Der Schnittpunkt Ihrer Cybersicherheit mit der Verwaltung von Domain-Namen

CSC-Einblicke

Contents

Verwaltung von Cyberrisiken mit der Geschwindigkeit von KI

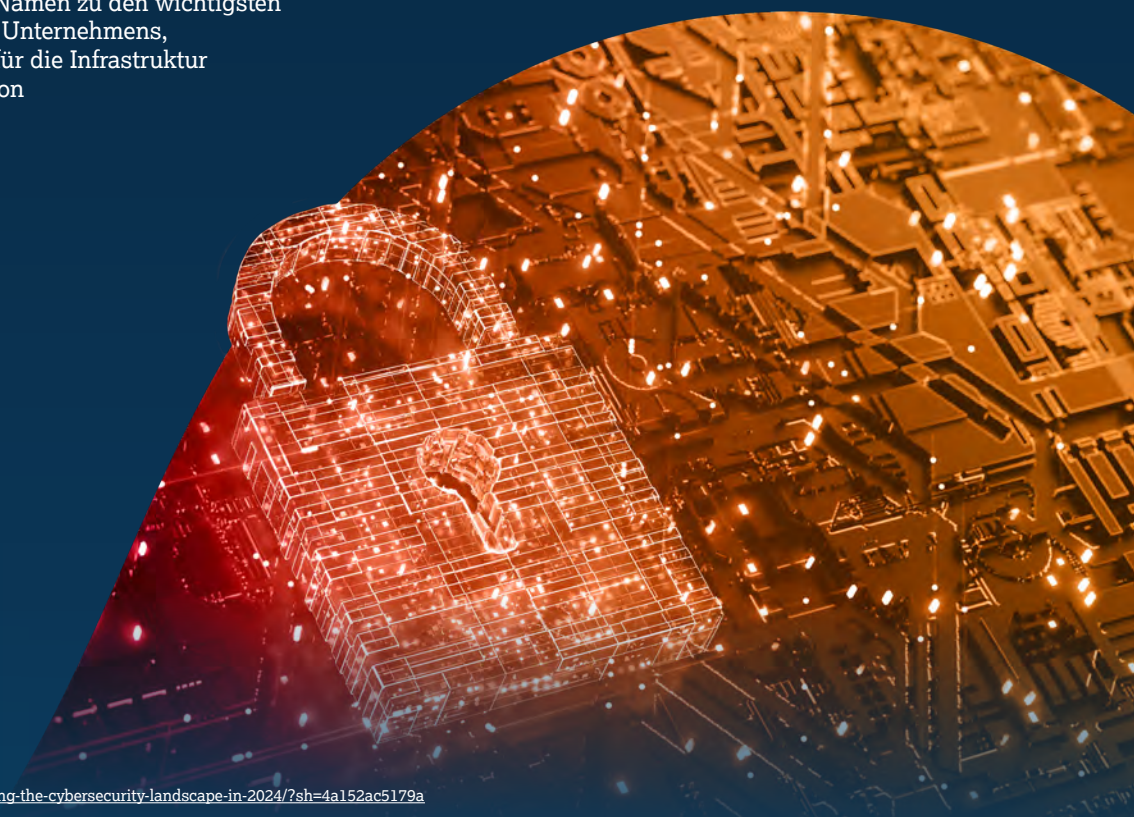
Angesichts des zunehmenden Einsatzes von künstlicher Intelligenz (KI) und der stetig wachsenden Komplexität von Cyber-Bedrohungen müssen sowohl Unternehmen als auch Einzelpersonen ihre Anstrengungen zum Schutz vor kritischen Cyberrisiken deutlich erhöhen. Was Kriminellen die Möglichkeit gibt, mehr Schaden in kürzerer Zeit anzurichten, unterstützt gleichzeitig auch bessere Cyberabwehrstrategien.[1] KI-Ergebnisse aus einer kürzlich durchgeführten Splunk-Studie[2] zeigen, dass 70 % der Führungskräfte im Sicherheitsbereich glauben, dass KI Angreifern mehr Vorteile bietet als Verteidigern. Dennoch experimentieren bereits 35 % mit KI für die Cyberabwehr.

Doch die Aussichten sind nicht nur düster. Ein kürzlich erschienener Bericht von Goldman Sachs legt nahe, dass generative KI das Bruttoinlandsprodukt (BIP) um 7 % erhöhen könnte, was für eine einzelne Technologie wahrlich bemerkenswert ist. Doch auch Cyberkriminelle nutzen generative KI bei gezielten Angriffen, um eine höhere Komplexität und schnellere Bereitstellung zu erreichen. Generative KI ermöglicht es Kriminellen zudem, personalisierte und gezielte Phishing-E-Mails zu erstellen, die frei von Rechtschreib- und Grammatikfehlern sind. Dadurch erschwert sich die Erkennung solcher E-Mails. Derzeit verfügbare KI-Tools aus dem Dark Web wie FraudGPT gestatten es Kriminellen, komplexere Social-Engineering-Deepfake-Angriffe zu starten, die die Emotionen oder das Vertrauen ihrer Ziele noch schneller manipulieren.

Domains als Grundlage für Cyberangriffe

Phishing-Angriffe, kompromittierte Geschäfts-E-Mails (BEC) und Social Engineering führen heutzutage zu noch komplexeren Angriffen durch Malware und Ransomware. Da überrascht es, dass Chief Information Security Officers (CISOs) ihren Domain-Namen und der online freiliegenden externen Angriffsfläche nicht mehr Aufmerksamkeit schenken. Sie verbringen viel Zeit damit, ihr Netzwerk zu verstärken, doch die Grenzen haben sich verschoben. Viele CISOs wissen nicht, wer ihre Domain-Registrare sind, geschweige denn, ob sie das richtige Maß an Sicherheit für eine Unternehmensumgebung bieten.

