Safuat Hamdy

Sicherheitsherausforderungen von IPv6

Der begrenzte Adressraum des IPv4-Protokolls wird in Bälde zum Umstieg und zur Einführung von IPv6 zwingen. Wer nicht in wenigen Jahren den Anschluss an das Internet verlieren möchte, sollte sich daher ernsthaft mit IPv6 auseinandersetzen, denn IPv6 ist mehr als ein „IPv4 mit längeren Adressen". Zahlreiche Architekturmerkmale von IPv6 bergen auch neue Sicherheitsrisiken, denen Netzwerkadministratoren durch entsprechende Konfigurationen begegnen sollten. Der Beitrag gibt einen Überblick über die wichtigsten Fallstricke.

1 Eine Frage der Zeit

Die Aufgabe des Internet-Protokolls (IP) besteht im Wesentlichen darin, Datenpakete von einem System über verschiedene Netzwerke hinweg zu einem Zielsystem zu vermitteln. Diese Vermittlung erfolgt anhand von IP-Adressen. Ohne eine gültige IP-Adresse kann ein System nicht am Internet teilnehmen.

Die Vergabe von IP-Adressen an sogenannte End-Sites erfolgt über Local Internet Registrys (LIRs), wobei es sich hierbei typischerweise um Internet Service Provider (ISP) handelt. Die LIRs weisen ihren Kunden Adressen oder Adressbereiche aus den Adressblöcken zu, die sie ihrerseits von Regional Internet Registrys (RIRs) erhalten. Für Europa ist dies beispielsweise RIPE NCC. Die RIRs erhalten Ihre Zuweisungen wiederum von der Internet Assigned Numbers Authority (IANA).

Benötigt ein Kunde mehr Adressen, als das LIR zur Verfügung stellen kann, dann fragt das LIR bei seinem zuständigen RIR nach einer weiteren Zuweisung. Sind auch die Pools des RIRs erschöpft, dann fragt das entsprechende RIR bei IANA – dem Grundgedanken nach – nach einem weiteren Adressblock.

Mit der Aufzehrung des IANA-Pools für IP-Adressen im Jahr 2012, in welchem IANA ihren letzten /8-Block vergeben hat, naht das Ende des IPv4-Protokolls. Zwar verfügen die RIRs noch über freie Adressblöcke, jedoch werden auch diese in absehbarer Zeit aufgebraucht sein.

Als grundsätzliche Antwort auf die sich abzeichnende Adressknappheit wurde IPv6 entwickelt. Seit etwa 2011 hat sich die Entwicklung von IPv6 soweit stabilisiert, dass nach allgemeinem Ermessen IPv6 bereit für den produktiven Einsatz ist. Da der Zeitpunkt akuter Adressknappheit absehbar naht, stellt sich nicht mehr die Frage, *ob* IPv6 eingeführt wird oder nicht, sondern *wann*.

Zwar sind verschiedene Vorgehensweisen denkbar, um beispielsweise ungenutzte Adressen oder Adressblöcke wieder einzuziehen und neu zu vergeben, dabei ergeben sich jedoch verschiedene verwickelte Probleme, deren Details für die weitere Diskussion in diesem Beitrag nicht von Belang sind. Zudem würde eine Einführung von IPv6 damit nur verzögert und verteuert, aber nicht vermieden – bei einer wachsenden Anzahl von Nutzern mit einer wachsenden Anzahl von Endgeräten, die alle vernetzt werden sollen, wären diese Maßnahmen kaum mehr als der sprichwörtliche Tropfen auf dem heißen Stein.

Aktuelle Versionen gängiger Betriebssysteme haben IPv6 bereits aktiviert. Zwar haben zahlreiche Organisationen noch Windows XP im Einsatz; hier kann IPv6 im Wesentlichen durch Ignorieren ausgewichen werden. Jedoch läuft der Support für Windows XP im kommenden Jahr aus; ein Umstieg auf modernere Betriebssystemversionen ist spätestens dann unumgänglich und führt also zwangsläufig dazu, dass die IT-Verantwortlichen eben doch mit IPv6 konfrontiert werden.

IPv6 ist nicht kompatibel zu IPv4. Eine Umstellung zieht daher einen vergleichbaren Aufwand nach sich, wie beispielsweise eine Umstieg von Windows XP auf Windows 7, und daher verläuft die Einführung von IPv6 in Unternehmen bisher eher zurückhaltend. Es lässt sich aber mittlerweile eine gewisse Bewegung feststellen. So bieten verschiedene ISP auch schon ihren Endkunden IPv6 an, und populäre Inhalte stehen teilweise bereits über IPv6 zur Verfügung.

Für die Einführung von IPv6 ist kein globaler Stichtag vorgesehen, es ist aber absehbar, dass die Einführung von IPv6 eher lawinenartig erfolgen wird. Die Forderung nach IPv6 für eine Anwendung könnte beispielsweise die Umstellung auf IPv6 an zahlreichen anderen Stellen nach sich ziehen.

Die Auseinandersetzung mit IPv6 wird auch für Unternehmen nunmehr unausweichlich. Wer in wenigen Jahren noch über das Internet erreichbar sein möchte, tut gut daran, sich kurzfristig eingehend mit IPv6 zu beschäftigen. Die Einführung von IPv6 erfordert einige Planung und eine gewisse Kenntnis. Da IPv6 zu den grundlegenden Infrastrukturkomponenten des Internets gehört, wird es von der Voraussicht und der Professionalität des jeweiligen Managements abhängen, ob die Einführung von IPv6 zur Sternstunde des IT-Betriebs oder zur Klippe am Abgrund wird.

