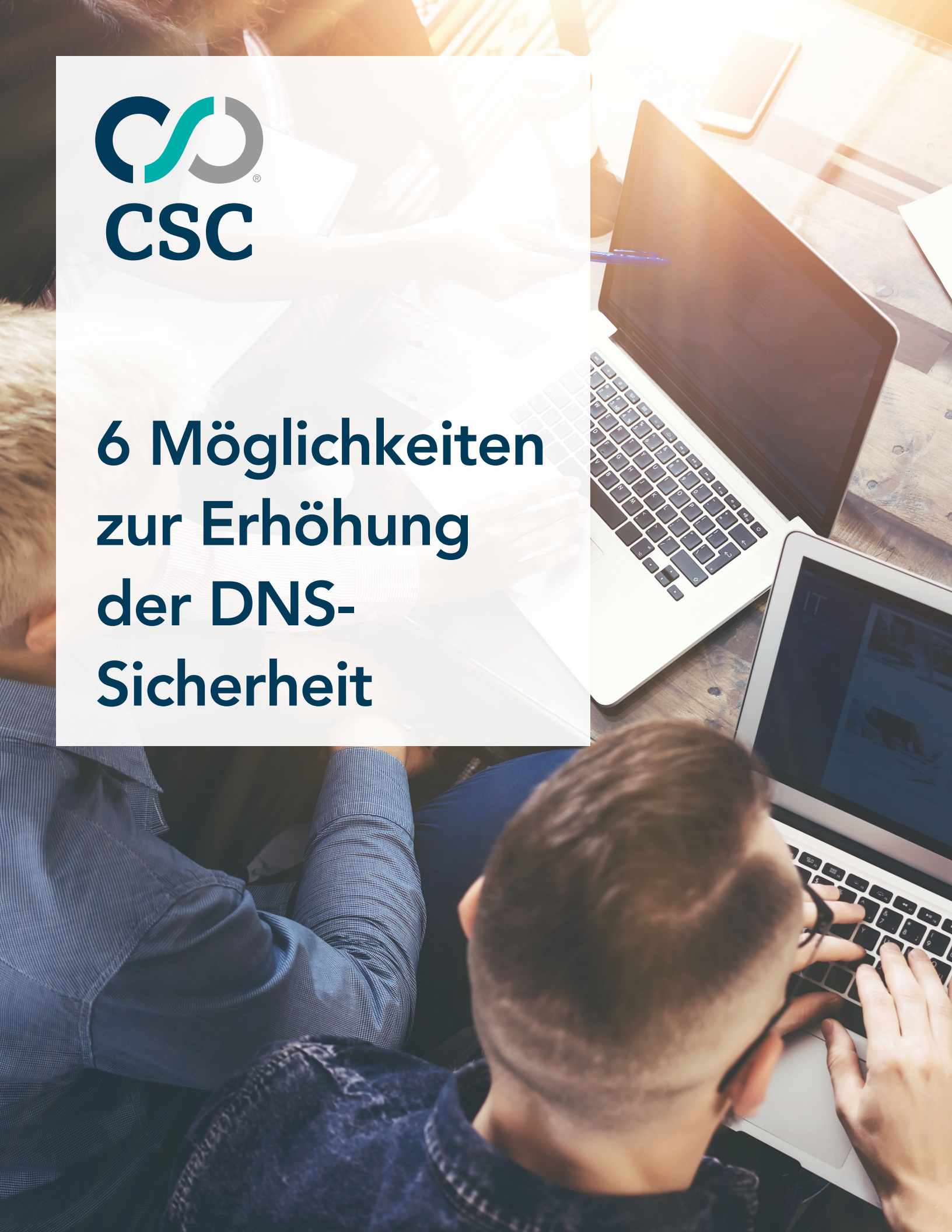

CSC

6 Möglichkeiten zur Erhöhung der DNS-Sicherheit

6 Möglichkeiten zur Erhöhung der DNS-Sicherheit

Das Domain Name System (DNS) gewann in den ersten, unschuldigen Tagen des Internets an Bedeutung. Zu dieser Zeit arbeiteten die ersten Internetnutzer eher für Regierungs- oder Bildungseinrichtungen, bei denen Vertrauen vorherrschte und man sich keine Gedanken um die Sicherheit machte. Da die Online-Community klein war und das Internet nur wenig genutzt wurde, wurde die Wichtigkeit des DNS weitgehend nicht verstanden und es blieb daher ungeschützt.

