Was sich durch IPv6 für die IT-Forensik ändert

Spurensuche

Martin Wundram, Alexander Sigel

Mit steigender Verbreitung von IPv6 entstehen für IT-Forensiker neue Herausforderungen bei der Untersuchung von Malware und Netzwerkangriffen sowie der Suche nach Tätern und ihren Angriffswegen. Die Werkzeuge sind aber größtenteils schon „IPv6-ready“.

Aus Sicht der IT-Forensiker sind nicht nur all die Neuerungen des kommenden Internetprotokolls IPv6 eine Herausforderung, sondern bereits dessen bloße Existenz. Muss zum Beispiel eine Sicherheitsabteilung dem Verdacht auf Sabotage im eigenen Netzwerk nachgehen – ein Fall, der in vielen Unternehmen leider gar nicht so selten ist –, so könnte sie zur Suche nach Einfallswegen Netzwerksensoren an neuralgischen Netzknoten platzieren, zum Beispiel vor dem Uplink.

Da oft große Datenmengen anfallen, stellt man solche Sensoren bei Bedarf mit Filtern so ein, dass sie irrelevante Datenströme auslassen, oder umgekehrt nur relevant erscheinende speichern. Was, wenn der Täter einen IPv6-Tunnel in das Unternehmensnetzwerk aufgebaut hat und die Forensiker lediglich an IPv4 denken? Was, wenn die Firewall ausschließlich IPv4-Regeln enthält, oder die Forensiker aus Unkenntnis die IPv6-Regeln nicht beachten und nicht auf Lücken untersuchen?

Es gibt mit IPv4 und IPv6 nun zwei verbreitete, miteinander verwobene und doch parallel existierende Bereiche. Dank Tunnel-Techniken wie Teredo und 6to4 sowie Mobilerweiterungen wie Mobile IPv6 fragen sich IT-Forensiker noch öfter als bisher, woher die Datenpakete kommen, wohin sie gehen und ob der Host wirklich an dem Ort steht, an dem es den Anschein hat. Die gigantische Masse an neuen IPv6-Adressen und -Adressblöcken erscheint zunächst aus Sicht der Forensik beeindruckend: Sind Port- und Netzwerkscans überhaupt noch realistisch? Werden sich IP-Adressen noch öfter ändern, und sind Täter überhaupt nicht mehr auffindbar? Oder werden durch statisch zugeordnete Adressen und Adressbereiche Anschlüsse und deren Nutzer umgekehrt sogar gläsern?

Im Hinblick auf IPv6 gliedert sich die IT-Forensik in zwei Bereiche: Traffic-Auswertung und System-Auswertung.

Grundfunktionen „an Bord“

Die aktuellen Versionen der verbreiteten Betriebssysteme bringen bereits alle nötigen Werkzeuge für grundlegende Aufgaben mit. Um einen Host per ICMPv6 zu kontaktieren, benutzt man unter Linux *ping* und unter Windows *ping* mit der Option *-6*. Dies stellt zugleich sicher, dass ein Host ausschließlich per ICMPv6 und nicht zusätzlich oder alternativ per ICMPv4 angesprochen wird. Für die bekannten Abfragen über das *whois*-Protokoll kommt weiterhin unverändert das Linux-Tool *whois* zum Einsatz.

Für Traceroutes benutzen die Linuxer *traceroute6*, und unter Windows lässt sich mit der Option *-6* für *tracert* die Verwendung von ICMPv6 erzwingen. Gelegentlich ist es erforderlich, Kopien von Webseiten zu erzeugen, etwa mit *wget*. Dessen einstellbare Optionen *-4* und *-6* bewirken, dass das Werkzeug ausschließlich Daten über das gewünschte Protokoll bezieht und auch URLs mit dem jeweils anderen Protokoll nicht folgt.

Diese Unterscheidungen können gerade bei forensischen Untersuchungen notwendig sein, da die Programme üblicherweise einfach irgendeinen passenden DNS-Record für die Verbindung verwenden, und das kann sowohl

ein A-Record als auch ein AAAA-Record sein. Dazu passend lässt sich etwa das *host*-Kommando unter Linux so konfigurieren, dass es die DNS-Auflösung entweder nur über IPv4 (Option *-4*) oder nur über IPv6 (Option *-6*) vornimmt. Beispielsweise funktioniert die Namensauflösung für Heise bei den Autoren nur per IPv4 (vergleiche die Ausgabe von *host -4 www.six.heise.de* mit *host -6 www.six.heise.de*).

