Juni 2024

ComConsult GmbH
Beratung + Planung + Schulung

# Der Netzwerk Insider


## Sicherheitsmanagement in kritischen Infrastrukturen

**von Thomas Steil**

*„Wir müssen größere, stärkere Risiken, mit den größten und stärksten Vorsichtsmaßnahmen, auf uns nehmen.“* Dieses Zitat, welches Rudyard Kipling zugeschrieben wird, hat für die Absicherung von Werten, Gebäuden und Infrastruktur nicht an Bedeutung verloren. Ressourcen sind begrenzt. Zudem stellen Sicherungsmaßnahmen oft eine Einschränkung für betriebliche Abläufe dar. Daher wird es nicht gelingen, in allen Bereichen den maximalen Schutz umzusetzen.

Seite 7

## Die immer noch unterschätzten IT-Energiekosten

**von Dr. Behrooz Moayeri**

Man sollte meinen, spätestens mit dem Anstieg der Energiekosten in den letzten Jahren, der in den Medien immer wieder thematisierten Energiewende und speziell mit der Diskussion über das Gebäudeenergiegesetz sei das Bewusstsein über die notwendige Energieeffizienz der Informationstechnik (IT) genug geschärft. Weit gefehlt, wie mir meine letzten Projekterfahrungen vor Augen geführt haben.

Seite 2

## Object Storage – Grundlagen und Use Cases

**von Dr. Markus Ermes**

Das Thema Object Storage begegnet mir im Projektgeschäft aktuell immer häufiger. Neu ist die Technologie dabei nicht. Besonders bekannt ist diese Art von Storage vor allem aus der Cloud, mit AWS S3 als vielleicht prominentester, aber auch sehr komplexer Object Storage.

Seite 27

Webinar der Woche

## Lizenz-Chaos entwirren

Seite 24

## Funk oder Kabel?

**von Dr. Joachim Wetzlar**

Die Frage, ob man in Büro oder Produktion besser auf Kabel oder stattdessen auf WLAN oder andere Funktechniken zurückgreift, haben wir an dieser Stelle schon verschiedentlich diskutiert. Doch wie sieht es beim weltumspannenden Internet aus? Läuft das nicht inzwischen alles über Satelliten?

Seite 21

# Die immer noch unterschätzten IT-Energiekosten

von Dr. Behrooz Moayeri

Man sollte meinen, spätestens mit dem Anstieg der Energiekosten in den letzten Jahren, der in den Medien immer wieder thematisierten Energiewende und speziell mit der Diskussion über das Gebäudeenergiegesetz sei das Bewusstsein über die notwendige Energieeffizienz der Informationstechnik (IT) genug geschärft. Weit gefehlt, wie mir meine letzten Projekterfahrungen vor Augen geführt haben.

## Formel für Energiekosten

Green IT ist kein neuer Begriff und stammt aus den 90er Jahren. Damals veröffentlichte die US-Umweltschutzbehörde EPA (https://www.epa.gov) das sogenannte EnergyStar-Label, mit dem energiesparende Monitore sowie andere IT-Geräte gekennzeichnet wurden. Vor Jahren wurden öffentliche Auftraggeber im deutschen Vergaberecht verpflichtet, in ihren Beschaffungen Energieeffizienz zu berücksichtigen.

Von ComConsult aktuell ausgearbeitete Ausschreibungsunterlagen berücksichtigen für die Kostenbetrachtung nicht nur die Beschaffung von Hardware, sondern auch die mit dem Betrieb der Hardware verbundenen Energiekosten. Selbst wenn unklar ist, welcher mittlere Verbrauch in Watt bzw. kW sich für ein Stück Hardware nach jahrelanger Nutzung ergeben haben wird, kann man von vertretbaren Annahmen ausgehen, zum Beispiel 50 % des maximalen Verbrauchs. Der Preis pro kWh ist variabel. Auch hier muss man eine Annahme treffen, was den mittleren Preis über die nächsten Jahre betrifft. Gehen wir von 0,50 Euro netto aus, obwohl die Preise nach dem Spitzenwert vor ungefähr zwei Jahren im Moment deutlich gesunken sind. Trotzdem sollte man eher skeptisch als euphorisch sein und langfristig besser von steigenden Preisen ausgehen, denn die Energiewende hat erst begonnen, und erhebliche Investitionen in neue Energiequellen und vor allem das Leistungsnetz wollen bezahlt werden.

In Rechenzentren und Technikräumen müssen wir zusätzlich noch berücksichtigen, dass solche Räume zu kühlen sind. Selbst moderne RZ-Flächen, die nach dem neuesten Stand der Klima- und Belüftungstechnik ausgestattet sind, fügen dem Verbrauch 20 bis 30 % hinzu. Man spricht vom Faktor Power Usage Effectiveness (PUE), der für neue Rechenzentren 1,3 nicht überschreiten darf. Wir haben es oft jedoch mit einer Mischung von sehr alten, alten und neuen Räumen zu tun. Es ist in den meisten Fällen gerechtfertigt, einen PUE-Wert von 2 der Kostenbetrachtung für IT zugrunde zu legen.

So kommen wir zu folgender Formel für die Energiekosten:

Zahl der zu betrachtenden Jahre * 365 Tage / Jahr * 24 Stunden / Tag * maximaler Verbrauch in kWh * 0,5 (Verhältnis zwischen mittlerem und maximalem Verbrauch) * 2 (für PUE) * 0,5 Euro / kWh

Pro kW ergeben sich somit bei einer Betrachtung von 5 Jahren Nutzungszeit:

5 * 365 * 24 * 0,5 * 2 * 0,5 Euro = 21.900 Euro netto

## Anteil an den Gesamtkosten

Der Hersteller Cisco gibt für den RZ-Switch Nexus 9364C-GX den maximalen Verbrauch 1622 Watt an und weist in Übereinstimmung mit der obigen Annahme einen „typischen“ (gleich mittleren) Wert von 811 Watt aus, d.h. 0,811 kW. Nach der obigen Formel verursacht ein solcher Switch über die gesamte Nutzungszeit von 5 Jahren Energiekosten in Höhe von 17.760,90

Euro. Der momentane Listenpreis des Geräts liegt laut einschlägigen Quellen im Internet bei 62,069,20 $, d.h. bei ca. 58.000 Euro. Selbst wenn man das Gerät gut mit Transceivern bestückt, kommt man bei Annahme üblicher Rabattsätze auf Hardware-Beschaffungskosten von nicht mehr als 30.000 Euro. Dies bedeutet, dass zu den Beschaffungskosten noch ein Aufschlag von ca. 70 % für Energie hinzukommt.

Bei Servern kann der Anteil von Energie- an den Gesamtkosten noch höher liegen. Ein typischer Server mit ungefähr demselben Verbrauch wie der oben genannte Cisco-Switch kostet in der Regel signifikant weniger als der Switch-Preis.

## Überraschte Techniker

Nicht selten erlebe ich die Überraschung unter Technikern, wenn sie mit dem signifikanten Anteil der Energiekosten an den Gesamtkosten konfrontiert werden. Viele, die bislang nur zwischen den technischen Eigenschaften einerseits und dem Beschaffungspreis andererseits abgewogen haben, müssen nun auch die Energiekosten betrachten. Anders ausgedrückt erfolgt die Kostenbetrachtung nun auf einem viel höheren Niveau, nicht selten dem doppelten. Unterschiede zwischen Gerätetypen und Herstellern können bei Berücksichtigung des Stromverbrauchs zu überraschenden Ausschreibungsergebnissen führen. Leider bedeutet modernere Technik nicht selten höhere Energiekosten. Leistungsfähigere Prozessoren verbrauchen häufig mehr Energie als ihre Vorgängermodelle. Gleiches gilt für Arbeits- und Massenspeicher.

Damit entsteht ein Dilemma. Hersteller können sich durch die Energiebetrachtung im Wettbewerb veranlasst sehen, ältere, dafür sparsamere Hardware anzubieten. Das wird bei der Technik-Fraktion des Auftraggebers Befremden auslösen. Ich erlebe es immer wieder, dass Techniker versuchen, irgendwie an der Energieeffizienz vorbeizumanövrieren, sei es durch Ansetzen eines zu niedrigen „typischen“ Verbrauchs, oder durch die Hoffnung auf ein Preiswunder im Strommarkt, oder in unrealistischer Erwartung einer viel effizienteren Kühlung, ohne dass man investieren muss.

## Der Markt kann Hersteller unter Druck setzen

Die Gleichung „neue Technik = höherer Verbrauch“ muss nicht immer stimmen. Je nach Technik ist möglicherweise sogar das Gegenteil der Fall. Beispiel Storage:

Drehende Festplatten haben den Vorteil, dass sie im Ruhezustand kaum Energie verbrauchen. Der Wechsel von HDD zu SSD war daher mit einem höheren Verbrauch verbunden. Die neue Generation von Storage, nämlich NVMe, senkt den Verbrauch jedoch wieder.

Bei den Prozessoren gilt, dass mit dem künftigen Übergang zur 5-nm-Technik ein niedrigerer Verbrauch erwartet wird.

Es ist durchaus vorstellbar, dass der Markt die Hersteller unter Druck setzt, wenn immer mehr Kunden bei ihren Kaufentscheidungen die Energieeffizienz berücksichtigen. Hersteller können durch mehr Wettbewerb zu Entscheidungen zugunsten effizienterer Technik gezwungen werden.

Die Entscheidungsträger bei den IT-Kunden müssen nicht unbedingt zu Umweltaktivisten mutieren, um den Energieverbrauch gebührend zu berücksichtigen. Die betriebswirtschaftliche Gesamtkostenbetrachtung reicht dafür aus.

## Beispiel Bitcoin

Was Geld betrifft, irren sich Börsen selten. Die insgesamt nach oben zeigende Tendenz des Bitcoin-Preises ist nach meiner Einschätzung auf die langfristige Verteuerung von Energie zurückzuführen. Neue Bitcoins werden technisch durch Herausfinden neuer Zahlen mit vorgegebenen Hash-Werten generiert. Im Gegensatz zur einfachen Operation der Hash-Bildung ist die Umkehrfunktion rechen- und damit energieintensiv. Deshalb ist das Hinzufügen eines neuen Blocks zum Bitcoin-Blockchain in Ländern lukrativer, wo der Energiepreis niedrig ist. Als Gewächshäuser getarnte Bitcoin-Farmen in an fossilen Energieträgern reichen Ländern werden nicht selten entdeckt. Es wird angesichts der weltweit steigenden Energiepreise jedoch immer schwieriger, einen Bitcoin zu schürfen. Knapperes Angebot bedeutet Verteuerung. Um Missverständnisse vorzubeugen, weise ich darauf hin, dass ich selbst keine Kryptowährungen besitze und Sie auf keinen Fall zu einem Run auf Kryptowährungen verleiten will. Denn da kann vieles auf den Preis drücken, von schärferen internationalen Regelungen gegen Geldwäsche bis zur höheren Besteuerung von Spekulationsgewinnen.

Hier möchte ich nur zeigen, dass der weltweite Handelsplatz für Kryptowährungen den internationalen Trend in Richtung teurer Energie antizipiert hat. Gleiches müssen wir in unseren Hardware-Beschaffungen tun.

# Im Netzwerk Insider vor 20 Jahren: Netzwerk- und Systemmanagement

von Dr. Markus Ermes

Vor 20 Jahren wurde im Netzwerk Insider über die Zukunft von Netzwerk- und Systemmanagement spekuliert. Was waren damals die Annahmen? Was hat sich getan? Wie gut waren die Vorhersagen?

## Die Situation vor 20 Jahren

Vor 20 Jahren war in vielen Bereichen ein Umbruch bei der Nutzung von Informationstechnik zu sehen. Angesichts der wachsenden Verbreitung von WLAN, dem Umstieg auf VoIP und der zunehmenden Implementierung von Ethernet in der Fertigung wurde mit einem deutlichen Anstieg der Nutzer- und Endgerätezahlen im Netzwerk gerechnet. Man ging von einem Faktor 10 aus.

In Verbindung mit der immer wichtigeren Rolle der IT-Sicherheit führte das zu der Annahme, dass sich das Netzwerkmanagement kurz- bis mittelfristig signifikant verändern wird, um den neuen Entwicklungen folgen zu können.

Doch was hat sich hier getan?

## Die Situation heute

Netzwerkmanagement war, ist und bleibt ein wichtiges Thema. Viele der Annahmen von damals haben sich bestätigt, vor allem das Zusammenspiel der verschiedenen Netzwerkbereiche (LAN, WLAN, Netzzugangskontrolle nach IEEE 802.1X) ist bei einigen Herstellern mittlerweile innerhalb der Management-Lösungen gut kombiniert. Doch nicht bei allen, und wenn man herstellerübergreifendes Netzwerkmanagement benötigt, wird die Auswahl knapp. Viele Kunden setzen daher immer noch mehrere Systeme ein, die jedoch weitaus mächtiger sind als vor 20 Jahren. Gerade die Themen Firewalling und Überwachung haben sich durch Telemetrie-Funktionen und neue Protokolle wie gRPC ebenfalls deutlich verbessert.

Bei der Leistungsanalyse im Netzwerk hat sich etwas getan, auch abseits der oben genannten Telemetrie-Funktionen. Application Performance Monitoring ist mittlerweile gut umsetzbar, und Profiling für eigenentwickelte Software verbreitet.

