März 2026

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Smart Building und IT-Sicherheit: Alles ist verbunden

von Dr. Andreas Kaup
Smart Buildings sind Gebäude mit einer modernen digitalen Infrastruktur, hochverfügbarer Konnektivität, moderner IT, einer Basis für das Internet of Things (IoT) und smarter Gebäudeautomation. Alle Informationen und sämtliche Funktionalitäten werden in einer Management-Plattform gebündelt.

Seite 7

SOC-Strukturen verstehen: Wege zu einer effektiven Sicherheitsüberwachung

von Esther Perl
Cyberangriffe werden schneller, gezielter und zunehmend professionell orchestriert. Für Unternehmen bedeutet das: Sicherheitsvorfälle können jederzeit auftreten, unabhängig von Branche oder Größe.

Seite 26

Tätigkeitsbericht der Bundesnetzagentur

von Dr. Behrooz Moayeri
Der den Mobilfunk betreffende Teil des Tätigkeitsberichts der Bundesnetzagentur – Telekommunikation 2024/2025 wurde bereits in einem Blog meines Kollegen Frederik Stückemann thematisiert. In diesem Beitrag gehe ich auf andere Inhalte aus diesem Bericht ein.

Seite 2

Digitalpakt 1.0 vs. 2.0 – einfach erklärt…

von Peter Steufmehl
Digitalpakt 2.0: Schulen werden dauerhaft modern

Schulen in Deutschland digital auf den neuesten Stand zu bringen, ist eine riesige Aufgabe. Ende 2025 gab es eine neue Einigung - den Digitalpakt 2.0. Damit beginnt eine neue Phase, in der es um viel mehr geht als nur um den käuflichen Erwerb von Laptops.

Seite 17

Webinar der Woche

Von der Theorie zur Praxis – OT-Security live erleben

Seite 25

Teurer RAM führt zu teuren Servern

von Dr. Markus Ermes
Wir haben es wahrscheinlich alle mitbekommen: Arbeitsspeicher und SSDs werden aktuell immer teurer. Innerhalb von weniger als 3 Monaten haben sich die Preise für RAM im Server-Bereich mehr als verdoppelt, und auch SSDs sind nicht von Preiserhöhungen verschont geblieben.

Seite 31

Tätigkeitsbericht der Bundesnetzagentur

von Dr. Behrooz Moayeri

Der den Mobilfunk betreffende Teil des Tätigkeitsberichts der Bundesnetzagentur – Telekommunikation 2024/2025 wurde bereits in einem Blog meines Kollegen Frederik Stückemann thematisiert. In diesem Beitrag gehe ich auf andere Inhalte aus diesem Bericht ein.

Glasfaserausbau

Bereits im ersten Absatz des Vorworts zu dem im Dezember 2025 veröffentlichten Tätigkeitsbericht der Bundesnetzagentur wird der Glasfaserausbau als Infrastrukturprojekt erwähnt. Einige Eckdaten:

- In Deutschlands Glasfaserausbau wird jährlich in zweistelliger Milliardenhöhe investiert. Zitat: „2024 haben die Unternehmen im Festnetz- und Mobilfunkbereich über 15 Milliarden Euro – und damit 500 Millionen Euro mehr als im Jahr zuvor – in Sachanlagen investiert."

- Dass der Glasfaserausbau hierzulande nicht so weit ist wie in anderen europäischen Ländern, wird im Bericht den Möglichkeiten des deutschen Kupfernetzes (DSL und TV-Kabel) zugeschrieben: „Fast 95 % der Haushalte hatten Ende 2024 die Möglichkeit, einen Internetanschluss mit mindestens 100 Mbit/s im Download zu buchen."

- Aus dem Bericht geht hervor: „Mitte 2025 waren ca. 5,8 Mio. Glasfaseranschlüsse vertraglich gebucht. Damit verfügten ca. 13 % aller Endkunden über eine aktive Glasfaserleitung. Weitere 3,7 Mio. Anschlüsse sind mit einer gänzlich fertiggestellten Glasfaseranbindung ausgestattet, die sie bislang aber nicht nutzen. Für insgesamt 9,5 Mio. bzw. 21 % der Endkundinnen und Endkunden steht also ein Glasfaseranschluss zur Verfügung, der keiner weiteren Bauarbeiten und Investitionen mehr bedarf. Hinzu kommen ca. 15,1 Mio. Haushalte, bei denen das Glasfasernetz in unmittelbarer Nähe des Grundstücks endet."

