Argumente für den Secondary-DNS-Service

Verbesserte Sicherheitsstrategien zum Schutz Ihrer Online-Assets

Das kann auch Ihnen passieren

Am 21. Oktober 2016 wurde ein bekannter Provider für verwaltete Domain Namen Systeme (DNS) durch einen DDoS-Angriff erschüttert. Der Angriff unterbrach nicht nur die Verfügbarkeit und die Dienste des DNS-Providers, sondern der Kollateralschaden griff auch auf eine Reihe bekannter Marken über, deren Websites und Anwendungen ebenfalls zeitweise ausfielen.

Nach dem Angriff kam die ernüchternde Realität, dass niemand gegen DDoS-Bedrohungen immun ist, insbesondere gegen Angriffe auf das DNS. Ebenso bedenklich war jedoch die allgemeine Wahrnehmung, dass die betroffenen Unternehmen nichts falsch gemacht hätten. Sie taten, was viele Berater damals empfahlen – sie vertrauten ihr DNS einem verwalteten Dienst an. Doch das Fehlen einer Absicherung erwies sich als fataler Fehler.

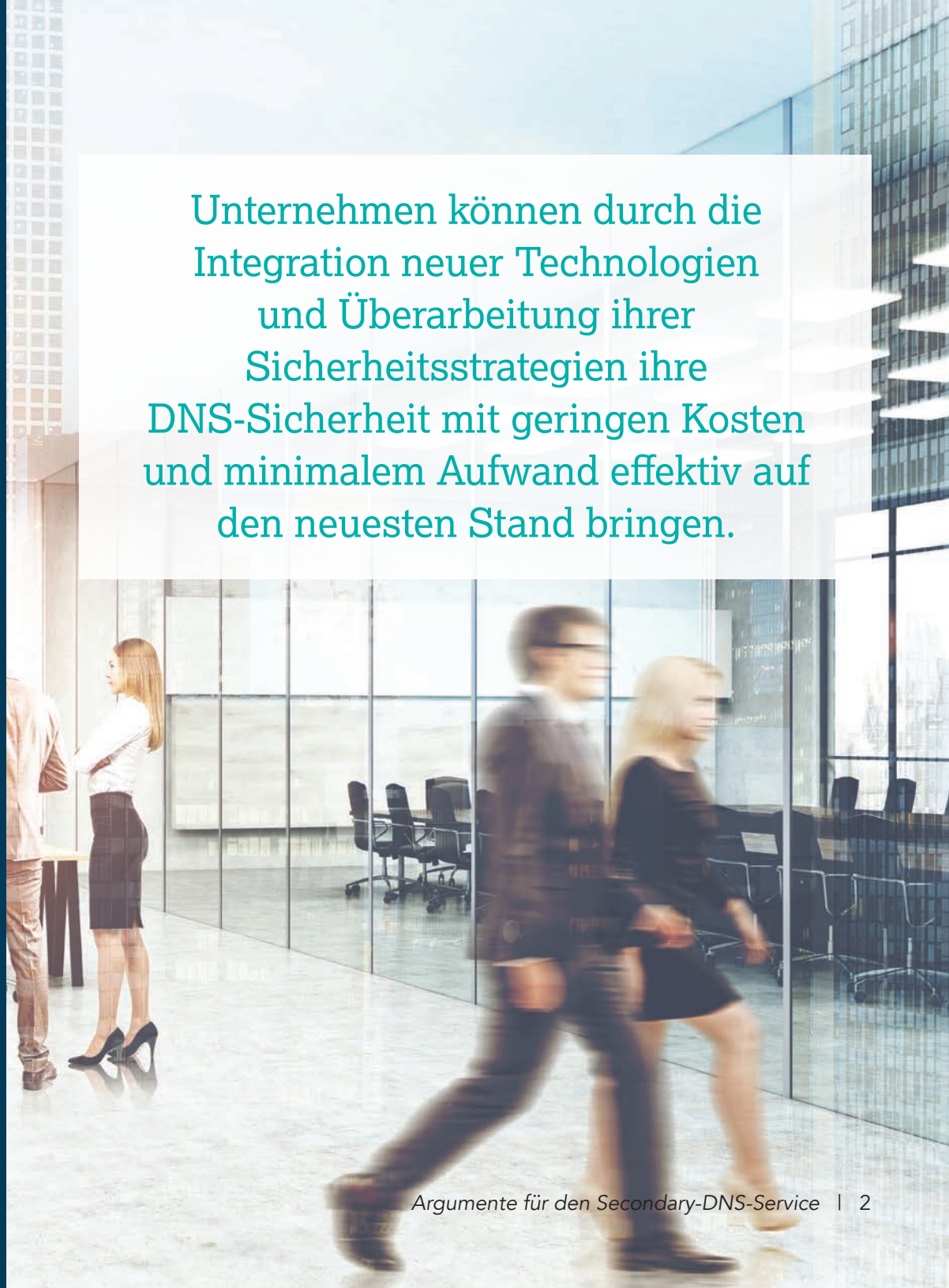
Der Angriff vom 21. Oktober signalisierte eine grundlegende Änderung in der Art und Weise, wie DDoS-Angriffe in Zukunft gestaltet sind. Dieser Angriff wurde mit Hilfe der Mirai Botnet-Malware gestartet, die atypische, mit dem Internet verbundene Geräte nutzt, z. B. Sicherheitskameras, digitale Videorekorder (DVRs) und Router für den Heimgebrauch. Zusammengenommen bildeten die gekaperten Geräte eine gefährlich starke Waffe mit großer Massenwirkung. Das Mirai Botnet löste einen verheerenden DDoS-Angriff in einem bisher unbekannten Ausmaß aus. Und aufgrund seiner Wirksamkeit war das Botnet ein gefährlicher Vorbote für das, was in Zukunft bevorsteht.

