April 2026

ComConsult
BERATUNG • PLANUNG • SCHULUNG

Der Netzwerk Insider

Auf dem Weg zur Post-Quanten-PKI:
Risiken verstehen und Vorbereitungen für den Q-Day treffen

von Jona Hermens

Der sogenannte „Q-Day“ rückt immer näher. Dieser beschreibt den Zeitpunkt, an dem Quantencomputer so leistungsfähig sind, dass mit ihnen die heute verbreiteten kryptografischen Verfahren geknackt werden können.

Seite 9

Server und Rechenzentren der Zukunft

von Dr. Behrooz Moayeri

Am 25. Februar dieses Jahres führte die ComConsult Akademie eine Sonderveranstaltung mit dem Titel „Server der Zukunft“ durch. Meine persönlichen Eindrücke von diesem Event lesen Sie in diesem Beitrag.

Seite 2

Small Language Models – die effiziente und sichere OnPrem-Lösung?

von Felix Horn

Die vergangenen drei Jahre haben eindrucksvoll gezeigt, welchen Einfluss Large Language Models (LLMs) auf unser privates, akademisches und berufliches Leben ausüben. Kaum jemand hat noch nie etwas von „ChatGPT“, „Gemini“ und Co. gehört.

Seite 14

Webinar der Woche

IT-Kosten im Griff – Kostentransparenz und Produktpreise

Seite 25

Wi-Fi 7 für das IoT?

von Dr. Joachim Wetzlar

Inzwischen ist es zwei Jahre her, dass die Wi-Fi Alliance ihr Zertifizierungsprogramm Wi-Fi CERTIFIED 7™ vorgestellt hat. Ich hatte Ihnen in [1] bereits darüber berichtet. Der entsprechende Standard IEEE 802.11be wurde im September 2024 fertiggestellt. Inzwischen kann man ihn über das IEEE GET Program™ frei herunterladen [2] (Sie müssen sich dazu vorab ein Konto bei IEEE einrichten).

Seite 26

Server und Rechenzentren der Zukunft

von Dr. Behrooz Moayeri

Am 25. Februar dieses Jahres führte die ComConsult Akademie eine Sonderveranstaltung mit dem Titel „Server der Zukunft“ durch. Meine persönlichen Eindrücke von diesem Event lesen Sie in diesem Beitrag.

Kühlung als große Herausforderung

In der Insider-Ausgabe vom Januar dieses Jahres schrieb ich über Kühlung als große Herausforderung bei Planung und Betrieb von Rechenzentren. Server- und RZ-Kühlung waren auch das Thema des ersten Vortrages meiner Kollegen Dr. Ermes und Dr. Rüßmann auf der Sonderveranstaltung Server der Zukunft. Ein paar Highlights daraus:

- Der Schmelzpunkt einiger Elektronik-Materialien liegt bei 157 Grad Celsius. Also muss die Wärme so abgeführt werden, dass ein möglichst großer Sicherheitsabstand zu diesem Schmelzpunkt eingehalten wird.
- Nanotechnologie wird die Dichte von elektronischen Bauelementen auf Chips und somit die Dichte der entstehenden Wärmeenergie erhöhen.
- Die heute in den meisten Rechenzentren angewandte Luftkühlung wird künftig angesichts der immer höheren Leistungsdichte mit Flüssigkeitskühlung kombiniert werden müssen.
- Von der raum- über reihen- zur schrankbasierenden Kühlung wird die gekühlte Einheit immer kleiner.
- Regulatorische Vorgaben bezüglich der Effizienz der RZ-Kühlung sind zu beachten.
- Für die Erhaltung eines zuverlässigen Stromnetzes müssen mehr Rechenzentren auf die Fläche von Ländern wie Deutschland verteilt werden.
- Modulare RZ-Container als Edge-RZ sind flexibler erweiterbar.