Im Bereich der Sicherheit hat sich außerdem Security Information and Event Management etabliert. So wurde schon vor 20 Jahren angedeutet, dass eine wesentliche Komponente des Sicherheitsmanagements das automatische Sammeln und Auswerten von Protokolldaten sein wird. Ja, technologisch hat es einige Fortschritte gegeben. Jedoch sind neue Verfahren (leider) noch nicht überall vollumfänglich im Einsatz. Dies liegt nicht unbedingt an der Technologie, sondern vielmehr an der Komplexität des Betriebs einer solchen Lösung.

## Fazit

Viele der Annahmen von vor 20 Jahren haben sich erfüllt, jedoch nicht in dem Umfang, den man sich nach 20 Jahren vielleicht wünschen würde. Dabei mangelt es nicht unbedingt an der entsprechenden Technologie – die war schon vor 20 Jahren abzusehen. Bei der Komplexität der heutigen IT-Umgebungen stellt der sichere und robuste Betrieb eines Netzwerkmanagements und der zugehörigen Sicherheitskomponenten die größte Herausforderung dar.

Zum Geleit

# Neue Trends im Netzwerk- und System-Management

**In den letzten Monaten hat sich die Welt des Netzwerk- und System-Managements wieder einmal deutlich verändert. Zum einen sind Verschiebungen innerhalb der Funktions-Schwerpunkte zu beobachten, zum anderen gewinnen neue Themen immer mehr an Bedeutung.**

Dabei sind alle Entwicklungen miteinander verzahnt, so dass Reduzierungen auf einzelne Änderungen häufig keinen Sinn machen. Im Endeffekt ist ein Redesign der vorhandenen Lösungen gefragt, das auch gleichzeitig zur Bereinigung der in den letzten Jahren angefallenen Administrations-Leichen dient.

Nachfolgend soll ohne Anspruch auf Vollständigkeit auf wichtige Entwicklungen eingegangen werden:

**Schwerpunkt Netzwerk-Management**

Netzwerke unterliegen weiter einem starken Wandel. Das aktuelle Schlagwort heißt Netzwerk-Konvergenz und beinhaltet die Integration neuer Anwendungsbereiche in Netzwerke, die bisher in eigenen, separaten Strukturen kommuniziert haben.

Mit dieser Konvergenz entstehen weiter gehende Anforderungen an eine geeignete Management-Lösung. Parallel verschiebt sich die Bedeutung von Netzwerk-Management. Netzwerk-Management ist auf dem besten Wege seine alte Bedeutung als zentrale und wichtigste Management-Technologie zurück zu erobern, allerdings unter völlig veränderten Rahmenbedingungen.

Zwei wichtige Themenbereiche der Konvergenz verdeutlichen als Beispiel sehr gut den Charakter der ablaufenden Änderungen im Netzwerk-Bereich.

**Dies sind:**
- die Integration von IP-Telefonie und
- die Eingliederung des Feldbus-Bereichs in der Fertigung.

Verallgemeinert kann festgestellt werden, dass sich mit Konvergenz nun Technologie-Bereiche im Netzwerk treffen, die völlig verschiedene Anforderungen an Netzwerke stellen.

Damit entsteht sofort der Bedarf nach einem Applikations- und Technologie-orientierten Netzwerk-Management, das den Bedarf einer Applikation gezielt abbildet.

Parallel erhöht sich innerhalb der nächsten 5 Jahre die Teilnehmerzahl in den Netzwerken durch diesen Trend massiv.

ComConsult Research prognostiziert eine Erhöhung, die im Einzelfall den Faktor 10 erreichen kann. Auch daraus entstehen weitergehende Anforderungen an das Client-Management. So wird die Trennung von Benutzern und Clients im Netzwerk und ggf. die Bildung von eigenen Überwachungsbereichen nur funktionieren, wenn die Clients identifiziert und zugeordnet werden können.

In den im Netzwerk laufenden Datenströmen wird dies häufig durch die Protokollzuordnung möglich sein, im Bereich der Zugangskontrolle wird aber eine Einzel-Identifikation unvermeidbar sein.

Die ablaufenden Veränderungen im Sinne der Zunahme der Teilnehmerzahlen generieren kein Lastproblem solange kabel-gebundene Netzwerke im Einsatz sind.

Hier steht der Wechsel auf 10 Gigabit im Rechenzentrum und im Backbone bevor. Speziell im Rechenzentrum wird er für zentrale Hochleistungskomponenten auch völlig unspektakulär erfolgen. Interpoliert man den Preisverfall und die Produktankündigungen der letzten Monate (speziell Cisco und Extreme), dann wird 10 Gigabit innerhalb von 3 Jahren Normalität werden.

Im Bereich der Funktionale nach IEEE 802.11 wird ein eigenes Management mit Technologie-spezifischen Überwachungs- und Alarmfunktionen entstehen müssen (Erkennung unzulässiger Access Points, Ausfall und Umschaltung von Access Points, Quality of Service-Management). Hierzu werden die Hersteller sicher in Kürze geeignete Module anbieten, die in die vorhandenen Management-Lösungen integriert werden können. Ggf. macht es auch Sinn, über eine messtechnische Lösung wie die von AirMagnet nachzudenken, die unabhängig von den Herstellern der eingesetzten WLAN-Komponenten eine Reihe der notwendigen Funktionen abdeckt.

Im Vordergrund aller notwendigen Veränderungen im Netzwerk stehen auf jeden Fall Strukturfragen. Im Mittelpunkt steht die Frage: ist unser bisheriges Netzwerk-Design tragfähig für die Integration völlig verschiedener Anwendungsbereiche mit einer starken Erhöhung der Teilnehmerzahlen oder bedarf es einzelner Änderungen.

Hier bleibt festzustellen, dass viele erfahrene Netzwerke diese Frage unterschätzen und mehr abwartend auf ihre starken Layer-3-Backbone-Netzwerke verweisen. Drei Beispiele sollen verdeutlichen, dass es damit nicht getan ist:

**Beispiel 1**

Mit der Integration von Feldbusbereichen auf der Basis von Ethernet müssen große Layer-2-Bereiche integriert werden. Die hier eingesetzten Geräte und Anwendungen sind häufig nicht Layer-3-tauglich. Gleichzeitig würden zum Teil aber so große Layer-2-Bereiche entstehen, dass dies das Risiko von Instabilitäten in sich birgt.

**Beispiel 2**

Das Thema Benutzertrennung im Netzwerk auch unter Berücksichtigung von mobilen Benutzern gewinnt stark an Bedeutung. Auf der Basis einer Einwahlprozedur sollen Endteilnehmern Rechte zugewiesen werden, von denen die Behandlung im Netzwerk abhängt. IEEE 802.1x kommt hier eine große Bedeutung zu. Ein gutes Beispiel für die Umsetzung derartiger Lösungen liefert Enterasys mit seinem UPN. Beachten Sie auch unser neues Seminar zu diesem Thema!

**Sollten Sie Interesse an dem vollständigen Artikel haben, schreiben Sie uns: insider@comconsult.com**

# IT-Lizenzmanagement in der Praxis

## Transparente, revisionssichere und effiziente Lizenzverwaltung im Unternehmen

## 01.07.-02.07.24 online

Tauchen Sie ein in die Welt des IT-Lizenzmanagements mit unserem umfassenden Praxisseminar. Von der Konsolidierung der Rohdaten über die Dokumentation von Nutzungsrechten bis hin zur Erstellung und Fortführung einer Lizenzbilanz wird alles verständlich erläutert. Erfahren Sie, wie Sie mit Excel und anhand von Fallbeispielen Ihr Wissen praxisnah umsetzen können. Innerhalb des Seminars werden die Grundlagen von License Compliance, die juristischen Aspekte und Fallstricke bei der Beschaffung von Lizenzen sowie Best Practices im Software Asset Management (SAM) besprochen und vertieft. Das Seminar macht Sie fit für eine transparente, revisionssichere und effiziente Lizenzverwaltung in Ihrem Unternehmen.

**Warum Sie diese Schulung besuchen sollten:**

Dieses Seminar bietet Ihnen die Möglichkeit, tief in das Lizenzmanagement einzutauchen und sowohl strategische als auch praktische Fähigkeiten zu entwickeln, um Ihr Unternehmen vor rechtlichen Risiken zu schützen und gleichzeitig Effizienz und Compliance zu maximieren.

**Sie lernen in diesem Seminar:**

- Lizenz-Compliance zu verstehen und Risiken zu minimieren,
- effektive Lizenznachweisführung und Umgang mit Lizenzaudits zu verstehen,
- Best Practices im Software Asset Management kennen und
- revisionssichere Dokumentation und Lizenzbilanz zu erstellen.

**Folgende Vorträge erwarten Sie:**

- Lizenz-Compliance: Risiken und Chancen
- SAM-Prozesse und Best Practices
- Revisionssichere Dokumentation und Lizenzbilanzerstellung
- Ermittlung der Lizenzbedarfe (Software Inventarisierung)
- Dokumentation der Nutzungsrechte, Erstellung von Lizenzbilanzen

Das Seminar richtet sich an Administratoren, Projektleiter, Einkäufer, Entscheider und Führungskräfte, die für Software, Software-Lizenzen und IT-Compliance-Themen verantwortlich sind und ihr Wissen im Bereich IT-Lizenzmanagement erweitern und vertiefen möchten.

**Ihr Referent**

Kristian Borkert ist IT-Jurist und Gründer der JURIBO Anwaltskanzlei. Als Rechtsanwalt und zertifizierter Datenschutzbeauftragter gehören die Vertragsgestaltung und -verhandlung sowie die Implementierung und Gestaltung von Geschäfts- und Compliance-Prozessen zu seinen Tätigkeitsschwerpunkten. Darüber hinaus verfügt Kristian Borkert über eine Qualifikation als Scrum Master und war als Legal Interim Manager tätig.

# Sicherheitsmanagement in kritischen Infrastrukturen

von Thomas Steil in Zusammenarbeit mit Drees & Sommer (Heinrich Schmidt, Mathias Franke, Silvio Buchholz, Thomas Luthardt)

„*Wir müssen größere, stärkere Risiken, mit den größten und stärksten Vorsichtsmaßnahmen, auf uns nehmen.*“ Dieses Zitat, welches Rudyard Kipling zugeschrieben wird, hat für die Absicherung von Werten, Gebäuden und Infrastruktur nicht an Bedeutung verloren. Ressourcen sind begrenzt. Zudem stellen Sicherungsmaßnahmen oft eine Einschränkung für betriebliche Abläufe dar. Daher wird es nicht gelingen, in allen Bereichen den maximalen Schutz umzusetzen. Es sollte jedoch im Gegenzug auch keine Aversion gegen Risikobehandlung eintreten oder unspezifische und scheinwirksame Sicherungsmaßnahmen ohne fallbezogene Betrachtung der spezifischen Situation und Anforderungen umgesetzt werden. Stattdessen sollte man sich darauf konzentrieren zu identifizieren, was für den konkreten Anwendungsfall wichtig oder kritisch ist und wie man Assets bestmöglich gegen die erkannten Risiken absichert.

Genau diesen Grundsatz verfolgt auch der Gesetzgeber in seinem Entwurf des Gesetzes zur Stärkung der Resilienz kritischer Anlagen. „*Betreiber kritischer Anlagen sind verpflichtet, **geeignete** und **verhältnismäßige** technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen.*“ (*Entwurf KRITIS-DachG, 2023*) Um individuell festzulegen, was geeignet und verhältnismäßig ist, werden im Entwurf des KRITIS-DachG Risikoanalysen und Risikobewertungen vorgeschrieben. Dies stellt auch das übliche Vorgehen dar, was seit jeher und vor Erarbeitung des Gesetzentwurfes Grundlage anderer Regularien war oder in der täglichen Praxis des Risikomanagements in verschiedenen Branchen und Geschäftsfeldern als selbstverständlich gilt. Für die Baubranche sind aus einer Risikoanalyse abgeleitete Sicherungsanforderungen in der Vergangenheit nur bei sehr spezifischen Assets, beispielsweise im Bereich von Rechenzentren, Banken, Versicherungen oder Verteidigung, Grundlage der Projektierung und Planung gewesen. Das durch die globalwirtschaftliche und globalpolitische Lage befeuerte steigende Sicherheitsbedürfnis und nicht zuletzt auch die immer weiter voranschreitende Abhängigkeit moderner Wirtschaftsunternehmen von der Informationstechnologie sorgt dafür, dass sich nunmehr alle Branchen und Geschäftsbereiche an den bisherigen Vorbildern orientieren. Die vorgenannte spezifische Gesetzgebung zu diesem Thema zeigt, dass sich diesbezüglich eine ausreichende Brisanz entwickelt hat. Im Folgenden soll ein grober Überblick über das übliche Vorgehen der Sicherheitsberatung im Kontext moderner Gebäude und Infrastrukturen gegeben werden. Dabei wird insbesondere auf die Risikoanalyse als Grundlage eingegangen, und es werden ausgewählte spezifische Themen, die nach Erfahrung der Verfasser dieses Artikels regelmäßig unterschätzt oder falsch bewertet werden, beschrieben.

