Auswirkungen der Zusammenarbeit mit einem Enterprise-Class-Domain-Registrar auf die allgemeinen Sicherheitsratings

SecurityScorecard.com
info@securityscorecard.com

214 West 29th St., 5th Floor
New York, NY 10001
1.800.682.1707

SecurityScorecard CSC

Kurzfassung

Die meisten Cyberangriffe, einschließlich Ransomware-Angriffe und E-Mail-Beeinträchtigungen (Business Email Compromise, BEC), beginnen mit Phishing, da das Phishing einen Ransomware-Angriff in der Anfangsphase ins Rollen bringt. Auch wenn Ransomware mittlerweile jedes Jahr milliardenschwere Verluste[1] verursacht, bieten die meisten Maßnahmen gegen Ransomware keinen ausreichenden Schutz vor Phishing-Risiken.

Untersuchungen haben ergeben, dass Phishing-Angriffe am häufigsten durch folgende Angriffe erfolgen: Arglistige Domainregistrierungen, zum Verwechseln ähnliche Domains, kompromittierte Domains, Domain Hijacking oder Email-header-Spoofing. Die Zusammenarbeit mit einem Enterprise-Class-Domain-Registrar kann helfen, diese Risiken zu reduzieren.

Die Auswahl des Domain-Registrars ist ausschlaggebend für den allgemeinen Sicherheitsstatus eines Unternehmens.

Untersuchungen von SecurityScorecard verdeutlichen, dass das Cybersicherheitsrating eines Unternehmens stark mit seiner Wahl des Domain-Registrars korreliert. Unternehmen, die bei der Domain-Verwaltung auf Enterprise-Class-Registrare (ECR) statt Registrare für Verbraucher (Consumer-Grade-Registrare, CGR) setzen, weisen im Schnitt ein um mindestens eine halbe oder ganze Stufe höheres Sicherheitsrating auf.

Merkmale eines Enterprise-Class-Registrars

Es gibt zwei Arten von Domain-Registraren: Consumer-Grade-Registrare (CGR) für Verbraucher und Enterprise-Class-Registrare (ECR) für Unternehmen. Registrare für Verbraucher (CGR) spezialisieren sich auf Domain-Services, Websites und E-Mail-Dienste für private Zwecke oder kleine Unternehmen. Es handelt sich dabei zwar nicht zwangsläufig um böswillige Akteure, aber sie bieten oft weder Domain-Sicherheitsfunktionen und -kontrollen noch einen fokussierten Schutz von geistigem Eigentum.

Enterprise-Class-Registrare (ECG) konzentrieren sich hingegen darauf, mit erweiterten Services und Tools für Cybersicherheit zu sorgen und geistiges Eigentum zu schützen, wobei ihr Fokus auf der Domain-Sicherheit liegt. Außerdem bieten sie keine Domain-Services über Retail-Websites oder Pay-per-Click, Domain-Spinning und Domain-Auktionsdienste, die die Rechtsverletzung von geistigem Eigentum und Markenzeichen erleichtern können.

Auf folgende wichtige Merkmale eines Enterprise-Class-Registrars sollten Sie achten:

- **Unternehmensweite Skalierung und Expertise** mit einem Domain-, DNS- und Zertifikatsverwaltungsangebot, das sich ausschließlich an Unternehmen richtet
- **Erweiterte Dienste** wie Domain-Registry-Lock, DMARC, DNSSEC, CAA-Einträge und DNS-Hosting-Redundanz
- **Bereitstellung von globalem und lokalem Support rund um die Uhr (24 x 7 x 365)** mit Domain-Registrierung weltweit
- **Implementierung von KYC-Methoden (Know Your Customer)** zur Gewinnung und Validierung von Kundeninteraktionen
- **Möglichkeiten zur Domain-, Marken- und Betrugsüberwachung** sowie für Durchsetzung und Takedowns

