System-Information: Zugangssystem aMOX (abcon memory-only-linux)

Die grundsätzliche **Aufgabenstellung** besteht darin, **Zielsysteme**, welche traditionell über Jahre/Jahrzehnte hinweg in einem abgeschotteten Bereich gelaufen sind, **von extern (über Internet) hardware-basierend erreichbar zu machen**. War früher der Zugang physikalisch exakt bestimmt und somit reglementiert, so verschiebt sich diese Grenze zunehmend in den logischen/virtuellen Bereich; physikalisch brauchen die Geräte jedenfalls Zugang zu externen Netzen. Die **Herausforderung** besteht darin, den logischen Zugang gekonnt einzuschränken. Richtschnur ist eine sinnvolle **Balance zwischen notwendigem Sicherheitslevel und dem damit einhergehenden Aufwand**:

- wie "einfach" kann sich der Benutzer mit dem System verbinden?
- wie „einfach“ ist die Verwaltung des Zugangs (Erfüllung der Sicherheitsanforderung und Ausfallssicherheit)?

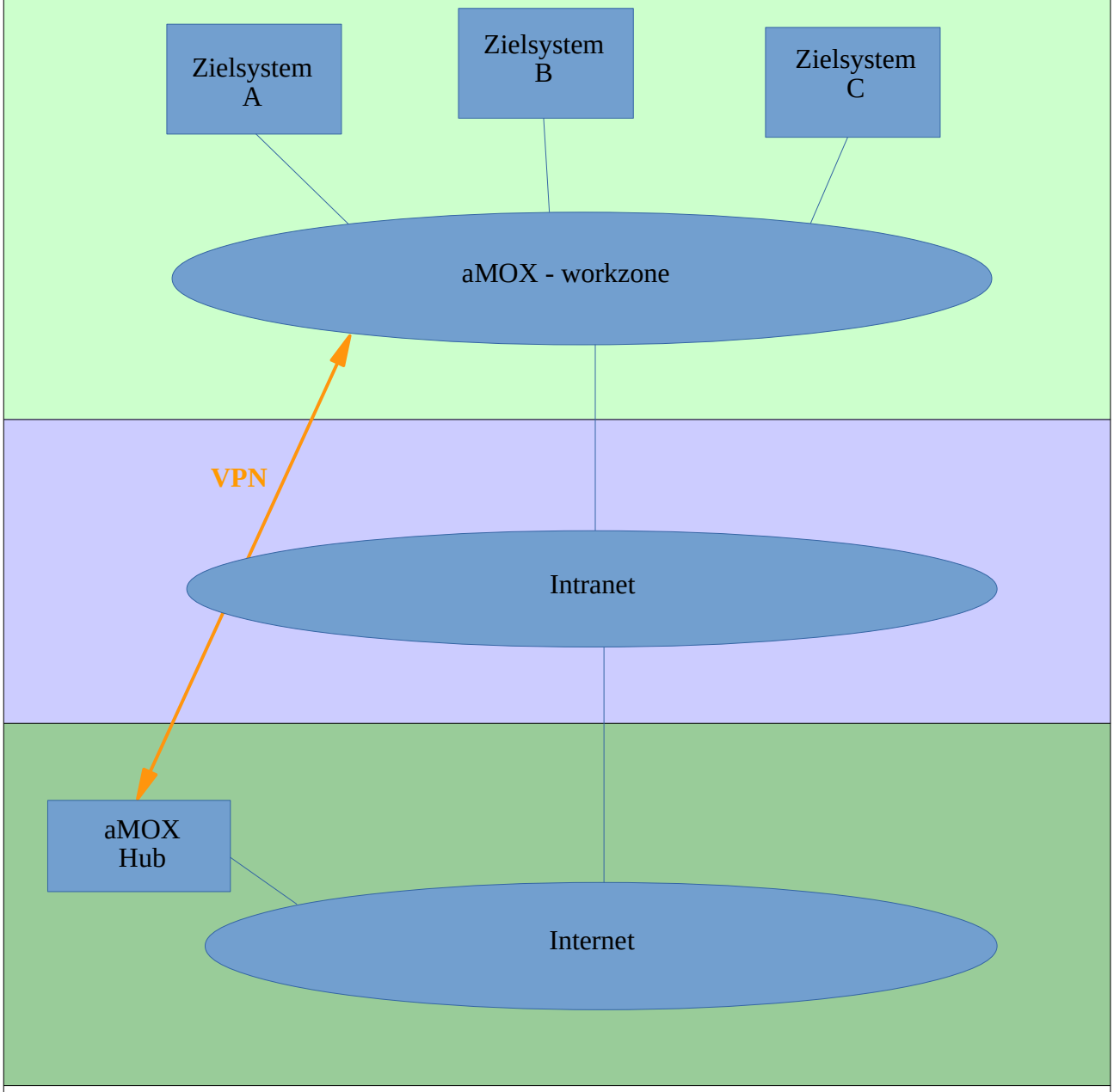
Exkurs

Aus technischer Sicht ist es ratsam, das Zielsystem mit seiner Kernaufgabe von den Aufgaben eines externen Zugangs los zu lösen. Das Zielsystem muss also den Zugang von extern nicht selbst verwalten, sondern diese Aufgabe wird von einem dafür speziell eingerichteten System, dem sogenannten Zugangssystem (zB aMOX) bewerkstelligt. Externer Zugang sowie Kernaufgabe bleiben somit physikalisch als auch logisch auf jeder Ebene klar getrennt. Damit kann verhindert werden, dass externe Zugangsprozeduren aufgrund Einschränkungen durch das Zielsystem (zB Designfehler bei angebotenen Diensten wie Webserver etc.) keine Einbußen zu Lasten der Sicherheit erleiden. Gleichzeitig kann der externe Zugang kein unnötiges Ausfallrisiko für das Zielsystem darstellen (Überlastung des Zielsystems durch den externen Zugang). aMOX