September 2026

ComConsult
BERATUNG • PLANUNG • SCHULUNG

Der Netzwerk Insider

Mit Quantum Key Distribution zum sicheren Schlüsselaustausch

von Dr. Philipp Rüßann

Quantencomputer stellen eine Gefährdung für unsere derzeitige asymmetrische Verschlüsselung dar und erfordern schon heute dringendes Handeln. Bestehende Sicherheitsmechanismen können jedoch resistenter gegen Angriffe durch Quantencomputer aufgestellt werden.

Seite 10

Wird MPLS durch SRv6 abgelöst?

von Dr. Behrooz Moayeri

In den letzten 25 Jahren wurden viele Netze auf Basis von Multi-Protocol Label Switching (MPLS) realisiert. Dieses Vierteljahrhundert war eine einzige Erfolgsgeschichte einer Technologie, die binnen kurzer Zeit zum dominierenden Verfahren für skalierbare Netze wurde. Nun wird in der Netzbranche darüber diskutiert, ob MPLS in absehbarer Zeit durch Segment Routing auf IPv6-Basis (SRv6) abgelöst wird.

Seite 2

Wenn Excel zur Schatzkarte wird

Warum gute IT-Dokumentation mehr wert ist als jede Hardware

von Ben Grünbauer

Ich glaube, jeder Arbeitnehmer in der IT kennt diese Situation. Egal, ob in einer beratenden Rolle oder als ausführende Kraft: Irgendwann steht man vor einer Excel-Tabelle, die vermutlich schon mehrere Generationen an Administratoren überlebt hat.

Seite 21

Webinar der Woche

Erste Hilfe für echte Schmerzen im IT-Projekt.

Seite 20

Kostenschätzungen für Rechenzentrums-Infrastruktur

in Zeiten steigender RAM-Preise

von Dr. Markus Ermes

Ich habe bereits darüber geschrieben – so wie auch Dr. Moayeri in seinem Beitrag. Die Aussichten waren und sind nicht unbedingt rosig: Preise für Arbeitsspeicher und SSDs, egal ob im Privat- oder Unternehmensumfeld, kennen aktuell nur eine Richtung, und zwar nach oben.

Seite 30

Wird MPLS durch SRv6 abgelöst?

von Dr. Behrooz Moayeri

In den letzten 25 Jahren wurden viele Netze auf Basis von Multi-Protocol Label Switching (MPLS) realisiert. Dieses Vierteljahrhundert war eine einzige Erfolgsgeschichte einer Technologie, die binnen kurzer Zeit zum dominierenden Verfahren für skalierbare Netze wurde. Nun wird in der Netzbranche darüber diskutiert, ob MPLS in absehbarer Zeit durch Segment Routing auf IPv6-Basis (SRv6) abgelöst wird.

Was ist SRv6?

Mein Kollege Dr. Dams hat bereits in einem Beitrag unter anderem über SRv6 geschrieben. An dieser Stelle nur eine kurze Antwort auf die Frage, was SRv6 ist:

SRv6 ist die auf IPv6 basierende Ausprägung von Segment Routing (SR). Beim Verfahren SR kann der erste Router im Übertragungspfad eine Liste von Segmenten vorgeben. Die nachfolgenden Router im Pfad halten sich an der vorgegebenen Segment-Liste als Anweisung für die Weiterleitung des Datenpakets. SRv6 nutzt den Umstand der Erweiterbarkeit von IPv6-Headern. Diese nehmen bei SRv6 die Liste der Zwischenstationen auf dem Übertragungspfad auf.

Solange es in Netzen nur IPv4 gab, erlaubte der begrenzte Adressraum keine Nutzung von IP-Adressen als sogenannte Segment-Identifier (Segment ID, SID). Die IPv4-Welt ist seit Jahrzehnten eine fragmentierte, weil die maximal möglichen ca. 4 Milliarden IPv4-Adressen keine eindeutige Abbildung aller Endgeräte und Netzknoten erlauben, zumal die Zuteilung der IPv4-Adressen in den letzten 50 Jahren alles andere als sparsam erfolgt ist. Mit IPv6 ist es möglich, auf absehbare Zeit alle zu vernetzenden Objekte der Welt mit eindeutigen Adressen zu versehen. Die durchgängige Adressierbarkeit der Welt schafft gute Voraussetzungen für die Implementierung von Segment Routing auf IPv6-Basis.

Wie funktioniert SRv6?