Zur Methodik einer Risikoanalyse verweisen Richtlinien, Branchenstandards und spezifische Normen wie z. B. die DIN EN 50600 regelmäßig auf die DIN EN ISO 31000 und 31010, welche den internationalen De-facto-Standard zum Risikomanagement darstellen. Die DIN EN ISO 31000 definiert einen klaren Prozess zum Risikomanagement, wobei die generische Darstellung und Beschreibung in der internationalen Normierung direkt für alle Anwender greifbar ist.

Auch die aus dem Verband der deutschen Sachversicherer hervorgegangene VdS Schadenverhütung GmbH bezieht sich in ihren Standards, Leitlinien und Empfehlungen auf die vorgenannten

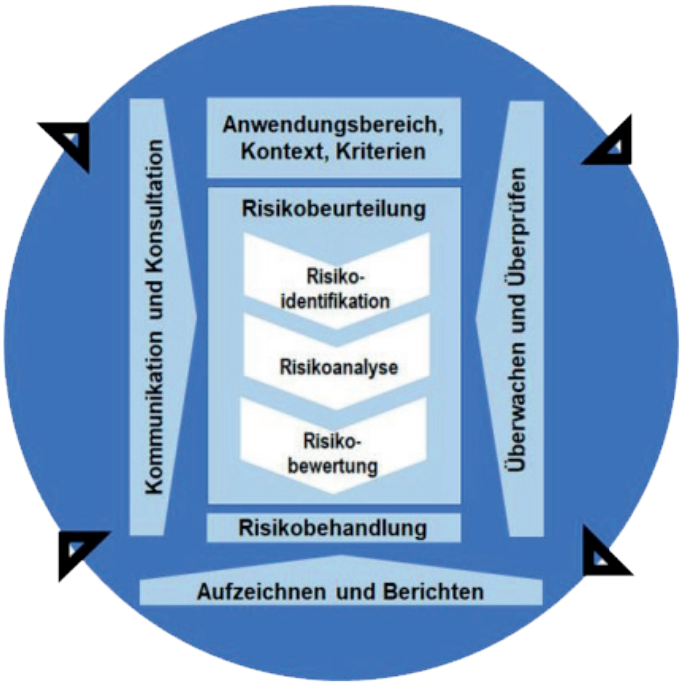



Abbildung 1: Der Risikomanagementprozess (Quelle: DIN-VERLAG)

internationalen Normen. Aus diesen ergeben sich von der Gefahrenanalyse bis zur Definition der Sicherungsmaßnahmen fünf Schritte, aus denen sich das Vorgehen greifbarer ableiten lässt (VdS 3143: 2012-09).

Um die möglichen Risiken zu eruieren, wird zunächst eine Gefahrenanalyse vorgenommen. Dazu werden alle abstrakten Bedrohungen ermittelt. Hier kommt es vor allem darauf an, ergebnisoffen und unvoreingenommen vorzugehen. Sicherlich hat jeder Ersteller einer Gefahrenanalyse den einen oder anderen Ansatz im Kopf, wie den Diebstahl von Rechnern oder das Hacken von Daten. Um keine potenzielle Gefahr unberücksichtigt zu lassen, sollte ein möglichst neutraler und umfänglicher Katalog erstellt werden. Idealerweise wird die Gefahrenanalyse daher nicht von einer einzelnen Person, sondern von mehreren Personen mit unterschiedlichen fachlichen Ausrichtungen erstellt. Das BSI unterstützt hier mit einer Auflistung von 47 elementaren Gefährdungen (BSI, 2022).

Der zweite Schritt befasst sich mit den potenziellen Tätern oder Akteuren, welche hinter den ermittelten Bedrohungen stehen könnten. Der VdS nimmt in dem Sicherungsleitfaden Perimeter die in Tabelle 1 dargestellte Klassifizierung vor.

Bei der Täterprofilanalyse sollte zum einen das Umfeld in Betracht gezogen werden. Ein Objekt im Zentrum einer Großstadt muss regelmäßig mit anderen Tätergruppen rechnen als Einrichtungen im ländlichen Raum. Zum anderen haben interne Gege-

| | | |
|---|---|---|
| Anzahl der Täter | Einzeltäter | Tätergruppen |
| Ortskenntnisse | Fremdtäter | Insider* |
| Professionalität | Gelegenheitstäter | Organisierte Kriminalität |
| Kenntnisse und Ausrüstung | Laie | Profi |
| Risikobereitschaft | vorsichtiger Täter | risikobereiter Täter |

*Aktuelle und ehemalige Mitarbeiter, Lieferanten, Handwerker, Kunden

Tabelle 1: Täterprofilanalyse (Quelle: VdS 3143: 2012-09)

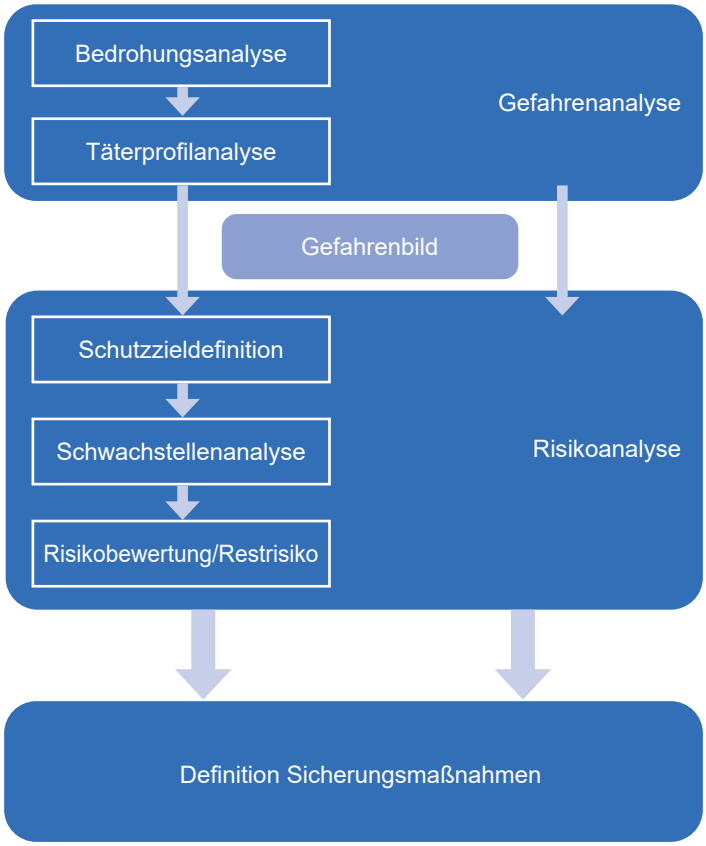



Abbildung 2: Prozessablauf zur Definition von Sicherungsmaßnahmen (Quelle: VdS 3143: 2012-09)

benheiten eine zentrale Bedeutung. Obwohl es in Unternehmen und Organisationen teils ein rotes Tuch ist, das Innentäterrisiko zu eruieren, ist es ein Fakt, dass Zwischenfälle in der Vergangenheit auf Innentäter oder zumindest auf Täter mit Insiderwissen zurückzuführen waren. Die Sabotage der Bahninfrastruktur vom 08.10.2022 war ein medienwirksames Beispiel für Vorfälle, die in dieser Dimension nicht ohne Insiderwissen möglich gewesen wären. Das Bundesamt für Verfassungsschutz hält das Innentäterrisiko für derart relevant, dass hierzu im Dezember 2022 ein eigenes Infoblatt herausgegeben wurde.

Es muss darüber hinaus die Frage gestellt werden, welche Prozesse, Produkte, Anlagen, Daten oder Kenntnisse für Täter wertvoll sein könnten. Gerade bei kritischer Infrastruktur kann hier unter Umständen auch die polizeiliche Kriminalprävention oder der Verfassungsschutz beratend unterstützen. Sicherlich gibt es ebenso Gefährdungen, die keinen Täter bedingen, wie Naturkatastrophen oder Pandemien.

Nachdem die Gefährdungen definiert wurden, schließt die eigentliche Risikoanalyse an. Um abschätzen zu können, welche Relevanz eine Bedrohung hat, sollte man sich im Klaren sein, welche individuellen Schutzziele verfolgt werden sollen. Der Diebstahl eines Rechners oder ein unbefugter Zutritt zum Verwaltungstrakt eines Gebäudes kann zwar unangenehm sein, muss aber nicht zwangsläufig einen großen Schaden verursachen. In diesem Zusammenhang ist es erforderlich zu definieren, welche Prozesse, Produkte, Anlagen, Daten oder Kenntnisse für die Organisation - nicht unbedingt für einen Täter - von wesentlicher Bedeutung sind bzw. ob der Verlust, die Beschädigung oder die Manipulation dieser Assets relevante Auswirkungen für die Organisation hat.

Mit diesen Inhalten können die Schutzziele in erster Instanz, also die Gefährdungen, gegen die Maßnahmen ergriffen werden sollen oder müssen, abgeleitet werden. Im Gegensatz dazu wird es

immer Gefährdungen geben, gegen die man sich nicht oder nicht mit vertretbarem wirtschaftlichem Aufwand schützen kann oder möchte. Klassische Beispiele aus der freien Wirtschaft sind kriegerische Handlungen, Terroranschläge oder extreme zivile Unruhen, wobei es durchaus andere Organisationen gibt, die Maßnahmen gegen diese Gefährdungen berücksichtigen müssen. Zu nennen sind hier Einrichtungen der staatlichen Sicherheit und Verteidigung oder Infrastrukturen mit hohem Schadenspotential wie Atomkraftwerke – selbst wenn diese nicht mehr am Netz sind. Mit dem Gefahrenbild auf der einen und den Schutzzielen auf der anderen Seite muss anschließend untersucht werden, welche Faktoren das Einwirken der Gefahren auf die schützenswerten Werte ermöglichen oder begünstigen – die objekt- bzw. fallspezifischen Schwachstellen. Gerade bei bestehenden Objekten sollte hierfür eine Ortsbegehung vorgenommen werden.

Alle bis hierhin gewonnenen Ergebnisse fließen jetzt in die Risikobewertung ein. Traditionell werden hierbei für die jeweilige Gefährdung die Auswirkungen bewertet, die mit den Schutzzielen korrelieren. Die erkannten Schwachstellen, die die Auswirkungen negativ verstärken können, sind mit zu berücksichtigen. Ein bestehendes Business Continuity Management ist von erheblichem Vorteil, da mit diesem üblicherweise die Auswirkungen von Zwischenfällen auf den Geschäftsprozess – auch in monetärer Hinsicht – bereits bewertet wurden.

Daraufhin wird die Eintrittswahrscheinlichkeit der identifizierten Gefährdungen ermittelt, welche durch die erkannten Schwachstellen ggf. erhöht wird. Hierzu können Statistiken und Erfahrungswerte, doch auch der gesunde Menschenverstand genutzt werden. Wichtig ist, dass die Bewertung möglichst neutral und unvoreingenommen und idealerweise unabhängig durch mehrere Personen erfolgt. Die lokalen Begebenheiten spielen hier ebenfalls eine wesentliche Rolle. Beispielsweise ist die Wahrscheinlichkeit eines Einbruchdiebstahls in näherer Umgebung eines bekannten Kriminalitätsschwerpunkts regelmäßig höher als in Nachbarschaft einer bewachten staatlichen Institution, z. B. einer Botschaft. Andererseits ist bei dieser das Anschlagsrisiko höher und die daraus ggf. folgenden Auswirkungen auf die eigene Liegenschaft sind wahrscheinlicher. Aus den Auswirkungen und der Eintrittswahrscheinlichkeit ergibt sich die Risikokategorie.

Im letzten Schritt werden die Sicherungsmaßnahmen definiert, also die Maßnahmen, die die Eintrittswahrscheinlichkeit und/oder die Auswirkung einer Gefährdung senken und damit die Risikokategorie mindern. In manchen Fällen lässt sich ein Risiko sogar abwenden oder annähernd ausschließen. Beispielweise kann die Pufferung einer elektrischen Versorgung über eine sogenannte unterbrechungsfreie Stromversorgung mit Batterieanlage in Kombination mit einer daran anschließenden Notstromversorgung die Risiken eines Stromausfalls derart minimieren, dass die Auswirkungen weitestgehend beschränkt sind. Dies ist glücklicherweise geübte Praxis in Krankenhäusern, die auf diesem Weg unterbrechungsfreie Operationen und Patientenversorgung ermöglichen. Wie eingangs erwähnt und so auch vom Gesetzgeber für das KRITIS-DachG vorgesehen, sollten die baulichen, technischen, und sicherheitsbezogenen und organisatorischen Maßnahmen stets geeignet und verhältnismäßig sein.

Was dabei geeignet und verhältnismäßig ist, kann nur der jeweilige Asset-Verantwortliche in Abstimmung mit seiner Geschäftsführung und einem ggf. vorhandenen Business Continuity Management bewerten. Dieser Personenkreis ist ebenso in der Lage zu bewerten, ob die geminderten und verbleibenden Restrisiken akzeptabel sind. Oftmals ist eine Versicherung der Restrisiken ebenfalls möglich. Diesbezüglich sei erwähnt, dass ein aktives Risikomanagement und die daraus resultierende Minderung von Risiken durch Sicherungsmaßnahmen auch positive Auswirkungen auf etwaige Versicherungsprämien haben und daher die Wirtschaftlichkeit der Sicherungsmaßnahmen vor diesem Hintergrund bewertet werden sollte.

