Jenseits der Firewall:

Implementierung von DNS-Schutz zur Minimierung von Online-Schwachstellen und -Bedrohungen

Jenseits der Firewall: Implementierung von DNS-Schutz zur Minimierung von Online-Schwachstellen und -Bedrohungen

Firewalls sind seit über 25 Jahren eine erste Verteidigungslinie für die Netzwerksicherheit. Sie bilden eine Barriere zwischen sicheren, vertrauenswürdigen und kontrollierten internen Netzwerken und nicht vertrauenswürdigen externen Netzwerken wie dem Internet.

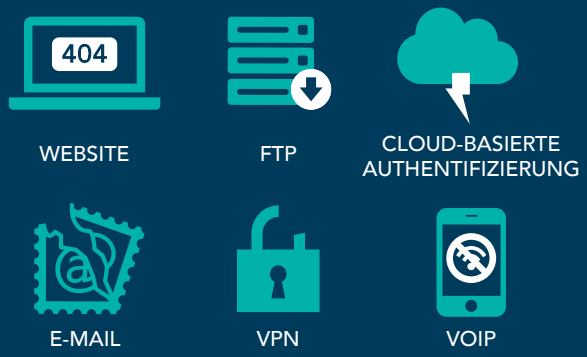
Und wir brauchen sie, denn Cyber-Kriminalität ist allgegenwärtig und wächst ständig. Viele im IT-Sicherheitsbereich reagieren, indem sie ihre Verteidigungslinien innerhalb ihrer Firewall stärken und Simulationen und Penetrationstests durchführen.

Aber angesichts des heutigen hohen Niveaus der Cyber-Kriminalität reicht eine Firewall allein nicht mehr aus.

Oft wird die Sicherheit von digitalen Assets, die außerhalb der Firewall liegen, übersehen. Damit meinen wir Domainnamen, das Domain Name System (DNS) und digitale Zertifikate. Gut verwaltete digitale Assets – insbesondere das DNS – sind entscheidend für den reibungslosen Geschäftsbetrieb.

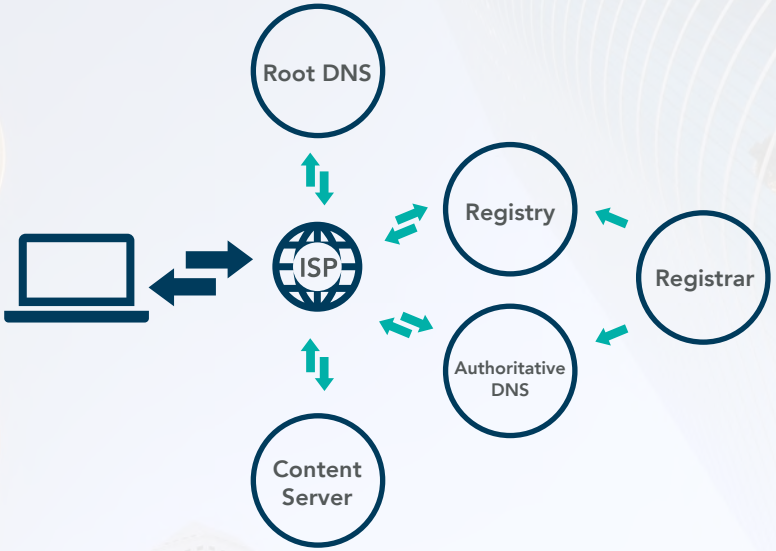
Das DNS bildet die zugrunde liegende Infrastruktur für die Funktionsweise des Internets und leitet als Verzeichnis Benutzer zu den richtigen Webinhalten. Wenn das DNS ausfällt, fallen Websites aus. Geschieht dies, ist die Nutzung von Telefon und E-Mail naheliegend, um den Geschäftsbetrieb aufrechtzuerhalten. Ein ausgefallenes DNS bedeutet aber, dass keine E-Mails, keine Telefone (VoIP) und keine Logins von entfernten Mitarbeitern mehr funktionieren. Ebenso funktioniert auch kein Datenübertragungsprotokoll (FTP) für die Übertragung großer Datensätze und verschiedene Multi-Faktor-Authentifizierungsdienste (z. B. für E-Mail, Google® und Microsoft®).

Der Ausfall dieser digitalen Assets hätte erhebliche Auswirkungen, z. B. Umsatzeinbußen, Datenverluste und Rufschädigung von Marken.



Das DNS ist anfällig. VORSICHT IST GEBOTEN!