IPv6 bietet nicht nur einen größeren Adressraum als IPv4, sondern berücksichtigt auch die Erfahrungen, die mit IPv4 gemacht wurden. Daraus entstand eine Architektur, die sich an verschiedenen Punkten deutlich von der IPv4-Architektur unterscheidet. Es wäre daher fahrlässig, IPv6 lediglich als IPv4 mit längeren Adressen zu betrachten. IPv6 enthält fraglos zahlreiche Verbesserungen im Vergleich zu IPv4, die aber nur dann zum Tragen kommen, wenn man sich auf IPv6 einlässt. Gleichzeitig wurde das Protokoll aber auch komplexer.

Dr. Safuat Hamdy

ist Security Consultant bei der Secorvo Security Consulting GmbH. Schwerpunkte: Sicherheits- und Webanwendungsaudits, sichere Softwareentwicklung und forensische Analysen.
E-Mail: safuat.hamdy@secorvo.de

Ziel dieses Beitrags ist die Vorstellung der sicherheitstechnischen Stolpersteine und Fußangeln, mit denen sich der IT-Betrieb bei der Einführung von IPv6 konfrontiert sieht. Die Beschreibung erfolgt im Wesentlichen ohne Angabe von technischen Details, da dies eine nähere Kenntnis von IPv6 erfordert, die hier nicht vorausgesetzt wird. Eine recht detaillierte Darstellung ist in [Hamdy_2013] zu finden, die technischen Einzelheiten sind beispielsweise in [Hagen_2009] nachzulesen.

Sicherheit bei IPv6 wird gern mit IPsec in Verbindung gebracht. Tatsächlich galt IPsec lange Zeit als das Hauptsicherheitsmerkmal von IPv6 und war zunächst für jede IPv6-Implementierung obligatorisch. Diese Anforderung wurde jedoch fallengelassen, da sich dies beispielsweise für die Micro-Controller in integrierten Steuersystemen nicht oder nur mit hohem Aufwand umsetzen lässt. Zudem ist IPsec nicht in der Lage, alle ihm zugedachten Aufgaben zu erfüllen oder die Protokollschwächen zu kompensieren, die IPv6 enthält.

Im Folgenden wird zunächst auf einige Aspekte von IPsec eingegangen, weil diese – der Idee nach – bei der Absicherung etwa der sogenannten Neighbor Discovery spielen. Dabei stellte sich frühzeitig heraus, dass das in der angedachten Form nicht machbar ist. Mithin ist noch offen, welchen Platz IPsec in der Sicherheitsarchitektur des Internets spielen wird.

2 IPsec

Bei der Nutzung von IP ergeben sich je nach Einsatzszenario verschiedene Schutzziele und daraus folgende Bedrohungen. Den spezifischen Bedrohungen kann an verschiedenen Stellen begegnet werden. Ist beispielsweise die Vertraulichkeit einer Datenübertragung gefordert, dann kann dies entweder auf der Ebene von IP mittels IPsec erfolgen oder auch auf Ebene der Anwendung.

IPsec beschreibt eine Reihe von Funktionen zur *kryptografischen* Absicherung des Netzwerkverkehrs auf Ebene von IP. Ursprünglich wurde IPsec im Zuge von IPv6 entwickelt, jedoch wurde IPsec frühzeitig nach IPv4 zurückportiert. Wie bei allen kryptografischen Protokollen liegt eine der Hauptschwierigkeiten bei IPsec in der *vertrauenswürdigen Schlüsselverteilung*.

Der Aufbau eines durch IPsec gesicherten Kanals erfolgt nach denselben Prinzipien, wie etwa für SSL/TLS [Esslinger_97], zunächst werden im sogenannten Handshake Parameter und Algorithmen ausgehandelt und Schlüssel festgelegt, anschließend wird der sichere Kanal gemäß Aushandlung etabliert. Anders als bei SSL/TLS kann auf den Handshake verzichtet werden, wenn die relevanten Parameter und Schlüssel manuell konfiguriert werden. Dies skaliert jedoch nicht und ist daher in den meisten Szenarien unpraktikabel.

IPsec wird typischerweise zum Betrieb von sogenannten virtuellen privaten Netzen (VPN) genutzt. Der Schlüsselaustausch erfolgt über Zertifikate, die ihrerseits manuell oder über eine Public-Key-Infrastruktur (PKI) verteilt werden.

Neben der grundsätzlichen Herausforderung einer vertrauenswürdigen Schlüsselverteilung weist IPsec eine weitere wichtige Einschränkung auf: IPsec kann – ebenfalls prinzipbedingt – nicht gut zur Absicherung von Multicast-Verkehr genutzt werden. Wichtige Mechanismen, wie die Neighbor Discovery (s. u.), setzen teilweise aber Multicast ein, so dass hier eine Diskrepanz besteht zwischen dem Anspruch, den IPsec erfüllen soll, und den konkreten Anforderungen.

3 Neighbor Discovery

Mit IPv6 wurden sämtliche relevanten Steuerprotokolle unter ICMPv6 vereinigt. Ein wichtiges Steuerprotokoll ist die sogenannte Neighbor Discovery (ND), die einige kritische Funktionen erfüllt. Die ND ist u. a. dafür zuständig, in einem LAN IPv6-Adressen in physische Adressen zu übersetzen; diese Aufgabe lag unter IPv4 beim Adress Resolution Protocol (ARP). Andere wichtige Aufgaben der ND sind beispielsweise die Erkennung von Adresskollisionen bei der Konfiguration von Netzwerkinterfaces (Duplicate Address Detection, DAD) sowie in der Bestätigung der Erreichbarkeit von Systemen im LAN (Neighbor Unreachability Detection, NUD).

