HAW HAMBURG

Bachelorarbeit

Kevin Hüsgen

DNS-Sicherheit am Beispiel eines mittelständischen Softwareunternehmens

Fakultät Technik und Informatik
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

Kevin Hüsgen

DNS-Sicherheit am Beispiel eines mittelständischen Softwareunternehmens

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Angewandte Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr.-Ing. Martin Hübner
Zweitgutachter: Prof. Dr. Klaus-Peter Kossakowski

Eingereicht am: 08.12.2020

Kevin Hüsgen

Thema der Arbeit

DNS-Sicherheit am Beispiel eines mittelständischen Softwareunternehmens

Stichworte

DNS, IT-Sicherheit, IT-Grundschutz, DNSSEC, DNS-over-TLS, DNS-over-HTTPS, Bedrohungsanalyse, Risikoanalyse, DNS-Sicherheit, DNSCurve, DNS-Cookies, TSIG, DoT, DoH

Kurzzusammenfassung

Das Ziel dieser Forschungsarbeit ist es, die Sicherheit von DNS anhand eines fiktiven, mittelständischen Softwareunternehmens aus der Versicherungsbranche zu analysieren. Dazu werden die Schwachstellen, Bedrohungen und Angriffe beim Betrieb von DNS analysiert und die Risiken für das Unternehmen evaluiert. Es werden DNS-Sicherheitserweiterungen vorgestellt und die identifizierten Bedrohungen im Hinblick auf diese überprüft. Ein Maßnahmenkatalog wurde erarbeitet, um die Risiken zu vermeiden oder zu reduzieren. Zum Schluss werden Empfehlungen ausgesprochen und im Bezug auf das Anwendungsszenario priorisiert.

Kevin Hüsgen

Title of Thesis

DNS security using the example of a medium-sized software company

Keywords

DNS, IT-Security, DNSSEC, DNS over TLS, DNS over HTTPS, Threat analysis, Risk analysis, DNS Security, DNSCurve, DNS Cookies, TSIG, DoT, DoH

Abstract

The goal of this research project is to analyze the security of DNS using a fictitious, medium-sized software company from the insurance industry. For this purpose, the weak points, threats and attacks in the operation of DNS are analyzed and the risks for the

company are evaluated. DNS security enhancements will be presented and the identified threats will be reviewed with regard to them. A catalog of measures was developed to prevent or reduce the risks. Finally, recommendations are made and prioritized in relation to the application scenario.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungen

ACL Access Control List.

BSI Bundesamt für Sicherheit in der Informationstechnik.

BYOD Bring-your-own-Device.

C&C Command-and-Control.

CA Certificate Authority.

CRL Certificate Revocation List.

CVE Common Vulnerabilities and Exposures.

DDoS Distributed-Denial-of-Service.

DHCP Dynamic Host Configuration Protocol.

DMZ Demilitarisierte Zone.

DNS Domain Name System.

DNSSEC Domain Name System Security Extensions.

DoDTLS DNS-over-DTLS.

DoH DNS-over-HTTPS.

DoS Denial-of-Service.

DoT DNS-over-TLS.

DTLS Datagram Transport Layer Security.

FQDN Fully Qualified Domain Name.

HMAC Keyed-Hash Message Authentication Code.

HTTP Hypertext Transport Protocol.

HTTPS Hypertext Transport Protocol Secure.

IANA Internet Assigned Numbers Authority.

IETF Internet Engineering Task Force.

ISC Internet Systems Consortium.

ISP Internet Service Provider.

KSK Key-Signing-Key.

MAC Message Authentication Code.

MTU Maximum Transmission Unit.

NIC Network Information Center.

NSA National Security Agency.

NTP Network Time Protocol.

PKI Public-Key-Infrastruktur.

POSIX Portable Operating System Interface.

PRSD Pseudorandom Subdomain Attack.

RCE Remote Code Execution.

RFC Request for Comments.

RPZ Respone Policy Zone.

RR Resource Record.

RRL Response Rate Limiting.

SaaS Software as a Service.

SLD Second-Level-Domain.

SOP Same-Origin-Policy.

SSH Secure Shell.

SSL Secure Socket Layer.

SSRF Server-Side-Request-Forgery.

TCP Transmission Control Protocol.

TLD Top-Level-Domain.

TLS Transport Layer Security.

TTL Time to Live.

UDP User Datagram Protocol.

VPN Virtual Private Network.

ZSK Zone-Signing-Key.

Auflistungen

1 Einleitung

1.1 Motivation

Das Domain Name System (DNS) ist eines der wichtigsten Protokolle im Internet, da es fast jeder Interaktion vorangeht. Aufgrund der Notwendigkeit von DNS ist es auch für Angreifer ein lukratives Angriffsziel. Der 2020 Global DNS Threat Report, der jährlich veröffentlicht wird, zeigt, dass 79% der befragten Unternehmen in der ersten Jahreshälfte 2020 einen DNS-Angriff wahrgenommen haben. Die durchschnittlichen Kosten eines Angriffs beliefen sich dabei auf 924.000$. 82% der Angriffe verursachten einen Ausfall der Infrastruktur. Dabei betrug die durchschnittliche Zeit für die Wiederherstellung 5,25 Stunden. 21% der Angriffe konnten erst nach sieben Stunden verhindert werden [47].

Der Bericht zeigt, dass DNS-Sicherheit immer wichtiger wird. Gaben 2019 noch 64% der Unternehmen an, DNS-Sicherheit als kritische Komponente in ihrer Infrastruktur zu betrachten, sind es 2020 schon 77% der Unternehmen [47].

Auch in der Vergangenheit gab es immer wieder größere IT-Sicherheitsvorfälle, die die DNS-Infrastruktur bedroht oder für Angriffe ausgenutzt haben. Einer der größten Cyberattacken der letzten Jahre wurde auf eine brasilianische Bank mittels DNS durchgeführt. Die Bank, die nicht näher genannt wurde, besitzt 5 Millionen Kunden und über 500 Filialen. Im Oktober 2016 haben Angreifer die DNS-Einträge der Bank geändert und somit die Kontrolle über die gesamte Infrastruktur der Bank übernommen. Anstelle der legitimen Webseite wurden Kunden auf gefälschte Webseiten umgeleitet und Passwörter gestohlen. Zusätzlich wurden sie beim Besuch mit Malware infiziert. Laut Kaspersky wurden auch Transaktionen über Bankautomaten auf die Server der Angreifer umgeleitet. Da die interne Infrastruktur genauso betroffen war, konnten keine E-Mails verschickt werden, um die Kunden über den Angriff zu informieren. Erst nach sechs Stunden konnte die DNS-Infrastruktur wieder unter die Kontrolle der Bank gebracht werden [53].

Dieser Angriff hat gezeigt, dass eine Übernahme des DNS gesamte Unternehmen für mehrere Stunden handlungsunfähig machen kann. Aufgrund der permanent fortschreitenden Vernetzung von Systemen durch das Internet der Dinge und neuen Architekturmustern wie Microservices wird DNS und DNS-Sicherheit sogar noch wichtiger [61].

1993 wurden die ersten Sicherheitsbedenken im Umgang mit DNS geäußert [50]. Daher wurde 1999 eigens der Standard Domain Name System Security Extensions (DNSSEC) eingeführt, um DNS mittels Signierung der DNS-Daten sicherer zu machen [45]. DNSSEC konnte sich allerdings bis heute nicht flächendeckend durchsetzen [37]. Durch neue Technologien wie DNS-over-TLS und DNS-over-HTTPS, die im März 2016 [60] und Oktober 2018 [57] definiert wurden und von etablierten Unternehmen wie Google oder Mozilla vorangetrieben werden, wurde die Diskussion um DNS-Sicherheit und -Privatsphäre neu entfacht [89].

1.2 Problemstellung und Zielstellung

Ziel der Arbeit ist es, anhand eines fiktiven Anwendungsszenarios Risiken, die bei der Verwendung von DNS auftreten, aufzuzeigen und mittels verschiedener DNS-Sicherheitserweiterungen zu überprüfen. Es soll außerdem ein Maßnahmenkatalog vorgestellt werden, mit dem das Risiko einer Bedrohung durch DNS reduziert werden kann. Zusätzlich sollen Empfehlungen für den Umgang mit DNS, im Bezug auf das Anwendungsszenario, ausgesprochen werden.

Dazu wurden drei Forschungsfragen definiert, die in dieser Arbeit beantwortet werden sollen:

1. Welche Bedrohungen ergeben sich, insbesondere für das Anwendungsszenario, durch die Nutzung von DNS?
2. Bei welchen Bedrohungen können die DNS-Sicherheitserweiterungen zum Einsatz kommen, um das Bedrohungsrisiko zu minimieren?
3. Welche DNS-Sicherheitserweiterungen und Maßnahmen eignen sich, insbesondere im Bezug auf das Anwendungsszenario, für die beschriebenen Bedrohungen?

1.3 Aufbau der Arbeit

Zunächst werden die Grundlagen von DNS erläutert und kryptografische Konzepte, die für ein Verständnis der DNS-Sicherheitserweiterungen nötig sind, eingeführt. Danach wird das Anwendungsszenario beschrieben und die Motive für eine hohe IT-Sicherheit erläutert. Im Bezug auf das Anwendungsszenario wird im Anschluss eine Bedrohungsanalyse durchgeführt. Die Bedrohungsanalyse gliedert sich in drei Teile. Zunächst werden die Systeme, die DNS verwenden, identifiziert. Die identifizierten Systeme werden im zweiten Teil benötigt, um die Bedrohungen, die sich gegen eine DNS-Infrastruktur ergeben, aufzuzeigen. Im letzten Teil der Bedrohungsanalyse wird eine Risikoanalyse durchgeführt, indem die identifizierten Bedrohungen anhand der identifizierten Systeme evaluiert werden. Im Kapitel 5, der Evaluation, werden die DNS-Sicherheitserweiterungen vorgestellt und aufgezeigt, welche Bedrohungen durch die Nutzung der jeweiligen Erweiterung reduziert oder sogar ausgeschlossen werden können. Außerdem werden neue Bedrohungen und Risiken beschrieben, die sich durch die Nutzung der DNS-Sicherheitserweiterungen ergeben. Nachdem die DNS-Sicherheitserweiterungen behandelt wurden, wird ein allgemeiner Maßnahmenkatalog vorgestellt. Im letzten Teil der Evaluation werden geeignete Maßnahmen aus diesem Katalog für das Anwendungsszenario ausgesucht und priorisiert. Zum Schluss werden die Ergebnisse zusammengefasst und diskutiert sowie ein Ausblick auf zukünftige Entwicklungen gegeben. Außerdem wird überprüft, ob die Forschungsfragen ausreichend beantwortet wurden.

1.4 Zielgruppe

Die Arbeit richtet sich an Personen, die sich mit DNS oder DNS-Sicherheit beschäftigen. Insbesondere für DNS- und Systemadministratoren, die eine DNS-Infrastruktur betreuen oder einführen wollen, ist diese Arbeit interessant. Aber auch IT-Sicherheitsexperten und IT-Führungskräfte können mit dieser Arbeit ihre DNS-Infrastruktur überprüfen. Dazu kann der vorgestellte Bedrohungskatalog auf das eigene Anwendungsszenario abgebildet und mittels der vorgestellten Maßnahmen evaluiert werden.

1.5 Einordnung und Abgrenzung

Diese Arbeit untersucht DNS und DNS-Sicherheit an einem fiktiven Fallbeispiel. Insbesondere die Risikoanalyse und die Empfehlungen der Maßnahmen werden speziell auf das Anwendungsszenario abgestimmt und sind daher nicht universell einsetzbar. Die Bedrohungsanalyse und die Betrachtung der DNS-Sicherheitserweiterungen sowie der Maßnahmenkatalog werden möglichst allgemein gehalten, damit diese als Grundlage für die Evaluation anderer Anwendungsszenarien genutzt werden können. Es wird bewusst nur DNS und ausgewählte DNS-Sicherheitserweiterungen betrachtet. Die DNS-Sicherheitserweiterungen werden nach Aktualität und Popularität ausgewählt. Dabei werden existierende Standards genauso wie aktuelle Entwürfe betrachtet. Auf ein ganzheitliches IT-Sicherheitskonzept für das Anwendungsszenario wird verzichtet. Andere Protokolle und Systeme werden nicht betrachtet. Die Vorgehensweise orientiert sich am IT-Grundschutz. Es gibt weitere Vorgehensweisen, wie beispielsweise die ISO-Reihe 27000, die in dieser Arbeit aber nicht betrachtet werden.

DNS und DNS-Sicherheit ist Gegenstand zahlreicher Forschungen und Veröffentlichungen. D. Atknis et al. veröffentlichten 2004 das erste Request for Comments (RFC), das die Bedrohungen gegen DNS betrachtet [15]. Insbesondere wurden die Bedrohungen betrachtet, die durch den Einsatz von DNSSEC verhindert werden sollen. Chandramouli und Rose vom National Institute of Standards and Technology (NIST) haben 2013 einen umfassenden Katalog zum sicheren Betrieb von DNS veröffentlicht [32]. 2015 wurden von Bortzmeyer die Probleme der Privatsphäre von DNS im RFC 7626 ausführlich beschrieben [20]. Lösungsmöglichkeiten wurden allerdings nicht vorgestellt.

2 Grundlagen

2.1 IT-Sicherheit

IT-Sicherheit beschäftigt sich mit der Sicherheit von informationstechnischen Systemen. Ein IT-System wird von Eckert als ein „geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen“[46, S. 3] definiert. In diesen IT-Systemen sind die Informationen und Daten die Güter, die durch die IT-Sicherheit geschützt werden sollen. Dabei wird auf drei Schutzziele der Informationssicherheit zurückgegriffen:

- (Informations-)Vertraulichkeit: Schutz vor unautorisierter Informationsgewinnung
- (Daten-)Integrität: Schutz vor unbefugter Datenänderung
- (System-)Verfügbarkeit: Schutz vor Störung und Ausfällen

Diese Schutzziele beschreiben die Anforderungen an sichere IT-Systeme. Sie können bei der Entwicklung neuer und der Evaluation bestehender Systeme eingesetzt werden. Security Engineering beschreibt eine systematische Vorgehensweise, um die Sicherheit von IT-Systemen zu evaluieren. Dabei werden zunächst die zu schützenden Güter identifiziert und dann überprüft, welche Bedrohungen für die identifizierten Güter existieren. Danach wird anhand der Eintrittswahrscheinlichkeit und der Schadenshöhe das jeweilige Risiko klassifiziert. Es wird versucht die Risiken mittels geeigneter Maßnahmen zu reduzieren. Zur Beibehaltung des Sicherheitsniveaus muss dieser Prozess in regelmäßigen Abständen durchgeführt werden [46].

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Vorgehensweise IT-Grundschutz entwickelt, um die Komplexität zur Erreichung eines ausreichenden Schutzbedarfs zu verringern. Im Gegensatz zum klassischem Security Engineering wird

beim IT-Grundschutz auf eine Risikoanalyse verzichtet und von allgemeinen Gefährdungen je System ausgegangen. Zusätzlich werden Maßnahmen für einen angemessenen Schutzbedarf empfohlen [27].

2.2 DNS

Das Domain Name System ist ein verteiltes System, dessen Hauptaufgabe die Beantwortung von Anfragen zur Namensauflösung ist. Dabei kann DNS mittels Vorwärtsauflösung zu einem Hostnamen eine IP-Adresse zurückliefern oder durch die Rückwärtsauflösung zu einer IP-Adresse den zugehörigen Hostname ermitteln [75]. Dadurch ist es möglich, dass sich Menschen nur einprägsame und aussagekräftige Namen wie *haw-hamburg.de* und nicht *134.28.219.14* merken müssen. DNS wird daher oft mit einem Telefonbuch verglichen [71].

DNS wurde erstmals 1983 von Paul Mockapetris, einem US-amerikanischen Informatiker, beschrieben [73] und 1987 in den Request for Comments (RFC) 1034 und 1035 standardisiert [75, 74].

DNS wird als verteilte, hierarchische Datenbank implementiert und kann als Wurzelbaum dargestellt werden. Abbildung 2.1 zeigt den Aufbau schematisch auf. Die Wurzel (dargestellt in Orange) wird als Root-Zone bezeichnet. Unterhalb der Root-Zone befinden sich die Top-Level-Domains (kurz TLD, dargestellt in Blau). Die TLDs wiederum beinhalten Second-Level-Domains (kurz SLD, dargestellt in Grün), die im Sprachgebrauch häufig nur als Domain bezeichnet werden. Unterhalb einer SLD können weitere Knoten liegen, die jeweils als Sub-Domain (dargestellt in Rot) bezeichnet werden. Eine Domain ist somit ein Teilbaum des gesamten Wurzelbaums. Ein Blatt des Baums beschreibt einen Host (dargestellt in Lila). Der vollständige Name des Hosts wird als Fully Qualified Domain Name (FQDN) bezeichnet und ergibt sich durch die Verkettung aller Vorgänger bis zur Wurzel, wobei zwischen den Knoten jeweils ein Punkt gesetzt wird [78, 17, 58]. Der FQDN des Hosts *users* lautet somit *users.informatik.haw-hamburg.de.*[1].

Die Root-Zone wird von 13 Nameservern verwaltet, die die Adressen A.root-servers.net bis M.root-servers.net besitzen. Tatsächlich stecken hinter den 13 Nameservern jedoch

[1] Der letzte Punkt beschreibt die Root-Zone und wird bei vielen Anwendungen (bspw. Browser) weggelassen

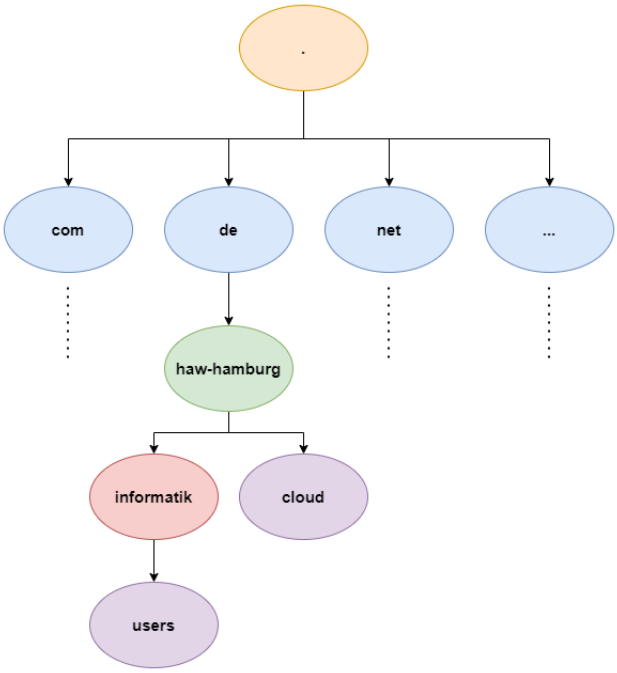


Abbildung 2.1: Schematischer Aufbau der DNS Hierarchie am Beispiel der HAW-Domain

hunderte von Servern, die an unterschiedlichen Orten in der Welt verteilt sind und mittels Anycast, einer Adressierungsart, bei der verschiedene Server dieselbe IP-Adresse besitzen, adressiert werden. Ein Nameserver bezeichnet dabei einen DNS-Server, der für eine bestimmte Domain verantwortlich ist [17]. Dabei ist zudem möglich, dass ein Nameserver Verantwortung durch Delegierung an andere Nameserver abgibt. Die Root-Zone wird von der Internet Assigned Numbers Authority (IANA) betrieben und beinhaltet die Verweise zu den autoritativen Nameservern der jeweiligen TLD. Jede TLD wird von einem Network Information Center (NIC) betrieben, die für die Verwaltung des darunterliegenden Namensraum und dem Betrieb der Nameserver zuständig sind [78]. Für die Verwaltung der TLD *.de* ist die DENIC eG zuständig [38]. Ein Endkunde kann bei einem Domain-Registrar (Provider) eine SLD registrieren. Domain-Registrare sind oft unabhängige Unternehmen, die als Vermittler zwischen dem Endkunden und dem NIC agieren und zusätzliche Dienste wie Webspace und E-Mail für die Domain bereitstellen [39].

Bei DNS handelt es sich um eine Client-Server-Anwendung, die folglich im OSI-Referenzmodell der Anwendungsschicht zugeordnet ist. Für die Kommunikation zwischen Client

und Server wird der Port 53 benutzt. Im Regelfall wird als Transportprotokoll das verbindungslose und unzuverlässige Protokoll User Datagramm Protocol (UDP) verwendet, wobei für größere Antworten auch auf das verbindungsorientierte und zuverlässige Transportprotokoll Transmission Control Protocol (TCP) zurückgegriffen werden kann [17]. Der Client wird als Resolver bezeichnet und der Server als Nameserver. Der Resolver kann die Namensauflösung entweder iterativ oder rekursiv durchführen. Die Abbildungen 2.2 und 2.3 zeigen beide Vorgehensweisen bei der Anfrage der Domain *cloud.informatik.haw-hamburg.de* auf. Da das DNS hierarchisch strukturiert ist, werden DNS-Anfragen von der Wurzel zum Blatt beantwortet. Bei der iterativen Namensauflösung muss der Resolver die Hierarchie durch mehrere Anfragen an die Nameserver durchlaufen. Die Nameserver antworten entweder mit der gesuchten IP-Adresse oder mit dem Namen des nächsttieferen Nameservers. Im Gegensatz dazu bekommt der Resolver bei der rekursiven Namensauflösung zu einer Anfrage genau die dazugehörige Antwort geliefert [88].

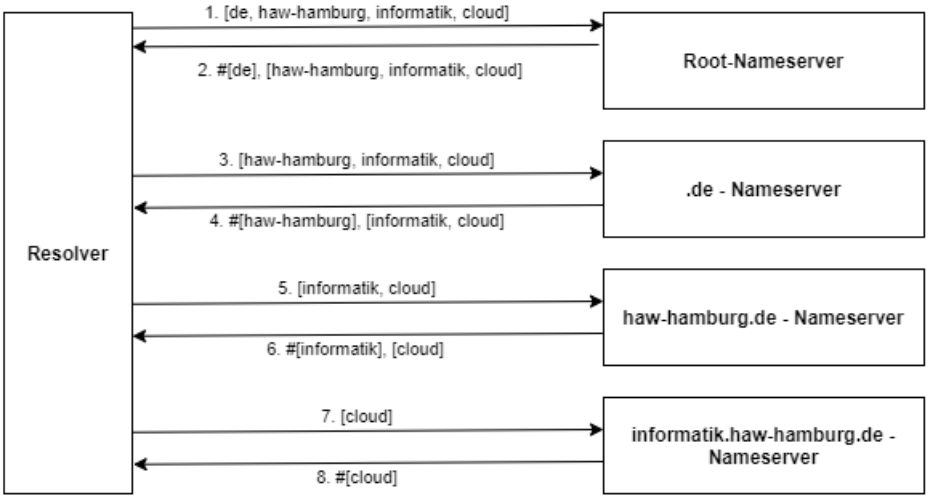


Abbildung 2.2: Prinzip der iterativen Namensauflösung

Quelle: Eigene Darstellung in Anlehnung an [88]

Im Regelfall wird die Namensauflösung von Endgeräten nicht iterativ durchgeführt, sondern es wird ein externer Resolver genutzt, der die Namensauflösung durchführt. Für das Endgerät agiert der externe Resolver analog zu einer rekursiven Namensauflösung, da für eine Anfrage eine Antwort produziert wird. Dieser Resolver wird daher auch rekursiver Resolver oder Resolving DNS-Server genannt. Im Gegensatz zum Beispiel aus der Abbildung 2.3 führt der rekursive Resolver die Namensauflösung jedoch iterativ durch,

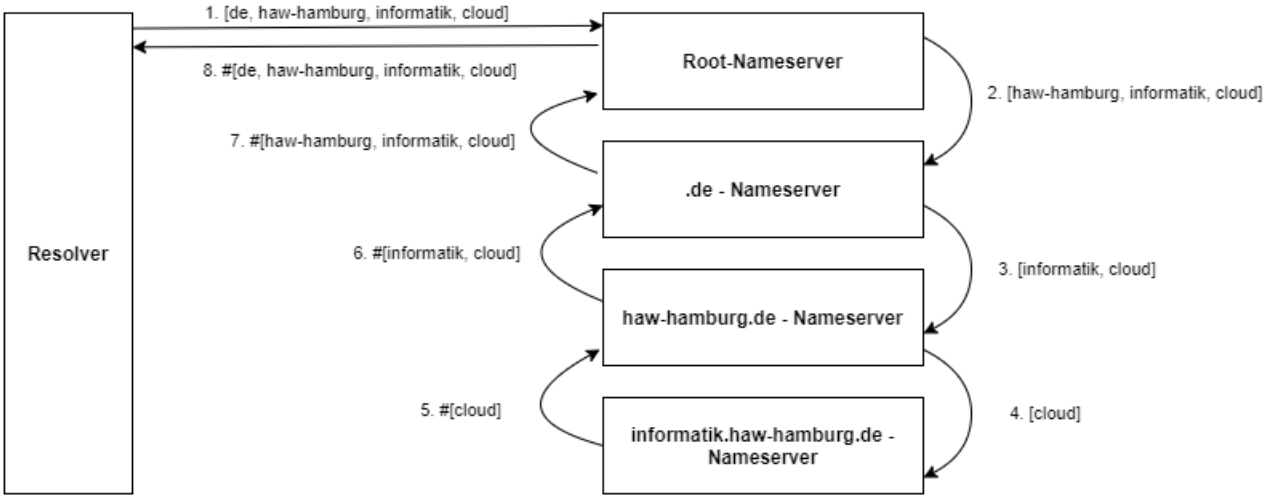


Abbildung 2.3: Prinzip der rekursiven Namensauflösung

Quelle: Eigene Darstellung in Anlehnung an [88]

da die autoritativen Nameserver für gewöhnlich keine rekursiven Anfragen bearbeiten. Zusätzlich besitzt der rekursive Resolver einen Cache, indem die Antworten für eine Zeit vorgehalten werden, um die Namensauflösung zu beschleunigen und die Last auf die Nameserver zu verringern [74][58].

Die Informationen einer Zone werden von dem autoritativen Nameserver bereitgestellt und werden als Resource Records (RR) bezeichnet. Mittlerweile gibt es viele verschiedene Typen von RR, die für unterschiedliche Funktionen im DNS benötigt werden. Die Tabelle 2.1 stellt eine beispielhafte Liste von RR-Typen dar [74]. Möchte ein Client beispielsweise die IPv4-Adresse von *haw-hamburg.de* erfahren, so wird der A-Resource-Record von *haw-hamburg.de* in der DNS-Anfrage erfragt und die IPv4-Adresse in der DNS-Antwort zurückgeliefert.

2.3 Kryptografische Grundlagen

2.3.1 Message Authentication Code (MAC)

Ein Message Authentication Code (MAC) dient der Sicherstellung der Integrität von Daten und der Authentizität der Kommunikationspartner. Sie werden oft dort eingesetzt,

Typ	Beschreibung
A	IPv4-Adresse
AAAA	IPv6-Adresse
CNAME	Alias eines kanonischen Namens
NS	Name des autoritativen Nameservers einer Zone
PTR	Bildet IP-Adresse auf Namen ab. Wird für Reverse DNS benötigt
SOA	Beinhaltet Informationen über die Zone, wie beispielsweise die E-Mail-Adresse des Zonenadministrators und der Standardwert der Lebensdauer eines RR
TXT	Beliebiger Text. Wird oft für zusätzliche Informationen oder Protokolle verwendet
MX	Name des Mail-Servers

Tabelle 2.1: Beispielhafte Typliste von Resource Records

wo Daten über unsichere Netzwerke übertragen werden müssen und sind Teil von vielen Sicherheitsprotokollen [46].

Ein MAC besteht aus einer Hashfunktion und einem zusätzlichen geheimen Schlüssel, der den Kommunikationspartnern bekannt sein muss. Möchten zwei Kommunikationspartner die Unverfälschtheit von Daten garantieren, können sie MACs einsetzen, die neben der Nachricht im Klartext verschickt werden. Diese MACs bestehen aus dem Hash der Konkatenation der Nachricht und des geheimen Schlüssels. Der Empfänger bekommt vom Sender die Klartextnachricht und den MAC überliefert. Dieser kann mittels der Klartextnachricht und dem geheimen Schlüssel wiederum einen MAC generieren und die beiden MACs vergleichen. Sollten sie identisch sein, so ist sichergestellt, dass die Nachricht nicht verändert wurde und der andere Kommunikationspartner derjenige ist, der er vorgibt zu sein.

Jeder Kommunikationspartner, der das gemeinsame Geheimnis besitzt, ist somit in der Lage, einen MAC zu verifizieren aber auch einen neuen MAC für eine Nachricht zu generieren. Ein MAC kann daher keine Verbindlichkeit sicherstellen, da bei mehr als zwei Kommunikationspartnern, jeder die Nachricht und den zugehörigen MAC erstellt haben kann [46].

Eine Erweiterung der MACs sind Keyed-Hash Message Authentication Codes (HMAC), die für die Generierung auf zwei Hashfunktionen zurückgreifen. Dabei wird der geheime Schlüssel in einen äußeren und inneren Schlüssel geteilt. Der innere Schlüssel wird mit

der Nachricht im Klartext konkateniert und der Hash gebildet. Der gebildete Hash wird wiederum mit dem äußeren Schlüssel konkateniert und erneut gehasht. Dadurch entsteht der endgültige HMAC [46].

2.3.2 Asymmetrische Verschlüsselung

Im Gegensatz zur symmetrischen Verschlüsselung wird bei der asymmetrischen Verschlüsselung kein gemeinsames Geheimnis zwischen zwei Kommunikationspartnern benötigt. Vielmehr besitzt jeder Teilnehmer einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel wird an die Kommunikationspartner verteilt und der private Schlüssel geheim gehalten. Mittels des öffentlichen Schlüssels kann eine Nachricht verschlüsselt und nur durch den privaten Schlüssel wieder entschlüsselt werden [46]. Dadurch ist gewährleistet, dass nur der Empfänger der Nachricht, also derjenige mit dem privaten Schlüssel, die Nachricht entschlüsseln kann. Zusätzlich eignen sich die asymmetrischen Verfahren für die Signierung von Daten. Im Gegensatz zu der Verschlüsselung verwendet der Sender bei der Signierung von Nachrichten seinen privaten Schlüssel für die Verschlüsselung. Der Empfänger kann anhand des öffentlichen Schlüssels des Senders durch Entschlüsselung überprüfen, ob die Nachricht tatsächlich vom Absender stammt [46]. Für die Entschlüsselung ist folglich immer der Schlüssel notwendig, mit dem die Verschlüsselung nicht durchgeführt worden ist.

Die mathematische Grundlage der asymmetrischen Verschlüsselung bilden Einwegfunktionen, die leicht berechenbar aber mit keinem effizienten Verfahren umkehrbar sind. Ein Beispiel für eine Einwegfunktionen ist die Berechnung des Produkt zweier großer Primzahlen. Die Berechnung des Produkts ist einfach, die Ermittlung der beiden Primzahlen aus dem Produkt jedoch nicht. Die Umkehrung der Verschlüsselung muss allerdings für einen legitimen Kommunikationspartner effizient möglich sein, daher werden Funktionen genutzt, die mittels zusätzlicher Informationen eine effiziente Entschlüsselung ermöglichen (Einwegfunktion mit Falltür). Ohne die zusätzlichen Informationen verhält sich die Funktion analog zu einer Einwegfunktionen [46].

Ein Beispiel für eine derartige Einwegfunktion mit Falltür ist das RSA-Verfahren. RSA wurde 1978 von den drei Forschern Ronald Rivest, Adi Shamir und Leonard Adleman entwickelt und gilt mittlerweile als de facto Standard für die asymmetrische Verschlüsselung und Signierung [46]. Die genaue Funktionsweise von RSA soll hier nicht behandelt werden und kann in [46] nachgelesen werden.

Asymmetrische Verfahren sind deutlich langsamer als symmetrische Verfahren und werden daher in der Praxis oft für den Schlüsselaustausch eines symmetrischen Verfahrens genutzt [46].

2.3.3 Public-Key-Infrastruktur (PKI)

Ein Problem bei den asymmetrischen Verfahren ist das Schlüsselmanagement des öffentlichen Schlüssels. Ein Angreifer, der die Kommunikation zwischen zwei Teilnehmern abfängt, hat die Möglichkeit den öffentlichen Schlüssel initial durch seinen eigenen zu ersetzen. Keiner der beiden Teilnehmer kann überprüfen, ob es sich bei dem empfangenen öffentlichen Schlüssel tatsächlich um den echten Schlüssel oder den Schlüssel eines Angreifers handelt. Ziel einer Public-Key-Infrastruktur (PKI) ist es, die Authentizität des öffentlichen Schlüssels sicherzustellen [46].

Kern einer PKI sind Zertifikate, die von einer vertrauenswürdigen Stelle ausgestellt werden und die Zuordnung eines öffentlichen Schlüssels zu einem Inhaber beglaubigen. Dazu wird sich der Möglichkeit der Signierung durch asymmetrische Verfahren bedient. Ein Zertifikat beinhaltet neben dem öffentlichen Schlüssel und weiteren Informationen, wie beispielsweise dem Ablaufdatum und Namen des Inhaber auch eine Signatur durch einen privaten Schlüssel [46].

Es gibt verschiedene Vertrauensmodelle, die für den Betrieb einer PKI genutzt werden können. Am gebräuchlichsten ist jedoch das hierarchische Vertrauensmodell, das im Folgenden vorgestellt wird. Bei dem hierarchischen Vertrauensmodell, handelt es sich um eine Hierarchie von Zertifikaten, die dazu genutzt wird eine Zertifizierungskette aufzubauen [46].

Das Wurzel-Zertifikat einer Zertifizierungskette wird als Vertrauensanker (Trust Anchor) bezeichnet und wird durch eine Certificate Authority (CA, Zertifizierungsstelle) betrieben. Das Wurzel-Zertifikat beinhaltet den öffentlichen Schlüssel der CA und wird durch dessen eigenen privaten Schlüssel signiert. Die Wurzel stellt dabei eine Besonderheit dar, da dieses Zertifikat den Endsystemen bekannt gemacht werden muss. Ausgehend von der Wurzel können weitere Zertifikate signiert werden, die wiederum benutzt werden können, um weitere Zertifikate zu signieren[2] [46].

[2] im Falle eines Intermediate-Zertifikats

Zertifikate können kompromittiert werden, beispielsweise wenn der private Schlüssel des Schlüsselpaars entwendet wurde. Daher werden von den Zertifikatsausstellern Sperrlisten (CRL) betrieben. Die Sperrlisten beinhalten die Zertifikate, die vor Ablauf ihres Gültigkeitsdatums gesperrt wurden [46]. Aufgrund der hierarchischen Baumstruktur ist eine Kompromittierung des privaten Schlüssels der Wurzel und derer Knoten, die eine Kante zur Wurzel besitzen, besonders kritisch. Daher unterliegen diese einem hohen Schutzbedarf.

Möchten zwei Benutzer miteinander kommunizieren, so tauschen sie ihre öffentlichen Schlüssel und die zugehörige Zertifikatskette, die alle Zertifikate bis zur Wurzel enthält, aus. Jedes Zertifikat beinhaltet den öffentlichen Schlüssel und die Signatur, die durch den privaten Schlüssel des darüberliegenden Zertifikats erzeugt wurde und somit mit dem öffentlichen Schlüssel desselben darüberliegenden Zertifikats überprüft werden kann. Jeder Kommunikationspartner kann demnach die Vertrauenskette bis zur Wurzel durchlaufen und überprüfen, ob die Signatur tatsächlich von dem darüberliegenden Zertifikat stammt. Da die Endsysteme die Vertrauensanker konfiguriert haben und diesen vertrauen, besitzen sie bereits den zugehörigen öffentlichen Schlüssel der Wurzel und können somit die gesamte Kette validieren.

3 Anwendungsszenario

3.1 Vorstellung des Unternehmens - Quality Software GmbH

Die Quality Software GmbH (QS) ist ein fiktives, mittelständisches Softwareunternehmen mit Sitz in Hamburg. QS wurde 2013 von zwei Absolventen der HAW Hamburg gegründet. Das Unternehmen wird von beiden Gründern als geschäftsführende Gesellschafter geleitet und beschäftigt rund 60 Mitarbeiter, davon 40 Entwickler. Der Rest des Personals setzt sich aus Business Analysten, UI/UX-Designern, Agile Coaches, Systemadministratoren für die interne Infrastruktur, Führungskräften und Assistenzen zusammen.

QS ist ein IT-Dienstleister für Versicherungsgesellschaften und hat sich auf Software für den Vertrieb von Versicherungsprodukten spezialisiert. Die von QS entwickelte Plattform „InsureCloud“ soll den Innen- und Außendienst bei der bedarfsgerechten Beratung von Kunden und beim Vertragsabschluss von Versicherungsprodukten unterstützen. Die Plattform wird als Software as a Service (SaaS) angeboten und wird mittels eines Lizenzmodells vertrieben, das monatlich pro Benutzer abgerechnet wird. „InsureCloud“ ist nach dem Bauskastenprinzip gestaltet, so dass Versicherungen die Software individuell an ihre Bedarfe anpassen und in vorhandene Geschäftsprozesse integrieren können. QS und ihr Produkt sind mittlerweile in der Versicherungsbranche etabliert und „InsureCloud“ wird bereits von einigen großen Versicherungsgesellschaften eingesetzt.

QS ist ein junges und agiles Unternehmen mit flachen Hierarchien. Die Mitarbeiter profitieren von flexiblen Arbeitszeiten sowie einer freien Wahl des Arbeitsplatzes vor Ort oder im Homeoffice. In Hamburg gibt es ein Büro mit begrenzten Arbeitsplätzen, an denen den Mitarbeitern ein Computer mit zwei Bildschirmen sowie ein Headset zur Verfügung steht. Ein Arbeitsplatz muss allerdings vorher über eine Webanwendung reserviert werden. Aufgrund der unterschiedlichen Arbeitszeiten der einzelnen Mitarbeiter setzt QS auf asynchrone Kommunikation wie E-Mails oder Chats. Jeder Mitarbeiter hat außerdem die

Möglichkeit mittels eines VoIP-Clients zu telefonieren. In Besprechungen können sich die Mitarbeiter optional per Videokonferenz hinzuschalten.