Nach der theoretischen Herleitung zur Identifikation und Behandlung von Risiken, die dem einen oder anderen Leser bereits geläufig sein dürften, stellt sich nun die Frage, was dies genau für die tägliche Praxis bedeutet. Dieser Artikel soll keine weitere generische Aufzählung von Risikobehandlungsmaßnahmen sein, die jeder Anwender im Kontext der Informationstechnik an irgendeiner Stelle schon einmal gelesen hat. Vielmehr soll der Fokus auf Risiken und deren Behandlung liegen, die zunächst artfremd zur Informationstechnik erscheinen, aber mit dieser in direktem oder indirektem Zusammenhang stehen und die Vertraulichkeit, Integrität und Verfügbarkeit als Grundsätze der Informationssicherheit wesentlich beeinflussen können. Nachfolgend sind vier ausgewählte Teilaspekte aus der täglichen Praxis der Verfasser dieses Artikels beschrieben, die häufig unterrepräsentiert sind oder sogar gänzlich außen vor gelassen werden.

| | | | | |
|---|---|---|---|---|
| **Existenzgefährdend**<br>Weiterexistenz ist in Gefahr | mittel | hoch | sehr hoch | sehr hoch |
| **Sehr kritisch**<br>Sehr hohe Schaden,<br>Ausfall wichtiger Funktionen für längeren Zeitraum | mittel | mittel | hoch | sehr hoch |
| **mittel / begrenzt**<br>keine hohen Schäden | gering | gering | mittel | hoch |
| **niedrig / tolerabel**<br>Geringe Sachschaden<br>Keine Funktionsbeeinträchtigungen | gering | gering | gering | gering |
| ***Auswirkung*** / ***Gefährdung*** | Sehr unwahrscheinlich / selten | möglich / unwahrscheinlich | häufig / wahrscheinlich | sehr häufig / wahrscheinlich |

Tabelle 2: Exemplarische Risikomatrix

## Perimeterschutz – die erste Verteidigungslinie

In einer Welt, die von ständigem technologischem Fortschritt und sozialen Veränderungen geprägt ist, steht die Sicherheit von physischen Objekten und Anlagen immer mehr im Mittelpunkt der Diskussionen. Perimeterschutz und physische Objektsicherheit sind zu entscheidenden Faktoren geworden, um die Sicherheit von Menschen, Eigentum und kritischer Infrastruktur zu gewährleisten.

Der Begriff Perimeter im Sinne einer Sicherheitskonzeption bezeichnet die äußerste Grenze der zu betrachtenden Schutzobjekte sowie einzelne Schwerpunkte innerhalb des Umfeldes. Der Perimeter beschreibt dabei ebenfalls vertikale und horizontale Grenzen oberhalb eines Objektes, die beispielsweise durch Flugkörper überschritten werden können. Eingehende Beispiele für den Perimeter sind Einfriedungen z. B. durch Zäune, doch auch die Gebäudeaußenhülle selbst, wenn keine Einfriedung existiert. Sind bestimmte Räume innerhalb eines Gebäudes, z. B. Serverräume, das zu schützende Asset, kann der Perimeter ebenso durch die Wände, Böden und Decken des Raumes gebildet werden.

Es steht außer Frage, dass ein Alarmsystem nur dann einwandfrei arbeitet, wenn es möglichst früh ungewünschte Ereignisse detektiert. In einem System ohne Freigeländesicherung kommt das Alarmsignal allerdings erst, wenn der Eindringling bereits versucht in das Gebäude einzudringen. Bezogen auf das Beispiel im Gebäudeinneren wird ein Eindringen in einen Raum erst bemerkt, wenn der Täter sich bereits in diesem befindet, sofern keine Detektion an einem früheren Punkt, beispielsweise an der Gebäudeaußenhülle, erfolgt. Der Schutz eines Assets ist also nicht nur auf die Grenzen des zu schützenden Objektes, also ein Gebäude, Raum oder Rack zu beziehen, sondern über dessen Grenzen hinaus zu betrachten.

Bleiben wir beim Beispiel der Einfriedung. Ein Zaun selbst stellt im Regelfall keine wirksame Barriere dar, zumindest dann nicht, wenn er aufgrund baurechtlicher oder anderer Vorgaben in seiner Höhe begrenzt ist. Selbst ein als sicher zu betrachtender Zaun mit einer Höhe von 2,5 m und aufgesetztem Stacheldraht kann mit entsprechenden Hilfsmitteln und ausreichender Intention vergleichsweise schnell überwunden werden. Was also bringt ein noch so stabiler und hoher Zaun? Die Antwort ist Zeit. Ein vorgelagerter Perimeter stellt die erste Schutzbarriere im Sicherheitssystem dar und hat vor allem die Verlängerung der Interventionszeit zum Ziel. Nebenbei hält er Gelegenheitstäter ab und erhöht den nötigen Aufwand eines Einbruchversuches. Das primäre Ziel ist jedoch die Kennzeichnung einer Grenze nach außen hin und die Schaffung eines Bereiches, in dem man entsprechende Überwachungsmaßnahmen umsetzen kann. Die Überwachungsmaßnahmen können dabei über eine passende Sensorik am Zaun oder intelligente Videoüberwachungssysteme umgesetzt werden.

Ein gut geplanter und implementierter Perimeterschutz schafft eine Barriere, die unbefugten Zugang verhindert und potenzielle Eindringlinge abschreckt. Dies kann physische Hindernisse wie Zäune, Mauern und Tore sowie elektronische Sicherheitssysteme wie Überwachungskameras und Bewegungssensoren umfassen.

Moderne Perimeterschutzsysteme sind nicht mehr auf statische Barrieren beschränkt. Sie integrieren fortschrittliche Technologien wie Videoüberwachungssysteme und Bewegungssensorik, um verdächtiges Verhalten zu erkennen und Alarme auszulösen. Dies ermöglicht eine effiziente Reaktion auf potenzielle Bedrohungen und minimiert Falschalarme. Die enge Verbindung zur IT-Sicherheit besteht darin, dass diese Systeme heute oft Teil eines umfassenden Netzwerks sind, denn auch im Netzwerk gibt es einen Perimeterbereich, der die Netzwerke abgrenzt.

Intelligente Perimeterschutzsysteme verwenden fortschrittliche Technologien, um nicht nur Eindringlinge, sondern auch digitale Bedrohungen zu erkennen. Die Integration von Firewalls, Intrusion-Detection-Systemen und Netzwerk-Monitoring in physische Si-

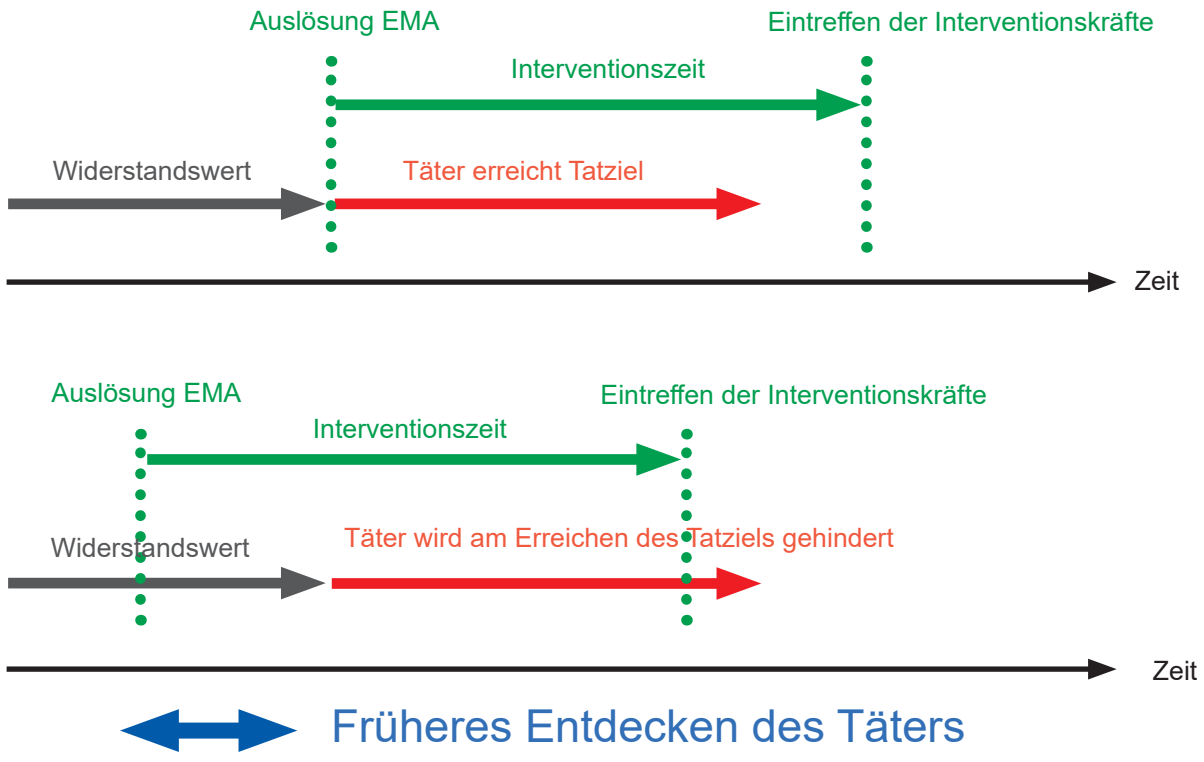



Abbildung 3: Beispiel für Perimeterschutz

cherheitssysteme ermöglicht eine umfassende Überwachung und Reaktion auf Cyberangriffe.

Der Perimeterschutz und die physische Objektsicherheit sind somit unerlässliche Elemente in der heutigen Welt, in der die Sicherheit von Menschen und Vermögenswerten immer mehr an Priorität gewinnt.

Durch die Integration von moderner Technologie und Sicherheitsexpertise können Unternehmen und Organisationen eine effektive Verteidigung gegen Bedrohungen jeder Art aufbauen.

Die Sicherheit von physischen Objekten und Daten sind in der heutigen digitalen Welt, in der Daten oft wertvoller sind als physische Vermögenswerte, untrennbar miteinander verbunden. Der Schutz digitaler Ressourcen rückt auch bei der physischen Objektsicherheit immer weiter in den Vordergrund.

Eine erfolgreiche Sicherheitsstrategie erfordert das Zusammenspiel von Perimeterschutz, physischer Objektsicherheit und IT-Sicherheit. Nur durch die enge Zusammenarbeit und Integration dieser Disziplinen können Unternehmen und Organisationen eine umfassende Verteidigung gegen Bedrohungen jeder Art aufbauen und die Sicherheit von Menschen, Vermögenswerten und Daten gewährleisten.

Dies zeigt sich bereits in dem Zusammenspiel von Zugangskontrollen, Einbruchmeldesystemen und der Videodetektion mit der IT und insbesondere IT-Sicherheit und damit verbundenen Verschlüsselungen und Datensicherungsmaßnahmen.

Einbruch in physische Räumlichkeiten kann digitale Informationen gefährden, und umgekehrt können erfolgreiche Cyberangriffe physische Schäden verursachen. Die Integration von IT-Sicherheitsprotokollen in physische Sicherheitssysteme ist daher von entscheidender Bedeutung.

Heute sind moderne Sicherheitssysteme in der Lage, physische und digitale Daten zu integrieren und zu analysieren. Dies ermöglicht eine noch schnellere und deutlich präzisere Reaktion auf Sicherheitsvorfälle.

Die Sicherheit von physischen Objekten und Daten ist in der heutigen digitalen Welt untrennbar verbunden. Eine erfolgreiche Sicherheitsstrategie erfordert das Zusammenspiel von Perimeterschutz, physischer Objektsicherheit und IT-Sicherheit. Nur durch die enge Zusammenarbeit und Integration dieser Disziplinen können Unternehmen und Organisationen eine umfassende Verteidigung gegen Bedrohungen jeder Art aufbauen und die Sicherheit von Menschen, Vermögenswerten und Daten gewährleisten. Dabei rücken die Netze der Gebäudetechnik immer mehr in den Fokus. Einerseits ist die Gebäudetechnik essenziell zur Sicherung der physischen Infrastruktur, andererseits findet man gerade hier alte Systeme, für die IT-Sicherheit bei der Errichtung noch nicht im Fokus stand. Diese Bestandssysteme bieten daher oftmals ein Einfallstor für Hackerangriffe. Eine Vielzahl der Bestandskomponenten war nie darauf ausgelegt, Teil eines komplexen Netzwerks zu sein, und bietet weder sichere Schnittstellen noch die Möglichkeit, diese nachträglich zu implementieren. Langsam dringen die ersten Controller in die Gebäudetechnik ein, die Zertifikate und Verschlüsselung unterstützen. Beispielsweise unterstützt BACnet/SC nun endlich TCP/IP und TLS. Auch können die Betreiber nun eigene digitale Zertifikate für die Gebäudetechnik verwenden und somit einen großen Schritt in Richtung sichereres Netzwerk gehen. Damit schließt die Gebäudetechnik nun endlich zur IT auf und wird mittelfristig ein Teil der IT-Landschaft werden.