Eine andere wichtige Teilaufgabe der Neighbor Discovery besteht in der Router Discovery (RD), mit der ein Router verschiedene Netzwerkparameter an die am LAN angeschlossenen Systeme verteilt. Zu diesen Parametern gehören die sogenannten Präfixe, dies sind die oberen (linken) 64 Bits einer IPv6-Adresse.

Sind die Router korrekt implementiert, dann ist die ND vor Angriffen aus anderen Netzen im Wesentlichen geschützt. Wenn der Angreifer jedoch Zugang zum LAN hat, dann sind die folgenden Angriffe auf die ND möglich:

- Ein Angreifer kann benachbarte Systeme mit ND-Nachrichten (und anderen ICMPv6-Nachrichten) fluten. Dadurch könnte die Netzwerkbandbreite oder die Rechenleistung der angegriffenen Systeme ausgelastet werden. Durch fehlerhafte Implementierungen kann es sogar zu Abstürzen kommen. Wenn die Implementierung beispielsweise nicht die Anzahl der Einträge im sogenannten Neighbor Cache begrenzt, kann durch einen einfach durchzuführenden Angriff der Betriebssystemspeicher komplett belegt werden.
- Eine spezielle Variante des vorangegangenen Punkts, die auch aus anderen Netzen leicht durchgeführt werden kann, besteht in der Anfrage nach Systemen mit nicht existierenden Adressen, beispielsweise durch Aufzählung eines Netzwerks mit einem Portscanner. Der Router, der für das entsprechende Präfix zuständig ist, muss die entsprechenden ND-Nachrichten versenden und auf die dazu gehörigen ND-Antworten warten. Bei einer Flutung mit Anfragen nach nicht existieren Adressen könnte der dafür vorgesehene Speicher komplett belegt werden, so dass legitime Anfragen nach bestehenden Systemen nicht mehr verarbeitet werden können.
- Ein Angreifer kann gefälschte RD-Nachrichten verschicken. Zum Zweck eines Man-in-the-Middle-Angriffs kann der Angreifer sein eigenes System zum bevorzugten Router für ein oder mehrere bestehende Präfixe erklären. Zur Durchführung eines Denial-of-Service-Angriffs könnte ein nicht existierendes System zum Router erklärt werden.
- Ein Angreifer kann zum Zweck eines Denial-of-Service-Angriffs über gefälschte RD-Nachrichten bestehende Präfixe ungültig machen oder neue Präfixe verbreiten. Hierbei würden die entsprechenden Präfixe von allen Systemen im LAN (fälschlicherweise) als am LAN befindlich betrachtet werden. Anstelle einer Weiterleitung an einen Router würde für Adressen mit den betroffenen Präfixen eine (vergebliche) ND durchgeführt.
- Ein Angreifer kann über gefälschte RD-Nachrichten falsche Parameter verbreiten. Denkbar ist beispielsweise eine Anweisung an alle Systeme, ihre Adresse von einem (nicht existierenden oder korrumpierten) DHCPv6-Server zu beziehen.
- Ein Angreifer kann ein System während der Konfiguration seines Netzwerkinterface im Rahmen der DAD davon abhalten, es

mit einer Adresse zu konfigurieren. Hierbei wird zum Zweck eines Denial-of-Service-Angriffs jede entsprechende ND-Anfrage mit einer widersprechenden ND-Antwort beantwortet.
- Ein Angreifer kann zum Zweck eines Denial-of-Service-Angriffs ein System im Rahmen der NUD davon überzeugen, dass ein System erreichbar ist, obwohl es eigentlich nicht mehr erreichbar ist. Das angegriffene System geht dann fälschlicherweise davon aus, dass das betroffene System (beispielsweise ein Router) Pakete korrekt entgegennimmt und verarbeitet bzw. weiterleitet.
- Ein Angreifer kann während der Adressauflösung gefälschte ND-Nachrichten verschicken, bei denen die darin angegebene physische Adresse gefälscht ist. Dieser Angriff entspricht dem „klassischen" ARP-Spoofing bei IPv4 [Fox_2005]. Zum Zweck eines Man-in-the-Middle-Angriffs könnte der Angreifer die eigene physische Adresse verwenden, für einen Denial-of-Service-Angriff könnte der Angreifer auf eine nicht existierende physische Adresse verweisen. Als Spezialfall hiervon könnte auch die physische Broadcast-Adresse oder eine Multicast-Adresse verwendet werden.
- Ein Angreifer kann zum Zweck eines Denial-of-Service-Angriffs gefälschte ND-Nachrichten im Namen eines existierenden Routers verschicken, in dessen Folge der Router von den anderen Systemen am LAN nicht mehr als Router betrachtet wird und alle Routen über den betreffenden Router aus den Routingtabellen der Systeme entfernt werden.
- Ein Angreifer kann gefälschte Redirect-Nachrichten verschicken. Für einen Man-in-the-Middle-Angriff könnte der Angreifer auf das eigene System, zum Zweck eines Denial-of-Service-Angriffs auf ein nicht existierendes System verweisen.

Noch weitere, hier nicht aufgeführte Angriffe sind unter bestimmten Umständen denkbar. Diese hängen beispielsweise von der Qualität der jeweiligen Implementierungen ab. Ein System, dessen IPv6-Implementierung lediglich älteren RFCs folgt, könnte gegen Angriffe verwundbar sein, denen durch Maßnahmen in neueren RFCs begegnet wird.

Prinzipiell kommen zum Schutz der Neighbor Discovery die in den folgenden Punkten benannten Gegenmaßnahmen in Betracht.