Globale Unternehmen nutzen das Internet für alles – für Webseiten, E-Mails, Authentifizierung, Voice-over-IP (VoIP), Kundenportale, Lieferantenanwendungen 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 Cyberrisiken zu quantifizieren und ihre Schadensmöglichkeiten zu erfassen. Damit gehören Domain-Namen zu den wichtigsten Elementen der Cybersicherheit eines Unternehmens, da das Internet und Domain-Namen für die Infrastruktur und Kontinuität des Unternehmens von entscheidender Bedeutung sind.



1. forbes.com/sites/emilsayegh/2023/12/19/navigating-the-cybersecurity-landscape-in-2024/?sh=4a152ac5179a
2. splunk.com/en_us/form/ciso-report.html

„Domain-Namen, die wichtige Geschäftsfunktionen ausführen, befinden sich in einem Ökosystem, das jedes Unternehmen als Teil der externen Angriffsfläche betrachten sollte. In ihrer Umgebung können Domain-Namen und Subdomains entweder buchstäblich kompromittiert (gekapert) oder böswillig registriert werden. Das bedeutet, dass Marken-Lookalikes, d. h. gefälschte Websites, eine Marke für bösartige Zwecke wie BEC-Angriffe oder Phishing- und Malware-Verbreitungsangriffe imitieren können. Viele sind überrascht zu hören, dass jede beliebige Person einen Domain-Namen registrieren kann, solange er verfügbar ist. Wenn Sie also keine Registrierungen für die Domains Ihrer Marke verwenden oder keine Homoglyphen und andere Strategien zum Schutz Ihrer Marke einsetzen, wird es im Internet immer wieder Betrüger geben, die versuchen, mit Ihrer Marke und deren etabliertem Vertrauen Geld zu machen. Dies wiederum gefährdet sowohl Ihren Umsatz als auch Ihren Ruf, ganz zu schweigen von den Sicherheitsbedenken der Verbraucher.“

Ihab Shraim, Chief Technology Officer,
Digital Brand Services von CSC im Gespräch mit Safety Detectives

Es gibt mehrere Möglichkeiten, Unternehmen und ihre Domains anzugreifen:

Kompromittierte Domains oder gekaperte Subdomains

Cyberkriminelle kompromittieren alle ungesicherten Domains. Um sich dagegen zu schützen, sollten Unternehmen mit einem mehrschichtigen, tiefgreifenden Verteidigungsansatz beginnen. In erster Linie müssen Unternehmen die Online-Präsenz ihrer Marke sichern, indem sie das Domain-Portfolio – das durch Übernahmen aus mehreren Marken bestehen kann – und den Online-DNS-Footprint (Domain-Namensystem) sichern.

Erstellung bösartiger, betrügerischer Domains

Einige Länder schränken zwar ein, wer sich mit ihren Endungen registrieren kann, indem sie eine eingetragene Marke, ein eingetragenes Unternehmen oder eine lokale Präsenz verlangen, doch die Tatsache, dass jeder jede Domain registrieren kann, ist alarmierend. Ziel dieser gefälschten Domain-Registrierungen ist es, sich das Vertrauen der Verbraucher in die anvisierte Marke zunutze zu machen und überzeugende Phishing-Angriffe, andere Formen des digitalen Markenmissbrauchs oder Verstöße gegen geistiges Eigentum (IP) einzuleiten. Dies führt zu Umsatzeinbußen, Traffic-Umleitungen und einer Beeinträchtigung des Markenrufs für das betreffende Unternehmen, während sich Betrüger eine goldene Nase verdienen. Es gibt unzählige Domain-Spoofing-Taktiken mit Permutationen und Homoglyphen, die von Phishern und böswilligen Dritten leicht ausgenutzt werden können. permutations and homoglyphs that are easily used by phishers and malicious third parties.

Registrierung frisch erloschener Marken-Domains durch Dritte

Unternehmen registrieren defensiv kritische Domain-Namen, um Online-Betrug für ihre Marke zu verhindern. Manchmal sind diese Unternehmen nach der Registrierung mit Kostendruck oder einer Verlangsamung einer Marke konfrontiert und lassen diese Domains wieder verfallen. Genau darauf warten Cyberkriminelle – und registrieren denselben Domain-Namen sofort erneut für bösartige Zwecke. Sie sind ständig auf der Suche nach verfügbaren Marken-Domains, die sie als Waffe einsetzen können.

