Aktuelles zu Network and Communication Services

85. DFN-Betriebstagung | 6.10.2026

Stefan Piger

Agenda

I. Housekeeping

II. Stand Leistungssteigerung DFN-Internet & Erneuerung Zugangsnetz

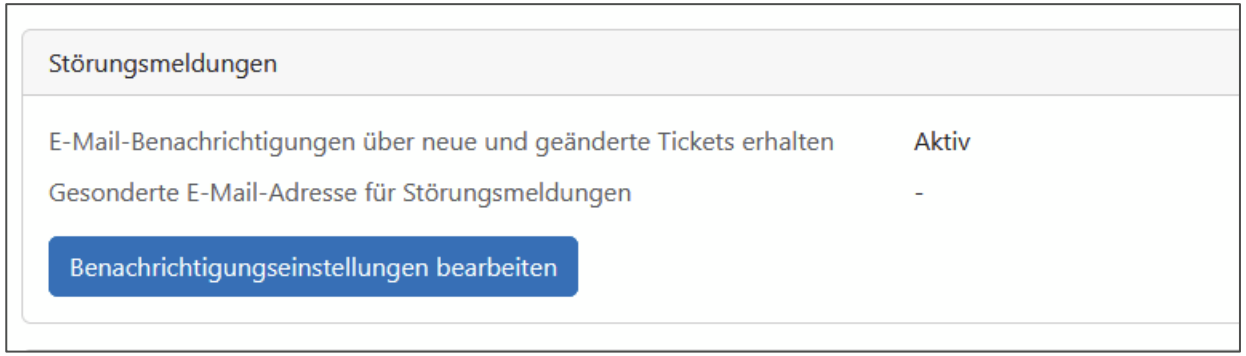
III. Kernnetz

Housekeeping

Teilnehmerportal – Neue Features



- „Default-“Wunsch: Aktualisieren Sie bitte Ihre Kontaktinformationen!
- Anzeige von Cluster- und Versorger-Strukturen
- Information über Ticketeröffnungen und Status-Updates zu Tickets
  - Jede(r) Portal-Nutzende kann diese Funktion individuell für sich aktivieren
  - Zusätzlich gibt es die Option eine weitere E-Mail-Adresse zu hinterlegen



Absicherung von Legacy IP-Adressraum

- BGP Hijacking und Route Leaking bedrohen Erreichbarkeit von Einrichtungen.
  - Mit RPKI existiert eine Abhilfe für diese Probleme.

- Aber: Viele Einrichtungen am X-WiN haben Legacy IP-Adressbereiche.
  - Route Origin Authorizations (ROAs) dürfen nicht ohne Bindung an RIPE angelegt werden.

- Es gibt Möglichkeiten RIPE-Services für Legacy IP-Adressraum zu nutzen.
  1. Einrichtung wird RIPE NCC Mitglied und registriert den Legacy IP-Adressraum selber.
  2. Einrichtung schließt ein Sponsoring LIR Agreement mit dem DFN-Verein.

- **Keine Lösung**: **Status Quo** bestehen lassen
  - Sprechen Sie für eine individuelle Beratung **hostmaster@dfn.de** an!

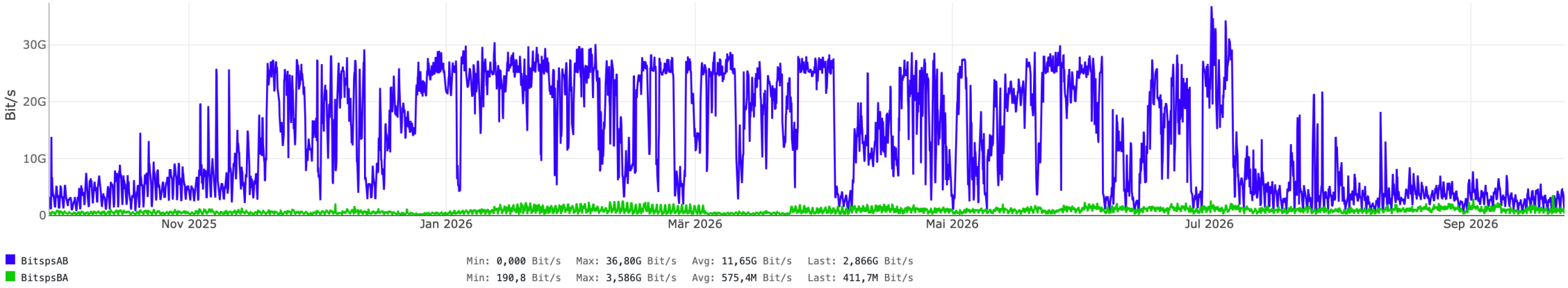
Legacy IP-Adressraum – Es geht voran, aber…

- Seit Mai 2026 wurden **22 Adressbereiche** (17 x /16, 5 x /24) bereinigt.
  - Hilfreich war hierzu auch ein Rundschreiben zum Thema von RIPE.
- Einrichtungen haben **überwiegend** die Option „**Sponsoring-LIR**“ gewählt.
  - Zwei Einrichtungen sind selber RIPE-Mitglied geworden.
- Die DFN-GS ist aktuell mit **fünf Teilnehmern** im Gespräch.
- Zu weiteren **23** Legacy-Adressbereichen gibt es noch **keine Kontakte**.
  - DFN-GS wird jeden betroffenen Teilnehmer nochmals anschreiben.

KI & Datenverkehr – Was kommt evtl. auf Sie zu?