Wachstum des Telekommunikationsmarktes nur bei der Telekom

Bekanntlich stagniert die deutsche Wirtschaft seit 2023. Dies gilt inflationsbereinigt auch für den Telekommunikationsmarkt. Laut Bundesnetzagentur stiegen die Außenumsatzerlöse (d.h. Erlöse der Telekommunikationsunternehmen in ihren Geschäften mit Unternehmen außerhalb der Branche) im deutschen Telekommunikationsmarkt 2024 auf 61,3 Mrd. Euro. Das waren 2,5 % mehr als 2023 (59,8 Mrd. Euro).

Von den 61,3 Mrd. Euro entfielen 27,4 Mrd. Euro auf die Deutsche Telekom AG. Dies entspricht einem Marktanteil von ca. 44,7 %. In 2023 lag er bei ca. 43,0 %, 2022 bei ca. 42,7 %. Die Deutsche Telekom baut ihren Marktanteil somit aus. Aus diesem Grund spricht die Bundesnetzagentur im Vorwort ihres Berichts nicht von einer Steigerung des Wettbewerbs, sondern davon, das Wettbewerbsniveau zu halten.

Während die Außenumsatzerlöse der Wettbewerber der Telekom absolut sinken, konnte der Marktführer seine Außenumsatzerlöse um kräftige 6,6 % erhöhen.

Festnetz versus Mobilfunk

Interessant ist auch der Umsatzvergleich zwischen Festnetz und Mobilfunk. Die Außenumsatzerlöse des Telekommunikations-

Smart Building und IT-Sicherheit: Alles ist verbunden

von Dr. Andreas Kaup

Smart Buildings sind Gebäude mit einer modernen digitalen Infrastruktur, hochverfügbarer Konnektivität, moderner IT, einer Basis für das Internet of Things (IoT) und smarter Gebäudeautomation. Alle Informationen und sämtliche Funktionalitäten werden in einer Management-Plattform gebündelt. Für die Realisierung eines solchen holistischen Ansatzes müssen Netz und IT-Infrastruktur von Anfang an bei der Planung mitgedacht werden, da sie das Nervensystem des Gebäudes abbilden. So können diverse gewerkeübergreifende Funktionalitäten und ein digitales Nutzererlebnis realisiert werden. Gleichzeitig kann die Datenverfügbarkeit die Energieeffizienz des Gebäudes maßgeblich steigern.

Ergänzend dazu benötigt der zukünftige Gebäudebetrieb ein Betreiberdatenmodell, in dem die Bedarfe des technischen und betriebswirtschaftlichen Gebäudemanagements zusammengeführt werden – eine Verbindung zwischen Facility- und Real-Estate-Management ohne Informations- und Datenbruch. Die Konsolidierung sämtlicher für den Gebäudebetrieb relevanter Informationen in einer zentralen digitalen Verwaltungsschale wird im Projekt „Gebäudebetrieb 4.0“ vom Smart-Building-Reallabor der Hochschule Mainz entwickelt. Ziel ist es, einen durchgängig digitalisierten, interoperablen, sicheren und effizienten Gebäudebetrieb zu ermöglichen.

Das Konzept Gebäudebetrieb 4.0 basiert maßgeblich auf einer Message-Queueing-Telemetry-Transport-(MQTT-)Kommunikationsstruktur. In diesem Artikel werden neben der Vorstellung einer Smart-Building-Topologie und des Gebäudebetriebs 4.0 insbesondere eine IT-Sicherheitsarchitektur für die MQTT-Struktur erläutert.

