Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IT IM UNTERNEHMEN UND IT-DIENSTLEISTER

Leitlinie IPv6

Warum Sie sich mit IPv6 befassen sollten

Diese Leitlinie gibt Hinweise und Empfehlungen zur Umstellung auf IPv6, ohne dabei auf technische Details einzugehen. Der Aufbau orientiert sich an den häufigsten Fragen zu IPv6.

1 Was ist IPv6?

Das Internet Protokoll (IP) dient zur Adressierung von Geräten in Netzen. Seit Anfang der 80er Jahre ist IP die Basis fast jeglicher Internet-Kommunikation. Am verbreitetsten ist aktuell noch die Version 4 (IPv4). Da IPv4 jedoch an seine Grenzen stößt, wird es aktuell durch Version 6 (IPv6) abgelöst.

2 Warum ist IPv6 relevant?

Nach mehreren Jahrzehnten ist IPv6 inzwischen im Alltag angekommen:

- In Deutschland sind etwa 35 % der Internet-Nutzer mit IPv6 versorgt.
- Windows, macOS, Linux, iOS und Android verwenden standardmäßig IPv6.
- Wenn IPv6 vorhanden ist, dann wird es meist gegenüber IPv4 bevorzugt.

Grund für die Verbreitung von IPv6 ist in erster Linie die Adressknappheit bei IPv4. Viele Internet-Nutzer bekommen inzwischen keine eigene öffentliche IPv4-Adresse mehr, sondern müssen sich diese mit anderen Nutzern teilen, wodurch einige Anwendungen nicht mehr funktionieren. Wer also Dienste im Internet anbietet, sollte diese im Sinne seiner Kunden IPv6-fähig machen.

Auch in der eigenen IT ist IPv6 bereits ein Thema:

- Die meisten Geräte im lokalen Netz beherrschen und nutzen schon IPv6.
- Mobile Endgerät werden in fremden Netzen – etwa am Flughafen – mit IPv6 konfrontiert.
- Vom Provider wird zur Internet-Anbindung oft bereits IPv6 bereitgestellt.

Spätestens jetzt ist die Zeit gekommen, sich mit IPv6 zu befassen.

3 Wie sollte man sich dem Thema widmen?

Eine schlagartige Umstellung aller IT auf IPv6 ist weder notwendig noch sinnvoll. Für die Migration gibt es verschiedene Strategien. In manchen Bereichen kann diese sehr einfach ausfallen.

Zunächst ist es wichtig sich bewusst zu machen, dass IPv6 an vielen Stellen im eigenen Netz bereits vorhanden ist und gewartet werden muss. Ein Protokoll, das unbemerkt im

Netzwerk mitläuft und nicht beachtet wird, kann sich schnell zur Sicherheitslücke ausweiten. Hat man sich ein Überblick verschafft, können gezielt Maßnahmen ergriffen werden.

3.1 Schulungen

An vielen Stellen ist IPv6 konzeptionell anders als IPv4, sodass etablierte Konzepte, Denk- und Vorgehensweisen nicht ohne Weiteres übertragen werden können [CSE-057]. Administratoren und IT-Sicherheitsbeauftragte müssen geschult und mit diesen Änderungen vertraut gemacht werden. Zudem sollte eine Testumgebung eingerichtet werden, in der die Mitarbeiter ihr erworbenes Wissen praktisch anwenden können.

3.2 Beschaffung

Bei der Beschaffung und Entwicklung neuer Hard- und Software muss auf die IPv6-Fähigkeit der Produkte geachtet werden. Eine Liste von Anforderungen an Produkte sind in [RIPE-554] und [ISi-LANA] zu finden. Da die IPv6-Kompatibilität noch nicht immer ausgereift ist, sollten alle Features geprüft werden. Hierzu kann die im vorherigen Abschnitt erwähnte Testumgebung genutzt werden.

3.3 Migrations-/Übergangstechniken

IPv4 und IPv6 sind wie zwei voneinander unabhängige Sprachen. Wenn ein IPv4-Gerät mit einem IPv6-Gerät kommunizieren möchte, so muss diese Sprachbarriere überwunden werden.

Dual-Stack
Die pragmatischste Lösung zur Überwindung der Sprachbarriere ist, eine der beiden Seiten im Dual-Stack zu betreiben. Ein Gerät bezeichnet man als Dual-Stack, wenn es sowohl IPv4 als auch IPv6 spricht. Dies ist beispielsweise für Server sinnvoll, die sowohl IPv4- als auch IPv6-Clients bedienen müssen.