Das einfach aussehende Akronym DNS täuscht über die Komplexität des Systems hinweg, das aus einem weltweiten Netz separater Einheiten besteht, die ständig Informationen austauschen. Diese komplexe Natur setzt das DNS mehreren potenziellen Fehlerquellen aus, da jeder Punkt im System für Angriffe anfällig sein könnte, die sich negativ auf Ihr Unternehmen auswirken.



10 Bedrohungen und Risiken im Zusammenhang mit DNS-Schwachstellen

1. DNS-Hijacking
2. DNS-Cache-Poisoning
3. Domain Shadowing
4. DNS-Ausfälle
5. Malware
6. DNS-Tunneling
7. Zero-Day-Angriffe
8. DDoS-Angriffe
9. Abgelaufene, gestohlene oder verlorene Domains
10. Abgelaufene, fehlende oder mangelhaft installierte digitale Zertifikate

Vierstufiger Ansatz Defense in Depth

Defense in Depth (tief gegliederte Verteidigung) ist das Konzept eines mehrschichtigen Sicherheitsansatzes, der Ihre digitalen Assets außerhalb der Firewall schützt.

STUFE 1:

Einsatz hochentwickelter Sicherheitsmerkmale für Ihre geschäftskritischen Domains.

Schützen Sie Ihre geschäftskritischen Domains, die Ihren Geschäftsbetrieb unterstützen, mit folgenden Merkmalen:

- Registry-Locks gegen DNS-Hijacking
- Domain Name System Security Extension (DNSSEC) zur Verhinderung von DNS-Cache-Poisoning
- Digitale Zertifikate (SSL) zur Verschlüsselung von Daten
- Domain-based Message Authentication, Reporting and Conformance (DMARC) zur Authentifizierung Ihrer E-Mails und zur Reduzierung der Bedrohung durch Phishing-Angriffe, die auf Mitarbeiter und Angestellte abzielen
- Certificate Authority Authorization (CAA)-Einträge zur Durchsetzung Ihrer Richtlinien zu digitalen Zertifikaten

1

2

3

4

Vierstufiger Ansatz Defense in Depth

Defense in Depth (tief gegliederte Verteidigung) ist das Konzept eines mehrschichtigen Sicherheitsansatzes, der Ihre digitalen Assets außerhalb der Firewall schützt.

STUFE 2:

Kontrolle der Nutzerberechtigungen.

Kontrollieren Sie, wer Zugriff auf Ihre geschäftskritischen Assets hat und welche Berechtigungen diese Personen haben. Verwalten Sie dann diese Berechtigungen aktiv. Sie sollten auf Knopfdruck auf Berechtigungen zugreifen können, Benachrichtigungen erhalten und Änderungen auf einer einzigen Plattform beobachten und genehmigen können. Dies hilft gegen unbefugte Änderungen wie DNS-Hijacking und Domain-Shadowing.

Vierstufiger Ansatz Defense in Depth

Defense in Depth (tief gegliederte Verteidigung) ist das Konzept eines mehrschichtigen Sicherheitsansatzes, der Ihre digitalen Assets außerhalb der Firewall schützt.

STUFE 3:

Sicherung des Portalzugriffs.

Sie sollten den Zugriff auf alle von Ihnen verwendeten Portale sichern. Jedes Portal sollte Multi-Faktor-Authentifizierung zur Gewährung des Zugriffs aufweisen, einschließlich IP-Validierung, Zwei-Faktor-Authentifizierung und Federated ID (oder Single Sign-On). Für die Zugriffsverwaltung und die Reduzierung des Risikos unbefugter Änderungen an Ihren digitalen Assets ist es auch hilfreich, eine Konsolidierung auf weniger Anbieter durchzuführen.

Vierstufiger Ansatz Defense in Depth

Defense in Depth (tief gegliederte Verteidigung) ist das Konzept eines mehrschichtigen Sicherheitsansatzes, der Ihre digitalen Assets außerhalb der Firewall schützt.

STUFE 4:

Enterprise-Class-Provider.

