Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN UND IT-DIENSTLEISTER

Zur Konzeption von IPv6-Netzen

IPv6 ist bereits auf allen gängigen Betriebssystemen standardmäßig aktiviert und wird in der Regel gegenüber IPv4 bevorzugt. Dementsprechend ist IPv6 in den meisten internen Netzen schon vorhanden.

Es ist daher notwendig, sich *jetzt* mit IPv6 zu beschäftigen – auch wenn für die meisten Organisationen derzeit noch kein technischer Bedarf besteht, ihre internen Netze umzustellen. Eine (Teil-)Migration sollte dennoch in Betracht gezogen werden, da IPv6 die Chance bietet, alte Netzstrukturen aufzuräumen und so die Netzsicherheit zu verbessern. Im Folgenden werden drei wesentliche Aspekte der Netzkonzeption bei IPv6 dargestellt.

1 Prinzip der kleinen Netze

Bei IPv4 müssen die knappen Adressräume möglichst effizient ausgenutzt werden. Dies hat zur Folge, dass sich Geräte mit unterschiedlichen Anforderungsprofilen oder unterschiedlichem Schutzbedarf in ein und demselben Subnetz befinden.

Unter IPv6 stehen sehr viel mehr Adressen und Subnetze zur Verfügung, als dies bei IPv4 der Fall war. Damit ist auch ein grundsätzlich neues Netzdesign möglich. Subnetze können nun an die Aufgabenstellung und den Schutzbedarf angepasst werden. So kann beispielsweise für jeden Typ von Anwendungsserver ein eigenes Subnetz eingerichtet werden. Auch Netzwerkdrucker und ähnliche Geräte können eigene Subnetze erhalten.

Auf der anderen Seite können bei IPv6 auch Netze zusammengelegt werden, die unter IPv4 getrennt werden mussten. In einem IPv6-Subnetz können nahezu beliebig viele Geräte untergebracht werden. Voraussetzung dafür ist, dass diese ein hinreichend ähnliches Anforderungsprofil und den gleichen Schutzbedarf besitzen.

2 Adresswahl

Zur Adressierung im internen Netz stehen bei IPv6 grundsätzlich zwei Adresstypen zur Auswahl:

1. Unique-local addresses (ULA)
2. Global-unicast addresses (GUA)

ULAs sind private Adressen, die jedoch im Gegensatz zu den RFC1918-Adressen bei IPv4 mit sehr hoher Wahrscheinlichkeit eindeutig sind, da 40 bit des Präfixes zufällig sind. Somit kommt es bei der Zusammenlegung von Netzen nicht zu Kollisionen und zur Notwendigkeit von Umnummerierungen. Beim Einsatz eines Sicherheits-Gateways, das alle eingehenden Verbindungen in interne Netzsegmente blockiert und alle ausgehenden Verbindungen über Application-Layer-Gateways/Proxies führt, sind ULAs für interne Netzsegmente grundsätzlich geeignet. Anhand ihres charakteristischen Präfixes lassen sich ULAs gut erkennen und am Internetübergang leicht filtern.

Bei nach außen gerichteten Systemen (Webserver, E-Mailserver, etc.) kann das Interface für die Management-Schnittstelle ULAs verwenden. Das von außen erreichbare Interface benötigt eine globale Adresse.

Auch für interne Netze ist eine Adressierung über GUAs denkbar. Es ist jedoch darauf zu achten, dass Fehler in der Konfiguration des Sicherheits-Gateways dazu führen können, dass interne Systeme aus dem Internet adressierbar werden.

Die Verwendung beider Adresstypen auf demselben Interface ist derzeitig nicht zu empfehlen.

3 ICMPv6

Das Internet Control Message Protocol (ICMP) ist ein Kernbestandteil der Internetprotokollfamilie und dient zum Austausch von Fehlermeldungen. Bei IPv4 ist es gängige Praxis, ICMP an der Firewall zu blockieren.

Unter IPv6 hat ICMPv6 eine deutlich stärkere Bedeutung bekommen und ist für Mechanismen, wie pMTUd[1], unerlässlich. Eine undifferenzierte Filterung von ICMPv6 kann Erreichbarkeitsprobleme mit sich bringen. Daher sollte bei IPv6 **keine generelle Sperrung von ICMPv6** erfolgen. Folgende ICMPv6-Typen sollten zumindest teilweise zugelassen werden (vgl. auch [RFC4890]). Nicht genannte Typen sollten gesperrt werden. Die Bezeichnungen „vom Internet“ und „zum Internet“ beziehen sich jeweils auf das System, dass die Verbindung aufbaut oder deren Endpunkt darstellt. In der Regel also das ALG.

IPv6-ICMP Nachricht (Typ)	Zwischen internen Netzen	Vom Internet	Zum Internet
Destination unreachable (1)	✓	✓	✓
Packet too big (2)	✓	✓	✓
Time exceeded (3)	✓	✓	✓
Parameter Problem (4)	✓	✓	✓
Echo-Request (128)	✓1	✗	✓1
Echo-Antwort (129)	✓2	✓2	✗
Multicast (130-132, 143, 151-153)	✓3	✓3	✓3
Router (133, 134)	✓3	✗	✗
Neighbor (135,136)	✓3	✓3	✓3
Redirect (137)	✓3/4	✗	✗
ICMP-Information (139)	✓1	✗	✗
ICMP-Information (140)	✓2	✗	✗
Reverse-Neighbor (141)	✓1	✗	✗
Reverse-Neighbor (142)	✓2	✗	✗

1 = von der Management-Station aus, 2 = zur Management-Station hin, 3 = ohne Forwarding, 4 = ausgehend vom Router

4 Weiterführende Informationen

Eine ausführlichere Darstellung der Konzeption von IPv6-Netzen inklusive Vorschlägen zur Gestaltung des Adressplans sowie einer Liste von Gefährdungen und Gegenmaßnahmen finden sich in [ISi-LANA2.0]. Implikationen von IPv6 auf vermeintlich reine IPv4-Netze werden in [CSE-v6v4] betrachtet.

Quellenangaben im Text:

[CSE-v6v4] Effekte von IPv6 auf reine IPv6-Netze, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-058.pdf;?__blob=publicationFile

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

[RFC4890] Recommendations for Filtering ICMPv6 Messages in Firewalls, tools.ietf.org/html/rfc4890

[RFC1918] Address Allocation for Private Internets, http://tools.ietf.org/html/rfc1918

1 Die path-MTU-discovery (pMTUd) ist ein Mechanismus zur Ermittlung der maximalen Paketgröße entlang eines Pfades.