3.1 IPsec

Als Bestandteil von ICMPv6 kann jede Nachricht der Neighbor Discovery prinzipiell mit IPsec gesichert werden. Dies ist jedoch nur bedingt möglich:

Die vorgesehene Nutzung von IPsec für die ND leidet unter einem Henne/Ei-Problem. Das IPsec-Schlüsselmanagement erfolgt über das Protokoll IKE. Dies wird jedoch über UDP betrieben, d. h. für eine Nutzung müssen bereits IP-Adressen konfiguriert sein. Die einzige Möglichkeit besteht dann in manuellem Schlüsselmanagement. Dies kommt aufgrund des Betriebsaufwands allenfalls für kleine Umgebungen oder solche mit höchstem Schutzbedarf in Frage. Stattdessen könnte man dann aber auch gleich die IP-Adressen sowie die Einträge für die Neighbor Caches manuell konfigurieren.

3.2 SEND und CGA

Secure Neighbor Discovery (SEND) und Cryptographically Generated Addresses (CGA) stellen eine Alternative zu IPsec bei der Absicherung der ND dar. Im Groben soll Folgendes erreicht werden:
- Nachweis der Legitimität der Absenderadresse: Im Rahmen der ND und RD müssen Systeme nachweisen, dass sie legitime Eigentümer der (ihrer) Absenderadresse sind.
- Authentisierung von ND- und RD-Nachrichten.
- Verteilung von Zertifikatsketten: RD-Nachrichten sowie Redirects sollten auf Grundlage vorinstallierter Vertrauensanker auf Echtheit geprüft werden.

Auch SEND hat zu verschiedenen Kritikpunkten geführt. So bleibt auch hier das Schlüsselmanagement die größte Herausforderung. Darüber hinaus eröffnet der Einsatz von SEND neue Angriffsvektoren gegen die einzelnen Systeme, da im Rahmen von SEND jedes System die Signatur jeder SEND-Nachricht verifizieren muss.

3.3 Manuelle Konfiguration

Eine weitere Möglichkeit zur Vermeidung der genannten Angriffe bestünde in der statischen Konfiguration der IP- und Link-Layer-Adressen sowie der Routingtabellen aller Hosts im LAN (vgl. [ISi-LANA], Punkt 7.2.7 A). Sieht man einmal davon ab, dass diese Lösung ebenfalls nicht skaliert und daher vom Betriebsaufwand nur für Umgebungen mit höchsten Ansprüchen an die Sicherheit in Frage kommt, ist hierbei penibel darauf zu achten, dass die so konfigurierten Systeme tatsächlich nicht durch im Netz auftretende ND-Nachrichten beeinflusst werden können.

3.4 Überwachung und Alarmierung

Neben der reinen Prävention sind auch Maßnahmen der Überwachung denkbar. So kann ein Sensor in einem LAN aufgestellt werden, der den Verkehr auf verdächtiges Verhalten wie beispielsweise ND-Fluten und andere Anomalien untersucht. Beispiele für diesen Ansatz sind die Tools RAguard, NDPmon, RAfixd und RAmond. Diese Produkte haben ihren Fokus in der Mehrzahl auf gefälschten Router Advertisements. Die Reaktionsmöglichkeiten gehen von reiner Alarmierung bis hin zur Behebung. So verbreitet beispielsweise RAfixd auf erkannte illegitime RD-Nachrichten sofort Korrektur-Nachrichten.

Es wurde jedoch festgestellt, dass die genannten Produkte ihrerseits anfällig gegen Angriffe im Zusammenhang mit Fragmentierung und Header-Erweiterungen sind (s. u).

3.5 Kleine LANs

Da Angriffe gegen die ND nur direkt im LAN funktionieren, ist eine Aufteilung in kleine Subnetze ein sehr effektives Mittel, um derartige Angriffe einzudämmen. Im Extremfall könnte jedes Gerät einem eigenen Subnetz zugewiesen werden, obgleich dies allgemein weder notwendig noch ratsam ist. Eine angemessene Gruppierung der Systeme in Subnetzen nach Funktion, Vertrauenswürdigkeit und Kritizität wird in den meisten Fällen ausreichend sein, insbesondere sollten Clients von Serversystemen getrennt werden.

In vielen Unternehmen und Organisationen ist es zudem zunehmend üblich, den Netzwerk-Zugang auf Link-Layer zu absichern, beispielsweise mit 802.1X. Über diese Maßnahme kann gesteuert werden, welche Systeme in welchem Subnetz untergebracht werden. Kommt dabei Link-Layer-Verschlüsselung zum Einsatz, dann kann diese Zuordnung bei korrekter Konfiguration und Implementierung praktisch nicht umgangen werden.

4 Header-Erweiterungen

In der IPv6-Architektur ändert sich im Vergleich zu IPv4 ein wichtiges Element, nämlich der IPv6-Header mit seinen Erweite-

rungen. Dieses Element erweist sich durchaus als sicherheitsrelevant. Der IPv6-Header ist im Vergleich zum IPv4-Header vereinfacht worden. Die wesentlichen Änderungen betreffen optionale Informationen: Optionen wurden aus dem Header gestrichen, diese finden sich nun in gesonderten Header-Erweiterungen (Extension Header). Dies hat gleich mehrere Vorteile, die der Effizienz der Verarbeitung und der Erweiterbarkeit zugute kommen:

- Der IPv6-Header hat nun eine feste Größe.
- Optionen werden aus dem IPv6-Header verbannt, belegen dort keinen Platz mehr und müssen dort – vor allem von Routern – nicht verarbeitet werden.
- Optionen brauchen nicht auf einem eng beschränkten Platz untergebracht zu werden.
- Neue Optionen können eingeführt werden, ohne den bestehenden IPv6-Header zu verändern oder bestehende Optionen zu „verbiegen".

