BERICHT ZUR CYBERSICHERHEIT

Oktober 2019

Vincent D'Angelo *Global Director, Corporate Development and Strategic Alliances*

Quinn Taggart *Senior Domain Product Manager*

Ken Linscott *Product Director, Domains and Security*

Letitia Thian *Marketing Manager*

Recherche und Editorial von CSC

Dieser CSC-Bericht zur Cybersicherheit ist eine umfassende Auswahl aller für Sie wichtigen Informationen über Cyber-Kriminalität und Cybersicherheit. Damit erhalten Sie die aktuellen Informationen an einem Ort und können schnell die für Sie und Ihre Marke wichtigen Neuigkeiten abfragen. In dieser Sonderausgabe beleuchten wir, wie im Verteidigungssektor Maßnahmen zur Domain-Sicherheit umgesetzt werden.

Domain-Sicherheit

CSC betreut mehr als 65

der weltweit GRÖSSTEN Marken

CSC unterstützt die Verwaltung der Online-Präsenz von mehr als 65 % der größten Marken der Welt (Interbrand®). Durch Nutzung firmeneigener Tools unterstützen wir unsere Unternehmenskunden bei der Aufdeckung von Sicherheitslücken und strategischer Möglichkeiten in ihrem Domain-Portfolio. Mit der gleichen Methodik analysieren wir die wichtigsten Domainnamen von Unternehmen auf der ganzen Welt, um zu sehen, wie es um deren Domain-Sicherheit steht.

In dieser Ausgabe richten wir den Blick auf Rüstungskonzerne aus aller Welt. Aufgrund der anhaltenden Angriffe auf staatliche Stellen und deren Auftragnehmer, die zu Datenschutzverletzungen[1] führen, ist es unerlässlich, dass wir weiter über diese Angelegenheiten berichten, da sie die Sicherheit einer Nation und das Wohlergehen ihrer Bürger beeinträchtigen können. Da Domainnamen, das Domain Name System (DNS) und digitale Zertifikate die grundlegende Infrastruktur des Internets antreiben, können sensible Apps, Tools, Systeme und Informationen, die auf diese Infrastruktur angewiesen sind, in die falschen Hände geraten, wenn sie nicht mit geeigneten DNS-Schutzmaßnahmen gesichert sind[2].

Wir haben einige der größten Rüstungskonzerne aus 24 Nationen analysiert, um herauszufinden, wie diese Branche Schutzmaßnahmen zur Domain-Sicherheit eingeführt hat.

Domain-Sicherheit und Beobachtungstrends

Basierend auf 100 Rüstungskonzernen aus aller Welt

DNS-Hijacking-Hintergrund

Wir begannen 2019 mit einer DNS-Hijacking-Warnung[3] der US-Behörde für Cybersicherheit und -infrastruktur. Seitdem gab es entsprechende Warnungen von Branchenexperten wie Brian Krebs[4] und Regierungsbehörden anderer Staaten wie dem britischen Cybersecurity Centre (NSCS) [5]. Diese Maßnahmen haben das Bewusstsein für die anhaltenden Risiken im Zusammenhang mit DNS- und Domainnamen-Hijacking-Vorfällen geschärft, aber die meisten Branchen sind weiterhin ungeschützt, wie die CSC-Berichte zur Cybersicherheit in den Sektoren Finanzen und Medien[6] zeigen. Diese Angriffe sind auch nicht auf Unternehmen einer bestimmten Branche, Größe oder geografischen Lage beschränkt. So wurde beispielsweise einem kalifornischen Krankenhaus kürzlich der Domainname gestohlen[7], wodurch der Zugriff auf seine Website, E-Mails, Apps und zugehörige Informationen verloren ging.

Registrar-Anbieter

29 % CORPORATE-REGISTRAR

71 % RETAIL-REGISTRAR

RISIKO

In der Vergangenheit waren Retail-Registrare häufige Ziele von Cyber-Angriffen. Unternehmen sollten mit einem Enterprise-Class-Registrar zusammenarbeiten, der stark in die Sicherheit auf technischer Ebene investiert und Sicherheitsschulungen für die Mitarbeiter anbietet. Dazu gehört die Vermittlung von Unternehmenswerten hinsichtlich der Wachsamkeit und von Wissen, wie man böswillige Absichten erkennt, insbesondere bei Kerndomains.

