BERICHT ZUR CYBERSICHERHEIT

Juni 2019

Ken Linscott *Product Director, Domains and Security*

Quinn Taggart *Senior Domain Product Manager*

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.

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. Mit unseren firmeneigenen Tools helfen wir unseren Unternehmenskunden bei der Aufdeckung von Sicherheitslücken und Strategiemöglichkeiten 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 konzentrieren wir uns auf die Medienbranche. Angesichts des technologischen Wandels und der zunehmenden Nutzung von On-Demand-Inhalten durch die Kunden wurden traditionelle Medien durch digitale und mobile Formate ersetzt. Soziale Medien, Online-Streaming und Internet-Werbung sind Beispiele, die in den letzten 25 Jahren in dieser Zeit des Wandels entstanden sind. Viele Medienmarken sind heute online präsent und sammeln mehr Kundendaten als zuvor. Angesichts der Erfassung von Anmelde- und Zahlungsinformationen durch Unternehmen und der Möglichkeit von Cyber-Angriffen, die die Medienvertriebskanäle stören oder sogar entführen, ist es unerlässlich, dass Marken Maßnahmen ergreifen, um sich und ihre Kunden vor dem Risiko von Angriffen und Verstößen zu schützen.

Hier haben wir einige der größten Medienkonzerne weltweit, ihre Einheiten und Marken in einem Spektrum von Kanälen analysiert, darunter Werbung, Verlagswesen, TV und Rundfunk sowie einige reine Online-Marken, um herauszufinden, wie Maßnahmen zur Domain-Sicherheit in dieser Branche umgesetzt werden.

Domain-Sicherheit und Beobachtungstrends

120 Medienmarken als Basis

Der letzte CSC-Bericht konzentrierte sich auf die Finanz- und Versicherungssektoren. Mit dem Fokus auf Medien ist es diesmal interessant zu beobachten, wie jeder Sektor die verschiedenen Elemente der Domain-Sicherheit behandelt. Nicht alle Sicherheitsmaßnahmen sind teuer – vor allem im Vergleich zu den Kosten eines einzigen Verstoßes – aber wir sehen immer noch, dass grundlegende Sicherheitselemente nicht so beachtet werden, wie man das angesichts der Zunahme der Cyber-Bedrohungen von Jahr zu Jahr erwarten würde. Beunruhigend ist vor allem die Tatsache, dass die einfachsten Sicherheitstechniken, die bei der allgemeinen Domain-Sicherheit und dem Benutzervertrauen ansetzen, für Unternehmen am schwierigsten zu implementieren sind.

Registrar-Anbieter

78% CORPORATE-REGISTRAR

22% RETAIL-REGISTRAR

RISIKO

In der Vergangenheit waren Retail-Registrare häufige Ziele für Cyber-Angriffe. 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

78 % der Unternehmen in der Medienbranche nutzen Corporate-Registrare

Bei der Beurteilung der Domain-Sicherheit stehen grundsätzlich einige Schlüsselelemente auf dem Prüfstand – Locks, E-Mail, Domain Name System (DNS) und Secure Sockets Layer (SSLs). Natürlich können einige dieser Elemente mit der Verwaltung des gesamten Domain-Portfolios durch einen namhaften Corporate-Registrar einfacher umgesetzt werden als mit einem Retail-Registrar. Das scheint der Grund dafür zu sein, warum die meisten Unternehmen in der Medienbranche ihre Domain-Portfolios von Corporate-Registraren verwalten lassen.

Registry-Lock

43% REGISTRY-LOCK AKTIVIERT

37% REGISTRY-LOCK NICHT AKTIVIERT

20% *REGISTRY-LOCK NICHT VERFÜGBAR

RISIKO

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

BEOBACHTUNGEN

43 % haben Registry-Locks eingerichtet

Diese Sperren werden immer beliebter, weil sie unbefugte Änderungen am DNS verhindern, die eine Website offline bringen oder Benutzer zu bösartigen Inhalten umleiten könnten.

DNS-Provider

25% INTERNES DNS

55% CORPORATE- ODER ENTERPRISE-DNS

20% SONSTIGE (HOSTING- ODER RETAIL-DNS)

RISIKO

DNS-Provider, die gebündelte DNS-Dienste anbieten (Non-Enterprise-Level Provider), bergen potenzielle Sicherheitsbedrohungen wie DDoS-Angriffe sowie Ausfallzeiten und Einnahmeverluste.

SSL Always On

78% SSL ALWAYS ON IM EINSATZ

22% SSL ALWAYS ON NICHT IM EINSATZ

RISIKO

Die sichere Verschlüsselung aller Online-Transaktionen mit SSL-Zertifikaten minimiert das Sicherheitsrisiko der Entführung von Web-Sitzungen durch Cyber-Kriminelle, um Identitätsdiebstahl zu begehen oder Malware auf Benutzergeräten zu installieren. 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.