ComConsult — Smart-Building-Planung

Bereits seit vielen Jahren beschäftigt sich ComConsult mit der Planung, dem Netzwerk und der IT-Infrastruktur von Smart Buildings. Alle Anforderungen, Herausforderungen und Chancen von Smart Buildings in einem einzigen Artikel abzubilden, wäre nicht möglich. Deshalb erhalten Sie einleitend eine Themen- und Artikelübersicht mit ausgewählten Zitaten:

- Moderne Gebäude: Eine Netzplanung für alle? Von Dr. Johannes Dams: „Das Gebäude der Zukunft braucht IT-Infrastrukturen, die über unterschiedliche Gewerke hinweg verschiedenste Endgeräte und Technologien auf IP-Basis vereinen“ [1].
- Sichere Kommunikationsprotokolle in der Gebäudeautomation – im Fokus: BACnet Secure Connect von Dr. Andreas Kaup: „Um eine Kommunikation zwischen allen Systemen der Gebäudeautomatisierung und -steuerung zu ermöglichen, bedarf es herstellerunabhängiger Kommunikationsprotokolle. Da die Netzwerke der Gebäudetechnik für moderne Gebäude keine geschlossenen Systeme mehr sind, wird die IT-Sicherheit in der Gebäudeautomation stetig wichtiger [2].
- Bauprojekte und die Planung des Netzes von Dr. Johannes Dams: „Bereits vor der eigentlichen IT-Planung sollte feststehen, welche Gewerke gegebenenfalls eigene Netze mitbringen (z. B. Medientechnik oder Gebäudetechnik). Anknüpfungspunkte sollten dabei festgelegt werden. Diese Entscheidung kann einen erheblichen Einfluss auf das Bauprojekt und den späteren Betrieb haben“ [3].
- GA-IT-Infrastruktur – Nachrüsten und Modernisierung der Gebäudeautomation gemäß GEG und EPBD von Dr. Andreas: „Kurz gesagt – eine Verpflichtung zur Datenerhebung und

Digitalpakt 1.0 vs. 2.0 – einfach erklärt…

von Peter Steufmehl

Digitalpakt 2.0: Schulen werden dauerhaft modern

Schulen in Deutschland digital auf den neuesten Stand zu bringen, ist eine riesige Aufgabe. Ende 2025 gab es eine neue Einigung - den Digitalpakt 2.0. Damit beginnt eine neue Phase, in der es um viel mehr geht als nur um den käuflichen Erwerb von Laptops.

Was ist neu?

Früher – Digitalpakt 1.0: Es ging vor allem um die Technik, also um WLAN und Geräte. Durch die Coronapandemie musste vieles oft sehr schnell umgesetzt werden. Zumindest war das die Erwartungshaltung.

Heute – Digitalpakt 2.0: Digitales Lernen soll nun zum festen Alltag und dauerhaft in den Schulalltag integriert werden und funktionieren.

Meine Fragestellungen

Ich habe mir angeschaut, wie die Maßnahmen organisiert sind und woher die Gelder zur Finanzierung kommen. Dabei vergleiche ich die neuen Regeln mit den Erfahrungen aus den letzten Jahren. Besonders wichtig ist mir dabei:

- Wie stellt man die Anträge auf Förderung?
- Wie kommen private Schulen an das Geld?
- Wie werden Förderschulen (zum Beispiel von Landschaftsverbänden) unterstützt? Hier habe ich einen persönlichen Bezug und möchte daher diesen Aspekt ebenfalls erwähnen.

Digitalpakt 2.0: Warum das Internet in der Schule jetzt Alltag wird

Früher dachte man, man kauft einmal Laptops und das war's. Heute weiß man: Digitale Bildung zu betreiben ist eine Daueraufgabe. Der Staat sieht es jetzt als seine Daueraufgabe an, dafür zu sorgen, dass die Technik in den Schulen funktioniert.

Ein Rückblick: Was bisher geschah – Digitalpakt 1.0

Zwischen 2019 und 2024 hat Deutschland so viel Geld in Schulen gesteckt wie noch nie zuvor – insgesamt 6,5 Milliarden Euro. Fast alle Schulen (rund 30.000) haben Geld bekommen. Damit wurden vor allem Laptops für Schüler und Lehrer gekauft und das Internet, somit die IT-Infrastruktur, in den Gebäuden verbessert. Fast das gesamte Budget wurde verplant und genutzt.