BEOBACHTUNGEN

29 % der Rüstungsunternehmen nutzen Corporate-Registrare

Bösartige Angriffe auf Domainnamen, E-Mails, das DNS und digitale Zertifikate haben zugenommen. Daher macht die Verwaltung des gesamten Domain-Namen-Portfolios durch einen seriösen Corporate-Registrar im Vergleich zu einem Retail-Registrar die Einführung und Überwachung von Sicherheitsstandards für Domainnamen wesentlich einfacher. Darüber hinaus wird die regelmäßige Bewertung von Schutzmaßnahmen, Prozessen, Tools und der Sicherheit von Domainnamenregistraren zu einem wichtigen Bestandteil der Aufstellung von Unternehmen in punkto Cybersicherheit werden.

Registry-Lock

13 % REGISTRY-LOCK AKTIVIERT

65 % REGISTRY-LOCK NICHT AKTIVIERT

22 % *REGISTRY-LOCK NICHT VERFÜGBAR

RISIKO

Nicht gesicherte Domains sind anfällig für Social-Engineering-Taktiken, die zu nicht autorisierten DNS-Änderungen und Domainnamen-Hijacking führen können. Einige Domains könnten eventuell ungesichert sein, da nicht jede Registry auf der Welt Lock-Services anbietet.*

BEOBACHTUNGEN

13 % haben Registry-Locks eingerichtet

Registry-Locks verhindern Domainnamen-Hijacking und unbefugte Änderungen am DNS, die eine Website offline bringen oder Benutzer zu bösartigen Inhalten umleiten könnten. Angesichts der anhaltenden Risiken durch DNS-Hijacking gegen Regierungen und wichtige Branchen wurde eine sehr geringe Akzeptanz dieser Schutzmaßnahme durch Rüstungskonzerne festgestellt.

Alarmierend ist, dass 69 % der Unternehmen, die den gleichen Domainnamen für ihre Haupt-Website, E-Mail und das DNS nutzen – und die auch für Registry-Locks in Frage kamen – nicht geschützt waren.

DNS provider

32% INTERNAL DNS

13% CORPORATE- ODER ENTERPRISE-DNS

55% SONSTIGE (HOSTING- ODER RETAIL-DNS)

RISIKO

Die Nutzung von DNS-Providern, die gebündelte DNS-Dienste anbieten (Non-Enterprise-Level Provider), birgt potenzielle Sicherheitsbedrohungen wie DDoS-Angriffe sowie Ausfallzeiten und Einnahmeverluste.

DNSSEC

3% DNSSEC EINGESCHALTET

97% DNSSEC AUSGESCHALTET

RISIKO

Die Nichtbereitstellung von DNSSEC – eines der kostengünstigsten Sicherheitsprotokolle – führt zu Schwachstellen im DNS. Das könnte auch dazu führen, dass ein Angreifer jeden Schritt des DNS-Lookup-Prozesses an sich reißt. Dadurch können Hacker die Kontrolle über eine Internet-Browsing-Sitzung übernehmen und Benutzer auf irreführende Websites umleiten.

HTTPS everywhere

77% HTTPS EVERYWHERE EINGESETZT

23% HTTPS EVERYWHERE NICHT EINGESETZT

RISIKO

Die sichere Verschlüsselung aller Online-Transaktionen mit digitalen Zertifikaten minimiert das Sicherheitsrisiko der Entführung von Web-Sitzungen durch Cyber-Kriminelle zur Begehung von Identitätsdiebstahl oder zur Installation von Malware auf Benutzergeräten. Sie hilft auch bei der Bekämpfung von Hackern, die in die Web-Kommunikation eindringen, was zu einer Datenschutzverletzung, zum Diebstahl von Kundendaten, einem DDoS-Angriff oder zur Verunstaltung einer Webseite führen könnte.