Die neue Flexibilität führt jedoch auch dazu, dass Filterregeln komplexer werden.

Der IPv6-Standard schreibt vor, dass jedes System eine beliebige Abfolge von Header-Erweiterungen verarbeiten können muss, wobei Router die Erweiterungen im Wesentlichen ignorieren. Es gibt einige (im Wesentlichen unverbindliche) Regeln:

- Jede (derzeit definierte) Erweiterung darf bis auf eine Ausnahme nur einmal vorkommen.
- Für die Abfolge mehrerer Erweiterungen gibt es eine Empfehlung.
- Die Abfolge der Erweiterungen muss sequenziell abgearbeitet werden, d. h. ein System darf nicht nach Erweiterungen suchen.

Die Komplexität der Erweiterungen ist im Wesentlichen den variablen Erweiterungen Hop-by-Hop Options und Destination Options geschuldet, die ihrerseits nur einen Rahmen für jeweils zu definierende Optionen bilden. Neben der Möglichkeit, unbekannte oder unsinnige Optionen verarbeiten zu müssen, macht auch das Padding die meisten Schwierigkeiten bei der effizienten Verarbeitung der variablen Erweiterungen. Exzessiver Gebrauch dieser Möglichkeiten kann vor allem dazu verwendet werden, Inhalte eines Pakets auf bestimmte Weise in dem Paket zu verteilen. Im Speziellen kann beispielsweise mit Hilfe des Paddings der TCP-Header soweit nach hinten verschoben werden, dass der Header in Kombination mit Fragmentierung (s. u.) nicht mehr im ersten Fragment steht und eine Filterentscheidung an einer Firewall damit recht aufwändig wird. Daneben können unbekannte Optionen und Padding dazu missbraucht werden, um Daten unauffällig abfließen zu lassen.

Aus Sicherheitssicht muss die Forderung nach der Verarbeitung beliebiger Erweiterungen zurückgewiesen werden. Da die meisten Erweiterungen in gewöhnlichen betrieblichen Szenarien nicht auftauchen, können die betreffenden Erweiterungen ausgefiltert werden. Dennoch bleiben Erweiterungen mit Blick auf zukünftige Entwicklungen eine sicherheitstechnische Herausforderung.

5 Fragmentierung

Unter IPv6 wird Fragmentierung grundsätzlich anders behandelt als unter IPv4, denn Fragmentierung wird nur noch beim Absender vorgenommen. Ist ein Paket zu groß für einen Streckenabschnitt, dann gibt der entsprechende Router vor diesem Abschnitt eine Fehlermeldung zurück – es ist dann die Aufgabe des Absenders, zu entscheiden, was nun passieren soll. Im Vergleich zu IPv4 ist dies eine große Verbesserung, da bei IPv4 die Router die Fragmentierung vornehmen, was in ungünstigen Fällen zu mehrfacher Fragmentierung führen kann. Zudem ist Fragmentierung recht aufwändig, so dass die Router bei IPv6 hier komplett entlastet werden.

Wird ein Paket unter IPv6 fragmentiert, dann werden die dafür notwendigen Informationen in einer eigenen Header-Erweiterung untergebracht. Auch dies dient der effizienteren Verarbeitung an Routern, da diese – im Wesentlichen – keine Erweiterungen verarbeiten dürfen. Abgesehen davon funktioniert Fragmentierung unter IPv6 prinzipiell genau wie IPv4.

Genau wie bei IPv4 kann Fragmentierung jedoch missbraucht werden. So kann ein Angreifer in Verbindung mit den variablen Header-Erweiterungen (s. o.) dafür sorgen, dass Filterentscheidungen schwieriger und aufwändiger zu treffen sind.

Die minimale Paketgröße bei IPv6 wurde auf 1.280 Bytes festgelegt. Eine Untersuchung der möglichen Header-Erweiterungen zeigt [Hamdy_2013], dass es (derzeit) kein legitimes Szenario gibt, bei dem der IPv6-Header samt Erweiterungen und Header der Payload nicht innerhalb eines Pakets dieser Größe untergebracht werden kann – Pakete, die so fragmentiert sind, dass keine einfache Filterentscheidung getroffen werden kann, können somit im Prinzip grundsätzlich verworfen werden.

6 Datenschutz

Die Rückkehr des Ende-zu-Ende-Prinzips, bei dem jedes System eine global eindeutige Adresse erhält, und die Beseitigung von Network Address Translation (NAT) bei IPv6 haben zu einigen Bedenken hinsichtlich der Privatsphäre der Nutzer geführt. Gleichzeitig wurden jedoch mit IPv6 die sogenannten Privacy Extensions (PEX) eingeführt. In diesem Abschnitt wird für drei unterschiedliche Szenarien die Tauglichkeit von NAT im Vergleich mit Privacy Extensions zur Wahrung der Privatsphäre diskutiert (vgl. auch [BVA_2013], Abschnitt 8.5). Dazu ist zunächst zu definieren, was eigentlich Wahrung der Privatsphäre bedeutet.