Von Supercomputing lernen

Das Problem der steigenden Leistungsdichte, mit dem alle Rechenzentren zunehmend konfrontiert werden, hat es in RZs mit Supercomputern schon immer gegeben. Insofern war es interessant zu hören, über welche Erfahrungen bei der Realisierung des ersten Exascale-Supercomputers in Europa namens Jupiter Herr Eickermann vom Forschungszentrum Jülich berichten konnte. Ich fand seinen Vortrag faszinierend, zumal daraus viele Erkenntnisse über die RZ-Planung der Zukunft gewonnen werden konnten:

- Bei Exascale-Rechnern handelt es sich um solche, die z. B. mehr als 1 Exa-Flops/s unterstützen (d.h. mindestens 1018 Floating Point Operations per Second).
- Bei Jupiter als dem leistungsfähigsten bekannten Supercomputer außerhalb der USA wurde für 150 kW pro Rack geplant. Die meisten Anwesenden in der Veranstaltung gaben für die von ihnen zurzeit betriebenen RZs maximale Werte um 10 kW pro Rack an.
- Auch die Dauer der Realisierung ist aufschlussreich: Im Juni 2022 gewann Jülich den Zuschlag für das EuroHPC Exascale System. Die Planung und Realisierung von 1200 m2 IT-Fläche mit bis zu 3 Tonnen Last pro Quadratmeter dauerte dreieinhalb Jahre.
- Die Speicherkapazität von Primär-Storage beläuft sich auf über 300 Petabytes (PB) brutto und über 200 PB netto. Hinzu

Auf dem Weg zur Post-Quanten-PKI

Risiken verstehen und Vorbereitungen für den Q-Day treffen

von Jona Hermens

Der sogenannte „Q-Day“ rückt immer näher (s. auch den Beitrag meines Kollegen Felix Horn). Dieser beschreibt den Zeitpunkt, an dem Quantencomputer so leistungsfähig sind, dass mit ihnen die heute verbreiteten kryptografischen Verfahren geknackt werden können. Häufig geht damit die Befürchtung einher, dass ab diesem Moment die gesamte vertrauliche Kommunikation nicht mehr geschützt ist und bestehende Verschlüsselungen kompromittiert werden können.

Doch wie realistisch ist dieses Szenario wirklich, und welche konkreten Schritte sind schon heute notwendig, um darauf vorbereitet zu sein?

Was ist durch Quantencomputing wirklich angreifbar?

Um diese Frage zu beantworten, ist eine genauere Betrachtung notwendig. Vorab ist wichtig zu verstehen, dass nicht alle bestehenden Sicherheitsmechanismen durch Quantencomputing plötzlich unsicher oder direkt angreifbar werden. Daher ist es entscheidend, dies differenziert zu betrachten, um herauszufinden, welche Bereiche tatsächlich betroffen sind und welche weiterhin als vergleichsweise sicher gelten.