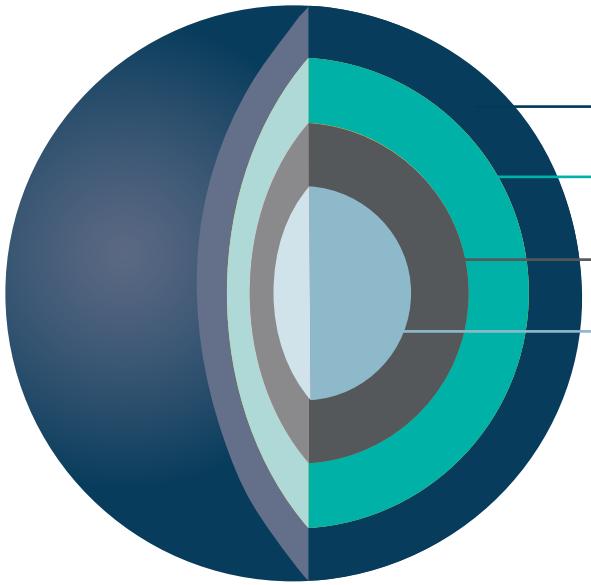
Wählen Sie Ihre Partner sorgfältig aus. Neben der Begrenzung der Anzahl der Anbieter und der verwendeten Portale, um die Angriffsfläche so gering wie möglich zu halten, ist es wichtig, keine Kompromisse bei der Qualität der Verwaltung von Domains, des DNS oder digitaler Zertifikate einzugehen. Die besten Enterprise-Class-Provider ermöglichen es Ihnen, das Management all dieser Vermögenswerte mit sicheren Systemen und Prozessen zu konsolidieren, um die Risiken und Bedrohungen zu minimieren. Enterprise-Class-Provider können auf die Kompetenzen und Unterstützung interner Analysten und strategischer Kundenbetreuer zurückgreifen, um Ihnen zu helfen, die einschlägigen Risiken zu verstehen und die richtigen Lösungen auszuwählen.

Sichtbarmachung von Sicherheitsbedrohungen außerhalb der Firewall

Wir bei CSC haben festgestellt, dass auf dem Markt Hilfsmittel fehlten, mit denen ein Unternehmen – insbesondere der Chief Information Security Officer – abschätzen kann, was mit den Assets außerhalb der Firewall passiert. Bestehende Dashboards konzentrieren sich auf Lücken in internen Netzwerken und Firewalls, wobei nur wenige Tools die schwerwiegenden Risiken außerhalb des Wirkungsbereichs der Firewall aufdecken.

CSC Security Center℠ wurde entwickelt, um IT-Experten bei der Reduzierung von Risiken durch ungeschützte digitale Assets zu unterstützen. Mit unserem firmeneigenen Algorithmus kann prognostiziert werden, welche Domainnamen in einem Portfolio entscheidend sind. Dabei werden mehrere Merkmale der Domain untersucht und die miteinander verbundenen Beziehungen nachvollzogen. Eine weitere Untersuchung der Domains identifiziert alle Risiken und hebt Empfehlungen zur Abwehr von Bedrohungen hervor.

Transparenz führt zu umsetzbaren Kontrollen und Richtlinien



Mit CSC Security Center können Unternehmen nun wichtige Domains und Sicherheitslücken identifizieren, einschließlich Risiken durch DNS-Cache-Poisoning, Domain- und DNS-Hijacking, DDoS-Angriffe und mehr. Wir empfehlen, einen Schritt weiter zu gehen, um Richtlinien einzuführen, die den richtigen Rahmen für die Stärkung der Sicherheit eines Unternehmens schaffen.

ENTERPRISE-CLASS-PROVIDER

- Nach ISO 27001 zertifizierte Rechenzentren
- SOC 2®-konform
- Penetrations-, Schwachstellen- und Sicherheitstests durch Drittanbieter
- ICANN- und Registry-zertifiziert
- Erstklassige Partnerschaft für das Domain Name System (DNS) und digitale Zertifikate
- Schulungen über Sicherheitsaspekte, Phishing und Social Engineering
- Mandatierte Clear-Desk-Richtlinie
- Obligatorische schriftliche Anfrage (niemals telefonisch)
- Daten- und DSGVO-konform (z. B. WHOIS-Verfahren)
- Richtlinie für automatische Verlängerungen unterstützt durch Kontoguthaben
- Richtlinie zur Sperrung von Registry-Übertragungen

SICHERUNG DES PORTALZUGRIFFS

- Richtlinie für obligatorische Zwei-Faktor-Authentifizierung
- Kostenlose IP-Validierung
- Kostenlose Federated ID

KONTROLLE DER NUTZERBERECHTIGUNGEN

- Sichtbarkeit höherer Berechtigungen mit Benachrichtigungen
- Richtlinie zu autorisierten Kontaktpersonen

EINSATZ HOCHENTWICKELTER SICHERHEITSMERKMALE FÜR IHRE GESCHÄFTSKRITISCHEN DOMAINS

- Identifikation geschäftskritischer Domains
- Erkennung von Sicherheitslücken
- Auto-Lock-Richtlinie

DNS-Hijacking-Angriffe stehen im Mittelpunkt der Cybersicherheit, und täglich neue Schlagzeilen machen 2019 zu einem Wendepunkt.

