Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN UND IT-DIENSTLEISTER

Effekte von IPv6 auf reine IPv4 Netze

Auf allen aktuellen Betriebssystemen ist IPv6 standardmäßig aktiviert. Dies ist durchaus wünschenswert, da die Unterstützung und der Einsatz von IPv6 Best Current Practice werden soll [RFC6540], eröffnet aber auch neue Angriffswege, die in diesem Dokument u. a. im Fokus stehen. Des Weiteren kann es zu unerwünschten Effekten kommen, wenn IPv6 nicht oder nur unzureichend konfiguriert ist. Aus diesem Grund ist es für Administratoren erforderlich, sich mit IPv6 auseinanderzusetzen.

Von den in diesem Papier behandelten Aspekten ist auch betroffen, wer vorerst nicht von IPv4 auf IPv6 umstellen möchte. Insbesondere dem Gefühl der vermeintlichen „Nicht-Betroffenheit“ soll begegnet werden. Grundsätzlich bestehen zwei Optionen zum Umgang mit dieser Thematik:

Theoretisch ließe sich IPv6 im Netz blockieren und an den Clients deaktivieren. Eine derart drastische Maßnahme kann jedoch auch negative Auswirkungen haben, da einige Dienste inzwischen IPv6 voraussetzen [Win-IPv6]. Des Weiteren wird mit einer solchen Maßnahme die Chance verpasst, den Umgang mit IPv6 frühzeitig zu erproben.

Besser ist es, ein Bewusstsein für das Vorhandensein von IPv6 zu entwickeln und sicher damit umzugehen. Im Folgenden werden drei relevante Implikationen von IPv6 auf bestehende Netze skizziert:

1 VPN-Tunnel

Insbesondere im mobilen Einsatz ist es gängige Praxis, einen VPN-Tunnel zum Unternehmensnetz aufzubauen. Über diese VPN-Verbindung kann der mobile Client verschlüsselt mit dem Firmennetz kommunizieren. Verbindungen ins Internet laufen ebenfalls über den VPN-Tunnel und über das Sicherheits-Gateway des Firmennetzes. Es ist Aufgabe des VPN-Produkts, direkte Verbindungen zu blockieren.

Einige VPN-Produkte können jedoch nur mit IPv4 umgehen und lassen alle IPv6-Verbindungen unberührt. Wenn der Zugangspunkt, z. B. ein öffentlicher Hotspot, sowohl IPv4 als auch IPv6 anbietet, so konfigurieren verbundene Clients in der Regel beide Protokolle. Wird nun ein IPv6-fähiger Server kontaktiert, so kann es passieren, dass die Verbindung über IPv6 – und dementsprechend am IPv4-VPN vorbei – aufgebaut wird. Es besteht keine Gewährleistung, dass der Teil der Kommunikation über den öffentlichen Zugangspunkt verschlüsselt erfolgt und dass die Verbindung über das Sicherheits-Gateway geführt wird.

Es sollte ein VPN-Produkt eingesetzt werden, das sowohl IPv4 als auch IPv6 unterstützt. Ist für die gewählte Konfiguration kein IPv6-fähiges VPN-Produkt verfügbar, so sollte beim Aufbau des VPNs auf allen Interfaces des Clients IPv6 deaktiviert werden.

2 IPv6-Tunnel

Microsoft Windows Betriebssysteme versuchen unter bestimmten Bedingungen, mit verschiedenen Tunnelmechanismen eine IPv6-Konnektivität zu erreichen. Ein Windows 7 Client versucht beispielsweise erst über ISATAP[1] und anschließend über Teredo[2] bzw. 6to4 einen Tunnel aufzubauen, wenn keine native IPv6-Anbindung zur Verfügung steht. Bei Windows 7 Clients in einer Domänen-Umgebung sind dies lediglich ISATAP und ggf. 6to4, jedoch nicht Teredo. Eine Teredo-Variante steht auch für Linux und Mac OS X zur Verfügung, wird dort aber in der Regel nicht standardmäßig aktiviert.

Bei Tunneln besteht die grundsätzliche Gefahr, dass Pakete ungeprüft das Sicherheits-Gateway passieren [RFC6169]. Hat ein Client erfolgreich einen IPv6-Tunnel aufgebaut, so könnte er in seinem Subnetz als IPv6-Router agieren und andere Rechner mit IPv6 versorgen. In diesem Fall könnte auch der Verkehr anderer Rechner durch das Sicherheits-Gateway getunnelt werden.