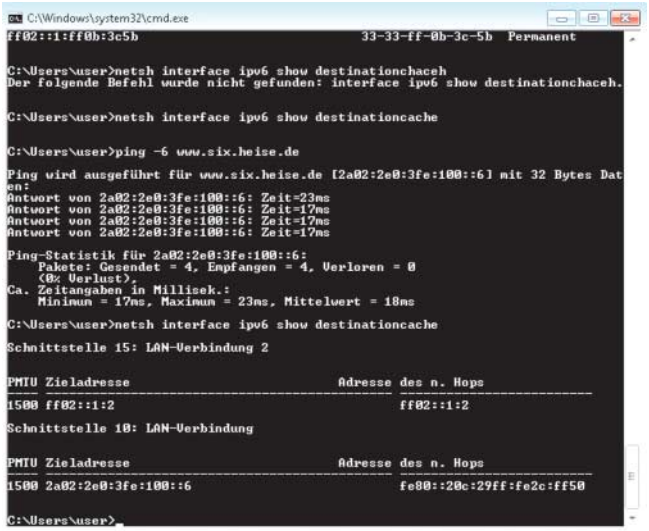
Auf alle Varianten untersuchen

Tools wie Wireshark und *tcpdump* sind seit längerer Zeit IPv6-fähig und erfolgreich für Netzwerk-Forensik im Einsatz. An ihrer Bedienung ändert sich grundsätzlich nichts. So kann der Forensiker einfach einen Speicherauszug (Dump) aller IPv6-Daten per *tcpdump* erstellen: *tcpdump -s 0 -w dump.file ip6*. Filter für Wireshark und *tcpdump* sind oft auf ein Protokoll festgelegt, ohne besonders darauf hinzuweisen. So meint der Filter *icmpv6* die Version 6, *icmp* hingegen meint nicht beide Versionen, sondern lediglich ICMPv4. Auf jeden Fall müssen bei Recherchen die Werkzeuge nun neben A-Records auch AAAA-Records abfragen, um alle infrage kommenden Systeme zu erkennen und zu erfassen.

Die in IPv4 weit verbreitete Network Address Translation (NAT) verletzt das Ende-zu-Ende-Prinzip und wurde historisch insbesondere zur Entschärfung der Adressknappheit eingeführt. Da sich eingehende Verbindungen dank NAT auf einfache Weise ausfiltern lassen und seit vielen Jahren auch im Heimbereich fast immer Router die Internetverbindung aufbauen sowie verwalten, entsteht der nicht unberechtigte Eindruck, dass hierdurch eine Sicherheitsschicht zwischen Internet und LAN entsteht. Insbesondere teilen sich oft mehrere Systeme eine „externe“ IP-Adresse und erscheinen so nach außen hin als ein einziges System.

Durch Einführung von IPv6 kommt es hier zu einem regelrechten Paradigmenwechsel, wenn NAT entfällt und Endkunden nicht mehr nur eine einzige extern erreichbare Adresse erhalten, sondern einen mindestens 64 Bit großen Pool möglicher Adressen. Endgeräte sind dann grundsätzlich direkt aus dem Internet heraus zu erreichen. Dies hat für IT-Forensiker mehrere Implikationen. Zum einen müssen sie dann ganze Netzwerke überwachen und nicht mehr nur einzelne IP-Adressen. Zum anderen wird hierdurch zumindest grundsätzlich die unmittelbare Zuordnung von Datenverbindungen zu konkreten Endgeräten möglich.

Da sich die Erzeugung des Interface Identifier historisch von der MAC-Adresse des Netzwerk-Interface ableitet, ist damit sogar eine Identifizierung der Hardware möglich. Aus Sicht der Forensiker sehr angenehm, aus Sicht vieler Benutzer eine handfeste Gefahr für Datenschutz und Anonymität. RFC 4941 definiert daher Privacy-Extensions-Maßnahmen, die die Anonymität von Benutzern wieder stärken sollen. Der Interface Identifier wechselt in regelmäßigen Abständen und lässt durch eine randomisierte Auswahl keine Rückschlüsse mehr auf das System zu.



Der Destination Cache offenbart, welche Systeme via IPv6 über welche Interfaces mit anderen Systemen kommuniziert haben (Abb. 1).

Aktuelle Betriebssysteme wie Windows 7 oder 8, Mac OS X und viele Linux-Distributionen haben diese Option bereits aktiviert. Ältere Versionen bieten diese Option entweder überhaupt nicht oder setzen ebenfalls eine manuelle Aktivierung voraus. Dies gilt insbesondere für Android, das erst auf Befehl seine MAC-Adresse verschleiert. Für IT-Forensiker bedeuten Systeme mit eingeschalteten Privacy Extensions zum einen fehlende Zuordnungsmöglichkeiten und zum anderen die Notwendigkeit, viele Spuren in Korrelation zu bringen, um daraus ein Gesamtbild zu erzeugen. Denn wenn Netzwerk-Interfaces mehrere und wechselnde Adressen parallel verwenden, ist eine exakte zeitliche Erfassung und Zuordnung aller Spuren und Informationen unabdingbar.