- Bis Ende 2025 keine auffälligen Transfers mit eindeutigem KI-Bezug

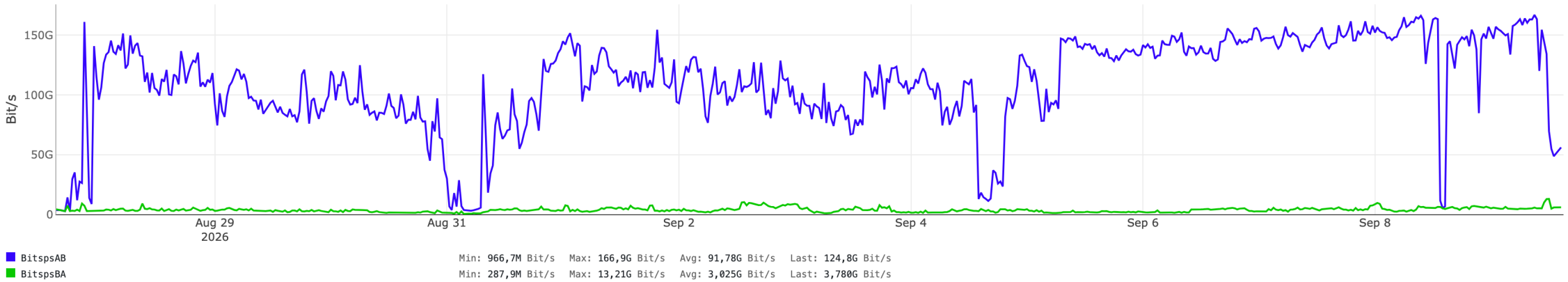
- Beispiel 1 – Universität kopiert KI-Trainingsdaten aus bei Microsoft gehostetem Repository



KI & Datenverkehr – Was kommt evtl. auf Sie zu?

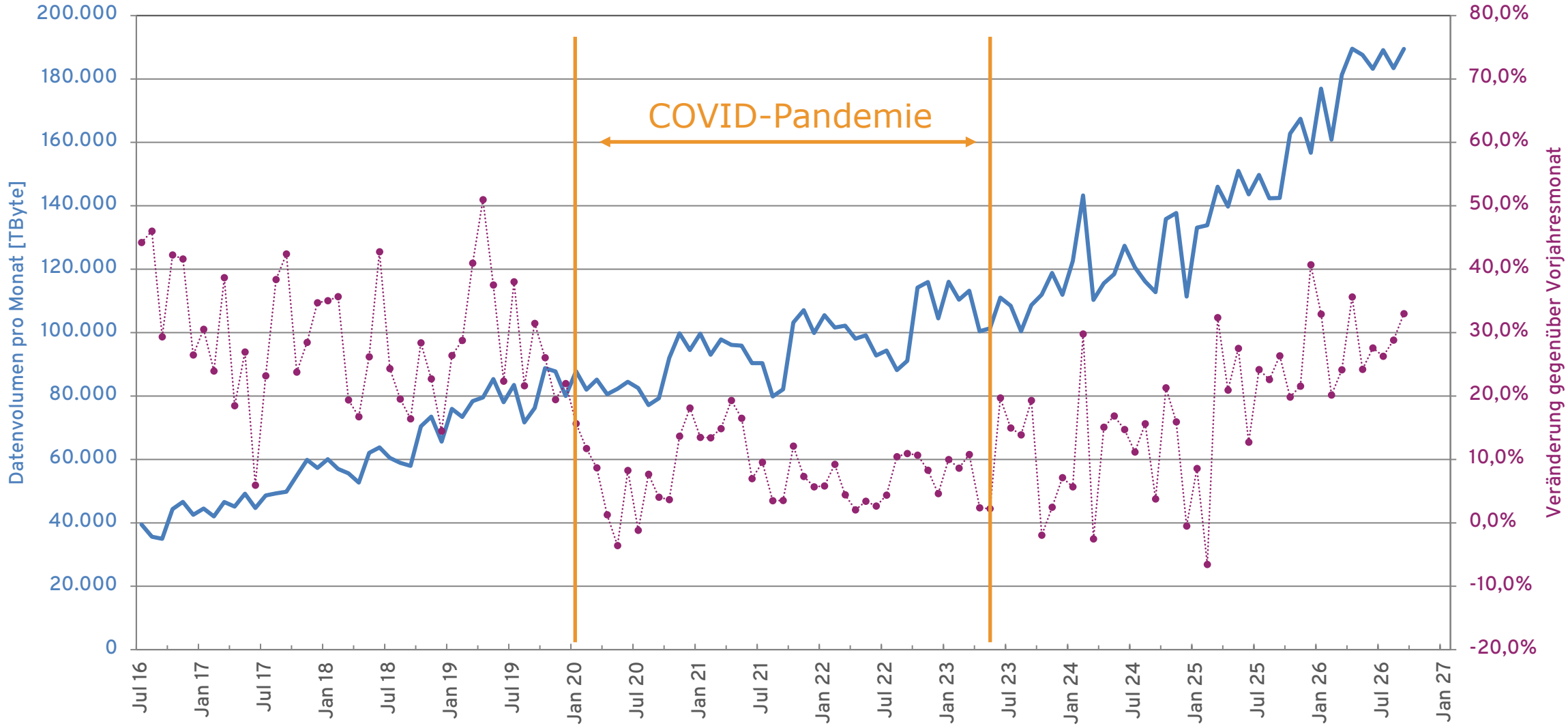
- Bis Ende 2025 keine auffälligen Transfers mit eindeutigem KI-Bezug

- Beispiel 2 – Forschungseinrichtung kopiert ca. 10 PB von Grass Foundation



Stand Leistungssteigerung DFN-Internet & Erneuerung Zugangsnetz

Warum Leistungssteigerung? Entwicklung Datenvolumen…



Leistungssteigerung – Aktueller Stand

- Bisher **676** Rückmeldungen auf Informationsmails erhalten.
  - **572** Teilnehmer nehmen Leistungssteigerung an.
  - 38 Teilnehmer wünschen Verschiebung der Realisierung der Leistungssteigerung oder haben den Dienst in der Zwischenzeit beendet.
  - 58 Teilnehmer wünschen Beibehaltung der bisherigen Bandbreite.

- **38** Teilnehmer haben nicht geantwortet.

- Für **564** Dienste wurde die Leistungssteigerung bereits umgesetzt.