QS stellt seinen Mitarbeitern für das Homeoffice einen Laptop und ein Headset bereit. Mitarbeiter dürfen aber auch ihre eigenen Geräte verwenden, indem sie sich über eine gesicherte VPN-Verbindung mit dem Firmennetz verbinden. Die Nutzung von privaten mobilen Endgeräten wird von QS gestattet.

3.2 Softwarearchitektur

Das Kerngeschäft von QS ist der Vertrieb und die Weiterentwicklung der Plattform „InsureCloud“. Mit „InsureCloud“ können Versicherungen ein ganzheitliches Profil des Versicherungsnehmers erstellen und dessen Bedarf passend zur aktuellen Lebenssituation ermitteln.

Die Architektur von „InsureCloud“ zeichnet sich durch eine Drei-Schichten-Architektur aus. Es existiert ein Frontend, das für die Repräsentation der Daten verantwortlich ist, ein Backend, das die Geschäftslogik beinhaltet und eine Persistenzschicht, die die korrekte und persistente Speicherung der Daten verantwortet. Frontend und Backend werden dabei jeweils in einem Cluster von Containern ausgeführt. QS erhofft sich dadurch mehrere Vorteile. Zuerst kann so die gesamte Anwendung einfach skaliert werden, indem neue Container dynamisch zugeschaltet werden und so die Last deutlich besser verteilt wird. Ein wesentlicher Anteil an der Einfachheit der Skalierung ist der Persistenzschicht zuzuordnen. Die Container besitzen keine persistenten Daten sondern nur temporäre Sitzungsdaten und kommunizieren mit der Persistenzschicht, die wiederum mit der Datenbank agiert. Die Persistenzschicht sorgt dafür, dass nur vollständig und korrekte Transaktionen in der Datenbank gespeichert werden. Ferner können Abstürze von einzelnen Komponenten durch gleichartige Komponenten in anderen Containern kompensiert werden, bis der Container neugestartet wurde. Ein weiterer Vorteil ist, dass neue Features inkrementell ausgerollt werden können. Die neuen Features stehen also erst wenigen Anwendern bereit, potentielle Fehler bei der Integration können entdeckt werden, ohne das der gesamte Benutzerkreis davon betroffen ist.

Die Container Cluster werden im hausinternen Rechenzentrum betrieben. Die Datenbank wird bei einem externen Dienstleister repliziert.

3.3 Bedeutsamkeit der Informationssicherheit

QS unterliegt, wie auch die Versicherungsgesellschaften, besonderen gesetzlichen Bestimmungen, da nicht nur mit personenbezogenen Daten sondern auch mit Gesundheitsdaten gearbeitet wird [29]. Personenbezogene Daten sind Informationen, die einer Person zuzuordnen sind oder über die eine Person eindeutig zugeordnet werden kann, wie z.B. ein eindeutiger Identifier [79]. Gesundheitsdaten hingegen vereinen alle Daten, die den früheren, aktuellen und künftigen körperlichen und geistigen Gesundheitszustand einer Person beschreiben [79]. QS benötigt die personenbezogenen Daten sowie die Gesundheitsdaten für eine korrekte bedarfsgerechte Beratung des Kunden.

Im November 2018 formulierte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in einem Rundschreiben die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT), um die speziellen Anforderungen an die IT in Versicherungsunternehmen zu berücksichtigen. Dabei konkretisiert die VAIT bereits bestehende Anforderungen aus dem Versicherungsaufsichtsgesetz (VAG), der Richtlinie Solvabilität II sowie den Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) und bildet somit die Grundlage für künftige Prüfungen [26]. QS als IT-Dienstleister im Assekuranzgeschäft[1] nimmt den Versicherungsgesellschaften eine wichtige Funktions- und Versicherungstätigkeit ab und ist dadurch den Versicherungsgesellschaften selbst, den Abschlussprüfern und der Aufsichtsbehörde verpflichtet. In §32 des Versicherungsaufsichtsgesetz heißt es, dass „[b]ei der Ausgliederung wichtiger Funktionen und Versicherungstätigkeiten [...] Versicherungsunternehmen außerdem sicherzustellen [haben], dass wesentliche Beeinträchtigungen der Qualität der Geschäftsorganisation, eine übermäßige Steigerung des operationellen Risikos sowie eine Gefährdung der kontinuierlichen und zufriedenstellenden Dienstleistung für die Versicherungsnehmer vermieden werden“ [28]. Die VAIT schlussfolgert, dass bei IT-Dienstleistungen vorab eine Risikoanalyse durchzuführen ist, insbesondere für IT-Dienstleistungen, „[...] die dem Unternehmen durch ein Dienstleistungsunternehmen über ein Netz bereitgestellt werden (z. B. Rechenleistung, Speicherplatz, Plattformen oder Software) und deren Angebot, Nutzung und Abrechnung dynamisch und an den Bedarf angepasst über definierte technische Schnittstellen sowie Protokolle erfolgen (Cloud-Dienstleistungen)“ [26]. Die VAIT behält sich vor, dass Regelungstiefe und -umfang nicht abschließend geklärt sind und das Unternehmen sich bei IT-Prozessen an gängigen Standards, wie z.B. dem IT-Grundschutz [27] oder

[1] Versicherungsgeschäft

den internationalen Sicherheitsstandards ISO 2700X orientieren sollen [26]. QS ist demnach gut beraten, die internen IT-Prozesse sowie die Infrastruktur anhand einer dieser Vorgehensweisen zu analysieren und somit den Schutzbedarf von IT-Anwendungen und IT-Systemen innerhalb der versicherungsrechtlichen Anforderungen an die IT zu gewährleisten. Die Informationssicherheit ist also ein Grundpfeiler in der Zusammenarbeit zwischen Versicherungsunternehmen und QS. Dabei spielt die Informationssicherheit für die Versicherungsgesellschaften eine genauso große Rolle wie für QS selbst.

QS Alleinstellungsmerkmal ist ihr einziges Produkt „InsureCloud“, daher kann ein schwerwiegender IT-Sicherheitsvorfall zum Vertrauensverlust bei den Versicherungsgesellschaften führen und somit wohlmöglich auch zu großem wirtschaftlichen Schaden. Aber auch schon kleine Ausfälle können die Wirtschaftlichkeit des Unternehmens beinträchtigen. QS orientiert sich bei den Schutzzielen an den Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) [27]. Die primären Schutzziele sind laut BSI Vertraulichkeit, Integrität und Verfügbarkeit. Übertragen auf den Anwendungsfall QS sind die Begrifflichkeiten wie folgt zu verstehen:

1. **Vertraulichkeit**
   Beispiel: QS arbeitet mit unterschiedlichen Versicherungsgesellschaften zusammen, die auf dem freien Markt miteinander konkurrieren. Mitarbeiter der unterschiedlichen Gesellschaften dürfen lediglich auf ihre eigenen Daten und Kunden zugreifen und nicht auf die Kundendaten der konkurrierenden Unternehmen. Die personenbezogenen Daten und Gesundheitsdaten der Kunden dürfen unter keinen Umständen Unbefugten zugänglich gemacht werden.

2. **Integrität**
   Beispiel: Da es sich bei der Software um eine Tarif- und Angebotssoftware mit besonderen Augenmerk auf die persönliche und bedarfsgerechte Beratung handelt, ist die Integrität der Daten besonders wichtig. Ein Beratungsprotokoll ist ein gesetzlich vorgeschriebenes Dokument, das die Beratung des Kunden dokumentiert [6]. Dieses Protokoll spiegelt die, zum Zeitpunkt der Beratung vorherrschenden, Lebensverhältnisse und somit den Bedarf an Versicherungsprodukten wider. Da es sich um ein rechtskräftiges Dokument handelt, ist es von besonderer Wichtigkeit, dass dieses Dokument nicht unbemerkt verändert wird.

3. **Verfügbarkeit**
   Beispiel: Einige Versicherungsgesellschaften benutzen ausschließlich das von QS

entwickelte System. Ein Ausfall des Systems würde für die Versicherungsunternehmen einen Ausfall der Produktion[2] bedeuten. Das System muss in den vereinbarten Servicezeiten jederzeit zum vereinbarten Service-Level erreichbar sein.

QS ist für verschiedene Angreifer ein interessantes Ziel. Für Konkurrenten von QS sind die Informationen über das System sehr wertvoll. Aber auch ein Angriff gegen die Verfügbarkeit von „InsureCloud“ ist denkbar, da die wirtschaftlichen Folgen für QS enorm wären. Versicherungsgesellschaften hingegen haben ein besonderes Interesse an den Kundendaten der konkurrierenden Unternehmen, um die Kunden mit ihren eigenen Produkten zu versorgen. Ferner besteht das Risiko, dass die Software von einem Mitarbeiter so manipuliert wird, dass Produkte von einem spezifischen Versicherungsunternehmen bevorzugt empfohlen werden. Für Geheimdienste und international agierende Organisationen sind die personenbezogenen Gesundheitsdaten von Interesse. Gleichermaßen für Angreifer, die die sensiblen Kundendaten verkaufen oder dem Unternehmen in anderer Form schaden wollen.

3.4 Motive für die Bedrohungsanalyse

Bei QS wurde bereits eine Bedrohungsanalyse, insbesondere im Hinblick auf „InsureCloud“ durchgeführt. Dabei wurden Mängel im Umgang mit DNS gesichtet. Daher möchte QS eine neue Bedrohungsanalyse mit besonderer Aufmerksamkeit auf DNS durchführen und überprüfen, inwieweit DNS und die DNS-Sicherheitserweiterungen für das Unternehmen zu bewerten sind. Diese Bedrohungsanalyse soll sich nicht nur auf das Produkt beziehen, sondern die gesamte Infrastruktur des Unternehmens betrachten. Dafür wurde von QS das übergeordnete Schutzziel „Schutz der DNS-Infrastruktur“ definiert, das die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit auf die DNS-Infrastruktur abbildet, um diese dann bezogen auf die Bedrohungs- und Risikoanalyse zu betrachten. Die Schutzziele werden in Tabelle 3.1 beschrieben. Vertraulichkeit ist normalerweise kein Schutzziel von DNS, da die Daten in autoritativen Nameservern öffentlich und jedem zugänglich sind [32]. Dennoch wird von QS das Schutzziel Vertraulichkeit definiert, da öffentliche DNS-Daten nicht dazu genutzt werden dürfen, dass die Schutzziele Integrität und Verfügbarkeit eingeschränkt werden. Außerdem betrachtet die Bedrohungs- und Risikoanalyse nicht nur die autoritativen Nameserver, die über öffentliche Informationen verfügen, sondern auch die rekursiven Resolver und die Stub-Resolver im Endsystem, die

[2] Neuabschlüsse, Cross- und Upselling

über DNS-Daten in Transaktionszusammenhängen verfügen und somit für QS unter die Vertraulichkeit fallen.

QS hat DNS in ihrer Sicherheitsstrategie bisher nicht beurteilt. Da es sich bei DNS um ein verteiltes System handelt, an dem viele unterschiedliche Komponenten und Parteien beteiligt sind, ist die Betrachtung von DNS im Kontext der Informationssicherheit deutlich komplexer als monolithische Systeme [69]. DNS wird von einigen Unternehmen, so auch von QS, teilweise oder komplett ausgelagert. Die fehlende Kontrolle über die DNS-Infrastruktur bietet einem Angreifer ein lukratives Angriffsziel. Da DNS oft die Grundvoraussetzung für die Kommunikation zwischen zwei Parteien ist, würde ein DNS-Sicherheitsvorfall das gesamte Netzwerk für längere Zeit beinträchtigen [69]. Für QS würde ein ungeplanter, mehrstündiger Ausfall vermutlich schwerwiegene wirtschaftliche Folgen bedeuten. Ein Angreifer, der die DNS-Einträge von „InsureCloud“ ändert, kann Benutzer der Versicherungsgesellschaften auf seine eigenen Server leiten und so wertvolle personenbezogene Kundendaten stehlen.

Übergeordnetes Schutzziel: Schutz der DNS-Infrastruktur	
IT-Schutzziele	**Beschreibung**
Verfügbarkeit	IT-Störungen dürfen nicht dazu führen, dass die interne DNS-Infrastruktur die Namensauflösung nicht mehr in angemessener Qualität und Quantität aufrechterhalten kann.
Integrität	IT-Störungen dürfen nicht dazu führen, dass 1. die DNS-Daten (bspw. auf dem Transportweg, in den Zonendateien, Caches und sonstigen Konfigurationsdateien) verfälscht werden. 2. die Authentizität der DNS-Daten nicht mehr gewährleistet ist.
Vertraulichkeit	IT-Störungen dürfen nicht dazu führen, dass 1. interne Informationen über DNS-Daten veröffentlicht werden. 2. interne Informationen (bspw. Dienste, Hostnames, IP-Adressen etc.) über DNS-Daten veröffentlicht werden, deren Bekanntwerden sekundär zu einer Beeinträchtigung der Verfügbarkeit oder Integrität von Systemen oder Daten führt. 3. die DNS-Transaktionen unberechtigten Dritten zugänglich gemacht werden oder eine Identifikation des anfragenden Benutzers ermöglichen.

Tabelle 3.1: Auf das übergeordnete Schutzziel „Schutz der DNS-Infrastruktur“ bezogene Definitionen der IT-Sicherheit

4 Bedrohungsanalyse

In diesem Kapitel werden die von Quality Software eingesetzten Systeme, die DNS verwenden, analysiert und mögliche Bedrohungen gegen eine DNS-Infrastruktur aufgezeigt sowie bewertet. Dazu wird eine Bedrohungsanalyse durchgeführt. Die Bedrohungsanalyse ist Teil des Security Engineering und verfolgt eine möglichst vollständige Erfassung der Bedrohungen eines IT-Systems und kann mittels verschiedener methodischer Vorgehensweisen durchgeführt werden [46]. Eine Bedrohung ist ein Ereignis oder eine Situation das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann. Ziel einer Bedrohung ist immer die Schwachstellen oder die Verwundbarkeiten eines Systems auszunutzen um die Schutzgüter zu gefährden [46]. Dabei entsteht für den Besitzer oder Benutzer der Information ein Schaden [27]. Die hier durchgeführte Bedrohungsanalyse orientiert sich am IT-Grundschutz für IT-Systeme mit hohem Schutzbedarf, da bei der Standard-Absicherung für IT-Systeme mit normalem oder niedrigem Schutzbedarf auf eine Bedrohungsanalyse verzichtet wird [27].

Der Prozess läuft wie folgt ab: Zuerst werden die Systeme identifiziert, die bei Verwendung von DNS beteiligt sind. Gleichartige Systeme werden, wie auch bei der Strukturanalyse des IT-Grundschutzes, zusammengefasst, um die Komplexität der Bedrohungsanalyse gering zu halten. Systeme sind gleichartig, wenn sie

- „vom gleichen Typ sind,
- ähnliche Aufgaben haben,
- ähnlichen Rahmenbedingungen unterliegen und
- den gleichen Schutzbedarf aufweisen“ [62, S.40].

Als nächstes werden potentielle Bedrohungen gegen die DNS-Infrastruktur aufgezeigt und erläutert, wie die jeweiligen Bedrohungen die Schutzziele beeinflussen können. Die Bedrohungen werden dabei thematisch klassifiziert, so dass diese in der späteren Evaluation im Bezug auf die DNS-Erweiterungen analysiert werden können um festzustellen,

ob und welche DNS-Erweiterung das Bedrohungsrisiko minimieren kann. Im letzten Teil wird das Risiko mittels des BSI-Standards 200-3 für das Anwendungsszenario beurteilt [24].

Eine ganzheitliche Bedrohungsanalyse betrachtet nicht nur DNS, sondern alle IT-Systeme und Informationen gleichermaßen. Diese wurde von QS bereits durchgeführt, daher soll in dieser Analyse der Fokus speziell auf DNS gerichtet werden.

4.1 Identifikation der verwendeten Systeme

Zu Beginn müssen, analog der Strukturanalyse, die Systeme hinsichtlich Einsatzumgebung und Verwendungszweck identifiziert werden [46]. Da es sich bei DNS um ein verteiltes System handelt, gibt es bei der Verwendung der Namensauflösung mehrere beteilige Komponenten, die gleichartig in folgenden Kategorien analysiert werden:

- Stub-Resolver im Endsystem
- Rekursiver Resolver
- Autoritativer Nameserver

4.1.1 Stub-Resolver im Endsystem

Da bei nahezu jeder Kommunikation im Netzwerk DNS verwendet wird und Benutzer beliebige Anwendungen auf ihren Geräten ausführen können, ist eine genaue Aufzählung der beteiligten Anwendungen auf den Clients mit sehr großem Aufwand verbunden. Daher wird der Fokus in der Identifikation auf die unterschiedliche Hardware sowie Betriebssysteme und Standardsoftware gerichtet.

Ein Stub bezeichnet in verteilten Systemen eine Softwarekomponente, die Dienste eines nur über das Netzwerk erreichbaren, entfernten Systems anbietet indem der Stub die lokalen Anfragen in Netzwerkaufrufe übersetzt und an das entfernte System delegiert. Für die lokalen Anwendungen bleibt die zugrundeliegende Netzwerkkommunikation verborgen, da der Aufruf der Funktionen unabhängig davon ist, ob diese lokal oder entfernt bearbeitet werden (Zugriffstransparenz) [88].

QS betreibt eine heterogene Umgebung, es werden Desktop-Clients, Server und Mobilgeräte von verschiedenen Herstellern mit unterschiedlichen Betriebssystemen genutzt. Dazu gehören beispielsweise Windows-Clients, Linux-Server, iOS- und Android-Mobilgeräte aber auch Drucker und sonstige netzwerkgebundene Peripherie. Jedes Betriebssystem, das Netzwerkkommunikation unterstützt, implementiert einen eigenen Stub-DNS-Resolver und bietet den Anwendungen Schnittstellen - sogenannte Systemcalls - zu diesem an.

Der Stub-Resolver im Betriebssystem kann durch verschiedene Schnittstellen die Namensauflösung durchführen. Unter Linux und Mac OS X wird beispielsweise die Portable Operating System Interface (POSIX)-Programmierschnittstelle *getaddrinfo()* verwendet [3]. Windows bietet den Anwendungen die Schnittstelle *DnsQuery_A()* an [72]. Da der Stub-Resolver die Anfragen nicht selbst beantwortet, werden die Anfragen an einen Stellvertreter weitergeleitet - dem rekursiven Resolver, der im nächsten Abschnitt betrachtet wird. Die Nutzung eines Stub-Resolvers hat mehrere Vorteile. Erstens wird die Komplexität in der Implementierung des DNS-Clients deutlich verringert und dadurch weniger fehleranfällig. Zweitens können Ressourcen beim Client gespart werden, da die eigentliche Arbeit der Namensauflösung delegiert wird. Drittens kann bei einem Verbund von Clients, die einen gemeinsamen rekursiven Resolver nutzen, der Cache geteilt werden, um so die Anfragezeiten deutlich zu verringern [74].

Damit der Client die Anfragen weiterleiten kann, müssen die zuständigen rekursiven Resolver dem Client bekannt gemacht werden. Das kann zum einen bei der Vergabe der IP-Adresse geschehen, indem der DHCP-Server die zu verwendenden Resolver übergibt [10]. Zum anderen gibt es die Möglichkeit die IP-Adressen der Resolver in Konfigurationsdateien zu hinterlegen oder im Betriebssystem fest zu konfigurieren.

Alternativ können Clients auch ohne Delegation die Namensauflösung durchführen, beispielsweise weil sie die erforderliche Software nachinstalliert haben oder Anwendungen verwenden, die direkt mit den zuständigen Nameservern kommunizieren. Dadurch können Limitierung in der Implementierung des vom Betriebssystem angebotenen Stub-Resolvers umgangen werden. Unter Linux-Betriebsystemen gibt es im Regelfall keinen DNS-Cache, Webbrowser implementieren daher oft einen eigenen DNS-Cache um die Anfragen schneller bearbeiten zu können ohne vorher den rekursiven DNS-Resolver anzufragen [20].

4.1.2 Rekursiver Resolver

Wie im vorherigen Abschnitt bereits erwähnt, benötigen Clients einen rekursiven DNS-Resolver zum Abfragen von Hostnames, sofern der Client nicht als Full-Resolver agiert. Die Begriffe Caching Resolver, Full-Resolver, nicht autoritativer oder rekursiver Nameserver werden in der Literatur als Synonym für die rekursiven DNS-Resolver verwendet.

Abbildung 4.1 zeigt den Ablauf einer typischen DNS-Anfrage aus dem Firmennetzwerk. Die Clients bekommen initial vom DHCP-Server die IP-Adresse des autoritativen Nameservers *NS2.corp* der Domäne *corp.quality-software.de* als zu verwendender Nameserver zugewiesen. Der Nameserver *NS2.corp* ist so konfiguriert, dass externe Anfragen außerhalb der eigenen Domäne weitergeleitet werden. Die bedingte Weiterleitung schickt die DNS-Anfragen an den Router des Unternehmens, der die Anfragen wiederum an den rekursiven Resolver des Internet Service Providers (ISP) oder an die autoritativen Nameserver von QS weiterleitet. ISPs bieten ihren Kunden einen rekursiven Resolver an, da die Clients im Regelfall nur den Stub-Resolver und die Router nur einen DNS-Proxy besitzen und somit keine eigene Namensauflösung durchführen könnten. Ein DNS-Proxy, oft auch DNS-Forwarder, beschreibt dabei eine Besonderheit in der DNS-Infrastruktur, da dieser die Anfragen lediglich weiterleitet. DNS-Proxies werden meist dort verwendet, wo die Hardware für die Namensauflösung nicht ausreichend leistungsfähig genug ist, wie beispielsweise in klassischen (WLAN-)Routern für den Privatgebrauch [18]. Das Unternehmen betreibt somit keinen eigenen rekursiven Resolver sondern verwendet zwei DNS-Proxies. Die IP-Adressen für die rekursiven Resolver bekommt der DNS-Proxy vom ISP, entweder durch DHCP oder Point-to-Point-Protocol-over-Ethernet, mitgeteilt [33].

Aufgrund der *Bring your own Device (BYOD)*-Unternehmensstrategie dürfen private Endgeräte für die Arbeit genutzt werden. Es ist durchaus möglich, dass in den privaten Geräten rekursive DNS-Resolver statisch konfiguriert sind. Das können Resolver von Unternehmen sein, die ihren DNS-Dienst freiverfügbar anbieten, wie beispielsweise Google[1] oder Cloudflare[2]. In diesen Fällen wird der Nameserver im Endgerät durch DHCP nicht verändert. Sollte der mobile Client jedoch keine statische Konfiguration des Nameservers besitzen, so wechselt der zuständige Resolver mit jedem Wechsel des Netzwerkes. Im privaten Heimnetzwerk ist davon auszugehen, dass der Client den rekursiven Resolver seines ISPs verwendet. Es können im Rahmen dieser Analyse nur die vom Unternehmen direkt genutzten Resolver in die Bedrohungsanalyse aufgenommen werden, trotzdem haben sie

[1] https://developers.google.com/speed/public-dns
[2] https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/

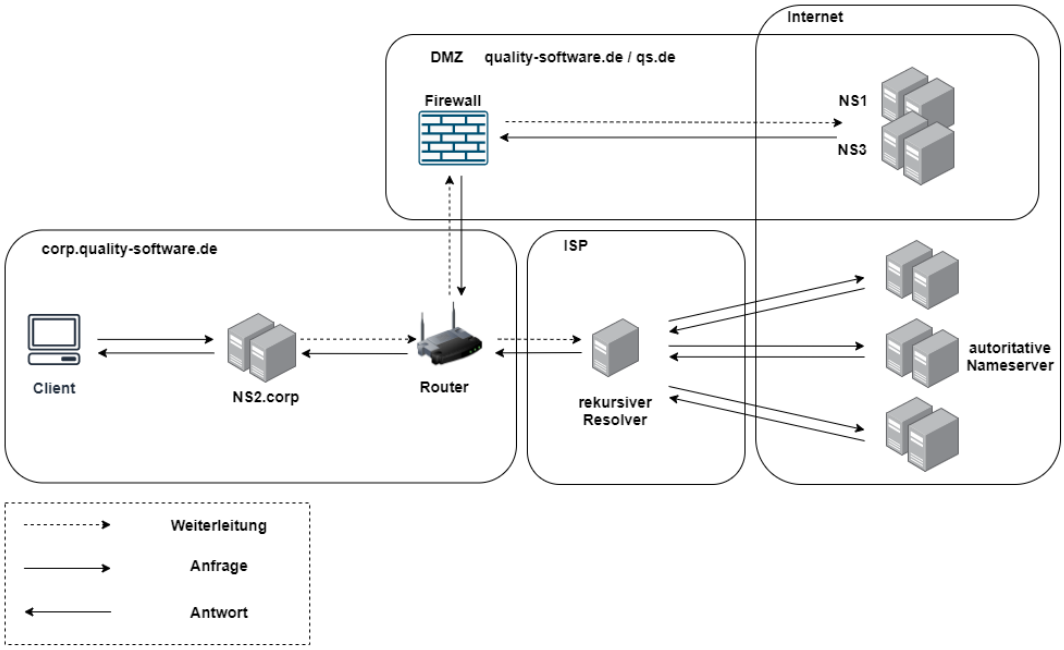


Abbildung 4.1: Schematische Darstellung einer DNS-Anfrage

direkte Auswirkungen auf die Clients und müssen in diesem Kontext berücksichtigt werden.

4.1.3 Autoritativer Nameserver

Abbildung 4.2 zeigt die hierarchische DNS-Struktur bei QS. QS betreibt für die internen Dienste einen eigenen autoritativen Nameserver NS2, der nur für die Sub-Domäne corp.quality-software.de autoritativ ist (dargestellt in Grün). NS2 wird für jeden Client, durch DHCP, als der zu verwendende Nameserver konfiguriert. Dadurch können Clients die internen Dienste erreichen, da diese von NS2 aufgelöst werden. Daneben wird für die Domain quality-software.de sowie qs.de der autoritative Nameserver NS1 betrieben, der unter anderem die öffentlichen Anfragen aus dem Internet beantwortet (dargestellt in Gelb und Lila) und für die Dienste innerhalb der Demilitarisierten Zone (DMZ), beispielsweise die Plattform „InsureCloud“, verantwortlich ist. NS1 wird durch einen dritten autoritativen Nameserver NS3 repliziert, um die Verfügbarkeit der Namensauflösung zu erhöhen. NS1, NS2 und NS3 werden im hauseigenen Rechenzentrum betrieben, das sich mit mehreren Unternehmen geteilt wird.

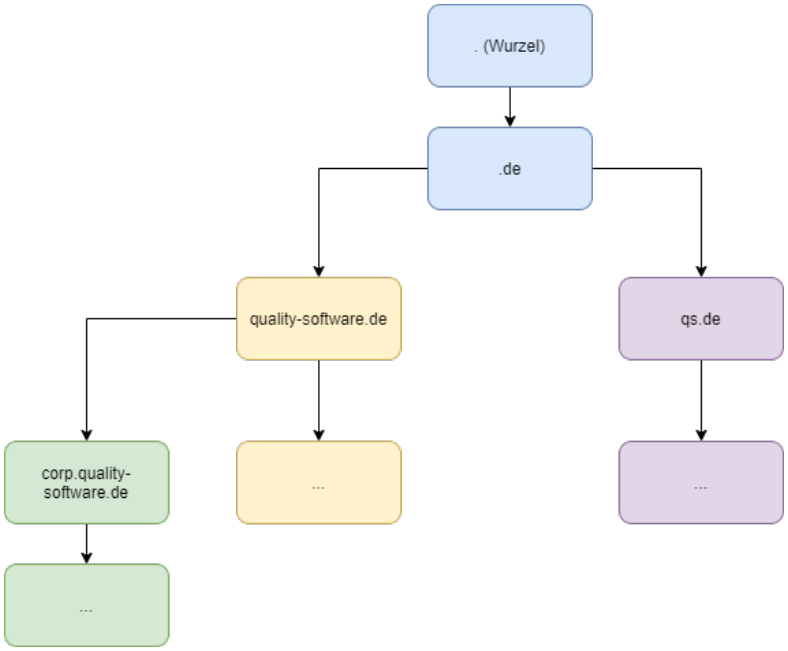


Abbildung 4.2: Hierarchische DNS-Struktur bei QS

Neben den autoritativen Nameservern müssen zusätzlich die registrierten Domains identifiziert werden, da diese für die DNS-Infrastruktur unabdingbar sind. Die Domains quality-software.de und qs.de zählen somit zu den identifizierten Systemen, die in der Bedrohungsanalyse betrachtet werden müssen.

4.2 Analyse möglicher Bedrohungen

Aus der Identifikation der Systeme ergeben sich mögliche Bedrohungen und Angriffsszenarien für die DNS-Infrastruktur von QS. In diesem Teil sollen diese Bedrohungen allgemeingültig aufgezeigt werden, um sie dann in der Risikoanalyse zu bewerten. Bedrohungen beschreiben dabei nicht nur bösartige Angriffe durch externe Parteien sondern auch interne Bedrohungen, die die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit im Bezug auf das übergeordnete Schutzziel „Schutz der DNS-Infrastruktur“ bedrohen. Es werden demnach gezielte Angriffe gegen die DNS-Infrastruktur genauso betrachtet wie unbeabsichtigte Konfigurationsfehler eines Systemadministrators. Im Englischen werden dafür die Begriffe „Security“ und „Safety“ verwendet. In jeder Bedrohungskategorie wird zu Beginn eine Tabelle dargestellt, in der die jeweiligen Bedrohungen auf die identifizierten Systeme und Schutzziele abgebildet werden. Die Tabelle 4.1 erläutert dabei die verwendeten Abkürzungen bezogen auf die verschiedenen Spalten.

Spalte	**Abkürzung**	**Beschreibung**
identifiziertes System	S	Stub-Resolver
	R	Rekursiver Resolver
	A	Autoritativer Nameserver
bedrohte Schutzziele	C	Vertraulichkeit
	I	Integrität
	A	Verfügbarkeit

Tabelle 4.1: Legende der verwendeten Abkürzungen bei der Bedrohungsanalyse

4.2.1 Bedrohungen gegen den Host

DNS ist ein Netzwerkdienst, der von den rekursiven Resolvern und autoritativen Nameservern angeboten und vom Stub-Resolver konsumiert wird. Wie jeder andere Host, der einen Dienst im Netzwerk anbietet, sind auch DNS-Server für generische Bedrohungen gegen allgemeine Netzwerkdienste empfänglich. Eine Bedrohung gegen den Host, auf dem die DNS-Serversoftware ausgeführt wird, ist demnach eine Bedrohung gegen die DNS-Infrastruktur. Die Bedrohungen gegen einen allgemeinen Server werden durch den Baustein SYS.1.1 „Allgemeiner Server“ des IT-Grundschutz-Kompendiums beschrieben. Bedrohungen gegen Clients werden durch den Baustein SYS.2.1 „Allgemeiner Client“

modelliert [27]. Aus den beiden Bausteinen werden im Folgenden die relevanten Bedrohungen im Kontext von DNS abgebildet und durch eigene Bedrohungen ergänzt. Die gesamten Bedrohungen gegen den Host können der Tabelle 4.2 entnommen werden.

Nr	**Bedrohung**	**identifiziertes System**	**bedrohte Schutzziele**
1	Software-Schwachstellen oder -Fehler	S R A	A C, I, A C, I, A
2	Datenverlust	S R A	A A A
3	Denial-of-Service-Angriffe	S R A	A A A
4	Bereitstellung unnötiger Betriebssystemkomponenten und Applikationen	R A	A A
5	Fehlplanung	R A	A A
6	Unbefugter physischer Zugriff	R A	C, I, A C, I, A
7	Malware	S R A	I, A I, A I, A

Tabelle 4.2: Bedrohungen gegen den Host

B1: Software-Schwachstellen oder -Fehler

DNS-Server sind komplexe Softwareanwendungen, die aus mehreren Millionen Zeilen Code bestehen und somit unentdeckte Schwachstellen beherbergen können [69]. Diese Schwachstellen können von einem Angreifer ausgenutzt werden, um Zugriff zum Firmennetzwerk zu erlangen. 2020 wurden bereits neun neue Sicherheitslücken für die am weites-

ten verbreiteten DNS-Software *BIND* veröffentlicht[3]. *BIND* gilt als DNS-Referenzsoftware und wurde erstmals im Juni 1986 veröffentlicht [7]. DNS-Softwareanwendungen sind folglich aufgrund ihrer Komplexität für Angriffe und Sicherheitslücken empfänglich, dabei ist es unerheblich, dass die Software schon seit Jahrzehnten benutzt und weiterentwickelt wird.

Aber auch ohne Fremdeinwirkung kann ein IT-Sicherheitsvorfall eintreten. Laufzeitfehler in der betriebenen DNS-Serversoftware können zu einer Bedrohung gegen die Verfügbarkeit und Integrität führen. Das Ausmaß der Bedrohung wird dabei durch die Zuständigkeit vorgegeben. Im Falle eines fehlerhaften rekursiven Nameservers ist das Ausmaß auf die internen Mitarbeiter und Dienste beschränkt. Ein rekursiver Nameserver, der nicht mehr jede Anfrage beantwortet oder gar überlastet ist, schränkt die Verfügbarkeit ein. Laufzeitfehler können allerdings auch dazu führen, dass der rekursive Nameserver die Antworten der anfragenden Clients vertauscht. Client A könnte somit die Antwort für die Anfrage von Client B erhalten. Vorstellbar ist auch, dass der rekursive Nameserver die Antworten der Clients komplett verändert. Dieses Szenario ist eine Bedrohung gegen die Integrität, da die Informationen im ersten Fall ausgetauscht und im anderen Fall komplett modifiziert werden. DNS-Server sind nebenläufig, da sie oft eine Vielzahl von Anfragen gleichzeitig verarbeiten müssen. Daher sind neben Laufzeitfehlern auch Wettlaufsituationen (Race Conditions) vorstellbar, die die Verfügbarkeit der DNS-Server beeinträchtigen.

Fehler in den autoritativen Nameservern können die gleiche Ursache haben, beeinträchtigen jedoch einen erweiterten Nutzerkreis. Ein fehlerhafter autoritativer Nameserver kann, genauso wie der fehlerhafte rekursive Nameserver, die Anfragen der Clients gar nicht, vertauscht oder komplett falsch beantworten. In diesem Fall wären jedoch nicht nur die internen Mitarbeiter und Dienste betroffen, sondern auch jeder, der einen Dienst innerhalb der autoritativen Domäne beanspruchen möchte.

Aber auch das Betriebssystem kann Schwachstellen beinhalten, die dazu führen können, dass die Namensauflösung nicht mehr ordnungsgemäß ausgeführt wird.

Eine weitere Bedrohung gegen die Verfügbarkeit und Integrität ist das Betreiben von unzureichend aktualisierten DNS-Servern sowie alter Versionen. Viele Angreifer suchen gezielt nach Softwareversionen mit bekannten Sicherheitslücken, um diese auszunutzen und somit die Kontrolle über den Dienst oder den Server zu übernehmen. Ein Angreifer, der die Kontrolle über einen autoritativen DNS-Server erlangt, kann alle Einträge

[3] https://kb.isc.org/docs/aa-00913 (Stand 20.08.2020)

verändern und somit Benutzer auf einen vom Angreifer präparierten Host leiten. Auch Stunden nachdem die Sicherheitslücke geschlossen wurde und die kompromittierten Einträge wieder auf die ursprünglichen Hosts zeigen, würden einige Benutzer immer noch auf die Hosts des Angreifers geleitet, da die Einträge in den Zwischenspeichern der rekursiven Resolvern, abhängig von der Time to Live (TTL), gepuffert werden [69]. Bei Übernahme eines rekursiven DNS-Resolvers würde der Angreifer jeglichen DNS-Verkehr des Opfers mitlesen können und somit die Vertraulichkeit bedrohen. Obwohl die Informationen öffentlich sind, fällt der Zugriff auf diese unter die Vertraulichkeit, da die DNS-Nachrichten immer in einem Transaktionszusammenhang stehen [66].

Die Tabelle 4.3 zeigt einige konkrete Schwachstellen und Sicherheitslücken für populäre DNS-Software auf. Die konkreten Schwachstellen werden nach dem *Common Vulnerability Scoring System*, einem Industriestandard zur Bewertung von Sicherheitslücken, bewertet. Die Bewertung setzt sich aus verschiedenen Metriken, wie beispielsweise der Angriffsvektor oder die Komplexität des Angriffs, zusammen. Dabei ist jeder Metrik ein Wert zugeordnet, der mittels vordefinierter Formeln sowie den Werten der anderen Metriken verrechnet wird. Es ergibt sich ein endgültiger Wert zwischen 0.0 und 10.0, der die Schwere der Sicherheitslücke angibt [49]. Wie in der Tabelle zu erkennen, sind die schwerwiegensten Schwachstellen jene, die eine Remote-Code-Ausführung (RCE) ermöglichen. Diese sind deshalb besonders kritisch, da ein Angreifer über DNS-Nachrichten beliebigen Code auf den Servern ausführen und somit den kompletten Server kompromittieren kann. Aber auch Pufferüberläufe, ausgelöst durch DNS-Nachrichten wie beispielsweise in der Schwachstelle CVE-2020-0836, werden als kritisch betrachtet, da sie die Verfügbarkeit der Namensauflösung einschränken.

B2: Datenverlust

Die Bedrohung Datenverlust betrifft die gesamte DNS-Infrastruktur. Die autoritativen Nameserver besitzen Zoneninformationen, um die Namensauflösung durchzuführen [69]. Ein Verlust der Zonendatei bedeutet, dass der autoritative Nameserver für seine Domäne keine Namensauflösung mehr durchführen kann. Die Stub-Resolver im Endsystem besitzen Konfigurationsdateien, in denen die zu verwendenden rekursiven Resolver konfiguriert sind [5]. Die rekursiven Resolver besitzen ebenfalls Konfigurationsdateien, die beispielsweise restriktieren, welche Clients den Dienst verwenden dürfen oder im Fall des DNS-Proxies, welche rekursiven Resolver die Anfragen empfangen sollen [63]. Datenverlust an einer dieser Komponenten bedroht somit die Verfügbarkeit der Namensauflösung.