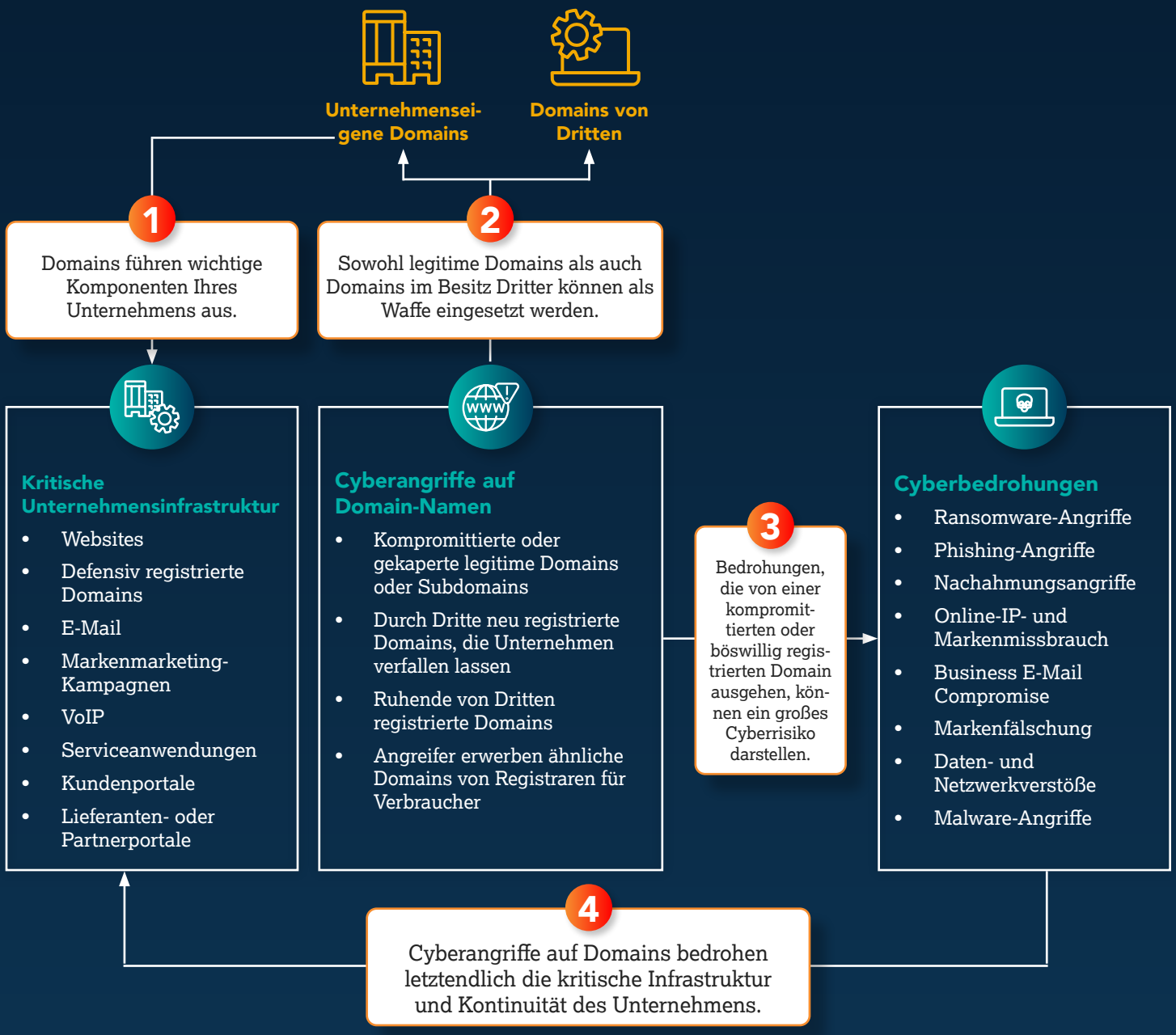
Ruhende Domains

Einige Cyberkriminelle registrieren Marken-Domains und behalten sie, um sie dann an das Zielunternehmen weiterzuverkaufen,

z. B. indem sie Holding- oder Parking-Seiten hosten oder die Nachricht „Website im Aufbau“ anzeigen. Sie planen möglicherweise sogar noch größere schädliche Aktivitäten wie Phishing- oder Malware-Angriffe. Ein ruhender Domain-Name, der mehr als sechs Monate nach dem ursprünglichen Registrierungsdatum als Waffe genutzt wird, wird als „U-Boot-Domain“ bezeichnet. Ruhende Domains fallen bei der anfänglichen Erkennung oft durchs Raster, da sie nicht sofort die Merkmale einer für einen Angriff registrierten Domäne aufweisen, z. B. einen aktiven MX-Datensatz, der normalerweise ein Warnsignal auslösen würde. Das lässt Cyberkriminellen viel Raum, um komplexere und personalisierte Angriffskampagnen mit verheerenden Auswirkungen zu entwickeln.

Neben dem Alter der Domain ist es auch wichtig, aktiv zu überwachen, wie nah die Domain-Registrierungen an zuvor identifizierten Bedrohungen liegen, und zu sehen, ob es ein Registrierungsmuster gibt. Registrierungsmuster sind nicht einfach an einem Ort zu erkennen, aber wenn Ihr Domain-Registrar KI und Technologien für maschinelles Lernen für seine eigenen Daten und für verschiedene Top-Level-Domains (TLDs) bereitstellt, können Muster über IP-Adressen hinweg erkannt werden. Außerdem ist es wichtig, auf nachahmende Verhaltensweisen in Ihrer Domain-Aktivität zu achten. Ein Beispiel: Wenn Ihre Marke eine Reihe neuer Domains für ein neues Produkt oder eine neue Dienstleistung registriert, tun Dritte das gleiche?

Externe Angriffsfläche einer Domain



Die meisten Cybersicherheitsrisiken sind der Unternehmensführung allgemein bekannt, z. B. wie wichtig der Schutz vor Datenschutzverletzungen, das Identitäts- und Schwachstellenmanagement, Zugriffskontrollen, Datenschutz, Schutz vor gestohlenen Anmeldedaten und Wachsamkeit in Bezug auf Social-Engineering-Taktiken sind. Wenn es jedoch um den alltäglichen Schutz der Cybersicherheit geht, wissen viele Teams offensichtlich nicht, wer für die Domain-Sicherheit ihres Unternehmens verantwortlich ist. Domain-Namen werden häufig für Marketing- und Markeninitiativen verwendet. Sicherheitsteams haben daher möglicherweise das Gefühl, dass der Schutz von Online-Domain-Namen dem Marketing oder der Rechtsabteilung obliegt. Wenn Unternehmen nicht wissen, wer ihre Domain-Registrare sind, sind sie sich wahrscheinlich auch nicht der Richtlinien bewusst, die die Registrare anwenden, sowie der Sicherheitsmaßnahmen, die für Marken-Domains gelten.