bietet darüber hinaus die Möglichkeit einer gesicherten, lokalen Netzwerk-Zone (workzone), welche für eine beinahe unbegrenzte Anzahl an Zielsystemen (Cluster) zur Verfügung stehen kann, und welche diese vor jeglichen Angriffsvektoren aus dem Netz (uplink) schützt. Es ist davon auszugehen, dass ein heute als sicher eingestuftes Zugangssystem in ein paar Jahren Sicherheitslöcher aufweisen wird. Fortlaufende Adaptionen des Zugangsystems bleiben unausweichlich und können unabhängig vom Zielsystem durchgeführt werden. Das Zielsystem kann fortwährend seine eigentliche Aufgabe stabil und robust erfüllen.

aMOX bringt 20 Jahre Erfahrung in linuxbasierender Netzwerktechnologie

- Server-basierte, vollautomatisierte VPN-Verbindung (state-of-the-art) für externen Zugang und/oder lokaler Zugang
- Zugangs- und Systemverwaltung
  - Zertifikat- und Schlüsselverwaltung
  - User-Logins mit Zugriffsberechtigungen
- Tools
  - Automatisiertes Backup-System
  - Automatisiertes Einspielen von Updates
  - Deployment-Prozess für neue Systeme
  - Desaster/Fallback und full-recovery-Routinen in wenigen Minuten
  - Diverse Hilfsmittel zur Fehlerbehebung
  - Weitere Möglichkeiten zur Fernwartung (spezielles Wartungs-VPN mit Bridge-Funktionaltät für quasi-Intranet)
- Features
  - Einfache Austauschbarkeit des Zugangssystem bei Sicherheitslücken - Zielsystem arbeitet davon unberührt weiter
  - Bessere Skalierbarkeit: man kann das Zugangssystem jederzeit ersetzen, falls es hardwaremässig zu klein dimensioniert sein sollte → aMOX kann auf jede HW, die von Linux unterstützt wird, aufgesetzt werden

Möglicher Systemaufbau mit aMOX (vereinfachte Darstellung)



Folgende HW-Systeme hat abcon als Endgeräte in Einsatz gebracht:	
aPIMOX: raspberry-pi	 
aAMOX: APU.2C2 ALIX.2D13