Was hat gefehlt?

Obwohl inzwischen viele Endgeräte vorhanden sind, haben sich Probleme ergeben, deren Ausmaß unterschätzt wurde:

- Wer repariert die Geräte, wenn sie kaputtgehen? (Wartung)
- Wer hilft, wenn die Technik streikt? (Support)
- Wie lernen Lehrer, mit den neuen Programmen zu unterrichten? (Fortbildung)

Umzug von Netzwerk-Komponenten für die Rechenzentren eines großen Dienstleisters

Mit Oliver Kloß sprach Christiane Zweipfennig

Ausfälle und End-of-Life-Status der Komponenten stellten Sicherheitsrisiko dar.

Die Modernisierung bestehender Netzwerk-Infrastrukturen in großen Rechenzentren ist mit erheblichem technischen und organisatorischen Aufwand verbunden. Insbesondere der Austausch und Umzug zentraler Komponenten wie Switches und Server erfordert eine sorgfältige Planung und eine präzise Umsetzung, um Ausfallzeiten zu minimieren und den laufenden Betrieb sicherzustellen.

Oliver Kloß absolvierte ein duales Studium zum mathematisch-technischen Softwareentwickler mit Schwerpunkt auf mathematischer Programmierung. Bereits vor Beginn seiner Ausbildung durchlief er ein einwöchiges Praktikum bei ComConsult. Nach seinem Anschluss entschied er sich für eine Tätigkeit im Beratungsumfeld und stieg im Januar 2024 bei ComConsult ein. Er ist im Competence Center Netze tätig und unterstützt dort bei der Konzeption und Planung von Gebäudenetzen, begleitet deren Umsetzung sowie die Übergabe an Betriebspartner. Aktuell arbeitet er im Rahmen eines Projekts an der Erneuerung der Netzwerk-Infrastruktur der Rechenzentren eines Dienstleisters mit, wovon er in diesem Interview erzählt.

Was hatte den Kunden veranlasst, die Netzwerk-Infrastruktur seiner Rechenzentren zu erneuern?

In den vergangenen Jahren kam es bei mehreren eingesetzten Switches wiederholt zu Ausfällen. Zudem hatten diese Systeme inzwischen ein Alter erreicht, in dem sie vom Hersteller nicht mehr mit aktuellen Updates versorgt wurden. Da dies ein erhebliches Sicherheitsrisiko darstellte, wurde die Entscheidung getroffen, die Rechenzentren – zumindest in wesentlichen Teilen – auf eine moderne, aktuelle Infrastruktur umzustellen.

Worum geht es bei diesem Projekt im Kern?

Der Schwerpunkt liegt auf der Erneuerung der Netzwerk-Komponenten, beginnend bei den Core-Switches bis hin zu den Access-Switches. Im Serverbereich werden zahlreiche Systeme auf die neue Infrastruktur migriert. Gleichzeitig entfallen einige Server, da bestimmte Funktionen in Cloud-Servi-

Umfangreiche Modernisierung von Netzwerk und Serverlandschaft

SOC-Strukturen verstehen: Wege zu einer effektiven Sicherheitsüberwachung

von Esther Perl

Weshalb ein Security Operations Center (SOC) heute eine entscheidende Rolle im Security Monitoring spielt

Cyberangriffe werden schneller, gezielter und zunehmend professionell orchestriert. Für Unternehmen bedeutet das: Sicherheitsvorfälle können jederzeit auftreten, unabhängig von Branche oder Größe. Gleichzeitig sind moderne IT-Landschaften hochdynamisch und verteilen sich über On-Premises-Systeme, Cloud-Services und mobile Arbeitsumgebungen. Dadurch steigt die Menge sicherheitsrelevanter Daten stetig, und die Anforderungen an eine zuverlässige Überwachung wachsen weiter.