Leider sind die Angreifer mit der zunehmenden Online-Präsenz von Unternehmen bestens vertraut, weshalb sie ein besonderes Interesse daran haben, Domain-Namen von Unternehmen anzugreifen, die nicht geschützt sind. Ohne verstärkte Sicherheitsposition befindet sich die IT-Abteilung im Auge des Sturms und muss einen Pfad voller Domain- und DNS-Angriffe beschreiten, der potenziell verheerende finanzielle und rufschädigende Folgen haben kann. Der Domain Security Report von CSC hat kürzlich die Unternehmen auf der Global 2000-Liste von Forbes analysiert und festgestellt, dass fast drei Viertel dieser Unternehmen weniger als 50 % aller Domain-Sicherheitsmaßnahmen implementiert haben. Diese Erkenntnis und die Tatsache, dass viele Unternehmen ihre Domain-Registrare im Allgemeinen nicht kennen, lässt vermuten, dass die Sicherheit von Domains oft auf die lange Bank geschoben wird – möglicherweise auch, weil sie nicht in deren Besitz sind.

Der Vorteil einer Zusammenarbeit mit einem Registrar der Enterprise-Klasse

Es gibt zwei allgemeine Kategorien von Domain-Registraren: für Verbraucher und für Unternehmen Registrare für Verbraucher machen mehr als 99 % aller Registrare weltweit aus und sind auf Domain-Services, Websites, E-Mail für die private Nutzung, Unternehmer und Start-ups in der Anfangsphase ausgerichtet. Registrare der Unternehmensklasse legen den Fokus hingegen auf die Arbeit mit Unternehmen und Markeninhabern, die erweiterte Geschäftsfunktionen, Expertise und personelle Unterstützung für die Domain- und DNS-Verwaltung sowie Sicherheit, Markenschutz, Betrugsabwehr, Daten-Governance und Cybersicherheit benötigen.

Verbraucherklasse und Unternehmensklasse im Vergleich

Registrare für Verbraucher

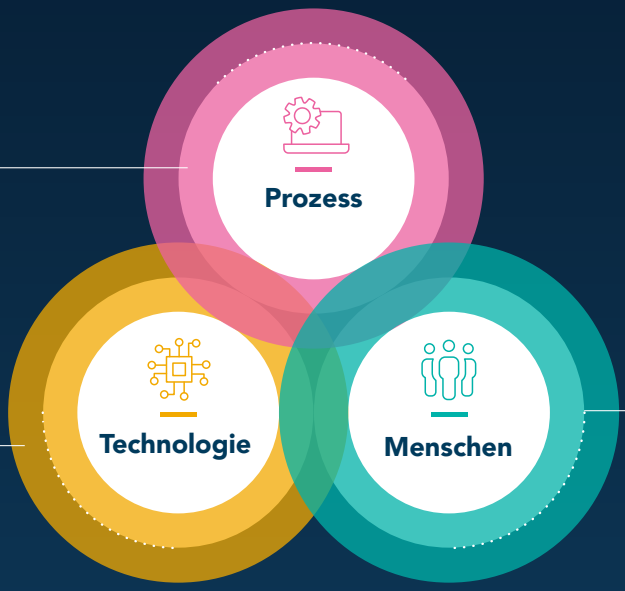
Ein Registrar für Verbraucher ist auf Domain-Services, Websites und E-Mail für die private Nutzung sowie Unternehmer und Kleinunternehmen, die gerade am Anfang stehen, spezialisiert.

Registrare für Unternehmen

Ein Registrar für Unternehmen 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 (Domain-Namensystem) sowie Sicherheit, Markenschutz, Betrugsabwehr, Daten-Governance und Cybersicherheit benötigen.

Registrare der Unternehmensklasse sind unerbittlich in Sachen Sicherheit

- ICANN- und Registry-zertifiziert
- Vollständige Erfassung aller Domains, DNS und Anbieter digitaler Zertifikate
- Anforderungen erfolgen immer schriftlich (nie telefonisch)
- Erfüllt allgemeine Datenschutzvorgaben und die Anforderungen der Daten-schutz-Grundverordnung (DSGVO)
- Richtlinie für Registry-Übertragungssperre



- Nach ISO 27001 zertifizierte Rechenzentren
- SOC 2® -Konformität
- Penetrations- und Schwachstellentests durch Dritte
- Regelmäßige Sicherheitstests, ein-schließlich SQL-Injection und XSS

- Identitätsüberprüfung nach dem Prinzip „Know Your Customer“ (KYC)
- Überprüfung des Office of Foreign Assets Control (OFAC)
- Weltweiter interner Support rund um die Uhr an 365 Tagen in den jeweiligen Landessprachen
- Regelmäßige Schulungen von Mitarbeit-enden im Bereich Cybersicherheit

Es empfiehlt sich, einen Anbieter der Unternehmensklasse zu wählen, der in Personal, Prozesse und Technologien investiert hat, die mit Blick auf die Sicherheit integriert sind. Zwar kann jeder behaupten, dass er Dienstleistungen anbietet, die den Anforderungen der heutigen globalen Unternehmen entsprechen, doch liegt es an den Unternehmen, ihre Hausaufgaben zu machen, um die Unterschiede zwischen den einzelnen Anbietern zu verstehen. Unternehmen müssen nachvollziehen können, wie sich die Wahl des Anbieters in die Entscheidungen über die allgemeine Sicherheitsposition ihres Unternehmens einfügt und wie es um die Einhaltung von Vorschriften und Risiken bestellt ist.

Sieben Schritte, die ein Registrar für Unternehmen umsetzen sollte, um Ihr Domain-Portfolio zu sichern

Wie die Verwaltung eines Portfolios digitaler Zertifikate kann auch die Verwaltung von Domain-Namen komplex sein. Mit diesen Schritten übernehmen Sie die Kontrolle über wichtige Unternehmensressourcen und reduzieren die Sicherheitsbedrohungen für Ihre Marke.

1

Wie die Verwaltung digitaler Zertifikate mit einer Public Key Infrastructure (PKI) sorgt die Verwaltung eines globalen Portfolios von Domain-Namen in einem Verwaltungssystem für konsistente Prozesse und die Sicherung von Werten, auf die sich Ihr Unternehmen verlässt.