- CSC Alerts Companies to Increased DNS Hijacking (CSC warnt Unternehmen vor zunehmendem DNS-Hijacking)
- DNS Hijacking Abuses Trust in Core Internet Service (DNS-Hijacking missbraucht das Vertrauen in den zentralen Internetdienst)
- Alert Regarding Published Reports of Attacks on the Domain Name System (Warnung im Hinblick auf veröffentlichte Berichte über Angriffe auf das Domain Name System)
- Emergency Directive 19-01 Mitigate DNS Infrastructure Tampering (Notfallrichtlinie 19-01 zur Minimierung von Manipulationen an der DNS-Infrastruktur)

Eine gegen nationale Sicherheitsorganisationen, Außenministerien und führende Energieunternehmen gerichtete globale Kampagne wurde identifiziert. Sie modifizierte DNS-Namensdatensätze so, dass sie Benutzer auf von Akteuren kontrollierte Server leiten. Ziel waren zunächst Drittanbieter wie DNS-Registrare, Telekommunikationsunternehmen und Internetdienstanbieter. Außerdem wurde das legitime digitale Zertifikat der Organisation für die Verwendung auf von den Akteuren kontrollierten Servern gestohlen.

„DNS-Angriffe führen dazu, dass Kriminelle Web-Traffic von einer legitimen Website auf eine betrügerische Website umleiten und damit Kunden und Unternehmen einem großen Risiko aussetzen“, erklärt Mark Flegg, Produktdirektor für Security Services bei CSC. „Die jüngsten Angriffe sind komplex und bösartig und nutzen Schwachstellen in der DNS-Infrastruktur, die viele Unternehmen einmal eingerichtet haben und dann vernachlässigen. Wir empfehlen unseren Kunden dringend, die verfügbaren Tools und Empfehlungen zu nutzen, um ihre digitale Infrastruktur zu sichern“.

Die Schwere der Angriffe veranlasste mehrere staatliche und internationale Organisationen zur Reaktion mit Richtlinien und Warnungen – ein beispielloser Vorgang im Bereich Domain-Sicherheit.

„Domain- und DNS-Hijacking sind keine neuen Sicherheitsbedrohungen. Darum haben wir das CSC Security Center entwickelt. Uns spornt an, dass es von Hunderten der weltweit größten Unternehmen genutzt wird, um diese für ihr Geschäft entscheidenden Online-Elemente zu schützen“, erläutert Mark Calandra, General Manager von CSC Digital Brand Services. „Die Raffinesse und die Auswirkungen der jüngsten Angriffswelle dienen als Weckruf, der die effektive Verwaltung von Domainnamen, DNS und digitalen Zertifikaten zu einer entscheidenden Komponente für die Verbesserung des Sicherheitsniveaus eines jeden Unternehmens mit einer Online-Präsenz machen muss“.

In unserem Blogbeitrag ***Confused About Domain Locks? Understand the Intricacies and Security Effectiveness*** *(Verstehen der Komplexität von Domain-Locks und ihrer Wirksamkeit für die Sicherheit) erfahren Sie mehr über das Risiko von DNS-Hijacking und darüber, wie man dieses Risiko mindern kann.*

Vier zentrale Richtlinien, die jedes Unternehmen für geschäftskritische Domains haben sollte:

Obligatorische Multi-Faktor-Authentifizierung zur Kontrolle des Benutzerzugriffs

Richtlinie für die automatische Verlängerung, um abgelaufene und verlorene Domains zu vermeiden

Auto-Lock-Richtlinie zur Verhinderung unbefugter Änderungen an Domains

Richtlinie zu digitalen Zertifikaten, die festlegt, welche Zertifizierungsstelle verwendet werden kann

Digital Asset Management ist mehr als die Verwaltung von Domain-Erneuerungen, Modifikationen und das Ersetzen von digitalen Zertifikaten. Wir sind davon überzeugt, dass wir unsere Kunden mit innovativer Technologie und branchenführenden Dienstleistungen aktiv bei der Umsetzung und Regulierung ihrer Richtlinien unterstützen können. Wir helfen unseren Kunden, ihr Unternehmen vor den Gefahren jenseits der Firewall zu schützen.

Um mehr über die Grundlagen der Domain-Sicherheit zu erfahren, lesen Sie bitte unsere Publikation **„Sicherheit digitaler Assets: Zurück zu den Grundlagen“.**

cscdigitalbrand.services/de