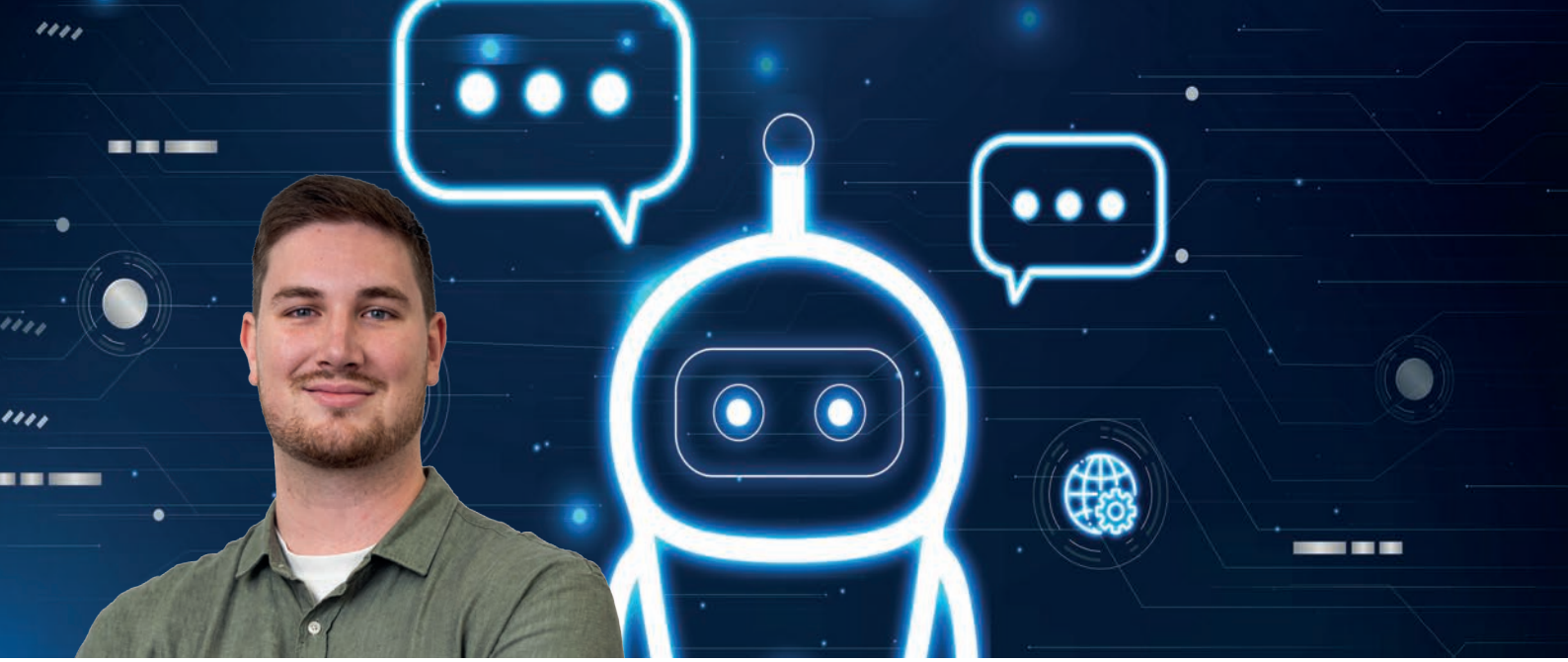
Im Fokus dieses Artikels stehen dabei vor allem kryptografische Verfahren, die in digitalen Zertifikaten und innerhalb einer Public Key Infrastructure (PKI) eingesetzt werden. Diese bilden die Grundlage zahlreicher Sicherheitsmechanismen in Netzwerken, Anwendungen und Kommunikationsprotokollen und sind somit von hoher Bedeutung in der Diskussion rund um den Q-Day.

Es können auch digitale Signaturen im Umfeld von PKI und Zertifikaten potentiell von quantenbasierten Angriffsszenarien betroffen sein.

Wie sicher ist das TLS-Protokoll?

Ein besonders relevantes Beispiel für den Einsatz von PKI-basierten Verfahren ist das Transport-Layer-Security-(TLS-)Protokoll. Bei einem üblichen TLS-Handshake wird während des Verbindungsaufbaus mithilfe asymmetrischer Kryptografie (etwa RSA) oder elliptischer Kryptografie (ECC) ein gemeinsamer Sitzungsschlüssel ausgehandelt. Die anschließende Kommunikation wird dann mit symmetrischer Verschlüsselung unter Verwendung dieses einen Sitzungsschlüssels geschützt.

