Juli 2024

ComConsult GmbH
Beratung + Planung + Schulung

# Der Netzwerk Insider

## Bauprojekte und die Planung des Netzes

**von Dr. Johannes Dams**

Immer wieder thematisieren wir im Insider die Herausforderungen von Netzwerkplanungen im Rahmen von Bauprojekten. Zuletzt sowohl auf unserer Sonderveranstaltung Netze als auch in einem Insider-Artikel vom Oktober 2023 von Sven Tekaat [1]. Während die Planung und Beglei-tung der Umsetzung von Netzwerken in Bauprojekten für uns zum Alltagsgeschäft gehören, ist es für die IT-Verantwortlichen unserer Kunden häufig eher eine Ausnahme vom Betriebs-alltag. Welches Unternehmen baut schon ständig neue Standorte und Gebäude?

Seite 7

## LAN und WLAN: Alles von einem Hersteller?

**von Dr. Behrooz Moayeri**

In mehreren aktuellen Projekten müssen wir die Beschaffung von LAN- und WLAN-Komponenten planen, zum Beispiel weil die bestehenden Komponenten das Ende ihres Lebenszyklus erreicht haben. Nun stellt sich die Frage, ob alle neuen LAN- und WLAN-Komponenten von einem Hersteller stammen sollten.

Seite 2

## Wie Smart Contracts zur Digitalisierung beitragen können

**von Prof. Dr. Tobias Fertig**

Die Blockchain-Technologie steht oft in einem schlechten Licht, da nicht selten hoher Strom-verbrauch und unregulierte Spekulationen mit Kryptowährungen in den Köpfen präsent sind. In den letzten Jahren haben sich jedoch die Technologie, die Standards und die Tools enorm weiterentwickelt.

Seite 24

Webinar der Woche

## Microsoft 365 Copilot in Aktion

Seite 21

## Eine neue Sicherheitslücke bei VMware und die Auswirkungen der neuen Lizenzpolitik

**von Dr. Markus Ermes**

Es ist schneller passiert, als ich es persönlich vermutet hätte: Es wurde eine Sicherheitslücke in Virtualisierungslösungen von VMware (bzw. jetzt Broadcom) bekannt, die einen Ausbruch aus virtuellen Maschinen erlaubt und alle gängigen Produkte betrifft.

Seite 18

# LAN und WLAN: Alles von einem Hersteller?

von Dr. Behrooz Moayeri

In mehreren aktuellen Projekten müssen wir die Beschaffung von LAN- und WLAN-Komponenten planen, zum Beispiel weil die bestehenden Komponenten das Ende ihres Lebenszyklus erreicht haben. Nun stellt sich die Frage, ob alle neuen LAN- und WLAN-Komponenten von einem Hersteller stammen sollten.

## Vorteile eines homogenen Netzes

Ein homogenes Netz mit Komponenten von nur einem Hersteller bietet sicher Vorteile. Zu den Vorzügen einer einheitlichen Produktumgebung im Netz zählen die folgenden:

- Herstellerspezifische Mechanismen gehen über Standardfunktionen hinaus.
- Das Service- und Maintenance-Modell ist in einem homogenen Netz einfacher.
- Der Schulungs- und Einarbeitungsaufwand kann in einer einheitlichen Netzlandschaft optimiert werden.
- Das Management eines Netzes mit Komponenten desselben Herstellers ist mit weniger Herausforderungen verbunden als in einem heterogenen Netz.
- Angesichts zunehmender Anforderungen an die Betriebssicherheit und Verfügbarkeit des Netzes ist es wichtig, bei Störungen und Problemen die Verantwortung einem einzigen Hersteller zuordnen zu können und jegliches Fingerpointing zwischen verschiedenen Herstellern auszuschließen.

An den oben genannten Argumenten hat sich in den letzten 30 Jahren nichts geändert.