BEOBACHTUNGEN

13% nutzen DNS-Provider der Enterprise-Klasse; 3 % nutzen DNSSEC

Die Präferenz der Nutzung von Retail-Domainnamen-Registraren durch Rüstungsunternehmen wird durch die Nutzung von DNS-Hosting durch DNS-Provider, die gebündelte DNS-Dienste anbieten, noch verstärkt, was die Angriffsmöglichkeiten für DDoS-Angriffe und verwandte Bedrohungsvektoren erhöht. Unsere Recherche ergab, dass 13 % der Rüstungsunternehmen DNS-Provider der Enterprise-Klasse bevorzugen, während 32 % ihre eigene DNS-Architektur und 55 % Retail-Provider nutzen. DNSSEC ist eine weitere Methode für den Schutz der gesamten Kommunikation zwischen Benutzern und Web-Assets, jedoch waren die Akzeptanzraten für DNSSEC mit nur 3 % sehr niedrig.

Typ der digitalen Zertifikate

4% EV

84% OV

12% DV

RISIKO

Digitale Zertifikate, die mehr Authentifizierung erfordern, wie z. B. Organization Validation (OV) und Extended Validation (EV), sind weniger anfällig für Probleme als Domain Validation (DV).

BEOBACHTUNGEN

84 % verwenden OV-Zertifikate (Organization Validated), doch 12 % nutzen DV-Zertifikate

Wenn das DNS die Tür zu einem Haus ist, ist ein digitales Zertifikat das Schloss. Die Tür kann noch so stabil sein. Sie bietet keinen Schutz, wenn das Schloss schwach ist. Ein wesentlicher Risikofaktor ist die Art und Weise, wie digitale Zertifikate validiert werden. Die Domainvalidierung (DV), die die niedrigste Stufe der Validierung erfordert, wird von 12 % der Rüstungskonzerne verwendet, was bedeutet, dass Hacker, die Zugang zu internen E-Mails erlangt haben, leicht digitale Zertifikate auf firmeneigenen Domains für böswillige Zwecke validieren können.

E-Mail-Authentifizierung

25% DMARC

85% SPF

3% DKIM

RISIKO

Die Authentifizierung des E-Mail-Kanals mit Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF) oder Domain Keys Identified Mail (DKIM) minimiert das Auftreten von E-Mail-Spoofing und potenziellem Phishing.

BEOBACHTUNGEN

25% use DMARC

Domain-based Message Authentication Reporting and Conformance (DMARC) ist ein E-Mail-Validierungssystem, das entwickelt wurde, um die E-Mail-Domain eines Unternehmens vor der Verwendung für E-Mail-Spoofing, Phishing-Betrug und andere Cyber-Kriminalität zu schützen. Seit die Einführung von DMARC von einigen Regierungen[8] vorgeschrieben wurde, wird eine zunehmende Übernahme dieser Schutzmaßnahme durch Rüstungskonzerne empfohlen und kann dazu beitragen, einige der Bedrohungen für die E-Mail-Kommunikation zu bewältigen.

CAA-Einträge

4% CAA-EINTRÄGE WERDEN GENUTZT

96% CAA-EINTRÄGE WERDEN NICHT GENUTZT

RISIKO

Ein Certificate Authority Authorization (CAA)-Eintrag ist ein in einer Zonendatei gespeicherter Ressource Record, durch den ein Domaininhaber angeben kann, welche Zertifizierungsstellen (CAs) berechtigt sind, ein Zertifikat für einen bestimmten Domainnamen auszustellen. Durch das Hinzufügen von CAA-Einträgen können Sie steuern, welche Zertifizierungsstellen (CAs) Ihr Unternehmen nutzt. Dies stellt sicher, dass nur der von Ihnen gewählte Provider ein Zertifikat für Ihre Domainnamen ausstellen kann und ist eine wesentliche technische Schutzmaßnahme, die die Durchsetzung von Richtlinien und die Abwehr von Cyber-Bedrohungen wie HTTPS-Phishing von entführten Subdomains ermöglicht.

