# Projektgruppe Zugang, Struktur und Sicherheit im Netz

3 Fragen zum Thema „IPv6 - Sicherheitsaspekte“

**Fragen an Herrn Christoph Weber**

- Welche Herausforderungen hinsichtlich betrieblichen Aspekten, Sicherheit und geographischer Lokalisierbarkeit sehen Sie im Zusammenhang mit der Zuweisung von IPv6-Adressblöcken von Providern zu Kunden?

- Gibt es sinnvolle Lösungsansätze hinsichtlich der Fragen von Sicherheits- und Datenschutzaspekten bei mobilen Endgeräten? Welche Forderungen sind an die Hersteller von Betriebssystemen und Applikationssoftware für Mobilgeräte zu richten?

- Welche Schwierigkeiten gibt es hinsichtlich der IPv6-Umstellung bei den Herstellern von Routern, Firewalls und anderen Netzwerkgeräten? Welche sicherheitsrelevanten Probleme ergeben sich durch den Parallelbetrieb von IPv4 und IPv6 auf den Geräten in der Übergangsphase?

## Fragen an Herrn Christoph Weber

### 1. Welche Herausforderungen hinsichtlich betrieblichen Aspekten, Sicherheit und geo-graphischer Lokalisierbarkeit sehen Sie im Zusammenhang mit der Zuweisung von IPv6-Adressblöcken von Providern zu Kunden?

Der Internetprovider wird der ihm zugeteilte IPv6 Adressblock in seine für ihn relevanten Sub-Adressblöcke für Wireless (Mobile,PWLAN), Wireline (xDSL,Cabel) und sonstige Funktionen (Service und Datacenter) grob unterteilen.

Die weitere Subuntereilung wird dann entsprechend seiner Netzwerktopologie und Netzwerkfunktion des Services weiter in kleinere Adressblöcke unterteilt. Dies mit dem Hauptziel, die Routingtabellen auf seinen Core-Netzwerkgeräten möglichst klein und für den täglichen Betrieb übersichtlich und einfach nachvollziehbar zu halten.

Diese Unterteilung führt dann meistens dazu, das grössere Adressblöcke einem Gebiet zugeordnet werden können, dass heisst, wenn die IPv6 Netzadress-Prefixe, nach dem sowieso vorgegebenen Provider-Prefix nahe zusammen liegen, sie vermutlich aus dem gleichen geographischen Gebiet kommen. Der Provider wird diese Grobzuteilung auch nicht anpassen, denn der betriebliche Aufwand ist gross und das Risiko für einen möglichen Serviceunterbruch ist nicht zu unterschätzen.

Der Aufwand für eine zufällige IPv6 Netzadress-Prefixe Verteilung für Endkunden über ein ganzes Land/Gebiet ist nur schwer umzusetzen, und extrem stark von der bestehenden Infrastuktur beim Provider abhängig. Dies würde auch dazu führen, dass für jedes Kundennetz ein einzelner Eintrag in der Core Routing Tabelle geführt würde, was zu exterm grossen und unübersichtlichen Routingtabellen führen würde. Kleine Lokale Provider sind, wie bis anhin, noch schneller auf ein geographisches Gebiet rückverfolgbar, hingegen grosse, landesweite Provider haben eher die Möglichkeit, die Örtliche Zuteilung zu "verstecken"

Funktionen, dass sich der Kunde auf dem Provider Portal einen neuen IPv6 Netzadress-Prefix zuteilen kann, sind zwar teilweise schon vorhanden und umgesetzt, doch auch die Neuvergabe geschieht, wie oben erwähnt, wieder aus dem gleichen Gebiets-Adressrange. Auch eine automatische zeitlich gesteuerte Adresszuteilung löst dieses Problem nicht, sondern kann für den Endkunden unangenehme folgen haben, denn wenn er beispielsweise über seinen Internetanschluss TV schaut, kann es zu einen kurzen Service Unterbruch kommen, was für

den Kunden nicht angenehm ist. Funktionen für eine Unterbruchsfreie neue Adresszuteilung für den Endkunden sind zurzeit nicht eingesetzt.