Bei diesem zweiten Teil des TLS-Handshakes, also bei der symmetrischen Verschlüsselung, wird der Sitzungsschlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln der übertragenen Daten verwendet. Dieser Sitzungsschlüssel muss daher beiden Kommunikationspartnern vorliegen und ausschließlich diesen



Small Language Models – die effiziente und sichere OnPrem-Lösung?

von Felix Horn

Die vergangenen drei Jahre haben eindrucksvoll gezeigt, welchen Einfluss Large Language Models (LLMs) auf unser privates, akademisches und berufliches Leben ausüben. Kaum jemand hat noch nie etwas von „ChatGPT“, „Gemini“ und Co. gehört. Was zu Beginn ein bisschen wie Magie wirkte, ist inzwischen zum festen Bestandteil des Alltags vieler Menschen geworden. Ob ein schnelles Rezept aus den letzten Resten im Kühlschrank, eine weniger aggressive Formulierung für die E-Mail an den Kollegen oder die Suche nach einem passenden Namen für ein neues Start-up – all das erledigen ChatGPT und vergleichbare Modelle mühelos.

Dem aufmerksamen Leser dürfte in den oben beschriebenen Anwendungsfällen etwas aufgefallen sein. Ein Rezept zu erstellen oder Inspiration für einen kreativen Namen zu suchen birgt in den seltensten Fällen ein Risiko. Eine Mail an den Kollegen hingegen kann auch gerne mal sensible, unternehmensinterne Informationen beinhalten. Was passiert mit den Daten in dem Moment, in dem ich ein öffentliches LLM damit beauftrage, diese weiterzuverarbeiten?

Für Führungskräfte ist es nahezu unmöglich, den Einsatz von KI grundsätzlich zu verhindern. Beschäftigte werden immer Wege finden, die Tools zu nutzen, die ihnen ihre Arbeit erleichtern. Diese Motivation gilt es grundsätzlich zu schätzen, nicht aber, wenn dies außerhalb der geregelten Freigabeprozesse geschieht. Letzteres Phänomen wurde bisher unter dem Begriff „Schatten-IT“ zusammengefasst. Im Zusammenhang mit nicht genehmigten KI-Anwendungen spricht man mittlerweile auch von „Schatten-KI“. Diesem Verhalten kann durch Regulatorik und Richtlinien entgegengewirkt werden. Hierzu haben wir bereits im August 2025 Gesetze und Standards vorgestellt, die sich mit dem Management und der Nutzung von KI-Systemen beschäftigen [1].

Falls die oben genannte Regulatorik nicht ausreicht oder eine weitere Maßnahme gegen die ungewollte Nutzung öffentlicher LLMs gewünscht ist, wäre es möglich, eine lokale LLM-Lösung bereitzustellen. Mithilfe einer sogenannten „On-Prem-KI“ könnte dem Kontrollverlust der Unternehmen- und Kundendaten vorgebeugt werden, und als Administrator hätte man die volle Kontrolle über die Nutzung dieses Systems.

Die teilweise sehr hohen Hardwareanforderungen von State-of-the-Art-LLMs und das notwendige technische Verständnis zur lokalen Integration dieser halten kleine und mittelständische Unternehmen jedoch oft davon ab, ein solches On-Prem-LLM zu implementieren. Neue Entwicklungen in Modellkompression und Speicheroptimierung erlauben es, effiziente „Small Language Models“ zu trainieren und somit die Hardwareanforderungen zu minimieren.

Der folgende Artikel setzt sich zum Ziel, die Hemmschwelle zur selbst gehosteten KI zu minimieren. Dazu werden zunächst Large Language Models vorgestellt, und es wird beschrieben, wie aus diesen dann schlankere und weniger ressourcenintensive Small Language Models hervorgehen. Es wird außerdem auf Dimensionierungsfragen einer lokalen KI im Unternehmenskontext eingegangen, und abschließend werden Tipps und Hinweise zur Implementierung vorgestellt.

