opentext™ | Cybersecurity

WHITEPAPER

Webroot DNS Protection

Schützen Sie Ihre Mitarbeiter und Ihr Netzwerk überall vor webbasierten Bedrohungen

Das Internet gehört zum heutigen Arbeitsalltag. Mitarbeiter müssen das Internet für unzählige arbeitsbezogene Zwecke nutzen, aber ohne sichere, private und sichtbare Kontrolle über den Internetdatenverkehr können Unternehmen einer Vielzahl von Sicherheitsbedrohungen ausgesetzt sein.

Das liegt daran, dass das Domain Name System (DNS) ein begehrter Angriffsvektor für böswillige Akteure ist. Das DNS ist ein Internetsystem zur Zuordnung von Internet Protocol (IP)-Adressen zu Domainnamen. Einfach ausgedrückt, interpretiert das DNS menschenfreundliche Hostnamen in PC-freundliche IP-Adressen.

Da das DNS als Adressbuch für das Internet dient, bietet es Bedrohungsakteuren standardmäßig Einblick in den Inhalt jeder Anfrage, und die Integrität der Anfrage kann gefährdet werden. Es ist daher nicht verwunderlich, dass Cyberkriminelle zunehmend DNS-Anfragen für ihre Angriffe nutzen:

- Mehr als ein Drittel aller Angriffe werden über DNS durchgeführt[1]
- Phishing und Malware sind die zwei häufigsten DNS-basierten Angriffe, denen Unternehmen ausgesetzt sind[2]
- 43 % der Unternehmen sichern ihre DNS-Server nicht[2]

80 %

der Malware führen Angriffe über das DNS aus.

Ungeschützt stellt das DNS ein Sicherheitsproblem für Unternehmen dar, da 80 % der Malware über das DNS Angriffe auslöst und Daten stiehlt.[3] Da Unternehmen häufig Remote- und Hybrid-Arbeitsmodelle anbieten, dient die Netzwerkfirewall nicht mehr als einzige, sichere Lösung für die Websicherheit. Diese Marktdynamik führt dazu, dass Unternehmen DNS-Sicherheit einführen müssen.

DNS-Sicherheit bietet eine Schutzebene zwischen einem Mitarbeiter und dem Internet, indem der Zugriff auf unangemessene Websites durch die Nutzung von intelligenten Bedrohungsdaten blockiert wird. Natürlich muss die richtige Lösung auch den Datenschutz maximieren, ohne die Sicherheit und Betriebseffizienz zu beeinträchtigen. Durch die Einführung von DNS-Sicherheit können Unternehmen ihre Netzwerke besser kontrollieren und gleichzeitig die Sicherheit und den Datenschutz gewährleisten, die erforderlich sind, um ihre Benutzer (egal, ob sie sich an einem anderen Ort oder im Büro befinden) vor dem Zugriff auf schädliche Websites zu schützen.

In diesem Whitepaper werden die Sicherheitsprobleme untersucht, die das DNS mit sich bringt, und wie Webroot DNS Protection Unternehmen hilft, sich vor den Risiken webbasierter Bedrohungen zu schützen.

Der Internetzugang ist für das heutige „Online"-Arbeitsleben unerlässlich. Aber welche Sicherheitsrisiken ergeben sich daraus für Unternehmen?

Remote-Mitarbeiter benötigen zusätzliche Sicherheit

Bei der heutigen Remote- und Hybrid-Belegschaft arbeiten viele Benutzer mit Ihren Geräten zu Hause, unterwegs oder im örtlichen Café. Da die Internetnutzung nicht mehr durch die Unternehmensfirewall eingeschränkt wird, um böswillige Akteure fernzuhalten, vergrößert sich die Angriffsfläche der digitalen Umgebung des Unternehmens.

Sicherheitsverantwortliche sind sich einig, dass diese erweiterte Angriffsfläche ein Problem darstellt: 66 % der CISOs gaben an, dass Remote-Arbeit ihre Organisation anfälliger für Cyberangriffe macht.[4]

Erfolgreiche Angriffe führen zu finanziellen Verlusten

Das DNS wurde in erster Linie entwickelt, um Internetanfragen korrekt und effizient zu beantworten und nicht, um deren Absicht zu hinterfragen. Infolgedessen sind Cyberangriffe, die das DNS nutzen, zu einer der größten Bedrohungen für das moderne Arbeitsleben geworden.