## Netze sind anders als vor 30 Jahren

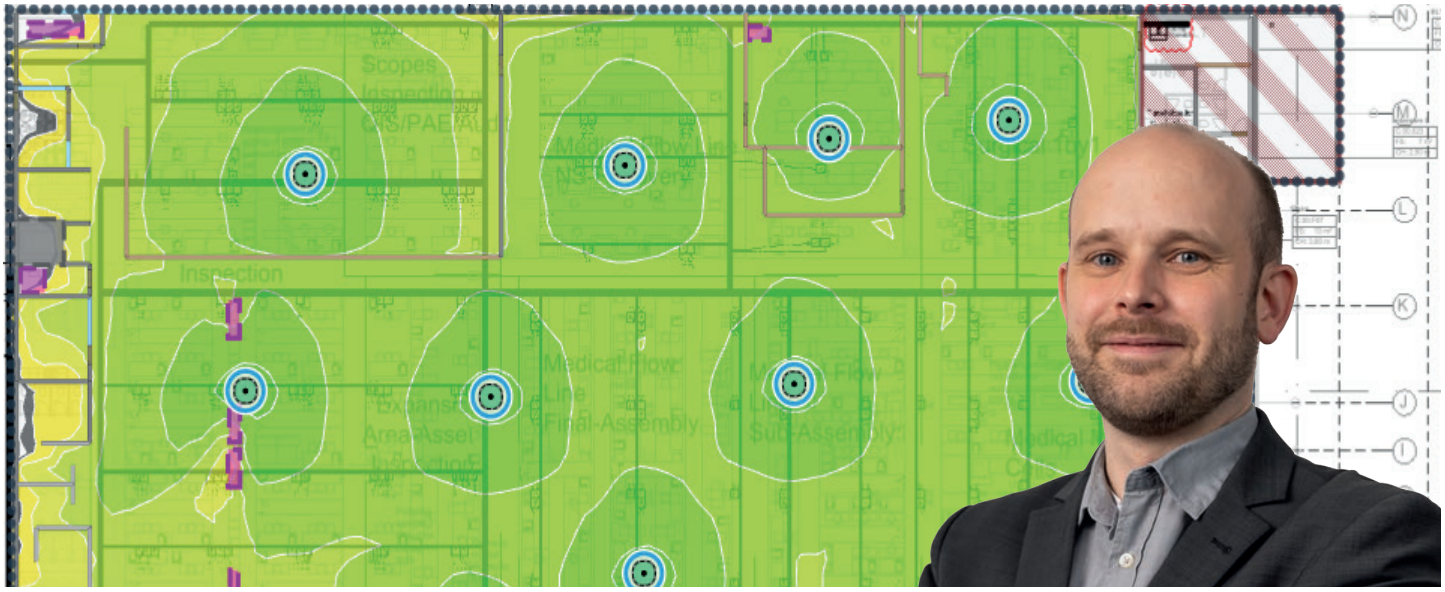
Während für eine homogene Netzlandschaft dieselben Vorzüge geltend gemacht werden können wie vor drei Jahrzehnten, sind die heutigen Netze in mancher Hinsicht anders als in den 1990er Jahren:

- LAN-Bereiche im RZ und außerhalb der Rechenzentren sind in der Regel aus Sicherheitsgründen entkoppelt. Im RZ gibt es hinsichtlich Bitraten und der zu unterstützenden Verfahren ganz andere Anforderungen zu erfüllen als außerhalb der Rechenzentren.
- Wireless LAN und kabelgebundenes LAN haben ihre weitgehend getrennten Eigenleben. Hersteller mit den besten WLAN-Lösungen haben nicht unbedingt die besten LAN-Komponenten und umgekehrt. Andererseits lässt sich die WLAN-Umgebung von einem Hersteller mit dem LAN eines anderen ohne größere Probleme kombinieren.
- Hersteller haben sich spezialisiert. Einige sind im RZ-Bereich sehr innovativ, andere im Bereich IP-Routing, wiederum andere im Access-Bereich.