- Das erste Ziel kann darin bestehen, als Client einer End-Site (z. B. das Heimnetz) nicht ausfindig gemacht werden zu können, d. h. ein Dienstanbieter (beispielsweise eine Nachrichtenseite) soll die Nutzungen des Dienstes zu verschiedenen Zeiten von einer bestimmten Site aus nicht miteinander korrelieren können. Mit anderen Worten, es soll nicht möglich sein, verschiedene Kommunikationsvorgänge einer Site zuzuordnen (Unverkettbarkeit).
- Das zweite Ziel kann darin bestehen, als Client in einer Gruppe anderer Clients innerhalb einer Site nicht aufgespürt werden zu können, d. h. ein Dienstanbieter mag zwar die Zugehörigkeit eines Nutzers zu einer Site feststellen können, nicht aber, welcher Client innerhalb der Site den betreffenden Dienst verwendet. Mit anderen Worten, es soll nicht möglich sein, zwischen den Clients einer Site zu differenzieren (Anonymität bzw. Pseudonymität).
- Das dritte Ziel kann darin bestehen, als einzelner mobiler Roaming Client (z. B. ein Smartphone) nicht verfolgt werden zu können (Abwehr von Tracking).

Für die Diskussion der nachfolgend im Detail dargestellten Szenarien sei zunächst auf einige Aspekte der Adressvergabe bei IPv6 im Vergleich zu IPv4 hingewiesen.

Zum Verständnis wird zunächst kurz auf die „Anatomie" einer IPv6-Adresse eingegangen. IPv6-Adressen haben eine Länge von

128 Bits, die einen unvorstellbar großen Adressraum aufspannen. Die Adresse ist aufgeteilt in ein 64-Bit langes Präfix, gefolgt von einer 64-Bit langen Interface-ID. Die Interface-ID wird im Rahmen der automatischen Adresskonfiguration typischerweise aus der physischen Adresse gebildet (z. B. aus der MAC-Adresse). Die Vergabe von IPv6-Adressen erfolgt so, dass ein Kunde von einem ISP ein Präfix bekommt, z. B. ein /48-Präfix, d. h. der Kunde bekommt keine einzelne Adresse sondern gleich mehrere Netze. Dieses Präfix wird vom Kunden durch Wahl einer beliebigen Subnet-ID (hier der Länge 16) auf ein 64-Bit langes Präfix erweitert. Die Kombination aus Präfix und Interface-ID ergibt die IPv6-Adresse.

- End-Sites bekommen üblicherweise ein festes IPv6-Präfix vom ISP zugewiesen, beispielsweise ein /48- oder ein /56-Präfix. Es ist davon auszugehen, dass allgemein bekannt sein wird, welche ISPs Präfixe aus welchem Adressbereich und welcher Größe an End-Sites vergeben. Somit kann davon ausgegangen werden, dass das Präfix die End-Site eines Nutzers identifiziert. Daran würde auch NAT nichts ändern.
- Selbst bei einer Vergabe von dynamischen IPv6-Präfixen an eine Site durch einen ISP wird eine dauerhafte Korrelation von Zugriffen allein auf Grundlage der IP-Adresse nur bedingt verhindert – bei der Verwendung von automatischer Adresskonfiguration zur Vergabe von IPv6-Adressen kann ein Client über die quasi-eindeutigen Interface-ID verfolgt werden. Dasselbe gilt, wenn die Interface-ID auf andere Weise statisch vergeben wird.
- Durch die Vergabe von dynamischen IPv4-Adressen an einen Node durch einen ISP wird dagegen eine dauerhafte Korrelation von Zugriffen allein auf Grundlage der IP-Adresse im Allgemeinen verhindert.

6.1 Szenario 1 – Heimnutzer

In diesem Szenario betrachten wir einen Nutzer, beispielsweise einen Heimnutzer, der von seinem ISP ein /56-Präfix zugewiesen bekommt. Wird dem Nutzer über einen längeren Zeitraum dasselbe Präfix zugewiesen, dann kann die Site des Nutzers innerhalb dieses Zeitraums verfolgt werden. Die Verwendung von Privacy Extensions verschleiert zwar den einzelnen Host, aber nicht die Site. Selbst eine Verwendung von wechselnden Subnet-IDs führt nicht zu Unverkettbarkeit, da die Site nach wie vor am Präfix zu erkennen ist. Der Einsatz von NAT hilft an dieser Stelle überhaupt nicht weiter.

Werden Präfix (vom ISP) und Subnet-ID (vom Nutzer) dynamisch vergeben, reicht das allein jedoch auch nicht aus. Wenn die Interface-IDs statisch vergeben werden, etwa über automatische Adresskonfiguration, dann verraten die Interface-IDs die Clients innerhalb der Site und damit auch die Site an sich.

Um eine dauerhafte Korrelation von Zugriffen allein auf Basis der IP-Adresse zu verhindern, müssen sowohl das Präfix als auch die Interface-ID und möglichst auch die Subnet-ID dynamisch vergeben werden.

6.2 Szenario 2 – Nutzer einer Site

In diesem Szenario betrachten wir eine Site mit statischem Präfix und einer signifikanten Anzahl von Nutzern, zwischen denen von außen eine Differenzierung nicht möglich sein soll. In diesem Szenario helfen Privacy Extensions genauso wie NAT oder die Verwendung eines Proxys, das Aufspüren eines bestimmten Clients zu verhingern. Bei Verwendung der Privacy Extensions bleibt das Ende-zu-Ende-Prinzip gewahrt. Im Fall von NAT würde das Ende-zu-Ende-Prinzip wieder aufgegeben. Bei Verwendung eines Proxys bliebe das Ende-zu-Ende-Prinzip erhalten und dennoch würden ausgehende Verbindungen von einer einzigen IP-Adresse kommend erscheinen. Da man auf dem Proxy auch gleich Content-Filterung vornehmen kann, ist die Verwendung von Proxys gegenüber NAT oder Privacy Extensions im Unternehmensumfeld in der Regel die bessere Wahl.