Bei SRv6 ist ein IPv6-Netz das Fundament (Underlay) für eine beliebig skalierbare Anzahl von Datenpfaden. Nur die Komponenten am Rand des Netzes müssen SRv6 unterstützen. Alle Netzknoten auf dem Pfad zwischen zwei Randknoten müssen nur IPv6 übertragen können. Die SRv6-fähigen Edge-Komponenten sind der Anfang (Ingress) und das Ende (Egress) des Pfades durch das IPv6-Netz. Der Ingress-Router gibt als Abschluss des Pfades die Adresse des Egress-Knoten sowie die Aktion vor, die der Egress-Router bei Empfang des Pfades durchführen muss. Die Aktion kann zum Beispiel das herkömmliche IP-Routing in einer Instanz für VRF (Virtual Routing and Forwarding) sein. So können zwei Teilnetze eines Virtual Private Network (VPN) über ein SRv6-Netz miteinander verbunden werden.

Als SID verwendet SRv6 statt eines eigenen Konstrukts IPv6-Adressen.

Potenzial für MPLS-Ablösung

Damit MPLS verschiedene, voneinander separierte VPNs unterstützen kann, wird in den meisten MPLS-Netzen eine MPLS-spezifische Encapsulation (Einpacken eines Pakets in einem ande-

Mit Quantum Key Distribution zum sicheren Schlüsselaustausch

von Dr. Philipp Rüßmann

Quantencomputer stellen eine Gefährdung für unsere derzeitige asymmetrische Verschlüsselung dar und erfordern schon heute dringendes Handeln. Bestehende Sicherheitsmechanismen können jedoch resistenter gegen Angriffe durch Quantencomputer aufgestellt werden. Ein Kernelement dabei ist der sichere Schlüsselaustausch – bei dem die Quantenphysik zur Lösung des Dilemmas beitragen kann. Quantum Key Distribution (QKD) bietet Möglichkeiten für einen abhörsicheren Schlüsselaustausch.

Chancen durch Quantencomputer

Quantencomputer funktionieren anders als klassische Computer:

- **Quantenbits**: Statt Transistoren, die zwischen Nullen und Einsen schalten, nutzen Quantencomputer Qubits, die auch alle Zwischenzustände für ihre Berechnungen nutzen können.
- **Exponentielles Wachstum der Rechenleistung**: Damit erschließen sich neue Möglichkeiten, und die Grenzen der klassischen Skalierung der Rechenleistung nach Moore's Law gelten für Quantencomputer nicht.
- **Hohe Fehlerraten und technische Herausforderungen**: Heutige Quantencomputer sind noch nicht in der Breite marktreif, sie sind noch in der Phase der Forschung und Entwicklung.
- **Spezialisierte Anwendungsfälle**: Quantencomputer werden die derzeitige IT nicht eins zu eins ersetzen, stattdessen werden sie für spezialisierte Anwendungsfälle wie Optimierungsprobleme zum Einsatz kommen.

Insgesamt lässt sich festhalten, dass die langfristige Zukunft der IT eine hybride Landschaft ist, die die Stärken unterschiedlicher Architekturen wie CPUs, GPUs und dann bald auch QPUs (Quantenbeschleuniger bzw. Quantum Processing Units) miteinander verbinden wird [1].

Quantencomputer könnten ihren Quantenvorteil (engl. Quantum Advantage) gegenüber klassischer Hardware auch bei energieeffizienterer (Quanten-)KI [2] zeigen oder eine Vielzahl von anderen technologischen Herausforderungen lösen. Die schnelle Entwicklung auf dem Gebiet der Quantencomputer der letzten Jahre, über die ich auch immer wieder in Beiträgen im ComConsult-Blog berichtet habe [3, 4], lässt also auf eine rosige Zukunft hoffen.

Herausforderungen und Gefahren durch den Q-Day

Das disruptive Potential der Quantencomputer bringt allerdings nicht nur Chancen mit sich. Die allgemeine Nachrichtenlage zu diesem Thema fokussiert sich oftmals auf potenzielle Gefahren für unsere allgegenwärtige Verschlüsselung [5]. In diesem Zusammenhang wird der Q-Day als der Tag definiert, an dem Quantencomputer leistungsfähig genug sind, um unsere heutige Verschlüsselungsmethoden zu gefährden. Man spricht hier auch von kryptographisch relevanten Quantencomputern (Cryptographically Relevant Quantum Computer, CRQC). Tabelle 1 fasst die Gefährdung für die klassische Kryptographie im „Quantenzeitalter" zusammen.