Zentralisierung

Automatisierung

2

Sobald alle Ihre Domain-Ressourcen zentralisiert sind, können Sie von der Automatisierung über eine Reihe von APIs (Application Programming Interfaces) profitieren – ähnlich wie die Verwaltung digitaler Zertifikate. Domain-Portfolio-APIs sollten z. B. folgende Optionen enthalten:

- Berichte zum Domain-Portfolio
- Domain-Verfügbarkeitsprüfungen für neue Registrierungen
- Domain-Registrierung mit Bestellvorlagen zur Abwicklung von Registrierungen für eine Vielzahl von Erweiterungen
- Nameserver- und WHOIS-Kontaktaktualisierungen
- Abrufen und Ändern von DNS-Datensätzen für Namen
- Verwaltung der URL-Weiterleitung
- Berichte zu 10 Arten sicherheitsbezogener Ereignisse in Ihren Domains für Anbieter von Audits oder SIEM-Integration (Security Information and Event Management)
- Verwaltung digitaler Zertifikate, einschließlich Bestellung, Erneuerung, Abruf, Neuausstellung und Widerruf von Zertifikaten; Statusprüfung für alle Bestell- und Aktualisierungsvorgänge verfügbar

3

Es spart Zeit, wenn Sie einen Anbieter beauftragen, der die verschiedenen Gerichtsbarkeiten für jeden Domain-Namen kennt und sicherstellt, dass Ihre Daten auf dem neuesten Stand sind und die Regeln des jeweiligen Landes bzw. der Region einhalten.

Compliance

Integration

4

Es ist sehr wichtig, dass Ihre Domain-Namen und DNS integriert sind, damit Änderungen schnell und sicher vorgenommen werden können.

5

Jedes Unternehmen ist anders und benötigt möglicherweise eine andere Einrichtung. So kann es z. B. sein, dass Sie Domains sehr dezentral verwenden oder dass sie nach Geschäftsbereichen aufgeteilt sind. Ein System, das von verschiedenen Gruppen verwaltet werden kann, erfordert ein hohes Maß an Anpassung, damit die richtigen Benutzer auf die richtigen Informationen zugreifen können. Darüber hinaus müssen Unternehmen komplexe Daten in ihrem Domain-Portfolio durchsuchen und verstehen. Unternehmen benötigen einen schnellen Zugriff auf Daten in einer sicheren, zuverlässigen und funktionsreichen Umgebung, die die Analyse großer Informationsmengen ermöglicht, um datengestützte Entscheidungen zu treffen. Zu den Berichten, die regelmäßig überprüft werden müssen, gehören:

- Live-Webseiten-Status: Einblicke, ob eine Domain in Inhalte aufgelöst wird
- Anzahl von Marken-Zeichenfolgen: Einblicke in die Darstellung verschiedener Marken im Portfolio
- Land: Einblicke, wie die globale Präsenz einer Marke genutzt wird

Flexibilität

Veränderungen in der Landschaft

6

Jedes Jahr werden immer mehr neue Domain-Namen eingeführt, und Sie müssen sicherstellen, dass Ihr Unternehmen die richtigen Entscheidungen für die Registrierung auf der Grundlage potenzieller Bedrohungen trifft. Es ist hilfreich, ein strategisches Beratungsteam zu haben, das Sie beim Schutz Ihrer Marke unterstützt. Es kann Ihnen dabei helfen, wichtige Fragen zu beantworten, z. B.:

- Habe ich die richtige Anzahl von Domains, oder sollte ich meine defensiven Registrierungen erweitern, um das Risiko zu verringern?
- Gibt es einen End-to-End-Workflow zur Abwehr domainbasierter Angriffe mit Bedrohungsinformationen?
- Woher weiß ich, wo ich eine Domain registrieren kann?
- Welche Risiken bestehen, wenn ich sie nicht registriere?
- Wie kann ich innerhalb meiner Organisation kommunizieren und Domains zentral registrieren?

7

Kein Unternehmen kann jede Variante des Domain-Namens registrieren. Mit einer effektiven Domain-Überwachungslösung können Sie daher erkennen, wenn Dritte Ihren Markennamen missbrauchen.

Überwachung

Arbeiten Sie mit einem Registrar der Unternehmensklasse zusammen, um die Auswirkungen der europäischen NIS2-Cybersicherheitsrichtlinie auf Ihre Domains und DNS zu bewerten.

Worum es sich handelt:

„Die Kommission erlässt bis zum 17. Oktober 2024 Durchführungsrechtsakte zur Festlegung der technischen und methodischen Anforderungen der Maßnahmen in Bezug auf Anbieter von DNS-Diensten, TLD-Namensregister, Cloud-Computing-Diensteanbieter, Anbieter von Rechenzentrumsdiensten, Anbieter von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider, Managed Security Services Provider, Anbieter von Online-Marktplätzen, von Online-Suchmaschinen und Plattformen für soziale Netzwerke sowie Anbieter von Vertrauensdiensten.“[3]

Warum das passiert:

„Die 2016 eingeführten EU-Cybersicherheitsvorschriften wurden durch die 2023 in Kraft getretene NIS2-Richtlinie aktualisiert. Sie modernisierte den bestehenden Rechtsrahmen, um mit der zunehmenden Digitalisierung und einer sich entwickelnden Bedrohungslandschaft im Bereich der Cybersicherheit Schritt zu halten. Durch die Ausweitung des Geltungsbereichs der Cybersicherheitsvorschriften auf neue Sektoren und Einrichtungen wird die Resilienz und Reaktionsfähigkeit öffentlicher und privater Einrichtungen, der zuständigen Behörden und der EU insgesamt weiter verbessert.“[4]

3. nis-2-directive.com/NIS_2_Directive_Article_21.html#:~:text=By%2017%20October%202024%2C%20the,service%20providers%2C%20content%20delivery%20network
4. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Risiken bei der Wahl eines Registrars für Verbraucher

Wenn Unternehmen Kosten einsparen wollen, scheint die Bereinigung des Domain-Portfolios ein leichtes Ziel zu sein. Diese kurzfristige Lösung kann langfristig dazu führen, dass Domains von bösartigen Akteuren angegriffen werden, die unter anderem die Einnahmen von der echten Marke abziehen.