Um potenzielle Angriffe rechtzeitig zu erkennen, braucht es ein kontinuierliches und strukturiertes Security Monitoring. Bereits in meinem zuletzt veröffentlichten Blog habe ich aufgezeigt, warum der Mensch und die Technik für ein Security Operations Center (SOC) und automatisiertes Security Monitoring zusammengehören. Doch der Betrieb eines SOC stellt Unternehmen vor großen Herausforderungen. Neben technologischen Fragen stehen vor allem Ressourcen, Fachkräftemangel und die Verfügbarkeit von Spezialwissen im Fokus. Viele Organisationen merken schnell: Ein SOC „nebenbei“ aufzubauen und zu betreiben ist kaum möglich – es erfordert klare Verantwortlichkeiten, Prozesse, Expertise und 24/7-Überwachungskapazitäten.

Damit rückt die Frage nach dem passenden SOC-Modell in den Mittelpunkt. Soll das SOC intern aufgebaut werden, um Wissen und Kontrolle im Unternehmen zu halten? Ist ein externes Managed SOC sinnvoll, das rund um die Uhr professionelle Überwachung bietet? Oder empfiehlt sich ein hybrider Ansatz, der die Stärken beider Modelle kombiniert? Jede Variante hat spezifische Vorteile, Risiken und organisatorische Implikationen. Die Wahl des richtigen Modells entscheidet letztlich darüber, wie effektiv Sicherheitsvorfälle erkannt, bewertet und bewältigt werden.

Was ein SOC eigentlich leistet – Funktionen, Prozesse und Rollen

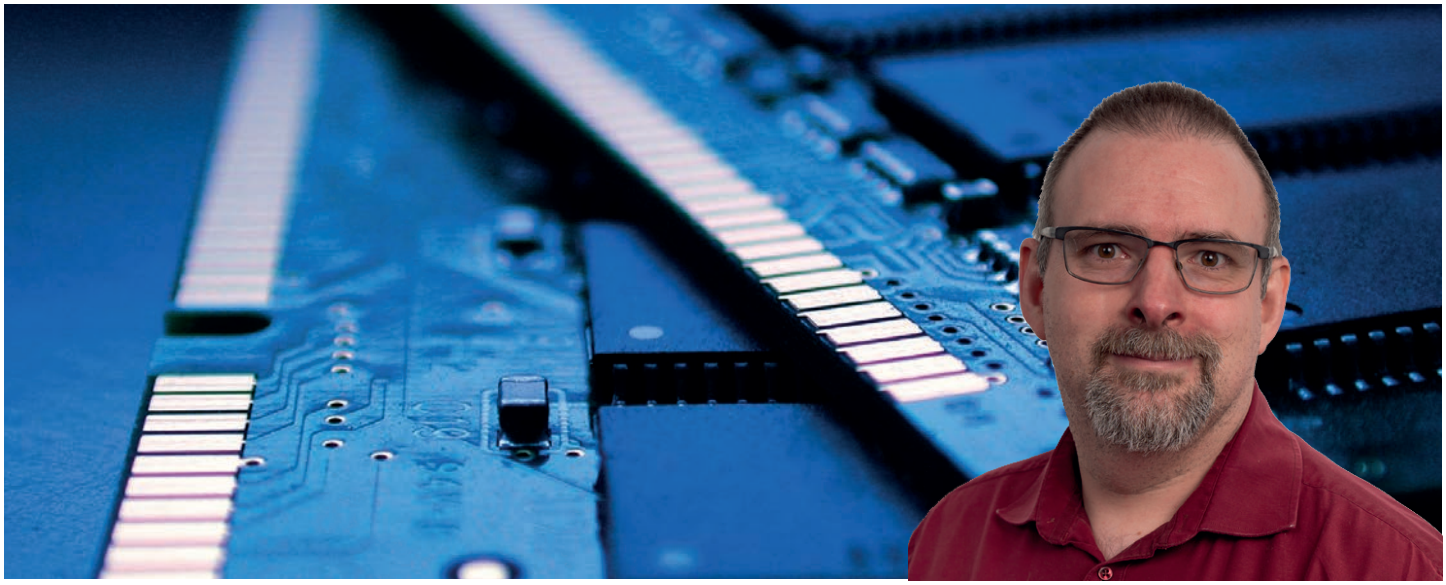
Kernaufgaben des SOC

Das SOC ist eine zentrale Instanz des Security-Monitorings zur Überwachung, Analyse und Steuerung von sicherheitsrelevanten Ereignissen in einem Unternehmen. Es ist die zentrale Stelle, an der sicherheitsrelevante Ereignisse zusammenlaufen, die von Systemen zur Angriffserkennung sowie von anderen Monitoring-Tools gemeldet werden.