Kategorie	Software	CVE	CVSS V3
Remote Code Execution	Microsoft DNS	CVE-2020-1350	10.0
		CVE-2018-8626	9.8
		CVE-2020-0761	8.8
		CVE-2020-0761	8.8
	bind	CVE-2008-0122	10.0
	Powerdns	CVE-2009-4009	10.0
Denial-of-Service	Microsoft DNS	CVE-2020-0836	7.5
		CVE-2020-0993	6.5
		CVE-2020-1228	6.5
	bind	CVE-2020-8617	7.5
		CVE-2020-8616	8.6
		CVE-2016-9131	5.0
	dnsmasq	CVE-2017-14496	7.8
	Powerdns	CVE-2019-3871	6.5
Privilege Escalation	bind	CVE-2017-3141	7.8
Buffer Overflow	dnsmasq	CVE-2019-14513	5.0
	bind	CVE-2014-0591	2.6

Tabelle 4.3: Konkrete Schwachstellen und Sicherheitslücken populärer DNS-Software

B3: Denial-of-Service-Angriffe

Die größte Bedrohung gegen eine DNS-Infrastruktur sind Angriffe, die versuchen die Verfügbarkeit von DNS einzuschränken [69]. Diese Art von Angriffen werden als Denial-of-Service (Verweigerung des Dienstes, kurz DoS) bezeichnet. Gehen diese Angriffe von einer großen Anzahl an Rechnern aus, so wird der Angriff als Distributed-Denial-of-Service bezeichnet (DDoS) [46]. Bei diesen Angriffen wird versucht, den TCP/IP-Netzwerkstack zu überlasten, indem der Angreifer unzählige Pakete (ICMP, UDP, TCP SYN) an das Opfer sendet. Grundsätzlich ist jede Komponente in der DNS-Infrastruktur durch DoS-Angriffe bedroht.

Eine Angriffstechnik, die die Verfügbarkeit der rekursiven Resolver und autoritativen Nameserver bedroht, sind Pseudorandom Subdomain Attacks (PRSD). Dabei fragt ein Angreifer eine Fülle von zufällig generierten Subdomains seines Ziels an. Diese DNS-Anfragen werden vom rekursiven Resolver des Angreifers an den autoritativen Nameserver des Ziels weitergeleitet, der durch die Fülle von Anfragen schlussendlich zusammenbricht. Der rekursive Resolver des Angreifers wird durch die Menge der Anfragen

und dem früher oder später auftretenden Absturz des autoritativen Nameservers passiv mitbedroht, da dieser weiterhin versucht die Namensauflösung durchzuführen [43].

Eine Besonderheit stellen die DNS-Denial-of-Service-Angriffe dar, die die DNS-Infrastruktur als Hebel benutzen um einen Denial-of-Service-Angriff durchzuführen (vgl. 4.2.6).

B4: Bereitstellung unnötiger Betriebssystemkomponenten und Applikationen

Diese Bedrohung betrifft die rekursiven Resolver und autoritativen Nameserver und geht davon aus, dass neben der eigentlichen DNS-Serversoftware auch weitere Anwendungen auf dem Host betrieben werden. Dadurch kann einerseits die Verfügbarkeit eingeschränkt werden, da die Kapazitäten für das Betreiben von weiteren Anwendungen eventuell nicht ausreichend sind. Anderseits kann ein Angreifer durch diese Anwendungen Zugriff auf den Host erhalten. Entweder durch Schwachstellen in der betriebenen Software oder weil der Angreifer berechtigeten Zugriff auf die Anwendungen und damit auf den Server hat [69]. Des Weiteren bieten Serverbetriebssysteme wie *Windows Server* autoritative und rekursive Nameserver üblicherweise als Dienst an. Werden diese Dienste unerkannt ausgeführt, so können sie einem Angreifer eine Zugangsmöglichkeit zum Netzwerk bieten, indem Schwachstellen in der DNS-Software ausgenutzt werden (vgl. 4.2.1) [32].

B5: Fehlplanung

Rekursive Resolver und autoritative Nameserver können durch unzureichende Kapazitäten, wie beispielsweise nicht ausreichend dimensionierte Hardware überlastet werden. Zusätzlich kann die Verfügbarkeit durch fehlende Replizierung der DNS-Server bedroht werden. Aber auch die falsche Positionierung eines DNS-Servers innerhalb des Netzwerks kann dazu führen, dass nicht alle Anfragen beantwortet werden. Das kann einerseits durch eine Bandbreitenlimitierung ausgelöst werden, anderseits durch die falsche Zuordnung zu einem Netzwerksegment, so dass nicht jeder Client mit dem DNS-Server kommunizieren kann [69].

B6: Unbefugter physischer Zugriff

Kann ein Angreifer den DNS-Server durch physischen Zugriff erreichen, so kann er die Verfügbarkeit einschränken, indem er den Server vom Netzwerk trennt oder ausschaltet. Es ist auch vorstellbar, dass der Angreifer dadurch Zugriff auf die DNS-Daten erhält um diese zu modifizieren [43].

B7: Malware

Auf Windows und Mac OS X-Betriebssystemen gibt es einen lokalen Cache für den Stub-Resolver, um die Anfragezeiten von bereits besuchten Diensten zu verkürzen. Dieser Cache kann durch Systemcalls direkt beeinflusst werden, um beispielsweise das Opfer auf eine vom Angreifer kontrollierten Dienst zu leiten. Da der Cache sich nach einem Neustart leert, ist es schwieriger den Angriff zu entdecken [69]. Eine weitere Möglichkeit, um das Opfer zu täuschen, besteht darin, dass die Schadsoftware die Einträge in der *hosts*-Datei modifziert. Die hosts-Datei ist ein Überbleibsel aus der Zeit vor DNS, in der die IP-Adressen und Hostnamen der zu erreichenden Rechner manuell eingegeben wurden. Das Betriebssystem hat dann anhand der Einträge in der Datei die Namen aufgelöst. Malware kann diese Datei nutzen um Dienste, wie beispielsweise die Aktualisierungsserver der Antivirensoftware zu blockieren oder um das Opfer auf gefälschte Webseiten weiterzuleiten [13]. Sofern es einer Malware gelingt auch rekursive und autoritative Nameserver zu befallen, so wird das Bedrohungsszenario auf einen größeren Opferkreis übertragen.

4.2.2 Fehlerhafte Konfiguration

> „Running a nameserver is not a trivial task“
>
> David Barr - RFC 1912

Da das Betreiben eines DNS-Servers mit einigen Schwierigkeiten verbunden ist, wurde eigens das RFC 1912 *Common DNS Operational and Configuration Errors* veröffentlicht, das Serveradministratoren bei der Einrichtung und beim Betrieb eines DNS-Servers unterstützen soll [16]. Die Tabelle 4.4 zeigt die Bedrohungen auf, die unter fehlerhafte Konfiguration definiert werden.

Nr	Bedrohung	identifiziertes System	bedrohte Schutzziele
8	Fehlende Trennung der Zuständigkeiten	R A	A A
9	Ausführung mit erweiterten Rechten	R A	C, I, A C, I, A
10	Nutzung von öffentlichen rekursiven Resolvern	S	C, I, A
11	Fehler in den Konfigurationsdateien	R A	A A

Tabelle 4.4: Bedrohungen durch fehlerhafte Konfiguration

B8: Fehlende Trennung der Zuständigkeiten

Wird auf einem autoritativen Nameserver zusätzlich ein rekursiver Resolver betrieben, so kann die dabei entstehende zusätzliche Last den autoritativen Nameserver überlasten und somit die Verfügbarkeit der Namensauflösung einschränken [69]. Ferner wird der autoritative Nameserver für weitere Angriffe verwundbar [43]. Vice Versa bedeutet das, dass die Bedrohung auch für einen rekursiver Resolver, der die Aufgaben eines autoritativen Nameservers übernimmt, gilt.

B9: Ausführung mit erweiterten Rechten

Unter fehlerhafter Konfiguration fällt außerdem das Ausführen des DNS-Servers mit erweiterten Rechten. Eine DNS-Serveranwendung wie *BIND*, die unter dem Root- oder Administratorbenutzer ausgeführt wird, bietet einem Angreifer die Möglichkeit, beim Ausnutzen einer Remote-Code-Ausführung (Remote Code Execution, RCE) beliebigen Code als Administrator auszuführen. Damit bekommt der Angreifer uneingeschränkten Zugriff auf das System.

B10: Nutzung von öffentlichen rekursiven Resolvern

Eine weitere Bedrohung birgt die Konfiguration des DNS-Resolvers im Endsystem. Clients können selbstständig konfigurieren, welchen rekursiven DNS-Resolver sie verwenden wollen. Das kann dazu führen, dass Benutzer einen öffentlich verfügbaren DNS-Dienst, beispielsweise von Google oder Cloudflare, nutzen. Somit werden interne Dienste nicht mehr aufgelöst und die Verfügbarkeit eingeschränkt. Ferner stellen diese Dienste für einen Angreifer ein lukratives Angriffsziel dar, da mit nur einem erfolgreichen Angriff mehrere Millionen Benutzer beeinflusst werden können. Der Datenschutz dieser Anbieter ist fraglich und wird kritisch diskutiert. So speichert Google bei jeder DNS-Anfrage zusätzlich zur angefragten Domain temporär die IP-Adresse des Clients sowie permanent weitere Daten wie beispielsweise den geografischen Standort des Clients [52]. Durch diese Daten lässt sich unter anderem das Surfverhalten der Benutzer analysieren.

B11: Fehler in den Konfigurationsdateien

Neben den bereits genannten Bedrohungen müssen auch Fehler in den Konfigurationsdateien der rekursiven Resolver und autoritativen Nameserver betrachtet werden. Unbeabsichtigte Syntaxfehler können dazu führen, dass ganze Zonen nicht mehr verfügbar sind. Aufgrund des Caches der rekursiven Resolver kann das bedeuten, dass der Fehler für mehrere Stunden die Infrastruktur beeinträchtigt [69]. Ferner ist vorstellbar, dass beim Anlegen oder Ändern von Resource Records unbeabsichtigte Fehler entstehen, die dazu führen, dass der Host nicht wie erwartet erreichbar ist. Eine weitere Fehlerquelle ist das unbeabsichtigte Zuweisen desselben Hostnames an unterschiedliche IP-Adressen. Das kann dazu führen, dass der korrekte Host nur sporadisch, abhängig vom Caching, TTL des Resource Records und der im Nameserver konfigurierten Zugriffsart (zyklisch oder zufällig), erreichbar ist.

4.2.3 Organisatorische Bedrohungen

Unter organisatorischen Bedrohungen werden diejenigen Bedrohungen verstanden, die sich durch fehlende strikte organisatorische Vorgaben und Kontrollen ergeben. Die Tabelle 4.5 stellt die Organisatorischen Bedrohungen dar.

Nr	Bedrohung	identifiziertes System	bedrohte Schutzziele
12	Fehlende organisatorische Abläufe	Domain	I, A
		A	C, I, A
13	Unzureichendes Berechtigungskonzept	R	C, I, A
		A	C, I, A
14	Missbrauch von administrativen Berechtigungen	S	C, I, A
		R	C, I, A
		A	C, I, A

Tabelle 4.5: Organisatorische Bedrohungen

B12: Fehlende organisatorische Abläufe

Aufgrund der dezentralen Infrastruktur von DNS können sich auch Bedrohungen durch die organisatorischen Abläufe ergeben. Eine dieser organisatorischen Bedrohung ist gegen die Domain der Firma gerichtet. Aufgrund der verschiedenen Abteilungen, die beim Betrieb einer Domain beteiligt sind, geht eine Bedrohung von mangelnder Kommunikation zwischen den DNS-Administratoren und den zuständigen Buchhaltern der Domain aus. Sollte die Domain nicht rechtzeitig bezahlt oder verlängert werden, kann es passieren, dass der Domain-Name-Registrar die Domain wieder zur Registrierung freigibt. Ferner ist möglich, dass der zuständige Kontakt für die Domain die Position gewechselt oder die Firma gar verlassen hat. Das macht es dem Registrar deutlich schwieriger die Firma darauf hinzuweisen, dass die Registrierung der Domain abläuft. Ein Angreifer hat dann die Möglichkeit die Domain vor der Firma zu erwerben, um Besucher auf einen von ihm präparierten Host zu leiten [69].

Eine weitere Bedrohung ergibt sich aus der Verwendung von privaten Kontaktinformationen zur Registrierung der Firmendomain. Sollte der entsprechende Mitarbeiter die Firma verlassen, so hat er immer noch Zugriff auf die Domain sowie die hinterlegten Nameserver und kann die Verfügbarkeit der öffentlichen Dienste, wie Webauftritt und E-Mail-Server, einschränken.

B13: Unzureichendes Berechtigungskonzept

Außerdem kann eine Bedrohung gegen die Verfügbarkeit und Integrität der DNS-Daten von fehlender Zugangskontrolle zu den DNS-Servern ausgehen. Ein Benutzer, der ohne Berechtigung auf den DNS-Server zugreifen kann, kann die DNS-Einträge sowie die Konfigurationsdateien ändern oder löschen. Dieses Szenario kann vor allem dann auftreten, wenn neben dem DNS-Server noch andere Anwendungen auf dem Server betrieben werden auf die der Benutzer zugreifen darf (vgl. 4.2.1).

Hinzu kommt, dass die DNS-Administratoren und die Mitarbeiter mit Zuständigkeit für die Informationssicherheit oft unterschiedliche Ziele haben und in verschiedenen Teams arbeiten. Kommunikationsprobleme zwischen den Abteilungen können entstehen, da DNS-Administratoren zu wenig Erfahrung im Umgang mit IT-Sicherheit und umgekehrt die Mitarbeiter der Informationssicherheit zu wenig Erfahrung im Umgang mit DNS haben [69]. Diese Ungleichverteilung von Wissen und Informationen kann die gesamte DNS-Infrastruktur bedrohen.

B14: Missbrauch von administrativen Berechtigungen

Es gibt mehrere Bedrohungsszenarien durch Missbrauch von administrativen Berechtigungen. Im ersten Szenario sind vor allem die Verfügbarkeit und die Integrität der DNS-Daten bedroht. Ein DNS-Administrator kann, ohne geeignete Gegenmaßnahmen, seine Berechtigung missbrauchen, um die DNS-Daten auf den autoritativen Nameservern zu verändern oder zu löschen. Aber auch eine Änderung der Whois-Daten beim Registrar ist vorstellbar, um die Kontrolle über die Domain der Firma zu erlangen [69]. Das zweite Szenario geht davon aus, dass der Angreifer die IP-Adressen der zu verwendenden Nameserver der Clients durch eine Änderung im DHCP austauscht und durch eigene Nameserver ersetzt. Dadurch können interne Namen nicht mehr aufgelöst werden und jeglicher DNS-Verkehr verändert und beobachtet werden (siehe auch B16: Ausspähen des DNS-Verkehrs).

4.2.4 Spionage

> „Whilst the data in the DNS is public, individual transactions made by an end user **should not** be public.“
>
> Sara Dickinson - https://dnsprivacy.org

Die Vertraulichkeit der DNS-Daten war kein Ziel beim Entwurfs von DNS. Daraus ergeben sich neue Bedrohungen, die in der Tabelle 4.6 zusammengefasst werden. Die Internet Engineering Task Force (IETF) hat mit dem in 2014 veröffentlichten RFC 7258 *Pervasive Monitoring Is an Attack* [48] deutlich gemacht, dass das Überwachen von Kommunikationsdaten ein Angriff gegen die Privatsphäre von Personen und Organisationen ist und, sofern möglich, verhindert werden muss [48].

Nr	**Bedrohung**	**identifiziertes System**	**bedrohte Schutzziele**
15	DNS als Infil- und Exfiltrationsmedium	S	C
16	Fingerprinting	R A	C C
17	Abhören des DNS-Verkehrs	S R A	 C C

Tabelle 4.6: Bedrohungen durch Spionage

B15: DNS als Infil- und Exfiltrationsmedium

DNS eignet sich zusätzlich aufgrund der wichtigen Rolle in Netzwerken als In- und Exfiltrationswerkzeug für vertrauliche Daten. Ein interner Angreifer kann die sensitiven Daten in der Fülle aller Anfragen an den rekursiven Resolver verstecken. Hinzu kommt, dass DNS-Verkehr durch Administratoren deutlich weniger auf ungewöhnliche Aktivitäten überwacht wird als andere Protokolle [77]. Es gibt mehrere Möglichkeiten, wie ein Angreifer die Daten exfiltrieren kann. Im ersten Angriffsszenario will der Angreifer nur die vertraulichen Daten transferieren. Dafür benötigt er eine Domain und einen Nameserver. Die Daten werden vom Angreifer codiert, nummeriert und geteilt, so dass diese noch in ein UDP-Paket passen und als DNS-Nachricht an den Nameserver geschickt. Die Nachricht beinhaltet die DNS-Anfrage mit den Daten, wobei die Daten als Sub-Domain der Angreiferdomain vorangestellt werden. Der Nameserver des Angreifers protokolliert diese Anfragen und setzt die Daten anhand der Nummerierung wieder korrekt zusammen. Im zweiten Angriffsszenario erstellt der Angreifer einen Tunnel, um Daten aus dem internen Netzwerk mit dem Netzwerk des Angreifers auszutauschen. Wie im ersten Szenario schickt der Angreifer codierte und nummerierte Daten als Anfrage zu einer Sub-Domain

an den eigenen Nameserver. Anstatt die Anfrage nur zu protokollieren, antwortet der Nameserver mit einem codierten TXT Resource Record. Es entsteht folglich eine bidirektionale Kommunikation über codierte DNS-Nachrichten, die sogar für VPN- oder SSH-Tunnel genutzt werden können[4]. Dem Angreifer gelingt es dadurch, auch in sehr beschränkten Netzwerken, vertrauliche Daten zu exfiltrieren. Dasselbe Angriffsszenario eignet sich auch, um Schadsoftware in ein internes Netzwerk einzuschleusen.

Aber auch in Botnetzen, wie beispielsweise Feederbot, werden DNS-Nachrichten zur Kommunikation mit einem Command-and-Control-Server (C&C-Server) benutzt. Die Bots müssen mit dem C&C-Server kommunizieren, um einerseits abgefangene Daten, wie beispielsweise Zugangs- oder Kreditkartendaten, zu übermitteln, andererseits benötigen sie vom Betreiber das nächste Angriffsziel oder die nächste Aufgabe. Damit diese bidirektionale Kommunikation möglichst lange unerkannt bleibt, verwenden Botnetz-Betreiber DNS-Nachrichten für die Übertragung [42].

B16: Fingerprinting

Fingerprinting bezeichnet das Abfragen von Servern, um Informationen über die ausgeführten Dienste sowie über das Betriebssystem zu erlangen [69]. Dieses Vorgehen wird oft eingesetzt, um den Server hinsichtlich möglicher Schwachstellen zu überprüfen. Sicherheitslücken und Schwachstellen werden unter dem Industriestandard Common Vulnerabilities and Exposures (CVE) veröffentlicht und klassifiziert. Die Liste der Schwachstellen, bis hin zu vorgefertigten Skripten um diese Schwachstellen auszunutzen, werden im Internet veröffentlicht und sind somit für einen potentiellen Angreifer zugänglich[5].

Durch gezielte Abfragen eines DNS-Servers können Informationen über das Betriebssystem und die verwendete DNS-Software in Erfahrung gebracht werden [69]. In Regelmäßigen Abständen scannt das Internet Systems Consortium (ISC) das Internet nach verfügbaren DNS-Servern und zeichnet die verwendeten Anwendungen inklusive Version auf. Diese Scans zeigen, dass viele DNS-Server mit alten Versionen betrieben werden und somit für bekannte Sicherheitslücken anfällig sind [34].

Da viele Unternehmen ihre eigenen autoritativen Nameserver hosten, besteht ein Risiko darin, dass ein Angreifer aufgrund von Fingerprinting eine Schwachstelle im Betriebssystem oder DNS-Server findet und ausnutzt (siehe B1: Software-Schwachstellen oder

[4] durch Tools wie DeNiSe, DNScapy, Iodine oder dnscat2
[5] beispielsweise auf https://www.mitre.org/ und https://www.exploit-db.com/

-Fehler). Da diese Art von Bedrohung leicht automatisiert werden kann, kann ein Unternehmen auch nur zufällig zum Ziel eines Angreifers werden.

Es eignen sich unterschiedliche Techniken damit ein Angreifer mittels DNS-Anfragen an Informationen über die betriebene Infrastruktur gelangt. Eine Variante sind Wildcard-Queries an autoritative Nameserver. Dafür muss der Angreifer nur eine einzige DNS-Anfrage stellen und bekommt vom Nameserver alle Resource Records der Domäne zurückgeliefert [74]. Name Guessing beschreibt ein weiteres Angriffsszenario, das DNS-Anfragen ausnutzt um an Informationen über Hosts des autoritativen Nameservers zu gelangen und kann genutzt werden, wenn die Nutzung von Wildcard-Queries deaktiviert wurde. Dabei schickt ein Angreifer viele generierte DNS-Anfragen an den autoritativen Nameserver des Opfers und versucht eine legitime Antwort zu produzieren. Sollte der Angreifer einen Hostname auflösen können, so hat dieser nun Kenntnis über den Host und kann weitere Angriffe durchzuführen [43]. Aber auch die Kenntnis der Hostnamen kann ein Risiko sein. So können diese Aufschluss über Produktiv- und Testumgebungen oder neue Produkte geben.

Eine weitere Variante sind sogenannte Version-Queries, die die Version des betriebenen DNS-Servers zurückliefert und vom Angreifer zum Ausnutzen von Schwachstellen des betriebenen DNS-Servers genutzt werden können [43].

B17: Abhören des DNS-Verkehrs

Diese Bedrohung zielt auf das Abhören des DNS-Verkehrs ab. Die DNS-Transaktionsdaten sind für einen Angreifer interessant, vor allem da die darrauffolgende Kommunikation mit dem Partner zumeist verschlüsselt abläuft. DNS ist demzufolge in der Kommunikation zwischen zwei Parteien oft das schwächste Glied in der Kette [20]. Es gibt mehrere Möglichkeiten für einen Angreifer den DNS-Verkehr abzuhören. Dabei ist die Kommunikation zwischen dem Stub-Resolver und dem rekursiven Resolver am wertvollsten, da diese Kommunikation nicht vom Caching der rekursiven Resolver beeinflusst wird [20].

Eine Möglichkeit zum Abhören des DNS-Verkehrs bieten die DNS-Server selbst an. DNS-Administratoren besitzen Zugriff auf die rekursiven und autoritativen Nameserver und können ihre Berechtigung ausnutzen um den DNS-Verkehr mitzulesen (siehe auch B13: Missbrauch von administrativen Berechtigungen aus 4.2.3). Dazu können Programme ausgenutzt werden, die die DNS-Software bereits standardmäßig mitbringt, wie beispielsweise *query log* von *BIND* oder *tcpdump* [20]. Im Falle des rekursiven Nameservers kann

ein DNS-Administrator jede Anfrage eines Clients abhören. Es lassen sich nicht nur Schlüsse über die genutzten Dienste und besuchten Websites ziehen, sondern auch zu den Arbeitszeiten des Benutzers. Diese Informationen könnten genutzt werden, um weitere Angriffe durchzuführen. Bei Beobachtung des autoritativen Nameservers können vor allem die Anfragen der rekursiven Resolver abgehört werden. Diese Anfragen sind für Angreifer deutlich weniger interessant, da aufgrund des Cachings der rekursiven Resolver nicht alle Anfragen an den autoritativen Nameserver geschickt werden und die rekursiven Resolver für eine Fülle von Clients die Namensauflösung betreiben. Es ist daher schwieriger für den Angreifer die Anfragen den richtigen Clients zuzuordnen. Dennoch können diese Informationen für einen Angreifer benutzt werden, um weitere Angriffe zu planen.

Eine weitere Möglichkeit zum Abhören des DNS-Verkehrs bietet sich einem Angreifer, sofern dieser die Kommunikation zu den rekursiven Resolvern oder autoritativen Nameservern belauschen kann. Sollte der Angreifer keine andere Lauschmöglichkeit haben, die darauffolgende Kommunikation zwischen den Parteien abzuhören, so kann er zumindest die DNS-Daten verwenden um weitere Informationen über das Opfer zu sammeln.

Wie kritisch das Abhören des DNS-Verkehrs sein kann, zeigt das von der National Security Agency (NSA) ins Leben gerufene Programm MORECOWBELL (MCB). MCB ist ein verteiltes System, das mittels DNS und HTTP-Anfragen die Verfügbarkeit von Zielen beobachtet und diese Daten an die NSA zurückliefert. Es wird gemutmaßt, dass die Infrastruktur unter anderem betrieben wird um die Wirksamkeit von Cyberangriffen gegen die Ziele zu ermitteln (sog. battle damage indication). MCB wird außerhalb der USA in mehreren Ländern, darunter Deutschland, betrieben damit unter anderem die Fülle der DNS-Anfragen nicht der US-Regierung zugeschrieben werden können [54].

4.2.5 Social Engineering

Die Domain ist ein wesentlicher Teil von DNS. Da Privatpersonen und Unternehmen in der Regel keine eigene Top-Level-Domain besitzen, müssen diese bei einer Registrierungsorganisation, wie beispielsweise der DENIC eG[6] für die Top-Level-Domain *.de*, angemietet werden. Dabei wird oft ein Provider als Mittelsmann eingesetzt. Dort ergibt sich das folgende Bedrohungsszenario, das zusätzlich in der Tabelle 4.7 dargestellt wird.

[6] www.denic.de

Nr	Bedrohung	identifiziertes System	bedrohte Schutzziele
18	Social Engineering	Domain A	A C, I, A

Tabelle 4.7: Bedrohungen durch Social Engineering

B18: Social Engineering

Social Engineering (auch Social Hacking) sind Angriffe nicht technischer Natur, die versuchen das Opfer dazu zu bringen, sensitive Informationen an den Angreifer preiszugeben [46] oder so zu manipulieren, dass es für den Angreifer vorteilhafte Aktionen ausführt. Da eine Domain nur bei einem Registrar angemietet werden kann und dieser die Domain, einschließlich Nameserver-Einträge, verwaltet, entsteht ein Bedrohungsszenario durch Social Engineering zur Übernahme der Domain (Domain-Hijacking) oder zur Manipulation der Resource Records. Bei Verwendung eines firmeneigenen autoritativen Nameservers für die Domain, besteht das Risiko in der Veränderung des NS Resource Records, da ein Angreifer diese Einträge ändern kann um so einen eigenen autoritativen Nameserver für die Domain bereitzustellen.

In beiden Fällen wird ein Helpdesk-Mitarbeiter des Domain-Name-Registrars vom Angreifer kontaktiert und versucht durch eine vorgetäuschte Notsituation Kontrolle über die Domain bzw. Zugang zum Verwaltungsportal zu erlangen. Der Angreifer gibt beispielsweise vor, dass er ein Mitarbeiter der Firma ist und sein Passwort für das Verwaltungsportal vergessen hat. Er führt aus, dass in der Firma aktuell die Mailserver ausgefallen sind und er deshalb sein Passwort nicht zurücksetzen kann, da die E-Mail zum Zurücksetzen des Passworts nicht übermittelt wird. Er bietet dem Helpdesk-Mitarbeiter als Legimitation eine Unterschrift auf Papier mit Firmenaufdruck per Fax an. Ferner nutzt er die Hilfsbereitschaft des Mitarbeiters aus, indem er behauptet, dass der Firmeninhaber androht den Angreifer zu kündigen, sofern dieser nicht sofort den angeblichen Fehler behebt. Die Aufgabe eines Helpdesk-Mitarbeiters ist es, dem Kunden zu helfen und ihn bei seiner Arbeit zu unterstützen, daher sind Helpdesk-Mitarbeiter meist besonders hilfsbereit [69]. Nachdem der Mitarbeiter das Passwort zurückgesetzt und dem Angreifer das neue Passwort mitgeteilt hat, hat dieser uneingeschränkten Zugriff auf die Domain. Er kann die Einträge der Nameserver verändern oder die Webpräsenz und Dienste durch eigene

Kopien austauschen. Ein Angreifer benötigt für diese Art von Angriff nicht zwangsläufig Kontakt mit dem Opferunternehmen und stellt dennoch eine Bedrohung gegen die Vertraulichkeit, Integrität und Verfügbarkeit dar.

4.2.6 DNS-Reflektierungsangriffe

Im Gegensatz zur Bedrohung B3: Denial-of-Service-Angriffe, in der die DNS-Infrastruktur durch Denial-of-Service-Angriffe direkt bedroht wird, ist in diesem Bedrohungsszenario die DNS-Infrastruktur der Hebel für einen Denial-of-Service-Angriff, indem ein Opfer mit DNS-Antworten überhäuft wird. Dafür werden offene rekursive Resolver als Verstärker missbraucht. Im Folgenden werden zwei Angriffsszenarien vorgestellt, mittels derer ein DNS-Denial-of-Service-Angriff durchgeführt werden kann. Eine Besonderheit dieser Angriffe ist, dass der Angreifer keine Verbindung mit dem Opfer aufbauen muss und somit für das Opfer anonym bleibt. Lediglich die IP-Adresse des anzugreifenden Dienstes muss dem Angreifer bekannt sein.

Die Bedrohungen zielen auf ein Einschränken der Verfügbarkeit ab. Dabei kann sowohl die eigene DNS-Infrastruktur ausgenutzt werden, als auch das Ziel dieser Angriffe sein. Im ersten Fall wird die Verfügbarkeit bedroht, da die Infrastruktur die Menge der Anfragen ggf. nicht mehr bearbeiten kann. Zusätzlich werden die Betreiber unwissentlich zum Mittäter einer Straftat. Der zweite Fall wird durch die Bedrohung B3: Denial-of-Service-Angriffe (vgl. 4.2.6) abgedeckt. Die Bedrohungen durch DNS-Reflektierungsangriffe werden in der Tabelle 4.8 zusammengefasst.

Nr	**Bedrohung**	**identifiziertes System**	**bedrohte Schutzziele**
19	DNS-Reflection	R	A
20	DNS-Amplification	R	A

Tabelle 4.8: Bedrohungen durch DNS-Denial-of-Service

B19: DNS-Reflection

Wie in 2.2 beschrieben, wird zur Kommunikation mit DNS das verbindungslose und nicht zuverlässige, sowie auch ungeschützte Transportprotokoll User Datagram Protocol (UDP) verwendet. DNS-Reflection-Angriffe nutzen die Fälschbarkeit von IP-Adressen

(IP-Spoofing) aus um ein Opfer mit massenweisen Antworten von rekursiven Resolvern zu überhäufen. Ein DNS-Reflection-Angriff läuft wie folgt ab: Ein Angreifer platziert die IP-Adresse des Opfers als Quell-IP-Adresse einer DNS-Anfrage. Diese DNS-Anfrage wird an einen offenen rekursiven Resolver verschickt, der die Antwort der Anfrage an das Opfer sendet. Das Opfer bekommt folglich eine Antwort auf eine DNS-Anfrage, die es nie gestellt hat (die Antwort wird reflektiert). Da nur eine Antwort jedoch für das Opfer nicht wahrnehmbar ist, verschicken Angreifer viele tausende von Anfragen, oft auch von verschiedenen Hosts, um die Stärke des Angriffes zu erhöhen [25]. Das Opfer wird so überlastet und kann nicht mehr alle Anfragen verarbeiten, was wiederum zu einer Einschränkung der Verfügbarkeit führt.

B20: DNS-Amplification

Ein DNS-Amplification-Angriff funktioniert nach demselben Prinzip wie ein DNS-Reflection-Angriff. Der Angreifer fälscht die IP-Adresse seines Opfers und verschickt tausende von DNS-Anfragen an einen offenen rekursiven Resolver. Bei dieser Art von Angriff wird sich aber einer Besonderheit von DNS bedient, und zwar das die UDP-Pakete von einigen DNS-Anfragen deutlich kleiner sind als die UDP-Pakete der DNS-Antworten [69]. Damit entsteht ein Hebel, der die zu verarbeiteten Daten auf Seiten des Opfers signifikant erhöht. So benötigt ein Angreifer deutlich weniger Ressourcen (Hosts und Anfragen) um die Verfügbarkeit von Diensten zu beeinträchtigen. Der Angriff wird durch die offenen rekursiven Resolver, die ohnehin mehrere Millionen von Anfragen problemlos bewältigen können, verstärkt[7].

Die Auflistung 4.1 zeigt eine Anfrage mittels *dig* [1] zur Namensauflösung des A-Records von *haw-hamburg.de*. Als rekursiver Resolver wurde hier auf einen öffentlichen Resolver von Google zurückgegriffen. An dieser Antwort lässt sich erkennen, dass die *Query Size* (Anfragegröße) 55 Bytes und die *Msg size* (empfangene Nachrichtengröße) 59 Bytes groß sind. In der zweiten Auflistung 4.2 wurde nicht nur nach dem A-Record, sondern nach allen Resource Records von *haw-hamburg.de* gefragt. Hier ist die Anfragegröße erneut 55 Bytes, die Antwort hingegen 680 Bytes groß. Die Antwort ist somit zwölf mal größer als die Anfrage.

Auflistung 4.1: DNS-Anfrage zur Auflösung des A-Records von *haw-hamburg.de*

```
; <<>> DiG 9.16.7 <<>> +qr @8.8.8.8 haw-hamburg.de A
```

[7] beispielsweise offene Resolver von Cloudflare oder Google

```
[...]
;; QUERY SIZE: 55
[...]
;; Query time: 13 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
[...]
;; MSG SIZE  rcvd: 59
```

Auflistung 4.2: DNS-Anfrage zur Auflösung aller Resource Records von *haw-hamburg.de*

```
; <<>> DiG 9.16.7 <<>> +qr @8.8.8.8 haw-hamburg.de ANY
[...]
;; QUERY SIZE: 55
[...]
;; Query time: 73 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
[...]
;; MSG SIZE  rcvd: 680
```

4.2.7 DNS-Spoofing

Spoofing bezeichnet eine Angriffsklasse von Maskierungsangriffen, die das Ziel haben eine falsche Identität vorzugeben [46]. Im Kontext von DNS bedeutet Spoofing, dass eine DNS-Antwort an einen Client verändert wird um ihn so auf einen anderen Dienst fehlzuleiten. Es wird somit die Integrität der DNS-Daten bedroht und die Verfügbarkeit der Ressource eingeschränkt. Die Tabelle 4.9 fasst die Bedrohungen durch DNS-Spoofing zusammen.

Nr	**Bedrohung**	**identifiziertes System**	**bedrohte Schutzziele**
21	Cache Poisoning	R	I, A
22	Man-in-the-Middle	S R A	C, I, A C, I, A C, I, A
23	DNS-Hijacking	S	C, I, A

Nr	Bedrohung	identifiziertes System	bedrohte Schutzziele
24	Zone Poisoning mittels Zonentransfers	A	C, I, A
25	Zone Poisoning mittels dynamischer Updates	A	I, A

Tabelle 4.9: Bedrohungen durch DNS-Spoofing

B21: Cache Poisoning

Cache Poisoning bezeichnet ein Angriffsszenario, bei dem der Cache des Opfers mit gefälschten Resource Records befüllt wird. Der Angriff wird auch manchmal nach seinem Entdecker Dan Kaminsky als *Kaminisky Attack* bezeichnet und läuft wie folgt ab: Ein Angreifer möchte den Cache des rekursiven Resolvers seines Opfers mit gefälschten Resource Records vergiften. Dazu muss er in der Lage sein, an den rekursiven Resolver seines Opfers beliebige DNS-Anfragen zu stellen. Das ist beispielsweise gewährleistet, wenn beide einen offenen Resolver von einem kostenlosen Anbieter oder ISP verwenden oder der rekursive Resolver des Opfers unbeabsichtigt offen zugänglich betrieben wird (vgl. 4.2.6). Der Angreifer wählt nun eine Domain aus, von der er ausgeht, dass das Opfer diesen Dienst in Zukunft benutzen wird und schickt an den rekursiven Resolver eine DNS-Anfrage zur Auflösung einer nicht existenten Sub-Domain. Der rekursive Resolver versucht daraufhin die Anfrage mittels des autoritativen Nameservers der ausgewählten Domain aufzulösen. Das Ziel des Angreifers ist es, die Antwort des autoritativen Nameservers erfolgreich zu fälschen und somit die Anfrage schneller als der legitime, für die Domain zuständige, autoritative Nameserver zu beantworten. In der gefälschten Antwort des Angreifers befindet sich ein NS Resource Record sowie ein Glue Record der den Nameserver der Domain auf eine vom Angreifer kontrollierte IP-Adresse zeigen lässt. Da rekursive Resolver die Resource Records von autoritativen Nameservern, abhängig von der TTL, zwischenspeichern, würde das Opfer beim Besuch der ausgewählten Domain auf die vom Angreifer kontrollierte Infrastruktur fehlgeleitet. Schlägt der Angriff fehl, so kann der Angreifer durch eine erneute Anfrage für eine andere, nicht existente, Sub-Domain den Angriff wiederholen.

Das Fälschen der Antwort funktioniert folgendermaßen: Jede DNS-Anfrage besitzt im Header eine 16-bit große Transkations-ID. Diese ID wird vom Anfragenden für jede An-

frage generiert und dient dem Client der Zuordnung der Antwort zur Anfrage [69]. DNS-Anfragen werden, seit Einführung der *Source Port Randomization*, von einem beliebigen freien Port des Clients verschickt [69]. Ein Angreifer muss, damit das Cache Poisoning erfolgreich ist, die Transkations-ID sowie den Quell-Port des Clients erraten. Das kann der Angreifer durch einfaches ausprobieren aller erdenklichen Möglichkeiten erreichen (Brute-Force-Methode). Insgesamt gibt es für die korrekte Kombination von Transaktions-ID und Quell-Port 2^{32} Möglichkeiten, die sich aus den 2^{16} möglichen Transaktions-IDs und 2^{16} möglichen Quell-Ports des Clients zusammensetzen [12].