Domain-Sicherheit sollte ein wesentlicher Teil der Cybersicherheit sein, um Marken online zu schützen, aber sie hat bei Domain-Registraren für Verbraucher nicht immer oberste Priorität.[5] Das Registraren für Verbraucher entgegengebrachte Vertrauen ist oft nicht gerechtfertigt, weil sie in der Regel der Domain-Sicherheit nicht genug Beachtung schenken. Dieses fehlgeleitete Vertrauen kann sich auf die allgemeine Sicherheitsposition eines Unternehmens auswirken.

Viele Unternehmen befinden sich in dem Irrglauben, dass alle Registrare gleich sind.

Domain-Registrare für Verbraucher bieten ihren Kunden eher Transaktionsbeziehungen und durchlaufen nicht die gleichen gründlichen Überprüfungsprozesse wie Anbieter der Enterprise-Klasse. Sie umfassen keine Lösungen für die Abwehr aller digitalen Risiken von Domain-Spoofing, Domain- und DNS-Hijacking, Subdomain-Takeover und Phishing-Angriffen. Einige Registrare für Verbraucher haben Geschäftspraktiken, die Marken unbeabsichtigt schaden können. Einige betreiben Domain-Marktplätze, die Marken- oder Warenzeichen-Domains abfangen, versteigern und an den Meistbietenden verkaufen, oder sie betreiben Domain-Namen-Spinning und befürworten die Registrierung von Marken-Domains, die Typo-Squatting fördern. Diese Praktiken gefährden zwar nicht direkt Unternehmen, fördern aber den Markenmissbrauch oder die Registrierung verwirrend ähnlicher Domains, die für schändliche Zwecke verwendet werden könnten.

Wir alle kennen die Redewendung „Eine Kette ist nur so stark wie ihr schwächstes Glied“. Jedes Unternehmen ist auf eine Kette von Lieferanten und Anbietern angewiesen, und je komplexer diese Lieferkette von Anbietern und Workflows, desto höher das Risiko von Angriffen. Ein Angriff auf die Lieferkette ist ein Cyberangriff, der stattfindet, wenn ein Angreifer das System einer Marke über einen Drittpartner mit Zugang zu Ihren Systemen und Daten kompromittiert. In der Regel wird der Anbieter mit der schwächsten Cybersicherheit ins Visier genommen.

Ein Angriff auf Ihren Provider wirkt sich auch auf Sie aus. In den letzten zwei Jahren gab es einige bemerkenswerte Angriffe auf die Lieferkette. Es ist wichtig, dass der Domain-Registrar für jedes Unternehmen sicher ist und nicht selbst gefährdet werden kann. Domain-Registrare sollten von einem Team überprüft werden, das die Rolle eines Domain-Registrars in der allgemeinen Sicherheitsposition des Unternehmens genau kennt. Es ist wichtig, die Verstöße eines Anbieters zu überwachen. Sicherheitsorientierte Domain-Registrare können den Sicherheitsteams einen Teil der Arbeit abnehmen und es Unternehmen ermöglichen, Bedrohungen in ihren Domains zu erkennen, bevor ein erheblicher Schaden für ihre Marke entsteht.

„Wie im Geschäftsbericht für 2022 beschrieben, der am 16. Februar veröffentlicht wurde, wurde das Unternehmen seit 2020 jedes Jahr von denselben Cyberangreifern angegriffen, zuletzt im vergangenen Dezember. Erwähnenswert ist auch, dass das Unternehmen bereits früher Opfer von Cyberangriffen war. Die Folgen für GoDaddy® sind eine Sache, aber die Verstöße haben vor allem zu Datenkompromittierungen bei mehr als 1 Million Benutzern des Unternehmens geführt.“[6]

-- *Dark Reading*, „What GoDaddy’s Years-Long Breach Means for Millions of Clients“

5. cpomagazine.com/cyber-security/the-glaring-gap-in-your-cybersecurity-posture-domain-security/
6. darkreading.com/cyber-risk/what-godaddy-years-long-breach-means-millions-clients

Minderung des Risikos von kompromittierten legitimen Domains mit einer mehrschichtigen Defense-in-Depth-Strategie

Um das Risiko von Cyberangriffen zu mindern, können die Prinzipien der Defense-in Depth-Verteidigung für die Domain-Sicherheit verwendet werden. Defense-in-Depth ist ein Ansatz, der als militärische Strategie zum Schutz eines bestimmten Objekts begann. Für die Domain-Sicherheit umfasst er den koordinierten Einsatz von mehrschichtigen Sicherheitsmaßnahmen.

Zwar kann jeder behaupten, dass er Dienstleistungen anbietet, die den Anforderungen der heutigen globalen Unternehmen entsprechen, doch jedes Unternehmen muss sich die Zeit nehmen, um die Unterschiede zwischen den einzelnen Anbietern zu verstehen. Unternehmen müssen nachvollziehen können, wie sich die Wahl des Anbieters in die Entscheidungen über die allgemeine Sicherheitsposition ihres Unternehmens und ihre Bedenken bezüglich IP-Verletzungen und Markengesetzen einfügt.

