



EMPFEHLUNGEN ZUR DOMAINSICHERHEIT: SCHÜTZEN SIE IHRE DOMAINS UND MARKEN VOR ONLINE-MISSBRAUCH UND BETRUG

Anwendung eines Defense-in-Depth-Ansatzes für die Domain-Verwaltung und-Sicherheit

Eliminierung des Risikos durch Drittparteien durch Bewertung von Sicherheit, Technologie und Prozessen Ihres Domain-Registrars zusammen mit Ihrem Anbieter für die Verwaltung des Domain-Name-Systems (DNS)

Schutz wichtiger Domains, des DNS und digitaler Zertifikate durch folgende Maßnahmen:

Implementierung der Zwei-Faktor-Authentifizierung

Kontrolle der Berechtigungen – sowohl der normalen als auch der erweiterten – und Überwachung aller Änderungen sowie Hinzufügen einer Richtlinie für autorisierte Kontaktpersonen

Überwachung von DNS-Aktivitäten und Schutz vor DDoS-Attacken (Distributed Denial of Service)

Verwendung von Sicherheitsmaßnahmen wie Domain-Registry-Locks, DNS-Sicherheitserweiterungen (DNSSEC), Domain-based Message Authentication Reporting and Conformance (DMARC), Certificate-Authority-Autorisierungs-Einträge (CAA-Einträge) und DNS-Hosting-Redundanz

Ständige Überwachung des Domain-Raums und der wichtigsten digitalen Kanäle

wie Marktplätze, Apps, soziale Medien und E-Mail auf Markenmissbrauch, Rechtsverletzungen, Phishing und Betrug

Identifizierung von Domain- und DNS-Spoofing-Taktiken wie Homoglyphen (Fuzzy Matches und internationale Domains), Cousin-Domains, Keyword Match und Homophone

Registrierung von Domains, die hochwertige Ziele im Zusammenhang mit Ihren Marken sein könnten (z. B. Homoglyphen oder länderspezifische Domains), um das Risiko zu verringern, dass Kriminelle sie nutzen

Identifizierung von Markenzeichen- und Urheberrechtsmissbrauch in Webinhalten, auf Online-Marktplätzen, in sozialen Medien und Apps

Fordern Sie eine [kostenlose Beratung](#) an und einer unserer Experten wird sich mit Ihnen in Verbindung setzen.

 cscdbs.com/de



Nutzung der Durchsetzung im globalen Maßstab, z. B. durch Takedowns und moderne Techniken bei der Internet-Sperrung

Nutzung der Phishing-Überwachung und eines Netzwerks von Browsern, Partnern, Internetdienstleistern und SIEM-Systemen (Security Information and Event Management) zur Betrugsabwehr

Nutzung einer Reihe von technischen und rechtlichen Ansätzen für die Durchsetzung, wobei von Fall zu Fall der am besten geeignete Ansatz zu wählen ist

Nutzung einer Kombination von Maßnahmen zur Durchsetzung bei Urheberrechtsverletzungen und Betrug:

Vorrangigen Durchsetzungsmaßnahmen die Streichung von Marktplätzen, die Sperrung von Seiten in sozialen Medien, die Streichung von mobilen Apps, Unterlassungsaufforderungen, die Entfernung betrügerischer Inhalte und die vollständige Eindämmung von Bedrohungsvektoren

Zweitrangige Durchsetzungsmaßnahmen die Sperrung von Domains auf Registrarebene, die Sperrung von Domains mit ungültigen WHOIS-Einträgen und Warnungen vor Betrug

Drittrangige Durchsetzungsmaßnahmen Verfahren gemäß der Uniform Domain-Name Dispute-Resolution Policy (UDRP) und der Uniform Rapid Suspension (URS), Domainerwerb, eingehende Untersuchungen und Testkäufe



Die folgenden Probleme treten häufig bei Domain-Registralen für Verbraucher auf:

Überprüfung der Geschäftsverfahren des Domain-Registrars dahingehend, dass sie nicht zu Betrug und Markenmissbrauch beitragen

Betrieb von Domain-Märkten, in denen Domains, die Markenzeichen enthalten, erfasst, versteigert und an den Meistbietenden verkauft werden

Domain-Spinning und Befürwortung der Registrierung von Domains, die Markenzeichen enthalten

Monetarisierung von Domains, die Markenzeichen enthalten, über Pay-per-Click-Websites

Häufig auftretende Verstöße, die zu DNS-Angriffen, Phishing und Business Email Compromise (BEC) führen