Der Suchraum wird deutlich verringert, sobald durch die Implementierung des Resolvers inkrementelle Transkations-IDs verwendet werden oder die Generierung der Transaktions-IDs anhand eines Musters nachvollzogen werden kann. Sollte der Quell-Port der Anfrage vordefiniert sein, entweder durch eine Konfiguration oder Implementierung eines Resolvers oder durch Firewalls im Unternehmen, so muss nur die Transaktions-ID erraten werden [12].

Der Angreifer kann den Suchraum allerdings auch durch Anwendung des Geburtstagsangriffs signifikant verringern. Ein Geburtstagsangriff ist ein Kollisionsangriff, der das Geburtstagsparadoxon ausnutzt [46]. Das Geburtstagsparadoxon besagt, dass die Wahrscheinlichkeit, dass zwei Menschen in einem Raum mit 23 Personen am gleichen Tag Geburtstag haben, über 50% beträgt. Da diese Annahme für die meisten Menschen nicht auf Anhieb intuitiv nachvollziehbar ist, wird dieses Phänomen als Paradoxon beschrieben [8]. Bisher hat der Angreifer immer nur versucht, für ein Paket eine Transaktions-ID sowie den Quell-Port zu erraten. Daher ist die Wahrscheinlichkeit, die korrekte Kombination zu treffen 1 zu 2^{32} (= 4.294.967.296). Schickt der Angreifer nun aber eine Fülle von Anfragen und versucht irgendeine beliebige Transaktions-ID und Quell-Port-Kombination zu treffen, so nähert sich die Wahrscheinlichkeit an 1 zu 291.700. Im Fall, dass nur die Transaktions-ID oder der Quell-Port gefunden werden muss, so müssen nur circa 1.140 Pakete verschickt werden. Abbildung 4.3 stellt jeweils die Kollisionswahrscheinlichkeiten bei unterschiedlicher Anzahl an Paketen unter der Verwendung der zwei Vorgehensweisen dar. Dabei ist zu erkennen, dass der Angreifer bereits ab 300 parallel verschickten Paketen, eine Wahrscheinlichkeit von 50% besitzt um die richtige Transaktions-ID zu erraten. Für die Berechnung der Wahrscheinlichkeiten wurde auf die Formel aus der Abbildung 4.4 zurückgegriffen.

Im November 2020 wurde auf der ACM Conference on Computer and Communications Security (CCS) eine neue Möglichkeit des DNS Cache Poisonings vorgestellt. Der Angriff

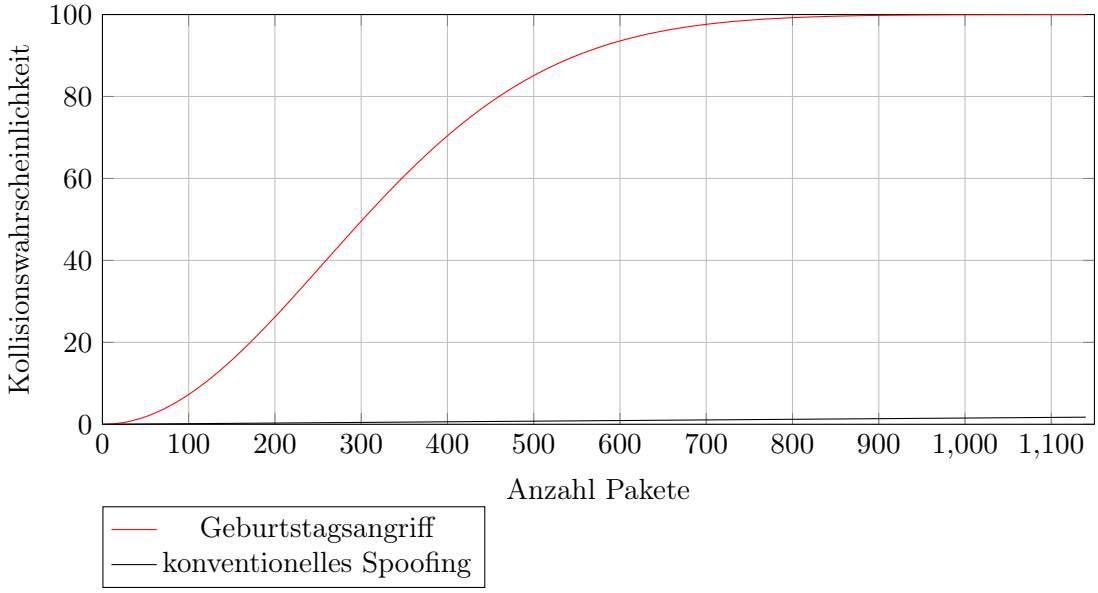


Abbildung 4.3: Geburtstagsangriff (rot) vs. konventionelles Spoofing (schwarz)

Quelle: In Anlehnung an [87]

$$\textit{Probability of Collision} = 1 - \left(1 - \frac{1}{t}\right)^{\frac{n \times (n-1)}{2}}$$

Abbildung 4.4: Wahrscheinlichkeit einer Kollision [87]

wird als SAD DNS (kurz für Side-channel Attacked DNS) bezeichnet. Die Forscher haben heraus gefunden, dass 34% der öffentlichen Resolver, darunter Google und Cloudflare, für den Angriff anfällig sind. SAD DNS benutzt ICMP und ICMP Rate Limiting um die offenen, verwendeten Quell-Ports eines rekursiven Resolvers zu finden. Dadurch ist es den Forschern gelungen, den Suchraum für Brute-Force-Angriffe deutlich zu verkleinern ($2^{16} + 2^{16} = 131.072$)[70].

B22: Man-in-the-Middle

Ein Angreifer, der Kontrolle über den Datenverkehr zwischen Stub-Resolver und rekursivem Resolver oder rekursivem Resolver und autoritativem Nameserver hat, kann mittels eines Man-in-the-Middle-Angriffs DNS-Anfragen abfangen und verändern. Dabei können sowohl die rekursiven Resolver als auch die Stub-Resolver betroffen sein, je nachdem an

welcher Stelle im Netzwerk der Angreifer die Pakete abfängt. Da die DNS-Nachrichten als unsignierte und unverschlüsselte UDP-Pakete verschickt werden, kann ein Empfänger die Authentizität sowie Integrität der Nachricht nicht festellen [15]. Man-in-the-Middle-Angriffe eignen sich zusätzlich zur Einschränkung der Verfügbarkeit der Namensauflösung, indem der Angreifer einige Resource Records aus den Antworten der Resolver entfernt oder durch *NXDOMAIN* ersetzt.

B23: DNS-Hijacking

Cache Poisoning und Man-in-the-Middle-Angriffe sind bösartige Bedrohungsszenarien die mittels Spoofing die Integrität der DNS-Daten und die Verfügbarkeit der Dienste bedrohen. Es gibt aber auch ein Bedrohungsszenario durch nicht bösartiges Spoofing. Einige Internet Service Provider leiten ihre Kunden bei Benutzung des ISP eigenen Resolvers auf eigene Webseiten um, sofern diese eine Domain anfragen, die nicht existiert. Der Benutzer bekommt folglich anstatt eines Fehlers, dass die Domain nicht existiert (*NXDOMAIN*) eine Webseite des Providers angezeigt, die die angefragte Webseite als Suchbegriff nutzt und dazu Suchergebnisse und Werbung anzeigt. Da diese Funktion nicht nur für die Anfragen von Webseiten gilt, sondern für jegliche DNS-Anfragen, kann es passieren, dass Anwendungen auf dem Client fehlerhaft reagieren. Sofern der Benutzer zwischen Firmennetzwerk und privaten Netzwerk hin und her wechselt, beispielsweise durch eine VPN-Verbindung, entsteht das Bedrohungsszenario, dass der Stub-Resolver die falschen Antworten des ISPs zwischenspeichert und somit die Verfügbarkeit der Dienste über die VPN-Verbindung einschränkt. Ein weiteres Problem besteht darin, dass vertrauliche Daten wie Session Cookies an diesen Dienst übermittelt werden können, sofern der DNS-Server kurzfristig nicht erreichbar ist [30]. Ferner können Provider gezwungen durch Regierungen oder gesetzliche Regelungen, die Verfügbarkeit von Diensten mittels Spoofing einschränken, indem sie legitime Domains als nicht existent an den Client zurückmelden.

B24: Zone Poisoning mittels Zonentransfers

Beim Betrieb von mehreren autoritativen Nameservern wird üblicherweise ein Nameserver als primärer Nameserver (Master) ausgewählt, auf dem die Zoneninformationen aktualisiert werden. Die anderen autoritativen Nameserver agieren als sekundäre Nameserver (Slave) und aktualisieren ihre Resource Records durch den primären Nameserver

mittels Zonentransfers. Dadurch entsteht für die Systemadministratoren weniger Wartungsaufwand, da die Zoneninformationen nur an einer Stelle gepflegt werden müssen [32]. Zonentransfers können durch zwei Verfahren angestoßen werden. Im ersten Verfahren schickt der primäre Nameserver nach einem Update seiner Zoneninformationen eine *DNS NOTIFY*-Transaktionsnachricht an die sekundären Nameserver, die daraufhin die kompletten Zoneninformationen des Masters abrufen und speichern. Im zweiten Verfahren ruft der sekundäre Nameserver in definierten Abständen den SOA Resource Record vom primären Nameserver ab und vergleicht die Seriennummern. Die Seriennummer wird bei jedem Update der Zoneninformationen inkrementiert und dient dem sekundären Nameserver als Indiz dafür, ob die eigenen Zoneninformationen aktualisiert werden müssen.

Da bei einem Zonentransfer deutlich mehr Daten als bei einer DNS-Anfrage oder Antwort veröffentlicht werden und somit die Bandbreite und Bearbeitungszeit der Anfrage steigt, kann ein Angreifer mittels einer Fülle von gefälschten *DNS NOTIFY*-Nachrichten die autoritativen sekundären Nameserver überlasten. Es existiert ein zweites Bedrohungsszenario, da die Zoneninformationen von einem Angreifer abgefangen und verändert werden können, so dass die Integrität der Daten auf den sekundären Nameservern gefährdet ist [32]. Die Zoneninformationen könnten einem Angreifer auch hilfreich sein um weitere Ziele im Netzwerk zu finden [69].

B25: Zone Poisoning mittels dynamischer Updates

Dynamische Updates werden in RFC 2136 [22] beschrieben und haben das Ziel, Zoneninformationen in autoritativen Nameservern dynamisch zu aktualisieren. Damit soll der Wartungsaufwand der Systemadministratoren verringert werden. Ein klassischer Anwendungsfall ist DHCP. Der DHCP-Server vergibt an einen Client eine neue IP-Adresse, da der Lease abgelaufen ist und schickt danach eine *UPDATE*-Nachricht an den autoritativen Nameserver, der daraufhin die Zuordnung des Clients aktualisiert [32]. Dynamische Updates können von einem Angreifer missbraucht werden und bieten daher verschiedene Bedrohungsszenarien.

Ein Angreifer könnte die *UPDATE*-Nachrichten fälschen und somit die Resource Records in den autoritativen Nameservern modifizieren. Es ist vorstellbar, dass der Angreifer legitime Einträge für Dienste wie beispielsweise Proxy-Server durch eigene Dienste ersetzt und somit den Datenverkehr umleitet [69]. Eine weitere Bedrohung geht davon aus, dass

der Angreifer die dynamischen Updates eines Clients aufzeichnet und zu einem späteren Zeitpunkt wieder einspielt (Replay Attacke) um die Verfügbarkeit einzuschränken. Der Angreifer könnte beispielsweise die Nachricht genau dann erneut einspielen, wenn der Lease der IP-Adresse des Clients abgelaufen ist. Der primäre Nameserver würde dem Client dann die alte IP-Adresse zuweisen, so dass dieser nicht mehr über seinen FQDN erreichbar ist [84].

4.2.8 DNS-Rebinding

Die Bedrohung DNS-Rebinding wird im Folgenden erläutert und in der Tabelle 4.10 zusammengefasst.

Nr	**Bedrohung**	**identifiziertes System**	**bedrohte Schutzziele**
26	DNS-Rebinding	S	I, A

Tabelle 4.10: Bedrohungen durch DNS-Rebinding

B26: DNS-Rebinding

Eine weitere Angriffsklasse beinhaltet Server-Side-Request-Forgery-Angriffe (SSRF). Diese Angriffe nutzen Dienste aus, um die für den Angreifer nicht direkt zugängliche interne Infrastruktur anzugreifen [90]. Das Opfer wird somit zum Proxy für den Angreifer. DNS-Rebinding beschreibt einen derartigen SSRF-Angriff mittels DNS. Dazu benutzt der Angreifer DNS-Einträge mit einer kurzen TTL für eine von ihm kontrollierte Domain [23]. Nachfolgend werden zwei Angriffe mittels DNS-Rebinding beschrieben.

Im ersten Angriffsszenario versucht der Angreifer die Same-Origin-Policy (SOP) vom Browsers des Opfers zu umgehen. SOP ist ein wesentliches Sicherheitsmerkmal von modernen Browsern und soll verhindern, dass clientseitige Skriptsprachen auf andere, nicht dem Ursprung des Skripts entsprechende, Domains zugreifen [23]. Der Angreifer bringt nun das Opfer dazu, die Domain des Angreifers zu besuchen. Nachdem das Opfer die Website besucht hat, wird ein Skript im Browser des Clients ausgeführt. Dieses Skript kann beispielsweise aktuelle Exploits gegen den Router des Opfers enthalten mit dem Ziel die Konfiguration so anzupassen, dass dem Angreifer Zugriff gewährt wird. Das Skript führt diese Aktionen aber erstmalig nicht gegen den Router des Opfers durch, sondern gegen

die Domain des Angreifers, da die SOP einen Zugriff auf den internen IP-Adressbereich verhindern würde. Aufgrund der kurzen TTL des Resource Record wird die Domain des Angreifers erneut vom DNS-Stub-Client angefragt. Diesmal gibt der autoritative Nameserver aber nicht die IP-Adresse des Webservers der Domain zurück, sondern die interne IP-Adresse vom Router des Opfers. Nun führt das Skript die Aktionen gegen den Router durch, da die SOP vom Browser umgangen worden ist.

Im zweiten Szenario benutzt der Angreifer Schwachstellen in öffentlich zugänglichen Diensten um einen DNS-Rebinding-Angriff auszuführen. Das können beispielsweise Webanwendungen sein, die dem Angreifer erlauben eigene Webhooks zu erstellen ohne die Antworten des DNS-Server zu validieren. Der vom Angreifer angelegte Webhook führt nach einem erfolgreichen DNS-Rebinding-Angriff die Aktionen gegen die interne Infrastruktur des Dienstes aus.

Beide Szenarios sind vorstellbar damit ein Angreifer Zugriff auf das interne Netzwerk des Opfers bekommt. Im internen Netzwerk bedroht der Angreifer die Vertraulichkeit, Integrität und Verfügbarkeit von Diensten und Daten. Er kann Daten veröffentlichen, verändern und löschen sowie interne Dienste angreifen, um die Verfügbarkeit einzuschränken.

Durch Frameworks wie beispielsweise Electron[8], entstehen weitere Bedrohungsszenarien durch DNS-Rebinding, da diese Webanwendungen auf den Desktop bringen und die Inhalte mittels eines integrierten, für den Ausführenden unsichtbaren, Webbrowser ausführen. Dabei sind besonders die Anwendungen betroffen, die eingebette Inhalte von dritten Parteien anzeigen können. Populäre Anwendung auf Basis von Electron sind beispielsweise die Texteditoren Microsoft Visual Studio Code[9] und Atom[10], sowie die Kommunikationsplattformen Microsoft Teams[11] und Slack[12].

4.2.9 Ausfall oder Störung von Dienstleistern

Nicht nur bei der Domain-Registrierung sind Privatpersonen und Unternehmen auf fremde Mithilfe angewiesen, sondern mitunter auch bei der Namensauflösung durch rekursive

[8] https://www.electronjs.org/
[9] https://code.visualstudio.com/
[10] https://atom.io/
[11] https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software
[12] https://slack.com/

Resolver. Dadurch entsteht das folgende Bedrohungsszenario, das in der Tabelle 4.11 zusammengefasst wird.

Nr	**Bedrohung**	**identifiziertes System**	**bedrohte Schutzziele**
27	Ausfall oder Störung von Dienstleistern	S R A	A A A

Tabelle 4.11: Bedrohungen durch Ausfall oder Störung von Dienstleistern

B27: Ausfall oder Störung von Dienstleistern

Da DNS ein verteiltes System ist, können Komponenten auch an externe Dienstleister ausgelagert werden. Dabei wird im Falle einer Störung oder gar eines Ausfalls der Infrastruktur des Dienstleisters die Verfügbarkeit der Namensauflösung bedroht. Je nachdem welche Komponente ausgelagert wurde, entweder der rekursive Resolver oder der autoritative Nameserver, betrifft die Bedrohung unterschiedliche Benutzer und Systeme.

4.3 Risikoanalyse

Die identifizierten, allgemeingültigen Bedrohungen gegen eine DNS-Infrastruktur werden nun in der Risikoanalyse bewertet und auf das Anwendungsszenario übertragen. Das Ergebnis der Risikoanalyse ist die Grundlage für die Evaluation, in der gezeigt werden soll, ob und wie die DNS-Sicherheitserweiterungen das Risiko minimieren können. Die durchgeführte Risikoanalyse orientert sich dabei am BSI-Standard 200-3, auf Basis des IT-Grundschutzes.

Der BSI-Standard sieht vor, dass zunächst eine Gefährdungsübersicht erstellt werden muss. Diese beinhaltet die im IT-Grundschutz klassifizierten elementaren und, darüber hinaus, weitere mögliche Gefährdungen, die auf die jeweiligen Bausteine abgebildet werden. Das Ziel der Gefährdungsübersicht ist dabei, herauszufinden inwieweit die Gefährdungen für das Zielobjekt relevant sind. Die Gefährdungsübersicht enthält, nach Abschluss der Zuordnung, die Zielobjekte mit den relevanten Gefährdungen, für die dann der Schutzbedarf ermittelt werden muss [24]. Die Identifizierung der Gefährdungen sowie die Ermittelung des Schutzbedarfs wurde bereits in der Bedrohungsanalyse durchgeführt. Daher wird direkt mit der Einschätzung der Risiken begonnen.

Das Risiko einer Bedrohung setzt sich aus der Eintrittshäufigkeit der Gefährdung und der Schadenshöhe zusammen. Die Schadenshöhe wird anhand der Auswirkung der Gefährdung, also direkte Schäden und Folgeschäden sowie am Aufwand zur Behebung des Schadens geschätzt. Die Eintrittshäufigkeit soll laut BSI, durch geeignetes Fachpersonal, ggf. unterstützend durch Statistiken und eigene Erfahrungen, eingeschätzt werden. Anstatt der Eintrittshäufigkeit wird in dieser Risikoanalyse von einer Eintrittswahrscheinlichkeit ausgegangen, da man die Bedrohungen gegen eine DNS-Infrastruktur unter anderem davon abhängig machen kann, wieviel Aufwand ein Angreifer zur Durchführung eines Angriffs benötigt [46]. Zusätzlich kann anhand von frei verfügbaren Sicherheitslücken und Exploits die Eintrittswahrscheinlichkeit besser abgeschätzt werden.

Dennoch werden die Risiken anhand von qualitativen Kategorien bewertet. Dafür wurden die Eintrittswahrscheinlichkeit und die Schadensauswirkungen als vierstufiges Klassifikationsschema definiert. Es gibt die Eintrittswahrscheinlichkeiten unwahrscheinlich, möglich, wahrscheinlich und sehr wahrscheinlich (vgl. Tabelle 4.12) sowie die Schadenshöhen vernachlässigbar, begrenzt, beträchtlich und existenzbedrohend (vgl. Tabelle 4.13), die direkt aus dem BSI-Standard übernommen wurden. Nachdem die Bedrohungen kategorisiert sind, werden die Ergebnisse für die Risikobewertung benutzt. Das engültige Risiko

kann zum Schluss anhand der Matrix aus Abbildung 4.5 erfasst werden. Zudem wurde in der Risikoanalyse ein Ampelsystem eingeführt, dass jedes Risiko auf eine Farbe abbildet. Grün deutet auf ein geringes Risko hin, Gelb auf ein mittleres, Orange auf ein hohes und Rot auf ein sehr hohes Risiko. Die Definition der einzelnen Risikokategorie kann aus der Tabelle 4.14 entnommen werden.

In der Risikoanalyse wird die aktuelle Infrastruktur von QS ohne zusätzliche Gegenmaßnahmen bewertet. Sofern von einer Bedrohung mehr als ein Grundwert verletzt wird, so wird bei der Klassifikation der Schadensauswirkungen vom ungünstigsten anzunehmenden Fall ausgegangen.

Eintritts-wahrscheinlichkeit	**Beschreibung**
unwahrscheinlich	Ein Angreifer kann kaum eine Schwachstelle finden und ausnutzen. Potentielle Schwachstellen werden durch regelmäßige Kontrolle entdeckt und behoben. Das Risiko kann aber nicht ausgeschlossen werden.
möglich	Ein versierter Angreifer mit tiefem Verständis über die Infrastruktur kann die Schwachstelle mit großem Aufwand ausnutzen. Entdeckte Schwachstellen können schnell behoben werden.
wahrscheinlich	Ein Angreifer kann mit vertretbarem Aufwand die Schwachstelle ausnutzen. Entdeckte Schwachstellen können nicht sofort behoben werden.
sehr wahrscheinlich	Ein Angreifer kann mittels öffentlicher Informationen und Exploits die Schwachstelle ausnutzen. Schwachstellen werden sofort ausgenutzt und können nicht entdeckt und behoben werden.

Tabelle 4.12: Kategorisierung von Eintrittswahrscheinlichkeiten

4.3.1 Stub-Resolver im Endsystem

Die Tabelle A.1 im Anhang stellt die gesamte Risikoanalyse für den Stub-Resolver im Endsystem abgebildet auf die Infrastruktur von QS dar. Die größten Risiken, dass sind die Risiken mit einem hohen und sehr hohem Risiko, werden im Folgenden erläutert:

1. **B7: Malware**
   Malware kann dafür sorgen, dass die DNS-Einträge in den Konfigurationen und

Schadenshöhe	Schadensauswirkungen
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell-bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 4.13: Kategorisierung von Schadensauswirkungen [24]

Caches des Clients verändert werden und somit die Verfügbarkeit der Namensauflösung einschränken. Hierbei geht insbesondere von den privaten Endgeräten der Mitarbeiter ein Risiko aus, da die von QS bereitgestellten Computer ein aktuelles Antivirenprogramm besitzen. Dadurch ist das Risiko für die firmeneigenen Computer gesenkt, dennoch kann durch einen befallenen Client weitere Schadsoftware in das Firmennetzwerk eindringen oder vertrauliche Daten das Firmennetzwerk verlassen, beispielsweise weil die Malware die DNS-Einträge der Softwareversionsverwaltung auf eine Version des Angreifers abgeändert hat. Es ergibt sich bei dieser Bedrohung ein hohes Risiko.

2. **B10: Nutzung von öffentlichen rekursiven Resolvern**
   Diese Bedrohung betrifft nur die privaten Endgeräte, da die von QS bereitgestellten Computer gegen eine Änderung des zu verwendenen Nameservers ausreichend geschützt sind. Die privaten Endgeräte können jedoch öffentliche rekursive Resolver konfigurieren, die auch die vom DHCP bereitgestellten Nameserver überschreiben. Dadurch ist eine Namensauflösung der internen Hosts nicht mehr möglich. Es ergibt sich dadurch ein hohes Risiko.

3. **B14: DNS als Infil- und Exfiltrationsmedium**
   Da die DNS-Infrastruktur und der DNS-Verkehr von QS nicht im besonderen Maße überwacht werden, kann ein interner Angreifer mittels DNS vertrauliche Daten, wie personenbezogene Gesundheitsdaten oder Geschäftsgeheimnisse, entwenden oder Schadsoftware, an den Antivirenprogrammen vorbei, einschleusen. Aufgrund dessen ergibt sich ein hohes Risiko.

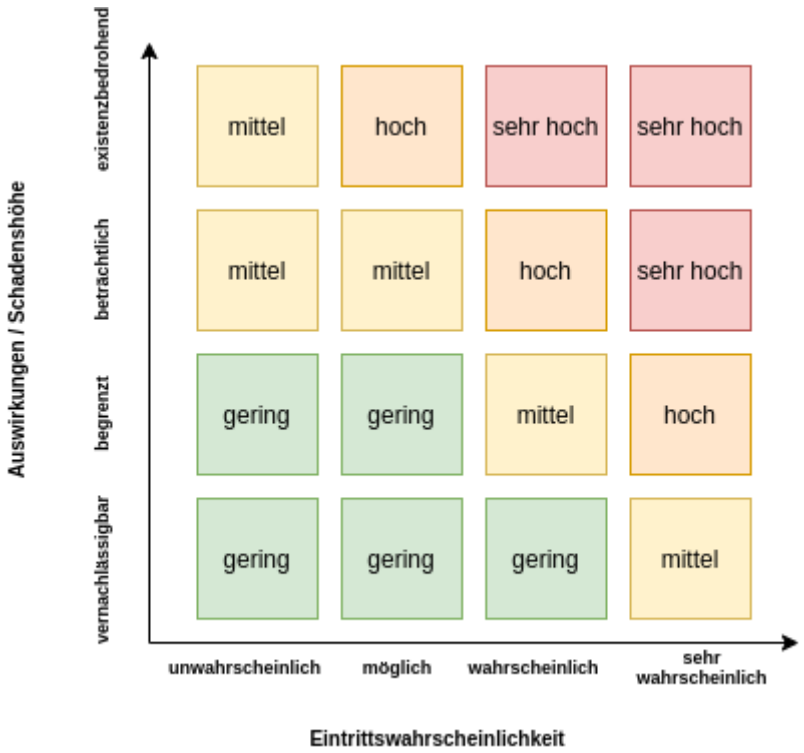


Abbildung 4.5: Matrix zur Einstufung von Risiken

Quelle: In Anlehnung an [24]

4. **B27: Ausfall oder Störung von Dienstleistern**
   Das Risiko für einen Ausfall oder eine Störung von Dienstleistern wird als sehr hoch bewertet und ist somit das größte Risiko für die Stub-Resolver. Die Stub-Resolver benötigen zwingend einen rekursiven Resolver, da ansonsten die Namensauflösung nicht durchgeführt werden kann. QS leitet die DNS-Anfragen, die der autoritative Nameserver NS2 nicht selbst autoritativ beantworten kann, an den rekursiven Resolver des ISPs weiter. Zwischen QS und dem ISP wurde kein Service-Level-Agreement abgeschlossen, das die Verfügbarkeit des rekursiven Resolvers definiert. Außerdem betreibt QS keine Maßnahmen zur Ausfallsicherheit, beispielsweise durch die Nutzung von rekursiven Resolvern anderer Dienstleister oder Betrieb eines eigenen rekursiven Resolvers. Da die Einschränkung der Verfügbarkeit alle Clients gleichermaßen betrifft und die Verfügbarkeit nicht schnell wiederhergestellt werden kann, ist das Risiko für QS sehr hoch.

Kategorie	Beschreibung
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

Tabelle 4.14: Definition von Risikokategorien [24]

Offenkundig beherbergt die Bedrohung *B7: Malware* noch weitere Risiken für QS, die aber nicht im Kontext von DNS stehen und daher in dieser Risikoanalyse nicht beurteilt werden.

4.3.2 Rekursiver Resolver

Aus der Identifikation der Systeme ergibt sich für QS kein rekursiver Resolver, sondern zwei DNS-Proxies, die die DNS-Nachrichten lediglich weiterleiten. Die eigentliche Namensauflösung wird von dem rekursiven Resolver des ISPs durchgeführt. Dieser wird in der Risikoanalyse allerdings durch die Betrachtung des Stub-Resolvers mit abgebildet.

4.3.3 Autoritativer Nameserver

Die Tabelle A.4 im Anhang stellt die gesamte Risikoanalyse für die autoritativen Nameserver NS1, NS2 und NS3 dar. Um die Risikoanalyse möglichst stringent durchzuführen

und um Wiederholungen zu vermeiden wurden die beeinträchtigen Grundwerte je autoritativer Nameserver zentral auf die Schadensauswirkungen abgebildet, so dass nur noch der Aufwand und die Zeit für die Beseitigung des Schadens berücksichtigt werden muss. Dabei wurde jeweils pro Grundwert die minimalen Schadensauswirkungen geschätzt. Die Tabelle A.2 zeigt dabei die minimalen Schadensauswirkungen für den autoritativen Nameserver NS1 sowie NS3 und die Tabelle A.3 die minimalen Schadensauswirkungen für NS2. Da die Nameserver unterschiedliche Zonen bedienen und somit für unterschiedliche Benutzer die Verfügbarkeit der Namensauflösung anbieten, wurden die Bedrohungen getrennt betrachtet. Dadurch können bei gleichen Bedrohungen unterschiedliche Risiken für die Systeme entstehen. Die größten Risiken für die autoritativen Nameserver werden im Folgenden erläutert:

1. **B3: Denial-of-Service**
   Das größte Risiko für die autoritativen Nameserver sind Angriffe gegen die Verfügbarkeit. Da die Nameserver NS1 und NS3 aus dem Internet erreichbar sind, sind diese für einen Angreifer ein leichtes Ziel. Dabei stehen dem Angreifer verschiedene Möglichkeiten, wie beispielsweise Packetflooding oder Pseudorandom Subdomain Attacks zur Verfügung um die Verfügbarkeit einzuschränken. QS einzige Mitigierungsstrategie ist die Lastverteilung auf die zwei Nameserver NS1 und NS3. Allerdings kann ein Angreifer mit genügend Anfragen beide Nameserver zur Überlast bringen. Hinzu kommt, dass die Nameserver Wildcard-Queries erlauben und dadurch für DNS-Amplification-Angriffe missbraucht werden können, was wiederum die Verfügbarkeit der Nameserver einschränkt. Das Risiko wird als sehr hoch angegeben.

2. **B11: Fehler in den Konfigurationsdateien**
   Bei QS werden die Zonendateien auf dem autoritativen Nameserver NS1 manuell gepflegt. Es wird zwar auf Software, wie beispielsweise *named-checkconf* zurürckgegriffen um die Syntax der Konfigurationsdateien zu überprüfen, diese können aber keine falsche Zuordnung in den Zonendateien erkennen. Semantische Fehler mit einer hohen TTL werden von den rekursiven Resolvern gecached und können somit die Verfügbarkeit für längere Zeit beeinflussen. Es ergibt sich ein hohes Risiko.

3. **B18: Social Engineering**
   Die zugehörigen Nameserver für die Domain *quality-software.de* und *qs.de* sind beim Registrar hinterlegt. QS hat einige Sicherheitsmaßnahmen umgesetzt um den Zugriff zum Verwaltungsportal der Domain einzuschränken. Allerdings kann ein

Angreifer mittels Social Engineering Zugriff auf das Verwaltungsportal bekommen und dort die autoritativen Nameserver ändern. Bis die Änderung an alle Nameserver propagiert sind, können bis zu 48 Stunden vergehen. Eine Änderung in den Urzustand kann genauso lange dauern. Rechnet man die TTL der Resource Records in den Caches der rekursiven Resolvern mit ein, so kann die gesamte Plattform „InsureCloud“ für mehrere Tage nicht zur Verfügung stehen. Ferner wird dieser Angriff wahrscheinlich erst dann bemerkt, wenn die Verfügbarkeit schon eingeschränkt wurde, die TTL in den Caches abgelaufen sind und die Änderung der Nameserver bereits vollständig propagiert worden sind. Es ergibt sich ein hohes Risiko.

4. **B24: Zone Poisoning mittels Zonentransfers**
   NS3 repliziert mittels Zonentransfer die Resource Records des primären Nameservers NS1. Die IP-Adresse von NS3 ist als einzige IP-Adresse für den Zonentransfer autorisiert. Ein Angreifer kann mittels IP-Spoofing die IP-Adresse des autoritativen Nameservers NS3 annehmen und den Zonentransfer anstoßen. Dadurch können beide Nameserver überlastet werden. Sofern der Angreifer Zugriff auf ein Switch oder Router hat, der logisch zwischen den beiden Nameservern an der Datenübertragung teilnimmt, so kann er die Zoneninformationen auf dem Transportweg verändern und somit die DNS-Einträge in NS3 vergiften. Das Szenario wird allerdings als unwahrscheinlich eingestuft, da die Netzwerkkomponenten ausreichend geschützt sind. Das Risiko wird als hoch eingeschätzt, da beide Nameserver überlastet werden können und somit die Verfügbarkeit der Namensauflösung für die Plattform eingeschränkt wird.

4.3.4 Domain

Die einzige Bedrohung, die gegen die Domains des Unternehmens gerichtet ist und mit einem hohen Risiko klassifiziert wurde, ist die Bedrohung **B18: Social Engineering**. QS hat bereits einige Sicherheitsmaßnahmen zum Schutz der Domain, im Besonderen zum Schutz vor unbefugten Zugriffs zum Verwaltungsportal, etabliert. Allerdings können diese bei einem Social Engineering-Angriff durch den Helpdesk-Mitarbeiter des Domain-Registrars aufgehoben werden. Eine Schutzmaßnahme gegen die unbefugte Manipulation von Domains stellt das Registrar Lock bereit [59]. Dabei handelt es sich um verschiedene Status, die bestimmte Operationen für eine Domain verbieten und nur von einer Registrierungsorganisation gesetzt und entfernet werden können. Der Status *serverTransferProhibited* zeigt beispielsweise an, dass die Domain nicht transferiert werden darf [14].

Diese zustätzlichen Sicherheitsmaßnahmen werden von QS bisher nicht eingesetzt, daher ergibt sich ein hohes Risiko.

4.3.5 Zusammenfassung

Nachdem die Risikoanalyse durchgeführt worden ist, ergeben sich für QS verschiedene Gefährdungen mit unterschiedlichem Risiko. Der BSI-Standard 200-3 sieht nun eine Risikobehandlungsstrategie vor, um den Umgang mit den verbleibenden Risiken aufzubereiten. Die Risikobehandlungsstrategie legt fest, dass die Risiken vermieden, reduziert, transferiert oder akzeptiert werden können, wobei für gewöhnlich nur geringe Risiken akzeptiert werden [24]. Da diese Sicherheitsanalyse speziell auf DNS gerichtet ist, werden im nächsten Kapitel die identifizierten Risiken anhand der DNS-Sicherheitserweiterungen betrachtet und überpüft, ob und in welchem Maß diese für eine Reduzierung der Risiken geeignet sind.

5 Evaluation

Kapitel 4 hat Sicherheitsrisiken beim Betrieb einer DNS-Infrastruktur für den Anwendungsfall aufgezeigt. Es wurden Schwachstellen, Bedrohungen und Angriffe gegen eine DNS-Infrastruktur erläutert und eine Risikoanalyse im Bezug auf das Anwendungsszenario durchgeführt. Die Risiken bei der Verwendung von DNS können behandelt werden, indem die Sicherheit von DNS verifiziert wird, geeignete Schutzmaßnahmen getroffen werden, auf die Verwendung von DNS verzichtet wird oder die Risiken akzeptiert werden. In diesem Kapitel wird zuerst die Sicherheit von DNS, mit besonderem Blick auf das übergeordnete Schutzziel *Schutz der DNS-Infrastruktur* (vlg. 3.1), anhand der DNS-Sicherheitserweiterungen überprüft und anschließend ein Maßnahmenkatalog zur Minimierung der identifizierten Risiken vorgestellt. Auf die Verwendung von DNS zu verzichten wird in diesem Kontext nicht betrachtet.

5.1 DNS-Sicherheitserweiterungen

Mittlerweile wurden mehr als 250 RFCs veröffentlicht, die auf DNS aufbauen und es erweitern. Darunter fallen einige RFCs, die versuchen DNS sicherer zu machen [31]. Populäre Vertreter sind DNSEC, DoT und DoH. Grundsätzlich können diese Protokollerweiterungen in zwei Kategorien aufgeteilt werden: Schutz der DNS-Daten und Schutz der DNS-Transaktionen. Schutz der DNS-Daten beschreibt dabei die Integrität und Authentizität der Resource Records (Signierung). Schutz der DNS-Transaktionen hingegen bezeichnet die Vertraulichkeit und Integrität auf dem Transportweg (Verschlüsselung).

5.1.1 Schutz der DNS-Daten

DNSSEC

Das Ziel von DNSSEC ist die Integrität und die Authentizität von DNS-Daten aber nicht die Vertraulichkeit. DNSSEC nutzt dazu kryptografische Signaturen. Es gibt zwei Arten von Schlüsselpaaren: Key-Signing-Keys (KSK) und Zone-Signing-Keys (ZSK). Der private ZSK wird für die Signierung aller Resource Records der eigenen Zone verwendet, wobei Resource Records in sogenannte Resource Record Sets zusammengefasst werden. Resource Record Sets beinhalten dabei alle Resource Records desselben Typs. Der private KSK signiert den öffentlichen ZSK. Der öffentliche Teil des KSK wird der übergeordneten Zone bekannt gemacht. Die übergeordnete Zone wiederum signiert den Hash des öffentlichen KSK mit ihrem eigenen ZSK und stellt diesen bereit. So entsteht eine Vertrauenskette bis zur Wurzel. Der Trust Anchor, der öffentliche Schlüssel des KSK der Wurzel, ist wiederum in den Endsystemen konfiguriert [46].

Für den Austausch der öffentlichen Schlüssel und Signaturen wurden eigens neue DNS Resource Records definiert. Die kryptografischen Informationen werden somit direkt im DNS gepflegt und das DNS selbst zur PKI. Die Tabelle 5.1 stellt die durch den Einsatz von DNSSEC neu hinzugekommen Resource Records dar. Die Verwendung dieser wird im Folgenden durch die Abbildung 5.1 verdeutlicht und erläutert.