Weiter müssen die Provider auch jeden Adresswechsel des Kunden aufzeichnen, einerseits für allfällige Abrechungen und Nachvollziehbarkeit, sowie für den allenfalls vom Staat geforderte Adressrückverfolgung.

Da sich der ganze IPv6 Netzaufbau noch stark in den Anfängen befindet, sind auch noch nicht alle technischen Möglichkeiten und Entwicklungen abgeschlossen, sicher wird sich in diesem Bereich technisch, wie auch organisatorisch und betrieblich noch viel ergeben, aber die Provider benötigen auch die Vorgaben von Kundenwünschen und vom Staat, um den entsprechenden Anforderungen gerecht zu werden.

## 2. Gibt es sinnvolle Lösungsansätze hinsichtlich der Fragen von Sicherheits- und Datenschutzaspekten bei mobilen Endgeräten? Welche Forderungen sind an die Hersteller von Betriebssystemen und Applikationssoftware für Mobilgeräte zu richten?

Für Mobile Telefongeräte, sowie andere via Wireless ins Internet verbundenen Geräte sollte man Grundsätzlich eine Lokale Firewall installiert haben. Denn Sie sind wegen des im IPv6 umgesetzten  Grundgedankens, das jedes System zu jedem anderen System im Internet eine direkte Kommunikation hat, direkten Angriffen aus dem Internet via IPv6 ausgesetzt, Daher wird der Grundgedanke, dass jedes Gerät sich selber verteidigen und schützen muss, immer wichtiger.

Inwieweit der Internetanbieter oder Mobile Provider gewisse Grundschutzfunktionen, wie Firewall und/oder Virenschutz anbieten kann und will, wird sich zeigen, denn einerseits fordern einige User die volle Netzwerktransparenz und Selbständigkeit, andererseits sind aber die meisten "durchschnitt" Nutzer technisch überfordert, wenn sie auf einem Gerät eine Lokale Firewall richtig konfigurieren müssen.

Hier wird sich wohl der Ansatz, dass der Provider eine vorkonfigurierte "Basic" Firewall zur Verfügung stellen wird, die der User auf Wunsch manuell ausschalten kann, als Service des Providers, eventuell als bezahlter Zusatz oder Mehrwert, durchsetzen.

Betriebsystem Entwickler müssen schon in der Grundfunktion des Betriebssystems eine Firewall Funktion einbauen, die einerseits den "normalen User" einen Grundschutz zur Ver-

fügung stellt, einfach angepasst und konfiguriert werden kann, andererseits auch dem "mehr Sicherheitsbewussten User".

Heutige Sicherheitsimplementierungen scheitern häufig daran, dass sie entweder nicht über die grafische Oberfläche bedient werden können, oder zu komplex sind, allenfalls nur via Command-line Befehlen zu konfigurieren sind.

Betriebsysteme sollten auch die Funktionen von Verschlüsselung im IPv6 nutzen, um eine sichere Verbindung mit ihrem Zielservern zu gewähren, doch diese Umsetzungen scheitern meistens aus zwei Hauptgründen, erstens ist der Aufwand in der Applikation für die richtige Umsetzung zu gross, zweitens ist der benötigte CPU Power auf den Mobile Gräten nicht ausreichend vorhanden, oder führt zu einer Verlangsamung der Software, was nicht erwünscht ist.

### 3. Welche Schwierigkeiten gibt es hinsichtlich der IPv6-Umstellung bei den Herstellern von Routern, Firewalls und anderen Netzwerkgeräten? Welche sicherheitsrelevanten Probleme ergeben sich durch den Parallelbetrieb von IPv4 und IPv6 auf den Geräten in der Übergangsphase?