Spulen wir zur heutigen Zeit vor, können wir die daraus resultierenden Probleme sehen. Jüngste Cyber-Angriffe verdeutlichen spezielle Techniken, mit denen böswillige Akteure den rechtmäßigen Web-Traffic eines Unternehmens abfangen und manipulieren, Daten sammeln, z. B. Anmeldeinformationen oder E-Mail-Adressen, und andere bösartige Aktivitäten wie Phishing durchführen. In einigen Fällen wurden kostenlose digitale Zertifikate, die eine geringe Validierung erfordern, verwendet, um in betrügerischer Absicht Glaubwürdigkeit vorzutäuschen, was das Problem für Marken und Kunden verschärft. Verbraucher mögen es überhaupt nicht, dass ihre personenbezogenen Daten Kriminellen zugänglich sind und von diesen gestohlen werden, wodurch Datenschutzverletzungen den Ruf und den Nettoprofit von Unternehmen auf der ganzen Welt beeinträchtigen. Außerdem gibt es noch das Problem der DDoSAngriffen, die sich explosionsartig ausbreitend und oft auf das DNS abzielen, um das Online-Geschäft lahmzulegen.

Für Unternehmen bedeutet dies ganz einfach – wenn das DNS nicht funktioniert, gibt es keine Website oder Internetpräsenz. Fällt das DNS aus, erreichen Kunden, die versuchen, eine Website zu besuchen, ihr Ziel einfach nicht. Ebenso wenig können Mitarbeiter Firmen-E-Mails versenden oder empfangen. Ist ein Unternehmen für Telefonate auf VoIP angewiesen, ist der Zugang unterbrochen. Fällt das DNS aus, müssen Unternehmen auf die Nutzung von Festnetzverbindungen und Mobilgeräten zurückgreifen, um ihre Kunden zu erreichen. Schließlich können externe Mitarbeiter nicht mehr über ein virtuelles privates Netzwerk auf Systeme zugreifen, so dass ein Unternehmen zwangsläufig zu wenig Personal hat, und zwar genau dann, wenn alle Hände benötigt werden.

Im Wissen um die Wichtigkeit einer robusten und sicheren DNS-Infrastruktur in Kombination mit der Verwaltung von Domainnamen und digitalen Zertifikaten entschied sich CSC für eine Partnerschaft mit Neustar® – seit über 20 Jahren Betreiber der größten und vertrauenswürdigsten DNS-Netzwerke – und empfiehlt sechs Möglichkeiten zur Erhöhung der DNS-Sicherheit.*

**Dieses Dokument basiert auf der Publikation „Five Ways Neustar Strengthens DNS Security" von Neustar.*

1 Abwehr von DDoS-Angriffen durch mehrschichtigen Schutz

Das Ausmaß groß angelegter DDoS-Angriffe hat sich explosionsartig erhöht. Solche Angriffe überschreiten heutzutage 1 Terra-Bit pro Sekunde (Tbps). Einige der größten registrierten Angriffe richteten sich gegen das DNS.

Es gibt zahlreiche Arten von auf das DNS abzielenden DDoS-Angriffen.

DNS-Amplification (DNS-Verstärkung) ist eine von vielen Angriffsmethoden. Bei dieser Attacke nutzen Angreifer die große Anzahl offener DNS-Server im Internet, die mit einer gefälschten IP-Adresse des Ziels für Antworten auf sehr kleine Suchanfragen genutzt werden können. Das Ziel erhält dann viele DNS-Antworten, die viel größer sind und seine Kapazität schnell überfordern. Der Zweck ist die Blockierung legitimer DNS-Anfragen durch Ausschöpfung der Netzwerkkapazität.