Ohne digitale Zertifikate kein Vertrauen

Mit Jona Hermens sprach Christiane Zweipfennig

Digitale Zertifikate bilden die Grundlage für sichere Authentisierung, Verschlüsselung und vertrauenswürdige Kommunikation in modernen Unternehmensnetzwerken. Mit der zunehmenden Vernetzung von IT-Systemen, Endgeräten und Anwendungen wächst die Bedeutung von Zertifikaten kontinuierlich. Gleichzeitig stellt die Einführung und Verwaltung einer Zertifikatsinfrastruktur viele Unternehmen vor organisatorische und technische Herausforderungen.

Jona Hermens absolvierte ein Bachelor- und Masterstudium im Studiengang Computational Engineering Science. Im Anschluss an sein Studium begann er seine Tätigkeit als Berater bei ComConsult im Bereich IT-Sicherheit. Dort arbeitet er seit mehr als zwei Jahren sowohl an konzeptionellen als auch an technischen Themen, insbesondere im Bereich Network Access Control (NAC), und spezialisierte sich im Rahmen seiner Projektarbeit auf den Einsatz von Zertifikaten und Public-Key-Infrastrukturen (PKI).

Was sind digitale Zertifikate und warum sind sie wichtig?

Zertifikate sind ein zentraler Bestandteil moderner IT-Sicherheit. Ich vergleiche sie immer gerne mit einem Ausweis: So wie sich eine Person mit ihrem Ausweis identifiziert, kann sich auch ein Gerät oder eine Person mithilfe eines digitalen Zertifikats eindeutig gegenüber einem Kommunikationspartner authentisieren.

Ein Zertifikat geht jedoch über eine reine Identifikation hinaus. Es ermöglicht nicht nur die eindeutige Authentisierung, sondern bildet auch die Grundlage für eine verschlüsselte Kommunikation und trägt damit wesentlich zur Vertraulichkeit von Daten bei. Darüber hinaus spielen Zertifikate eine wichtige Rolle bei der Sicherstellung der Integrität von Informationen. Durch digitale Signaturen kann nachgewiesen werden, dass Daten während der Übertragung nicht verändert oder manipuliert wurden.

> Digitale Zertifikate gewährleisten Authentisierung, Verschlüsselung und Integrität.

Grundsätzlich können Zertifikate für unterschiedlichste Anwendungsfälle ausgestellt werden – beispielsweise für Geräte oder für Benutzer bei der E-Mail-Kommunikation. Entscheidend ist dabei, dass ein Zertifikat eindeutig einer bestimmten Identität und einem konkreten Einsatzzweck zugeordnet ist. Zwar ist es technisch möglich, ein Zertifikat für mehrere Szenarien oder Geräte zu verwenden, aus Sicherheitsgründen sollte dies jedoch vermieden werden.

Was beinhalten digitale Zertifikate und wie funktionieren sie?

Digitale Zertifikate enthalten eine Reihe von Informationen, die für eine sichere Authentisierung und verschlüsselte Kommunikation erforderlich sind. Ein wesentlicher Bestandteil ist dabei der öffentliche Schlüssel, der die Grundlage für kryptografische Verfahren bildet. Darüber hinaus enthalten Zertifikate Informationen zu den verwendeten Algorithmen und Signaturen, die es Kommunikationspartnern ermöglichen, eine sichere und verschlüsselte Verbindung zu berechnen und aufzubauen.

Wenn Excel zur Schatzkarte wird

Warum gute IT-Dokumentation mehr wert ist als jede Hardware

von Ben Grünbauer

Ich glaube, jeder Arbeitnehmer in der IT kennt diese Situation. Egal, ob in einer beratenden Rolle oder als ausführende Kraft: Irgendwann steht man vor einer Excel-Tabelle, die vermutlich schon mehrere Generationen an Administratoren überlebt hat. Oder man bekommt einen prall gefüllten Aktenordner in die Hand gedrückt, aus dem man nun herausfinden soll, welches Kabel eigentlich wohin führt. Im besten Fall sind die Pläne noch lesbar, im schlechtesten hilft nur noch die Hoffnung, dass sich jemand daran erinnert.

Nicht selten fällt dann im Nachgang der Satz: „Frag am besten den Kollegen XY, der weiß das alles." Und genau das beschreibt das eigentliche Problem ziemlich gut. Die Dokumentation liegt nicht auf dem Server, sondern befindet sich im Kopf eines einzelnen Mitarbeiters.