DNSSEC

3% DNSSEC EINGESCHALTET

97% DNSSEC AUSGESCHALTET

RISIKO

Wenn DNSSEC – eines der kostengünstigsten Sicherheitsprotokolle – nicht eingeführt ist, führt dies zu Schwachstellen im DNS bis dahin, dass ein Angreifer jeden Schritt des DNS-Lookup-Prozesses an sich reißen kann. Dadurch können Hacker die Kontrolle über eine Internet-Browsing-Sitzung übernehmen und Benutzer auf irreführende Websites umleiten.

BEOBACHTUNGEN

55 % der Unternehmen nutzen Enterprise-Level-DNS-Provider; 3 % nutzen DNSSEC

Die Präferenz für Corporate-Registrare scheint auch eine Vorliebe für Enterprise-Level-DNS-Provider nach sich zu ziehen, wenn man sieht, dass sie von mehr als der Hälfte der Unternehmen genutzt werden. Fast 25 % nutzen ihre eigene DNS-Architektur und 20 % nutzen einen Retail-Provider. Das DNS gehört gewiss zu den Bereichen, in denen Unternehmen nicht an Qualität und Zuverlässigkeit sparen sollten – das DNS ist der Motor einer Onlinepräsenz. 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.

SSL-Typ (EV, OV oder DV)

2% EV

74% OV

24% DV

RISIKO

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

BEOBACHTUNGEN

74 % nutzen OV-Zertifikate, doch 24 % verwenden DV-Zertifikate

Ähnlich wie beim DNS ist es nicht klug, bei digitalen Zertifikaten zu sparen. Wenn das DNS die Tür zu einem Haus ist, ist SSL 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 SSLs validiert werden. Die Domain-Validierung, die die niedrigste Validierungsstufe erfordert, wird von 24 % der Medienmarken verwendet, was bedeutet, dass ein Hacker, der Zugang zu internen E-Mails erhält, leicht SSLs auf firmeneigenen Domains für böswillige Zwecke validieren könnte. Dies geschah bei einem aktuellen Angriff über den Retail-Registrar GoDaddy®.

E-Mail-Authentifizierung

27% DMARC

79% SPF

6% DKIM

RISIKO

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

BEOBACHTUNGEN

27 % nutzen DMARC

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. Für Unternehmen, die mit Millionen von Nutzern kommunizieren, sind die niedrigen Akzeptanzraten überraschend.

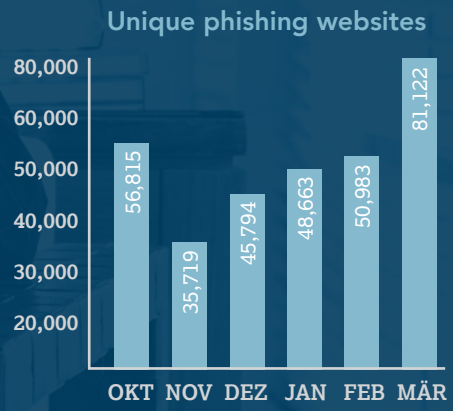
Phishing und E-Mail-Betrug

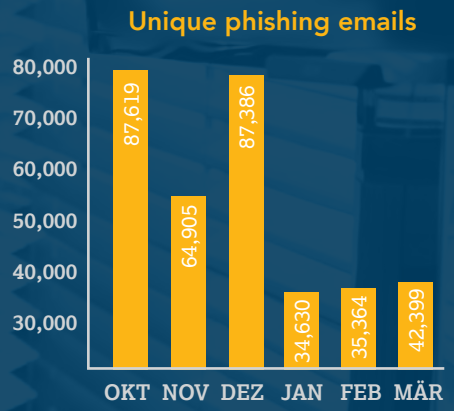
Deutlicher Anstieg der Phishing-Websites im Jahresverlauf

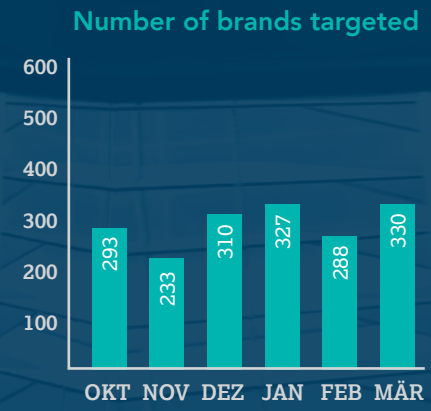
Im ersten Quartal 2019 hatten ca. 58 % der Phishing-Websites SSL-Zertifikate. Dies ist ein deutlicher Anstieg im Vergleich zu 46 % im Vorquartal und weniger als 5 % Ende 2016. Es gibt zwei mögliche Gründe für diesen Anstieg. Erstens können Angreifer Domain-validierte Zertifikate erstellen, die frei verfügbar sind. Zweitens verwenden generell mehr Websites SSLs und da die meisten Phishing-Angriffe auf legitimen, gehackten Websites gehostet werden, steigt damit auch die Zahl der Phishing-Websites mit SSLs. 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 ersten Quartal 2019 bei 180.768, was einem Anstieg von 31 % gegenüber dem Vorquartal entspricht.