Erneuerung Zugangsnetz

- Anbindung an das Kernnetz erfolgt in zwei Varianten:
  - Teilnehmer **mit direkter Anbindung** („Anwenderkabel“), für diese werden lokale Router-Interfaces oder DWDM-Verbindungen benötigt
  - Teilnehmer **mit Carrier-Verbindung** („Teilnehmeranbindung“), für diese mussten neue Verbindungen beauftragt werden
- Aktueller Stand
  - **969** Verbindungen wurden bisher beauftragt,
    - davon 662 **neu** zu realisierende.
  - **849** Verbindungen wurden bisher übergeben,
    - davon 559 **neu** zu realisierende.
- Mittlere Bereitstellungszeit liegt bisher bei etwa 260 Tagen.

Was dauert da so lange? Es sind nicht nur die Carrier…

- Fall 1: (26 Monate und kein Ende absehbar)
  - Freigabe Campusverkabelung erst erteilt nach Rückbau Alt-Technik des Carriers
  - Versorgungsschächte abgesackt bzw. eingestürzt
  - Umstellung Stadt IT-Systeme -> keine Freigaben / verkehrsrechtliche Anordnungen (VAO)

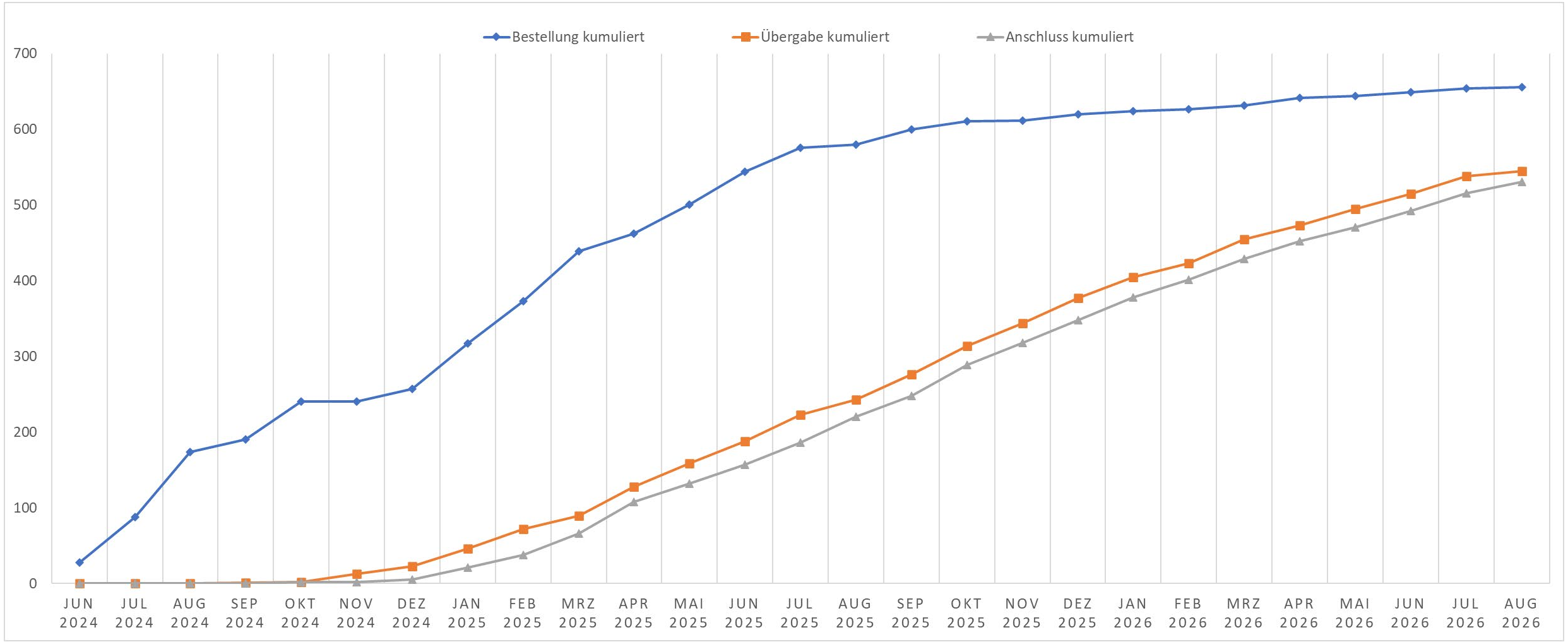
- Fall 2: (12 Monate und kein Ende absehbar)
  - Abstimmung Sicherheitsvorgaben des Teilnehmers
  - Inhouse-Verkabelung einbetoniert (Sicherheitsvorgaben RZ), keine Neuverlegung möglich
  - Abstimmung Heißumschaltung vorhandener IVK zwischen zwei Vorgänger-Carriern und einem Nachfolger-Carrier

- Fall 3: (18 Monate, aber übergeben und seit gestern in Betrieb!)
  - Absacken Schacht
  - Verkehrsbetriebe erteilen fünf Monate lang keine Freigabe für Reparatur

Was dauert da so lange? Es sind nicht nur die Carrier…

- Vermieter verweigert seit über einem Jahr Gebäudeeigentümererklärung
- Denkmalschutz verursacht über 1 Jahr Verzögerung; nachfolgend Insolvenz des Generalunternehmers für das Bauvorhaben
- TNA bis zur Grundstückgrenze durch Carrier fertiggestellt; Freigabe des staatlichen Eigentümers für die weitere Verlegung wurde verweigert
- Tiefbauvorgaben der Gemeinde (Kabelpflug) mit archäologischer Begleitung
- Gerüst auf Schacht / Muffe
- Keine Freigabe des Eigentümers wegen denkmalgeschütztem Rosengarten