Auch ich durfte in vergangenen Projekten einige dieser Dokumentationen kennenlernen, oder besser gesagt: ihre Nachfolger erstellen. Gerade bei Rechenzentrumsprojekten oder Infrastrukturumzügen merkt man sehr schnell, wie wertvoll eine saubere Dokumentation ist. Fehlt sie oder ist sie über Jahre hinweg nicht gepflegt worden, wird aus einer einfachen Planungsaufgabe schnell Detektivarbeit. Plötzlich muss nachvollzogen werden, welches Kabel noch aktiv ist, welche Systeme tatsächlich produktiv genutzt werden und welche Anwendungen voneinander abhängig sind. Dinge, die mit einer gepflegten Dokumentation innerhalb weniger Minuten beantwortet wären, kosten dann mehrere Gespräche, Vor-Ort-Begehungen und nicht selten auch einige Schweißperlen.

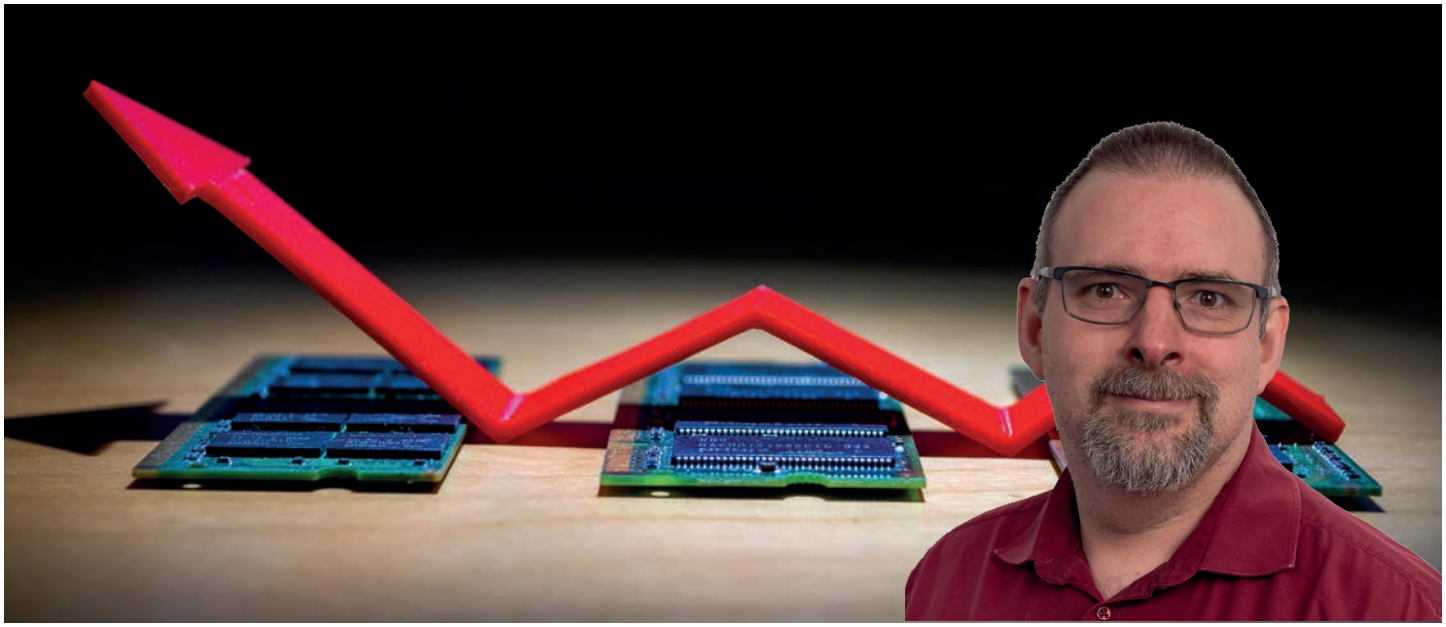
Dabei wünscht man sich als Berater zu Beginn eines Projektes nur eins: eine vollständige und aktuelle Dokumentation der vorhandenen IT-Infrastruktur. Bonuspunkte gibt es, wenn neben den Systemen selbst auch deren gegenseitige Abhängigkeiten sauber dargestellt sind. Welche Anwendung kommuniziert mit welcher Datenbank? Welcher Server hängt an welchem Storage? Welche Switch-Ports versorgen welche Systeme? Genau diese Informationen entscheiden später darüber, ob ein Projekt strukturiert geplant werden kann oder ob zunächst einmal die gesamte Infrastruktur neu aufgenommen werden muss.

