für Unternehmen ist es eine große Herausforderung, alle ihre digitalen Vermögenswerte zu erfassen und zu erkennen, welche davon kritisch, funktional oder redundant (also nicht mehr erforderlich) sind. Noch erschreckender ist die Tatsache, dass bei Tausenden Domain-Portfolios, die von CSC verwaltet werden, einer von fünf DNS-Einträgen in einem Zustand belassen wurde, in dem er für Subdomain-Hijacking anfällig ist.

## WICHTIGE ERKENNTNISSE

CSC hat über 6 Millionen DNS-Einträge aus seiner Datenbank auf A- und CNAME-Einträge untersucht und etwas mehr als 440.000 DNS-Einträge ausgefiltert, die auf eine Cloud-Infrastruktur verweisen, bei der das Potenzial für eine Kompromittierung durch Subdomain-Hijacking gegeben ist. Wir taten dies, um den aktuellen Stand der Subdomain-Verwaltung von Unternehmen zu ermitteln. Anhand dieser 440.000 DNS-Einträge konnten wir feststellen, dass viele Unternehmen anfällig für Subdomain-Hijacking sind.

**21 % der DNS-Einträge verweisen auf Inhalte, die nicht aufgelöst werden können;** dies kann Unternehmen anfällig für Subdomain-Hijacking machen.


**63 % zeigen Fehlerstatuscodes wie „404 not found“ oder „502 bad gateway“.** Viele Domainnamen mit konfigurierten DNS-Einträgen führen zu einer unerwünschten Antwort.

**Bei einem hohen Prozentsatz von 38 % wird der interne Serverfehler (internal server error) angezeigt,** was zeigt, dass Unternehmen ihre DNS-Pflege und Cyber-Hygiene verbessern müssen.

## UNTERSUCHTE DNS-EINTRÄGE

| | |
|---|---|
| **Zonen, die NICHT aufgelöst werden** | **62.87%** |
| Internal server error | 38.12% |
| Not found | 20.78% |
| Bad request | 2.41% |
| Service unavailable (generell temporär) | 1.30% |
| Bad gateway | 0.11% |
| Gateway timeout | 0.10% |
| No content | 0.03% |
| Gone | 0.01% |
| Negotiation circular reference | 0.00% |
| Upgrade required | 0.00% |
| Unable to process entity | 0.00% |
| Not acceptable | 0.00% |
| Load balancing issue | 0.00% |
| Network connect timeout error | 0.00% |
| Conflict | 0.00% |
| **Zonen, die aufgelöst werden** | **37.13%** |
| Permanent redirect | 20.10% |
| Unauthorized | 5.71% |
| OK | 4.68% |
| Forbidden | 3.49% |
| Temporary redirect | 2.87% |
| Temporary redirect since http/1.1 | 0.14% |
| Permanent redirect (RFC 7538) | 0.10% |
| Success | 0.03% |
| Method not allowed | 0.00% |
| User defined resource error | 0.00% |
| Proxy authentication required | 0.00% |
| | **100.00%** |

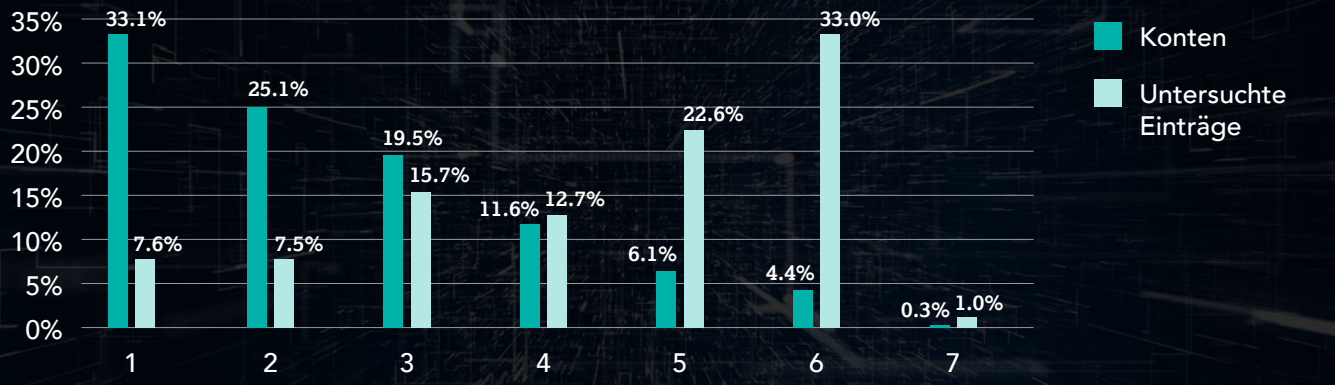
## **RISIKOFAKTOREN:** VERBREITETE NUTZUNG VON CLOUD-ANBIETERN

Von allen untersuchten Einträgen werden **mehr als 82 %** bei Cloud-Anbietern gehostet.