**A1:**

Die Hersteller gehen nun immer vermehrt daran, IPv6 in ihre Geräte zu implementieren, doch durch das immer noch erscheinen von neuen Normen (RFC's) sind auch diese teilweise verunsichert, oder noch sie bringen Produkte auf den Markt, die bei erscheinen schon nicht mehr den Aktuellen Normen entsprechen, und dann aufwendig angepasst werden müssen.

Die immer noch neu erscheinenden Normen zeigen auch, dass die schon 15 Jahre zurückliegende Grundversion den heutigen Anforderungen an Sicherheit und Funktion nicht mehr genügt. So dass Sich in diesen Bereichen immer noch starke Entwicklungen und Fortschritte ergeben, die dann auch entsprechend umgesetzt werden.

Die Implementationen in Security Netzwerkgeräten, wie Firewalls, sind aber zurzeit noch rudimentär, sie erfüllen knapp die "Basic" Funktionen, die von den Kunden gefordert werden. Erweiterte Funktionen sind nicht, oder nur teilweise implementiert, diese werden aber von den Kunden gefordert und schrittweise dann auch implementiert. Hier zeigt es sich aber, dass auch die Hersteller nicht genau wissen, was und welche Funktionen notwendig oder wichtig sind, bzw. wie der Schutz wirksam ungesetzt werden kann.

Die Entwicklungsabteilungen sind noch nicht richtig mit IPv6 vertraut, weil sie zuwenig Wissen im IPv6 Umfeld haben, und schlicht die Erfahrung fehlt, wie man das Umsetzt, denn es ist für alle Neuland. Bei IPv4 dauert diese Entwicklung ja auch noch an, so ist anzunehmen, dass es bei IPv6 auch Jahre gehen wird.

**A2:**

Beim Parallel Betrieb von IPv6 und IPv4 ergibt sich Grundsätzlich mal auf allen Stufen, das gleiche Problem, der doppelte Aufwand für alles, sei das Firewall Funktion, Web Services oder Applikationen.

Es besteht hier die grössere Möglichkeit, dass etwas vergessen oder nicht berücksichtig wird.

Die Meisten Betriebssysteme unterstützen heute schon IPv6, das gilt sowohl für klassische Clients und Server, wie für all die Mobile Geräte, und ist auch meistens schon per "Grundeinstellung" eingeschalten.

Auch wenn die meiste Kommunikation heute nur via IPv4 geht, so besteht immer noch die Möglichkeit, dass ein Angreifer diese IPv6 Funktion nutzt, dies ist vor allem beispielsweise im Wirelessumfeld denkbar, wo der Angreifer seine IPv6 Infrastruktur aufbaut, uns versucht, denn Datenverkehr auf IPv6 umzulenken, um so an Informationen zu gelangen. Diverse Scenarien sind auch schon erfolgreich umgesetzt worden.

Auch je nach Übergangslösung, können auch neue Unsicherheiten auftauchen. Der User sieht beispielsweise nicht, über welches Protokoll er mit einer Webseite kommuniziert, dh. ss kann dort versucht werden, wenn die Hauptkommunikation via IPv6 erfolgt, auch ein Zugriff via IPv4 zu erzwingen, so dass einen Zuordnung von IPv4 und IPv6 Adresse möglich ist. Einige Dualstack Implementationen wie 6RD (Rapid Deployment) haben eine direkte Abhängigkeit von des verwendeten IPv6 Prefixes und der IP Adresse des End User Routers (CPE), so dass auch hier Rückschlüsse gezogen werden können.

Weitere Lösungen wie NAT64, wo der Provider einen Übergang zwischen der IPv6 Welt seiner Kunden und der alten IPv4 Welt herstellt, bringen Probleme mit Zertifikaten von alten IPv4 Servicen und dem NAT hervor, die allenfalls missbraucht werden könnten.

Alle diese Punkte, sowie weitere hier nicht genannte, zeigen deutlich, dass sich die Entwickler, Techniker und Anwender noch nicht dem Ausmass der Security Probleme bewusst sind, oder schon gar alle spezifiziert wären, sowie für viele Punkte noch keine annehmbare und sichere Lösung vorhanden ist.