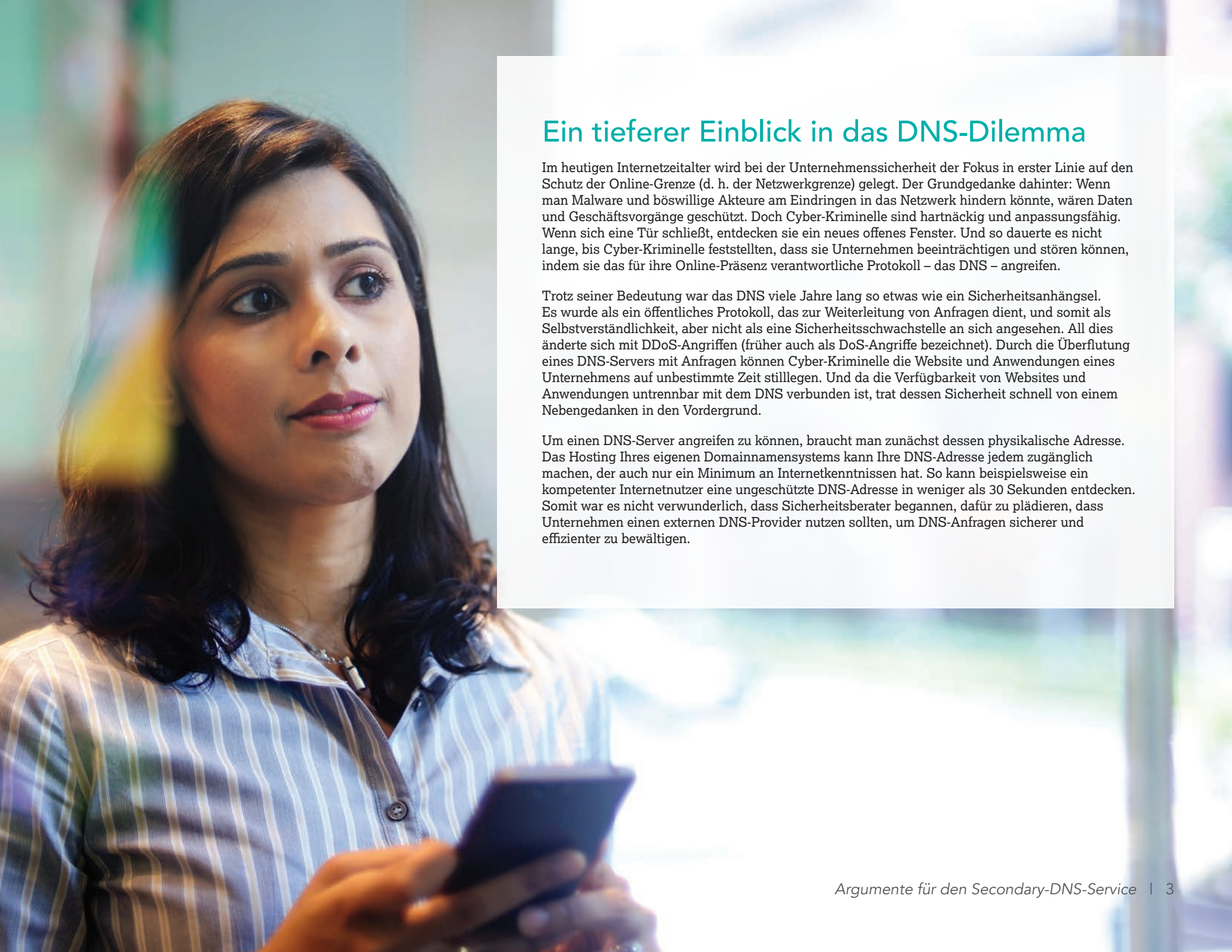
Aber vor allem war der Angriff eine unschätzbare Lektion bezüglich der neuen Anforderungen an das DNS, nämlich, dass Unternehmen nicht ihre gesamte Online-Präsenz ausschließlich einem DNS-Service anvertrauen sollten. Die Unternehmen, die sich ausschließlich auf einen DNS-Provider verlassen hatten, zeigten die realen Folgen der Abhängigkeit von einem Single Point of Failure. Wenn diese Unternehmen ihr DNS auf mehrere Dienste aufgeteilt hätten, dann wäre der Ausfall ihrer Websites, Apps und anderer Online-Assets weniger wahrscheinlich gewesen – selbst während des Angriffshöhepunkts.