Die Realität sieht allerdings häufig anders aus. Dokumentationen sind unvollständig, über Jahre hinweg gewachsen oder auf die verschiedensten Werkzeuge verteilt. Hier eine Excel-Datei, dort ein Visio-Plan, irgendwo ein Wiki-Eintrag und zusätzlich noch ein paar Informationen in Microsoft Teams oder auf einem Netzlaufwerk. Natürlich existieren manche Dokumente auch mehrfach, allerdings mit unterschiedlichen Versionsständen. Wer schon einmal versucht hat herauszufinden, welche Version aktuell ist, kennt das Ergebnis meistens schon vorher: Am Ende kontrolliert man alles lieber noch einmal selbst.

Besonders spannend wird es, wenn jede Fachabteilung ihre eigene Dokumentation pflegt. Das Netzwerkteam dokumentiert die Switches, die Serveradministration führt ihre Inventarliste, das Storage-Team hat wiederum eine eigene Übersicht und irgendwo existiert noch eine Patchliste aus einem früheren Projekt. Alle Dokumentationen für sich genommen mögen sogar korrekt sein, gemeinsam ergeben sie jedoch häufig kein vollständiges Gesamtbild. Hinzu kommen unterschiedliche Namenskonventionen oder kreative Bezeichnungen, sodass ein und dasselbe System an mehreren Stellen unterschiedliche Namen trägt. Spätestens dann beginnt das große Rätselraten darüber, ob überhaupt vom gleichen Server gesprochen wird.

Kostenschätzungen für Rechenzentrums-Infrastruktur in Zeiten steigender RAM-Preise

von Dr. Markus Ermes



Ich habe bereits darüber geschrieben – so wie auch Dr. Moayeri in seinem Beitrag (https://www.comconsult.com/massive-kostensteigerungen-durch-teurere-hardware/). Die Aussichten waren und sind nicht unbedingt rosig: Preise für Arbeitsspeicher und SSDs, egal ob im Privat- oder Unternehmensumfeld, kennen aktuell nur eine Richtung, und zwar: nach oben!

Glücklich ist darüber, mit Ausnahme der Speicher-Hersteller, wahrscheinlich niemand. Die Situation bedeutet bei Beschaffungen aktuell deutlich höhere Preise, geringere Verfügbarkeit, längere Lieferzeiten und fast schon unverschämt kurze Preisbindungen. Es ist mir in Projek-ten schon begegnet, dass die Preisbindung bei einer Ausschreibung kürzer war als die Stillhaltefrist, die bis zur Beauftragung einzuhalten war.

Langfristige Planungen

Es gibt allerdings auch Projekte, in denen die aktuellen Preisentwicklungen zwar ärgerlich sind, die eigentliche Problematik aber an ganz anderer Stelle liegt: Immer wieder unterstützen meine Kollegen und ich bei der Planung von Rechenzentren (RZs). Die richtige Planung eines RZs ist eine Herausforderung, auch was die Dauer angeht. Ein RZ plant man nicht von heute auf morgen! Und wenn die Planung steht, gehen die zeitaufwendigen Arbeiten erst richtig los: Alle Phasen der HOAI müssen betrachtet und ausgeführt werden. Was aus eigener Erfahrung schon bei einem privaten Bauprojekt lange dauern kann, inklusive möglicher Verzögerungen, ist im Umfeld von Rechenzentren mindestens ebenso kompliziert. So kommt es in Projekten schonmal vor, dass mit der Fertigstellung eines RZs erst in acht bis zehn Jahren gerechnet wird.

Die Schnelllebigkeit der IT

Acht bis zehn Jahre sind in der IT nach wie vor eine Ewigkeit. Ich kann derzeit nicht abschät-zen, was in einem RZ in acht Jahren Standard sein wird. Natürlich: Server werden schneller, SSDs größer und die Netzleistung wird zunehmen. Im Allgemeinen bleiben bei der für den jeweiligen Zeitpunkt gleichwertigen Leistung auch die Preise relativ konstant. Die Inflation spielte zwar schon immer eine Rolle, weshalb ein entsprechender Puffer eingeplant werden muss. Dieser Aspekt ist jedoch beherrschbar.

Es kann aber in acht Jahren bereits eine neue Technologie geben, die heute niemand auf dem Schirm hat. Wer hätte sich – außer KI-Forschern sowie Unternehmen und Universitäten mit Supercomputern – vor 10 Jahren träumen lassen, welche Leistungsdichte und welchen Kühlungsbedarf moderne KI-Server haben? Flüssigkühlung? Brauchen doch nur Gamer und Supercomputer!

NVIDIA hat bereits angekündigt, dass die nächste Generation ih-