Eine weitere weit verbreitete Angriffsart ist das DNS-Fluten, das sich gegen DNS-Server richtet, die bestimmte Websites hosten. Hierbei wird versucht, serverseitige Assets, wie beispielsweise Speicher oder die Zentraleinheit (CPU), mit einer Flut von UDP-Anfragen zu überlasten, die durch die Ausführung von Scripts auf missbrauchten Botnet-Maschinen erzeugt werden.

Mehrschichtiger Schutz gegen DDoS-Attacken

Für die Abwehr aller Arten von DNS-basierten Angriffen sollte eine Lösung verwendet werden, die einen mehrschichtigen DDoS-Schutz bietet.

DNS-Knoten sollten für die Überwachung auf schädlichen sowie auf mengenmäßig abnormalen Traffic von verdächtigen Orten mit Hardware für die DDoS-Abwehr ausgestattet sein. In vielen Fällen erfolgt die Abwehr lokal.

Wenn ein Angriff ein zu großes Ausmaß erreicht, sollte bösartiger Datenverkehr automatisch in ein Abwehrnetzwerk umgeleitet werden, d. h. in eine völlig separate, speziell aufgebaute Infrastruktur. Dadurch wird eine mögliche Beschädigung der IPs des Ziel-Nameservers begrenzt. Sobald der Angriff isoliert ist, kann ein rund um die Uhr einsatzbereites Sicherheitsteam aggressivere Gegenmaßnahmen umsetzen.

2 Isolierung von Nameservern durch Segmentierung

In der gesamten Branche ist ein hochskalierbares DNS zu einem cloud-basierten Dienst mit Hunderten oder Tausenden von Kunden – jeder mit zahlreichen Domains – geworden, die in einzelnen Netzwerken zusammengefasst sind und gemeinsam einen Nameserver nutzen.

Dies erhöht die Chancen, dass man das Leid eines anderen spürt. Wenn Sie einen Fremd-DNS-Provider nutzen, richten sich die meisten Angriffe gegen dessen Netzwerk nicht auf Sie, sondern auf eine Domain, die den von Ihrem Provider zugewiesenen Nameserver mitbenutzt.

Es ist klug, die Auswirkungen eines DDoS-Angriffs zu isolieren.

Entscheiden Sie sich für einen DNS-Provider, der das DNS-Netzwerk in Segmente unterteilt: jedes mit einem Nameserver-Announcement, das nur von einer kleinen Gruppe Kunden gemeinsam genutzt wird. Wenn weniger Kunden Hostnamen und IP-Adressen gemeinsam nutzen, ist die Wahrscheinlichkeit erheblich geringer, dass Sie einen Welleneffekt erleben.

Hier ist eine Analogie: Stellen Sie sich vor, Sie wären in einer großen Halle mit 10.000 Personen und eine Person springt auf und schreit so laut, dass niemand den Redner hören kann. Jetzt stellen Sie sich das gleiche Szenario vor, aber mit nur 20 anderen Personen. Die Wirkung des Schreihalses ist nur auf die 20 Personen beschränkt. Nehmen wir an, der Schreihals ist ein DDoS-Angriff. Sobald er (der Angriff) beginnt, verschiebt die Nameserver-Segmentierung und die DDoS-Abwehrstrategie den gesamten Raum sofort in einen schalldichten Bereich, evakuiert die braven Zuschauer und arbeitet daran, den Schreihals zu beruhigen, bevor alle anderen wieder hereingelassen werden. Es ist offensichtlich, dass mit nur 20 Personen das Schreien weniger Personen betreffen würde, die einfacher durch diesen Angriff zu navigieren wären.

Geschützt sein, egal ob Sie oder jemand anderes angegriffen wird

Dieser Ansatz ermöglicht die Verschiebung einzelner Nameserver-Announcements vom DNS-Netzwerk in das DDoS-Abwehrnetzwerk, ohne dass die Anfrageauflösung wesentlich verzögert wird. Ihr DNS-Provider sollte in der Lage sein, den angegriffenen Kunden wirksamen und sofortigen Schutz zu bieten UND jeglichen Kollateralschaden von Kunden abzuwenden, die sich noch im DNS-Netzwerk befinden.

Werden cloud-basierte DNS-Dienste genutzt, ist Announcement auf einem segmentierten Nameserver eine wirksame Maßnahme zum Schutz Ihres DNS-Traffic.