Dieser Prozentsatz spiegelt den Trend wider, dass Unternehmen in den letzten Jahren verstärkt Cloud-Anbieter beauftragen, anstatt die traditionellen internen Rechenzentren zu nutzen. Die Nutzung von Cloud-Anbietern verschafft Unternehmen Zugang zu neuen Technologien, ermöglicht ihnen mehr Flexibilität und Dynamik und ist kostengünstiger. Allerdings birgt dies für Unternehmen, die nun mehr DNS-Einträge als je zuvor verwalten müssen, mehr Risiken.

## **RISIKOFAKTOREN:** DEZENTRALISIERUNG DER PROVIDER BEI UNTERNEHMEN MIT GRÖSSEREN PORTFOLIOS

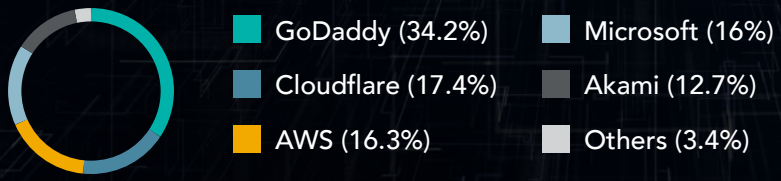
### ANZAHL DER GENUTZTEN PROVIDER




58 % der untersuchten Unternehmen scheinen bei der Konsolidierung ihrer Subdomains bei nur einem oder zwei Cloud-Anbietern besser abzuschneiden, besitzen jedoch tendenziell kleinere Portfolios, die leichter zu verwalten sind.

Dagegen nutzten 11 % der in dieser Studie untersuchten Unternehmen fünf oder mehr Cloud-Anbieter. Auf diese Unternehmen entfallen mehr als die Hälfte aller untersuchten DNS-Einträge, und einige haben große Portfolios mit Tausenden von Einträgen pro Unternehmen. Dies zeigt, dass Unternehmen mit großen Portfolios möglicherweise keine zentrale Verwaltung ihrer Cloud-Anbieter haben, was es für sie schwierig macht, einen guten Überblick über alle ihre DNS-Einträge zu behalten.

### VERTEILUNG DER GENUTZTEN CLOUD-ANBIETER




Über 96 % aller untersuchten DNS-Datensätze sind auf fünf der größten Cloud-Anbieter verteilt – GoDaddy®, Cloudflare®, AWS, Microsoft® und Akamai.

## EINDÄMMUNG VON CYBER-BEDROHUNGEN DURCH SUBDOMAIN MONITORING

Große Unternehmen mit breitgefächerten Markenportfolios und internationalen Niederlassungen sind sich oft nicht bewusst, wie groß ihr digitaler Fußabdruck ist. Digitale Datensätze sammeln sich mit der Zeit an, was die Erhaltung der Cyber-Hygiene zu einer echten Herausforderung macht.

Ohne eine geeignete Überwachung der digitalen Datensätze und entsprechende Administration entwickeln Unternehmen ein „Rauschen", das Cyber-Hygiene und Pflege erschwert und Cyberkriminellen leichte Beute bietet. Diese Ansammlung inaktiver Zonen, die nicht auf Inhalte verweisen, wird als „dangling DNS" bezeichnet und birgt die Gefahr des Subdomain-Hijacking. Das öffnet Tür und Tor für andere Cyberangriffe wie Phishing, Malware und Ransomware, die zu Reputationsschäden, Vertrauensverlust bei den Verbrauchern und noch schädlicheren Daten und Sicherheitsverletzungen führen können. Administratoren, die die Vorgeschichte der einzelnen Domains nicht kennen, zögern, diese veralteten Einträge zu löschen, da sie befürchten, dass sie mit kritischen Infrastrukturen verbunden sind und versehentlich der Geschäftsbetrieb zum Erliegen kommen könnte.

Für Unternehmen ist es eine Herausforderung, alle ihre digitalen Vermögenswerte zu erfassen und zu erkennen, welche davon kritisch, funktional oder redundant (also nicht mehr erforderlich) sind. Die Pflege von DNS-Datensätzen ist eine der am schlechtesten bewältigten Aufgaben in der Geschäftswelt. Das liegt an der mehr als 20-jährigen Geschichte mit verschiedenen Eigentümern, Richtlinien, Anbietern und natürlich der damit verbundenen Scheu, etwas zu löschen, bei dem man sich unsicher ist.

Darüber hinaus ist Subdomain-Hijacking eine von vielen Bedrohungen für die Domain-Sicherheit, die es heutzutage gibt. Dazu gehören Domain- und DNS-Hijacking, Domain-Shadowing und Cache-Poisoning. Diese Bedrohungen dienen oft als Grundlage für noch schwerwiegendere Phishing- und Ransomware-Angriffe sowie für die Business Email Compromise (BEC), E-Mail-Spoofing oder sogar Datenschutzverletzungen.

Wir empfehlen allen Unternehmen den Einsatz einer Subdomain-Überwachungslösung, die nicht nur eine Warnung ausgibt, wenn Änderungen an den DNS-Einträgen festgestellt werden, sondern auch den Kontext liefert, damit fundierte Entscheidungen getroffen und geeignete Maßnahmen ergriffen werden können, um einen Subdomain-Hijack zu verhindern.

Hier erfahren Sie mehr über die Subdomain Monitoring-Lösung von CSC.

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



DBS04052023