Vor dem Hintergrund der oben genannten Entwicklungen ist die Frage nach einer einheitlichen Quelle für den Bezug von Netzkomponenten oder der Diversifizierung neu zu beantworten.

## Nachteile der Abhängigkeit von einem Hersteller

Hersteller von Netzkomponenten sind profitorientierte Unternehmen. Im Netzwerk Insider vom Mai 2024 habe ich am Beispiel VMware die Nachteile der Abhängigkeit von einem Hersteller dargestellt, nachdem ich in der Insider-Ausgabe im April 2024 getitelt hatte, dass Hersteller und ihre Kunden unterschiedliche Interessen haben. Das gilt auch für LAN- und WLAN-Hersteller. Daher denken zurzeit einige Organisationen, die bisher nur Netzkompo-



# Bauprojekte und die Planung des Netzes

von Dr. Johannes Dams

Immer wieder thematisieren wir im Insider die Herausforderungen von Netzwerkplanungen im Rahmen von Bauprojekten. Zuletzt sowohl auf unserer Sonderveranstaltung Netze als auch in einem Insider-Artikel vom Oktober 2023 von Sven Tekaat [1]. Während die Planung und Begleitung der Umsetzung von Netzwerken in Bauprojekten für uns zum Alltagsgeschäft gehören, ist es für die IT-Verantwortlichen unserer Kunden häufig eher eine Ausnahme vom Betriebsalltag. Welches Unternehmen baut schon ständig neue Standorte und Gebäude?

Damit ist verständlich, dass ohne diese Erfahrung viele Probleme vorher nicht bekannt sind. Doch auch bei der Projektsteuerung und den Bauherren fehlt oftmals der Weitblick, den IT in modernen Gebäuden erfordert.

Bei unseren Projekten zeigen sich immer wieder Reibungspunkte zwischen der IT-Planung und dem eigentlichen Bauprojekt. Daher möchte ich die Gelegenheit nutzen, um nochmal den Fokus auf diese Themen zu lenken.

Die grundlegende Komplexität des Themas IT- und Netzwerkplanung sollte in einem Bauprojekt allen Beteiligten klar sein.

## Die Rolle als Planer und wie man Bauprojekte als „Aktiv-Planer“ erlebt

Als Planer für das aktive Netzwerk hat man im Bauprojekt vor allem die Aufgabe festzulegen, welche Switches, Router, Firewalls und WLAN-Komponenten benötigt werden und wo diese verbaut werden. Für WLAN-Access-Points ist die Festlegung der Montageposition von besonderer Bedeutung.

Oberflächlich betrachtet ist damit die Rolle des Fachplaners der Netztechnik sehr einfach. Im Detail wird man jedoch schnell feststellen, dass die zentrale Rolle der IT für alle Bereiche der späteren Gebäudenutzung besonderen Abstimmungsbedarf bedeutet.
Die Art der Abstimmung variiert je nach Projekt. Man kann sich vorstellen, dass verschiedene Teile der IT- bzw. Netzplanung unterschiedlich stark mit den klassischen Bereichen des Bauprojekts verflochten sind. Beispielsweise benötigen die aktiven Netzkomponenten zwar Schrankplatz und damit auch einen IT-Raum, doch kann ihre Planung relativ unabhängig erfolgen. Abgesehen natürlich von Stromversorgung, Klimatisierung und Sicherheitstechnik für den Raum. Im Gegensatz dazu haben die im Gebäude in der Fläche verteilten Positionen der WLAN-Access-Points größeren Einfluss auf das Bauprojekt, da sie Architektur, Optik, Kabelwege etc. betreffen.