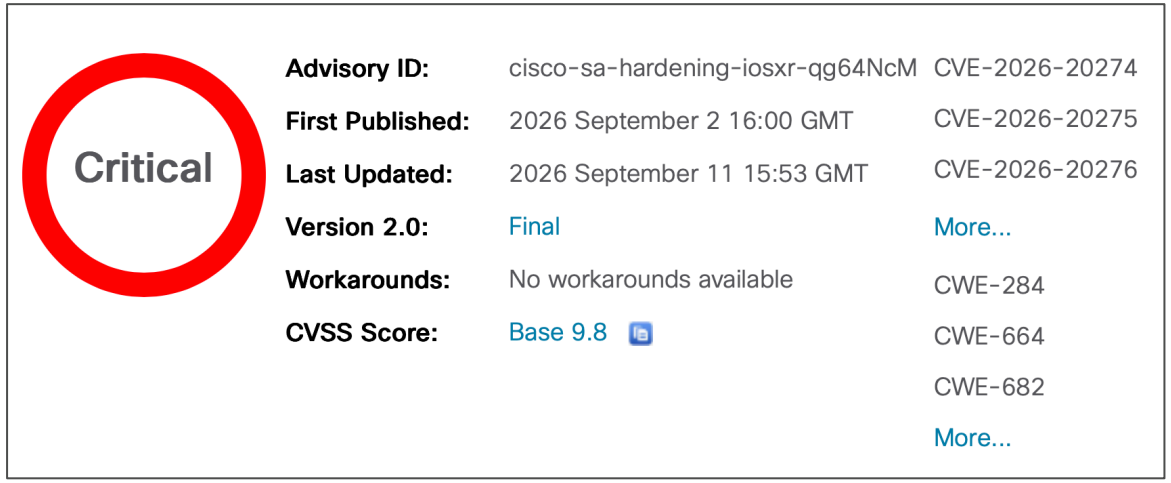
Erneuerung Zugangsnetz – Zeitlicher Verlauf



Kernnetz

IP-Plattform – Aggregationsplattform

- **Security Vulnerabilities** in aktuell auf der **Aggregations-Plattform** eingesetzter **IOS-XR** Version
- Workarounds?
  - „There are no workarounds that address these vulnerabilities."
- Wie hoch ist die Dringlichkeit?
  - „These vulnerabilities were found during internal testing and are not known to be actively exploited."
  - Aber…



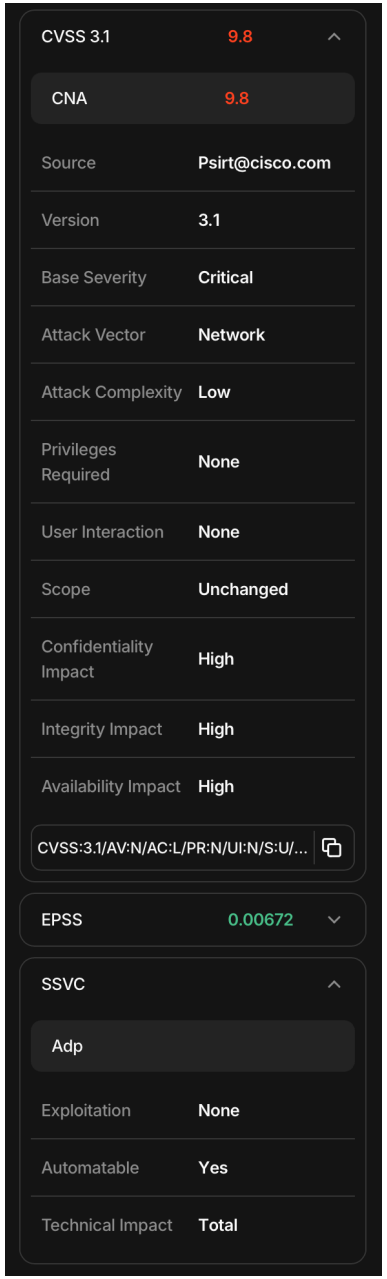
Quelle: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxr-qg64NcM#vp

IOS-XR – Einschätzung der Schwachstellen

- Enthaltene CVEs

CVE ID	Highest CVSS Score	Vulnerability Class (Highest-Level CWE)	Description
CVE-2026-20274	9.8	CWE-664	Improper control of a resource through its lifetime (covers buffer copy without checking size of input, stack-based buffer overflow, heap-based buffer overflow, out-of-bounds read, use of externally-controlled format string, numeric truncation error, use after free, exposure of resource to wrong sphere, operation on a resource after expiration or release, allocation of resources without limits or throttling, out-of-bounds write, use of out-of-range pointer offset, and initialization of a resource with an insecure default)
CVE-2026-20275	8.8	CWE-682	Incorrect calculation (covers incorrect calculation of buffer size, integer overflow or wraparound, and integer underflow (wrap or wraparound))
CVE-2026-20276	8.6	CWE-691	Insufficient control flow management (covers reachable assertion and loop with unreachable exit condition)
CVE-2026-20277	8.2	CWE-693	Protection mechanism failure (covers use of insufficiently random values)
CVE-2026-20278	8.8	CWE-707	Improper neutralization (covers improper neutralization of special elements used in a command, improper neutralization of directives in dynamically evaluated code, improper validation of array index, improper validation of specified quantity in input, and improper validation of specified index, position, or offset in input)
CVE-2026-20279	9.8	CWE-284	Improper access control (covers improper certificate validation, missing authentication for critical function, missing authorization, and incorrect authorization)
CVE-2026-20280	8.8	CWE-703	Improper check or handling of exceptional conditions (covers improper handling of length parameter inconsistency and not failing securely)

- Keine weiteren Details von Seiten Cisco zur Einschätzung der Kritikalität
- Auf vulners.com findet sich zu CVE-2026-20274 diese Klassifizierung



Aggregations-Plattform – Was tun?

- Faktenlage gebietet **zeitnahes Einspielen der Security-Patches**

- Zu diesem Zeitpunkt ist auch ein Upgrade auf eine neue Major-Release in Vorbereitung.

- Daher **zwei Optionen** für weiteres Vorgehen:
  1. Einspielen von Security-Patches für aktuelle Software-Version
  2. Upgrade auf neue Major-Release (einschließlich Security-Patches)

- **Entscheidung für Option 2** nach Klärung offener Punkte mit Cisco-TAC.