Allerdings haben wir noch immer die Herausforderung, gewachsene Bestandsnetze abzusichern und zu integrieren. Die oftmals schlechte oder nicht vorhandene Dokumentation erschwert diese Aufgabe ungemein. Einen guten Einstieg in den Aufbau und Absicherung von Netzen der Gebäudetechnik bieten hier die BSI-Grundschutz-Bausteine INF.13 Technisches Gebäudemanagement und INF.14 Gebäudeautomation, die zusammen mit den entsprechenden Umsetzungshinweisen seit 2022 Teil des BSI-IT-Grundschutz-Kompendiums sind (s. Netzwerk Insider 02/2022).

Denn die Übergänge zwischen IT und Gebäudetechnik werden immer fließender. Wenn man heute einen Meetingraum in einem modernen Gebäude nutzt, detektiert der Raum die Anwesenheit, passt die Lüftung an den CO2-Gehalt der Raumluft an, regelt die Temperatur, stellt eine Videokonferenz zur Verfügung und verdunkelt auf Wunsch die Fenster und passt die Beleuchtung an. Dafür müssen aber IT, Gebäudetechnik und Medientechnik ineinandergreifen. Die letzten Inseln wie der Brandschutz werden ebenfalls immer IT-lastiger, und mit IP500 sind auch schon Funkprotokolle für solche Systeme am Markt verfügbar, die neben einer neuen Übertragungstechnik die Integration in die IT-Landschaft ebenso erleichtern sollen.

Denn Brände sind eine der ältesten und damit greifbarsten Gefahren, denen sich der Mensch seit seinem Bestehen ausgesetzt sieht. Selbst in unserer hochmodernen, durchorganisierten und kontrollierten Welt werden Brände trotzdem immer wieder auf erschreckende Weise real und existenzbedrohend.

Dabei ist es unerheblich, ob wir hier von der digitalen oder der analogen Welt sprechen. Denn ohne Hardware kann keine Software existieren. Und diese „Hardware“ besteht nicht nur aus Platinen und Leitungen, sondern benötigt geschützte Plätze, eine gesicherte Energieversorgung und gesunde und fähige Menschen, die das alles bauen, verwalten und warten. Und um das zu tun, werden wiederrum Betriebsmittel, Transport- und Unterbringungsmöglichkeiten für Mensch und Maschinen benötigt, wodurch sich dieser Kreislauf immer weiter aufspannt.

Dabei ist Brand nicht nur Feuer. So wird neben der zerstörerischen Macht der freigesetzten Wärmeenergie die zwangsläufige Begleiterscheinung „Rauch“ oftmals unterschätzt. Denn dieser kann weit schwerwiegendere Folgen haben, weil sich Rauch schneller verbreitet und eine nicht erkennbare Zusammensetzung besitzt.

Zerstört Hitze Menschen und Gegenstände ganz direkt, bringen Rauchgase giftige, korrodierende und krebserregende Stoffe in Mensch, Tier und (sensible) Gegenstände und verbleiben als Ruß auf jeder Oberfläche.

Um sich davor zu schützen, entsinnt der Mensch seit jeher Methoden und Systeme, um Bränden vorzubeugen und sie im Fall der Fälle wirksam bekämpfen und eindämmen zu können.

Und um hier allgemeine Standards zu setzen, werden im Bau- und Arbeitsschutzrecht Schutzziele definiert und konkrete Maßnahmen zu deren Erreichung gefordert.

Diese umfassen bauliche Maßnahmen wie Brandwände zur Unterteilung von Gebäuden und zum Schutz von Nachbarnutzun-

gen, Rettungswege für eine gesicherte Möglichkeit der Entfluchtung und Rettung durch die Feuerwehr. Zusätzlich beinhalten sie Anlagentechnik wie Brandfrüherkennungs-, Alarmierungs- und Löschsysteme sowie organisatorische Maßnahmen in Form von Mitarbeiterschulungen, Räumungsübungen und die dafür erforderlichen Konzepte und Dokumente.

Der Schutz von Menschenleben, Tieren, Gebäuden und Sachgütern ist nur ein Aspekt. Brandschutz dient ebenso dem Erhalt von Produktionskapazitäten, Arbeitsplätzen, Marktanteilen und dem Unternehmensimage. Zudem ist Brandschutz realer Umweltschutz. Nicht nur, dass der Ausstoß enormer Treibhausgasmengen verhindert wird, sondern es werden auch Werte erhalten, die somit nicht mit viel Energie erzeugt und ersetzt werden müssen. Daher stellt Brandschutz Nachhaltigkeit im ureigensten Sinne dar, der dem Erhalt einer lebenswerten und gleichzeitig sicheren Welt dient.

Dabei sind gesetzliche Brandschutzvorgaben nicht starr, sondern ermöglichen es, über Abweichungen, Erleichterungen oder Ingenieurmethoden die vorgegebenen Schutzziele nutzungs- und objektspezifisch zu erreichen. Und bei frühzeitiger Einbindung in die Planung können sowohl Kosten als auch Aufwand auf ein überschaubares Maß beschränkt werden, sowie erforderliche Maßnahmen ein weites Feld von Synergien bieten.

Nur wer Sicherheit ganzheitlich denkt, erreicht ganzheitlich Sicherheit.

Es ist die Aufgabe der Planung, aus den Zielvorgaben verschiedene Designvarianten zu entwickeln. Im Anschluss daran ist es natürlich wichtig herauszufiltern, welche dieser Varianten aus wirtschaftlicher und technischer Sicht zu empfehlen sind und dabei die Zielvorgaben am besten erfüllt.

Dazu gibt es eine neue Methode „Resilienz-KPIs“, welche in der ISO 22237-31 beschrieben wird. Diese Methode bietet uns die Möglichkeit, die Resilienz kritischer Infrastrukturen zu analysieren und zu bewerten und somit die verschiedenen Designvarianten miteinander zu vergleichen.

Mittels der KPIs können die Verlässlichkeit, die Zuverlässigkeit sowie die Verfügbarkeit des ganzen Systems bewertet werden. Dabei lassen sich Single- und Double-Points of Failure definieren, welchen Aufschluss über mögliche Schwachstellen im jeweiligen Design geben. Durch die frühzeitige Aufdeckung solcher Mängel kann sichergestellt werden, dass fehlerbehaftete Designs nicht umgesetzt werden, bevor die betreffenden Punkte erneut überarbeitet wurden und letztlich die Zielvorgaben erreichen.

Für die Anwendung der KPI-Methode wird das Infrastruktur-Modell in ein Resilience Block Diagram übertragen. Zu jeder einzelnen Komponente werden entsprechende Auswahl-Sicherheitsdaten hinterlegt. Auf dieser Basis wird dann das Gesamtsystem berechnet. Aufgrund der Ergebnisse dieser Berechnung lassen sich die Varianten dann sehr einfach miteinander vergleichen, um letztlich die Variante herauszufiltern, welche die Anforderungen bestmöglich erfüllt.

NW
NETZWERK

ComConsult GmbH
Beratung + Planung + Schulung

# DAS NETZWERK IM BAUPROJEKT

## DIE PLANUNG DER AKTIVEN NETZWERKKOMPONENTEN ALS HÄUFIG ÜBERSEHENES DETAIL

NETZWERKPLANUNG | NEUBAU | MODERNE GEBÄUDE-INFRASTRUKTUR | LAN | WLAN

NW

Kaum ein Bauprojekt kommt heutzutage ohne eine entsprechende IT-Infrastruktur aus. In vielen Fällen wird die IT-Infrastruktur erst spät in den Bauprozess integriert, was potenzielle Risiken birgt. Um diese Risiken zu minimieren, empfiehlt es sich eine IT-Planung begleitend zum Bauprojekt, zum Beispiel analog zu den HOAI-Phasen (Honorarordnung für Architekten und Ingenieure), zu durchlaufen. Neben der Verkabelung sollte ein besonderes Augenmerk auf den aktiven Komponenten, der Netzwerkarchitektur und der WLAN-Planung liegen. Mit unserer Erfahrung unterstützen wir Sie gerne bei der reibungslosen Integration Ihrer IT-Infrastruktur.

# Neue Seminare im Juli/August

EMV und Potentialausgleich im Umfeld von IT- und RZ-Versorgungsnetzen
01.-02.07.2024 online

IT-Lizenzmanagement in der Praxis
01.-02.07.2024 online

Windows-Server 2022 – Einstieg und Administration – Praxis-Workshop
01.-03.07.2024 online

Sensoren – eine Einführung in die Grundlagen und die neuesten Entwicklungen
08.07.2024 online

Exchange Server Troubleshooting
10.-11.07.2024 online

IT-Projektvertragsmanagement für Nichtjuristen
16.-17.07.2024 Bonn

GENERATION X, Y und Z
25.07.2024 online

Professionelles Change Management – Veränderungen erfolgreich umsetzen
21.08.2024 online

IT-Projektmanagement im Kontext der VUCA-Welt und Agilität
21.-22.08.2024 online

Microsoft 365 Copilot Masterclass: Maximieren Sie Ihre Produktivität!
26.-27.08.2024 online

Digitalisierung im IT-Einkauf
28.08.2024 online

# IT-Projektvertragsmanagement für Nichtjuristen

## Verhandlung, Gestaltung und Durchführung von IT-Projektverträgen

## 16.07.-17.07.2024 Bonn

## Neues Seminar

IT-Projektverträge zu verhandeln und durchzuführen stellt hohe Anforderungen an alle Beteiligten. Der Vertrag ist sehr rechtslastig: Gewährleistungsregelungen und Haftungsfolgen müssen von Beginn an bedacht, die Leistungen daran ausgerichtet und dementsprechend beschrieben werden. Fehler bei der Auswahl des Vertragspartners sowie bei der Vertragsgestaltung können sich kostenintensiv auswirken und hohe Folgekosten produzieren.

Der Referent stellt im Seminar zunächst die wichtigsten Aspekte für die Auswahl des richtigen IT-Dienstleisters für ein Projekt dar und gibt wertvolle Anregungen zu Vertragsverhandlungen. Sodann werden die Essentials für die Vertragsgestaltung behandelt und anhand von Beispielfällen dargestellt. Bei der Vertragsgestaltung für das Projekt gilt es dann, die wichtigsten Risiken im Vertrag umsichtig abzusichern. Dies kann längere Verhandlungen erfordern, da beide Vertragspartner im Ausgangspunkt unterschiedliche Interessen haben. Der Referent zeigt dabei auf, welche Regelungen für den Projektvertrag in welcher Art und Weise gestaltet werden können, um das gemeinsame Interesse der Vertragspartner, die erfolgreiche Projektdurchführung, bedachtsam und angemessen im Projektvertrag zu regeln.

Weiterhin behandelt der Referent bestimmte wiederkehrende Probleme bei der Vertragsdurchführung und erläutert mögliche Maßnahmen dagegen. Schließlich bewerten die Teilnehmer anhand eines bereitgestellten IT-Projektvertragsmusters Änderungswünsche eines potenziellen Kunden zum Vertragsentwurf, es werden gemeinsam Lösungsmöglichkeiten erarbeitet und im Vertragsentwurf als dessen Fortschreibung formuliert.

**In diesem Seminar lernen Sie:**

- Vertragsvorbereitung: Ziele bei der Vertragsgestaltung
- Professionelle Formulierungen für Verträge
- Do's and Don'ts bei Vertragsverhandlungen
- Verhandlungstechniken bei Abschluss von Verträgen
- Vertragsauslegung: Was gibt der Vertrag her?
- Welcher Vertragstyp am besten geeignet ist
- Besonderheiten für internationale Verträge
- Vertragsgestaltung: Die wichtigsten Regelungen für den Projektvertrag
- Vertragsdurchführung: Typische Probleme und Maßnahmen dagegen
- Vertragsverhandlungen: Umgang mit Forderungen nach Änderungen im Vertragstext

**Ihr Referent**

Dr. Meinhard Erben ist Rechtsanwalt und Managing Partner von KANZLEI DR. ERBEN ATTORNEYS. Die Kanzlei berät seit 25 Jahren beide Marktseiten sowie die öffentliche Hand im Zusammenhang mit dem Abschluss, der Gestaltung und der Durchführung von IT-Verträgen. Dr. Erben ist Autor verschiedener Fachbücher im IT-Recht und wird seit vielen Jahren als Wirtschaftsanwalt für Unternehmen speziell im Bereich IT-Vertragsrecht sowie IT/IP-Recht empfohlen. Dr. Erben ist nebenberuflich als Referent tätig, sowie als Dozent an der Dualen Hochschule Mannheim (Graduiertenkolleg) im Studiengang IT-Management.

# Konzeptionierung und Ausschreibung einer Videoüberwachungsanlage

Mit Marcus Steinhorn sprach Christiane Zweipfennig

Videoüberwachung ist für den physischen Schutz insbesondere kritischer Infrastrukturen ein unverzichtbares Element eines Sicherheitskonzeptes. Wie bei jeder anderen Planung von Sicherheitssystemen geht auch der Planung von Videoüberwachungsanlagen eine umfassende Anforderungs- und Bedarfsanalyse voraus.