1

Wie Sie prüfen, ob Sie einen Domain-Registrar für Unternehmen nutzen

Wenn es um das Domain-Ökosystem geht, kann sich die Wahl des Domain-Registrars auf Teams auswirken, die für Cybersicherheit und IT, Rechtsfragen (General Counsel), Risiken und Compliance (Chief Risk Officer) sowie Phishing-Angriffe, Online-Betrug und Markenmissbrauch verantwortlich sind. Um das Domain-Namensportfolio eines Unternehmens zu verwalten, müssen Sie mit einem Anbieter zusammenarbeiten, der in den Schutz seiner eigenen Systeme investiert hat.

2

Arbeiten Sie nur mit einem Registrar, der sicheren Zugriff auf Ihre Domain-Verwaltungsplattform bietet

Die zweite Ebene bei einem Defense-in Depth-Ansatz für die Domain-Sicherheit besteht darin, sicherzustellen, dass Ihr Registrar einen sicheren Zugriff auf das Domain- und DNS-Verwaltungssystem vorschreibt. Registrare sollten für alle ihre Kunden eine Zwei-Faktor-Authentifizierung verlangen. Sie sollten auch IP-Validierung und föderierte IDs anbieten, damit sich ihre Kunden mit der Gewissheit, dass sie über eine sichere Authentifizierung bei ihrer Domain-Verwaltungsplattform verfügen, bei ihrem Netzwerk anmelden können.

3

Stellen Sie sicher, dass alle Benutzerberechtigungen kontrolliert und verwaltet werden

Bei der Zusammenarbeit mit einem Registrar ist es entscheidend, dass dieser granulare Berechtigungsstufen anbietet. Der Registrar sollte Ihnen den Zugriff auf die Verwaltung von Benutzerzugängen und Berechtigungen ermöglichen. Er sollte einen Überblick über erhöhte Berechtigungen bieten, einschließlich Benachrichtigungen bei Änderungen. Das ist besonders im Falle eines Cyberangriffs wichtig. Wenn sich ein Angreifer Zugang zu einem Registrierungssystem verschafft, legt er entweder einen neuen Benutzer an oder ändert die Berechtigungen eines bestehenden Benutzers, sodass er Schaden anrichten kann.

4

Nutzen Sie erweiterte Funktionen zur Domain-Sicherheit

Die vierte Ebene des Defense-in Depth-Ansatzes besteht darin, erweiterte Sicherheitsfunktionen für einzelne Domains anzuwenden. Sobald Sie die entsprechenden Domain-Namen identifiziert haben, ist es an der Zeit, die entsprechenden Kontrollmechanismen anzuwenden. Erstens gibt es eine Registrierungssperre, d. h. die Sperrung des Domain-Namens auf Registrierungsebene, die die Automatisierung zwischen einem Registrar und einer Registrierung deaktiviert. Das bedeutet, dass der DNS nicht ohne ein manuelles Passwort geändert werden kann, das von einem autorisierten Kontakt verifiziert werden muss, um den Domain-Namen freizugeben. Dies ist eine äußerst sichere und effektive Methode, um sicherzustellen, dass das DNS eines wichtigen Domain-Namens nicht ohne die entsprechende Autorisierung geändert werden kann.

Subdomain-Hijacking, ohne gehackt zu 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 Cyberhygiene zu einer echten Herausforderung macht. Unternehmen setzen beim Zugriff auf neue Technologien immer mehr auf Cloudanbieter, doch die damit verbundene Zunahme der DNS-Datensätze und die zunehmend komplexeren Umgebungen bergen für sie ein erhöhtes Risiko. Ohne einen Überblick über die digitalen Datensätze und eine tägliche Überwachung werden die digitalen Assets von Unternehmen schnell unübersichtlich, was die Cyberhygiene komplexer macht und es Cyberkriminellen leicht macht, Schwachstellen auszunutzen.

„Digitale Datensätze sammeln sich im Laufe der Zeit an, und Administratoren, die sich nicht über die Geschichte der einzelnen Domains im Klaren sind, zögern, ältere Datensätze zu löschen, weil sie befürchten, dass diese mit kritischen Infrastrukturen verbunden sind. Diese Anhäufung inaktiver DNS-Zonendatensätze, die nicht auf Inhalte verweisen, wird als ‚Dangling DNS' bezeichnet und stellt ein Risiko für Subdomain-Hijacking dar, bei dem ein Angreifer die Kontrolle über eine legitime Subdomain erlangt, die nicht mehr in Gebrauch ist, um seine eigenen betrügerischen oder bösartigen Inhalte zu hosten."

Mark Flegg, global director of security services in *SC Media*, „How to ensure DNS records don't become a security hazard"

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. Beispielsweise berichtete ZDNet, dass eine globale Computing-Plattform Opfer von Subdomain-Hijacking wurde, bei dem Kriminelle auf den Subdomains des Unternehmens Poker-Casinos anzeigten.

Die Ausnutzung unsicherer DNS-Datensätze ermöglicht weitere Cyberangriffe, wie beispielsweise Phishing- und Malware-Verbreitung, die zu Einnahmeverlusten, Datenextraktion, Verlust des Kundenvertrauens und Reputationsschäden führen können. Laut einer Studie des österreichischen IT-Sicherheitsberatungsunternehmens Certitude Consulting, die kürzlich in Security Week veröffentlicht wurde, sind Tausende von Unternehmen anfällig für solche Angriffe. Die Verwaltung von DNS-Datensätzen muss unbedingt ein fester Bestandteil der modernen Cyberhygiene sein. Seit mehr als 20 Jahren sind Unternehmen dem Risiko eines Missmanagements ausgesetzt, da sie unterschiedliche Eigentümer, Richtlinien und Anbieter für die Verwaltung ihres DNS einsetzen. Dies wird noch komplizierter, wenn sie Fusionen und Übernahmen durchlaufen, bei denen auch die Angst besteht, dass etwas gelöscht wird, bei dem sich die Eigentümer unsicher sind.