Wie schnell müssen die Upgrades durchgeführt werden?

- Aggregations-Plattform umfasst **56 Systeme**.

- Option 1: Business As Usual
  - Vorgehen: Upgrades zweier Router an drei Tagen pro Woche jeweils zwischen 5:30 und 7:30
  - Szenario: Es sind keine Exploits verfügbar, Schwachstellen werden nicht ausgenutzt

- Option 2: As Soon As Possible
  - Vorgehen: Upgrades auch tagsüber und am Wochenende, ohne Rücksicht auf Verfügbarkeit von Teilnehmer-Diensten
  - Szenario: Exploits sind verfügbar, Schwachstellen werden aktiv ausgenutzt

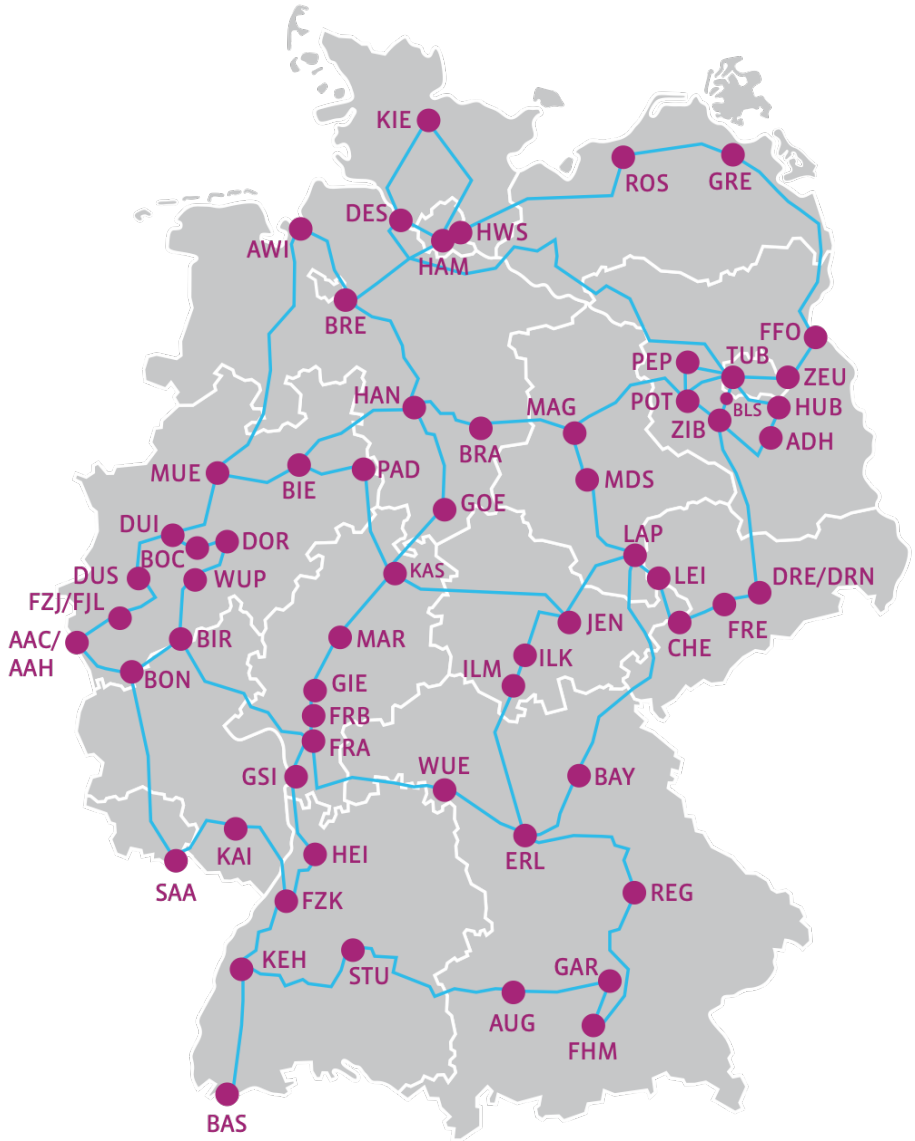
- Option 3: So schnell wie möglich, aber zu Randzeiten mit Option auf Eskalation
  - Vorgehen: Upgrades jeweils zweier Router an fünf Werktagen pro Woche morgens und abends
  - Szenario: Verfügbarkeit von Exploits noch nicht gegeben, zeitnahes Ausnutzen aber nicht ausgeschlossen

Entscheidung für Vorgehen nach Option 3

- 14.9.26: Erstes Upgrade eines Produktions-Routers
  - Upgrade war erfolgreich!
- Weiteres Vorgehen: Vier Upgrades pro Werktag
  - Wartungsmeldungen nach initialer Phase wie gewohnt mit einer Woche Vorlauf
  - Kontinuierliche Beobachtung der Sicherheitslage durch DFN-GS und DFN-CERT
  - Bei Verschärfung der Lage Vorgehen nach Option 2, d.h. Upgrades auch tagsüber und am Wochenende
- Bisher keine Meldungen über Ausnutzung der Schwachstellen.
- Letztes Upgrade an einem System ist für heute Abend terminiert.