Das SOC-Team, bestehend aus spezialisierten Security Analysten mit unterschiedlichen Erfahrungsstufen, steuert gemeinsam mit den unterstützenden Systemen die Erkennung und Behebung von Sicherheitsvorfällen. Es prüft die gemeldeten sicherheitsrelevanten Ereignisse, ordnet diese ein und leitet bei Bedarf Sofortmaßnahmen ein. Ein weiterer zentraler Aufgabenbereich ist die

Teurer RAM führt zu teuren Servern

von Dr. Markus Ermes



Wir haben es wahrscheinlich alle mitbekommen: Arbeitsspeicher und SSDs werden aktuell immer teurer. Innerhalb von weniger als 3 Monaten haben sich die Preise für RAM im Server-Bereich mehr als verdoppelt, und auch SSDs sind nicht von Preiserhöhungen verschont geblieben. Zusätzlich hat Western Digital (WD) gerade kommuniziert, dass nahezu alle 2026(!) produzierten, drehenden Platten bereits verkauft sind.

Die Ursache

Wie viele aktuelle Entwicklungen in der IT, so sind** auch die Preiserhöhungen bei RAMs, GPUs, SSDs und demnächst vielleicht HDDs auf den aktuellen KI-Hype zurückführen: Die für einen vermeintlichen Fortschritt benötigten und immer größeren KI-Modelle haben einen unstillbaren Hunger auf Speicher in all seinen Formen – sei es extrem schneller Speicher für Beschleuniger, Arbeitsspeicher oder Speicher, auf dem die Trainingsdaten abgelegt werden sollen. Zusammen mit den aktuellen Planungen für riesige Rechenzentren ergibt sich eine enorme Nachfrage, während das Angebot bisher zwischen großen und kleinen Kunden aufgeteilt wurde. Da aber die Marge im Bereich KI viel höher ist und das Geld (noch) locker sitzt, können die Hersteller von Speicherbausteinen nahezu beliebige Preise verlangen.

Was bedeutet das für „normale“ Unternehmen?

Schauen wir uns die Auswirkungen an einem Beispiel an: Immer mehr Virtualisierungslösungen setzen auf verteilten Storage, bei dem in den Servern verbaute Speichermedien (typischerweise SSDs) zu einem gemeinsamen Storage zusammengefasst werden, ohne einen dedizierten, zentralen Speicher zu benötigen. Durch die Preiserhöhungen können die Mehrkosten für einen typischen Server zwischen 25 und 50 % liegen!

Je größer die CPU und je kleiner RAM und lokaler Storage, desto weniger macht die Preiserhöhung aus. Die Tendenz geht jedoch zu Servern mit mehr Arbeitsspeicher und Storage, besonders bei KI-Systemen. Auch bei den GPUs steigen die Preise langsam, da sie ebenfalls RAM benötigen.

Insgesamt zeigt sich also, dass der aktuelle KI-Hype auch signifikante Auswirkungen auf andere Bereiche und Firmen hat, die ihre Server-Landschaft erneuern oder erweitern möchten.

Die Auswirkungen auf Privatleute

Für normale Privatleute, die alte Systeme erneuern, oder Gamer, die in 4k spielen wollen, ist die Situation ähnlich: Die Preise für PCs und schnelle Gaming-Rechner haben sich etwa verdoppelt. Die Hersteller von Arbeitsspeicher greifen für Privatkunden nicht umsonst wieder zu DDR4- und teilweise DDR3-RAM, sodass alten Systemen noch eine kleine Gnadenfrist bleibt.

Ist ein Ende der Preisspirale in Sicht? Meiner Meinung nach nicht direkt.

Der Ausbau der Kapazitäten kommt! Aber langsam…

Micron, der aktuell drittgrößte RAM-Hersteller, mit einem Marktan-