Der *Bericht zu Unterdomains-Hijacking-Schwachstellen* von CSC untersuchte mehr als 440.000 DNS-Datensätze und stellte fest, dass über 21 % der DNS-Datensätze auf Inhalte verweisen, die nicht aufgelöst werden können, sodass viele Unternehmen anfällig für Subdomain-Hijacking sind. Darüber hinaus zeigen über 277.000 (63 %) Fehlerstatuscodes wie „404 not found“ oder „502 bad gateway“ an. Die Verwaltung von DNS-Datensätzen ist aufgrund der langen Geschichte verschiedener Eigentümer, Richtlinien und Anbieter eine der am häufigsten vernachlässigten Aufgaben. Digitale Datensätze sammeln sich im Laufe der Zeit an, und Administratoren, die sich nicht über die Geschichte der einzelnen Domains im Klaren sind, zögern, ältere Datensätze zu löschen, weil sie befürchten, dass diese mit kritischen Infrastrukturen verbunden sind. Dangling DNS sind dem Risiko des Subdomain-Hijacking ausgesetzt. Beim Subdomain-Hijacking erlangt ein Angreifer die Kontrolle über eine legitime Subdomain, die nicht mehr verwendet wird, und hostet dort eigene betrügerische oder schädliche Inhalte. Das öffnet ein Gateway für andere Cyberangriffe wie Phishing, Malware und Ransomware.

21%

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

Online-Markenschutz als Notwendigkeit für Cybersicherheit

In böswilliger Absicht registrierte Domain-Namen sind oft der Vorläufer von gezielten Phishing- oder BEC-Kampagnen, die mit tödlicher, herunterladbarer Malware ausgestattet sein können. Um diese ersten Angriffe zu verhindern, müssen Unternehmen den Zustand ihrer Domain-Landschaft bewerten und die Trennung zwischen den Teams beseitigen, die für diesen Aspekt der digitalen Markeninitiativen zuständig sind. Sicherheitsteams müssen ihre Domains und Marken aktiv online überwachen, um das Potenzial dafür verringern, dass Web-Domains ihren Markennamen oder eine Version davon für betrügerische Aktivitäten verwenden.

Die Absicherung Ihrer Domains ist der Ausgangspunkt, um Phishing zu stoppen.

Unternehmen brauchen einen besseren Einblick in Kriminelle, die möglicherweise ähnliche Domains registrieren oder neu registrieren und versuchen, sich als ihre Online-Marke auszugeben. Dieser Einblick kann Unternehmen dabei helfen, Sicherheitsvorfälle sofort zu erkennen und dagegen vorzugehen.

In der Vergangenheit haben viele Unternehmen nicht verstanden, wie groß die Herausforderungen und das Wachstum von Kanälen sind, über die Online-Verletzungen stattfinden. Unternehmen investieren Zeit und Geld in den Aufbau vertrauenswürdiger Marken, doch all das könnte umsonst sein, wenn sie Opfer von Online-Kriminalität werden. Die beste Möglichkeit für Unternehmen, ihre Marke zu schützen, ist die Implementierung eines Online-Markenschutzprogramms, das Online-Überwachung und Durchsetzungsmaßnahmen kombiniert, um betrügerische Inhalte zu entfernen. Ergänzende Lösungen, wie die Verwendung von Blockierungsnetzwerken, die Partnerschaften mit Browseranbietern, Internet Service Providern (ISPs) und anderen SIEMs beinhalten können, um betrügerische Websites für Internetnutzer zu blockieren, können ebenfalls zu einem umfassenderen Ansatz beitragen. Der Einsatz dieser Methoden zur Verfolgung und Beseitigung von Aktivitäten von Rechtsverletzern sollte auch mit einem Programm zur sicheren Verwaltung von Domainnamen einhergehen, das es dem Markeninhaber ermöglicht, sein eigenes offizielles Domain-Portfolio zu verwalten und zu schützen.

Die revolutionäre neue Art, Ihr Cyberrisiko online zu senken

Als führender Domain-Registrar der Unternehmensklasse für die größten Marken der Welt revolutioniert CSC das Domain-Namen-Ökosystem. Wir bei CSC sind der Meinung, dass Informationen zur Domain-Sicherheit Macht bedeuten.

DomainSec-Plattform

DomainSecSM ist die erste vollumfängliche Lösung für den Schutz und die Verteidigung der Domain-Ökosysteme von Marken. Es ist die innovativste Lösung für die Verwaltung und Sicherheit von Unternehmens-Domains auf dem Markt, gekoppelt mit einem Online-Marken- und Betrugsschutz der nächsten Generation. Dank der Kombination von Daten aus diesen Lösungen in einer Plattform kann CSC eine exponentiell bessere Cybersicherheit bieten,

um die Sicherheitsposition des Unternehmens zu stärken. Wir können Marken dabei unterstützen, ihr Zero-Trust-Sicherheitsmodell zu verfeinern, das über die bloße Absicherung der Grenzen hinausgeht. Diese einzigartige Plattform nutzt proprietäre Technologie, die maschinelles Lernen, künstliche Intelligenz und Clustering kombiniert, um mithilfe führender Indikatoren intelligente Sicherheitseinblicke 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 CSC

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 Domain-Sicherheit und -Management sowie digitalem Markenschutz und Betrugssicherung. Angesichts der erheblichen Investitionen, die globale Unternehmen in ihre Sicherheitsposition tätigen, kann unsere Plattform DomainSecSM 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 außerdem Online-Markenschutz – eine Kombination aus Online-Markenüberwachung und Durchsetzungsmaßnahmen – mit einem mehrdimensionalen Überblick über verschiedene Bedrohungen außerhalb der Firewall, die auf bestimmte Domains abzielen. Betrugsschutzdienste, die Phishing in den frühen Phasen des Angriffs bekämpfen, runden unsere Lösungen ab. 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.

Kontaktieren Sie uns

cscdbs.com/de