Marcus Steinhorn ist seit 12 Jahren Berater bei ComConsult. Während er anfangs im Bereich Unified Communications tätig war, wechselte er nach zwei Jahren in das Competence Center IT-Infrastrukturen. Dort beschäftigte er sich hauptsächlich mit der Neu- und Erweiterungsplanung von passiven IT-Infrastrukturen, Stromversorgung wie Netzersatz- und USV-Anlagen sowie mit Infrastruktur-Audits zur baulichen und technischen Bewertung der Sicherheit von Rechenzentren und IT-Räumen. In den vergangenen Jahren widmet er sich zunehmend der Konzeption von Videoüberwachungsanlagen sowie von Zutritts- und Zeiterfassungssystemen. Von einem solchen Projekt berichtet er in diesem Interview.

## ComConsult wurde von einem weltweit führenden Technologieunternehmen der optischen Industrie mit der Konzeptionierung und Ausschreibung der auf dem Gelände eingesetzten Videoüberwachungsanlage beauftragt. Was war für den Kunden der Anlass zu dieser Maßnahme?

Auf dem Campus des Kunden gab es kaum Videoüberwachung.

Im Zuge einer KRITIS-Überprüfung stellte sich heraus, dass der Standort des Kunden als schützenswert und daher seine Bereiche als kritische Infrastruktur einzustufen waren, weshalb die Videoüberwachungsanlage erneuert werden sollte.

### Videoüberwachung zur Erhöhung der Sicherheit kritischer Infrastrukturen

## Was ergab die Bestandsaufnahme der vorhandenen Infrastruktur?

Ein marktführender Hersteller hatte für etwa ein Drittel des Perimeters – also der Zaunanlage beziehungsweise des Übergangs vom öffentlichen in den geschützten privaten Bereich – die Videoüberwachungsanlage bereits geplant. Diesen unvollständigen Testaufbau haben wir als Bestandsanlage vorgefunden.

### Lückenhafter Testaufbau als Bestandsanlage

## Worin bestand zusammengefasst eure Aufgabe?

### Zielsetzung: flächendeckende Videodetektion

Unsere Aufgabe war es, eine lückenlose ganzheitliche Videoüberwachung auf dem Gesamtperimeter zu planen. Wir sollten die vorgefundenen Lücken in dem schon gebauten Bereich schließen und die Überwachung auf die gesamte Zaunanlage erweitern. Ziel war eine flächendeckende Detektion, um zuverlässig mit Kameras zu erfassen, ob zum Beispiel eine Person einen bestimmten Bereich betritt oder versucht, den Zaun zu übersteigen.

## Welche Kameras sollten installiert werden?

### Wärmebildkameras zur Hauptüberwachung, PTZ-Kameras zum Erfassen von Details

Es war eine Auflage des Betriebsrates, dass im normalen Regelbetrieb keine Personen auf den Videoaufzeichnungen erkennbar sein durften. Deshalb sollte die Hauptüberwachung über knapp 60 Wärmebildkameras erfolgen, bei denen man auf den Aufnahmen nur eine Wärmebildsignatur erkennt und nicht die Personen selber oder Details wie Gesichter. Die Wärmebildkameras sollten über die gesamte Länge des Zauns und stellenweise Gebäudewände oder Fensterfronten so aufgebaut werden, dass sie sich gegenseitig sehen konnten, damit wirklich jede Fläche überwacht war. Diese Kameras erkennen, wenn eine Person in einen gewissen Bereich hereingeht und in welche Richtung sie sich bewegt. Hat die Wärmebildkamera einen Alarmfall detektiert, wird eine optische Kamera auf den Bereich aufgeschaltet. Diese sogenannten Pan-Tilt-Zoom-Kameras – kurz PTZ-Kameras – sind schwenkbar und haben eine ferngesteuerte Richtungs- und Zoomsteuerung. Die PTZ-Kameras, von denen rund ein Dutzend angebracht werden sollten, liefern dann Detailbilder an die Leitstelle. Weiterhin war geplant, an Zugängen wie Drehkreuzen und Schrankenanlagen Bullet-Kameras anzubringen, um die Personen zu erfassen, die dort passieren. Im Bedarfsfall kann dann in Abstimmung mit dem Betriebsrat auf diese verschlüsselten Videodaten zugegriffen werden, um sie weiter zu analysieren.

## Welche Anforderungen bestanden an die Kameras?

Es gilt, bei der Planung eine Vielzahl von Parametern entsprechend der Gegebenheiten vor Ort zu berücksichtigen. Ein Eckpfeiler ist der sogenannte DORI-Standard. DORI steht für Detection, Observation, Recognition, Identification. Dabei handelt es sich um Vorgaben aus der IEC EN62676-4, die festlegen, welche spezifischen Anforderungen in einer Szene für die vordefinierte Anwendung gelten müssen. In diesem Standard ist geregelt, wie viel Pixel pro Meter man in einem Bildausschnitt haben muss, um ein gewisses Merkmal der Überwachung zu erzielen. Wenn zum Beispiel eine Person identifiziert oder zugeordnet werden soll, muss die Auflösung natürlich viel höher sein, als wenn man nur die Szenerie einer großen Fläche überwachen möchte. Für die PTZ-Kameras, die beim Kunden eingesetzt werden sollten, gab es eine Vorgabe von 250 Pixeln pro Meter, die laut DORI-Standard als Mindestmaß für das Identifizieren von Personen gilt. Eine weitere Anforderung an die Kameras war, dass das Gehäuse eine bestimmte Schutzklasse aufzuweisen hatte. Zum Schutz vor Sabotage und Vandalismus gab es ebenso Vorgaben, in welcher Höhe die Kameras anzubringen waren. In diesem Zusammenhang wurde auch festgelegt, dass der Bereich unterhalb einer Kamera von einer anderen erfasst werden musste, damit letztere einen eventuellen Fremdzugriff aufzeichnen konnte. Zudem war es wichtig, dass die Bilddaten der Kameras – zusätzlich zur Speicherung an zentraler Stelle – auch auf der Kamera zwischengespeichert werden konnten, um die Videodaten bei Netzwerkausfall oder Systemneustart nicht zu verlieren.

### 250 Pixel pro Meter als Richtwert, um Personen und Details zu erkennen.

## Welche Anforderungen bestanden an das Netzwerk?

### Wegeredundanz durch drei redundante LWL-Ringe

Analoge Kameras mit Übertragung über Koaxialkabel sterben immer mehr aus. Heute kommen bei der Videoüberwachung fast nur noch IP-Kameras zum Einsatz, die digitale Signale bereitstellen, die von einem Netzwerk per Internet-Protokoll weiterverarbeitet werden. Die Planung des IP-Netzwerkes stellte in dem Projekt eine Herausforderung dar, denn es galt, in diesem Perimeter große Strecken zu überbrücken. Da bei Kupferkabeln die Übertragungsfähigkeit bei hundert Metern erschöpft ist und Redundanz geschafft werden sollte, wurde für das Übertragungsnetz eine Ringstruktur aus LWL-Kabeln gewählt. Es wurden an einzelnen Masten Kästen mit Industrieswitches angebracht und im Rahmen der Reichweite eines Kupferkabels die Kameras aus den umliegenden Masten an diese Verteiler angebunden. Das Firmengelände des Kunden war in drei Perimeter unterteilt: das Hauptwerksgelände, ein Außengebäude und ein Außenlager. Deshalb wurden drei redundante LWL-Ringe geplant, denn durch den Ringschluss war eine Wegeredundanz gegeben: Falls ein Kabel irgendwo ausfällt, gibt es immer noch die Anbindung über eine andere Strecke. Bei der Planung der Verkabelung mussten verschiedene Anforderungen beachtet werden. Die Kabel sollten nicht frei zugänglich, sondern im geschützten Bereich im Inneren des Geländes liegen und wir mussten darauf achten, dass die Verteiler am Mast immer mindestens drei bis vier Meter Abstand zum Boden hatten.

## Was gab es hinsichtlich der Starkstromanlage und dem Blitz- und Überspannungsschutz zu beachten?

**Blitzeinschlag hat durch LWL-Ringe geringe Auswirkungen.**

Wenn man Komponenten aus einem IP-Netzwerk im Außengelände montiert, muss immer das Thema Blitz- und Überspannungsschutz berücksichtigt werden. Sollte ein Blitz in einen Mast einschlagen, kann dieser über das Kupferkabel möglicherweise in das Gebäude gelangen und dort die Infrastruktur im Verteilerraum zerstören. Wir umgingen das Problem damit, dass wir LWL-Ringe einsetzten und die IT-Infrastruktur jenseits des betroffenen Mastes nicht berührt wurde. Natürlich musste dennoch im Ernstfall die Stromversorgung sichergestellt werden. Hier war für die entsprechenden Maßnahmen ein Fachplaner aus einem anderen Gewerk zuständig.

## Für die Videoüberwachung wurde ein neues, vollständig auf IP-Technik basiertes Videokontrollsystem geplant. Dabei sollte die Zentraltechnik in zwei redundanten Rechenzentren angesiedelt werden. Welche Anforderungen gab es bei der Planung zu berücksichtigen?

**Zentraltechnik in zwei georedundanten Rechenzentren**

Die Zentraltechnik sollte aus Redundanzgründen in zwei Rechenzentren, die sich in verschiedenen Brandabschnitten befanden, untergebracht werden. Im hier beschriebenen Projekt gab es bereits zwei georedundante Rechenzentren, die in verschiedenen Werken untergebracht waren. Die Technik für die Videoüberwachung sollte in die vorhandene redundante Rechenzentrumsinfrastruktur des Kunden integriert werden. In dem videoüberwachten Rechenzentrum im Werk konnte der eine Teil der Zentraltechnik untergebracht werden, während eine zweite Ausführung der Zentraltechnik in einem Rechenzentrum an einem anderen Standort in der Nähe aufgebaut wurde. Wir haben die gesamte Technik redundant geplant: von der Stromversorgung über die Ringeinspeisung und die Netzersatzanlage bis hin zur Klimaanlage.

## Für das Video-Management-System sollten verschiedene Bedienplätze eingerichtet werden. Welche waren das?

Es sollten drei Arbeitsplätze mit je drei Monitoren in der Alarmempfangsstelle, kurz AES, eingerichtet werden. Es ist Standard, dass in der AES zwei Personen die Videoaufzeichnungen auf den Monitoren überwachen. Der dritte Bedienplatz wird aus Redundanzgründen eingerichtet. Zusätzlich sollten einfache Bedienplätze mit einem Monitor an den Pforten entstehen. Diese Plätze haben nicht den Funktionsumfang wie die Arbeitsplätze in der AES und die Pförtner sehen nur die Live-Bilder aus ihrem unmittelbaren Bereich.

**Zwei Bedienplätze in der Alarmempfangsstelle sind der Standard.**

## Warum war die Beschaffenheit des Geländes eine besondere Herausforderung?

**Einsatz von Wärmebildkameras wegen Nebelfelder**

Der Industriecampus mit rund zehn Industriehallen und Bürogebäuden liegt in einem Tal. Die Planung war durch die geographischen Gegebenheiten schwieriger, als es auf den Lageplänen zunächst den Anschein hatte. Wir mussten die Höhenunterschiede, die sich an vielen Stellen durch die Hanglange ergaben, mitberücksichtigen. Es gab am Perimeter viel Grünbewuchs, der teilweise im öffentlichen Bereich und nicht auf dem Areal des Kunden stand. Ein Problem waren auch Nebelfelder, die je nach Jahreszeit am Standort immer wieder auftreten. Die Nebelfelder waren mit ein Grund, warum sich der Kunde für eine Lösung mit Wärmebildkameras entschieden hat.

## Nach einem groben Konzept habt ihr die Ergebnisse in ein Feinkonzept überführt und am Ende eine funktionale Leistungsbeschreibung erstellt.

**Funktionale Leistungsbeschreibung benennt Qualitätsanforderungen an das neue System.**

Ja, genau. Im ersten Schritt haben wir in Absprache mit dem Kunden eine Anforderungsanalyse erstellt, der sich nach einer Begehung vor Ort und in Abstimmung mit dem Betriebsrat und dem Kunden die Entwicklung eines Grobkonzepts anschloss, das später in eine Feinkonzeption überführt wurde. Während das Grobkonzept die Vorhaben allgemein beschreibt, ist das Feinkonzept wesentlich präziser und detaillierter. Dort nennen wir zum Beispiel konkret Systeme und Hersteller, wobei in diesem Projekt der Hersteller für die Kameras schon vom Kunden vorgegeben war. Auf ein Leistungsverzeichnis, in dem detailliert beschrieben wird, wie viele Kameras mit welchen Spezifikationen und welche Kabel in welcher Menge benötigt werden, hat der Kunde verzichtet. Wir haben

eine funktionale Leistungsbeschreibung erstellt, in der wir in Form eines Katalogs Funktion und Zweck des neuen Systems nach unterschiedlichen Gewichtungen beschrieben haben – so z. B. die genaue Positionierung der PTZ-Kameras. ComConsult begleitet dann im Anschluss häufig die folgende Ausschreibung und unterstützt den Kunden in der Bauphase. In diesem Projekt war unsere Aufgabe mit der Abgabe der funktionalen Leistungsbeschreibung beendet.