Am stärksten betroffene Branchen

Erstmals ist die Kategorie Software as a Service (SaaS) und Webmail der Sektor, der am meisten von Phishing betroffen war, während Online-Zahlungsdienste und Finanzinstitute im ersten Quartal 2019 unter den drei am stärksten von Phishing betroffenen Branchen bleiben.

QUELLE: APWG Phishing Activity Trends Report, 1. Quartal 2019

Meist genutzte Top-Level-Domains (TLDs) in Phishing-Websites

Ältere TLDs, d. h. TLDs, die vor langer Zeit etabliert wurden und von vielen Websites genutzt werden, hosten erwartungsgemäß die meisten Phishing-Angreifer. Allerdings bergen länderbezogene TLDs, die umfunktioniert wurden, sowie einige neue generische TLDs, die oft zu niedrigen Kosten angeboten werden, in Relation zu allen Domains der Welt oft bemerkenswerte Mengen an Phishing.

TLD-Art:

Ältere gTLD | ccTLD | Neue gTLD

.com Nr. 1 • 2.098 Domains	.pw Nr. 2 • 374 Domains	.net Nr. 3 • 175 Domains	.org Nr. 4 • 154 Domains
.uk Nr. 5 • 121 Domains	.cf Nr. 6 • 84 Domains	.info Nr. 7 • 83 Domains	.br Nr. 8 • 82 Domains
.ml Nr. 9 • 78 Domains	.ga Nr. 10 • 68 Domains	.in Nr. 11 • 58 Domains	.us Nr. 12 • 45 Domains
.ru Nr. 13 • 44 Domains	.tk Nr. 14 • 40 Domains	.gq Nr. 15 • 37 Domains	.it Nr. 16 • 37 Domains
.xyz Nr. 17 • 37 Domains	.online Nr. 18 • 33 Domains	.pl Nr. 19 • 28 Domains	.ca Nr. 20 • 26 Domains

QUELLE: APWG Phishing Activity Trends Report, 4. Quartal 2018

Jedes Unternehmen ist gefährdet:

Beispiele aus den Nachrichten

AMERIKA

Große US-Zeitungen durch Ryuk Ransomware-Angriff lahmgelegt

Ransomware legte die Infrastruktur großer Zeitungen lahm und beeinträchtigte die Veröffentlichung und Verteilung der Printausgaben im ganzen Land.

csoonline.com/article/3330645/major-us-newspapers-crippled-by-ryuk-ransomware-attack.html

AMERIKA

Newsquest Websites durch Sicherheitsverletzung beeinträchtigt

Hunderte Titel von der Website einer Mediengruppe wurden mit Malware infiziert, die Mobil- und Webbrowser entführte, als Benutzer versuchten, auf lokale Nachrichten zuzugreifen. Sie wurden auf eine nicht angegliederte Website weitergeleitet, um Preise zu gewinnen.

uknip.co.uk/2019/02/newsquest-websites-compromised-by-security-breach/

FRANKREICH

Video-Sharing-Plattform Ziel von Credential Stuffing-Angriffen

Cyber-Kriminelle wählten eine Video-Sharing-Plattform als Ziel für Credential Stuffing- oder Brute-Force-Angriffe, indem sie Passwörter erraten oder erbeutete Passwörter aus Datenschutzverletzungen erneut nutzen, um Benutzerkonten zu entführen.

securityboulevard.com/2019/01/video-sharing-platform-targeted-by-credential-stuffing-attacks/

PHILIPPINEN

Große Hightech-Teams greifen Websites alternativer Medien auf den Philippinen an

Politisch motivierte Hacktivisten greifen philippinische Medien-Websites mit DDoS-Angriffen an, die den normalen Datenverkehr um das 40.000-fache übersteigen, und starten bis zu 40 Angriffe pro Woche.

news.abs-cbn.com/news/02/07/19/big-rich-tech-teams-attack-ph-alternative-media-websites

AMERIKA

Neue Mirai-Malware-Variante zielt auf Signs TVs und Präsentationssysteme ab

Forscher haben einen neuen Stamm des Mirai-Botnetzes entdeckt, der auf IoT-Geräte von Unternehmen abzielt, um möglicherweise massive DDoS-Angriffe zu starten, ähnlich dem Mirai-Angriff von 2016 auf einen DNS-Anbieter, der wichtige Websites und Internetdienste in Nordamerika und Europa unterbrach.