Dual-Stack erhöht jedoch den Aufwand für Verwaltung und Konfiguration. Dadurch steigt die Fehleranfälligkeit und die Angriffsfläche vergrößert sich. Aus diesem Grund sollte Dual-Stack nur im unbedingt notwendigen Umfang eingesetzt werden. Dual-Stack ist eine Übergangstechnologie, die notwendig ist, bis sich IPv6 so weit verbreitet hat, dass IPv4 wegfallen kann.

Proxy
Eine Alternative ist die Verwendung anwendungsspezifischer Proxys als Übersetzer. Diese Funktion kann beispielsweise im Sicherheits-Gateway realisiert werden. Man kann auch gezielt Proxys vor Server schalten, wenn diese Server nicht als Dual-Stack betrieben werden können oder sollen.

3.4 Einrichtung

Erste Migrationsschritte sind bereits mit wenig Aufwand zu realisieren. Einige erfordern eine längerfristige Planung. Ausführliche Informationen zur Umstellung finden sich in [ISi-LANA].

Internet-Anbindung
Die Internet-Anbindung für Unternehmen um IPv6 zu erweitern, ist in der Regel ohne viel Aufwand möglich. Die meisten Internet-Anbieter können nativ, d. h. ohne Tunnel, IPv6 bereitstellen.

Internet-Dienste
Um Internet-Dienste IPv6-fähig zu machen, gibt es mehrere Möglichkeiten. Der offensichtlichste Weg ist den Server Dual-Stack, also mit IPv4 und IPv6, anzubinden. Ist dies nicht möglich, weil beispielsweise die Applikation dies nicht unterstützt, kann ein vorgeschalteter Proxy-Server helfen. Dieser nimmt Anfragen über IPv6 entgegen und übersetzt diese für den Anwendungsserver, der dann wie gewohnt arbeiten kann.

Neben des Ertüchtigen des Anwendungsservers muss natürlich auch im DNS ein Eintrag für die IPv6-Adresse des Servers hinterlegt werden und der DNS-Server selbst IPv6-fähig gemacht werden.

Mobile Endgeräte

Laptops, Smartphones und Tablets werden unterwegs oft mit fremden Netzen verbunden. Wenn diese dann unerwartet mit IPv6 in Berührung kommen, kann dies unerwünschte Effekte haben, die die Sicherheit der Kommunikation beeinträchtigen [CSE-058]. Daher müssen mobile Endgeräte und die auf ihnen eingesetzte Software, wie Firewall und VPN-Client, explizit mit IPv4 und IPv6 getestet werden.

Sicherheits-Gateway

Das Sicherheits-Gateway wird auf absehbare Zeit im Dual-Stack betrieben werden müssen. Alle Komponenten des Sicherheits-Gateways müssen daher auch den Umgang mit IPv6 beherrschen. Dazu zählen auch der Umgang mit Extension-Headers und Hilfsprotokollen, wie ICMPv6.

Lokales Netz

Das lokale Netz (LAN) bietet die meisten Gestaltungsmöglichkeiten, da sich mit IPv6 eine praktisch beliebige Zahl an Subnetzen realisieren lässt. So kann etwa für jede Klasse von Geräten (Drucker, Mailserver), jeden Konferenzraum und jedes Büro ein eigenes Subnetz konfiguriert werden. Dieses Prinzip der kleinen Netze kann die Sicherheit im Netz beträchtlich verbessern [CSE-057].

Die Vorteile von IPv6 lassen sich nur dann voll ausschöpfen, wenn Teile des Netzes IPv6-only – also ohne IPv4 – betrieben werden. Einzelnen Geräten kann bei Bedarf gezielt IPv4 über einen Tunnel bereitgestellt werden. Geräte, die kein IPv6 unterstützen, werden in einem separaten IPv4-Segment für Altlasten gekapselt.

4 Fazit

IPv6 ist Alltag und lässt sich nicht länger ignorieren. Mit einigen einfachen Schritten lassen sich bereits erste Erfolge der Migration realisieren. Die Einführung von IPv6 bietet die Gelegenheit, etablierte Vorgehensweisen und Konzepte zu überprüfen und anzupassen, um auf diese Weise die Sicherheit im Netz durch eine modernisierte Architektur grundlegend zu verbessern.

5 Literatur

[CSE-057] Konzeption von IPv6-Netzen, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_057.html

[CSE-058] Effekte von IPv6 auf reine IPv4 Netze, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_058.html

[ISi-LANA] Sichere Anbindung lokaler Netze an das Internet (Version 2.1), https://www.isi-reihe.de

[RIPE-554] Requirements for IPv6 in ICT Equipment, https://www.ripe.net/publications/docs/ripe-554

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.