Beurteilung der Domain-Sicherheit von Forbes Global 2000-Unternehmen

Der CSC-Bericht zur Domain-Sicherheit 2021 verdeutlichte, dass Web-Domains weiterhin mangelhaft geschützt und dadurch gefährdet sind, obwohl immer mehr Global 2000-Unternehmen Maßnahmen zur Modernisierung ihres Geschäfts und ihres operativen Betriebs umsetzen. 2021 haben Unternehmen vermehrt Ransomware-Angriffe, E-Mail-Beeinträchtigungen (Business Email Compromise, BEC), Phishing-Angriffe, Angriffe auf die Lieferkette sowie Online-Marken- und Markenzeichenmissbrauch verzeichnet. Trotz der zunehmenden Cyberrisiken bleibt das Ausmaß der von Forbes Global 2000-Unternehmen ergriffenen Maßnahmen unverändert.

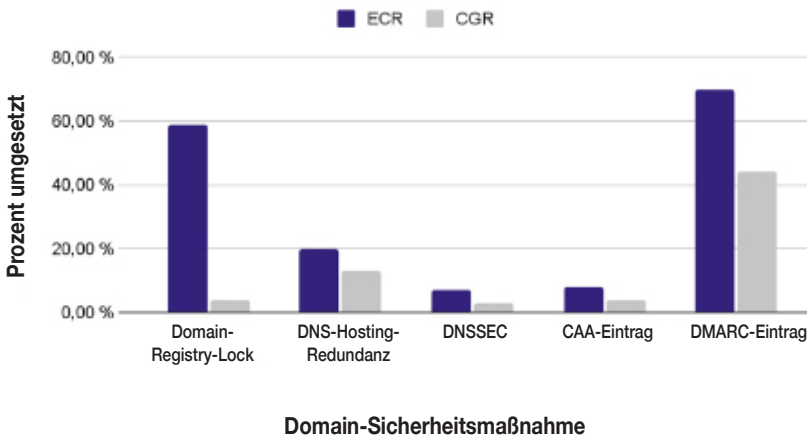
Die zentralen Ergebnisse des Berichts zeigen, mit welchen Domain-Sicherheitsrisiken Forbes Global 2000-Unternehmen konfrontiert sind:

- **70 % der Homoglyphen-Domains** (Fuzzy Matches) – eine Taktik, die häufig beim Phishing und Markenmissbrauch eingesetzt wird – sind im Besitz von Dritten und bei Registraren für Verbraucher (CGR) registriert
- **Von diesen Domain-Registrierungen wurden 60 %** in den letzten zwei Jahren vorgenommen, was zeigt, dass sich diese Angriffsmethode schnell verbreitet
- **81 % der Unternehmen sind einem größeren Risiko** für das Domain- und DNS-Hijacking ausgesetzt, weil sie grundlegende Maßnahmen für die Domain-Sicherheit wie Registry-Lock für Domains NICHT eingeführt haben
- **57 % der Unternehmen vertrauen Domain-Registraren für Verbraucher,** die nur begrenzten Schutz vor Domain- und DNS-Hijacking, Distributed Denial of Service (DDoS), Man-in-the-Middle-Angriffen (MitM) oder DNS-Cache-Poisoning bieten
- **Nur 50 % setzen DMARC ein**

Zur Verdeutlichung dieser Ergebnisse wurde verglichen, welche Domain-Sicherheitsmaßnahmen die ECR-Gruppe im Vergleich zur CGR-Gruppe umsetzte.

Umsetzung von Maßnahmen zur Gewährleistung der Domain-Sicherheit in Forbes 2000-Unternehmen

ECR-Gruppe und CGR-Gruppe im Vergleich



Mit einem Enterprise-Class-Registrar wird ein um eine halbe oder ganze Stufe höheres SecurityScorecard-Gesamtrating erzielt

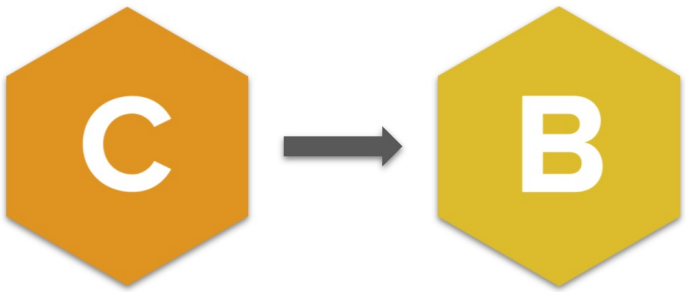
Sicherheitsratings verdeutlichen, dass die Domain-Sicherheit als Priorität behandelt werden muss