Angenommen ein Client möchte den A-Record von *www.haw-hamburg.de* auflösen und alle beteiligten Systeme sind DNSSEC-fähig. Der Client führt eine rekursive DNS-Abfrage aus und erhält als Antwort die zugehörige IP-Adresse und einen RRSIG-Record. Der RRSIG-Record ist die kryptografische Signatur des Resource Record Sets und ist ein Hash, der durch den privaten ZSK der SLD *haw-hamburg.de* erzeugt wurde. Um die Signatur zu überprüfen benötigt der Client den öffentlichen ZSK. Somit muss der Client eine erneute Anfrage, zur Auflösung des DNSKEY, an *haw-hamburg.de* stellen. Der autoritative Nameserver antwortet mit dem öffentlichen ZSK und einem RRSIG-Record. Der RRSIG-Record beinhaltet die Signatur des öffentlichen ZSK, unterschrieben vom privaten KSK. Mit dem öffentlichen Schlüssel kann der Client die Signatur der ursprünglichen Anfrage validieren. Allerdings muss der Client noch sicherstellen, dass der ZSK vertrauenswürdig ist. Dazu muss er den erhaltenden RRSIG überprüfen. Der Client stellt eine erneute Anfrage und fragt nach dem öffentlichen KSK. Als Antwort bekommt er den öffentlichen KSK, mit dem die Signatur der vorherigen Anfrage überprüft werden kann. Um den KSK zu validieren, muss er den DS-Record für *haw-hamburg* in der TLD *.de*

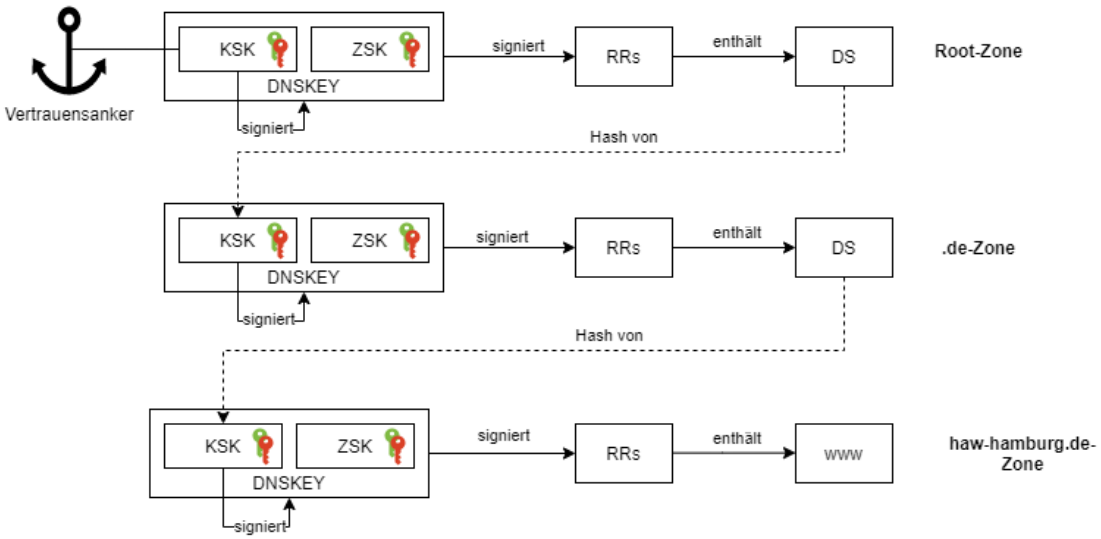


Abbildung 5.1: DNSSEC Vertrauenskette

Quelle: Eigene Darstellung in Anlehnung an [76]

anfragen. Dieser enthält den Hash des öffentlichen KSK, der durch den ZSK der TLD *.de* unterschrieben wurde. Die Validierung des ZSK und nachfolgender DNS-Antworten läuft nach derselben Vorgehensweise ab.

Die Verwendung von zwei Schlüsseln ist von DNSSEC nicht explizit vorgegeben, d.h. DNSSEC kann auch mit einem Schlüssel betrieben werden [11]. Die Verwendung von zwei Schlüsseln hat aber einige Vorteile. Ein Vorteil ist, dass der ZSK einfacher gewechselt werden kann, da dies ohne die Kooperation mit der darüberliegenden Zone möglich ist. Dadurch kann der ZSK zusätzlich mit einer geringeren Schlüssellänge erstellt werden, dass wiederum die Größe der DNSSEC-Antworten verringert.

Die Signierung der Resource Records stellt sicher, dass die Namensauflösung korrekt durchgeführt und zu dem Namen die richtige IP-Adresse zurückgeliefert wurde. Zusätzlich kann DNSSEC das Nichtvorhandensein von Resource Records validieren. Damit wird verhindert, dass ein Angreifer Resource Records aus Antworten unbemerkt entfernt. DNSSEC ist Ende-zu-Ende-überprüfbar, d.h. der Client kann, angefangen vom empfangenen Resource Record, die Vertrauenskette bis zur Wurzel validieren.

Tabelle 5.2 stellt die durch den korrekten Einsatz von DNSSEC ausgeschlossenen und gemilderten Bedrohungen aus Kapitel 4 dar. Es wird davon ausgegangen, dass der KSK

Typ	Beschreibung
RRSIG	Signatur des Resource Records Sets aus dem ZSK
DNSKEY	Öffentlicher ZSK oder KSK, abhängig vom Flag der Antwort
DS	Hash des öffentlichen KSK der darunterliegenden Zone
NSEC	Verweis auf den nächsten Resource Record
NSEC3	Verweis (Hash) auf den nächsten Resource Record

Tabelle 5.1: Für DNSSEC definierte Resource Record Typen

und der ZSK nicht auf den autoritativen Nameservern hinterlegt sind. DNSSEC sorgt dafür, dass Cache Poisoning-Angriffe verhindert werden. Ein Angreifer kann zwar immer noch schneller als der legitime autoritative Nameserver antworten, da die Antwort aber nicht durch den ZSK signiert wurde, würde die Validierung der Antwort fehlschlagen. Somit kann das Opfer die bösartige Antwort einfach verwerfen. Aus diesem Grund wird auch die Bedrohung DNS-Hijacking verhindert, sofern zwischen den Resolvern eine Vertrauensbeziehung besteht.

Ferner werden durch DNSSEC weitere Bedrohungen gemildert aber nicht aufgehoben. Die Bedrohungen im Bezug auf eine Veränderung der DNS-Daten in den Zonendateien der autoritativen Nameserver (B1, B6, B7, B9, B12, B13, B14) werden durch DNSSEC gemildert, da die Änderungen an den Zonendateien zwar durchgeführt aber nicht signiert werden können. Auch eine Änderung der Nameserver beim Registrar durch Social Engineering (B18) ist zwar immer noch möglich, führt jedoch zu einer fehlgeschlagenden Validierung beim rekursiven Resolver da der NS-Record nicht validiert werden kann. Die Bedrohung Man-in-the-Middle besteht weiterhin, da ein Angreifer weiterhin den DNS-Verkehr mitlesen kann und somit noch die Vertraulichkeit bedroht.

DNSSEC kann jedoch nur dann die DNS-Daten schützen, wenn es hinreichend eingesetzt wird. Abbildung 5.2 zeigt die Wachstumsentwicklung der DNSSEC signierten .de-Domains der letzten fünf Jahre gegenübergestellt zu allen .de-Domains, die in den letzten fünf Jahren existierten. Dabei ist zu erkennen, dass gerade einmal 1,5% der .de-Domains mittels DNSSEC signiert sind. Damit DNSSEC jedoch ausreichend Schutz vor unbefugter Veränderung der DNS-Daten gewährleisten kann, muss eine flächendeckende Nutzung von DNSSEC etabliert werden.

Wie bereits erwähnt, ergeben sich einige neue Bedrohungen, Probleme und Risiken bei der Verwendung von DNSSEC die im Folgenden erläutert werden.

Ausgeschlossene Bedrohung	**identifiziertes System**
B21: Cache Poisoning	R
B23: DNS-Hijacking	S
Gemilderte Bedrohung	**identifiziertes System**
B1: Software-Schwachstellen oder -Fehler	R, A
B6: Unbefugter physischer Zugriff	R, A
B7: Malware	R, A
B9: Ausführung mit erweiterten Rechten	R, A
B12: Fehlende organisatorische Abläufe	R, A
B13: Unzureichendes Berechtigungskonzept	R, A
B14: Missbrauch von administrativen Berechtigungen	A
B18: Social Engineering	A
B22: Man-in-the-Middle	R

Tabelle 5.2: Behandelte Bedrohungen durch Einsatz von DNSSEC

Stub-Resolver als einfache Softwarekomponenten führen für gewöhnlich die Validierung der Resource Records nicht aus, da die Validierung mit einigem Aufwand verbunden ist, sondern benötigen für die Validierung einen sogenannten validierenden Resolver. Im Regelfall ist der rekursive Resolver für den Stub-Resolver auch gleichzeitig der validierende Resolver. Der validierende Resolver setzt, nachdem er die Validierung durchgeführt hat, im Header der DNS-Antwort ein AD-Bit (Authenticated Data). Anhand dieses Flags kann der Stub-Resolver feststellen, ob die Validierung erfolgreich war oder nicht. Es muss also ein Vertrauensverhältnis zwischen dem Stub-Resolver und dem rekursiven Resolver bestehen, da ein bösartiger rekursiver Resolver dieses Bit auch bei unverifizierten DNS-Daten setzen kann. Daher wird im RFC 3655 empfohlen, insbesondere in ungewissen und unsicheren Netzen, nicht ohne weiteres dem, vom DHCP bereitgestellten, rekursiven Resolver zu vertrauen sondern, sofern möglich, einen Full-Resolver zu betreiben, der die Validierung durchführt [94]. Das ist bei einigen Clients, wie beispielsweise Smartphones, aber nicht ohne weiteres möglich.

Eine weiteres Problem bei der Verwendung von DNSSEC sind die benötigten Ressourcen zur Durchführung der Validierung. Die Validierung benötigt Zeit, die kryptografischen Operationen Rechenleistung und das Abfragen der Vertrauenskette zusätzliche Bandbreite. Die rekursiven Resolver können zwar, bedingt durch ihre Caches, auf einige Validierungen, insbesondere bei populären Domains, verzichten, spätestens nach Ablauf der TTL muss die Validierung aber erneut durchgeführt werden. Dieses Szenario wurde in der

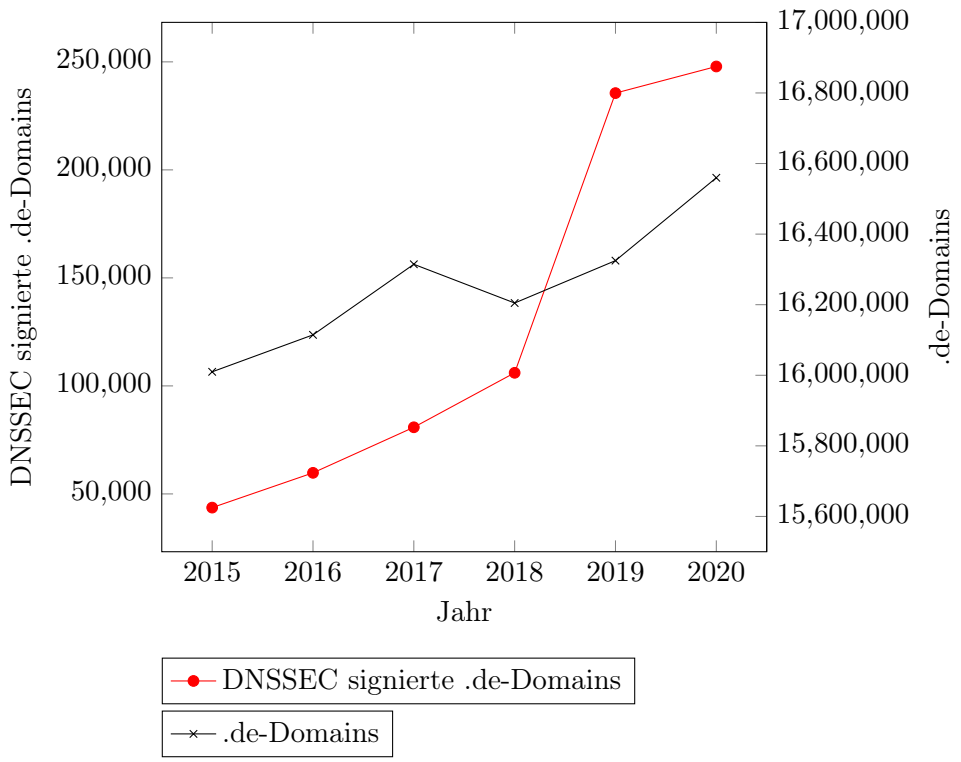


Abbildung 5.2: Wachstumsentwicklung der mit DNSSEC signierten .de-Domains

Quelle: Eigene Darstellung mit Daten aus [37]

Wissenschaft ausgiebig diskutiert. Eine vorgeschlagene Lösungmöglichkeit ist, dass der validierende Resolver kurz vor Ablauf der TTL eigenständig den Resource Record anfragt und validiert (sog. prefetch) [95]. Nachteilig dabei sind die ggf. unnötige verbrauchten Ressourcen wie Rechenleistung, Bandbreite und Speicherplatz. Bei einer gut gewählten Heuristik kann der Zeitgewinn jedoch immens sein. Einige Nameserver, darunter *BIND*, bieten dieses Feature an [63].

Eine Designentscheidung bei der Entwicklung von DNSSEC war, dass DNSSEC möglichst kompatibel mit bestehenden Stub-Resolvern sein soll. Ein Problem dabei ist, dass die Stub-Resolver mit vordefinierten Timeouts arbeiten und DNS-Anfragen bei fehlender Antwort einfach erneut schicken. Da die Validierung der Vertrauenskette, sofern der Eintrag nicht zwischengespeichert ist, aber deutlich länger als eine normale DNS-Anfrage dauert, kann es passieren, dass der Stub-Resolver die Anfrage erneut schickt.

DNSSEC erhöht folglich die Last auf die rekursiven Resolver und macht diese somit anfälliger für DDoS-Angriffe. Zusätzlich können DNSSEC signierte Nameserver für einen

DNS-Amplification-Angriff missbraucht werden. Aufgrund der Schlüsseldaten und Signaturen, die bei der Verwendung von DNSSEC zusätzlich übertragen werden müssen, ergeben sich Hebel die weitaus größer sind als bei der Verwendung von einfachen *ANY*-Queries ohne DNSSEC. Da die Validierungsdaten von den autoritativen Nameservern bereitgestellt werden, ergibt sich eine Umverteilung der bedrohten Systeme. Angreifer können direkt die gefälschten DNS-Anfragen an DNSSEC validierte Nameserver schicken und somit auf die rekursiven Resolver verzichten. Vorteilhaft für den Angreifer ist dabei, dass die autoritativen Nameserver einer öffentlichen Domain ihren Dienst für gewöhnlich allen Benutzern des Internets anbieten und somit keine Zugriffsbeschränkung für bestimmte IP-Adressbereiche existieren. Die Auflistung 5.1 zeigt eine Anfrage zur Auflösung aller Resource Records der DNSSEC signierten Domain *dfn.de*. Dabei ist zu erkennen, dass die Antwort 34-mal größer ist, als die Anfrage.

Auflistung 5.1: DNS-Anfrage zur Auflösung aller Records der DNSSEC signierten Domain *dfn.de*

```
; <<>> DiG 9.16.7 <<>> @8.8.8.8 +qr +dnssec dfn.de ANY
[...]
;; QUERY SIZE: 47
[...]
;; Query time: 26 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
[...]
;; MSG SIZE  rcvd: 1605
```

Ein weiteres Hindernis bei der flächendeckenden Einführung von DNSSEC ist die Synchronisierung der Zeit. Bisher gab es im DNS lediglich die relative Zeit, die durch die TTL der Resource Records beschrieben wurde. Dabei war es unerheblich, wie beispielsweise die absolute Uhrzeit des rekursiven Resolvers lautet, ein Resource Record der nur eine TTL von fünf Minuten hat, wurde fünf Minuten nach dem Query aus dem Cache entfernt. DNSSEC führt nun aber die absolute Zeit ein, die die Lebensdauer der Signaturen angibt. Dadurch ist es zwingend erforderlich, dass die beteiligten Kommunikationspartner eine synchronisierte Zeit besitzen. Durch diese Bedingung kann aber ein Henne-Ei-Problem entstehen, da die Synchronisierung, beispielsweise durch das Network Time Protocol (NTP), oft auf DNS zurückgreift um die Adresse des Zeitservers abzufragen (bspw. `de.pool.ntp.org`) [56].

Sofern der ZSK abseits des zugehörigen autoritativen Nameservers gespeichert wird, sind dynamische Updates nicht mehr möglich, da bei einem Update der DNS-Einträge die Zone neu signiert werden müsste. Ferner werden Zonentransfers nicht durch DNSSEC abgebildet und können somit manipuliert werden.

Durch die Verwendung von DNSSEC und NSEC Resource Records ergibt sich zusätzlich ein Bedrohungsszenario durch sogenanntes Zone Walking. Der NSEC-RR wurde eingeführt, um das Nichtvorhandensein eines DNS-Eintrags zu validieren. Ein Resource Record, der nicht existiert, kann schließlich nicht signiert werden. Dabei werden die DNS-Einträge ringförmig verkettet, so dass ein Hostname immer auf einen anderen existierenden Hostname zeigt. Ein fundamentales Desginproblem der NSEC-RR ist, dass ein Angreifer diese Liste durchlaufen kann um die komplette Zone abzubilden. Mittlerweile gibt es eine Alternative, die NSEC3-Records, die die Hostnames als Hashwert anstatt des Klarnamens darstellen [67]. Dadurch wird das Zone Walking erschwert, aber nicht unmöglich gemacht.

Ein weiteres Problem stellt das Austauschen der Schlüssel (hier KSK) dar, insbesondere das Austauschen des Wurzel-Schlüssels. Die Schlüssel haben in der Regel ein Ablaufdatum und müssen spätestens vor Ablauf ausgetauscht werden. Ein Problem dabei ist das Caching der rekursiven Resolver, da diese die Schlüsseldaten und Signaturen bis zum Ablauf der TTL zwischenspeichern und ein Schlüsselaustausch zu einer fehlgeschlagenden Validierung führen würde. Somit müssen bei einem Schlüsselaustausch die Resource Records durch beide Schlüssel (alt und neu) signiert werden. Bei der Wurzel-Zone gibt es zusätzlich noch das Problem, dass der Public-Key des KSK in den Resolvern fest konfiguriert ist und dieser auf sichere Art und Weise ausgetauscht werden muss.

Darüber hinaus bietet DNSSEC keinen Schutz auf der *letzten Meile* der Übertragung vom rekursiven Resolver zum Stub-Resolver. Ein Angreifer hat dort immer noch die Möglichkeit, die Daten zu verändern, da der Stub-Resolver die Validierung nicht durchführt. An dieser Stelle setzten die Protokolle an, die als Ziel den Schutz der DNS-Transaktionen haben und später behandelt werden. Zusätzlich kann DNSSEC nicht feststellen, ob die DNS-Daten semantisch korrekt oder ob diese vor der Signierung unrechtmäßig verändert worden sind. Auch die Feststellung, ob der initial angegebene autoritative Nameserver einer Domain überhaupt rechtmäßig ist, kann mittels DNSSEC nicht durchgeführt werden. Im Bezug auf das übergeordnete Schutzziel (vgl. 3.1) kann daher gesagt werden, dass DNSSEC alleine nicht ausreichend ist, um die Integrität der DNS-Daten sicherzustellen.

Die Verfügbarkeit und Vertraulichkeit kann durch DNSSEC nicht verbessert werden, die Verfügbarkeit wird sogar durch die zusätzlichen Daten noch weiter bedroht.

TSIG

TSIG, kurz für Transaction Signature, ist eine Protokollerweiterung für DNS, die das Ziel hat, die Integrität und die Authentizität der DNS-Daten zu gewährleisten. Vertraulichkeit ist kein Ziel von TSIG, die DNS-Daten werden folglich nicht verschlüsselt. Stattdessen werden Message Authentication Codes (MACs) zur Sicherstellung der Unverfälschtheit der Nachrichten verwendet. Der Schlüssel wird dabei initial manuell an die Kommunikationspartner verteilt. TSIG wird im RFC 2845 spezifiziert und ist ein vorgeschlagener Standard [91].

Die Tabelle 5.3 zeigt die durch die Anwendung von TSIG ausgeschlossenen Bedrohungen auf. Da der Aufwand des Schlüsselaustauschs bei TSIG mit der Anzahl der Hosts quadratisch steigt, ist eine flächendeckende Nutzung von TSIG praktisch unmöglich. Daher kann TSIG nur bei einer vordefinierten Menge an Hosts zum Einsatz kommen. Geeignete Anwendungsfälle für die Nutzung von TSIG sind die autoritativen Nameserver beim Zonentransfer sowie beim dynamischen Update eines DNS-Eintrags.

Ausgeschlossene Bedrohung	**identifiziertes System**
B24: Zone Poisoning mittels Zonentransfers	A
B25: Zone Poisoning mittels dynamischer Updates	A

Tabelle 5.3: Behandelte Bedrohungen durch Einsatz von TSIG

Der große Vorteil gegenüber DNSSEC ist die geringe Komplexität des Protokolls, die allerdings bei einer zunehmenden Anzahl von Kommunikationspartnern steigt. Zusätzlich muss der Schlüssel initial sicher übertragen sowie auf dem Server sicher und nicht zugänglich gespeichert werden. Ferner verwendet TSIG, analog DNSSEC, für die Verhinderung von Replay-Angriffen Timestamps, daher müssen die Uhren der beteiligten Kommunikationspartner synchronisiert sein [91].

TSIG eignet sich aufgrund des schwierigen Schlüsselmanagements bei einer Vielzahl von Hosts nicht als einzige Möglichkeit zur Sicherung der Integrität der DNS-Daten. Da bei Zonentransfers oder dynamischen Updates jedoch meistens nur wenige vordefinierte

Teilnehmer, wie beispielsweise primäre und sekundäre Nameserver sowie DHCP-Server, beteiligt sind, ist es dort eine sinnvolle Erweiterung.

5.1.2 Schutz der DNS-Transaktionen

DNS-over-TLS (DoT)

DNS-over-TLS (DoT) wird im RFC 7858 [60] spezifiziert und verfolgt das Ziel, die DNS-Kommunikation zwischen Stub-Resolver und rekursivem Resolver durch Verschlüsselung zu sichern. Zwischen rekursivem Resolver und den autoritativen Nameservern wird DoT nicht eingesetzt, obwohl das durch das RFC nicht explizit ausgeschlossen wird [60]. Das Ziel von DoT ist die Vertraulichkeit und Integrität der DNS-Daten auf dem Transportweg sicherzustellen. Es garantiert nicht die Integrität der Resource Records in den autoritativen Nameservern und Caches der rekursiven Resolver.

Im Gegensatz zu regulärem DNS, verwendet DoT bei der Kommunikation eine TCP-Verbindung, die zusätzlich durch das Verschlüsselungsprotokoll Transport Layer Security (TLS), vormals Secure Socket Layer (SSL), gesichert ist. TLS verwendet ein asymmetrisches Verschlüsselungsverfahren, um symmetrische Schlüssel auszuhandeln. Die Authentizität der öffentlichen Schlüssel wird durch Zertifikate sichergestellt. Die kryptografischen Verfahren, die bei TLS verwendet werden, sind nicht fest definiert, sondern Client und Server einigen sich auf ein Verfahren, das beide beherrschen. Die symmetrischen Schlüssel werden jedoch nicht übertragen, sondern mittels eines *Pre-Master Secrets* von beiden Parteien beim TLS-Handshake lokal erstellt. Die Schlüssel werden für die Verschlüsselung der Nachricht und Sicherstellung der Integrität durch Message Authentication Codes benutzt und sind nur für die Sitzung gültig [46]. Die genaue Funktionsweise von TLS kann in [82] nachgelesen werden. Die Nutzung von TLS für Anwendungsprotokolle ist nicht ungewöhnlich. So wurde bereits das Hypertext Transport Protocol (HTTP) durch Anwendung von TLS sicherer gemacht (HTTPS) [81].

Der Stub-Resolver kann DNS-over-TLS mit zwei Nutzungsprofilen betreiben. Das erste Profil wird als striktes Nutzungsprofil beschrieben und sorgt dafür, dass strikt TLS verwendet wird und somit alle DNS-Anfragen verschlüsselt werden und der rekursive Resolver mittels Zertifikat authentifiziert wird. Das führt dazu, dass bei einer fehlenden Verschlüsselung keine DNS-Anfragen beantwortet werden. Das zweite, opportunistische, Profil hingegen fällt auf die vom Client implementierten Sicherheitsfunktionen zurück.

Das sind entweder Authentifizierung und Verschlüsselung, nur Verschlüsselung oder Übertragung im Klartext [40].

Tabelle 5.4 zeigt die durch den Einsatz von DoT ausgeschlossenen und gemilderten Bedrohungen auf. Es wird davon ausgegangen, dass DoT im strikten Nutzungsprofil betrieben wird. Da die DNS-Daten zwischen dem Stub-Resolver und rekursivem Resolver verschlüsselt sind, können diese von einem Angreifer nicht mehr auf dem Transportweg abgehört oder verändert werden. Dadurch werden die Bedrohungen *Abhören des DNS-Verkehrs* und *Man-in-the-Middle* verhindert. Ein Angreifer, der die Kontrolle über einen rekursiven Resolver hat, kann jedoch auch bei DoT die DNS-Abfragen mitlesen, beispielsweise im Query-Log der DNS-Software. Da bei DoT TCP verwendet wird und TCP ein verbindungsorientiertes Protokoll ist, werden die DNS-Reflektierungsangriffe *DNS-Reflection* und *DNS-Amplification* blockiert. Allerdings sind TCP-Reflection-Angriffe möglich, wobei das Opfer mit SYN-ACK-Paketen überhäuft wird. Außerdem kann bei Verwendung eines ISP-fremden rekursiven Resolvers klassisches DNS-Hijacking durch ISPs verhindert werden. DNS-Hijacking ist dennoch möglich, da die DNS-Daten nicht signiert sind und somit eine Änderung oder Entfernung von Resource Records nicht überprüft werden kann. Daher wird die Bedrohung nur als gemildert eingestuft.

Beim Betrieb von DoT im opportunistischen Nutzungsprofil sind die ausgeschlossenen Bedrohungen *Abhören des DNS-Verkehrs* und *Man-in-the-Middle* ggf. wieder möglich. Bei fehlender Authentifizierung kann ein Angreifer seinen eigenen öffentlichen Schlüssel bereitstellen, ohne das dieser überprüft wird. Dadurch kann er beim Aushandeln des Schlüssels mitlesen, die symmetrischen Schlüssel errechnen und somit die DNS-Daten abhören und verändern.

Ausgeschlossene Bedrohung	**identifiziertes System**
B17: Abhören des DNS-Verkehrs	S
B19: DNS-Reflection	R
B20: DNS-Amplification	R
B22: Man-in-the-Middle	S
Gemilderte Bedrohung	**identifiziertes System**
B23: DNS-Hijacking	S

Tabelle 5.4: Behandelte Bedrohungen durch Einsatz von DNS-over-TLS

Für die Kommunikation über DoT wurde eigens der Port 853 spezifiziert. Das hat einerseits den Vorteil, dass der DNS-Verkehr von Netzwerkadministratoren durch Regeln

geroutet werden kann, beispielsweise um die DNS-Anfragen an einen eigenen Resolver umzuleiten oder um DNS-Anfragen von definierten Clients zu blockieren. Andererseits kann dadurch identifiziert werden, ob und wann ein Client eine DNS-Anfrage stellt oder nicht. In sehr beschränkten Netzwerken kann der Port allerdings blockiert sein, wodurch der Client auf unverschlüsseltes DNS zurückgreifen müsste.

Genauso wie bei DNSSEC existiert bei DoT zusätzlich ein Mehraufwand für die DNS-Kommunikation. Im Falle von DoT muss die TLS-Verbindung aufgebaut werden, dadurch wird Rechenleistung und Bandbreite benötigt. Insbesondere die Rechenleistung ist bei einigen Clients, wie beispielsweise IoT-Geräten oft nicht vorhanden, so dass diese überlastet werden können. Dabei spielt die Lebensdauer der TLS-Session eine große Rolle. Sofern der Client und der Server immer über dieselbe TLS-Verbindung kommunizieren, können die benötigen Ressourcen deutlich verringert werden. Allerdings ist das einerseits von der Implementierung der Stub-Resolver und andererseits von dem konfigurierten Timeout der rekursiven Resolver abhängig. Stub-Resolver unter Linux, die auf die vom Betriebssystem bereitgestellten POSIX-Schnittstellen *getaddrinfo()* oder *gethostbyname()* zurückgreifen, öffnen für jede einzelne DNS-Anfrage eine neue TCP-Verbindung [60]. Bei einer hohen Lebensdauer der TLS-Verbindung ergibt sich für die rekursiven Resolver zusätzlich das Problem des Sitzungsmanagements, da für jede Sitzung Speicher allokiert werden muss. Das macht die rekursiven Resolver anfälliger für DDoS-Angriffe.

Hinzu kommt, dass die Latenz gegenüber einfachem DNS steigt, da bei einer TCP-Verbindung mit anschließender TLS-Verbindung anstelle von einem Paket mindestens vier Pakete (eins beim TCP-Handshake, zwei beim TLS-Handshake, mind. eins für die DNS-Anfrage) verschickt werden müssen. Es wird daher vom RFC empfohlen, mehrere DNS-Anfragen zu bündeln um die Latenz zu verringern und TCP-Erweiterungen wie Fast Open oder TLS Session Resumption zu verwenden [60]. Allerdings ergeben sich dadurch wieder neue Bedrohungen, daher muss zwischen dem Performancegewinn und den Risiken abgewogen werden.

Außerdem ist DNS-over-TLS nicht ohne weiteres von bestehenden Stub-Resolvern einzusetzen, sondern benötigt im Regelfall eine Aktualisierung des Betriebssystems oder die Einführung neuer Software [60]. Somit kann es passieren, dass Anwendungen eigene DoT-konforme Stub-Resolver implementieren, die eventuell auf andere, dem Betriebssystem unbekannte, Zertifikate zurückgreifen. Diese, für den Benutzer unbekannten, Zertifikate stellen dabei ein Sicherheitsrisiko dar, da sie bei einer Kompromittierung nicht ohne weiteres zurückgezogen werden können.

DoT wird aktuell noch nicht von jedem rekursiven Resolver unterstützt. Beispielsweise bietet *BIND* DoT nur über die zusätzliche Software *stunnel*[1] an [41]. Dadurch kann es für Unternehmen schwierig sein, DoT in bestehende DNS-Lösungen zu integrieren.

Da eine Authentifizierung des Kommunikationspartner für DoT im strikten Nutzungsprofil unerlässlich ist, können die verschiedensten Probleme beim Betreiben einer PKI auftreten. Das RFC 7858 [60] behandelt diesen Punkt nicht explizit, dennoch müssen die Probleme betrachtet werden. Es könnte beispielsweise passieren, dass der Client nicht das erforderliche Wurzelzertifikat besitzt oder das Zertifikat bereits zurückgezogen worden ist. Das würde dazu führen, dass der Client die Namensauflösung nicht durchführen kann oder der Client möglicherweise mit einem kompromittierten Resolver kommuniziert. Diese Fehler müssen vom Stub-Resolver ausreichend behandelt sowie Fallback-Lösungen eingeführt werden.

DoT eignet sich insbesondere um die Privatsphäre der Benutzer zu sichern. Das kann allerdings nur gewährtleistet werden, sofern DoT im strikten Nutzerprofil verwendet wird. Aufgrund der Tatsache, dass die Integrität der Resource Records nicht sichergestellt ist sowie die in der Praxis fehlende Verschlüsselung zwischen rekursivem Resolver und autoritativen Nameserver, ist DoT als einzige Sicherheitserweiterung nicht ausreichend.

DNS-over-HTTPS (DoH)

DNS-over-HTTPS (DoH) wird im RFC 8484 [57] spezifiziert und verfolgt, analog zu DoT, das Ziel, die DNS-Kommunikation auf dem Transportweg zwischen Stub-Resolver und rekursivem Resolver durch Verschlüsselung zu sichern. Dabei wird für die Kommunikation auf das Protokoll Hyptertext Transfer Protocol Secure (HTTPS) zurückgegriffen, das wiederum aus dem HTTP-Protokoll mit zusätzlicher TLS-Verbindung besteht. Für DoH ist kein eigener Port reserviert, die DNS-Anfragen sollen vielmehr über den HTTPS-Port 443 erfolgen.

Tabelle 5.5 stellt die durch den korrekten Einsatz von DoH ausgeschlossen und gemilderten Bedrohungen dar. Es ist zu erkennen, dass DoH dieselben Bedrohungen wie DoT behandelt. Das ist nicht verwunderlich, da DoH genauso wie DoT über eine TLS-Verbindung kommuniziert.

[1] https://www.stunnel.org/

Ausgeschlossene Bedrohung	**identifiziertes System**
B17: Abhören des DNS-Verkehrs	S
B19: DNS-Reflection	R
B20: DNS-Amplification	R
B22: Man-in-the-Middle	S
Gemilderte Bedrohung	**identifiziertes System**
B23: DNS-Hijacking	S

Tabelle 5.5: Behandelte Bedrohungen durch Einsatz von DNS-over-HTTPS

Da DoH keinen eigenen Port besitzt werden DNS-Anfragen an den Standard HTTPS-Port 443 gesendet. Die DNS-Anfragen können somit nicht mehr vom normalen HTTPS-Verkehr unterschieden werden. Für den Benutzer hat das den Vorteil, besonders gegenüber DoT, dass es für einen Angreifer nicht ersichtlich ist, ob ein Client DNS-Anfragen schickt oder nicht. Allerdings birgt DoH das Problem, dass das HTTP-Protokoll über weitaus mehr Metadaten als reines TLS verfügt. Durch die Metadaten, wie beispielsweise dem User-Agent oder HTTP-Cookies könnte es möglich sein, einen Client zuzuordnen. Zudem ist eine Kontrolle des DNS-Verkehrs, beispielsweise durch Firewall-Regeln, unter DoH nicht mehr möglich. Für Netzwerkadministratoren hat das den Nachteil, dass nicht ohne weiteres verhindert werden kann, dass ein Client einen DoH-fähigen rekursiven Resolver konfiguriert. Ferner wird ein Blockieren von DNS-Anfragen verhindert, da dann zusätzlich der HTTPS-Verkehr blockiert werden müsste. Somit können Command-&-Control-Server oder andere bösartige Domains nicht blockiert werden, ohne das gesamte Netzwerk zu stören. Zusätzlich eignen sich bei DoH die TXT-Records für die Übermittlung einer bösartigen Payload oder die Übermittlung der als nächstes ausgeführten Anweisung, wie zuletzt bei der Malware Godlua. Godlua ist eine DDoS-Malware, die für die Kommunikation mit dem Command-&-Control-Server DoH benutzt hat [85].

Gegenüber DoT hat DoH den Vorteil, dass der Port 443 vermutlich auch in sehr beschränkten Netzwerken zugelassen wird und somit weiterhin sichere DNS-Abfragen möglich sind.

Genauso wie bei DoT gibt es bei DoH das Problem, dass die Clients DoH nicht ohne weiteres verwenden können. Bei den DoH-Clients zeigt sich aber eine Verschiebung der Zuständigkeit vom Betriebssystem zu den Anwendungen. Insbesondere in Webbrowsern werden eigene DoH-Clients angeboten, so dass diese die DNS-Kommunikation unabhängig vom Betriebssystem durchführen. Dadurch ergibt sich die Bedrohung, dass

dieselben Namen durch die verschiedenen Implementierungen unterschiedlich aufgelöst werden können. Ferner ist die Konfiguration der zu verwendenden rekursiven Resolver in den Anwendungen hinterlegt. Das kann zu Problemen führen, insbesondere da einige Browser, beispielsweise Mozilla Firefox, in Kooperation mit öffentlichen rekursiven Resolvern (hier Cloudflare[2]) die IP-Adressen dieser Anbieter vorkonfigurieren [93]. Somit können in Firmenumgebungen die vordefinierten Resolver umgangen werden. Das kann zu den verschiedensten Problemen führen, insbesondere können interne Dienste nicht mehr über den Webbrowser aufgelöst werden.

Ein weiteres Problem stellt die Verfügbarkeit von DoH in aktueller DNS-Software dar. Abgesehen davon, dass DoH aktuell nicht nativ und zentral in die Stub-Resolver der Betriebssysteme eingebettet wird, ist die Verfügbarkeit bei rekursiven Resolvern eingeschränkt. Beispielsweise bietet *BIND* DoH noch nicht an (Version 9.16.4) [41]. Dadurch wird eine Integration in bestehende DNS-Lösungen, insbesondere von Unternehmen, deutlich erschwert. Ferner wird für das Betreiben eines DoH-fähigen rekursiven Resolver ein Webserver benötigt, der wiederum Softwareschwachstellen und -Fehler beinhalten kann und somit neue Risiken birgt.

DoH lässt sich als DNS-Sicherheitserweiterung nur begrenzt nutzen. Insbesondere der Verzicht auf einen eigenen Port sowie der Paradigmenwechsel, weg von einem zentralen DNS-Client im Betriebssystem hin zu DoH-Clients pro Anwendung, behindern die Nutzung in Unternehmensumgebungen. Wie bei DoT kann durch DoH die Integrität der DNS-Daten nicht festgestellt sowie der Transportweg zwischen rekursiven Resolver und autoritativen Nameserver nicht geschützt werden. Für Privatpersonen ist DoH und die Einbettung im Browser eine gute und einfache Möglichkeit, um die DNS-Daten vor Spionage oder Veränderung durch den ISP zu schützen (DNS-Hijacking). DoT und DoH können jedoch dazu führen, dass DNS zentralisiert wird und für die Unternehmen ein Monopol auf DNS-Anfragen entsteht.