Die Unterschiede dieser Aspekte zwischen diversen Bauprojekten und die unterschiedliche Rolle des Netz-Planers können anhand einiger Beispiele anschaulich dargestellt werden:

- Bauprojekt im europäischen Ausland, Produktionsgebäude:
  - Zentrale Rolle des IT-Planers: Vertretung der IT-Anforderungen der zentralen IT-Abteilung und Detailplanung
  - Standards des späteren Nutzers (und anderer Standorte) müssen eingehalten werden. Eine Grobkonzeption ist in diesem Fall bereits vorhanden.
  - Lokale Normen sind zu berücksichtigen.
  - Strukturierung der IT-relevanten Themen, damit die Umsetzung den Standards folgt.

# Eine neue Sicherheitslücke bei VMware und die Auswirkungen der neuen Lizenzpolitik

von Dr. Markus Ermes

Es ist schneller passiert, als ich es persönlich vermutet hätte: Es wurde eine Sicherheitslücke in Virtualisierungslösungen von VMware (bzw. jetzt Broadcom) bekannt, die einen Ausbruch aus virtuellen Maschinen erlaubt und alle gängigen Produkte betrifft. Dabei gibt es gute und schlechte Nachrichten:

Die gute Nachricht ist, dass bereits Patches für die Sicherheitslücke existieren.

Die schlechte Nachricht ist, dass mit dem Ende der kostenlosen ESXi-Version nicht alle Nutzer davon profitieren können.

## Der neueste Patch für VMware-Virtualisierungslösungen

Am 24.5.2024 wurde ein Patch für diverse Virtualisierungsprodukte veröffentlicht – von den eher Workstation-fokussierten Lösungen Workstation und Fusion bis hin zum vielleicht wichtigsten Produkt im VMware-Portfolio, dem ESXi-Hypervisor.

Schaut man sich die Patch-Notes an, so sieht man: Der Patch schließt einige Sicherheitslücken, die laut Common Vulnerability Scoring System (CVSS) als „hoch“ und auf der Webseite von Broadcom sogar als „kritisch“ eingestuft werden.

Besonders interessant (speziell für Angreifer) ist dabei die Tatsache, dass diese Sicherheitslücken einen Ausbruch aus der jeweils angegriffenen virtuellen Maschine erlauben und im schlimmsten Fall sogar zu Code-Ausführung auf dem physischen Host führen können. Das ist in einem stark konsolidierten Rechenzentrum keine schöne Vorstellung. Dieses Szenario wird dadurch abgeschwächt, dass zur Ausnutzung bestimmte andere Voraussetzungen erfüllt sein müssen.

Allerdings ist der Patch da, dann ist das doch alles kein Problem, oder? Nun ja, man muss hier zwei Aspekte berücksichtigen. Einer davon ist eine generelle Herausforderung in vielen IT-Abteilungen, der andere hat seinen Ursprung in der neuen Lizenzpolitik von Broadcom nach der Übernahme von VMware.

## Aspekt 1: Einspielen von Updates

Ja, dass die Sicherheitsupdates verfügbar sind, ist natürlich sehr gut. Und man könnte meinen: Dann spiele ich die Updates halt morgen ein, und alles ist gut. Doch so einfach ist es mit einer in vielen Rechenzentren so zentralen Lösung wie einem Hypervisor nicht. Wenn hier etwas schiefgeht, kann das ein komplettes Unternehmen lahmlegen. Daher muss ein solches Update gut geplant und getestet werden. Das ist nichts Neues. Man testet das Update in einer möglichst abgeschotteten Umgebung und stellt

# Wie Smart Contracts zur Digitalisierung beitragen können

von Prof. Dr. Tobias Fertig

Die Blockchain-Technologie steht oft in einem schlechten Licht, da nicht selten hoher Stromverbrauch und unregulierte Spekulationen mit Kryptowährungen in den Köpfen präsent sind. In den letzten Jahren haben sich jedoch die Technologie, die Standards und die Tools enorm weiterentwickelt. Die Anzahl der Entwickler von Smart Contracts wächst, und immer mehr Anwendungsfälle für Smart Contracts werden identifiziert. Dennoch fehlt einiges an Arbeit, um eine breite Akzeptanz der Technologie zu erzielen.