SecurityScorecard analysierte die Sicherheitsratings der 50.000 am meisten verfolgten Unternehmen auf seiner Plattform. Die Ergebnisse dieser Analyse unterstreichen, dass die Gewährleistung der Domain- und DNS-Sicherheit mit einem vertrauenswürdigen Enterprise-Class-Domain-Registrar als Priorität behandelt werden muss. Unternehmen, die für die Domain-Verwaltung mit Enterprise-Class-Registraren zusammenarbeiteten, erzielten ein im Schnitt um mindestens eine halbe Stufe höheres Rating als Unternehmen, die einen Registrar für Verbraucher nutzten. In unserer Analyse war dies ausschlaggebend für den Unterschied zwischen einem Gesamtwert von „C“ und „B“.

Die Studie von SecurityScorecard untermauert, dass die Auswahl des Domain-Registrars eine kritische Entscheidung darstellt. Sie erhält zwar oft nicht die nötige Aufmerksamkeit, ist aber entscheidend für den allgemeinen Sicherheitsstatus eines Unternehmens.

Quantifizierung der Auswirkungen von Enterprise-Class-Domain-Registraren auf den allgemeinen Sicherheitsstatus eines Unternehmens

Von den 50.000 von SecurityScorecard analysierten Unternehmen wiesen jene, die einen Registrar für Verbraucher verwendeten, ein durchschnittliches SecurityScorecard-Rating von 76,92 auf. Unternehmen, die mit einem Enterprise-Class-Registrar zusammenarbeiteten, erreichten hingegen ein durchschnittliches SecurityScorecard-Rating von 81,73 und schnitten daher um etwa 5 Punkte besser ab. Das heißt, dass die ECR-Gruppe eine ganze Stufe höher eingestuft worden wäre als die CGR-Gruppe und statt des Ratings „C“ das Rating „B“ erhalten hätte.



Risikofaktor DNS-Zustand verzeichnete den schlechtesten Wert, obwohl er ein bedeutender Bewertungsfaktor ist

Die SecurityScorecard-Plattform misst verschiedene DNS-Konfigurationseinstellungen, hierzu gehört auch, wie die OpenResolver-Konfigurationen aussehen und ob empfohlene Konfigurationen, einschließlich DNSSEC, SPF, DKIM und DMARC, vorhanden sind.

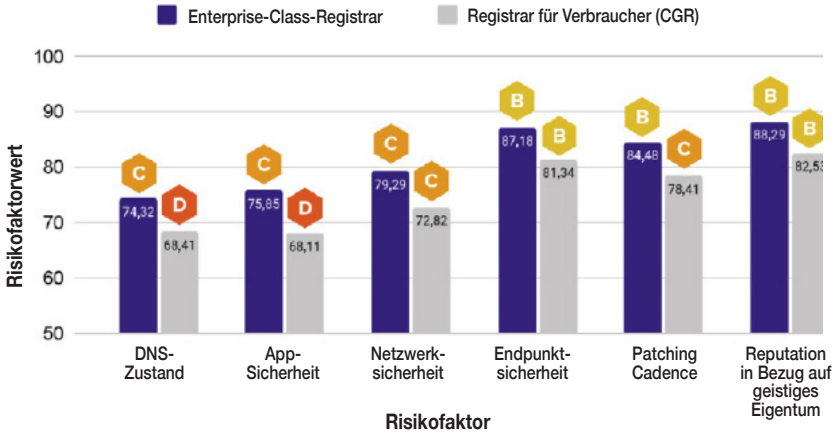
Obwohl der DNS-Zustand einen bedeutenden Bewertungsfaktor im Bewertungsalgorithmus von SecurityScorecard darstellt, erzielten die analysierten Unternehmen in dieser Kategorie im Schnitt nur einen Wert von 71,36 (Rating C). Der DNS-Zustand war damit der Risikofaktor mit dem schlechtesten Ergebnis unter den analysierten Faktoren. Die durchschnittliche SecurityScorecard-Bewertung des DNS-Zustands belief sich bei der ECR-Gruppe auf 74,32, bei der CGR-Gruppe hingegen auf 68,41. Im Schnitt erzielte die ECR-Gruppe also ein um fast 6 Punkte besseres Ergebnis. Das heißt, dass die ECR-Gruppe um einen ganzen Grad besser abschneiden würde und die Bewertung „C“ erhalten würde, während die CGR-Gruppe mit der Note „D“ bewertet werden würde.