DNS-over-DTLS (DoDTLS)

Zusätzlich zu DoT und DoH existiert noch die DNS-Sicherheitserweiterung DNS-over-DTLS (DoDTLS). DoDTLS wird im RFC 8094 [80] experimentell als Alternativvorschlag zu DoT spezifiziert. DoDTLS nutzt für die Übertragung das ungesicherte Transportprotokoll UDP sowie Datagram Transport Layer Security (DTLS) [80]. DTLS ist in großen

[2] https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/

Teilen mit TLS identisch. Da UDP keinerlei Zuverlässigkeit sowie Garantie auf Reihenfolge bietet, sind jedoch einige Anpassungen im Protokoll durchgeführt worden. Diese können unter [83] nachgelesen werden.

Tabelle 5.6 zeigt die durch DoDTLS ausgeschlossenen und gemilderten Bedrohungen auf. Aufgrund der Ähnlichkeit zu DoT, schafft es DoDTLS dieselben Bedrohungen zu behandeln. Die Kommunikation zwischen Stub-Resolver und rekursivem Resolver ist verschlüsselt, daher wird ein Abhören der Verbindung ausgeschlossen. Analog zu TLS werden die Pakete verschlüsselt und mittels Message Authentication Codes (MAC) validiert, daher können Man-in-the-Middle-Angriffe und DNS-Hijacking erkannt werden. Analog zu den anderen Protokollen ist auch bei DoDTLS DNS-Hijacking immer noch möglich, sofern der Angreifer die Kontrolle über den rekursiven Resolver hat, da DoDTLS keine Integrität der DNS-Daten sicherstellt. Eine Besonderheit bei UDP sind die Reflektierungsangriffe, da die Quell-IP-Adresse gefälscht werden kann. DTLS kann diese Bedrohung mit zustandslosen Cookies verhindern, die der Server initial für jeden Client beim DTLS-Handshake erstellt [83]. Daher kann auch DoTLS die DNS-Reflection und DNS-Amplification-Angriffe verhindern.

Ausgeschlossene Bedrohung	**identifiziertes System**
B17: Abhören des DNS-Verkehrs	S
B19: DNS-Reflection	R
B20: DNS-Amplification	R
B22: Man-in-the-Middle	S
Gemilderte Bedrohung	**identifiziertes System**
B23: DNS-Hijacking	S

Tabelle 5.6: Behandelte Bedrohungen durch Einsatz von DNS-over-DTLS

Ein Vorteil gegenüber DoT ist die kürzere RTT bei einer Wiederaufnahme der TLS-Session, da bei DoT ohne TCP Fast Open ein TCP-Handshake durchgeführt werden muss [80].

Ein Problem bei der Verwendung von DoDTLS stellt die Verwendung von Anycast bei mehreren rekursiven Resolvern dar. Da UDP im Gegensatz zu TCP verbindungslos ist, wird zwischen dem Stub-Resolver und rekursivem Resovler keine Verbindung aufgebaut. Es kann also passieren, dass bei einer DNS-Anfrage über DoDTLS ein anderer Server antwortet, als jener mit dem der Client ursprünglich einen DTLS-Handshake durchgeführt

hat [80]. Somit muss der Client erneut den DTLS-Handshake durchführen, was wiederum die Latenz der Anfrage erhöht.

DNS-Antworten über DoDTLS, die größer sind als die kleinste Maximum Transmission Unit (MTU) aller beteiligten Kommunikationspartner, müssen fragmentiert werden. DTLS verlangt allerdings, dass jeder DTLS-Record in ein Datagramm passen muss. Daher muss bei der Verwendung von DoDTLS zusätzlich DNS-over-TLS unterstützt werden, damit Anfragen, die größere Antworten produzieren, über DoT erneut angefragt werden [80]. Das schließt einen alleinigen Betrieb von DoDTLS aus.

In der experimentellen Form ist aktuell nur eine Sicherung der Übertragung zwischen Stub-Resolver und rekursivem Resolver angedacht. Die DNS-Nachrichten zwischen den rekursiven Resolvern und autoritativen Nameservern wird nicht durch DoDTLS verschlüsselt [80]. Aufgrund dessen und aufgrund der Tatsache, dass es sich bei DoDTLS noch um ein experimentelles Protokoll handelt und es bisher nur vereinzelte Implementierungen gibt, eignet sich DoDTLS noch nicht als DNS-Sicherheitserweiterung.

DNS-Cookies

DNS-Cookies sind eine Möglichkeit, um die DNS-Transaktionen gegen Veränderungen durch einen Off-Path-Angreifer zu schützen. Sie werden im RFC 7873 beschrieben und sind ein vorgestellter Standard [44].

DNS-Cookies erweitern das reguläre DNS-over-UDP und beschreiben zwei Arten von Cookies: Client-Cookies und Server-Cookies. Client-Cookies werden vom Client bei der DNS-Anfrage erzeugt und setzen sich aus dem Hash[3] der IP-Adresse des Client, der Server-IP-Adresse sowie einem Geheimnis, das nur dem Client bekannt ist, zusammen. Der Server-Cookie wiederum besteht aus dem Hash der Client-IP-Adresse, einem Geheimnis, das nur dem Server bekannt ist, sowie dem empfangenen Client-Cookie. Bei jeder DNS-Anfrage schickt der Client seinen Client-Cookie mit. Sofern der Client aus einer vorherigen Antwort des DNS-Servers bereits einen Server-Cookie von diesem besitzt, wird dieser ebenfalls in der DNS-Anfrage übermittelt. Anhand des Server- und Client-Cookie kann der DNS-Server überprüfen, ob es sich um einen legitimen Client handelt, da ein Client mit einer gefälschten IP-Adresse nicht über den Server-Cookie verfügt. Der Server beantwortet die DNS-Anfrage und schickt zusätzlich den Client- und Server-Cookie zurück. Sofern der Client noch nicht mit dem Server kommuniziert hat und

[3] Im RFC wird von einer pseudozufälligen Funktion gesprochen

keinen Server-Cookie übermittelt, greifen je nach Konfiguration unterschiedliche Policies. Der Server kann die Anfrage beantworten und einen Server-Cookie für die nächste Anfrage übermitteln, nur einen Server-Cookie zurückschicken oder die Anfrage still verwerfen [44].

Tabelle 5.7 stellt die durch DNS-Cookies ausgeschlossen und gemilderten Bedrohungen dar. Dabei wird davon ausgegangen, dass beide Kommunikationspartner DNS-Cookies unterstützen, da nur dann die Bedrohungen behandelt werden können.

DNS-Cookies bieten dem rekursiven Resolver die Möglichkeit invalide DNS-Anfragen, die keinen Server-Cookie besitzen, schon vor der Weiterverarbeitung zu verwerfen. Somit können die Anfragen an die autoritativen Nameserver und ggf. die zusätzlichen Berechnungen von kryptografischen Signaturen bei der Verwendung von DNSSEC vermieden werden. Dadurch werden bei einem Denial-of-Service-Angriff die rekursiven Resolver weniger belastet. Zusätzlich werden die autoritativen Nameserver bei diesen Angriffen geschützt, da sie durch die betroffenen rekursiven Resolver weniger angefragt werden. Darüber hinaus werden die Bedrohungen *DNS-Reflection* und *DNS-Amplification* gemildert, da der Server bei fehlendem Cookie, die Anfrage bedingt oder gar nicht bearbeitet (je nach Policy). Durch DNS-Cookies können außerdem Cache Poisoning-Angriffe ausgeschlossen werden, da der rekursive Resolver bei der Namensauflösung einen DNS-Cookie mitschickt und somit nur die Antworten akzeptiert, die seinen eigenen Client-Cookie enthalten. In der Theorie sind Cache Poisoning-Angriffe mit DNS-Cookies nicht ausgeschlossen, allerdings sind diese Angriffe in der Praxis aufgrund der Entropie des Client-Cookies nahezu unmöglich und werden daher hier als ausgeschlossen klassifiziert [44].

Ausgeschlossene Bedrohung	**identifiziertes System**
B21: Cache Poisoning	R
Gemilderte Bedrohung	**identifiziertes System**
B3: Denial-of-Service	R, A
B19: DNS-Reflection	R
B20: DNS-Amplification	R

Tabelle 5.7: Behandelte Bedrohungen durch Einsatz von DNS-Cookies

Analog zu DoDTLS gibt es bei DNS-Cookies ein Problem bei der Verwendung von mehreren Resolvern oder Nameservern und Anycast. Daher ist es erforderlich, das Geheimnis für den Server-Cookie über einen sicheren Kanal an alle Server zu verteilen. Es wird empfohlen das Geheimnis, je nach Sicherheitsbewusstsein, regelmäßig zu wechseln [44].

Das kann insbesondere in diesem Szenario zu größerem manuellen Aufwand führen, was wiederum dazu führen könnte, das der Geheimnisaustausch nur in großen Abständen durchgeführt wird. Dadurch wird die Chance vergrößert, dass ein Angreifer das Geheimnis erfolgreich errät.

Eine Hürde bei der Verwendung von DNS-Cookies ist, dass beide Parteien DNS-Cookies und somit EDNS unterstützen müssen, da DNS-Cookies ansonsten keinen Nutzen bringen. Allerdings werden DNS-Cookies mittlerweile von *BIND* in der Standardkonfiguration aktiviert [63].

Ein Vorteil von DNS-Cookies ist, dass der DNS-Server keinen Zustand speichern muss. Der Server kann mittels seines Geheimnisses überprüfen, ob der vom Client übertragene Server-Cookie tatsächlich korrekt ist, indem er aus der Anfrage einen neuen Server-Cookie generiert und die Hashes vergleicht. Ferner wird aufgrund der Entropie des Client-Cookies die Source Port Randomization nicht mehr zwangsläufig benötigt, um einen Cache Poisoning-Angriff zu erschweren.

Für einen On-Path-Angreifer behandeln DNS-Cookies allerdings keine Bedrohungen, da dieser den Cookie abfangen und verwenden könnte. Außerdem werden die DNS-Daten nicht verschlüsselt oder signiert und wären somit für Änderungen empfänglich. Daher reichen DNS-Cookies als einzige DNS-Sicherheitserweiterung nicht aus, um die DNS-Infrastruktur zu schützen.

DNSCurve

Das Ziel von DNSCurve ist das Sicherstellen der Integrität und Vertraulichkeit der DNS-Transaktionen sowie die Verfügbarkeit des DNS. Dabei wird die Kommunikation zwischen rekursiven Resolver (DNSCurve-Cache) und den autoritativen Nameservern[4] verschlüsselt. Eine Verschlüsselung der Kommunikation zwischen Stub-Resolver und rekursivem Resolver ist nicht vorgesehen.

Der Kern von DNSCurve ist die sogenannte kryptografische Box, die neben DNSCurve vom Mathematiker Daniel J. Bernstein entwickelt wurde. Die kryptografische Box stellt sicher, dass die beinhaltete Nachricht von niemanden geöffnet oder verändert worden ist und dass sie von dem zu erwartenden legitimen Kommunikationspartner stammt. Dazu

[4] Strenggenommen handelt es sich dabei um einen DNSCurve-fähigen DNS-Server, der neben dem autoritativen Nameserver auf demselben Server betrieben wird, und die DNS-Anfragen nach den kryptografischen Operationen lokal weiterreicht

wird auf asymmetrische Verschlüsselung, symmetrische Verschlüsselung, Nonces (number used once) und Message Authentication Codes (MAC) zurückgegriffen [19]. Die genaue Funktionsweise der kryptografischen Box soll hier nicht weiter erläutert werden.

Tabelle 5.8 zeigt die durch DNSCurve ausgeschlossen und gemilderten Bedrohungen auf. Es wird davon ausgegangen, dass der rekursive Resolver sowie der autoritative Nameserver DNSCurve-fähig sind.

Die Verschlüsselung der DNS-Nachrichten sorgt dafür, dass die Kommunikation zwischen rekursivem Resolver und autoritativem Nameserver von einem Angreifer nicht mehr abgehört werden kann. Ferner sorgt die Verschlüsselung sowie die MACs für die Integrität und Authentizität der Nachricht, so dass Man-in-the-Middle und Cache Poisoning-Angriffe verhindert werden können. Durch die Nutzung von Nonces werden Replay-Angriffe verhindert. Ferner können durch DNSCurve die Auswirkungen der DNS-Reflektierungsangriffe gemildert werden, da die DNS-Antworten die gleiche Größe wie die DNS-Anfragen besitzen. Zusätzlich können die Auswirkungen von Denial-of-Service-Angriffen durch automatisches Verwerfen von gefälschten Paketen reduziert werden [36].

Ausgeschlossene Bedrohung	**identifiziertes System**
B17: Abhören des DNS-Verkehrs	R, A
B21: Cache Poisoning	R
B22: Man-in-the-Middle	R, A
Gemilderte Bedrohung	**identifiziertes System**
B3: Denial-of-Service	R, A
B19: DNS-Reflection	R
B20: DNS-Amplification	R

Tabelle 5.8: Ausgeschlossene Bedrohungen durch Einsatz von DNSCurve

Das größte Problem bei DNSCurve ist die Online Verschlüsselung der Transaktionen, da die privaten Schlüssel im Gegensatz zu DNSSEC in den autoritativen Nameservern jederzeit vorhanden seien müssen. Bei der Nutzung von Anycast muss derselbe private Schlüssel an alle Nameserver verteilt werden, da der zugehörige öffentliche Schlüssel in dem NS-Record der Zone abgelegt wird. Das ist ein extremes Sicherheitsrisiko, insbesondere in der Wurzelzone oder den TLD-Zonen, da diese über die gesamte Welt verteilt sind und von verschiedenen Organisationen und Regierungen betrieben werden. Grothoff et al. führen an, dass aufgrund der Online Verschlüsselung zusätzlich eine Bedrohung für

Denial-of-Service-Angriffe entstehen kann, sofern die Hardware nicht ausreichend dimensioniert ist [55].

Eine weitere Hürde ist das Betreiben von zusätzlicher Software auf den Nameservern (DNSCurve-Cache und DNSCurve-Server). Zusätzliche Software kann neue Softwareschwachstellen und -Fehler beinhalten, zumal diese noch nicht von vielen Administratoren eingesetzt wird und somit weniger bewährt ist. Ferner muss die Software an alle Nameserver ausgerollt werden, da nur dann ein zuverlässiger Schutz gewährleistet ist. Bei Nichtvorhandensein des *Magic String* „uz5“, der als Erkennungsmerkmal eines DNSCurve-fähigen Servers in den NS-Records dem öffentlichen Schlüssel vorangestellt wird, fällt DNSCurve auf unsicheres DNS zurück [36].

DNSCurve kann nicht feststellen, ob der autoritative Nameserver kompromittiert wurde und ob die beinhaltenden DNS-Daten valide sind. Ferner bietet DNSCurve keinen Schutz der Kommunikation zwischen Stub-Resolver und rekursivem Resolver. Aufgrund dessen und zusätzlich aufgrund der geringen Verbreitung von DNSCurve ist es als einzige DNS-Sicherheitserweiterung nicht ausreichend um die DNS-Infrastruktur zu schützen.

Ein Protokoll, das auf DNSCurve aufbaut, ist DNSCrypt. DNSCrypt sichert dabei die Kommunikation zwischen Stub-Resolver und rekursivem Resolver [2]. DNSCrypt wurde bisher in keinem RFC beschrieben und wird daher in dieser Analyse nicht betrachtet [9].

5.2 Maßnahmen

Die DNS-Sicherheitserweiterungen wurden auf die Bedrohungen abgebildet und bewertet. Tabelle 5.9 stellt eine Reihe von möglichen Maßnahmen dar, die im Folgenden beschrieben werden.

M1: Umsetzung von DNSSEC

Wie bereits erläutert kann DNSSEC eine Fülle von Bedrohungen behandeln. Dabei ist sicherzustellen, dass die zugehörigen Schlüssel offline und vor unrechtmäßigem Zugriff gesichert sind. Zusätzlich ist sicherzustellen, die Schlüssel, insbesondere die ZSK, in regelmäßigen Abständen zu wechseln. Bei der Umsetzung sollte außerdem evaluiert werden,

Index	**Maßnahme**
M1	Umsetzung von DNSSEC
M2	Einführung von DNS-over-TLS
M3	Betrieb eines eigenen rekursiven Resolvers
M4	Nutzung von DNS-Cookies
M5	Verwendung von TSIG
M6	Pflege einer ACL
M7	Nutzung von Query Name Minimisation
M8	Konfiguration von Response Rate Limiting
M9	Nutzung von Anycast
M10	Betrieb eines Hidden-Masters
M11	Betrieb eines Paketfilters
M12	Überwachung der DNS-Server
M13	Konfiguration von 0x20-Encoding
M14	Nutzung von RPZ
M15	Deaktivieren von Wildcard-Queries
M16	Festlegen eines Registrar Locks
M17	Absicherung der Hosts
M18	Anpassung von organisatorischen Prozessen
M19	Nutzung von Zwei-Faktor-Authentisierung

Tabelle 5.9: Maßnahmenkatalog zur Sicherstellung des übergeordneten Schutzziels

ob die Maßnahmen *M8: Konfiguration von Response Rate Limiting* und *M15: Deaktivieren von Wildcard-Queries* zur Reduzierung der Bedrohungen der DNS-Amplification-Angriffe, die durch DNSSEC verstärkt werden, umgesetzt werden können.

M2: Einführung von DNS-over-TLS

Zum Schutz der Übertragung zwischen Stub-Resolver und rekursivem Resolver sollte DNS-over-TLS eingesetzt werden. Dadurch wird verhindert, dass ein Angreifer die DNS-Daten abhört oder auf dem Transportweg verändert. DoT wird gegenüber DoH bevorzugt, da DoT besser in den Betriebssystemen unterstützt wird und der DNS-Verkehr zusätzlich durch die Verwendung eines eigenen Ports geroutet werden kann. Um die größte Sicherheit zu gewährleisten, sollte DoT im strikten Nutzungsprofil betrieben werden.

M3: Betrieb eines eigenen rekursiven Resolvers

Die Stub-Resolver benötigen für die Namensauflösung einen rekursiven Resolver. Beim Betrieb eines firmeneigenen rekursiven Resolvers können die Bedrohungen, die sich durch die Nutzung eines externen rekursiven Resolvers ergeben, besser behandelt werden. Die Stub-Resolver profitieren von verbessertem Datenschutz und Unabhängigkeit gegenüber des ISPs oder anderen Unternehmen, die einen DNS-Service anbieten. Insbesondere im Hinblick auf die Einführung von DNS-over-TLS ist der Betrieb eines rekursiven Resolvers sinnvoll. Es ist sicherzustellen, dass dieser nur aus dem internen Netzwerk erreichbar und ausreichend repliziert sowie dimensioniert ist.

M4: Nutzung von DNS-Cookies

Die autoritativen Nameserver sollten DNS-Cookies unterstützten, damit diese nicht indirekt für DNS-Reflektierungsangriffe, Cache Poisoning und Denial-of-Service-Angriffe missbraucht werden können. Wie vom RFC empfohlen, ist es erforderlich, dass das Server-Geheimnis in regelmäßigen Abständen geändert wird.

M5: Verwendung von TSIG

Dynamische Updates und Zonentransfers sollten mittels TSIG signiert werden, um eine Veränderung auf dem Transportweg auszuschließen.

M6: Pflege einer Access Control List

Die Nutzung der rekursiven Resolver und internen autoritativen Nameserver sollte durch eine Access Control List (ACL) zusätzlich beschränkt werden. Dabei sollten die IP-Adressbereiche explizit angegeben werden, die Namensauflösung, Zonentransfers oder dynamische Updates durchführen dürfen.

M7: Nutzung von Query Name Minimisation

Query Name Minimisation (QNAME minimisation) sorgt dafür, dass bei einer rekursiven Namensauflösung jeder autoritative Nameserver nur den Teil der DNS-Anfrage erhält, der für die Auflösung in diesem Schritt notwendig ist [21]. Dadurch wird die Privatsphäre der Nutzer erhöht. Allerdings ist dazu der Betrieb eines eigenen rekursiven Resolvers notwendig (vgl. M3).

M8: Konfiguration von Response Rate Limiting

Die autoritativen Nameserver, insbesondere die aus dem Internet erreichbaren, sollten Response Rate Limiting (RRL) unterstützten. RRL sorgt dafür, dass die autoritativen Nameserver auf die Anfragen von Clients reagieren können, beispielsweise wenn ein Client eine Vielzahl von Anfragen stellt. Durch Heuristiken kann der autoritative Nameserver mit einer hohen Wahrscheinlichkeit erkennen, ob dieser gerade für einen Angriff missbraucht wird und somit die Antworten an den entsprechenden Client reduzieren oder ganz vermeiden [65]. Dadurch können unter anderem die Auswirkungen der Bedrohungen die sich durch die Umsetzung von DNSSEC, im Speziellen die DNS-Amplification-Angriffe, ergeben, reduziert werden. Aber auch die Auswirkungen von Denial-of-Service-Angriffen gegen die autoritativen Nameserver, wie beispielsweise die Pseudorandom Subdomain Attacks, können durch RRL gemildert werden.

M9: Nutzung von Anycast

Durch Anycast wird die Last auf die DNS-Server (autoritativ und rekursiv) besser verteilt. Dadurch können die Auswirkungen durch Denial-of-Service-Angriffe verringert werden.

M10: Betrieb eines Hidden-Masters

Hidden-Master sind versteckte primäre Nameserver, die nicht direkt von den Resolvern angefragt werden, sondern nur als zentraler Verwaltungsort für die Zoneninformationen dienen [43]. Es ist sicherzustellen, dass der Hidden-Master nicht aus dem Internet erreichbar ist und keine DNS-Anfragen beantwortet. Durch die Einführung des Hidden-Masters kann unter anderem gewährleistet werden, dass die Zoneninformationen nur aus dem internen Netz verändert werden können. Im Bezug auf die Maßnahme *M9: Nutzung von Anycast* kann ein Hidden-Master die Komplexität bei der Synchronisierung der beteiligten Nameserver reduzieren.

M11: Betrieb eines Paketfilters

Paketfilter sollten eingesetzt werden, um die DNS-Anfragen der Clients an einen eigenen rekursiven Resolver umzuleiten. Dadurch ist sichergestellt, dass die Anfragen der Stub-Resolver, die einen öffentlichen rekursiven Resolver fest konfiguriert haben, von dem firmeneigenen Resolver bearbeitet werden.

M12: Überwachung der DNS-Server

Durch die Überwachung der DNS-Server können Auffälligkeiten schnell entdeckt und behandelt werden. Es muss zumindest die Auslastung der Ressourcen, die Anzahl und Herkunft der Anfragen sowie Validierungsfehler im Bezug auf DNSSEC beobachtet werden. Ferner sollten die Log-Dateien der DNS-Serversoftware sowie des Betriebssystems in regelmäßigen Abständen überprüft werden. Darüber hinaus muss sichergestellt werden, durch zusätzliche Software oder Überwachung der Anfragen, dass der rekursive Resolver nicht für einen DNS-Tunnel missbraucht wird.

M13: Konfiguration von 0x20-Encoding

Das 0x20-Encoding kann eingesetzt werden, um vor Cache Poisoning-Angriffen zu schützen. 0x20-Encoding sorgt dafür, dass die DNS-Anfrage aus willkürlichen Groß- und Kleinbuchstaben besteht und somit die Entropie der DNS-Anfrage erhöht. Das funktioniert, da die DNS-Antwort denselben Namen wie die DNS-Anfrage beinhalten soll. Dadurch werden Cache Poisoning-Angriffe erschwert, da der Angreifer neben der Transkations-ID und dem Quell-Port die richtige Kombination aus den Klein- und Großbuchstaben der DNS-Anfrage erraten muss [35]. Laut dem DNS-Standard ist es für die Resolver und Nameserver unerheblich, ob der QNAME groß- oder klein geschrieben wird. Allerdings wurde von Problemen bei einigen Nameserver-Implementierungen berichtet, daher wird 0x20-Encoding nur eingeschränkt empfohlen und muss ggf. vorher validiert werden [64].

M14: Nutzung von RPZ

Reponse Policy Zones (RPZ), auch als DNS Firewall bezeichnet, sind eine Möglichkeit um DNS-Anfragen an vordefinierte Domains zu blockieren. Dazu nutzt der rekursive Resolver eine Liste mit zu blockierenden Domains (Blocklist). Die Liste kann von einer dritten Partei gepflegt und mittels Zonentransfer übermittelt werden oder durch das Unternehmen selbst befüllt sein. Dadurch kann der rekursive Resolver bei der DNS-Anfrage eines Stub-Resolvers, beispielsweise bei bösartigen Domains, ein *NXDOMAIN* zurückliefern und somit verhindern, dass der Client die bösartige Domain besucht [86].

M15: Deaktivieren von Wildcard-Queries

Die autoritativen Nameserver sollten Wildcard-Queries nicht beantworten. Dadurch kann sichergestellt werden, dass ein Angreifer keine Informationen über die gesamte Zone mittels einer einzigen DNS-Anfrage enthält. Außerdem werden so die zu übertragenden Daten verringert, was wiederum dazu führt, dass die autoritativen Nameserver für DNS-Reflektierungsangriffe weniger attraktiv sind.

M16: Festlegen eines Registrar Lock

Mittels Registrar Locks können die Domains und hinterlegten NS-Records gegen Manipulation gesichert werden. Dadurch werden die Auswirkungen von Social Engineering-Angriffen verringert, da eine Übernahme der Domain verhindert wird.

M17: Absicherung der Hosts

Die Hosts müssen mittels geeigneter Maßnahmen abgesichert werden. Maßnahmen sind

- regelmäßige Updates, insbesondere sicherheitsrelevante Patches,
- regelmäßige Überprüfung der Benutzerkonten und Rechte,
- regelmäßige Backups und
- ausreichende Dimensonierung der Hardware.

Durch diese Maßnahmen können die Auswirkungen der meisten Bedrohungen gegen die Hosts reduziert werden.

M18: Anpassung von organisatorischen Prozessen

Unter dieser Maßnahme werden alle menschlichen Faktoren zusammengefasst, die für den Betrieb einer DNS-Infrastruktur benötigt werden. Darunter zählen ein

- Vier-Augen-Prinzip bei der Pflege der Zoneninformationen,
- Schulungen der DNS-Administratoren,
- Einführung eines Berechtigungskonzepts und
- regelmäßige Aktualisierung der hinterlegten Informationen beim Domain-Registrar.

M19: Nutzung von Zwei-Faktor-Authentisierung

Das Verwaltungsportal beim Registrar sollte durch einen zweiten Faktor geschützt werden.

5.3 Empfehlungen

Da eine Umsetzung aller Maßnahmen für erheblichen Aufwand sorgen würde und nicht praktikabel ist, werden die vorgestellten Maßnahmen nun im Bezug auf das Anwendungsszenario priorisiert. Dabei werden die Ergebnisse aus der Risikoanalyse herangezogen und versucht, die Risiken, mittels geeigneter Maßnahmen, zu reduzieren.

Es wird empfohlen, zuerst die autoritativen Nameserver mittels geeigneter Maßnahmen zu schützen, da diese für die Plattform „InsureCloud“ und somit für die Wirtschaftlichkeit des Unternehmens, unerlässlich sind. Aus der Risikoanalyse ergab sich als höchstes Risiko die Bedrohung *B3: Denial-of-Service*. Daher wird als erstes empfohlen, die Maßnahme *M8: Konfiguration von Response Rate Limiting* umzusetzen, um somit die Auswirkungen der Denial-of-Service-Angriffe sowie DNS-Amplification-Angriffe zu verringern. Darüber hinaus sollte die Maßnahme *M9: Nutzung von Anycast* evaluiert werden, da dadurch die Last bei einem Denial-of-Service-Angriff zwischen den beiden autoritativen Nameservern NS1 und NS3 aufgeteilt werden kann.

Ein weiteres hohes Risiko ist die Bedrohung *B24: Zone Poisoning mittels Zonentransfers*, die durch die Maßnahme *M5: Verwendung von TSIG* ausgeschlossen werden kann. Daher sollte QS TSIG einführen. Das Schlüsselmanagement wird bei den drei autoritativen Nameservern als handhabbar angesehen. Die Bedrohungen *B11: Fehler in den Konfigurationsdateien* und *B18: Social Engineering* sollten durch die Maßnahmen *M18: Anpassung von organisatorischen Prozessen* und *M16: Festlegen eines Registrar Locks* behandelt werden. Durch die Einführung eines Registrar Locks werden gleichzeitig die Auswirkungen der Bedrohung *B18: Social Engineering* gegen die Domains von QS reduziert.

Nachdem diese Maßnahmen umgesetzt wurden, wird für einen erhöhten Schutzbedarf die Maßnahme *M1: Umsetzung von DNSSEC* empfohlen, um die autoritativen Nameserver und DNS-Daten zu schützen. Wie bereits gezeigt, kann DNSSEC eine Fülle von Bedrohungen behandeln. Dadurch kann die DNS-Infrastruktur von QS, insbesondere die Plattform „InsureCloud“, gegen mutwillige Veränderung der DNS-Daten geschützt werden. Die Kunden von QS haben, sofern sie einen validierenden Resolver benutzen, die Möglichkeit die Korrektheit der Resource Records zu validieren.

Als letztes wird empfohlen Maßnahmen gegen die Risiken, die die Stub-Resovler betreffen, umzusetzen. Die Bedrohung mit dem größten Risiko *B27: Ausfall oder Störung von Dienstleistern* sollte zuerst durch die Maßnahme *M3: Betrieb eines eigenen rekursiven*

Resolvers ausgeschlossen werden. Dadurch kann zusätzlich die Bedrohung *B10: Nutzung von öffentlichen rekursiven Resolvern* besser behandelt werden. Für einen Ausschluss der Gefahr muss allerdings die Maßnahme *M11: Betrieb eines Paketfilters* umgesetzt werden, um die DNS-Anfragen an externe öffentliche Resolver abzufangen und durch den eigenen Resolver zu beantworten.

Sofern der Betrieb eines eigenen rekursivem Resolvers QS zu aufwändig oder unwirtschaftlich ist, so sollten zumindest zwei unterschiedliche DNS-Provider genutzt werden. So kann das Risiko eines Ausfalls eines Dienstleisters besser kompensiert werden. Zusätzlich sollte dann die Maßnahme *M2: Einführung von DNS-over-TLS* umgesetzt werden, um die Kommunikation zwischen den Parteien zu verschlüsseln.

Die Bedrohung *B14: DNS als Infil- und Exfiltrationsmedium* kann durch die Maßnahme *M12: Überwachung der DNS-Server* behandelt werden, indem der rekursive Resolver auf ungewöhnliche DNS-Abfragen überwacht wird. Das letzte Risiko, die Bedrohung *B7: Malware* sollte durch die Maßnahme *M17: Absicherung der Hosts* behandelt werden. Insbesondere wird empfohlen, die Hosts mit aktuellen Sicherheitsupdates und Antivirensoftware zu versorgen und die Konfiguration in regelmäßigen Abständen zu überprüfen.

6 Schlussbetrachtung

In diesem Kapitel werden die erarbeiteten Ergebnisse zusammengefasst und kritisch betrachtet. Außerdem wird ein Ausblick in die Zukunft von DNS und DNS-Sicherheit gegeben.

6.1 Diskussion

Im Rahmen dieser Arbeit wurden verschiedene Bedrohungen beim Betrieb einer DNS-Infrastruktur betrachtet. Die identifizierten Systeme wurden in drei Kategorien zusammengefasst und analysiert. Im Hinblick auf das IT-Grundschutz-Kompendium konnten dadurch die Bedrohungen individueller betrachtet werden. Diese Granularität ist beim IT-Grundschutz nicht vorhanden, weshalb dort wichtige Bedrohungen, wie beispielsweise *B15: DNS als Infil- und Exfiltrationsmedium*, nicht in der Gefährdungslage aufgezeigt werden. Der IT-Grundschutz behandelt lediglich den Betrieb eines DNS-Servers, wobei auf eine Aufteilung in autoritativen und rekursiven DNS-Server sowie Stub-Resolver verzichtet wird. Ferner werden im IT-Grundschutz neun Bedrohungen beim Betrieb eines DNS-Servers explizit beschrieben. Diese Arbeit konnte allerdings zeigen, dass deutlich mehr Bedrohungen beim Betrieb einer DNS-Infrastruktur zu berücksichtigen sind. Diese Bedrohungen wurden außerdem ausführlich, unter Beachtung der beteiligten Komponenten, erläutert.

Im Gegensatz zum IT-Grundschutz werden die erarbeiteten Maßnahmen jedoch nicht in verschiedene Schutzbedarfskategorien eingestuft. Vielmehr werden Maßnahmen aufgezeigt, die für jedes Unternehmen individuell betrachtet werden müssen. Das bedeutet allerdings, dass der Aufwand für die Unternehmen steigt, da diese die eigene DNS-Infrastruktur zuerst analysieren müssen. Dadurch kann aber der Aufwand zur Umsetzung der Maßnahmen verringert werden, da nicht wie beim IT-Grundschutz alle Maßnahmen für einen normalen Schutzbedarf umgesetzt werden müssen. Die Unternehmen reagieren

auf die identifizierten Risiken durch Auswahl und Priorisierung der geeigneten Maßnahmen. Wie die Empfehlungen für das Anwendungsszenario zeigen, können aufgrund dessen schon wenige und gezielte Maßnahmen für einen angemessenen Schutz der DNS-Infrastruktur sorgen. Dadurch ist dieses Verfahren effizienter und das Unternehmen kann Zeit und Geld sparen.

Genauso wie beim IT-Grundschutz wurde auf eine quantitative Einschätzung der Maßnahmen verzichtet, da das Abschätzen des Umfangs immer abhängig von der bereits bestehenden Infrastruktur ist. So kann beispielsweise der Aufwand der Maßnahme *M5: Verwendung von TSIG* nicht eingeschätzt werden, da der Aufwand mit der Anzahl der autoritativen Nameserver steigt (Schlüsselaustausch).

Darüber hinaus wurden verschiedene DNS-Sicherheitserweiterung, wie DNSSEC, DoT und DoH vorgestellt und deren Anwendungsfälle erläutert und dessen Probleme und Limitationen aufgezeigt. Das IT-Grundschutz-Kompendium betrachtet als alleinige Sicherheitserweiterung lediglich DNSSEC, wobei nicht auf die Probleme, die durch DNSSEC entstehen, hingewiesen wird. Allerdings wird im DNS-Baustein unter *Wissenswertes* auf Handlungsempfehlungen beim Betrieb von DNSSEC in einem separaten Dokument hingewiesen. Die Arbeit konnte außerdem zeigen, dass die Kommunikation zwischen Stub-Resolver und rekursivem Resolver durch einen Angreifer abgefangen, verändert oder verhindert werden kann. Die gewonnenen Informationen lassen sich wiederum für andere Angriffe nutzen. Daher muss insbesondere im Unternehmenskontext eine Absicherung dieses Kanals für ein unverschlüsseltes Protokoll, wie DNS, betrachtet und für jeden Anwendungsfall individuell abgeschätzt werden.

Der erste Schritt, die konzeptionelle Betrachtung von DNS und DNS-Sicherheit, ist erfolgt. In weiteren Arbeiten kann die Erstellung einer vollumfassenden Sicherheitsstrategie für den Anwendungsfall betrachtet werden.

6.2 Fazit

Ziel dieser Arbeit ist es, DNS und DNS-Sicherheit anhand eines fiktiven Anwendungsszenarios zu betrachten und zu überprüfen, welche Risiken bei der Nutzung von DNS bestehen und ob diese durch ausgewählte DNS-Sicherheitserweiterungen verringert oder vermieden werden können. Es wurde aufgezeigt, dass der Betrieb einer DNS-Infrastruktur mit einigen Risiken verbunden ist und das DNS für Angriffe ausgenutzt werden kann.

Somit kann die erste Forschungsfrage „Welche Bedrohungen ergeben sich, insbesondere für das Anwendungsszenario, durch die Nutzung von DNS?“ als beantwortet angesehen werden.

Zusätzlich zeigte sich, dass keine DNS-Sicherheitserweiterung alleine einen vollumfänglichen Schutz bietet. Deshalb ist für einen effektiven Schutz immer die anwendungsspezifische Kombination von mehreren Erweiterungen erforderlich. Dabei muss beachtet werden, dass einige DNS-Sicherheitserweiterungen nicht geeignet sind, da sie aufgrund von Designentscheidungen im Unternehmenskontext nicht handhabbar sind. Außerdem wurden weitere Probleme und Risiken aufgedeckt, die sich durch die Nutzung der Sicherheitserweiterungen ergeben. Die zweite Forschungsfrage „Bei welchen Bedrohungen können die DNS-Sicherheitserweiterungen zum Einsatz kommen, um das Bedrohungsrisiko zu minimieren?“ kann daher als beantwortet betrachtet werden.

Zum Schluss wurden 19 Maßnahmen erarbeitet, mit denen auf die Risiken sinnvoll reagiert werden kann. Es wurde gezeigt, dass es ausreichend ist, zehn Maßnahmen umzusetzen, um das Risiko für den Anwendungsfall zu reduzieren. Damit wird die dritte Forschungsfrage „Welche DNS-Sicherheitserweiterungen und Maßnahmen eignen sich, insbesondere im Bezug auf das Anwendungsszenario, für die beschriebenen Bedrohungen?“ als beantwortet angesehen.

6.3 Limitationen und Ausblick

Diese Arbeit ist nicht frei von Limitationen, da sich auf ein fiktives Anwendungsszenario bezogen wird. Daher sollte in weiterführenden Forschungen evaluiert werden, inwiefern die vorgestellten Maßnahmen auf andere Klassen von Anwendungsfällen angewandt werden können. Ferner wurden nur ausgewählte Standards und Entwürfe für die Evaluation ausgewählt. Die Ergebnisse aus der Bedrohungsanalyse könnten für weitere Forschungen mit anderen DNS-Sicherheitserweiterungen, wie beispielsweise DNS-over-QUIC, genutzt werden.