Tatsächlich waren fast 79 % der Unternehmen bereits von DNS-Angriffen betroffen, und sie kosten zudem viel Geld. Jeder erfolgreiche DNS-Angriff kostet Unternehmen durchschnittlich 924.000 USD. [5]

Angriffe führen zu Betriebsausfällen

Cyberkriminelle nutzen eine Reihe von Techniken, um ihre DNS-Angriffe auszulösen und ihre Schaddaten zu übermitteln. Einmal drinnen, kann der Angreifer Malware installieren, vertrauliche Daten stehlen, Code ändern und sogar neue Zugangspunkte installieren.

Wir alle kennen die Horrorgeschichten: Ein einziger erfolgreicher Angriff kann den Betrieb stören und IT-Teams wochenlang mit der erfolgreichen Wiederherstellung der Systeme beschäftigen. In der Tat mussten 82 % der Unternehmen aufgrund von DNS-Angriffen erhebliche Ausfallzeiten ihrer Anwendungen hinnehmen, unabhängig davon, ob sie intern oder in der Cloud betrieben wurden.[5]

Ein moderner Ansatz zum Schutz des Internetzugangs: Webroot DNS Protection

Webroot macht es Unternehmen leicht, DNS-Sicherheitsrisiken mit präzisem, effektivem Schutz für alle Ihre Benutzer zu begegnen, egal ob sie remote oder im Büro arbeiten.

Webroot DNS Protection schützt Ihr Netzwerk und Roaming-Benutzer, indem es das DNS filtert und Malware und andere netzwerkbasierte Angriffe eliminiert. Unsere DNS Protection basiert auf unserer branchenführenden BrightCloud Threat Intelligence, die ML und KI der sechsten Generation nutzt, um Ihrem Unternehmen eine zeitnahe und genaue Filterung von Domänen, URLs und IP-Adressen zu ermöglichen. Außerdem unterstützt unsere Lösung uneingeschränkt DoH (DNS over HTTPS), um sicherzustellen, dass alle verschlüsselten DNS-Anfragen sicher und genau sind.

Schützen Sie Ihr Unternehmen mit Webroot DNS Protection

Das DNS ist darauf ausgelegt, Internetanfragen einfach aufzulösen und sie in ihre eindeutigen IP-Adressen (Internet Protocol) zu übersetzen. Dadurch kann dieser Klartextdienst auf viele verschiedene Arten für Cyberangriffe ausgenutzt werden. Mit Webroot DNS Protection kann sich Ihr Unternehmen vor den mit dem DNS verbundenen Sicherheitsrisiken schützen.

Webroot DNS Protection ermöglicht Ihnen, das Netzwerk Ihres Unternehmens zu kontrollieren und gleichzeitig die Sicherheit und den Datenschutz zu gewährleisten, die erforderlich sind, um Ihre Benutzer (Remote- und Roaming-Benutzer) vor dem Zugriff auf bösartige Websites zu schützen.

Remote-Schutz

Webroot bietet eine effektive DNS-Sicherheitsebene zum Schutz Ihrer Remote-Mitarbeiter. Mit dem DNS Protection Agent können alle DNS-Anfragen (auch von Remote-Benutzern) gefiltert und protokolliert werden, unabhängig davon, welche Internetverbindung verwendet wird. Richtlinien können auf Gruppen- oder individueller Ebene festgelegt werden, um den Zugriff auf schädliche und nicht autorisierte Domänen zu beschränken und Sicherheitsverletzungen zu stoppen, bevor sie das Netzwerk beeinträchtigen.

Präzise Filterung

Unsere DNS Protection basiert auf unserer BrightCloud Threat Intelligence (BCTI), die ML und KI der sechsten Generation nutzt, um eine zeitnahe und präzise DNS-Filterung bereitzustellen. DNS-Anfragen werden präzise gefiltert und Phishing- und Malware-Seiten in Echtzeit blockiert, während Unternehmen der Verwaltungsaufwand für Fehlalarme erspart bleibt.