## Fazit

Für die Sicherung kritischer Infrastrukturen ist eine lückenlose und effiziente Überwachung essenziell. Eine detaillierte Anforderungsanalyse, ergänzt durch präzise technische und geographische Anpassungen, ist von großer Bedeutung. Der Einsatz von Wärmebildkameras und PTZ-Kameras zeigt eine innovative Herangehensweise, die sowohl Datenschutzanforderungen als auch Sicherheitsbedürfnisse erfüllt. Durch die funktionale Leistungsbeschreibung wurde eine klare und umsetzbare Grundlage geschaffen, die den hohen Ansprüchen des Kunden gerecht wird und eine zuverlässige Überwachung ermöglicht.

# IT-Projektmanagement im Kontext der VUCA-Welt und Agilität

## Tipps für erfolgreiche Projekte im unberechenbaren, dynamischen Umfeld

## 21.08.-22.08.2024 online

## Neues Seminar

VUCA steht für Volatility (Volatilität), Uncertainty (Unsicherheit), Complexity (Komplexität) und Ambiguity (Mehrdeutigkeit). Das Seminar richtet sich an alle Projektleitenden, die in der dynamischen Welt, die durch permanente Änderungen gekennzeichnet ist, ein Projekt zum Erfolg führen wollen.

Jede Methode ist so gut wie derjenige, der sie anwendet. Um Experte für erfolgreiche Projekte in der VUCA-Welt zu werden, ist dieses Seminar der Schlüssel.

Wir besprechen die wesentlichen Einflüsse der VUCA-Welt auf ein Projekt und vergleichen die unterschiedlichen Projektmanagementmethoden hinsichtlich ihrer Resilienz bzgl. plötzlicher Veränderungen.

Dabei stellen wir das Beste aus allen Projektmanagementwelten zusammen und transformieren dies auf Ihre persönlichen Rahmenbedingungen, sodass Sie mit einem pragmatischen und sofort umsetzbaren Projektmanagementvorgehen für Ihre Projekte gewappnet sind.

Diese Inhalte helfen, den Teilnehmenden ein umfassendes Verständnis für das Thema zu geben, frühzeitig umsetzbare Maßnahmen zu ergreifen und sie bei der Anwendung agiler Methoden in einer volatilen, unsicheren, komplexen und mehrdeutigen Umgebung erfolgreich zu unterstützen.

**Sie lernen in diesem Seminar:**

- die VUCA-Welt und ihre Auswirkungen auf IT-Projekte kennen,
- die Unterschiede zwischen traditionellen und agilen Methoden zu verstehen,
- mit dem „Besten aus allen Projektmanagement-Welten“ maximale Resilienz für Ihre Projekte zu gewährleisten,
- exemplarische Beispiele aus der Praxis anzuwenden und
- die zukünftigen Entwicklungen im IT-Projektmanagement einzuordnen.

**Ihr Referent**

Ole Banthien begleitet seit 2012 verschiedene Kunden als Trainer, Coach, Berater und Projektleiter sowohl im agilen als auch im klassischen Umfeld. Er ist qualifiziert und zertifiziert in ITIL®, (Expert Qualifikation), PRINCE2®, MSP® (Managing Successful Programmes), COBIT®5, SDI™ (Service Desk Analyst und Accredited Trainer für Service Desk), PRINCE®2agile, ITIL® Practitioner, Professional Scrum Master und FitSM. Alle Trainings absolviert er in Deutsch oder in Englisch.

# Funk oder Kabel?

von Dr. Joachim Wetzlar

Die Frage, ob man in Büro oder Produktion besser auf Kabel oder stattdessen auf WLAN oder andere Funktechniken zurückgreift, haben wir an dieser Stelle schon verschiedentlich diskutiert. Doch wie sieht es beim weltumspannenden Internet aus? Läuft das nicht inzwischen alles über Satelliten?

Es wird Ihnen bekannt sein, und in den Nachrichten hört man zuweilen davon, wenn eines zerstört wurde: Das Internet basiert heute auf Seekabeln. Inzwischen liegen weit mehr als 1 Mio. Kilometer Glasfaserkabel im Meer. Alleine in den Jahren 2023 bis 2025 wird man ca. 300.000 Kilometer Kabel auf 78 Strecken neu verlegt haben. Die Investitionen dafür belaufen sich auf mehr als 10 Mrd. Dollar [1].

Das ist ein gewaltiger Aufwand. Er erinnert an die großen Schwierigkeiten, in der Mitte des 19. Jahrhunderts das erste transatlantische Telegraphenkabel von Irland nach Neufundland zu verlegen. Mit dem damals größten verfügbaren Schiff „Great Eastern“ waren zahlreiche Anläufe nötig, bis die erste Verbindung zustande kam. Nur wenige Tage später war das Kabel bereits defekt.

Viel einfacher war dagegen die Funktelegraphie, die Anfang des 20. Jahrhunderts erstmals den Atlantik überspannte. Man brauchte lediglich Sender und Empfänger. Die Infrastruktur dazwischen stand zum Nulltarif zur Verfügung, wenn auch nicht immer verlässlich. Die Gründe dafür waren damals noch unbekannt.

Letztlich revolutionierten die geostationären Satelliten der 70er Jahre die weltumspannende Kommunikation. Ich erinnere mich an ein Telefonat, das ich mit Kanada führen durfte. Mein Gesprächspartner war deutlich zu verstehen. Nur die lange Signallaufzeit erforderte eine gewisse Gesprächsdisziplin.

Warum nutzen wir also heute wieder das gute alte Kabel? Zum einen weil geostationäre Satelliten mit viel Latenz verbunden sind. Zum anderen skalieren Glasfaserkabel besser als Satelliten. Die Gesamtkapazität aller Seekabel beträgt derzeit knapp 4 Pbit/s; das entspricht 40.000 Satelliten mit einer angenommenen Kapazität von je 100 Gbit/s.

Die Probleme des Seekabels sind jedoch immer noch dieselben wie am Anfang. Die Bedingungen auf dem Meeresboden sind alles andere als günstig. Erdbeben, Erdrutsche, die Fischerei und auch Sabotage lassen Seekabel immer wieder brechen. Dass Haie Kabel anfressen, scheint dagegen eher eine Mär zu sein. In früheren Zeiten, als die Isolation von Seekabeln noch aus Jute bestand, gab es allerdings zerstörerischen Befall von Bohrwürmern.

Etwa 200 Kabelbrüche zählt man pro Jahr. Zuletzt wurden im Roten Meer gleich mehrere Kabel beschädigt, wahrscheinlich vom Anker eines Frachters, der zuvor mit Raketen angegriffen worden war. Der Aufwand zur Erhaltung des Internets ist also nicht unerheblich und bleibt doch den meisten von uns verborgen. Einen spannenden Artikel zu diesem Thema las ich kürzlich in [2]. Ich erzähle Ihnen ein wenig davon:

- Zunächst einmal muss man die defekte Stelle möglichst genau lokalisieren. Dafür eignet sich das altbekannte Verfahren der optischen Reflektometrie. Mit einem OTDR (Optical Time Domain Reflectometer) leuchtet man von Land in die Kabelenden hinein. Aus der Laufzeit der reflektierten Impulse lassen sich Orte von Störstellen bis auf wenige Meter genau bestimmen.

- Nun benötigt man ein Schiff, das mit Seilwinden und passenden Werkzeugen ausgestattet ist. In der Nähe der vermuteten Störstelle zieht es spezielle Haken über den Meeresgrund und versucht damit das Kabel zu erwischen und an die Oberfläche zu ziehen. So machte man es bereits vor 150 Jahren, nur hat man die Werkzeuge inzwischen optimiert. Möglicher-

weise muss man das Kabel zunächst durchschneiden, um es nach oben ziehen zu können. Dafür gibt es ebenfalls entsprechendes Werkzeug. In flacherem Wasser, d.h. bis zu 2000 Meter Tiefe, setzt man inzwischen auch Tauchroboter (Remotely-operated Vehicles, ROVs) ein.

- Hat man das erste Kabelende auf diese Weise gefunden, wird es mit einer Boje markiert und das gegenüberliegende Ende auf dieselbe Weise gesucht. Das zieht man an Bord des Schiffes und spleißt ein neues Stück Glasfaserkabel an. Die Spleiße werden wie auch an Land üblich in Spleißkassetten zusammengefasst. Umhüllt wird alles mit einer wasserdichten Muffe.

- Zuletzt fährt das Schiff zurück zur Boje, während es Muffe und entsprechende Länge neuen Kabels achteraus ins Meer zurückgleiten lässt. Dort angekommen wird das zweite Kabelende mit dem neuen Kabel verbunden und schließlich alles im Meer versenkt. Die durch das neue Kabel entstandene Überlänge wird nach Möglichkeit in einer Schleife abgelegt.

Von weltweit insgesamt ca. 80 Kabellegern sind nur gut 20 Schiffe dafür ausgerüstet, defekte Seekabel reparieren zu können. Viele dieser Schiffe haben inzwischen ein Alter erreicht, in dem man Tanker und Massengutfrachter meist schon abgewrackt hätte. Entsprechend alt ist auch das mit Spezialwissen ausgestattete Personal auf diesen Schiffen.

Es fehlt an Nachwuchs. Einerseits fokussiert sich die Internet-Industrie eher auf das Verlegen neuer Kabel als auf die Wartung der vorhandenen. Andererseits ist die Seefahrt nicht jedermanns Sache. Können Sie sich vorstellen, regelmäßig wochenlang von zu Hause fort zu sein und auf einem Schiff zu leben, das vielleicht nicht allen Komfort eines Kreuzfahrtschiffes bietet? Darüber hinaus könnte es Sie frustrieren, dass Sie superschnelles Internet am Laufen halten, während Sie selbst gerade einmal E-Mails oder Chat-Nachrichten verschicken können, weil das Internet an Bord für mehr nicht ausreicht (ja, ich kann ein Lied davon singen).

Allen Widrigkeiten zum Trotz scheint es, als sei beim weltumspannenden Internet der Wettbewerb zugunsten des Kabels ausgegangen. Wirklich? Verschiedentlich war zu lesen, man habe niedrig fliegende Satelliten (Low Earth Orbiters, LEOs) als Internet-Zugangstechnik nicht zuletzt zu dem Zweck erfunden, weite Strecken schneller überbrücken zu können als mit dem Kabel. Kürzere Signallaufzeit ergäbe insbesondere geldwerte Vorteile beim sogenannten Hochfrequenzhandel.

In der Tat, die Satellitenverbindung ist schneller, rechnen Sie es nach (vergessen Sie dabei nicht, dass sich Licht im Glas nur etwa mit zwei Dritteln der Geschwindigkeit fortbewegt wie im Vakuum)! Alles nur eine Verschwörungstheorie? Wer weiß, womöglich schwingt auch beim Internet das Pendel irgendwann zurück in Richtung des Funks. Vielleicht in einer Variante mit Laser-Licht?

## Verweise


[1] https://submarine-cable-map-2024.telegeography.com/
[2] https://www.theverge.com/c/24070570/internet-cables-undersea-deep-repair-ships


**ComConsult GmbH** - Pascalstraße 27 - 52076 Aachen - Germany
Tel: +49 2408 951-0 - info@comconsult.com - www.comconsult.com