3 Verwendung eines Nicht-Open-Source-Resolvers

DNS-Resolver – das sind die Server, die auf Domainnamen-Anfragen antworten – stellen sicher, dass Benutzer zu den richtigen Websites weitergeleitet werden. Die geläufigste Softwareanwendung zur Verwaltung des DNS ist Berkeley Internet Name Domain (BIND). BIND wurde 1983 an der University of California in Berkeley entwickelt und macht bis heute die überwiegende Mehrheit der globalen Nameserver-Implementierungen aus. Der Quellcode von BIND ist Open Source, d. h. jetzt vollständig öffentlich zugänglich, und kann von böswilligen Hackern leicht ausgespäht und ausgenutzt zu werden.

Vermeidung von Resolver-Bedrohungen

CSC hat sich für eine Partnerschaft mit Neustar entschieden, da dieses Unternehmen dieses Problem schon vor Jahren gelöst hat. Es entwickelte einen firmeneigenen Code und bat fremde Sicherheitsauditoren, diesen auf Schwachstellen zu überprüfen. Sie fanden keine, die Angreifer aus der Ferne ausnutzen könnten, um entweder eingeschränkte Rechte zu stehlen oder die Verzeichnisauflösung zu beeinträchtigen.

Neben der Unterstützung von Standard-DNS-Spezifikationen und Request for Comments (RFCs) verbesserten sie ihre Resolver mit erweiterten DNS-Fähigkeiten sowie zusätzlicher Redundanz und Sicherheit. Die meisten älteren DNS-Server-Implementierungen können dieses Niveau niemals erreichen.

4 Einsatz von DNS-Sicherheitserweiterungen (DNSSEC)

Wenn sie Internetnutzern helfen, die gewünschten Websites zu finden, fragen sich DNS-Server gegenseitig ab. Um die Dinge zu beschleunigen, speichern Server die Ergebnisse für eine bestimmte Zeitspanne im Cache. Wenn es eine Anfrage nach dem gleichen Namen gibt, bevor der Ressourcendatensatz abgelaufen ist, sendet ein Server die Antwort im Cache, anstatt eine andere Maschine abzufragen.

DNS-Cache-Poisoning ermöglicht Pharming-Angriffe

Obwohl dies die Effizienz steigert, ist es aber auch eine Einladung zum Cache-Poisoning. Dies geschieht, wenn ein DNS-Server, der in der Regel von Kriminellen kompromittiert wird, eine falsche Antwort auf eine DNS-Anfrage liefert. Benutzer landen auf gefälschten Websites, die persönliche Daten abfragen oder einfach Malware aktivieren.

Wie kann das passieren? In vielen Fällen überprüfen DNS-Server nicht, ob sich die Antworten, die sie von anderen Servern erhalten, auf die ursprüngliche Anfrage beziehen. Ein Server speichert schädliche Daten im Cache und gibt sie an andere weiter, die DNS-Clients des betroffenen Computers sind.

DNSSEC ist der Schlüssel für den Schutz

DNSSEC besteht aus einer Reihe von Sicherheitserweiterungen, die DNS-Antworten authentifizieren. Das Geheimnis dahinter ist eine Reihe von Kombinationen aus öffentlichen und privaten Schlüsseln zum Signieren von Datenressourcen. Dies funktioniert durch die Bereitstellung eines öffentlichen Schlüssels, mit dem der Resolver des Benutzers bestätigen kann, dass eine DNS-Antwort mit der kryptographischen Version übereinstimmt. Alle Transaktionen sind signiert, Angreifer können die Pakete nicht einfach fälschen.

Einfacher ausgedrückt schützt DNSSEC den DNS-Prozess durch die Abwehr von Cache-Poisoning, Pharming-Angriffen und anderen ernsthaften Bedrohungen. Stellen Sie sicher, dass dieser Schutz eingeschaltet ist.

DNSSEC-Akzeptanz

In unseren CSC Cyber-Sicherheitsberichten in den letzten Jahren haben wir alarmierend niedrige DNSSEC-Akzeptanzraten festgestellt, die bei großen Unternehmen weltweit aus verschiedenen Branchen nur zwischen 0 und 5 % liegen.