Das Problem wird durch das Tempo, mit dem sich heutzutage die Cyber-Kriminalität weiterentwickelt, noch verschärft. Eine solide Strategie zur Begrenzung von Cyber-Angriffen kann in weniger als sechs Monaten überholt sein. Dies gilt insbesondere für DNS-Angriffe, da Kriminelle das Störungspotenzial erkennen und daher auf DNS-Schwachstellen zielen.

Dieses Dokument basiert auf der Publikation „The Case for a Secondary DNS Service“ von Neustar®.

Unternehmen können durch die Integration neuer Technologien und Überarbeitung ihrer Sicherheitsstrategien ihre DNS-Sicherheit mit geringen Kosten und minimalem Aufwand effektiv auf den neuesten Stand bringen.





Ein tieferer Einblick in das DNS-Dilemma

Im heutigen Internetzeitalter wird bei der Unternehmenssicherheit der Fokus in erster Linie auf den Schutz der Online-Grenze (d. h. der Netzwerkgrenze) gelegt. Der Grundgedanke dahinter: Wenn man Malware und böswillige Akteure am Eindringen in das Netzwerk hindern könnte, wären Daten und Geschäftsvorgänge geschützt. Doch Cyber-Kriminelle sind hartnäckig und anpassungsfähig. Wenn sich eine Tür schließt, entdecken sie ein neues offenes Fenster. Und so dauerte es nicht lange, bis Cyber-Kriminelle feststellten, dass sie Unternehmen beeinträchtigen und stören können, indem sie das für ihre Online-Präsenz verantwortliche Protokoll – das DNS – angreifen.

Trotz seiner Bedeutung war das DNS viele Jahre lang so etwas wie ein Sicherheitsanhängsel. Es wurde als ein öffentliches Protokoll, das zur Weiterleitung von Anfragen dient, und somit als Selbstverständlichkeit, aber nicht als eine Sicherheitsschwachstelle an sich angesehen. All dies änderte sich mit DDoS-Angriffen (früher auch als DoS-Angriffe bezeichnet). Durch die Überflutung eines DNS-Servers mit Anfragen können Cyber-Kriminelle die Website und Anwendungen eines Unternehmens auf unbestimmte Zeit stilllegen. Und da die Verfügbarkeit von Websites und Anwendungen untrennbar mit dem DNS verbunden ist, trat dessen Sicherheit schnell von einem Nebengedanken in den Vordergrund.