Außerdem wurde in dieser Arbeit DNS als einziges System zur Namensauflösung betrachtet. Es gibt jedoch auch Alternativen zu DNS, wie beispielsweise Namecoin oder GNU Name System (GNS), die in weiterführenden Forschungen betrachtet werden können. Namecoin ist eine Kryptowährung, die das Ziel hat, eine von der ICANN unabhängige und

dezentrale Namensauflösung anzubieten. Dabei steht die Privatsphäre der Nutzer im Vordergrund. Der Namensraum besteht aus der inoffiziellen TLD *.bit*, die nur über Namecoin erreichbar ist [4]. GNS ist ein alternatives System zur Namensauflösung und mit DNS kompatibel. GNS basiert allerdings nicht auf einer hierarchischen Struktur, sondern auf einem gerichteten Graphen. Der Namensraum von GNS besteht aus der inoffiziellen TLD *.gnu* [51]. Diese beiden Alternativen könnten mit den Ergebnissen aus dieser Arbeit betrachtet werden. Beispielsweise könnte überprüft werden, ob diese Systeme für dieselben Bedrohungen empfänglich sind. Auch eine Gegenüberstellung der jeweiligen Systeme, um die Gefährdungen miteinander zu vergleichen, ist für aufbauende Forschung vorstellbar. Interessant wäre auch, ob es ähnliche Risiken gibt und mit welchen Sicherheitsmaßnahmen diesen entgegen gewirkt wird. Die Ergebnisse könnten ggf. für einen sicheren Betrieb von DNS genutzt werden.

Die IETF Working Group DNS PRIVate Exchange (DPRIVE), die unter anderem DoT und DoDTLS spezifiziert haben, hat bereits angekündigt, sich auf die Kommunikation zwischen rekursivem Resolver und autoritativem Nameserver zu konzentrieren. Dabei soll die Vertraulichkeit der DNS-Transaktionen im Vordergrund stehen [92]. Vorstellbar ist, dass DoT für die Kommunikation zwischen rekursivem Resolver und autoritativem Nameserver genutzt werden soll. 2019 wurde die IETF Working Group Adaptive DNS Discovery (add) gegründet, um technische Maßnahmen zu entwickeln, damit ein Stub-Resolver im Internet oder privaten Netzwerken die rekursiven Resolver findet, die eine Verschlüsselung (DoT oder DoH) unterstützen [68]. Es bleibt abzuwarten, inwieweit die identifizierten Probleme und Bedrohungen durch diese Erweiterungen behandelt werden können oder ob es dadurch nicht zu zusätzlichen Bedrohungen kommt.

Literaturverzeichnis

[1] : *dig(1): DNS lookup utility - Linux man page*. – URL https://linux.die.net/man/1/dig. – Zugriffsdatum: 2020-10-31

[2] : *DNSCrypt - Official Project Home Page*. – URL https://www.dnscrypt.org/. – Zugriffsdatum: 2020-11-14

[3] : *getaddrinfo(3) - Linux manual page*. – URL https://man7.org/linux/man-pages/man3/getaddrinfo.3.html. – Zugriffsdatum: 2020-10-07

[4] : *Namecoin*. – URL https://www.namecoin.org/. – Zugriffsdatum: 2020-11-28

[5] : *resolv.conf(5) - Linux manual page*. – URL https://man7.org/linux/man-pages/man5/resolv.conf.5.html. – Zugriffsdatum: 2020-10-29

[6] *Beratungsprotokoll (Versicherungsvermittlung)*. Dezember 2019. – URL https://de.wikipedia.org/w/index.php?title=Beratungsprotokoll_(Versicherungsvermittlung)&oldid=194661233. – Zugriffsdatum: 2020-09-16. – Page Version ID: 194661233

[7] *BIND*. August 2020. – URL https://en.wikipedia.org/w/index.php?title=BIND&oldid=974033247. – Zugriffsdatum: 2020-09-17. – Page Version ID: 974033247

[8] *Birthday problem*. September 2020. – URL https://en.wikipedia.org/w/index.php?title=Birthday_problem&oldid=977594569. – Zugriffsdatum: 2020-09-30. – Page Version ID: 977594569

[9] *DNSCrypt*. August 2020. – URL https://en.wikipedia.org/w/index.php?title=DNSCrypt&oldid=975292995. – Zugriffsdatum: 2020-11-14. – Page Version ID: 975292995

[10] Alexander, S. ; Droms, R.: DHCP Options and BOOTP Vendor Extensions / RFC Editor. URL https://www.rfc-editor.org/info/rfc2132. – Zugriffsdatum: 2020-09-03, März 1997 (RFC2132). – Forschungsbericht. – RFC2132 S

[11] Arends, R. ; Austein, R. ; Larson, M. ; Massey, D. ; Rose, S.: DNS Security Introduction and Requirements / RFC Editor. URL https://www.rfc-editor.org/info/rfc4033. – Zugriffsdatum: 2020-11-04, März 2005 (RFC4033). – Forschungsbericht. – RFC4033 S

[12] Ariyapperuma, Suranjith ; Mitchell, Chris J.: Security vulnerabilities in DNS and DNSSEC. In: *The Second International Conference on Availability, Reliability and Security (ARES'07)*, April 2007, S. 335–342

[13] Arntz, Pieter: *Hosts file hijacks*. September 2016. – URL https://blog.malwarebytes.com/cybercrime/2016/09/hosts-file-hijacks/. – Zugriffsdatum: 2020-09-30. – Section: Cybercrime

[14] Assigned Names and Numbers, Internet C. for: *EPP Status Codes | What Do They Mean, and Why Should I Know? - ICANN*. – URL https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en. – Zugriffsdatum: 2020-10-31

[15] Atkins, D. ; Austein, R.: Threat Analysis of the Domain Name System (DNS) / RFC Editor. URL https://www.rfc-editor.org/info/rfc3833. – Zugriffsdatum: 2020-08-03, August 2004 (RFC3833). – Forschungsbericht. – RFC3833 S

[16] Barr, D.: Common DNS Operational and Configuration Errors / RFC Editor. URL https://www.rfc-editor.org/info/rfc1912. – Zugriffsdatum: 2020-08-17, Februar 1996 (RFC1912). – Forschungsbericht. – RFC1912 S

[17] Baun, Christian: *Computernetze kompakt: Eine an der Praxis orientierte Einführung für Studium und Berufspraxis*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2020 (IT kompakt). – URL http://link.springer.com/10.1007/978-3-662-59897-9. – Zugriffsdatum: 2020-11-21. – ISBN 978-3-662-59896-2 978-3-662-59897-9

[18] Bellis, R.: DNS Proxy Implementation Guidelines. (2009). – URL https://www.rfc-editor.org/info/rfc5625. – Zugriffsdatum: 2020-10-29. – Number: RFC 5625. – ISSN 2070-1721

[19] Bernstein, Daniel J. ; Lange, Tanja ; Schwabe, Peter: *Public-key authenticated encryption: crypto_box*. – URL https://nacl.cr.yp.to/box.html. – Zugriffsdatum: 2020-11-14

[20] Bortzmeyer, S.: DNS Privacy Considerations / RFC Editor. URL https://www.rfc-editor.org/info/rfc7626. – Zugriffsdatum: 2020-08-03, August 2015 (RFC7626). – Forschungsbericht. – RFC7626 S

[21] Bortzmeyer, S.: DNS Query Name Minimisation to Improve Privacy. (2016). – URL https://www.rfc-editor.org/info/rfc7816. – Zugriffsdatum: 2020-11-14. – Number: RFC 7816. – ISSN 2070-1721

[22] Bound, Jim ; Rekhter, Yakov: *Dynamic Updates in the Domain Name System (DNS UPDATE)*. – URL https://tools.ietf.org/html/rfc2136. – Zugriffsdatum: 2020-10-01

[23] Brahmasani, Siva ; Sivasankar, E.: Two level verification for detection of DNS rebinding attacks. In: *International Journal of System Assurance Engineering and Management* 4 (2013), Juni, Nr. 2, S. 138–145. – URL https://doi.org/10.1007/s13198-013-0153-x. – Zugriffsdatum: 2020-09-29. – ISSN 0976-4348

[24] Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 200-3: Risikoanalyse auf Basis von IT-Grundschutz*. – URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf?__blob=publicationFile&v=7. – Zugriffsdatum: 2020-08-03

[25] Bundesamt für Sicherheit in der Informationstechnik: Zunahme von DDoS-Angriffen durch DNS-Reflection.

[26] Bundesanstalt für Finanzdienstleistungsaufsicht: *Versicherungsaufsichtliche Anforderungen an die IT (VAIT)*. März 2019

[27] Bundesanzeiger Verlag GmbH ; Deutschland ; Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz-Kompendium*. 2018. – OCLC: 1027470677. – ISBN 978-3-8462-0906-6

[28] Bundesministerium der Justiz und für Verbraucherschutz: *Gesetz über die Beaufsichtigung der Versicherungsunternehmen*. – URL https://www.gesetze-im-internet.de/vag_2016/. – Zugriffsdatum: 2020-09-22

[29] Bundesministerium für Wirtschaft und Energie: Orientierungshilfe zum Gesundheitsdatenschutz. (2018), November, S. 100

[30] Böck, Hanno: *T-Online-Navigationshilfe: Telekom beendet DNS-Hijacking - Golem.de.* – URL https://www.golem.de/news/t-online-navigationshilfe-telekom-beendet-dns-hijacking-nach-strafanzeige-1905-141370.html. – Zugriffsdatum: 2020-09-26

[31] Cambus, Frederic: *StatDNS - DNS related RFCs.* – URL https://www.statdns.com/rfc/. – Zugriffsdatum: 2020-11-04

[32] Chandramouli, Ramaswamy ; Rose, Scott: Secure Domain Name System (DNS) Deployment Guide / National Institute of Standards and Technology. URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf. – Zugriffsdatum: 2020-08-06, September 2013 (NIST SP 800-81-2). – Forschungsbericht. – NIST SP 800–81–2 S

[33] Cobb, S.: PPP Internet Protocol Control Protocol Extensions for Name Server Addresses / RFC Editor. URL https://www.rfc-editor.org/info/rfc1877. – Zugriffsdatum: 2020-10-07, Dezember 1995 (RFC1877). – Forschungsbericht. – RFC1877 S

[34] Consortium, Internet S.: *Biannual survey: Versions of DNS software.* – URL https://ftp.isc.org/www/survey/reports/current/fpdns.txt. – Zugriffsdatum: 2020-08-17

[35] Dagon, David ; Vixie, Paul: *Use of Bit 0x20 in DNS Labels to Improve Transaction Identity.* – URL https://tools.ietf.org/html/draft-vixie-dnsext-dns0x20-00. – Zugriffsdatum: 2020-11-15

[36] Dempsky, Matthew: *DNSCurve: Link-Level Security for the Domain Name System.* – URL https://tools.ietf.org/html/draft-dempsky-dnscurve-01#ref-naclcrypto. – Zugriffsdatum: 2020-11-14

[37] DENIC eG: *Monatsauswertung DNSSEC - DENIC eG.* – URL https://www.denic.de/wissen/statistiken/monatsauswertung-dnssec/. – Zugriffsdatum: 2020-11-04

[38] DENIC eG: *Nameservice - DENIC eG.* – URL https://www.denic.de/service/nameservice/. – Zugriffsdatum: 2020-11-21

[39] DENIC eG: *Registrierung - DENIC eG.* – URL https://www.denic.de/domains/de-domains/registrierung/. – Zugriffsdatum: 2020-11-21

[40] Dickinson, S. ; Gillmor, D. ; Reddy, T.: Usage Profiles for DNS over TLS and DNS over DTLS / RFC Editor. URL https://www.rfc-editor.org/info/rfc8310. – Zugriffsdatum: 2020-11-10, März 2018 (RFC8310). – Forschungsbericht. – RFC8310 S

[41] Dickinson, Sara ; Mankin, Allison ; Overeinder, Benno: *DNS Privacy Implementation Status - DNS Privacy Project.* – URL https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status. – Zugriffsdatum: 2020-11-11

[42] Dietrich, Christian J. ; Rossow, Christian ; Freiling, Felix C. ; Bos, Herbert ; Steen, Maarten v. ; Pohlmann, Norbert: On Botnets That Use DNS for Command and Control. In: *2011 Seventh European Conference on Computer Network Defense*. Gothenburg, Sweden : IEEE, September 2011, S. 9–16. – URL http://ieeexplore.ieee.org/document/6377756/. – Zugriffsdatum: 2020-10-31. – ISBN 978-0-7695-4762-6 978-1-4673-2116-7

[43] Dooley, Michael ; Rooney, Timothy: *DNS security management*. Hoboken, New Jersey : Piscataway, NJ : John Wiley and Sons, Inc. ; IEEE Press, 2017 (IEEE Press series on networks and services management). – OCLC: ocn974672804. – ISBN 978-1-119-32827-8

[44] Eastlake, D. ; Andrews, M.: Domain Name System (DNS) Cookies / RFC Editor. URL https://www.rfc-editor.org/info/rfc7873. – Zugriffsdatum: 2020-11-04, Mai 2016 (RFC7873). – Forschungsbericht. – RFC7873 S

[45] Eastlake 3rd, D.: Domain Name System Security Extensions. (1999). – URL https://www.rfc-editor.org/info/rfc2535. – Zugriffsdatum: 2020-11-22. – Number: RFC 2535. – ISSN 2070-1721

[46] Eckert, Claudia: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Berlin, Boston : De Gruyter, August 2018. – URL http://www.degruyter.com/view/books/9783110563900/9783110563900/9783110563900.xml. – Zugriffsdatum: 2020-08-05. – ISBN 978-3-11-056390-0

[47] EFFICIENT IP: *IDC 2020 Global DNS Threat Report | DNS Attacks Defense.* – URL https://www.efficientip.com/resources/idc-dns-threat-report-2020/. – Zugriffsdatum: 2020-11-21

[48] FARRELL, S. ; TSCHOFENIG, H.: Pervasive Monitoring Is an Attack / RFC Editor. URL https://www.rfc-editor.org/info/rfc7258. – Zugriffsdatum: 2020-08-03, Mai 2014 (RFC7258). – Forschungsbericht. – RFC7258 S

[49] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS: *CVSS v3.1 Specification Document.* – URL https://www.first.org/cvss/specification-document. – Zugriffsdatum: 2020-10-22

[50] GALVIN, James M.: *DNS Security: A Historical Perspective.* – URL https://www.ietfjournal.org/dns-security-a-historical-perspective/. – Zugriffsdatum: 2020-11-22

[51] GNUNET E.V.: *GNUnet.* – URL https://gnunet.org/de/gns.html. – Zugriffsdatum: 2020-11-28

[52] GOOGLE IRELAND LIMITED: *Your Privacy | Public DNS | Google Developers.* – URL https://developers.google.com/speed/public-dns/privacy. – Zugriffsdatum: 2020-09-17

[53] GREENBERG, Andy: How an Unprecedented Heist Hijacked a Bank's Entire Online Operation. In: *Wired.* – URL https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/. – Zugriffsdatum: 2020-11-21. – ISSN 1059-1028

[54] GROTHOFF, CHRISTIAN ; WACHS, MATTHIAS ; APPELBAUM, JACOB ; ERMERT, MONIKA: NSA's MORECOWBELL: knell for DNS. (2017). – URL http://goodtimesweb.org/surveillance/2015/MORECOWBELL-Analysis-Grothoff-etal.pdf. – Zugriffsdatum: 2020-10-18

[55] GROTHOFF, Christian ; WACHS, Matthias ; ERMERT, Monika ; APPELBAUM, Jacob: Towards Secure Name Resolution on the Internet (v1.1).

[56] HARDAKER, W. ; GUDMUNDSSON, O. ; KRISHNASWAMY, S.: DNSSEC Roadblock Avoidance / RFC Editor. URL https://www.rfc-editor.org/info/rfc8027. – Zugriffsdatum: 2020-11-05, November 2016 (RFC8027). – Forschungsbericht. – RFC8027 S

[57] Hoffman, P. ; McManus, P.: DNS Queries over HTTPS (DoH) / RFC Editor. URL https://www.rfc-editor.org/info/rfc8484. – Zugriffsdatum: 2020-08-03, Oktober 2018 (RFC8484). – Forschungsbericht. – RFC8484 S

[58] Hoffman, P. ; Sullivan, A. ; Fujiwara, K.: DNS Terminology / RFC Editor. URL https://www.rfc-editor.org/info/rfc8499. – Zugriffsdatum: 2020-11-04, Januar 2019 (RFC8499). – Forschungsbericht. – RFC8499 S

[59] Hollenbeck, Scott ; Veeramachaneni, Srikanth ; Yalamanchilli, Suresh: *VeriSign Registry Registrar Protocol (RRP) Version 2.0.0.* – URL https://tools.ietf.org/html/rfc3632. – Zugriffsdatum: 2020-12-02

[60] Hu, Z. ; Zhu, L. ; Heidemann, J. ; Mankin, A. ; Wessels, D. ; Hoffman, P.: Specification for DNS over Transport Layer Security (TLS) / RFC Editor. URL https://www.rfc-editor.org/info/rfc7858. – Zugriffsdatum: 2020-08-03, Mai 2016 (RFC7858). – Forschungsbericht. – RFC7858 S

[61] ICANN Security and Stability Advisory Committee: *The DNS and the Internet of Things: Opportunities, Risks, and Challenges.* Mai 2019. – URL https://www.icann.org/en/system/files/files/sac-105-en.pdf. – Zugriffsdatum: 2020-11-22

[62] Informationstechnik, Bundesamt für Sicherheit in der: *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise.* – URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile&v=3. – Zugriffsdatum: 2020-08-05

[63] Internet Systems Consortium: *BIND 9 Administrator Reference Manual — BIND 9 documentation.* – URL https://bind9.readthedocs.io/en/v9_16_7/. – Zugriffsdatum: 2020-10-29

[64] Internet Systems Consortium: *Case-Insensitive Response Compression May Cause Problems With Mixed-Case Data and Non-Conforming Clients - BIND 9.* – URL https://kb.isc.org/docs/aa-01113. – Zugriffsdatum: 2020-11-15

[65] Internet Systems Consortium: *Introduction to Response Rate Limiting (RRL).* – URL https://kb.isc.org/docs/aa-01000. – Zugriffsdatum: 2020-11-14

[66] Koch, Peter: Vertraulichkeit für den Auskunftsdienst im Internet?: Überlegungen zur Verschlüsselung und anderen Ergänzungen zum Domain Name System (DNS).

In: *Datenschutz und Datensicherheit - DuD* 38 (2014), Juli, Nr. 7, S. 458–461. – URL http://link.springer.com/10.1007/s11623-014-0206-6. – Zugriffsdatum: 2020-08-19. – ISSN 1614-0702, 1862-2607

[67] Laurie, B. ; Sisson, G. ; Arends, R. ; Blacka, D.: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. (2008). – URL https://www.rfc-editor.org/info/rfc5155. – Zugriffsdatum: 2020-12-05. – Number: RFC 5155. – ISSN 2070-1721

[68] Leiba: *Adaptive DNS Discovery (add)* -. – URL https://datatracker.ietf.org/wg/add/about/. – Zugriffsdatum: 2020-11-28

[69] Liska, Allan ; Stowe, Geoffrey: *DNS Security*. Elsevier, 2016. – URL https://linkinghub.elsevier.com/retrieve/pii/C20140045649. – Zugriffsdatum: 2020-08-03. – ISBN 978-0-12-803306-7

[70] Man, Keyu ; Qian, Zhiyun ; Wang, Zhongjie ; Zheng, Xiaofeng ; Huang, Youjun ; Duan, Haixin: DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels. In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. Virtual Event USA : ACM, Oktober 2020, S. 1337–1350. – URL https://dl.acm.org/doi/10.1145/3372297.3417280. – Zugriffsdatum: 2020-11-15. – ISBN 978-1-4503-7089-9

[71] Meinel, Christoph: *Meinels Web-Tutorial: Das Domain Name System - das Telefonbuch des Internets*. – URL https://www.spektrum.de/kolumne/das-domain-name-system-ist-das-telefonbuch-des-internets/1732674. – Zugriffsdatum: 2020-11-21

[72] Microsoft Corporation: *DnsQuery_A function (windns.h) - Win32 apps*. – URL https://docs.microsoft.com/en-us/windows/win32/api/windns/nf-windns-dnsquery_a. – Zugriffsdatum: 2020-10-07

[73] Mockapetris, P. V.: Domain names: Concepts and facilities. (1983). – URL https://www.rfc-editor.org/info/rfc882. – Zugriffsdatum: 2020-11-21. – Number: RFC 882. – ISSN 2070-1721

[74] Mockapetris, P.V.: Domain names - concepts and facilities / RFC Editor. URL https://www.rfc-editor.org/info/rfc1034. – Zugriffsdatum: 2020-08-06, November 1987 (RFC1034). – Forschungsbericht. – RFC1034 S

[75] Mockapetris, P.V.: Domain names - implementation and specification / RFC Editor. URL https://www.rfc-editor.org/info/rfc1035. – Zugriffsdatum: 2020-08-03, November 1987 (RFC1035). – Forschungsbericht. – RFC1035 S

[76] Müller, Moritz ; Thomas, Matthew ; Wessels, Duane ; Hardaker, Wes ; Chung, Taejoong ; Toorop, Willem ; Rijswijk-Deij, Roland v.: Roll, Roll, Roll your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover. In: *Proceedings of the Internet Measurement Conference*. Amsterdam Netherlands : ACM, Oktober 2019, S. 1–14. – URL https://dl.acm.org/doi/10.1145/3355369.3355570. – Zugriffsdatum: 2020-11-24. – ISBN 978-1-4503-6948-0

[77] Nadler, Asaf ; Aminov, Avi ; Shabtai, Asaf: Detection of malicious and low throughput data exfiltration over the DNS protocol. In: *Computers & Security* 80 (2019), Januar, S. 36–53. – URL http://www.sciencedirect.com/science/article/pii/S0167404818304000. – Zugriffsdatum: 2020-09-29. – ISSN 0167-4048

[78] Postel, J. ; Reynolds, J. K.: *Domain requirements*. – URL https://tools.ietf.org/html/rfc920. – Zugriffsdatum: 2020-11-21

[79] Rat der Europäischen Union: *Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*. April 2016. – URL https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02016R0679-20160504. – Zugriffsdatum: 2020-09-22

[80] Reddy, T. ; Wing, D. ; Patil, P.: DNS over Datagram Transport Layer Security (DTLS) / RFC Editor. URL https://www.rfc-editor.org/info/rfc8094. – Zugriffsdatum: 2020-08-03, Februar 2017 (RFC8094). – Forschungsbericht. – RFC8094 S

[81] Rescorla, E.: HTTP Over TLS. (2000). – URL https://www.rfc-editor.org/info/rfc2818. – Zugriffsdatum: 2020-12-01. – Number: RFC 2818. – ISSN 2070-1721

[82] Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.3 / RFC Editor. URL https://www.rfc-editor.org/info/rfc8446. – Zugriffsdatum: 2020-08-03, August 2018 (RFC8446). – Forschungsbericht. – RFC8446 S

[83] Rescorla, E. ; Modadugu, N.: Datagram Transport Layer Security Version 1.2. (2012). – URL https://www.rfc-editor.org/info/rfc6347. – Zugriffsdatum: 2020-11-14. – Number: RFC 6347. – ISSN 2070-1721

[84] Sadaf Yasmin ; Muhammad Yousaf ; Amir Qayyum: Security issues related with DNS dynamic updates for mobile nodes: a survey. Islamabad, 2010. – URL https://www.researchgate.net/publication/220791666_Security_issues_related_with_DNS_dynamic_updates_for_mobile_nodes_a_survey. – Zugriffsdatum: 2020-10-01

[85] Scherschel, Fabian A.: *Godlua: Hacker verstecken Malware-Traffic im DNS-over-HTTPS-Protokoll.* – URL https://www.heise.de/security/meldung/Godlua-Hacker-verstecken-Malware-Traffic-im-DNS-over-HTTPS-Protokoll-4463479.html. – Zugriffsdatum: 2020-11-21

[86] Schryver, Vernon ; Vixie, Paul: *DNS Response Policy Zones (RPZ).* – URL https://tools.ietf.org/html/draft-ietf-dnsop-dns-rpz-00. – Zugriffsdatum: 2020-11-15

[87] Secureworks Inc.: *DNS Cache Poisoning - The Next Generation.* – URL https://www.secureworks.com/blog/dns-cache-poisoning. – Zugriffsdatum: 2020-09-24

[88] Steen, Maarten v. ; Tanenbaum, Andrew S.: *Distributed systems.* Third edition (Version 3.01 (2017)). London : Pearson Education, 2017. – OCLC: 1006750554. – ISBN 978-1-5430-5738-6 978-90-815406-2-9

[89] Strotmann, Carsten ; Schmidt, Jürgen: *Private Auskunft.* 2018. – URL https://www.heise.de/select/ct/2018/14/1530492966691096. – Zugriffsdatum: 2020-11-22

[90] The OWASP Foundation: *Server Side Request Forgery Software Attack | OWASP Foundation.* – URL https://owasp.org/www-community/attacks/Server_Side_Request_Forgery. – Zugriffsdatum: 2020-09-29

[91] Vixie, P. ; Gudmundsson, O. ; Eastlake, D. ; Wellington, B.: Secret Key Transaction Authentication for DNS (TSIG) / RFC Editor. URL https://www.rfc-editor.org/info/rfc2845. – Zugriffsdatum: 2020-11-03, Mai 2000 (RFC2845). – Forschungsbericht. – RFC2845 S

[92] Vyncke, Éric: *DNS PRIVate Exchange (dprive)* -. – URL https://datatracker.ietf.org/wg/dprive/about/. – Zugriffsdatum: 2020-11-28

[93] Weiss, Eva-Maria: *Firefox aktiviert in den USA DNS-over-HTTPS standardmäßig.* – URL https://www.heise.de/newsticker/meldung/Firefox-aktiviert-in-den-USA-DNS-over-HTTPS-standardmaessig-4667693.html. – Zugriffsdatum: 2020-11-11

[94] Wellington, B. ; Gudmundsson, O.: Redefinition of DNS Authenticated Data (AD) bit / RFC Editor. URL https://www.rfc-editor.org/info/rfc3655. – Zugriffsdatum: 2020-11-05, November 2003 (RFC3655). – Forschungsbericht. – RFC3655 S

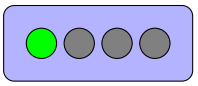
[95] Woolf, Suzanne ; Kumari, Warren ; Migault, Daniel ; Arends, Roy: *Highly Automated Method for Maintaining Expiring Records.* – URL https://tools.ietf.org/html/draft-wkumari-dnsop-hammer-03. – Zugriffsdatum: 2020-11-05

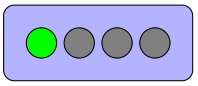
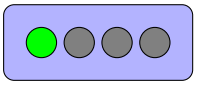
A Anhang

A.1 Risikoanalyse

A.1.1 Stub-Resolver

Tabelle A.1: Risikoanalyse für den Stub-Resolver im Endsystem

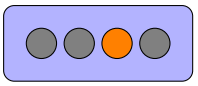
<table>
<tr><td colspan="3">Stub-Resolver im Endsystem</td></tr>
<tr><td>Gefährdung:
B1: Software-Schwachstellen oder -Fehler</td><td colspan="2">Beeinträchtigte Grundwerte:
Verfügbarkeit</td></tr>
<tr><td>Eintrittswahrscheinlichkeit:
unwahrscheinlich</td><td>Auswirkungen:
begrenzt</td><td>Risiko:
gering
  </td></tr>
<tr><td colspan="3">Beschreibung
Der Stub-Resolver als Softwarekomponente des Betriebssystems kann durch Schwachstellen (bsp. Buffer Overflows) angegriffen werden, um die Verfügbarkeit der Namensauflösung einzuschränken.
Bewertung
Der Stub-Resolver ist kein vollwertiger Full-Resolver und somit weniger fehleranfällig. Clients kommunizieren im internen Netzwerk hinter einer Firewall und sind deshalb nicht direkt angreifbar. Daher wird die Eintrittswahrscheinlichkeit als unwahrscheinlich angesehen. Die Auswirkungen werden als begrenzt klassifiziert. Dadurch ergibt sich ein geringes Risiko.</td></tr>
</table>

Stub-Resolver im Endsystem		
Gefährdung: **B2: Datenverlust**	Beeinträchtigte Grundwerte: Verfügbarkeit	
Eintrittswahrscheinlichkeit: unwahrscheinlich	Auswirkungen: vernachlässigbar	Risiko: **gering** 
Beschreibung Der Stub-Resolver benötigt zur Namensauflösung die zu verwendenden rekursiven Resolver. Diese können fest konfiguriert sein oder dem Client bei Verbindung mit einem Netzwerk mitgeteilt werden. Ein Verlust der Konfiguration führt dazu, dass die Namensauflösung nicht mehr durchgeführt werden kann. **Bewertung** Je nach Betriebssystem erfordert das Löschen der Konfiguration höhere Rechte oder Eingaben auf der Kommandozeile. Die Computer des Unternehmens sind mit restriktiven Berechtigungen ausgestattet, so dass ein Benutzer die Konfigurationsdateien nicht löschen kann. Sollten die Konfigurationen gelöscht worden sein, so können die zu verwendenden Resolver durch ein Neuverbindung mit dem Netzwerk wiederhergestellt werden, da diese per DHCP verteilt werden. Das ist insbesondere für die privaten Endgeräten relevant, auf denen die Benutzer uneingeschränkte Rechte haben. Die Eintrittswahrscheinlichkeit wird daher mit unwahrscheinlich ausgegeben. Die Auswirkungen werden als vernachlässigbar eingeschätzt. Dadurch ergibt sich ein geringes Risiko.		
Gefährdung: **B3: Denial-of-Service-Angriffe**	Beeinträchtigte Grundwerte: Verfügbarkeit	
Eintrittswahrscheinlichkeit: unwahrscheinlich	Auswirkungen: begrenzt	Risiko: **gering** 
Beschreibung Der Stub-Resolver ist wie jede andere Netzwerkkomponente durch Denial-of-Service-Angriffe verwundbar, um die Verfügbarkeit der Namensauflösung einzuschränken.		

Stub-Resolver im Endsystem

Bewertung

Die Eintrittswahrscheinlichkeit wird als unwahrscheinlich eingestuft, da die Clients für gewöhnlich hinter einer Firewall agieren. Die Schadensauswirkungen sind auf den Client beschränkt und werden als begrenzt eingestuft. Dadurch ergibt sich ein geringes Risiko.

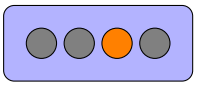
Gefährdung: **B7: Malware**	Beeinträchtigte Grundwerte: Verfügbarkeit, Integrität	
Eintrittswahrscheinlichkeit: wahrscheinlich	Auswirkungen: beträchtlich	Risiko: **hoch** 

Beschreibung

Die DNS-Einträge in den Konfigurationsdateien oder Caches der Clients können durch Malware geändert werden und die Verfügbarkeit von Diensten einschränken.

Bewertung

Die Eintrittswahrscheinlichkeit wird mit wahrscheinlich angegeben, da eine Änderung von DNS-Einträgen des Clients, beispielsweise zum Blockieren der Aktualisierungsserver von Antivirensoftware, bei Malware üblich ist. Es kann ferner nicht davon ausgegangen werden, dass auf allen Clients eine aktuelle Antivirensoftware installiert ist, da Mitarbeiter auch eigene Geräte für die Arbeit nutzen können. Die Auswirkungen werden als beträchtlich angesehen, da die Änderung dazu führen kann, dass weitere Schadsoftware den Client befällt und die Schadsoftware im internen Netzwerk verteilt wird. Das Risiko ist deshalb hoch.

Gefährdung: **B10: Nutzung von öffentlichen rekursiven Resolvern**	Beeinträchtigte Grundwerte: Verfügbarkeit, Integrität, Vertraulichkeit	
Eintrittswahrscheinlichkeit: wahrscheinlich	Auswirkungen: beträchtlich	Risiko: **hoch** 

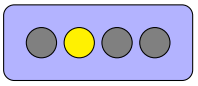
Stub-Resolver im Endsystem

Beschreibung

Diese Bedrohung betrifft vorallem die Stub-Resolver der privaten Endgeräte. Clients können einen öffentlichen rekursiven Resolver konfigurieren. Dieser kann interne Dienste nicht auflösen. DNS-Anfragen können aufgezeichnet und für fremde Zwecke missbraucht werden. Angriffe gegen die Resolver betreffen einen großen Nutzerkreis.

Bewertung

Aufgrund des aktiven Marketings dieser Anbieter, ist es wahrscheinlich, dass einige Clients öffentliche Resolver benutzen. Die Auswirkungen gegen die Verfügbarkeit und Vertraulichkeit werden als begrenzt eingestuft. Die Verfügbarkeit kann schnell wieder hergestellt werden, indem der korrekte Nameserver verwendet wird. Bzgl. der Vertraulichkeit ist anzunehmen, dass die Provider die Transaktionsdaten anonymisieren. Die Auswirkungen gegen die Integrität werden, im Falle eines erfolgreichen Angriffs gegen die rekursiven Resolver, als beträchtlich angesehen. Daher werden die Auswirkungen als beträchtlich eingestuft. Dadurch ergibt sich ein hohes Risiko.

Gefährdung:	Beeinträchtigte Grundwerte:	
B13: Missbrauch von administrativen Berechtigungen	Verfügbarkeit, Integrität, Vertraulichkeit	
Eintrittswahrscheinlichkeit: unwahrscheinlich	Auswirkungen: beträchtlich	Risiko: **mittel** 

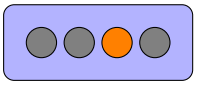
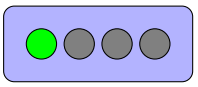
Beschreibung

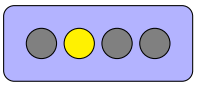
Die zu verwendenden rekursiven Resolver werden an die Clients verteilt. Eine Änderung dieser führt dazu, dass ggf. interne Dienste nicht mehr erreichbar sind. Außerdem kann ein interner Angreifer, die DNS-Daten mitschneiden und verändern, sofern der rekursive Resolver unter seiner Kontrolle steht.

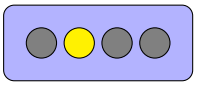
Bewertung

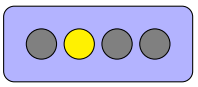
Die Eintrittswahrscheinlichkeit wird als unwahrscheinlich angesehen, da den DNS-Administratoren vertraut wird. Die Auswirkungen werden als beträchtlich eingestuft, da alle Grundwerte bedroht werden. Es ergibt sich ein mittleres Risiko.

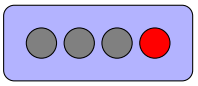
Gefährdung:	Beeinträchtigte Grundwerte:

Stub-Resolver im Endsystem		
B14: DNS als Infil- und Exfiltrationsmedium	Verfügbarkeit, Vertraulichkeit	
Eintrittswahrscheinlichkeit: möglich	Auswirkungen: existenzbedrohend	Risiko: **hoch** 
Beschreibung Ein Angreifer kann den Stub-Resolver dazu missbrauchen, Firewalls zu umgehen und Vertrauliche Daten zu entwenden oder Malware einzuschleusen. Abhängig von der Datenmenge kann die Verfügbarkeit der internen Infrastruktur eingeschränkt werden. **Bewertung** Die Eintrittswahrscheinlichkeit wird als möglich eingestuft, da die DNS-Infrastruktur aktuell nicht im besonderen Maße überwacht wird diese Art von Angriff nicht identifiziert werden kann. Ein Angreifer der vertrauliche personenbezogene Daten stiehlt, hinterlässt einen großen wirtschaftlichen Schaden (Reputation, Bußgelder), daher werden die Auswirkung als existenzbedrohend angesehen. Das Risiko ist daher hoch.		
Gefährdung: **B17: Abhören des DNS-Verkehrs**	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittswahrscheinlichkeit: möglich	Auswirkungen: begrenzt	Risiko: **gering** 
Beschreibung Ein Angreifer kann auf dem Transportweg, entweder zwischen Stub-Resolver und rekursiven Resolver oder zwischen rekursiven Resolver und autoritativen Nameservern, die DNS-Nachrichten abhören. Gleiches gilt bei vorhandenen Zugriff auf die rekursiven Resolver, in den Logs oder an der Netzwerkschnittstelle. **Bewertung**		

Stub-Resolver im Endsystem		
Der DNS-Proxy wird mit geeigneten Berechtigungstrukturen, die mehrmals jährlich überprüft werden, betrieben. Der rekursive Resolver wird vom ISP bereitgestellt. Es ist davon auszugehen, dass der ISP ebenfalls geeignete Schutzmaßnahmen eingeführt hat. Durch Übernahme einer Netzwerkkomponente, wie Router oder Switch, kann ein Angreifer allerdings den Netzwerkverkehr aufgrund der fehlenden Verschlüsselung der DNS-Transaktionen abhören. Die Eintrittswahrscheinlichkeit wird deshalb als möglich angegeben. Die Auswirkungen werden als begrenzt klassifiziert, da der Angreifer die DNS-Transaktionen zwar lesen kann, um Rückschlüsse über die Kommunikationspartner zu ziehen, die weitere Kommunikation allerdings verschlüsselt, und somit für den Angreifer nicht abhörbar, abläuft.		
Gefährdung: **B22: Man-in-the-Middle**	Beeinträchtigte Grundwerte: Verfügbarkeit, Integrität, Vertraulichkeit	
Eintrittswahrscheinlichkeit: möglich	Auswirkungen: beträchtlich	Risiko: **mittel** 
Beschreibung Ein Angreifer kann zwischen Stub-Resolver und rekursiven Resolver die DNS-Transaktionen verändern und somit Clients auf eigene Dienste fehlleiten, sofern dieser Zugriff auf eine, am Datenverkehr beteiligte, Netzwerkkomponente hat. **Bewertung** Da die DNS-Nachrichten nicht signiert oder verschlüsselt werden, kann ein Angreifer die DNS-Daten abfangen und verändern. Die Eintrittswahrscheinlichkeit wird analog der Bedrohung *B17: Abhören des DNS-Verkehrs* als möglich angegeben. Die Auswirkungen werden aufgrund der Bedrohung gegen alle Schutzziele, insbesondere der Integrität der DNS-Daten, als beträchtlich eingestuft. Es ergibt sich ein mittleres Risiko.		
Gefährdung: **27 - DNS-Hijacking**	Beeinträchtigte Grundwerte: Verfügbarkeit, Integrität, Vertraulichkeit	
Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:

Stub-Resolver im Endsystem		
sehr wahrscheinlich	vernachlässigbar	**mittel** 
Beschreibung DNS-Hijacking kann dazu führen, dass interne Dienste nicht mehr aufgelöst oder vertrauliche Daten unbeabsichtigt veröffentlicht werden. **Bewertung** DNS-Hijacking ist bei vielen ISPs üblich. Daher wird die Eintrittswahrscheinlichkeit als sehr wahrscheinlich eingestuft. Die Auswirkungen sind aber vernachlässigbar. Die internen Dienste werden durch den Nameserver NS2 aufgelöst und nur dem Nameserver unbekannte Anfragen an den ISP weitergeleitet. Dadurch sind nur noch die externen Dienste bedroht. Aufgrund der Verbreitung von HTTPS und den Warnhinweisen in modernen Browsern, die bei Verwendung einer unverschlüsselten Verbindung angezeigt werden, sind die Auswirkungen durch unbeabsichtigtes Teilen eines Session-Cookies im Zusammenhang mit DNS-Hijacking gering. Das Risiko wird als mittel eingestuft.		