Unterstützung für DNS over HTTPS (DoH)

Mit der Einführung von DoH ist es schwierig geworden, den verschlüsselten DNS-Verkehr zu kontrollieren. Webroot begegnet diesem Problem mit unserer Lösung, die DoH vollständig unterstützt. Der Webroot DNS Protection-Remote-Agent nutzt außerdem DoH für die gesamte Kommunikation mit dem Core, bietet eine sichere DNS-Auflösung und stellt gleichzeitig sicher, dass die gesamte Kommunikation verschlüsselt ist und von einer vertrauenswürdigen Quelle stammt. Auf diese Weise können Unternehmen die Empfehlungen der NSA erfüllen.

Flexible Bereitstellungsoptionen

Webroot DNS Protection bietet zwei Bereitstellungsoptionen: als eigenständige Lösung oder in Kombination mit Webroot Endpoint Protection (EPP). Der DNS Protection Agent kann direkt auf einem System installiert oder über Webroot EPP verwaltet werden. Die Webroot EPP-Option bietet einen integrierten Ansatz, der es Unternehmen ermöglicht, Endpunkt- und DNS-Sicherheit zentral zu verwalten. Diese Kombination kann dazu beitragen, in Ihr Unternehmen eindringende Bedrohungen um etwa 33 % zu reduzieren. Die eigenständige DNS-Option ermöglicht es Unternehmen, Webroot DNS Protection als Sicherheitsebene bereitzustellen und gleichzeitig vorhandene Investitionen in eine EPP- oder EDR-Lösung eines Drittanbieters separat zu nutzen.

Einfache Verwaltung

DNS Protection lässt sich ganz einfach über die Webroot Management Console verwalten, die eine zentrale Oberfläche für die Verwaltung aller Webroot-Produkte bietet. Über die Konsole können Kunden DNS Protection schnell bereitstellen und verwalten, wodurch IT- und Sicherheitsteams den Verwaltungsaufwand reduzieren und die Effizienz steigern können.

Helpdesk-Kosten werden reduziert

DNS Protection verhindert, dass Bedrohungen über die DNS-Ebene in Ihr Unternehmen eindringen. Dadurch wird die Zahl der Kompromittierungen und Infektionen sowie die damit verbundenen Kosten für die Behebung von Problemen reduziert, mit denen Ihre IT-Mitarbeiter konfrontiert werden. Dies trägt dazu bei, die Anzahl der Anrufe bei Ihrem Helpdesk aufgrund von Infektionen zu reduzieren.

Eine Erfolgsgeschichte: Mit Webroot DNS Protection reduziert MSP Helpdesk-Anrufe um 40 %

Sedona Technologies wurde 1986 gegründet und ist ein großer und etablierter IT- und Engineering-Dienstleister mit einer erfolgreichen Managed-Services-Abteilung. Das Unternehmen hat Niederlassungen in über 30 Städten der USA und erzielt einen Jahresumsatz von über 110 Millionen USD.

DNS-Sicherheitsherausforderungen

Als der MSP sein Angebot an Sicherheitsdiensten um Schutz auf Netzwerkebene erweitern wollte, stieß er in der Einführungsphase einer proxy-basierten Lösung auf Schwierigkeiten. Bei Sedona-Kunden, deren Benutzer DNS-Anfragen an schädliche Websites stellten, kam es häufig zu Infektionen.

„Ursprünglich haben wir uns nicht für eine DNS-Lösung entschieden, sondern eher für eine proxy-basierte Lösung. Aber die Zusammenarbeit mit unserem Partner gestaltete sich sehr schwierig. Die Anzahl der Schritte, die nötig waren, um das Produkt für einen Kunden zum Laufen zu bringen, erforderte weit mehr Ressourcen als vorgesehen."

Dies veranlasste Sedona dazu, andere Möglichkeiten zu prüfen, um seine Kunden zu schützen und gleichzeitig Ressourcen zu schonen.