Um einen DNS-Server angreifen zu können, braucht man zunächst dessen physikalische Adresse. Das Hosting Ihres eigenen Domainnamensystems kann Ihre DNS-Adresse jedem zugänglich machen, der auch nur ein Minimum an Internetkenntnissen hat. So kann beispielsweise ein kompetenter Internetnutzer eine ungeschützte DNS-Adresse in weniger als 30 Sekunden entdecken. Somit war es nicht verwunderlich, dass Sicherheitsberater begannen, dafür zu plädieren, dass Unternehmen einen externen DNS-Provider nutzen sollten, um DNS-Anfragen sicherer und effizienter zu bewältigen.

Geeignete Sicherheitsaufstellung für das autoritative DNS

Das Wichtigste, was Unternehmen tun können, um ihr autoritatives DNS zu schützen, ist die Implementierung einer Lösung mit Primary- und Secondary-DNS. Nach der Erfahrung mit dem Mirai Botnet empfehlen Branchenanalysten (z. B. Gartner), dass Unternehmen für bessere Leistung und Sicherheit einen Secondary-DNS-Service haben sollten.

Ein Secondary-DNS-Service darf nicht mit einem redundanten DNS-Provider verwechselt werden. Es geht nicht darum, einen Plan B zu haben, falls Plan A scheitert. Stattdessen geht es darum, einen intelligenteren Plan A zu haben, der den DNS-Traffic effizient auf zwei vertrauenswürdige Netzwerke aufteilt. Diese Strategie schützt nicht nur Ihre Marke vor einem einzelnen DDoS-Angriff, sondern verbessert auch Ihre DNS-Redundanz, indem sie die Last auf zwei Netzwerke verteilt.

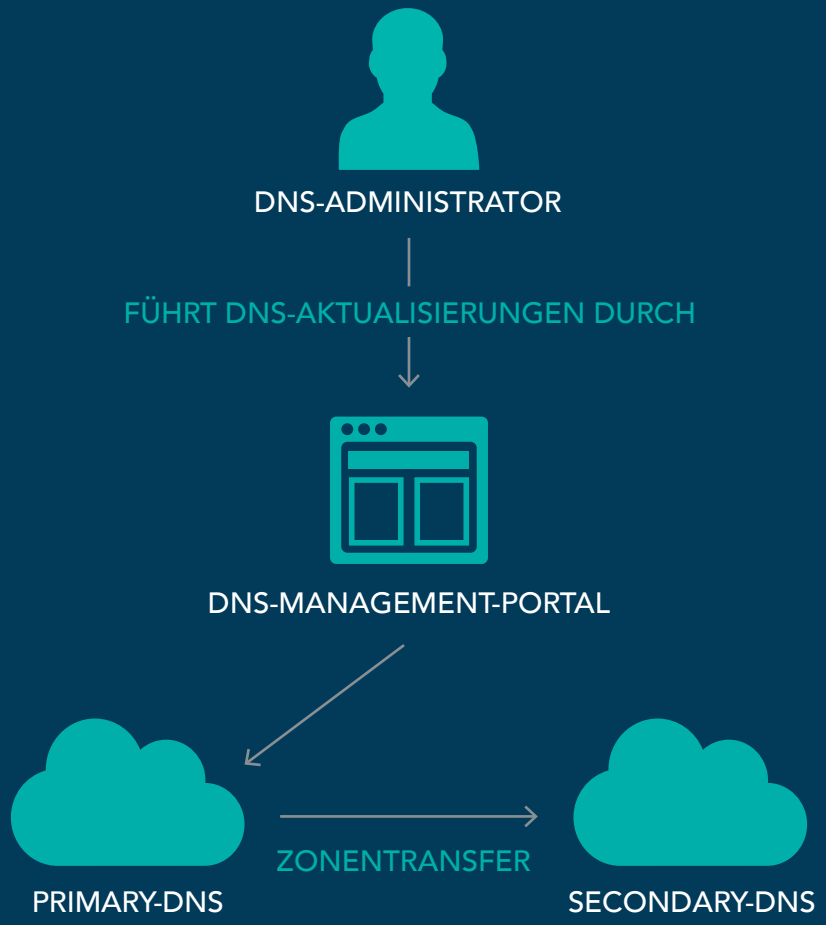
Die Suche nach einem verwalteten Secondary-DNS-Dienst ist das Erste, was Sie tun sollten, um Ihre DNS-Sicherheit zu erhöhen. Die zweite Maßnahme ist die Auswahl eines DNS-Providers, der einen internen DDoS-Abwehrdienst für seine verwalteten DNS-Netzwerke anbietet. Da immer mehr Geräte mit dem Internet verbunden sind und das Potenzial für immer mehr und breiter gefächerte Botnet-Armeen schaffen, ist eine separate Schicht für den Schutz gegen DDoS-Attacken für Unternehmen sinnvoll. Noch besser ist es, wenn Sie Ihr DNS durch ein isoliertes (air-gapped) Netzwerk „verbergen“ können, sodass es nicht direkt dem Internet ausgesetzt ist. Damit können Sie die Anzahl der Angriffe auf Ihr DNS drastisch reduzieren.