Spezifikation von Verteilerräumen

Mit Mark Groten sprach Christiane Zweipfennig

Verteilerräume bilden das Rückgrat moderner Gebäudetechnik, da hier Strom-, Daten- und Kommunikationsleitungen zentral zusammenlaufen. Um einen sicheren und zuverlässigen Betrieb zu gewährleisten, müssen sie bestimmten baulichen und technischen Anforderungen entsprechen. Schon bei der Planung der Räume ist es entscheidend, diese Vorgaben zu berücksichtigen, um späteren Störungen, hohen Wartungskosten oder Sicherheitsrisiken vorzubeugen. Eine durchdachte Umsetzung sorgt somit für Effizienz, Sicherheit und Langlebigkeit der gesamten Infrastruktur.

Mark Groten begann seine berufliche Laufbahn als Elektroinstallateur, absolvierte berufsbegleitend die Technikerschule und trat nach deren erfolgreichem Abschluss vor rund 30 Jahren bei ComConsult ein. Sein Tätigkeitsschwerpunkt liegt im Competence Center IT-Infrastrukturen im Bereich der passiven IT-Infrastruktur. Dazu zählen die Planung und Konzeption von Verkabelungssystemen, Technik- und Serverräumen, Verteilerschränken, Klimatisierung sowie der elektrotechnischen Stromversorgung. Er verantwortet damit sämtliche infrastrukturelle Grundlagen, die für den sicheren und zuverlässigen Betrieb von IT-Systemen, Rechnerräumen, Serverräumen und Etagenverteilern erforderlich sind. In diesem Interview berichtet er davon, welche technischen Vorgaben und Rahmenbedingungen bei der Planung von Datenverteilerräumen eine Rolle spielen.

Was sind ganz allgemein die Anforderungen an Datenverteilerräume?

Besonders bei Betreibern kritischer Infrastrukturen wie beispielsweise Krankenhäuser sollten Verteilerpunkte grundsätzlich in gesicherten, separaten Räumen installiert werden. Diese Räume dienen der Unterbringung von Verteilerschränken und weiterem technischen Equipment und müssen definierte bauliche sowie technische Anforderungen erfüllen.

Besonderen Wert wird dabei auf einen wirksamen Zutrittsschutz gelegt, um unbefugten Personen den Zugang zu verwehren. Darüber hinaus sind geeignete Umgebungsbedingungen sicherzustellen, etwa eine zuverlässige Stromversorgung, eine angemessene Klimatisierung sowie weitere infrastrukturelle Voraussetzungen, um einen sicheren und störungsfreien Betrieb der IT-Systeme zu gewährleisten. Hierbei sollte man sich immer Gedanken um Verfügbarkeitsanforderungen und dadurch notwendige zu schaffende Redundanzen machen (Stromversorgung, Klimatisierung…).

> Verteilerpunkte sollten grundsätzlich in gesicherten, separaten Räumen installiert werden.

Wie sollten Lage und Zugang von Verteilerräumen im Gebäude idealerweise gestaltet sein?

Im Rahmen der Planung wird zunächst der vorgesehene Raum hinsichtlich seiner Eignung geprüft. Häufig besteht seitens des Auftraggebers die Vorstellung, vorhandene, bislang anderweitig genutzte Räume – etwa im Kellergeschoss – als Technik- oder Verteilerräume zu verwenden. In der Praxis erweisen sie sich jedoch oftmals als ungeeignet. Kellerräume sind nicht selten von Feuchtigkeit, Staubbelastung oder potenziell eindringendem Wasser betroffen. Diese Risiken sind zwingend zu berücksichtigen, da Wasser naturgemäß nicht nach oben fließt und somit insbesondere tieferliegende Bereiche gefährdet sind.

Wi-Fi 7 für das IoT?

von Dr. Joachim Wetzlar

Inzwischen ist es zwei Jahre her, dass die Wi-Fi Alliance ihr Zertifizierungsprogramm Wi-Fi CERTIFIED 7™ vorgestellt hat. Ich hatte Ihnen in [1] bereits darüber berichtet. Der entsprechende Standard IEEE 802.11be wurde im September 2024 fertiggestellt. Inzwischen kann man ihn über das IEEE GET Program™ frei herunterladen [2] (Sie müssen sich dazu vorab ein Konto bei IEEE einrichten).