6.3 Szenario 3 – Mobiler roaming Client

Dieses Szenario hat Ähnlichkeit zu Szenario 1 mit dynamischer Vergabe des Präfixes. Hierbei wird ein einzelner mobiler Host betrachtet, der sich von Netz zu Netz bewegt (Roaming). Hosts, deren Interfaces über automatische Adresskonfiguration konfiguriert werden, bekommen stets dieselbe Interface-ID. Ein Roaming Host kann über die Interface-ID über die Netzgrenzen hinweg verfolgt werden.

Neben den „üblichen" Bedenken in Bezug auf die Wahrung der Privatsphäre kommt als potenzielle Bedrohung hinzu, dass hierüber ein räumliches Bewegungsprofil (Tracking) des Nutzers erstellt werden kann. Die Privacy Extensions wurden dafür entworfen, um in genau diesem Szenario Abhilfe zu schaffen, indem sie dafür sorgen, dass regelmäßig eine zufällige temporäre Interface ID gewählt wird.

An dieser Stelle würde auch NAT ggf. helfen, wenn alle Betreiber der besuchten Netze dies konsequent durchführen würden. Hierbei würde jedoch die Verantwortung zur Wahrung der Privatsphäre in die Hände der einzelnen Betreiber gelegt. Daher ist es vorzuziehen, durch Verwendung von Privacy Extensions eigenverantwortlich die eigenen Anforderungen an den Datenschutz durchzusetzen.

6.4 Fazit zum Datenschutz

Die Privatsphäre wird durch IPv6 nicht mehr oder weniger bedroht als durch IPv4. Mechanismen wie Cone-NAT oder Proxys können hier in einigen Szenarien zur Wahrung der Privatsphäre beitragen, ebenso die dynamische Vergabe von Präfixen. Jedoch sollte man dabei Folgendes bedenken: Die IP-Adresse ist nur eine Möglichkeit, Nutzer zu verfolgen. Auf Anwendungsebene hinterlassen vor allem Browser weitere Spuren, die zum Tracking von Nutzern und zur Verkettung von Ereignissen geeignet sind. Wer gezielt Anonymität im Netz sucht, sollte unabhängig vom genutzten Netzwerkprotokoll einen entsprechenden Dienst in Anspruch nehmen.

7 Weitere Aspekte

7.1 Netzwerkabtastung

Die IPv6-Adressarchitektur hat aus Sicherheitssicht eine interessante Wirkung auf die Möglichkeit einer Netzwerkabtastung, beispielsweise mit einem Portscanner wie nmap: In IPv4-Netzen können mit Hilfe eines Portscanners Netze auf aktive Hosts überprüft werden, indem der Netzbereich aufgezählt wird und an jede zum Netz gehörige Adresse ein oder mehrere Testpakete geschickt werden. Dies ist selbst für die größten IPv4-Netze noch praktikabel. Da ein IPv6-Netzwerk dagegen jedoch grundsätzlich mindestens 2^{64} Adressen umfasst, verbietet sich diese Vorgehensweise für IPv6-Netze schon auf den ersten Blick. Eine detaillierte

Betrachtung hierzu wurde in RFC 5157 vorgenommen, die durch Fernando Gont verfeinert wurden [Gont_2011, Gont_2012].

Unter Umständen ist jedoch die Aufzählung aller *wahrscheinlich* in Frage kommenden IPv6-Adressen praktikabel. Wenn Adressen in einem Netz beispielsweise in IPv4-typischer Manier sequenziell beginnend bei der niedrigsten oder höchsten Adresse vergeben werden, dann ist eine Aufzählung der entsprechenden Systeme nicht weiter aufwändig. Ebenso ist es denkbar und plausibel, dass Administratoren die Portnummer des Dienstes in die Adresse einbetten – ein solches Schema ist für potenzielle Angreifer ebenso voraussagbar wie die Verwendung von Adressen, deren Schreibweise sich dicht an einprägsamen Begriffe anlehnt.

Schwieriger ist eine Aufzählung im Fall von Interface-IDs, die z. B. aus 48-Bit-MAC-Adressen gebildet werden, jedoch ist dies nicht unmöglich. Die MAC-Adressen werden nicht vollkommen zufällig vergeben, sondern die oberen 24 Bits kennzeichnen u. a. den Hersteller der Netzwerkschnittstelle und sind relativ leicht vorhersagbar.[1] Es verbleiben die unteren 24 Bits, deren Aufzählung so aufwändig ist, wie die eines Class-A-Netzes unter IPv4. Somit entspricht der Aufwand einer Abtastung dem eines Scans einiger Class-A-Netze – aus praktischer Sicht ist dies prinzipiell noch machbar. Werden IPv6-Adressen jedoch pseudozufällig vergeben, dann ist die Aufzählung der Systeme in den entsprechenden Netzen jenseits jeder Praktikabilität.

7.2 Privacy Extensions in Unternehmensnetzen

Gelegentlich tauchen in Gesprächen, in Vorträgen oder in schriftlichen Beiträgen Bedenken gegen die Verwendung von Privacy Extensions in Unternehmensnetzen auf. Die Quelle der Bedenken ist ein – zumindest subjektiv wahrgenommener – Kontrollverlust, etwa für die Nachvollziehbarkeit der Aktivitäten im Netz. Dem kann durch geeignete Überwachung und Protokollierung bei der Zugangskontrolle entgegengewirkt werden, was allerdings einvernehmliche Regelungen mit dem Datenschutz und/oder mit der Mitarbeitervertretung erfordern kann.