X-WiN Kernnetzknoten

- Außerbetriebnahme von Oldenburg (EWE) am 14.7.26
  - Kündigung durch Standort
  - Teilnehmeranbindungen nach AWI, BRE und MUE migriert
  - Kernnetzverbindungen nach AWI und MUE durchgeschleift und mit weiterem ILA-Standort verstärkt
- Außerbetriebnahmen von ADH und HUB erfolgen zeitnah
  - Letzte VPN-Verbindung ist zum 1.10. außer Betrieb gegangen.
- Umzüge
  - Alt-Standorte FRA, FZK und GOE beräumt
  - JEN und HAM weiter in Arbeit



Neuer Peering-Knoten in Berlin

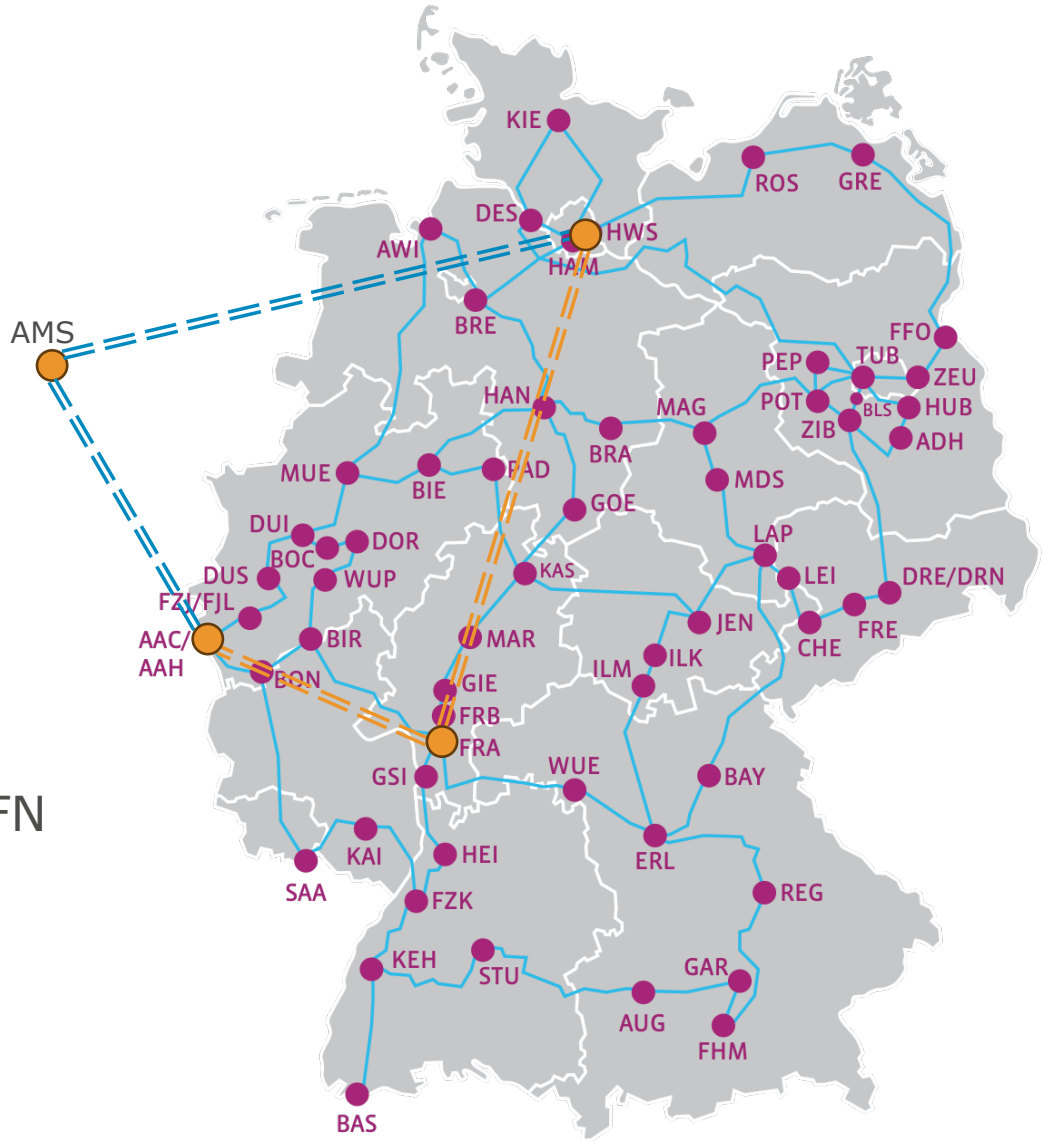
- Ziel: Erhöhung der Peering-Redundanzen
- Berlin bietet sich als Peering-Standort in Deutschland an.
  - Lage im Osten Deutschlands -> gute Ergänzung zu bestehenden Peering-Standorten
  - Verfügbarkeit von relevanten Peering-Partnern
- Einbindung in Faserplattform einfach
  - Standort liegt an Glasfaserstrecke TUB <-> ZIB
- Stand Aufbau und Inbetriebnahme – erledigt ☑



Spectrum Sharing mit SURF

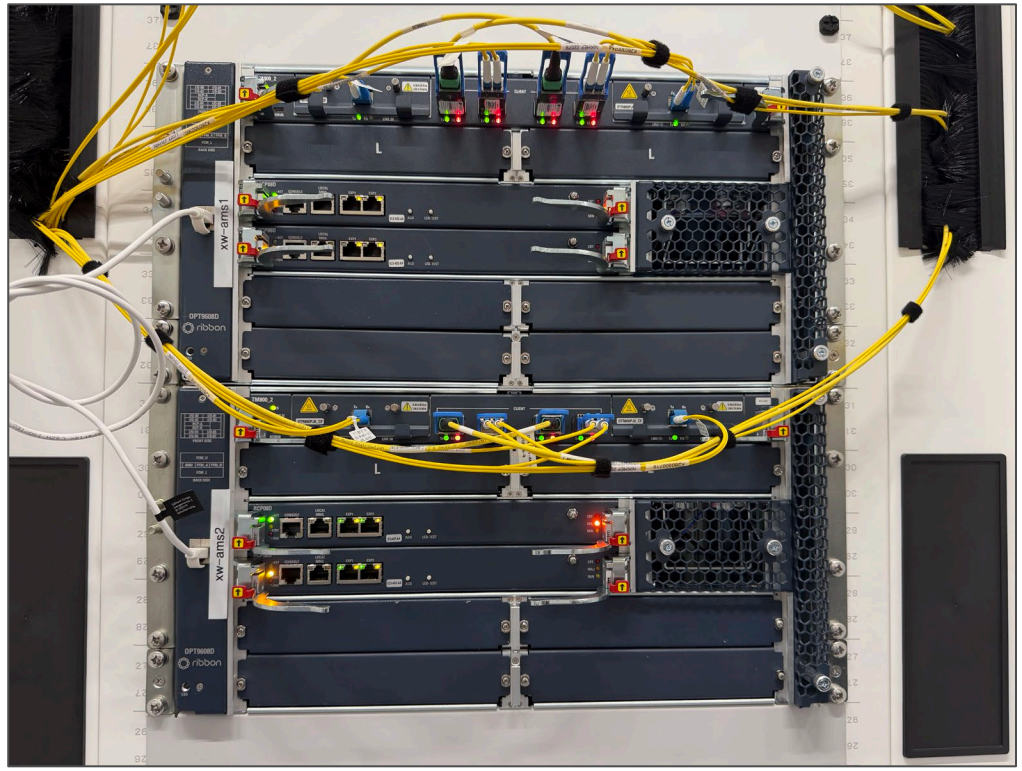
- Ziele des Projekts:
  - DFN: Netzknoten in Amsterdam, um weitere PNI und Redundanz zu DE-CIX über AMS-IX realisieren zu können
  - SURF: Netzknoten in Frankfurt für Anbindung an DE-CIX und Backbone-Redundanz