Wir bei ComConsult machen nun unsere ersten Gehversuche mit Wi-Fi 7. Unsere neuen Büros, die wir bezogen haben werden, wenn Sie diesen Netzwerk Insider in Händen halten, verzichten gänzlich auf drahtgebundene Verbindungen. Stattdessen wurden Access Points der neuesten Generation ausgerollt, und unser Installations-Team probiert die verschiedenen neuen Konfigurations-Möglichkeiten aus. Über entsprechende Erfolge und Misserfolge werden wir auf unseren kommenden Veranstaltungen berichten.

Wi-Fi 7 / IEEE 802.11be wird auch mit dem Namen “Extremely High Throughput” (EHT) belegt. Mit 8 Spatial Streams, 4096 QAM und 320 MHz breiten Kanälen soll sich eine Brutto-Bitrate von 23 Gbit/s erzielen lassen. Soweit die Theorie. Nur werden Sie – zumindest hier in Europa – kaum Enterprise-WLANs mit 320 MHz breiten Kanälen errichten können.

Im Gegenteil: Nach wie vor lässt sich im WLAN der größte Gesamtdurchsatz, sozusagen Bit pro Sekunde pro Kubikmeter, mit möglichst schmalen Kanälen erzielen. In diesem Fall stören sich die Access Points gegenseitig am wenigsten. Außerdem finden wir in der Praxis zahlreiche Endgeräte aus Alt-Installationen vor, die nur eine Bandbreite von 20 MHz unterstützen, also etwa „Legacy Devices“ gemäß IEEE 802.1a.

In diesem Zusammenhang ist es interessant, dass nun die Wi-Fi Alliance ein Wi-Fi-7-Zertifikat für Endgeräte angekündigt hat, die nur 20 MHz breite Kanäle nutzen können [3]. Wohlgemerkt, es geht nicht um Legacy Devices, sondern um Endgeräte, die Features aus IEEE 802.11be unterstützen. Im Standard werden sie als „20 MHz-only non-AP Stations“ bezeichnet.

Welche Features müssen auf 20 MHz Kanalbandbreite beschränkte Endgeräte beherrschen? Hier eine Auswahl:

- 4096 QAM: Die Quadraturamplitudenmodulation wurde mit Wi-Fi 7 bekanntlich noch einmal aufgebohrt. Pro Zeiteinheit lassen sich somit 20 % mehr Daten übertragen als noch mit Wi-Fi 6, das „nur“ bis zu 1024 QAM unterstützte.
- 512 Compressed Block Ack: Bis zu 512 Pakete (MAC Protocol Data Units, MPDUs) lassen sich auf einmal senden und mit einem einzigen Paket quittieren. Dadurch spart man einen Haufen Wartezeit, Präambel und Header ein.
- Multiple RUs (MRU): Dies ist eine neue Spielart von OFDMA (Orthogonal Frequency Division Multiple Access), das bereits mit Wi-Fi 6 eingeführt wurde. Mit OFDMA wird einer Station genau eine Gruppe von Unterträgern (Resource Unit, RU) zugewiesen. Eine RU umfasst z. B. 26, 52, 106 oder 242 Unterträger. Mit Wi-Fi 7 wird es nun möglich, einer Station mehrere benachbarte RUs zuzuweisen, z. B. 52+26 Unterträger. Dadurch lässt sich das zur Verfügung stehende Frequenzspektrum besser auf verschiedene Stationen verteilen.
- Downlink/Uplink Multi-User MIMO: Ähnlich wie bei MRU können mehrere Endgeräte gleichzeitig unterschiedliche Daten vom Access Point empfangen oder an ihn absenden. Dies geschieht unter Nutzung verschiedener Spatial Streams, sozusagen durch die Verwendung mehrerer Antennen.