Viele Organisationen haben bereits vor einigen Jahren geprüft, ob die Blockchain-Technologie für ihre Zwecke einsetzbar ist. Oftmals wurden Ideen verworfen, da der Aufwand zu hoch war und passende Infrastrukturen fehlten. Doch hat sich in den letzten Jahren viel getan, und passende Infrastrukturen sind vorhanden – auch in Deutschland. Deshalb ist es schade, wenn an alten Ansichten festgehalten wird und viele Anwendungsfälle in den Schubladen verschwinden. Mit diesem Artikel möchte ich Ihren Wissensstand aktualisieren und Sie dazu anregen, erneut die Anwendbarkeit der Blockchain-Technologien zu prüfen.

Ich selbst habe in 2023 eine Machbarkeitsstudie zu Genehmigungsverfahren industrieller Anlagen durchgeführt. Generell fehlt es bei Genehmigungsverfahren in Deutschland an Digitalisierung, da die meisten Anträge aktuell noch analog auf Papier erstellt werden müssen. Selbst wenn eine elektronische Übermittlung erfolgt, werden die Genehmigungsbescheide auf Papier ausgestellt, und alle zugehörigen Unterlagen gestempelt. Der Stempel soll dabei die Manipulationssicherheit erwirken, die eine digitale Lösung nicht gewährleisten kann. Hierbei werden ganze Kopierräume bei Konzernen verschlissen, um die nötigen Dokumente auf analogem Wege bereitzustellen.

Mithilfe der Blockchain-Technologie konnten wir jedoch ein Konzept entwickeln, welches trotz oder Dank der Digitalisierung eine sehr hohe Manipulationssicherheit bietet. Wir setzten dabei auf Smart Contracts, die Hash-Werte der zugehörigen Dokumente mit einem Zeitstempel versehen. Somit ist auch nach vielen Jahren sichergestellt, dass keine Manipulation rückwirkend möglich ist. Die Behörden waren erleichtert und stimmten der Digitalisierung zu. Auch den Industriepartnern konnte die Angst vor dem Verlust von Betriebsgeheimnissen genommen werden. In den Smart Contracts werden keine sensiblen Daten gespeichert, sondern lediglich Hash-Werte und Zeitstempel. Es ist somit unmöglich, über die Blockchain an sensible Daten zu gelangen. Nur wer die Daten bereits besitzt, kann diese validieren.

Zugegeben, der Anwendungsfall ist hier sehr klein gehalten, dennoch löst er zwei schwerwiegende Probleme: den Schutz der Betriebsgeheimnisse und die Angst vor Manipulation. Gerade die Reduktion des Anwendungsfalls auf das Wesentliche macht die Nutzung von Smart Contracts so interessant. Deshalb empfehle ich immer zu Beginn, den Anwendungsfall möglichst klein zu halten. Dadurch bleibt er realisierbar, und die Komplexität der Smart Contracts überschaubar.

Doch was ist eigentlich mit dem Problem der fehlenden Infrastruktur und den hohen Energiekosten? Je nach benötigter Infrastruktur gibt es aktuell viele Möglichkeiten. Ich empfehle immer Ethereum-basierte Technologien, damit das Problem eines Vendor-Lock-Ins reduziert wird. Ethereum besitzt die größte Community und die meisten Entwickler-Tools, weshalb sehr viele Lösungen für Ethereum-basierte Technologien verfügbar sind. So betreibt beispielsweise die govdigital eG (https://www.govdigital.de/) unter der Leitung von Peter Niehues eine nationale, konsortiale Blockchain basierend auf Ethereum. Die Besonderheit dieser Infrastruktur liegt darin, dass sie bereits über alle Bundesländer