Ob die Bedenken gegen Privacy Extensions gerechtfertigt sind, hängt von den konkreten Einsatzszenarien und Anforderungen ab. Derzeit sind sogenannte Stable Privacy Extensions im Gespräch, bei denen die Interface-ID pseudozufällig, aber abhängig vom Präfix gebildet wird, so dass für ein Netz (d. h. für ein Präfix) immer dieselbe Interface-ID gewählt würde, für unterschiedliche Netze jedoch auch stets unterschiedliche Interface-IDs. Diese Art von Privacy Extension hätten Wirkung auf die oben diskutierten Szenarien 1 und 2; eine abschließende Beurteilung steht noch aus.

7.3 Produkte und Implementierungen

IPv6 wurde zwar bereits vor 15 Jahren zum ersten Mal spezifiziert, jedoch lange Zeit von den Herstellern weitgehend ignoriert. Erst in jüngerer Zeit bemühen sich viele Hersteller ernsthaft, IPv6 in ihre Produkte zu integrieren. Da IPv6 auch heute noch gelegentlich Nachbesserungen erfährt, ist zu erwarten, dass diese Nachbesserungen erst mit Verzögerungen in existierende Produkte einfließen. Daher ist vor allem bei der Beschaffung von Hardware darauf zu achten, dass alle sicherheitskritischen RFCs angemessen umgesetzt wurden.

Zu IPv6 existieren mittlerweile zahlreiche RFCs. Um einfacher die Übersicht zu behalten, hat RIPE ein Dokument herausgegeben [RIPE_554], in dem an verschiedene Gerätetypen präzise Anforderungen gestellt werden, welche RFCs mindestens erfüllt sein müssen. Ein weiter gehender Prüfkatalog wurde unter Federführung des Bundesverwaltungsamts für die öffentliche Verfaltung erarbeitet [BVA_2013], der in den meisten Fällen im Wesentlichen von beliebigen Organisationen übernommen werden kann.

Darüber hinaus sollte berücksichtigt werden, dass eine vom Hersteller angegebene IPv6-Unterstützung u. U. noch nicht alle Aspekte eines Produktes umfasst. So existieren nach Untersuchungen der Firma ERNW noch zahlreiche Firewalls namhafter Hersteller, die zwar IPv6-Verkehr regeln können, deren Management-Oberflächen etwa über SSH, HTTP oder SNMP, jedoch nicht mit IPv6 ansprechbar sind.[2] Ebenso verhält es sich noch oft mit Protokollen wie RADIUS, NTP, Syslog oder Routing-Protokollen. Dies ist bestenfalls kurios; gefährlich wird es, wenn ein Malware- oder Spam-Schutz oder eine UTM-Lösung zwar beispielsweise Pattern-Updates auch über IPv6 beziehen kann, aber aktiv nur den IPv4-Verkehr inspiziert und den IPv6-Verkehr unkontrolliert passieren lässt. Bei der Beschaffung von derartigen Produkten sollte unbedingt darauf geachtet werden, dass die relevanten Funktionen auch für IPv6 uneingeschränkt zur Verfügung stehen.

8 Fazit

Die Einführung von IPv6 ist nicht trivial, stellt andererseits aber auch kein unüberwindliches Hindernis dar. Wie in allen anderen Bereichen der IT- und Informationssicherheit leistet nicht die Technik, sondern leisten Organisation und Planung den größten Beitrag. Eine angemessene Planung erfordert jedoch auch angemessenes Wissen, Können und Erfahrung. Hier sind die IT-Verantwortlichen gefragt, Mittel und Zeit bereitzustellen, um den IT-Betrieb auch in wenigen Jahren noch sicherzustellen.

Literatur

[BVA_2013] C. Schmoll et al.: *IPv6 – Migrationsleitfaden für die öffentliche Verwaltung*, Bundesverwaltungsamt, 2013

[Esslinger_1997] B. Esslinger, M. Müller: *Secure Sockets Layer (SSL) Protocol*. DuD 12/1997, S. 691-697.

[Fox_2005] D. Fox: *ARP Poisoning*. DuD 10/2005, S. 614.

[Gont_2011] F. Gont: *Hacking IPv6 Networks*. Vortragsfolien zu DEEPSEC 2011

[Gont_2012] F. Gont: *Network Reconnaissance in IPv6 Networks*. IETF Internet Draft, Dezember 2012

[Hagen_2009] S. Hagen: *IPv6 – Grundlagen, Funktionalität, Integration*, 2. Auflage, Sunny Edition, 2009

[Hamdy_2013] S. Hamdy: *IPv6 – Die grundlegenden Funktionen, Bedrohungen und Maßnahmen*, Secorvo White Paper, 2013.

[ISi-LANA] ISi-Projektgruppe: *Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA) – Version 2.0*, in *BSI-Standards zur Internet-Sicherheit (ISi-S)*, Bundesamt für Sicherheit in der Informationstechnik, 2012

[RFC_2460] S. Deering, R. Hinden: *Internet Protocol, Version 6 (IPv6) Specification*, 1998

[RIPE_554] M. Käo, J. Žorž, S. Steffan: *Requirements for IPv6 in ICT Equipment*, RIPE-554, 2012

1 Mit zunehmender Virtualisierung von Server-Systemen wird die Vorhersage besonders einfach. Aber auch bei realer Hardware werden in vielen Unternehmen für die Mehrzahl der Rechner nur wenige Baureihen von einigen bekannten Herstellern eingesetzt.

2 *Overview of the Real-World Capabilities of Major Commercial Security Products*, Workshop auf dem IPv6 Security Summit 2013.