Im Tunnel getarnt

Da trotz zunehmender Verbreitung IPv6 weiterhin nicht flächendeckend für Endkunden zur Verfügung steht, aber auch allgemein in bestehenden Infrastrukturen eine Umstellung nicht immer möglich oder gewollt ist, gibt es verschiedene Tunneltechniken. Dienstleister wie SixXS und HE bieten jedermann kostenfrei IPv6-Tunnel inklusive fest zugeordnetem IPv6-Adressraum an. So kommen auch „IPv4-only“-Benutzer durch Tunneleinrichtung in das IPv6-Netz.

Aus Sicht der IT-Forensik entstehen dadurch zwei Problembereiche. Zunächst können Täter durch Verwendung eines Tunnels ihre IPv4-Adresse verschleiern. Bei Anbietern wie SixXS liefert eine *whois*-Abfrage zur jeweiligen IPv6-Adresse die Zuordnung zu einem Handle (zum Beispiel „descr: SixXS assignment to end-user MWV12-SIXXS“). Dieses und weitere Daten muss man aber wieder bei SixXS erfragen, was wertvolle Zeit kosten kann oder sogar unbeantwortet bleibt. Einfacher ist es bei 6to4- und Teredo-Tunnel-Adressen, denn hier ist die IPv4- codierter Bestandteil der IPv6-Adresse [a].

iX-TRACT

- Viele Forensik-Werkzeuge, vor allem auch unter den Betriebssystembordmitteln, sind jetzt schon IPv6-tauglich. Allerdings sollte man in der Regel jedes der beiden Protokolle gezielt ansprechen.
- Die Tauglichkeit der Werkzeuge allein nützt dem Forensiker noch nichts, eine Kenntnis der IPv6-spezifischen Stolperfallen – etwa aktive Autokonfiguration – ist unerlässlich.
- Viele Aspekte wie die Ausgestaltung der Anonymität oder der Einsatz von Verschlüsselung sind noch offen, sei es seitens der Hersteller oder der Nutzung durch den Endkunden. Auf die Forensik wird das Auswirkungen haben.

Da alle aktuellen Betriebssysteme gleich mehrere Tunneltechniken unterstützen, bieten sie viele neue Einfallstore als Angriffswege und damit neue Möglichkeiten, Daten an der Firewall vorbeizuschmuggeln. Netzwerkforensische Auswertungen müssen daher unbedingt die Suche nach aktiven oder „schlafenden“ Tunneln einbeziehen.

In Verbindung mit der Dual-Stack-Implementierung und aktiver Autokonfiguration entsteht damit ein drittes Problem, das zugleich einen interessanten Kniff für forensische Untersuchungen bietet. Sobald etwa Teredo-Interfaces eine passende Gegenstelle finden oder ein Router im LAN anfängt, Router-Advertisements zu senden, erhalten Systeme wie Linux, Windows, Mac OS X, Android et cetera eine gültige IPv6-Adresse und sind damit aus dem Internet heraus unmittelbar erreichbar. Täter könnten daher unauffällig einen eigenen SixXS-Tunnel-Router in einem LAN platzieren, auf diese Art im Netzwerk ein zweites „Schattennetzwerk“ aufbauen und darüber die angeschlossenen Systeme erreichen, sofern keine speziellen Gegenmaßnahmen greifen. Umgekehrt können IT-Forensiker versuchen, einem ungesprächigen zu untersuchenden System einen Tunnel-Router „an die Seite zu stellen“ und dann zum Beispiel per Port-Scan zu schauen, ob Verbindungen über die IPv6-Adresse möglich sind.