DNS-Zustand wirkt sich auf andere wichtige Risikofaktoren aus

Unsere Studie zeigte auch, dass die ECR-Gruppe bei anderen Faktoren wie der Anwendungssicherheit, der Netzwerksicherheit, der Endpunktsicherheit, der Patching Cadence sowie der Reputation in Bezug auf geistiges Eigentum um mindestens 5 Punkte besser abschnitt als die CGR-Gruppe und damit bei mehreren Risikofaktoren um eine ganze Stufe besser bewertet wurde.

Durchschnittliche Risikofaktorwerte

ECR und CGR im Vergleich



Diese Analyse untermauert, dass proaktive Domain-Sicherheitsmaßnahmen den DNS-Zustand und andere Faktoren verbessern und zu einem insgesamt höheren Sicherheitsrating führen.

CSC und SecurityScorecard: Eine auf den Grundlagen der Cyberrisikoprävention aufbauende Allianz

SecurityScorecard, der weltweit führende Anbieter von Sicherheitsratings, und CSC gingen eine strategische Allianz ein, um Kunden mehr Informationen über die Domain-Sicherheit zu liefern. Mit sinnvollen, proaktiven Schutzmaßnahmen gegen Domain- und DNS-Angriffe können Unternehmen und Cyberversicherungen potenzielle Cyberrisiken, Marken-Phishing-Versuche und Sicherheitsverletzungen besser verhindern.

Obwohl die Gewährleistung der Domain-Sicherheit einen Defense-in-Depth-Ansatz mit erweiterten Sicherheitsmaßnahmen und operativen Protokollen erfordert, ist auch die Auswahl des Registrars von großer Bedeutung. Dies verdeutlichen die Auswirkungen der Lieferketten bei Vorfällen wie dem Angriff auf SolarWinds. Klassische DNS-Sicherheitsansätze richten den Fokus stärker auf DNS-Resilienz, Auflösung und relevante Maßnahmen zum Schutz vor DDoS-Attacken. Eine wichtige Gefahr für den DNS-Zustand, die heute übersehen wird, ist die Manipulation von Domains und DNS für böswillige Angriffe auf Unternehmen und ihre Kunden.

Die drei Säulen der Domain-Sicherheit

CSC konzentriert sich bei der Domain-Sicherheit auf drei Punkte:

1. Es wird sichergestellt, dass legitime Domains und das zugehörige DNS beim ausgewählten Domain-Registrar oder DNS-Hosting-Anbieter nicht kompromittiert werden (durch DNS-Hijacking, Domain-Hijacking, Subdomain-Hijacking)
2. Domains werden überwacht und bösartige Domains von Dritten deaktiviert
3. Es wird sichergestellt, dass E-Mail-Authentifizierung zum Schutz vor E-Mail-Spoofing eingesetzt wird

Best Practices von CSC für die Domain-Sicherheit

Sämtliche Unternehmen in allen Branchen – und insbesondere diejenigen, die aufgrund von COVID-19 jetzt noch stärker gefährdet sind – sollten einen mehrschichtigen Defense-in-Depth-Ansatz für die Domain-Sicherheit verfolgen, der mit der Zusammenarbeit mit einem Enterprise-Class-Domain-Registrar beginnt.