- Vorgehen:
  - Kopplung der Netzinfrastrukturen von SURF und DFN über benachbarte Knoten in Aachen und Hamburg.
  - Bereitstellen von 450 GHz Spektrum auf blauen Strecken (SURF für DFN) bzw. orangenen Strecken (DFN für SURF).

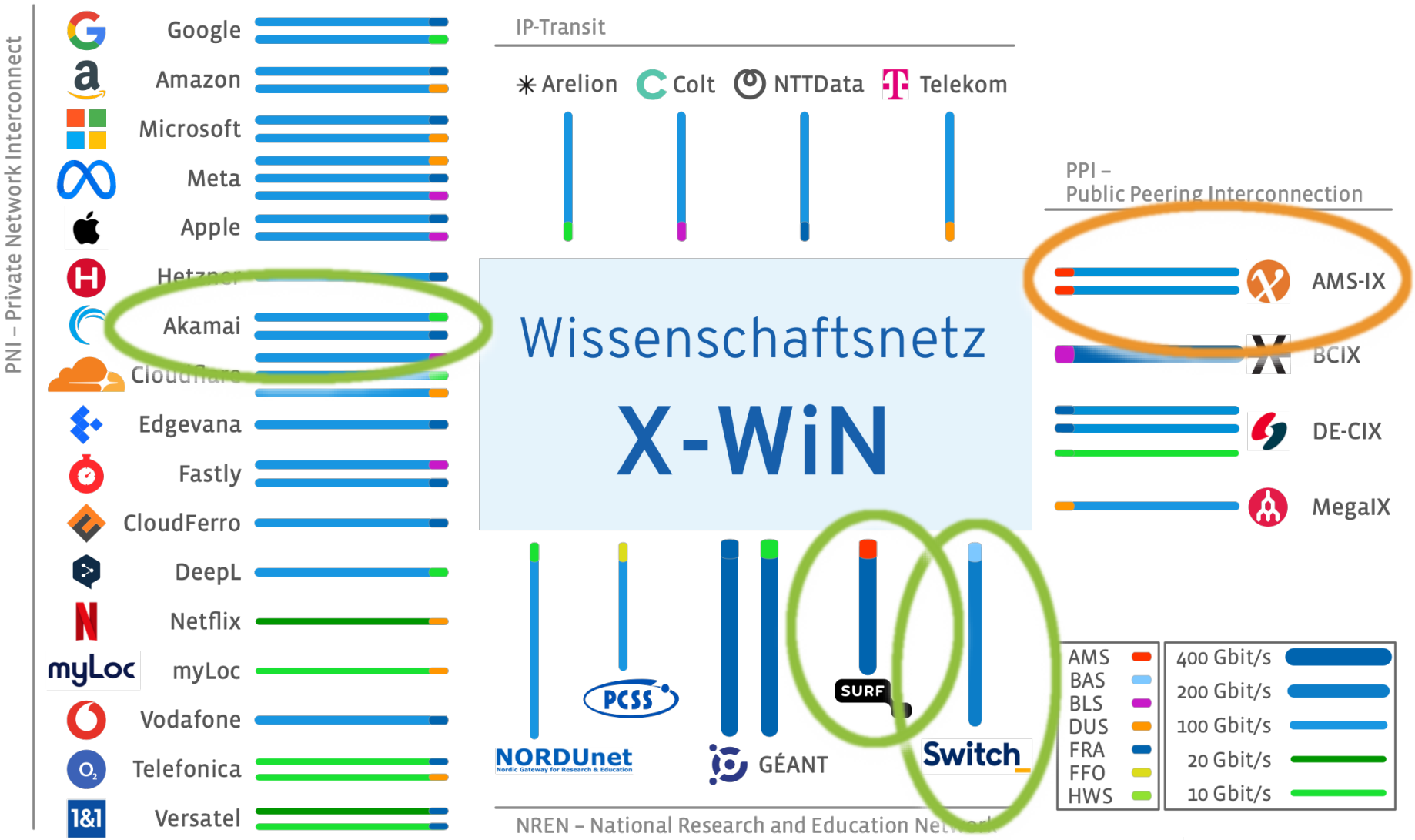


Neuer Peering-Knoten in Amsterdam

- DFN-Knoten in Amsterdam: „Nur“ DWDM-Technik
  - Management-Karten und Muxponder
  - keine Verstärker oder ROADMs
- Konnektivität nach Amsterdam
  - Beleuchtung beider Strecken (AMS-AAC und AMS-HWS) mit je zwei Verbindungen à 800 Gbit/s.
  - Dritter 150 GHZ-Kanal auf beiden Strecken dient als Reserve.
  - Die Verbindungen terminieren auf der IP-Plattform in Hamburg (HWS) und Essen (DUI).
- Stand Aufbau und Inbetriebnahme – erledigt ☑