BEOBACHTUNGEN

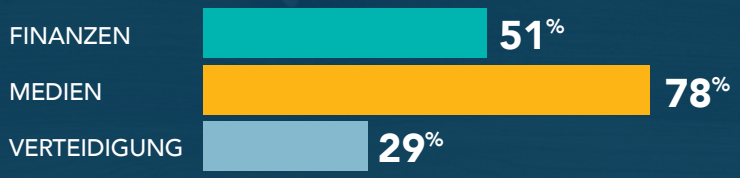
4 % nutzen CAA-Einträge

Als wir auf CAA-Einträge in der Verteidigungsindustrie schauten, stellten wir fest, dass diese nur von 4 % der Unternehmen genutzt werden. Aber trotzdem gestattete die Hälfte der Unternehmen die Ausstellung von Zertifikaten durch Retail-Anbieter. Dies ist vergleichbar mit den 3 % der börsennotierten Unternehmen aus aller Welt, die CAA-Einträge nutzen.

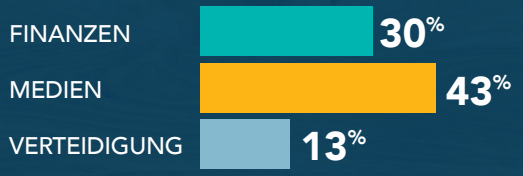
Schutzmaßnahmen zur Domainnamensicherheit in den Sektoren Verteidigung, Medien und Finanzen

Die letzten zwei CSC-Berichte befassten sich mit den Sektoren Finanzen und Medien. Mit dem Schwerpunkt Rüstungskonzerne in diesem Bericht scheint es, dass diese Unternehmen verschiedene Elemente der Domainnamensicherheit langsamer einführen. Das gilt insbesondere hinsichtlich Registry-Locks, die Nutzung eines Domain-Namen-Registrars für Unternehmen, DNS-Hosting-Provider der Enterprise-Klasse und DMARC. Wie bereits von CSC erwähnt, werden die meisten dieser Schutzmaßnahmen von Branchenführern empfohlen.

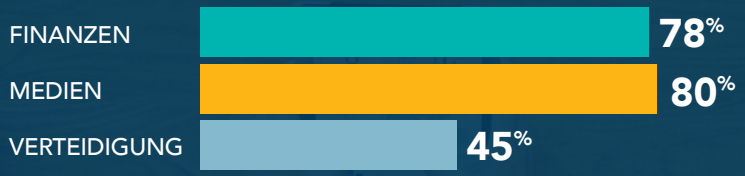
CORPORATE-REGISTRAR



REGISTRY-LOCK AKTIVIERT



ENTERPRISE- ODER INTERNES DNS

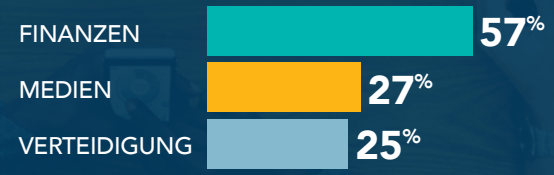


DNSSEC EINGESCHALTET

HTTPS EVERYWHERE

TYP DER DIGITALEN ZERTIFIKATE (EV ODER OV)

DMARC EINGESETZT



Außerdem sind nicht alle Sicherheitsmaßnahmen mit hohen Kosten verbunden – vor allem im Vergleich zu den Kosten einer einzigen Datenschutzverletzung – aber noch immer stellen wir fest, dass die grundlegenden Sicherheitselemente nicht das Maß an Akzeptanz im Verteidigungssektor erreicht haben, das man von der Zunahme der Cyberbedrohungen Jahr für Jahr erwarten würde. Beunruhigend ist vor allem die Tatsache, dass die einfachsten Sicherheitstechniken, die bei der allgemeinen Domain-Sicherheit und dem Benutzervertrauen ansetzen, anscheinend für Unternehmen am schwierigsten umzusetzen sind.