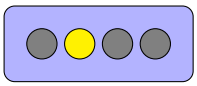
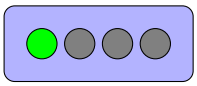
Gefährdung: **B26: DNS-Rebinding**	Beeinträchtigte Grundwerte: Verfügbarkeit, Integrität	
Eintrittswahrscheinlichkeit: unwahrscheinlich	Auswirkungen: beträchtlich	Risiko: **mittel** 
Beschreibung Clients können durch DNS-Rebinding Angriffe als Proxies missbraucht werden, um Angriffe gegen die interne Infrastruktur des Unternehmens durchzuführen. **Bewertung**		

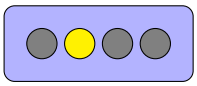
<table>
<tr><td colspan="3">Stub-Resolver im Endsystem</td></tr>
<tr><td colspan="3">QS benutzt den vom ISP angebotenen rekursiven Resolver, der private IP-Adressbereiche in DNS-Antworten filtert. Daher wird die Eintrittswahrscheinlichkeit als unwahrscheinlich eingestuft. Die Auswirkungen werden als beträchtlich eingestuft, da ein Angreifer im Falle eines erfolgreichen Angriffs die komplette interne Infrastruktur bedroht. Es ergibt sich ein mittleres Risiko.</td></tr>
<tr><td>Gefährdung:
B27: Ausfall oder Störung von Dienstleistern</td><td colspan="2">Beeinträchtigte Grundwerte:
Verfügbarkeit</td></tr>
<tr><td>Eintrittswahrscheinlichkeit:
sehr wahrscheinlich</td><td>Auswirkungen:
beträchtlich</td><td>Risiko:
sehr hoch
  </td></tr>
<tr><td colspan="3">Beschreibung
QS hostet lediglich einen DNS-Proxy, der die DNS-Anfragen an den rekursiven Resolver des ISPs weiterleitet.
Bewertung
Die Eintrittswahrscheinlichkeit wird mit sehr wahrscheinlich eingestuft, da mit dem ISP kein Service-Level-Agreement über die Verfügbarkeit des rekursiven Resolvers abgeschlossen wurde. Außerdem gibt es keinen Ausfallschutz durch Anbindung an unterschiedliche ISPs. Die Auswirkungen werden als beträchtlich eingeschätzt, da die Namensauflösung nicht sofort wieder hergestellt werden kann und alle internen Dienste und Benutzer davon betroffen sind. Es ergibt sich ein sehr hohes Risiko.</td></tr>
</table>

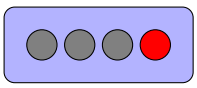
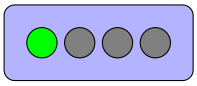
A.1.2 Autoritativer Nameserver

Sofern nicht anders angegeben, beinhaltet NS1 auch immer den sekundären Nameserver NS3, da dieser unter den gleichen Rahmenbedingungen betrieben wird.

Tabelle A.4: Risikoanalyse für den autoritativen Nameserver

Autoritativer Nameserver			
Gefährdung: **B1: Software-Schwachstellen oder -Fehler**		Beeinträchtigte Grundwerte: Verfügbarkeit, Integrität, Vertraulichkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	möglich	beträchtlich	**mittel** 
NS2	unwahrscheinlich	begrenzt	**gering** 
Beschreibung Die autoritativen Nameserver können Schwachstellen beherbergen, die ein Angreifer ausnutzen kann, um die Verfügbarkeit einzuschränken oder DNS-Daten zu verändern oder zu gewinnen. **Bewertung** Die autoritativen Nameserver werden in regelmäßigen Abständen aktualisiert, damit bekanntgewordene Sicherheitslücken geschlossen werden. Dennoch ist nicht auszuschließen, dass NS1 mittels eines Zero-Day-Exploits angegriffen wird. Die Eintrittswahrscheinlichkeit für NS1 wird daher als möglich angesehen. Die Eintrittswahrscheinlichkeit für NS2 ist unwahrscheinlich, da NS2 nur aus dem internen Firmennetzwerk erreichbar ist. Die Schadensauswirkungen für NS1 werden als beträchtlich klassifiziert, da die Dienstleistung den Kunden nicht mehr zur Verfügung steht oder die Kunden Opfer eines Phishing-Angriffs werden können. Die Schadensauswirkungen für NS2 sind begrenzt.			
Gefährdung:		Beeinträchtigte Grundwerte:	

Autoritativer Nameserver			
B2: Datenverlust (hier Verlust der Zoneninformationen)		Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1 & NS2	unwahrscheinlich	beträchtlich	**mittel** 
Beschreibung Datenverlust, insbesondere der Verlust der Zoneninformationen, führt dazu, dass die Namensauflösung nicht mehr durchgeführt werden kann. **Bewertung** Die autoritativen Nameserver werden auf aktueller Hardware mit SSD-Festplatten im Raid 10 Verbund betrieben. Daher ist eine hohe Datenverfügbarkeit gewährleistet. Die Eintrittswahrscheinlichkeit für die Nameserver wird deshalb als unwahrscheinlich eingestuft. Da die Zoneninformationen aktuell nicht zusätzlich durch Backups gesichert werden, würde das Wiederherstellen der Zoneninformationen großen manuellen Aufwand bedeuten. Aufgrund dessen werden die Auswirkungen als beträchtlich klassifiziert. Es ergibt sich ein mittleres Risiko.			

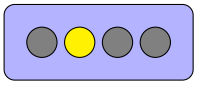
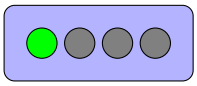
Gefährdung: **B3: Denial-of-Service-Angriffe**		Beeinträchtigte Grundwerte: Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	sehr wahrscheinlich	beträchtlich	**sehr hoch** 
NS2	unwahrscheinlich	begrenzt	**gering** 
Beschreibung			

Autoritativer Nameserver

Die Nameserver können Ziel eines Denial-of-Service-Angriffes werden. Dabei ist insbesondere Nameserver NS1 bedroht, da dieser die Namensauflösung für die Plattform „InsureCloud“ durchführt. Ein Angreifer kann durch diese Angriffe die Namensauflösung beeinflussen und somit die Erreichbarkeit der Plattform für die Kunden einschränken.

Bewertung

Die Eintrittswahrscheinlichkeit für NS1 wird als sehr wahrscheinlich eingestuft, da der Nameserver über das Internet erreichbar ist und die Plattform für Konkurrenten ein lukratives Ziel ist. Hinzu kommt, dass QS aktuell über keine Infrastruktur zur DDoS-Mitigierung verfügt. Die Schadensauswirkungen für NS1 werden als begrenzt eingestuft, da der Nameserver durch den sekundären Nameserver NS3 repliziert wird und dieser als zweiter Nameserver die Namensauflösung durchführen kann. Sofern genügend Anfragen geschickt werden, können jedoch beide Nameserver ausfallen. Deshalb werden die Auswirkungen schlussendlich für NS1 und NS3 als beträchtlich eingeschätzt. Die Eintrittswahrscheinlichkeit für NS2 wird als unwahrscheinlich eingeschätzt, zumal der Nameserver nur aus dem internen Netzwerk erreichbar ist. Die Auswirkungen für NS2 werden als begrenzt eingestuft.

Gefährdung: **B4: Bereitstellung unnötiger Betriebssystemkomponenten und Applikationen**		Beeinträchtigte Grundwerte: Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	unwahrscheinlich	beträchtlich	**mittel** 
NS2	unwahrscheinlich	begrenzt	**gering** 

Beschreibung

Autoritativer Nameserver

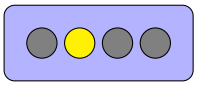
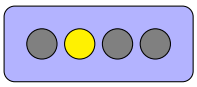
Neben der DNS-Software können weitere Anwendungen oder unnötige Betriebssystemkomponenten betrieben werden, die die Ressourcen des Hosts konsumieren. Dadurch kann die Verfügbarkeit eingeschränkt werden, da der Nameserver nicht über die benötigten Ressourcen allein verfügen kann.

Bewertung

Die Nameserver werden unter Debian 10 „Buster“ LTS (Long Term Support), einer freien Linuxdistribution, betrieben. Als Installationsmedium wurde auf die minimale Netzwerkinstallation zurückgegriffen. Eine Installation von weiteren Paketen kann nur durch die Systemadministratoren erfolgen. Die Server werden von den Administratoren mehrmals im Jahr überprüft und gewartet. Dabei wird unter anderem überflüssige Software entfernt. Die Eintrittswahrscheinlichkeit wird daher als unwahrscheinlich eingeschätzt. Die Auswirkungen für NS1 werden als beträchtlich eingestuft. Die Auswirkungen für NS2 sind begrenzt.

Gefährdung: **B5: Fehlplanung**

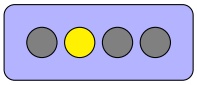
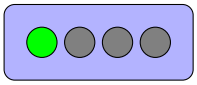
Beeinträchtigte Grundwerte: Verfügbarkeit

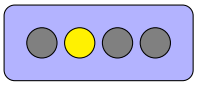
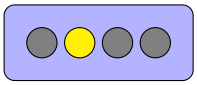
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	unwahrscheinlich	beträchtlich	**mittel** 
NS2	wahrscheinlich	begrenzt	**mittel** 

Beschreibung

Der Einsatz der autoritativen Nameserver muss ausreichend geplant sein. Darunter fällt der Standort sowie die logische Segmentierung im Netzwerk und die Replizierung der Server, damit die Verfügbarkeit stets gewährleistet ist.

Bewertung

Autoritativer Nameserver			
NS1 wird durch NS3 repliziert, allerdings fehlt es an einer Replizierung von NS2. Deshalb ist ein Verlust der Verfügbarkeit für NS2 wahrscheinlich und für NS1 unwahrscheinlich. Die Auswirkungen werden als beträchtlich für NS1 und als begrenzt für NS2 eingeschätzt.			
Gefährdung: **B6: Unbefugter physischer Zugriff**		Beeinträchtigte Grundwerte: Verfügbarkeit, Integrität, Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	unwahrscheinlich	beträchtlich	**mittel** 
NS2	unwahrscheinlich	begrenzt	**gering** 
Beschreibung Die autoritativen Nameserver werden auf physischer Hardware innerhalb des hauseigenen Rechenzentrums betrieben. Die Nameserver können von Unbefugten manipuliert oder entfernt werden. **Bewertung** Das firmeneigene Rechenzentrum wird nach aktuellen Sicherheitsstandards betrieben. Nur Systemadministratoren dürfen, nach vorheriger Anmeldung, gemeinsam mit einem Kollegen das Rechenzentrum betreten, um Wartungsarbeiten durchzuführen. Dabei ist der Zugang rund um die Uhr überwacht. Die Eintrittswahrscheinlichkeit wird daher als unwahrscheinlich eingeschätzt. Die Auswirkungen werden als beträchtlich für NS1 eingeschätzt, da die Verfügbarkeit nicht ohne weiteres wiederhergestellt werden kann. Die Auswirkungen für NS2 werden als begrenzt klassifiziert. Auch hier kann die Verfügbarkeit nicht sofort wiederhergestellt werden.			
Gefährdung: **B7: Malware** (hier Manipulation der Zoneninformationen)		Beeinträchtigte Grundwerte: Integrität, Verfügbarkeit	

Autoritativer Nameserver			
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	unwahrscheinlich	existenzbedrohend	**mittel** 
NS2	unwahrscheinlich	beträchtlich	**mittel** 

Beschreibung

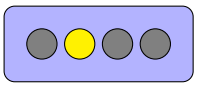
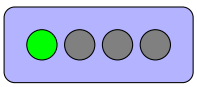
Malware kann die Zoneninformationen der autoritativen Nameserver verändern oder löschen und somit die Verfügbarkeit der Namensauflösung und Integrität der DNS-Daten gefährden.

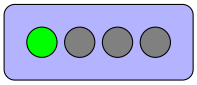
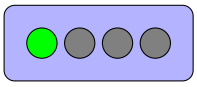
Bewertung

Die Nameserver werden in einem festen Intervall aktualisiert und aktuelle Sicherheitspatches eingespielt. Zusätzliche Software kann nur von den Systemadministratoren mittels Administratorzugang eingespielt werden. Daher wird für die Nameserver die Eintrittswahrscheinlichkeit als unwahrscheinlich eingeschätzt. Die Auswirkungen für NS1 werden als existenzbedrohend eingeschätzt, da der Urzustand nicht sofort wiederhergestellt werden kann. Einerseits aufgrund von fehlender Replizierung und Datensicherung (siehe auch B2: Datenverlust), andererseits weil die veränderten Resource Records in den Caches der rekursiven Resolver und Benutzer gespeichert werden. Die Auswirkungen für NS2 werden als beträchtlich eingeschätzt.

Gefährdung:	Beeinträchtigte Grundwerte:
B8: Fehlende Trennung der Zuständigkeiten	Verfügbarkeit

	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:

Autoritativer Nameserver			
NS1	unwahrscheinlich	beträchtlich	**mittel** 
NS2	unwahrscheinlich	begrenzt	**gering** 
Beschreibung Rekursive Resolver und autoritative Nameserver können überlastet werden, sofern diese auf einem einzigen Host betrieben werden. **Bewertung** NS1, NS3 und NS2 werden auf drei unterschiedlichen Hosts betrieben, auf denen kein zusätzlicher rekursiver Resolver betrieben wird. Daher ist die Eintrittswahrscheinlichkeit für die Nameserver unwahrscheinlich. Da die Auswirkungen primär auf die Verfügbarkeit beschränkt sind, werden diese für NS1 und NS3 als beträchtlich und für NS2 als begrenzt eingeschätzt.			

Gefährdung: **B9: Ausführung mit erweiterten Rechten**		Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	möglich	begrenzt	**gering** 
NS2	möglich	begrenzt	**gering** 

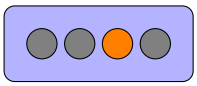
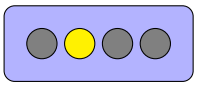
Autoritativer Nameserver

Beschreibung

Die DNS-Serversoftware auf den autoritativen Nameservern kann mit erweiterten Rechten ausgeführt werden. Bei Übernahme des Dienstes (durch Schwachstellen, siehe Bedrohung B1) kann ein Angreifer die erweiterten Rechte ausnutzen, um das komplette System zu übernehmen oder weitere Hintertüren einzubauen.

Bewertung

Die Dienste werden mit einem extra Benutzer und Gruppe *named* ausgeführt. Der Benutzer besitzt keine privilegierten Berechtigungen. Eine nachträgliche unbeabsichtigte Änderung der Konfiguration wird als möglich eingeschätzt. Da das Ausführen eines DNS-Servers mit erweiterten Rechten nicht sofort zum Verlust der Grundwerte führt, sondern die Bedrohung auch darauf setzt, dass Schwachstellen in der DNS-Software ausgenutzt werden (siehe B1: Software-Schwachstellen oder -Fehler), werden die Schadenauswirkungen für die Nameserver als begrenzt eingeschätzt.

Gefährdung:		Beeinträchtigte Grundwerte:	
B11: Fehler in den Konfigurationsdateien (hier Fehler in den Zoneninformationen)		Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	wahrscheinlich	beträchtlich	**hoch** 
NS2	wahrscheinlich	begrenzt	**mittel** 

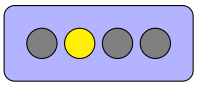
Beschreibung

Fehler in den Zonendateien können dazu führen, dass einzelne Hosts nicht mehr korrekt aufgelöst werden.

Bewertung

Autoritativer Nameserver

Es gibt das Programm *named-checkconf* (mitgeliefert in der BIND-Installation), dass die Syntax der Konfigurationsdatei überprüft und von den DNS-Administratoren genutzt wird, allerdings werden falsche Zuordnungen in den Zonendateien dadurch nicht erkannt. Die Eintrittswahrscheinlichkeit für Fehler in den Zoneninformationen werden daher als wahrscheinlich klassifiziert. Die Schadensauswirkung für NS1 wird als beträchtlich eingeschätzt, da die Verfügbarkeit zwar durch Beseitigung der Fehler auf Seiten von QS schnell wiederhergestellt werden kann, jedoch das Caching der rekursiven Resolver die Verfügbarkeit für längere Zeit beeinträchtigen kann. Da das Caching der rekursiven Resolver für NS2 keine Rolle spielt, werden die Schadenauswirkungen als begrenzt eingeschätzt.

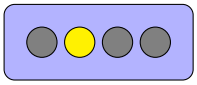
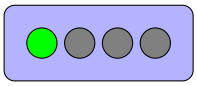
Gefährdung: **B12: Fehlende organisatorische Abläufe** (hier Kontaktinformationen beim Provider)		Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	unwahrscheinlich	existenzbedrohend	**mittel** 

Beschreibung

Die zuständigen autoritativen Nameserver für die Domains des Unternehmens werden bei einem Registrar hinterlegt. Eine Änderung der IP-Adressen führt dazu, dass die Namensauflösung nicht mehr durchgeführt werden kann. Sollte ein Angreifer einen eigenen Nameserver hinterlegen, so kann er die DNS-Daten verändern und somit die Opfer fehlleiten.

Bewertung

Autoritativer Nameserver
Die Domain wurde bei einem Registrar mittels einer eigens dafür angelegten E-Mail-Adresse *domain@quality-software.de* registriert. Diese E-Mail-Adresse ist keiner natürlichen Person zugeordnet sondern wird von allen DNS-Administratoren gemeinsam verwaltet. Die Kontaktdaten beim Registrar sind generisch und keiner natürlichen Person zugeordnet. Der Zugang zum Verwaltungsportal ist durch einen zweiten Faktor, einem USB-Sicherheitsschlüssel, abgesichert. Zusätzlich wird den DNS-Administratoren grundsätzlich vertraut. Die Eintrittswahrscheinlichkeit wird aufgrund dessen als unwahrscheinlich eingeschätzt. Die Schadensauswirkung werden als existenzbedrohend eingestuft, da die Wiederherstellung auf die korrekten Nameserver einerseits durch das Caching, andererseits durch den Prozess der Domain-Propagation beeinflusst werden und im schlimmsten Fall mehrere Tage dauern kann.

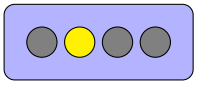
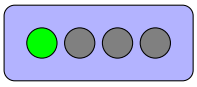
Gefährdung: **B13: Unzureichendes Berechtigungskonzept**		Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	unwahrscheinlich	beträchtlich	**mittel** 
NS2	unwahrscheinlich	begrenzt	**gering** 

Beschreibung

Eine fehlendes oder unzureichendes Berechtigungskonzept kann dazu führen, dass unbefugte Benutzer Zugriff auf die autoritativen Nameserver bekommen. Dort können von diesen Benutzern, beabsichtigt oder unbeabsichtigt, Zoneninformationen geändert oder gelöscht werden.

Bewertung

Autoritativer Nameserver
Nur die DNS-Administratoren haben Zugriff auf die autoritativen Nameserver. Der Zugriff ist nur mittels Public-Key-Authentifizierung und Passwort möglich. Die gespeicherten öffentlichen Schlüssel auf den Servern werden in regelmäßigen Abständen überprüft. Die Eintrittswahrscheinlichkeit wird daher als unwahrscheinlich eingeschätzt. Die Auswirkungen für NS1 sind beträchtlich und für NS2 begrenzt.

Gefährdung: **B14: Missbrauch von administrativen Berechtigungen**		Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	unwahrscheinlich	beträchtlich	**mittel** 
NS2	unwahrscheinlich	begrenzt	**gering** 

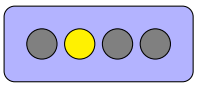
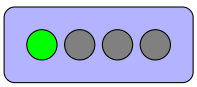
Beschreibung

DNS-Administratoren können ihre Berechtigungen missbrauchen, um Zoneninformationen auf den autoritativen Nameservern zu ändern.

Bewertung

Da den DNS-Administratoren grundsätzlich vertraut wird, wird die Eintrittswahrscheinlichkeit mit unwahrscheinlich eingeschätzt. Die Auswirkungen für NS1 sind beträchtlich und für NS2 begrenzt.

Gefährdung: **B16: Fingerprinting**		Beeinträchtigte Grundwerte: Vertraulichkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:

Autoritativer Nameserver			
NS1	wahrscheinlich	begrenzt	**mittel** 
NS2	unwahrscheinlich	vernachlässigbar	**gering** 

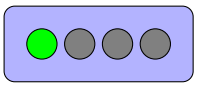
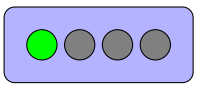
Beschreibung

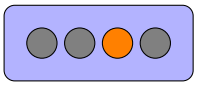
Die autoritativen Nameserver können von einem Angreifer durch gezieltes Abfragen missbraucht werden, um weitere Informationen über das Netzwerk und die verfügbaren Dienste zu gewinnen. Liefern die autoritativen Nameserver genug Informationen über den DNS-Dienst selbst zurück, kann ein Angreifer mittels dieser Informationen geeignete Schwachstellen ausfindig machen und ausnutzen (vgl. B1: Software-Schwachstellen oder -Fehler).

Bewertung

Die Versionsinformationen der Nameserver wurden in der bind-Konfigurationsdatei *named.conf* durch *Not supported* ersetzt. Wildcard-Queries sind erlaubt, dadurch entsteht zusätzlich das Risiko, dass der autoritativen Nameserver NS1 für einen DNS-Amplification-Angriff missbraucht wird. Die Eintrittswahrscheinlichkeit für NS1 wird als wahrscheinlich eingeschätzt, da diese Angriffe von Angreifern automatisiert durchgeführt werden und NS1 deshalb auch nur zufällig zum Ziel werden kann. Die Eintrittswahrscheinlichkeit für NS2 wird als unwahrscheinlich eingeschätzt. Die Schadensauswirkung für NS1 ist begrenzt und für NS2 vernachlässigbar.

Gefährdung:		Beeinträchtigte Grundwerte:	
B17: Abhören des DNS-Verkehrs		Vertraulichkeit	
hier			
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:

Autoritativer Nameserver			
NS1	unwahrscheinlich	begrenzt	**gering** 
NS2	unwahrscheinlich	begrenzt	**gering** 
Beschreibung Die Kommunikation zwischen den autoritativen Nameservern und den Endnutzern (rekursiver Resolver, Full-Resolver) kann durch einen Angreifer abgehört werden. Entweder durch Zugriff auf die autoritativen Nameserver oder durch Zugriff auf eine Netzwerkkomponente, die am Datenverkehr beteiligt ist. **Bewertung** Die autoritativen Nameserver und Komponenten sind gegen unbeabsichtigten physischen Zugriff ausreichend abgesichert. Die Eintrittswahrscheinlichkeit wird daher als unwahrscheinlich eingeschätzt. Die Auswirkungen werden jeweils als begrenzt betrachtet.			

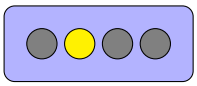
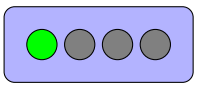
Gefährdung: **B18: Social Engineering** hier Übernahme des autoritativen NS		Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	möglich	existenzbedrohend	**hoch** 
Beschreibung Die IP-Adresse des autoritativen Nameservers NS1, der beim Registrar für die Domain des Unternehmens angegeben ist, kann durch Social Engineering-Angriffe eines Angreifers verändert werden.			

Autoritativer Nameserver

Bewertung

Das Unternehmen hat bereits einige Sicherheitsmaßnahmen umgesetzt, um den Zugriff zum Verwaltungsportal der Domain einzuschränken, wie beispielsweise der Einsatz eines zweiten Faktors. Allerdings sind die Sicherheitsmaßnahmen nur so gut wie das schwächste Glied in der Kette von Sicherheitsmaßnahmen. Eine Veränderung des autoritativen Nameservers wird als möglich angesehen, da Social Engineering-Angriffe gegen Domain-Registraren schon oft vorgekommen sind. Die Auswirkungen sind existenzbedrohend, da erstens alle Schutzgüter bedroht sind und zweitens das Caching der rekursiven Resolver sowie die Domain-Propagation eine sofortige Wiederherstellung des alten Nameservers verzögert. Hinzu kommt, dass der Angreifer nach einem erfolgreichen Angriff den Zugang für QS sperren kann, beispielsweise durch Veränderung der Kontaktdaten, so dass eine Wiederherstellung des Urzustands noch weiter verzögert wird.

Gefährdung:	Beeinträchtigte Grundwerte:
B22: Man-in-the-Middle (hier MitM zwischen Endnutzer und autoritativen Nameserver)	Vertraulichkeit, Integrität, Verfügbarkeit

	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	unwahrscheinlich	existenzbedrohend	**mittel** 
NS2	unwahrscheinlich	begrenzt	**gering** 

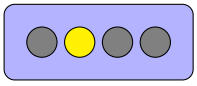
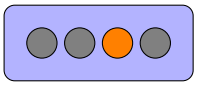
Beschreibung

Sofern der Angreifer die Möglichkeit hat die Kommunikation zwischen autoritativen Nameservers und Endnutzer (rekursiver Resolver, Full-Resolver) abzufangen, so kann er die DNS-Nachrichten verändern und den Benutzer somit auf andere Dienste fehlleiten.

Bewertung

Autoritativer Nameserver

Die autoritativen Nameserver werden in einem Rechenzentrum mit aktuellen Sicherheitsstandards und Zugriffskontrollen betrieben. Daher wird die Eintrittswahrscheinlichkeit zur Übernahme einer Netzwerkkomponente auf Seiten von QS als unwahrscheinlich angesehen. Die Auswirkungen für NS2 werden als begrenzt und für NS1 als existenzbedrohend eingeschätzt.

Gefährdung: **B24: Zone Poisoning mittels Zonentransfers**		Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS1	möglich	beträchtlich	**mittel** 
NS3	möglich	existenzbedrohend	**hoch** 

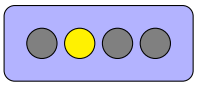
Beschreibung

Zonentransfers können genutzt werden, um den autoritativen Nameserver NS1 zu überlasten oder Zoneninformationen auf dem sekundären Nameserver NS3 zu verändern. Diese Bedrohung betrifft den Nameserver NS2 nicht, da dort kein Zonentransfer stattfindet.

Bewertung

Autoritativer Nameserver

Lediglich der sekundäre Nameserver NS3 wurde in der Konfigurationsdatei des Nameservers NS1 als erlaubtes Ziel des Zonentransfers hinterlegt (allow-transfer). Da dort aber nur die IP-Adressen hinterlegt wird, kann ein Angreifer die IP-Adresse des sekundären Nameservers fälschen und somit den Zonentransfer anstoßen. Die Eintrittswahrscheinlichkeit wird auf möglich geschätzt. Sofern der Angreifer Zugriff auf Netzwerkkomponenten zwischen den beiden Nameservern hat, so kann dieser die Zoneninformationen für NS3 abfangen und verändern. Das wird allerdings von QS als unwahrscheinlich eingeschätzt, da die Komponenten ausreichend abgesichert sind. Die Auswirkungen für den Nameserver NS1 wird als beträchtlich und für den Nameserver NS3 als existenzbedrohend eingeschätzt.

Gefährdung: **B25: Zone Poisoning mittels dynamischer Updates**		Beeinträchtigte Grundwerte: Integrität, Verfügbarkeit	
	Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
NS2	möglich	beträchtlich	**mittel** 

Beschreibung

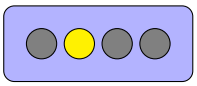
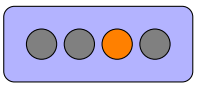
Im internen Firmennetzwerk werden dynamische Updates benutzt, damit ein Client auch bei wechselnder IP-Adresse immer über seinen FQDN erreichbar ist. Dynamische Updates können von einem internen Angreifer missbraucht werden um den autoritativen Nameserver zu überlasten oder die Namensauflösung durch falsche Zuordnung zu einem Client einzuschränken.

Bewertung

Dynamische Updates sind durch den autoritativen Nameserver NS2 auf eine IP-Adresse in der Konfigurationsdatei begrenzt worden. Lediglich UPDATE-Nachrichten des DHCP-Servers werden vom Nameserver bearbeitet. Da es im internen Netzwerk jedoch keine Erkennung von IP-Spoofing gibt, kann ein interner Angreifer die IP-Adresse des DHCP-Servers fälschen und somit valide UPDATE-Nachrichten verschicken. Die Eintrittswahrscheinlichkeit wird als möglich eingeschätzt, da für diese Art von Angriff tieferes Verständnis über die Netzwerkinfrastruktur sowie DNS von Nöten ist. Die Schadensauswirkungen werden als beträchtlich klassifiziert.

A.1.3 Domain

Tabelle A.5: Risikoanalyse für die Domain

Domain		
Gefährdung: B12: Fehlende organisatorische Abläufe (hier Verlust der Domain)	Beeinträchtigte Grundwerte: Integrität, Verfügbarkeit	
Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
unwahrscheinlich	existenzbedrohend	**mittel** 
Beschreibung Die Domains wurden bei einem Domain-Registrar registriert. Sofern versäumt wird, die Domains rechtzeitig zu verlängern, können diese von Dritten erworben und genutzt werden. **Bewertung** Die Eintrittswahrscheinlichkeit wird analog der Bedrohung B12: Fehlende organisatorische Abläufe der autoritativen Nameserver als unwahrscheinlich eingeschätzt, da bereits gute Sicherheitsmaßnahmen umgesetzt worden sind. Aufgrund der Wichtigkeit bezogen auf das Image und der Wirtschaftlichkeit des Unternehmens werden die Auswirkung als existenzbedrohend eingestuft. Es ergibt sich ein mittleres Risiko.		
Gefährdung: B18: Social Engineering (hier Übernahme der Domain)	Beeinträchtigte Grundwerte: Integrität, Verfügbarkeit	
Eintrittswahrscheinlichkeit:	Auswirkungen:	Risiko:
möglich	existenzbedrohend	**hoch** 
Beschreibung Ein Angreifer kann mittels Social Engineering die Domains *quality-software.de* oder *qs.de* transferieren oder Zugang zum Verwaltungsportal der Domains bekommen. **Bewertung**		

Domian
Es wurden bereits einige Sicherheitsmaßnahmen umgesetzt, um den Zugang zum Verwaltungsportal abzusichern. Allerdings können diese von einem Helpdesk-Mitarbeiter leicht außer Kraft gesetzt werden. Aktuell werden von QS keine weiteren Maßnahmen zum Schutz der Domain, wie beispielsweise Registrar Locks, eingesetzt. Ein erfolgreicher Social Engineering-Angriff könnte somit den Verlust der Domain bedeuten. Die Eintrittswahrscheinlichkeit wird daher als möglich beschrieben. Die Schadenauswirkungen werden als existenzbedrohend angesehen. Es ergibt sich ein hohes Risiko.

Beeinträchtigter Grundwert	**Beschreibung**	**minimale Schadens-auswirkung**
Vertraulichkeit	Die DNS-Transaktionen können von einem Angreifer missbraucht werden, um Rückschlüsse über die verschiedenen Benutzer der Plattform zu gewinnen. Diese Daten können auch genutzt werden, um weitere Angriffsziele zu finden oder die Aktivitäten der Benutzer vorauszusagen.	begrenzt
Integrität	Eine Gefährdung der Integrität der DNS-Daten kann dazu führen, dass die Benutzer der Plattform fehlgeleitet und Opfer eines Phishing-Angriffs werden. Dadurch können sensible personenbezogene Daten sowie Gesundheitsdaten der Kunden gestohlen werden. Aufgrund des Cachings der rekursiven Resolver können die Benutzer, auch Stunden nachdem der Urzustand wiederhergestellt worden ist, noch fehlgeleitet werden. Außerdem ist indirekt die Verfügbarkeit bedroht.	beträchtlich
Verfügbarkeit	Wird die Verfügbarkeit der Namensauflösung eingeschränkt, so ist die Plattform „InsureCloud“ ggf. nur noch sporadisch oder gar nicht mehr erreichbar. Zwischen QS und den Versicherungsgesellschaften besteht ein Service-Level-Agreement, dass die Plattform zu 99,9% in den produktiven Arbeitszeiten der Gesellschaften zur Verfügung stehen muss. Ein ungeplanter Ausfall kann zu wirtschaftlichen Schäden und Reputationsverlust führen. Für das interne Firmennetzwerk bedeutet ein Ausfall der Namensauflösung, dass unter anderem die Verfügbarkeit des E-Mail-Verkehrs eingeschränkt ist.	beträchtlich

Tabelle A.2: Minimale Schadensauswirkungen für die autoritativen Nameserver NS1 und NS3

Beeinträchtigter Grundwert	**Beschreibung**	**minimale Schadens-auswirkung**
Vertraulichkeit	Über die DNS-Transaktionen können die genutzten Dienste und Webseiten der Mitarbeiter ausspioniert werden, um diese zu überwachen oder weitere Angriffe zu planen. Die Verletzung der Privatsphäre wird dabei besonders kritisch von QS betrachtet.	begrenzt
Integrität	Durch eine Veränderung der DNS-Nachrichten können die Mitarbeiter auf fremde Hosts fehlgeleitet und dort Opfer eines Phishing-Angriffs werden. Dadurch können Angreifer beispielsweise vertrauliche Zugangsdaten abfangen und missbrauchen. Aber auch das Einschleusen von Malware ist möglich.	beträchtlich
Verfügbarkeit	Verlust der Verfügbarkeit führt zu dazu, dass interne Dienste, wie beispielsweise der Verzeichnisdienst Microsoft Active Directory oder Entwicklungswerkzeuge (Versionsverwaltung, Wissensmanagementsoftware, Projektmanagementsoftware) nicht mehr aufgelöst werden können. Da jede DNS-Anfrage an den Nameserver geschickt wird und dieser die Anfrage an den rekursiven Resolver des ISPs weiterleitet, ist auch die externe Namensauflösung gestört.	begrenzt

Tabelle A.3: Minimale Schadensauswirkungen für den autoritativen Nameserver NS2

Glossar

Anycast Adressierungsart in Computernetzwerken, bei der mehrere Computer dieselbe IP-Adresse besitzen. Durch das Border Gateway Protocol (BGP) wird das Paket im Internet zum geografisch nächsten Computer geroutet.

Botnet Verbund von infizierten Geräten, wie Computer oder IoT-Geräten, die für Angriffe genutzt werden können.

Buffer Overflow Ein Pufferüberlauf entsteht, wenn einem Speicherbereich mehr Daten zugefügt werden, als dieser reserviert oder noch zur Verfügung hat. Dadurch werden andere Speicherbereiche überschrieben.

Container Anwendungen, die in einer isolierten Laufzeitumgebung, ausgeführt werden. Dabei besitzt der Container, im Unterschied zur Virtualisierung, kein eigenes Betriebssystem, sondern teilt sich das Betriebssystem mit dem Host.

Demilitarisierte Zone Internes Computernetzwerk, das vom Internet aus erreichbar ist. Dadurch besitzen die Systeme in dem Netzwerk einen besonderen Schutzbedarf.

Magic String Zeichenkette, die als Erkennungsmerkmal genutzt wird und nicht als Eingabe erwartet wird.

Malware Bösartige Software, die unerwünschte Operationen ausführt und dem Opfer ggf. Schaden zufügt.

Portable Operating System Interface Standard von Betriebssystem-Schnittstellen auf Unix-Betriebssystemen.

Privilege Escalation Unbefugte Erhöhung der Rechte und Privilegien von Anwendungen und Benutzern.

Remote-Code-Ausführung Ausnutzung von Sicherheitslücken, um unautorisierten und bösartigen Code auszuführen.

Request for Comments Veröffentlichungen mit dem Ziel, Internetstandards zu entwickeln oder über diese zu informieren.

Time to Live Beschreibt eine Lebensdauer oder einen Gültigkeitsrahmen von Daten. Beispielweise wird die Gültigkeit von Resource Records anhand einer Time to Live definiert.

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Gemäß der Allgemeinen Prüfungs- und Studienordnung ist zusammen mit der Abschlussarbeit eine schriftliche Erklärung abzugeben, in der der Studierende bestätigt, dass die Abschlussarbeit „— bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit [(§ 18 Abs. 1 APSO-TI-BM bzw. § 21 Abs. 1 APSO-INGI)] — ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt wurden. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich zu machen."

Quelle: § 16 Abs. 5 APSO-TI-BM bzw. § 15 Abs. 6 APSO-INGI

Erklärung zur selbstständigen Bearbeitung der Arbeit

Hiermit versichere ich,

Name: _____

Vorname: _____

dass ich die vorliegende Bachelorarbeit – bzw. bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit – mit dem Thema:

DNS-Sicherheit am Beispiel eines mittelständischen Softwareunternehmens

ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

_____	_____	_____
Ort	Datum	Unterschrift im Original