5 Erhöhung der Ausfallsicherheit mit einem privaten DNS-Netzwerk

Ein altes Sprichwort lautet: Eine Kette ist nur so stark wie ihr schwächstes Glied. Aber was wäre, wenn Sie Ihre Abwehrkräfte erhöhen könnten, indem Sie die schwachen Glieder beseitigen? Durch die Reduzierung der Abhängigkeit von öffentlichen Internetverbindungen hat das private Netzwerk im Wesentlichen den mittleren und gefährlichsten Teil der DNS-Transaktion eliminiert, in dem die überwiegende Mehrheit der DDoS-Angriffe und DNS-Cache-Poisoning-Versuche stattfindet. Fragen Sie Ihren Provider, ob er dies als zusätzlichen Service anbietet.

Ein privates Netzwerk bietet drei wesentliche Vorteile:

Geringere Latenzzeit

In einigen Fällen können andere Probleme mit der Internetverbindung, selbst wenn das DNS einwandfrei funktioniert, zu einer Verschlechterung der DNS-Leistung führen, was die Benutzererfahrung verschlechtert. Das private Netzwerk bietet ein Online-Erlebnis, das sowohl schnell als auch effizient ist, da der DNS-Traffic eine Vernetzung zum allgemeinen Internet vermeidet.

Mehr Sicherheit

Die aktuellen, durch das Internet der Dinge verstärkten DDoS-Angriffe, die das Internet unzugänglich machen, werden bald der Vergangenheit angehören. Ein privates Netzwerk zur DNS-Auflösung innerhalb von Provider-Netzwerken minimiert externe Bedrohungen wie DDoS-Angriffe und Cache Poisoning-Versuche.

Höhere Zuverlässigkeit

Im Falle eines DDoS-Angriffs oder eines größeren Ausfalls werden Anfragen weiterhin innerhalb der privaten Netzwerke, in denen DNS bereitgestellt wird, aufgelöst. Diese Ausfallsicherheit gewährleistet ein hervorragendes Interneterlebnis für Benutzer, die nach Websites und anderen wichtigen Online-Objekten suchen.

6 Identifizierung von Sicherheitslücken bei Ihren wichtigen digitalen Assets

Unternehmen müssen in der Lage sein, ihre geschäftskritischen Domains zu erkennen und kontinuierlich zu überwachen, um sicherzustellen, dass sie mit den richtigen Schutzmaßnahmen geschützt sind.

Wir haben festgestellt, dass niemand Unternehmen dabei unterstützt, und deshalb haben wir CSC Security Center℠ entwickelt, eine intelligente Plattform, die die Bedrohungen in wichtigen Domains und innerhalb der DNS-Infrastruktur, auf der sie aufbauen, kennt und Unternehmen auf Gefahrenbereiche aufmerksam macht.

Dieser einzigartige Ansatz verändert die Art und Weise, wie Domains und DNS gesichert werden, und hilft Unternehmen bei der besseren Erkennung ihrer Sicherheitslücken. CSC Security Center hilft insbesondere bei der

- Erkennung, welche Domains geschäftskritisch sind und eine 100%ige Verfügbarkeit erfordern
- Identifizierung aller aktuellen DNS-Provider und Abschätzung aller Sicherheitsrisiken bei Anbietern
- Identifizierung aller fehlenden Sicherheitsfunktionen, wodurch das Risiko von DNS-Cache-Poisoning, Domain- oder DNS-Hijacking, Domain-Shadowing, DDoS-Angriffen und Phishing erhöht wird.

Fordern Sie weitere Informationen darüber an, wie das CSC Security Center und unsere DNS-Management-Dienste Ihnen bei der Abwehr von Cyber-Bedrohungen helfen können.

CSC unterstützt mit der Aufdeckung von Sicherheitslücken, die in elementaren Internet-Assets wie Domainnamen, DNS und digitalen Zertifikaten vorhanden sind, Unternehmen, die bedeutende Investitionen in ihre Sicherheit tätigen. 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 der DSGVO, zu vermeiden. 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.

cscdigitalbrand.services/de