

DNS Security



Häufig unterschätzt, aber unverzichtbar
- die erste Linie der Cyberverteidigung

Warum ist DNS Security der Schlüssel zu sicherem Surfen und ein wirksamer Schutz vor Cyberkriminalität?

In unserem Whitepaper finden Sie Best Practices für die Implementierung einer DNS-Abwehr als Grundschutz Ihrer IT-Organisation.

Über den Autor

Felix Lange ist seit Dezember 2018 Teil des avodaq Teams. Er arbeitet dort als Senior Security Consultant und Team Lead im Bereich Infrastruktur Security. Seine Leidenschaft für Netzwerke und IT-Security wurde bereits in der Abiturientenberufsausbildung zum Industrietechnologen geweckt und prägt seither seinen beruflichen Weg.

Felix bringt bei avodaq nicht nur sein tiefes technisches Know-how ein, sondern auch seine Begeisterung für die Zusammenarbeit mit verschiedensten Kunden und anderen Fachbereichen. Die Vielfalt und Komplexität unterschiedlichster IT-Umgebungen motivieren ihn jeden Tag aufs Neue.



Inhaltsverzeichnis

- 4 Management Summary
- 5 Warum ist das DNS ein Einfallstor für Cyberangriffe?
- 6 So funktioniert DNS Security
- 8 Typische Bedrohungsszenarien
und wie DNS Security dagegen helfen kann
- 10 Implementierung von DNS Security
Schritt für Schritt zu einem besseren Schutz
- 12 Wie unterscheiden sich Lösungen für DNS Security?
- 14 Sicherheitsmaßnahmen ganzheitlich denken
- 15 DNS Security im Einsatz
- 16 Fazit

Management Summary

Der Großteil der Cyberangriffe läuft über das Internet und dessen Domain Name System (DNS). Daher kann bereits ein vorschneller Mausklick über die Zukunft der Organisation entscheiden. Mit einer Lösung zur DNS Security lässt sich schnell und wirkungsvoll vorbeugen: Der Service checkt Web Domains und blockiert Zugriffe, bevor schadhafte Software in das eigene Netzwerk gelangt.

Das Internet hat der Menschheit zweifellos viel gebracht: Man kann dort Informationen finden, Services buchen und Produkte kaufen – aber sich auch gefährliche Software direkt auf den Rechner laden. Etwa von schadhaften Websites, auf die man gelangt, wenn man in einer E-Mail auf den falschen Link klickt. Das Domain Name System (DNS) des Internets ist kompromisslos: Es leitet das Opfer umgehend weiter zur Malware.

Dabei gibt es eine effektive Methode, um sich und seine Organisation vor Bedrohungen wie Ransomware und Phishing zu schützen: DNS Security. Das Verfahren ist erprobt, schnell, einfach und skalierbar, denn es blockt einen Großteil der Angriffe ab und kommt als Service aus der Cloud.

In diesem Whitepaper erfahren Sie, wie DNS Security funktioniert und weshalb es entscheidend ist, den Schutzmechanismus zu implementieren. Laut aktueller Studienlage nutzen über 90 Prozent der Malware das DNS, um Daten zu entwenden, Traffic umzuleiten oder mit den Angreifern zu kommunizieren.

Zudem geht das Whitepaper auf konkrete Bedrohungsszenarien ein, erläutert schrittweise die Implementierung und verweist auf Best Practices, um DNS Security optimal einzusetzen.

Mit DNS Security schützen Sie Ihr Unternehmen vor Malware, Phishing und Command-&-Control-Servern – und Sie reduzieren das Risiko, zum Opfer von Cyberangriffen zu werden.

90%

der Malware nutzt das DNS