Vorteile von Webroot DNS Protection

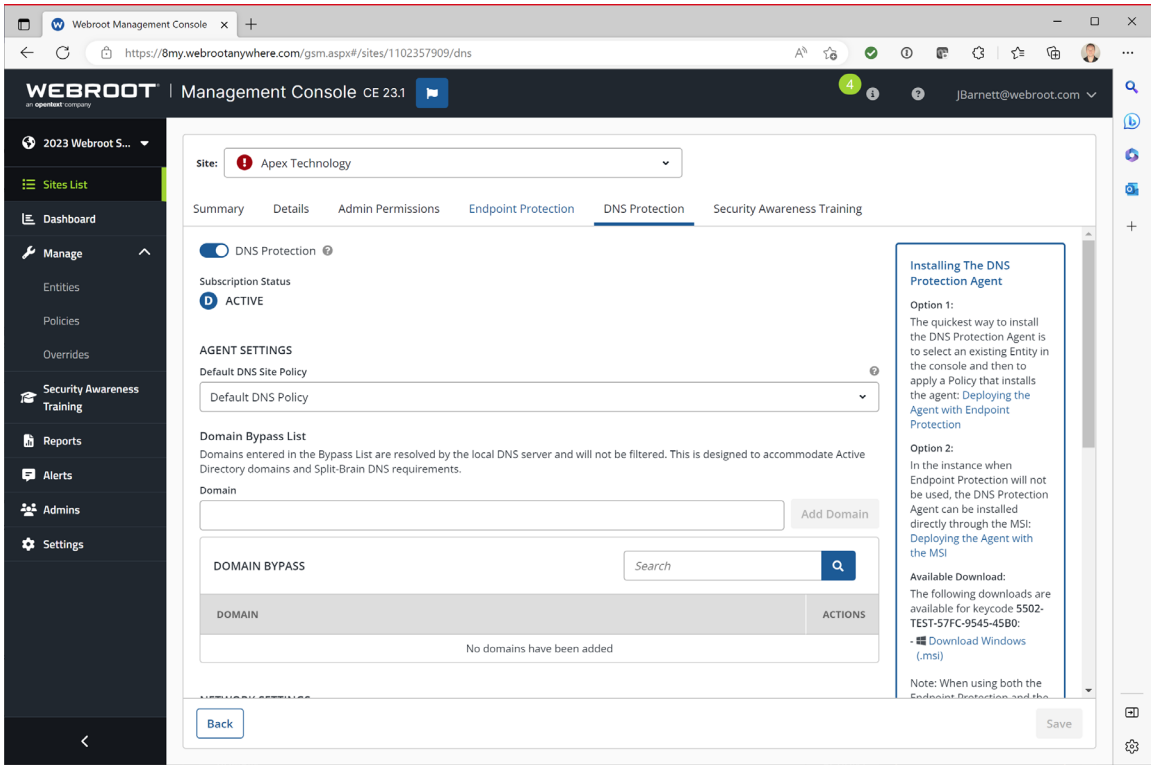
„Wir brauchten eine einfachere, optimierte Lösung. Wir haben viele Produkte von verschiedenen Anbietern evaluiert, und die Entscheidung für Webroot basierte letztendlich auf der Erfahrung aus der direkten Zusammenarbeit mit den Mitarbeitern. Sie haben zugehört. Es gab keine Verzögerungen. Das Serviceniveau übertraf einfach alles andere.“

Was geschah, nachdem Sedona zu Webroot DNS Protection wechselte?

- Täglich werden 270 Internet-Bedrohungen im gesamten Kundenstamm blockiert
- 51 Spear-Phishing-Versuche wurden monatlich in einem einzigen Quartal abgewehrt
- 40 % weniger Helpdesk-Anrufe

„Für unsere Kunden mit DNS Protection sind die Helpdesk-Anrufe um fast 40 % zurückgegangen.“

– Jason Ballard
IT-Lösungsmanager
Sedona Technologies



1. Global Cyber Alliance, 2021
2. EfficientIP 2022 Global DNS Threat Report, conducted by IDC
3. Cyber Theory. The Threats from Unsecured DNS and Domains.
4. Verizon. Mobile Security Index. 2022.
5. Webinar Care. DNS Security Statistics 2023. January 2023.

opentext™ | Cybersecurity

OpenText Cybersecurity bietet umfassende Sicherheitslösungen für Unternehmen und Partner jeder Größe. Von Prävention, Erkennung und Reaktion bis hin zu Wiederherstellung, Untersuchung und Compliance hilft unsere einheitliche End-to-End-Plattform Kunden dabei, Cyberresilienz über ein ganzheitliches Sicherheitsportfolio aufzubauen. Angetrieben durch umsetzbare Erkenntnissen unserer Echtzeit- und Kontext-Bedrohungsintelligenz profitieren OpenText Cybersecurity-Kunden von hochwirksamen Produkten, einer konformen Erfahrung und vereinfachter Sicherheit, um das Management von Geschäftsrisiken zu unterstützen. WP_021323