X-WiN Außenanbindungen

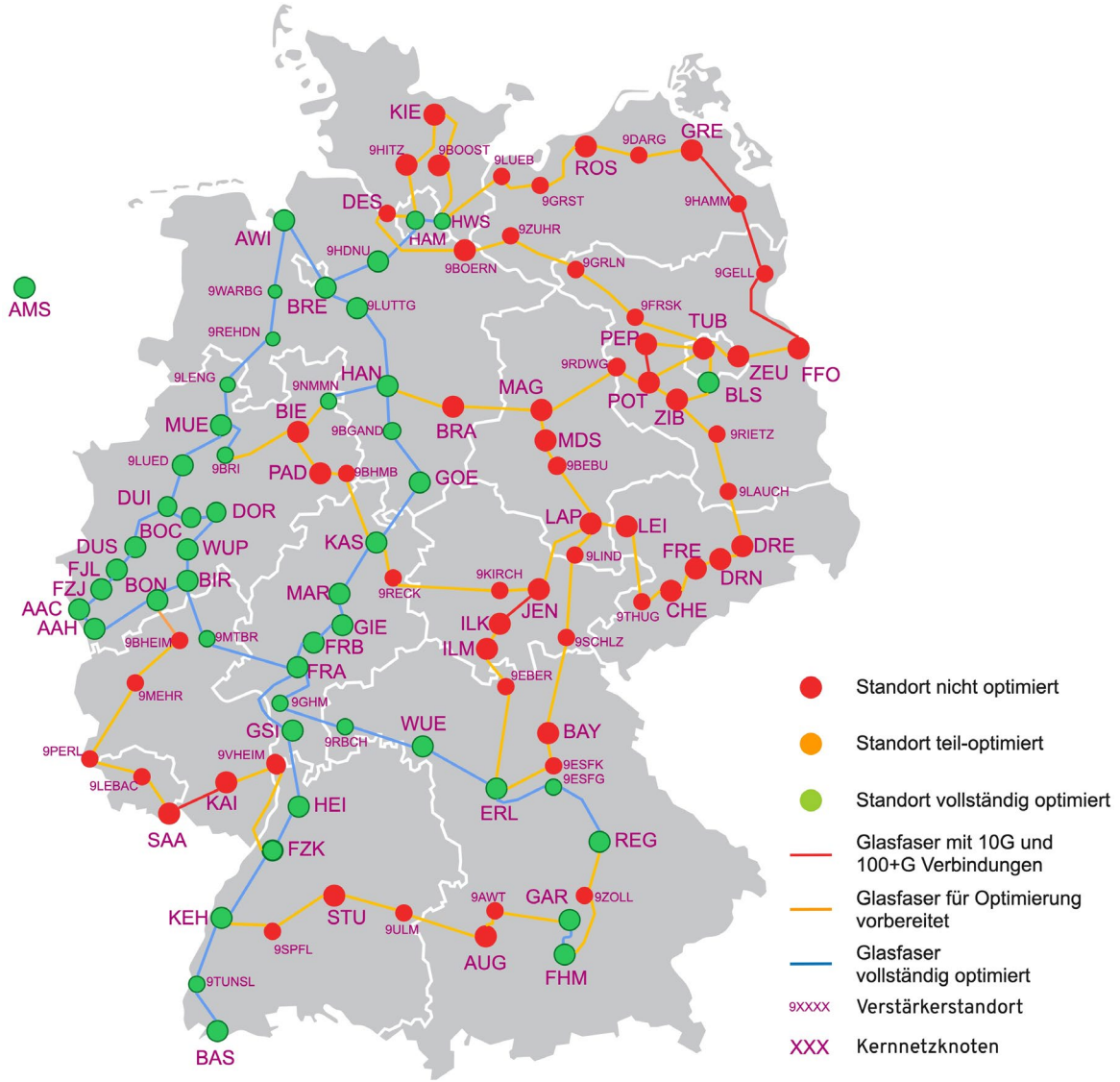


Projekt X-WiN All-Coherent

- Ziel: Optimierung OSNR für neue/kommende Übertragungstechniken (≥800G)

- Vorgehen: Umbau der Optischen Plattform auf rein kohärentes Line-System
  - Schritt 1: Migration der 1G- und 10G-Verbindungen auf IP-Plattform oder auf 100G-Verbindungen auf der Optischen Plattform.
  - Schritt 2: Entfernung der DC-Module und Austausch der Line-Verstärker an allen Standorten. Alle Arbeiten werden abends ab 21 Uhr durchgeführt.

- Stand: **49** von **113** Standorten optimiert



Forum Wissenschaftsnetz – morgen 9:00-11:00

- **Teilnehmeranbindungen – Learnings aus Realisierung und Betrieb**
  - Daniel Micklisch, Robert Stoy | NACS | DFN-Geschäftsstelle
- **DNSSEC**
  - Ulrich Wisser | Technical Engagement Manager, Europe | ICANN (Internet Corporation for Assigned Names and Numbers) | Schweden
- **Netzsicherheit – Mehr Nutzer. Weniger Bots: wie das DESY unerwünschten Traffic aussperrt**
  - Moritz Hamminger | Netzwerkmanagement | DESY - Deutsches Elektronen Synchrotron | Hamburg
- **Lifecycle and Automation - A Datacenter Network Journee**
  - Marc André Orians | Teamleiter Datacenter Network | DKFZ – Deutsches Krebsforschungszentrum | Heidelberg

Haben Sie noch Fragen?

- Kontakt
  - Dr.-Ing. Stefan Piger
    Bereichsleiter Network and Communication Services

    E-Mail: piger@dfn.de
    Telefon: +49 30 884299-329

    Anschrift:
    DFN-Verein, Geschäftsstelle
    Alexanderplatz1
    10178 Berlin