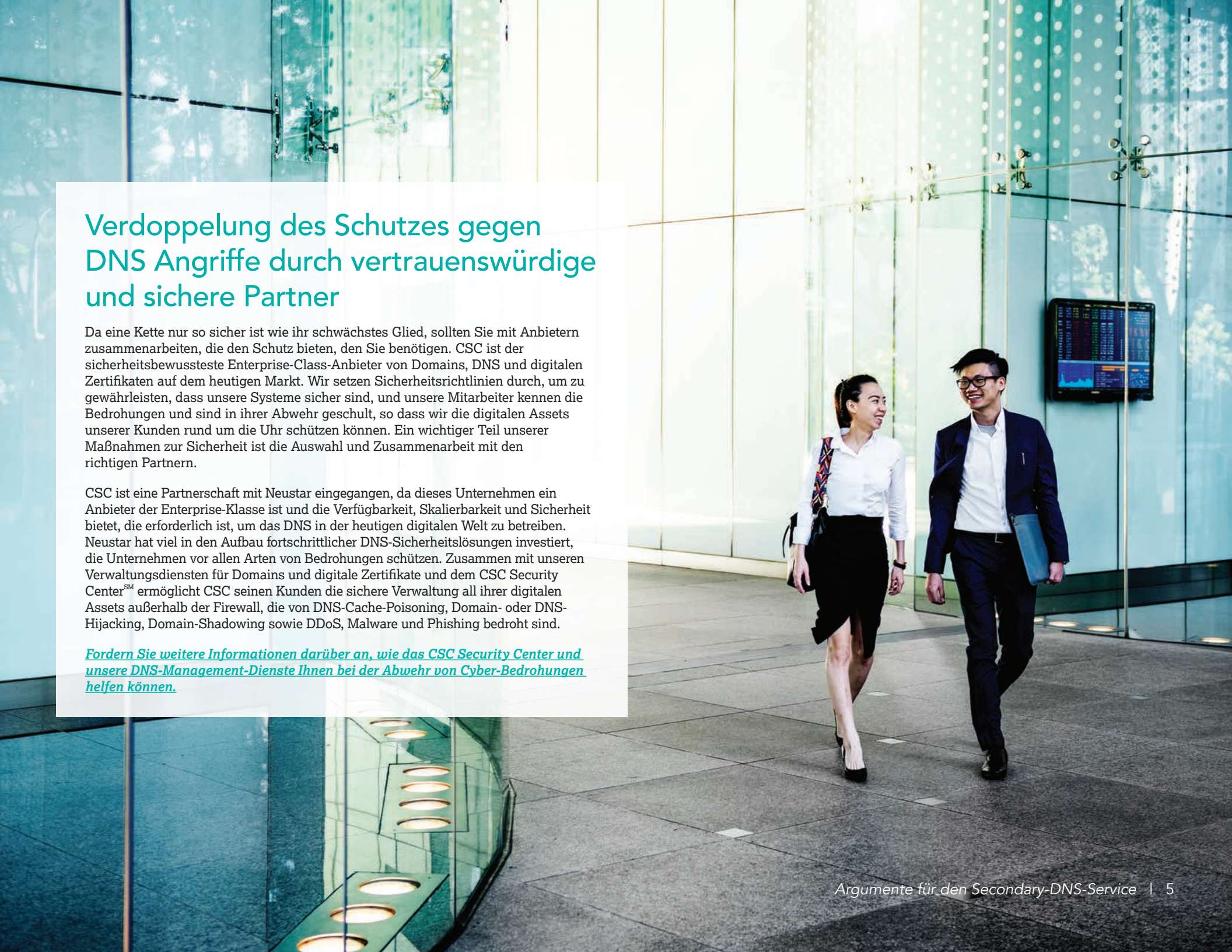
Maßnahmen für mehr Sicherheit des autorativen DNS:

- Verwalteter Primary- und Secondary-DNS-Service
- Auswahl eines DNS-Providers, der einen internen DDoS-Abwehrdienst für sein DNS-Netzwerk anbietet
- Verstecken der DNS-Systeme vor direkter Internet-Einwirkung

SO FUNKTIONIEREN PRIMARY- UND SECONDARY-DNS

1. Der DNS-Administrator meldet sich beim DNS-Management-Portal an.
2. Der DNS-Administrator aktualisiert einen DNS-Eintrag.
3. Die Änderung wird über das DNS-Netzwerk verbreitet.
4. Das Secondary-DNS wird darüber benachrichtigt, dass eine Aktualisierung stattgefunden hat und führt einen Zonentransfer durch, um den aktualisierten Datensatz zu erhalten.





Verdoppelung des Schutzes gegen DNS Angriffe durch vertrauenswürdige und sichere Partner

Da eine Kette nur so sicher ist wie ihr schwächstes Glied, sollten Sie mit Anbietern zusammenarbeiten, die den Schutz bieten, den Sie benötigen. CSC ist der sicherheitsbewussteste Enterprise-Class-Anbieter von Domains, DNS und digitalen Zertifikaten auf dem heutigen Markt. Wir setzen Sicherheitsrichtlinien durch, um zu gewährleisten, dass unsere Systeme sicher sind, und unsere Mitarbeiter kennen die Bedrohungen und sind in ihrer Abwehr geschult, so dass wir die digitalen Assets unserer Kunden rund um die Uhr schützen können. Ein wichtiger Teil unserer Maßnahmen zur Sicherheit ist die Auswahl und Zusammenarbeit mit den richtigen Partnern.

CSC ist eine Partnerschaft mit Neustar eingegangen, da dieses Unternehmen ein Anbieter der Enterprise-Klasse ist und die Verfügbarkeit, Skalierbarkeit und Sicherheit bietet, die erforderlich ist, um das DNS in der heutigen digitalen Welt zu betreiben. Neustar hat viel in den Aufbau fortschrittlicher DNS-Sicherheitslösungen investiert, die Unternehmen vor allen Arten von Bedrohungen schützen. Zusammen mit unseren Verwaltungsdiensten für Domains und digitale Zertifikate und dem CSC Security Center℠ ermöglicht CSC seinen Kunden die sichere Verwaltung all ihrer digitalen Assets außerhalb der Firewall, die von DNS-Cache-Poisoning, Domain- oder DNS-Hijacking, Domain-Shadowing sowie DDoS, Malware und Phishing bedroht sind.

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

Copyright ©2019 Corporation Service Company. Alle Rechte vorbehalten.

CSC ist ein Service-Unternehmen und bietet keine Rechts- oder Finanzberatung an. Die hier veröffentlichten Materialien dienen nur zu Informationszwecken. Bitte wenden Sie sich an Ihren Rechts- oder Finanzberater, um herauszufinden, inwiefern diese Informationen auf Sie zutreffen.