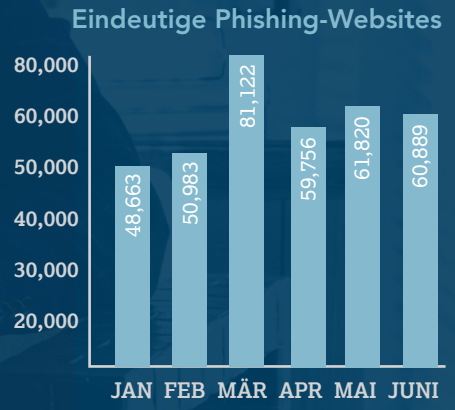
Phishing und E-Mail-Betrug

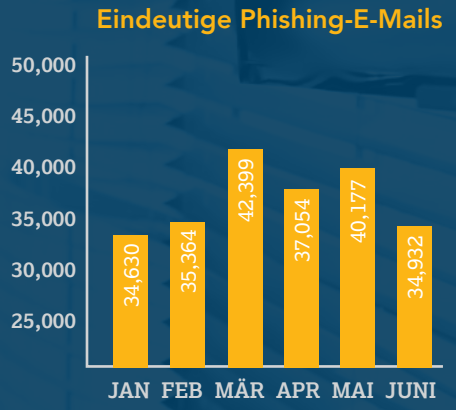
Deutlicher Anstieg der Phishing-Websites im Jahresverlauf

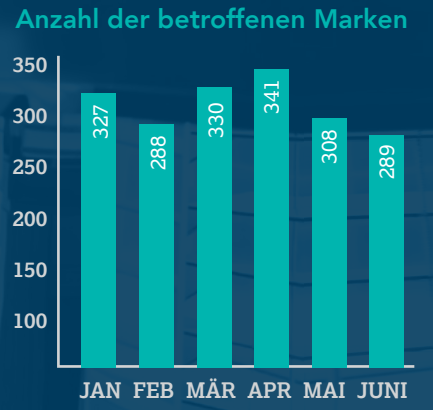
Zum zweiten Quartal 2019 verfügten mehr als 55 % der Phishing-Websites über digitale Zertifikate, wodurch der Hinweis für Benutzer, ob sie sich auf einer sicheren Website befinden oder nicht, ad absurdum geführt wird. Phishing-Sites sehen mit dem HTTPS seriöser aus. Damit täuschen sie Internetnutzer und wenden eine Internetsicherheitsfunktion gegen Nutzer. So wird es böswilligen Akteuren ermöglicht, persönliche Identitätsdaten und Anmeldeinformationen zu stehlen.

Phishing-Angriffe

Die Zahl der Phishing-Websites lag im zweiten Quartal 2019 bei 182.465, was einem leichten Anstieg gegenüber dem Vorquartal entspricht. Die Gesamtzahl der Angriffe in der ersten Jahreshälfte 2019 war jedoch mit 25 % deutlich höher als in der zweiten Jahreshälfte 2018.







Am stärksten betroffene Branchen

Software-as-a-Service (SAAS), Webmail, Online-Zahlungsdienstleistungen sowie Banken und Finanzinstitute bleiben im zweiten Quartal 2019 die drei am stärksten von Phishing betroffenen Branchen.

QUELLE: APWG Phishing Activity Trends Report, 2. Quartal 2019

Meist genutzte Top-Level-Domains in Phishing-Websites

Ältere Top-Level-Domains (TLD), d. h. TLDs, die vor langer Zeit etabliert wurden und von vielen Websites genutzt werden, hosten erwartungsgemäß die meisten Phishing-Angreifer. Allerdings hosten wiederverwendete länderspezifische TLDs sowie einige neue generische TLDs, die oft zu niedrigen Kosten angeboten werden, im Vergleich zu allen Domains der Welt beträchtliche Phishing-Inhalte.

Type of TLD:

Ältere gTLD | ccTLD | Neue gTLD

↑ / ↓ Rangfolgewechsel + / - Mengenänderung

.com +714 → Nr. 1 • 2,812 Domains	.net +33 War Nr. 3 ↑ Nr. 2 • 208 Domains	.br +64 War Nr. 8 ↑ Nr. 3 • 146 Domains	.org -9 → Nr. 4 • 145 Domains
.uk +16 → Nr. 5 • 137 Domains	.top Nr. 6 • 120 Domains	.info +36 → Nr. 7 • 119 Domains	.in +47 War Nr. 11 ↑ Nr. 8 • 105 Domains
.au Nr. 9 • 80 Domains	.xyz +26 War Nr. 17 ↑ Nr. 10 • 63 Domains	.icu Nr. 11 • 59 Domains	.cl Nr. 12 • 47 Domains
.ga -21 War Nr. 10 ↓ Nr. 13 • 47 Domains	.ml -35 War Nr. 9 ↓ Nr. 14 • 43 Domains	.cf -43 War Nr. 6 ↓ Nr. 15 • 41 Domains	.co Nr. 16 • 41 Domains
.ru -6 War Nr. 13 ↓ Nr. 17 • 38 Domains	.pl +9 War Nr. 19 ↑ Nr. 18 • 37 Domains	.id Nr. 19 • 36 Domains	.it -1 War Nr. 16 ↓ Nr. 20 • 36 Domains