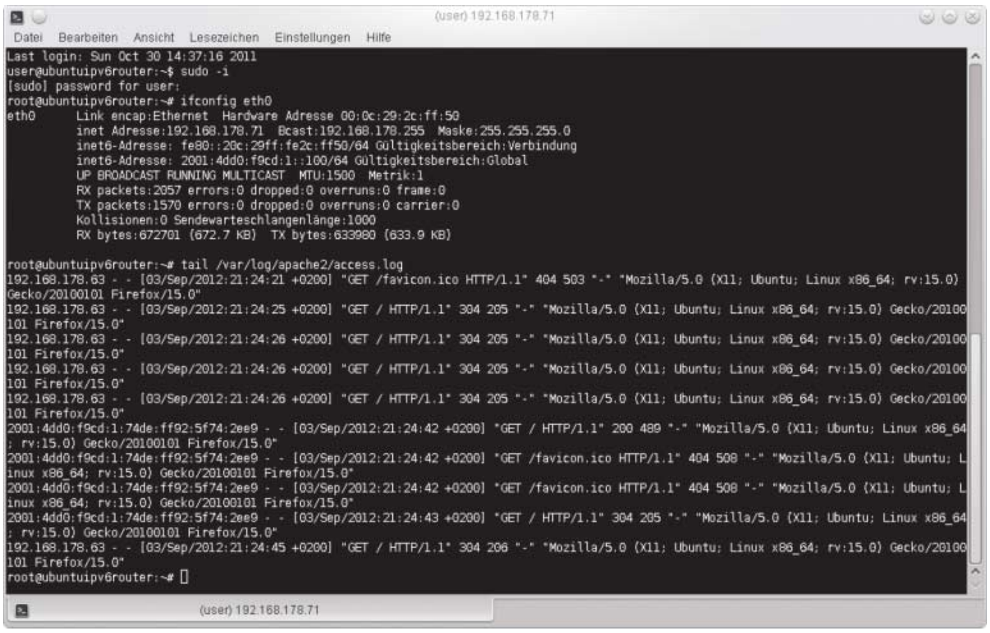
Besonderheiten mobiler Geräte

Mobile IPv6 (RFC 6275) erfindet das Rad nicht neu, kann IT-forensische Auswertungen aber doch deutlich erschweren. Die Technik ermöglicht es mobilen Geräten, dauerhaft unter derselben IPv6-Adresse erreichbar zu sein und darüber zu kommunizieren. Mobile IPv6 verhält sich ähnlich wie VPN. Angriffe auf eine IPv6-Adresse oder von einer solchen müssen daher nicht zwangsläufig in den Räumen des zugehörigen Unternehmens erfolgen, sondern können sich auf ein räumlich entferntes Notebook oder Smartphone beziehen. Der Home Agent (HA) übernimmt dabei als „Schattenrechner“ eine Stellvertreter-Rolle für den entfernten Client, der kontinuierlich bei seinem Agent seine aktuelle Care-of-Adresse meldet, unter der er erreichbar ist. IT-Forensiker sollten daher bei der Suche nach konkreten Geräten prüfen, ob diese per Mobile IPv6 angebunden sind, und bei Bedarf auch Logfiles des Home Agent sichern.

Ermittler müssen aus den genannten Gründen bei der Einrichtung eines eigenen IPv6-Forensik-Labors besondere Sorgfalt walten lassen. Ein Tunnel inklusive Router ist schnell konfiguriert. Aber sind die eigenen Systeme auch ausreichend gesichert? Sperrt die Firewall neben IPv4 unerwünschten eingehenden sowie ausgehenden IPv6-Traffic? Andernfalls wird das eigene IPv6-Labor schnell ungewollt von außen erreichbar. Auch bei IPv6 gilt: Labornetze zur Untersuchung von Malware und kompromittierten Systemen nach Möglichkeit überhaupt nicht mit externen Netzen verbinden.

DHCP: Abschied in Etappen

In einem solchen Testlabor kann man sich mit den Werkzeugen der quelloffenen THC-IPv6-Angriffs-Suite [b] vertraut machen. So lassen sich verschiedene Angriffe selbst ausprobieren, mit dem Ziel,



Der Apache-Logfile-Auszug zeigt ein munteres Nebeneinander der beiden Protokolle, das der Forensiker aufschlüsseln und entsprechend auswerten muss (Abb. 2).

Angriffsmuster und Spuren zu erkennen und besser beurteilen zu können.

Auch in Sachen Forensik bezogen auf die Netzwerkknoten (System-Auswertung) gibt es einige Neuerungen. Zwar existiert mit DHCPv6 weiterhin eine zentrale Verwaltungsinstanz der IP-Adressen, die üblicherweise auch für forensische Auswertungen nützliche Logdaten erzeugt. Es fallen jedoch häufig weniger Protokolldaten an, da die neue Stateless Address Autoconfiguration in Verbindung mit einem Advertisements sendenden IPv6-Router insbesondere für kleine Netzwerke ausreicht.