Clientseitig sollte der Aufbau von Tunneln unterbunden werden. Dieses Verhalten betrifft in erster Linie Windows-Systeme. Hierzu kann beispielsweise das Fix it „Deaktivieren von IPv6-Tunnelschnittstellen“ verwendet werden [KB929852]. Alternativ können die Interfaces einzeln über den Befehl

```
netsh interface { isatap | 6to4 | teredo } set state disabled
```

deaktiviert werden.

Am Sicherheits-Gateway werden bei korrekter Konfiguration (*default deny*) alle Tunnel-Varianten blockiert. Folgende Sperren sollten überprüft werden:

- Protokoll 41 im IPv4-Header (blockiert ISATAP und 6to4)
- UDP-Pakete mit Destination Port 3544 (blockiert Teredo)

3 Angriffe

Hat ein System einen IPv6-Tunnel erfolgreich aufgebaut, so kann es auch anderen Rechnern im selben Subnetz anbieten, die IPv6-Verbindung zu nutzen. Das tunnelnde System wird damit zum Gateway und kann für Man-in-the-Middle-Angriffe genutzt werden.

Auch wenn keine IPv6-Anbindung nach außen besteht, sind Angriffe möglich. Beispielsweise lässt sich durch das Flooding mit ICMPv6-Nachrichten auf Systemen im gleichen Subnetz die Systemlast derart steigern, dass die Systeme nicht mehr benutzbar sind.

Grundsätzlich sollten bei IPv6 die gleichen Sicherheitsmaßnahmen umgesetzt werden, wie bei IPv4. Insbesondere sollten Clients über eine IPv6-Firewall verfügen. Angriffe auf die Adressautokonfiguration können in einem gewissen Umfang mit RA-Guard[3] [RFC6105] oder vergleichbaren Techniken mitigiert werden. Da viele Angriffe nur innerhalb eines Subnetzes funktionieren, sollten Subnetze lediglich Geräte mit gleichen Anforderungen und gleichem Schutzbedarf beinhalten. Im Extremfall bedeutet dies ein separates Subnetz für einzelne Systeme oder System-Cluster (siehe hierzu auch [CSE-v6Konz]).

Werkzeuge zum Testen der eigenen Netze, wie [THC-IPv6] und [SI6-TK], sind öffentlich verfügbar. Maßnahmen gegen die meisten Angriffe sind vorhanden (böswillige Innentäter ausgenommen). Die Umsetzung der Maßnahmen und die Einarbeitung in IPv6 sind sinnvoller als die Deaktivierung.

1 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) ist ein Transitionsmechanismus zur Übertragung von IPv6-Paketen über IPv4-Netze.
2 Teredo ist ebenfalls ein IPv6-Transitionsmechanismus. Teredo verwendet UDP zur Kapselung von IPv6 in IPv4.
3 Der Router Advertisement Guard (RA-Guard) ist ein Mechanismus zur Verhinderung von rogue (entarteten) Router Advertisements.

4 Literatur

[CSE-v6Konz] Konzeption von IPv6-Netzen, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-057.pdf;?__blob=publicationFile

[Draft-v6v4] Security Implications of IPv6 on IPv4 Networks, http://tools.ietf.org/html/draft-gont-opsec-ipv6-implications-on-ipv4-nets

[ISi-LANA2.0] Sichere Anbindung lokaler Netze an das Internet v2.0, http://www.bsi.bund.de/isi-ipv6

[KB929852] Deaktivieren von IPv6-Komponenten, http://support.microsoft.com/kb/929852/de

[RFC2460] Internet Protocol Version 6 (IPv6) Specification, http://tools.ietf.org/html/rfc2460

[RFC6105] IPv6 Router Advertisement Guard, http://tools.ietf.org/html/rfc6105

[RFC6169] Security Concerns with IP Tunneling, http://tools.ietf.org/html/rfc6169

[RFC6540] IPv6 Support Required for All IP-Capable Nodes, http://tools.ietf.org/html/rfc6540

[SI6-TK] SI6 Networks' IPv6 Toolkit, http://www.si6networks.com/tools/ipv6toolkit/

[THC-IPv6] The Hacker's Choice IPv6-Toolkit, http://www.thc.org/thc-ipv6/

[Win-IPv6] The Argument against Disabling IPv6, http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.