QUELLE: APWG Phishing Activity Trends Report, 2. Quartal 2019

Jedes Unternehmen ist gefährdet

Beispiele aus den Nachrichten

AMERIKA

Schutz vor Manipulationen an der DNS-Infrastruktur

Die Behörde für Cybersicherheit und Infrastruktur des Heimatschutzministeriums der Vereinigten Staaten verfolgte eine Reihe von Manipulationsvorfällen und gab eine Notfallrichtlinie zur Überprüfung von DNS-Einträgen und zur Ergreifung erforderlicher Maßnahmen wie die Überprüfung von DNS-Einträgen und die Sicherung des Portalzugriffs an die Bundesbehörden heraus, um DNS-Hijacking zu verhindern.

cyber.dhs.gov/ed/19-01/

Warnhinweis zu veröffentlichten Berichten über Angriffe auf das Domain Name System

Die Internet Corporation for Assigned Names and Numbers (ICANN) gab eine Warnung an Organisationen heraus. Darin wurden diese aufgefordert, bewährte Verfahren und Maßnahmen wie DNSSEC und Registry-Locks umzusetzen, um ihre Systeme vor bösartigen Aktivitäten gegen das DNS zu schützen.

icann.org/news/announcement-2019-02-15-en

Tiefgründige Recherche über kürzliche weit verbreitete DNS-Hijacking-Angriffe

KrebsOnSecurity untersuchte die komplexen und weit verbreiteten DNS-Hijacking-Angriffe, um ihre Herkunft und ihr Ausmaß zu verstehen, und zeigte, dass mehrere Regierungen auf der ganzen Welt durch Datenschutzverletzungen bei wichtigen Internet-Infrastruktur-Providern betroffen waren.

krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

Geheimdienst untersucht Datenschutzverletzung bei IT-Dienstleister für die US-Regierung

Ein IT-Dienstleister für mehr als 20 US-Bundesbehörden war von einer Datenschutzverletzung durch Malware aus einem E-Mail-Anhang betroffen. Dies gefährdete E-Mail-Korrespondenz und Anmeldeinformationen, durch die Zugang zu Datenbanken der betroffenen Behörden erlangt werden könnte.

krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/

GROSSBRITANNIEN

Hinweis über andauernde DNS-Hijacking-Angriffe und Empfehlungen zum Schutz davor

The U.K. National Cyber Security Centre published an advisory that the large global DNS hijacking campaign continues to show activity affecting multiple regions and sectors, and provided mitigation advice around registrar, nameservers, and web application security.

ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice

BULGARIEN

Eine ganze Nation wurde gehackt

Bulgaria's national tax agency was breached, compromising the personal data and financial records of 5M citizens in a country with a population of 7M.

edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/

ECUADOR

Fast jeder Ecuadorianer ist Opfer einer Datenschutzverletzung

Detaillierte personenbezogene Daten von etwa 20 Millionen Einwohnern Ecuadors, einschließlich des Präsidenten, waren auf dem Server eines lokalen Dienstleisters ungeschützt, darunter waren Daten aus staatlichen Registern und anderen Organisationen.

engadget.com/2019/09/17/ecuador-data-breach-20-million-citizens/

AUSTRALIEN

ACSC stellt schützenden DNS-Service für staatliche und kritische Infrastrukturen bereit

Das australische Cyber Security Centre erprobt die Einführung eines DNS-Sicherheitsdienstes, der durch die örtliche Regierung und wichtige Infrastrukturen übernommen werden soll.

itnews.com.au/news/acsc-to-deploy-protective-dns-service-for-govt-critical-infrastructure-520138

Empfehlungen

DiD-Ansatz (Defense in Depth)