Es wird vermutlich in kleinen IPv6-LANs keine DHCP-Server mehr geben, die „Buch führen“. Dafür gibt es nun den Neighbor Cache, der vergleichbar mit der ARP-Tabelle Informationen über die Link-Layer-Adressen benachbarter Kommunikationspartner verwaltet (abrufbar zum Beispiel unter Windows mit *netsh interface ipv6 show neighbors*). Der Destination Cache geht über die Erfassung von LAN-Nachbarn hinaus und speichert alle IPv6-Systeme, an die Daten gesendet wurden, inklusive dem verwendeten Next Hop (abrufbar etwa unter Windows mit *netsh interface ipv6 show destinationcache*). Daraus erschließt sich, über welche Interfaces mit welchen Systemen kommuniziert wurde – für Forensiker eine sehr hilfreiche Informationsquelle. Doch leider haben beide Caches nur eine begrenzte Speicherdauer. So verwirft Windows Einträge im Destination Cache bereits nach circa 30 Sekunden (Abb. 1).

Live-Forensik erfordert aufgrund dieser Neuerungen eine bessere Vorbereitung und die Abfrage weiterer Informationen: Verfügt das live zu untersuchende System über einen IPv6-Stack? Ist der Stack aktiv? Ist es ein Dual-Stack-System? Sind Tunnel eingerichtet? Welche Einträge stehen in den Caches? Ist eine lokale Firewall vorhanden, aktiv und berücksichtigt diese auch IPv6?

Onlinequellen

[a] Teredo
en.wikipedia.org/wiki/Teredo_tunneling

[b] THC-IPv6-Angriffs-Suite
www.thc.org/thc-ipv6

Informationen über reguläre Ausdrücke zur Suche nach IPv6-Adressen

[c] www.vankouteren.eu/blog/2009/05/working-ipv6-regular-expression/#more-84

[d] vernon.mauery.com/content/projects/linux/ipv6_regex

[e] blogs.msdn.com/b/mpoulson/archive/2005/01/10/350037.aspx

[f] intermapper.ning.com/profiles/blogs/a-regular-expression-for-ipv6

Will man die Suche nach anderen IPv6-Systemen per Netzwerk-Scan trotz der enormen Adressräume versuchen? Will man ergänzend oder alternativ das Netzwerk passiv nach Router Advertisements und Neighbor-Discovery-Nachrichten sniffen oder den Monitorport des zentralen Switch auswerten? Administratoren sind ordnungsliebende Menschen, die nicht selten den Interface Identifier bei Serversystemen statisch setzen und dabei niedrige Zahlen verwenden (1, 2, 3,…). Ein Netzwerk-Scan über eng begrenzte Bereiche kann also dennoch gute Ergebnisse liefern.

Logfiles von IPv6-fähigen Programmen mischen meist IPv4- und IPv6-Einträge ohne spezielle Trennung. So sind Apache- oder SSHD-Logfiles weiterhin nach zeitlicher Abfolge sortiert und führen im jeweiligen IP-Feld einfach je nach Gegenstelle entweder eine IPv4- oder eine IPv6-Adresse (Abb. 2). Die forensische Auswertung von Logfiles muss daher beide Adresstypen einbeziehen, solange nicht IPv6 oder alternativ IPv4 mit Gewissheit ausgeschlossen werden kann. Die Webseiten [c–f] liefern weitere Informationen über die zum Teil beeindruckend langen regulären Ausdrücke zur Suche nach IPv6-Adressen.

Fazit

Aufgrund der gestiegenen Komplexität durch die voraussichtlich länger andauernde Parallelexistenz von IPv4 und IPv6 ist es in der IT-Forensik noch wichtiger als bisher, genaue Zeitquellen zu verwenden und exakte Zeitstempel zu erzeugen. Nur so lassen sich die größeren Informationsmengen korrelieren. Überwachungstools müssen Tunnel-Traffic decodieren können, und für die Auswertung von IT-Systemen sollten Forensiker noch mehr Logfiles einbeziehen (DHCP-Datenbank, DNS Query Logs, SNMP, ARP und Neighbor sowie Destination Cache et cetera).

Ob die feste Implementierung von IPSec zu mehr Verschlüsselung führen wird oder ob hier aus Anwendersicht einfachere und schlankere Lösungen verstärkt zum Einsatz kommen und von Forensikern berücksichtigt werden müssen, muss sich zeigen. Eine Herausforderung für forensische Untersuchungen bleibt der Themenkomplex der Anonymität/Identifizierbarkeit in seiner derzeitigen Vielfalt der MAC-Adressen-basierten Interface Identifier, per Zufall erzeugten Identifier, wechselnden oder statischen Endkunden-Präfixe. (ur)

Martin Wundram

ist Geschäftsführer der TronicGuard GmbH und Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung.

Alexander Sigel

ist Sachverständiger für IT-Forensik und Geschäftsführer der DigiTrace GmbH.

Alle Links: www.ix.de/ix1210122