zdnet.com/article/new-mirai-malware-variant-targets-signage-tvs-and-presentation-systems/

Empfehlungen

1. DOMAINS AUTOMATISCH VERLÄNGERN

Wenn die bei Retail-Registraren hinterlegte Kreditkarte abläuft oder gekündigt wird, wird die automatische Verlängerung hinfällig und Domains gehen offline, oder schlimmer noch, werden gelöscht. Die Zusammenarbeit mit einem Corporate-Registrar stellt sicher, dass Domains automatisch verlängert werden, es sei denn, ein Unternehmen zeigt ausdrücklich an, dass bestimmte Domains nicht verlängert werden. Dies gibt die Gewissheit, dass Domains nicht wegfallen.

cscdigitalbrand.services/blog/an-abandoned-domain-name-could-hurt-you/

2. WICHTIGE DOMAINS SPERREN

Die Support-Struktur ist ein weiterer Grund, warum Sie mit einem Corporate-Registrar zusammenarbeiten sollten. Sie gewährleistet die Balance aus Technologie und Experten, die sich in der Branche auskennen. Um wichtige Domains sperren zu können, müssen Unternehmen wissen, welche von ihnen wichtig sind – und das ist möglicherweise nicht leicht zu erkennen. CSC Security Center℠ bietet uns die Technologie für die Identifizierung wichtiger Domains. Dabei betrachten wir mehr als nur den Datenverkehr und analysieren mehrere Vektoren, um die Layer-Sicherheit zu gewährleisten.

cscglobal.com/service/csc/press-csc-alerts-companies-to-increased-dns-hijacking/

3. MASSNAHMEN ZUR DOMAIN-SICHERHEIT EINFÜHREN

Ohne ein gutes Fundament bröckelt die Festung. Sobald ein Domain-Namen-Registrar für Unternehmen an Bord ist, sollten das Domain-Portfolio und die vorhandenen Schutzmaßnahmen sorgfältig erfasst werden. Die Sicherheitslandschaft entwickelt sich ständig weiter, so dass ein engagierter, vertrauenswürdiger Partner für die Entwicklung der Strategie unerlässlich ist. Sicherheit ist keine einmalige Sache, sondern muss periodisch weiterentwickelt werden, da Cyber-Kriminelle ebenfalls neue Angriffstechniken entwickeln.

cscdigitalbrand.services/blog/dns-the-neglected-building-block-part-5/

4. ANDERE INTERESSENVERTRETER EINBEZIEHEN

Domain-Sicherheit und Portfoliomanagement sind keine Einmannaufgaben, sondern betreffen Interessenvertreter aus den Bereichen Marketing, Recht, Markenmanagement und IT. Wenn es um die Verwaltung des Domainportfolios geht, ist der Beitrag aller wertvoll. Wir empfehlen Unternehmen, ein Domain-Gremium zu gründen, da Sicherheit die Aufgabe aller ist.

5. AUFSICHTSGREMIUM MIT DEN DNS-RISIKEN VERTRAUT MACHEN

Angesichts globaler Angriffe und Rechtsverletzungen im großen Maßstab hat die Cybersicherheit für den Firmenvorstand neben der Einhaltung gesetzlicher Vorschriften oberste Priorität. Das DNS trägt zu vier der zehn größten im „Business Continuity Institute Horizon Scan Report“ identifizierten Risiken bei.

cscdigitalbrand.services/blog/dns-the-neglected-building-block-part-6/

CSC hilft Unternehmen, online zu wachsen. Wir helfen unseren Kunden, ihre wertvollen Marken zu verwalten, voranzubringen und vor den Bedrohungen der Online-Welt zu schützen. Führende Unternehmen weltweit wählen uns als zuverlässigen Partner, davon mehr als 65 % der Interbrand® 100 Best Global Brands. Durch die Nutzung modernster Technologien sorgt Digital Brand Services für außergewöhnliche Ergebnisse über unsere einzigartige Kundenbetreuungsstruktur. Mit unserem fachkundigen Team haben Sie jeden Tag einen persönlichen Ansprechpartner, um sicherzustellen, dass Ihre Marke die Stärke besitzt, um im 21. Jahrhundert zu bestehen. Wir helfen bei der Konsolidierung und Sicherung, Überwachung und Durchsetzung und anschließend bei der Optimierung und Förderung Ihrer Marke, damit Sie den maximalen Nutzen aus Ihrer digitalen Präsenz ziehen, Ihr digitales geistiges Eigentum schützen und Kosten reduzieren können.

cscdigitalbrand.services