EINSATZ HOCHENTWICKELTER SICHERHEITSMERKMALE FÜR IHRE GESCHÄFTSKRITISCHEN DOMAINS

MultiLock, DNSSEC, HTTPS, DMARC und CAA Records

KONTROLLE DER NUTZERBERECHTIGUNGEN

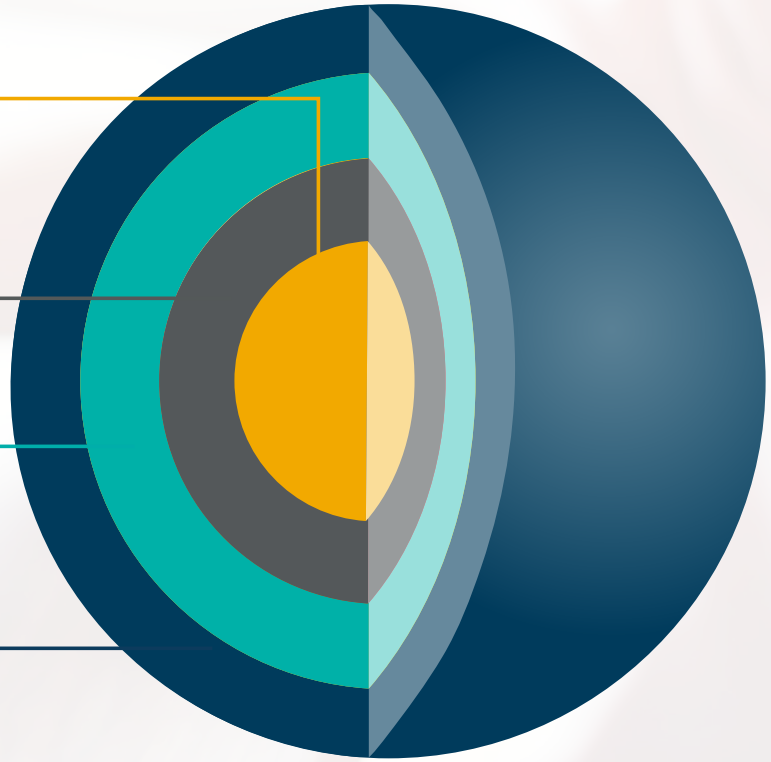
Sichtbarkeit höherer Berechtigungen und Benachrichtigungen

SICHERUNG DES PORTALZUGRIFFS

IP-Validierung, Zwei-Faktor-Authentifizierung und Federated ID

ENTERPRISE-CLASS-PROVIDER

Systeme, Mitarbeiter, Strategien und Prozesse



Mit der Aufdeckung von Sicherheitslücken, die in elementaren Internet-Assets wie Domainnamen, DNS und digitalen Zertifikaten vorhanden sind, unterstützt **CSC** Unternehmen, die bedeutende Investitionen in ihre Sicherheit durchführen. Durch Nutzung firmeneigener Sicherheitslösungen schützt CSC Unternehmen vor Cyber-Bedrohungen gegen ihre digitalen Assets und hilft ihnen, verheerende Umsatzeinbußen, Rufschädigung ihrer Marken oder erhebliche Geldbußen durch Richtlinien wie die DSGVO zu vermeinden. Neben den Internet-Assets schützt CSC Online-Marken, die über gefälschte Websites, Betrug und IP-Verletzungen missbraucht werden, und hilft durch das Angebot von Durchsetzungs- und Beratungsdiensten zum Schutz vieler der weltweit größten Marken bei deren Überwachung und Schadensminderung. Erfahren Sie mehr unter ***cscdigitalbrand.services/de***.

Referenzen

1.krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/
2.cscglobal.com/cscglobal/pdfs/DBS/Digital-Asset-Security-Checklist-EN.pdf
3.us-cert.gov/ncas/alerts/AA19-024A
4.krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-DNS-hijacking-attacks/
5.ncsc.gov.uk/news/ongoing-DNS-hijacking-and-mitigation-advice
6.cscglobal.com/cscglobal/pdfs/DBS/Cyber-Security-Report-June-2019-EN.pdf
7.beckershospitalreview.com/cybersecurity/hackers-steal-california-hospital-s-website-domain-email-addresses.html
8.eweek.com/security/dmarc-email-security-adoption-soars-as-us-government-deadline-hits