CSC empfiehlt vier Schlüsselstrategien:

1. Anwendung eines Defense-in-Depth-Ansatzes für die Domain-Verwaltung
2. Überprüfung der Geschäftsverfahren des Domain-Registrars dahingehend, dass sie nicht zu Betrug und Markenmissbrauch beitragen
3. Ständige Überwachung des Domain- und DNS-Raums und der wichtigsten digitalen Kanäle wie Marktplätze, Apps, soziale Medien und E-Mail auf Markenmissbrauch, Rechtsverletzungen, Phishing und Betrug
4. Nutzung der Durchsetzung im globalen Maßstab, z. B. durch Takedowns und moderne Techniken bei der Internet-Sperrung

Fazit

Da Ransomware-Angriffe und Sicherheitsbedrohungen infolge der verstärkten Arbeit aus dem Homeoffice weiter zunehmen, ist die Auswahl eines seriösen Domain-Registrars ein wichtiger Faktor für die Reduzierung von Cybersicherheitsrisiken und den Online-Markenschutz. Die Zusammenarbeit mit einem Enterprise-Class-Registrar, der Sicherheit, Daten-Governance und globalen Support als Priorität behandelt, ist entscheidend für den Schutz der Marke und der Kunden eines Unternehmens.

SecurityScorecard und CSC haben sich zusammengetan, um auf Sicherheitsrisiken durch mangelnde Domain-Schutzmaßnahmen aufmerksam zu machen und diese zu reduzieren. Domain-Sicherheit beginnt mit der Auswahl des richtigen Domain-Registrars.

Schlusswort

Melden Sie sich hier für eine kostenlose SecurityScorecard Enterprise-Lizenz an, mit der Sie Ihr Unternehmen und bis zu fünf Anbieter überwachen können.

Registrieren Sie sich hier für eine kostenlose Domain-Sicherheitsprüfung von CSC.

[1] https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=75f066bf71c6

Ressourcen

Für eine vollständige Liste der Best Practices siehe:

CSC-Bericht zur Domain-Sicherheit 2021

CSC-Blog

Fünf Schritte zu einem modernen Cyber-Risikomanagement-Team

Die perfekte Bewertung: Wie Sie von Ihrem Vorstand die Bestnote für die Cybersicherheit erhalten

SecurityScorecard-Blog

Informationen über CSC

CSC ist vertrauenswürdiger Anbieter erster Wahl für die Forbes Global 2000-Unternehmen und die 100 Best Global Brands® in den Bereichen Domainverwaltung, Domain Name System (DNS), Verwaltung digitaler Zertifikate sowie digitaler Marken-, Betrugs- und Phishing-Schutz. Wir schützen Online-Assets von Unternehmen vor Cyberbedrohungen, indem wir unsere eigenen Sicherheitslösungen einsetzen. So helfen wir den Unternehmen, verheerende Einnahmeverluste, Reputationsschäden für ihre Marke oder hohe Geldstrafen zu vermeiden. Darüber hinaus bieten wir mit einer Kombination aus Online-Markenüberwachung und Durchsetzung einen ganzheitlichen Ansatz für den Schutz digitaler Assets. Mehr Informationen über unsere Domain-Verwaltung, Sicherheit, Markenschutz und Anti-Fraud-Dienstleistungen finden Sie unter cscdbs.com.

Informationen über SecurityScorecard

SecurityScorecard hilft Unternehmen, sich und Dritte durch eine kontinuierliche, nicht störende Überwachung zu schützen. Beim Sicherheitsansatz von SecurityScorecard liegt der Fokus darauf, Schwachstellen aus externer Perspektive so zu identifizieren, wie dies ein Hacker tun würde. Die firmeneigene SaaS-Plattform von SecurityScorecard bietet eine beispiellose Breite und Tiefe von kritischen Datenpunkten, einschließlich einer breiten Auswahl von Risikokategorien wie Anwendungssicherheit, Malware, Patching Cadence, Netzwerksicherheit, Hacker-Gespräche, Social Engineering und nicht autorisierte Weitergabe von Informationen.

Wenn Sie eine E-Mail mit der aktuellen Bewertung Ihres Unternehmens erhalten möchten, besuchen Sie bitte instant.securityscorecard.com.

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard HQ
214 West 29th St., 5th Floor
New York, NY 10001