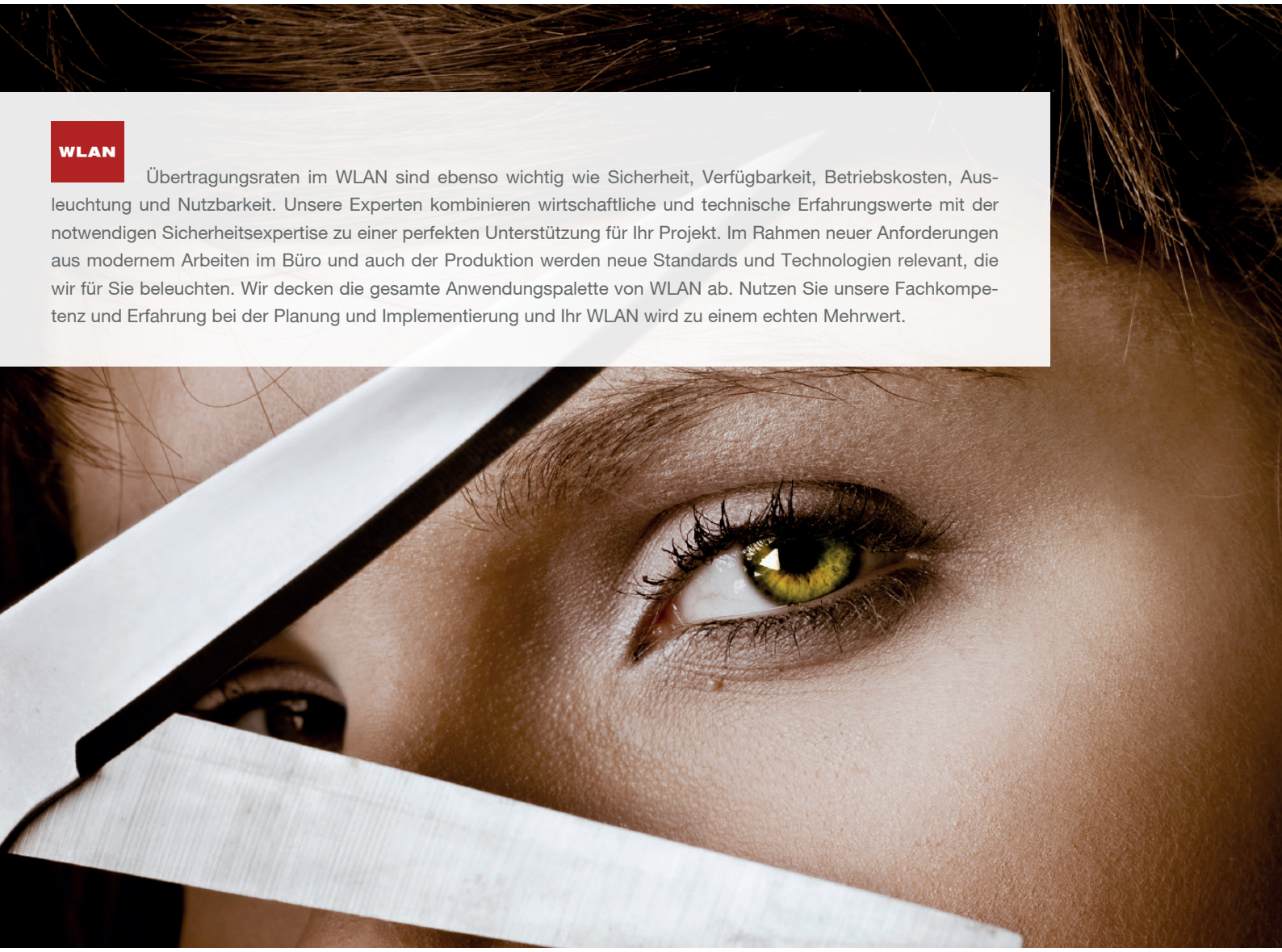
**WLAN**
WIRELESS LOCAL AREA NETWORK

**ComConsult GmbH**
Beratung + Planung + Schulung

# KABEL AB!

## EIN WLAN FÜR ALLE ANWENDUNGSBEREICHE.

INDUSTRIAL WLAN | FMC | ZELLPLANUNG | CONTROLLER DESIGN | SICHERHEIT | MANAGEMENT | STÖRUNGSBEHANDLUNG



**WLAN**

Übertragungsraten im WLAN sind ebenso wichtig wie Sicherheit, Verfügbarkeit, Betriebskosten, Ausleuchtung und Nutzbarkeit. Unsere Experten kombinieren wirtschaftliche und technische Erfahrungswerte mit der notwendigen Sicherheitsexpertise zu einer perfekten Unterstützung für Ihr Projekt. Im Rahmen neuer Anforderungen aus modernem Arbeiten im Büro und auch der Produktion werden neue Standards und Technologien relevant, die wir für Sie beleuchten. Wir decken die gesamte Anwendungspalette von WLAN ab. Nutzen Sie unsere Fachkompetenz und Erfahrung bei der Planung und Implementierung und Ihr WLAN wird zu einem echten Mehrwert.

# Kostenlose Webinare der Woche

**Alle unsere Webinare finden Sie unter: https://www.comconsult.com/webinare/**

## Lizenz-Chaos entwirren: Audit, OSS und EU-Regeln meistern. Neue Trends entdecken
06.06.24 10:45-11:45 Uhr

In einer Welt, in der Software das Rückgrat des Unternehmenserfolgs bildet, ist ein proaktives Lizenzmanagement entscheidend. Dieses Webinar stellt drei zentrale und aktuelle Themen in den Mittelpunkt, die für jedes moderne Unternehmen von Bedeutung sind und rüstet Sie mit dem notwendigen Wissen aus, um Ihr Lizenzportfolio effizient zu managen, Risiken zu minimieren und Compliance sicherzustellen.

**Zusammenfassung der Inhalte des Webinars:**
- Audit-Vorbereitung und Lizenz-Compliance
- Integration von Open-Source-Software und Update zum EU Cyber Resilience Act
- Blick in die Zukunft: Trends und Modelle im Lizenzmanagement

Dieses kostenlose Webinar bietet Ihnen die Gelegenheit, über den neuesten Stand der Entwicklungen im IT-Lizenzmanagement informiert zu bleiben. Machen Sie sich bereit, Ihre Lizenzstrategien zu überdenken, Risiken zu reduzieren und Compliance in einer sich schnell wandelnden digitalen Welt sicherzustellen.

Dauer: 1 Stunde
Preis: kostenlos
Referent: Kristian Borkert
IT-Jurist und Gründer der JURIBO Anwaltskanzlei

## Sensoren – eine Einführung in die Grundlagen und die neuesten Entwicklungen
06.06.24 15:00-16:00 Uhr

In diesem kostenlosen Webinar vermittelt Ihnen unser Experte die Grundlagen der modernen Sensorik. Als Schnittstellen zwischen der realen und der virtuellen Welt sind Sensoren heute wichtiger denn je: Sie nehmen als „künstliche Sinnesorgane“ physikalische Größen auf und wandeln sie in elektronisch verarbeitbare Signale um. Computer, Fahrzeuge, Roboter, Kameras, Überwachungs- und Regelungssysteme bekämen ohne Sensoren keine Daten zur Verarbeitung.

Das Webinar gibt einen kurzen Überblick über die Vielzahl und die Funktionsprinzipien wichtiger Sensorsysteme.

**Zusammenfassung der Inhalte des Webinars:**
- Was ist ein Sensor?
- Anwendungen und aktuelle Trends in der Sensorik
- Funktionsweise eines Sensors an einem Beispiel: CCD-Bildsensor
- Vom Einzelsensor zum Internet of Things

Dauer: 1 Stunde
Preis: kostenlos
Referent: Prof. Dr. Rolf Heilmann
Physiker und Dozent an der Hochschule München

# Sonderveranstaltung Technologietage

## Neue und aktuelle Technologien

## 09.09.-10.09.2024 Aachen | online

In der IT gibt es keinen Stillstand, das merken auch wir als Berater nahezu täglich. In dieser Veranstaltung präsentieren wir neue Themen aus dem Projektgeschäft der ComConsult. Dabei orientieren wir uns an den Erfahrungen der Kunden sowie an unseren eigenen.

Denn nicht alles, was neu ist, muss auch relevant sein! Und es gibt Themen, die zwar nicht mehr taufrisch, doch aufgrund von Rahmenbedingungen aktuell von Bedeutung sind.

Die IT ist im ständigen Wandel. Netze verändern sich auf dem Kabel und über Funk, “klassische” Gebäudetechnik wird durch smarte Komponenten ergänzt und künstliche Intelligenz wird immer präsenter. Und die IT-Sicherheit darf auch nicht auf der Strecke bleiben. In dieser Sonderveranstaltung erhalten sie Einblicke in neue Technologien und Entwicklungen.

Zusätzlich bleibt es dank des einzigartigen Veranstaltungsorts nicht nur bei grauer Theorie. Es wird vor Ort eine Führung geben, die den Einsatz neuer Technologien in der realen Welt demonstriert.

**In diesem Seminar lernen Sie:**

Die Liste der vorgesehenen Themen liest sich wie die Vorhabens- und Projektliste der nächsten Jahre für jedes Unternehmen, das die neuesten Technologien für mehr Effizienz und Innovation nutzen möchte:

- Overlay-Netze in diversen Umgebungen (Campus, RZ)
- Smart Technologies – aktuelle Entwicklungen und neue Ansätze
- Künstliche Intelligenz und Large Language Models im Alltag
- Funk-Technologien – WiFi 7 und darüber hinaus
- Neue Entwicklungen im Bereich IT-Security für Clients

**Warum Sie diese Schulung besuchen sollten:**

Die IT ist im ständigen Wandel. Netze verändern sich auf dem Kabel und über Funk, “klassische” Gebäudetechnik wird durch smarte Komponenten ergänzt und künstliche Intelligenz wird immer präsenter. Und die IT-Sicherheit darf auch nicht auf der Strecke bleiben. In dieser Sonderveranstaltung erhalten sie Einblicke in neue Technologien und Entwicklungen.

Zusätzlich bleibt es dank des einzigartigen Veranstaltungsorts nicht nur bei grauer Theorie. Es wird vor Ort eine Führung geben, die den Einsatz neuer Technologien in der realen Welt demonstriert.

**Ihr Moderator**

Dr. Markus Ermes hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau und Nutzung von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage und Cloud-basierten Diensten liegen. Seine Kenntnisse im HPC-Bereich geben zusätzlich Einblicke in modernste Hochleistungstechnologien (CPU, Storage, Netzwerke), die in Zukunft auch im Rechenzentrum Einzug erhalten können.

# Sonderveranstaltung Technologietage

## Programmübersicht

### Montag, 09.09.2024

**9:45 - 10:15 Uhr**
**Keynote**
- SDN und Overlays auf dem Vormarsch
- Entwicklungen im Bereich Smart Building
- KI überall
- Funktechnologien – Neues über den Äther
- Sicherheit am Edge

*Dr. Markus Ermes, ComConsult GmbH*

**10:15 - 11:00 Uhr**
**Overlays und SDN im RZ: Der aktuelle Stand**
- Overlays: Eine kurze Wiederholung
- Die verbreitetsten Technologien im RZ
- Koexistenz von Lösungen
- Betrieb von SDN
- Ein Blick in die Glaskugel

*Dr. Markus Ermes, ComConsult GmbH*

**11:15 - 12:00 Uhr**
**Projekterfahrungen und Einblicke in Campus-Fabric-Netze**
- Überblick über vorhandene Technologien und Ansprüche der Hersteller
- Ansprüche, Anforderungen und die Realität
- Wie stelle ich sicher, dass eine Fabric richtig geplant ist und funktioniert?
- Fallstricke, Hürden und Herausforderungen

*Dr. Johannes Dams, ComConsult GmbH*

**12:00 - 12:45 Uhr**
**Wi-Fi 7**
- Was bringt die neue Evolution im Wireless LAN?
- Wie steht es mit der Praxistauglichkeit im Unternehmensumfeld?
- Welche Planungsparameter gilt es zu beachten?

*Michael Schneiders, Stephan Bien, ComConsult GmbH*

**13:45 - 14:30 Uhr**
**Datensicherung in unsicheren Zeiten**
- Datensicherung als Plan B gegen Ransomware
- Gründe für Tape Revival
- Worauf beim Backup zu achten ist.

*Dr. Behrooz Moayeri, ComConsult GmbH*

**14.30 - 15:15 Uhr**
**Object Storage – eine Einführung**
- Grundlagen von Object Storage
- Unterschiede zum klassischen Storage
- S3 – der wohl bekannteste Object Storage
- Weitere Beispiele

*Dr. Markus Ermes, ComConsult GmbH*

**15:30 - 16:15 Uhr**
**TP-Verkabelung, alles ganz einfach! Oder?**
- Büroverkabelung skalierbar und für alle passend, geht das?
- Gemeinsame Nutzung von IT-Technikräumen durch mehrere Mieter und den Vermieter
- Qualitätsansprüche: höher oder niedriger?
- Besonderheit: IT-Verkabelung in Wohnquartieren
- Probleme gezeigt an Planungsbeispielen

*Hartmut Kell, ComConsult GmbH*

**16:15 - 17:00 Uhr**
**Herausforderungen moderner Campus-Netze**
- In welcher Umgebung müssen zukunftssichere Netzwerke spielen können?
- Welche Herausforderungen ergeben sich bei der Auslegung eines modernen Netzwerks?
- Welche Herausforderungen stellen sich im täglichen Betrieb?
- Worauf gilt es bei der Planung bzw. Umsetzungsvorbereitung zu achten?

*Sven Tekaat, ComConsult GmbH*

### Dienstag, 10.09.2024

**9:00 - 9:45 Uhr**
**Wird Wi-Fi 7 zum 5G-Killer?**
- Zusammenfassung vom Vortag: Die wichtigen Features von Wi-Fi 7
- Was macht 5G so besonders?
- Kapazität versus Echtzeitfähigkeit
- Sinnvolle Einsatzszenarien

*Dr. Joachim Wetzlar, ComConsult GmbH*

**9:45 - 10:30 Uhr**
**5G Messen und Simulieren**
- Welches Messequipment gibt es und wo liegen die Unterschiede?
- Durchführung von Mobilfunkmessungen
- Vergleich von Messung und Simulation
- Live-Demo einer Mobilfunkmessung

*Frederik Stückemann, ComConsult GmbH*

**10:45 - 11:45 Uhr**
**Führung Demofabrik Aachen**
- Aktuelle Entwicklungen der Industrie 4.0

**11:45 - 12:30 Uhr**
**KI und UCC**
- Ansätze und Technologien
- Was es gibt und was bald kommt.
- Formen und Ausprägungen von KI im Unternehmen
- Umsetzung von KI-Projekten

*Nils Wantia, ComConsult GmbH*

**13:30 - 14:15 Uhr**
**IT im Smart Building**
- Grundlegende IT-Anforderungen an Smart Buildings
- Sonderfälle der IT
- Einbindung der IT in Bauvorhaben
- Sicherheitsrichtlinien & Co

*Thomas Steil, ComConsult GmbH*

**14:15 - 15:00 Uhr**
**Smart Home vs. Smart Building**
- Technologien und Gerätelandschaft
- Ansätze für die Umsetzung
- Datenanalyse
- Automatisierung
- Unterschiede zum Enterprise-Segment (Smart Building)

*Nils Wantia, ComConsult GmbH*

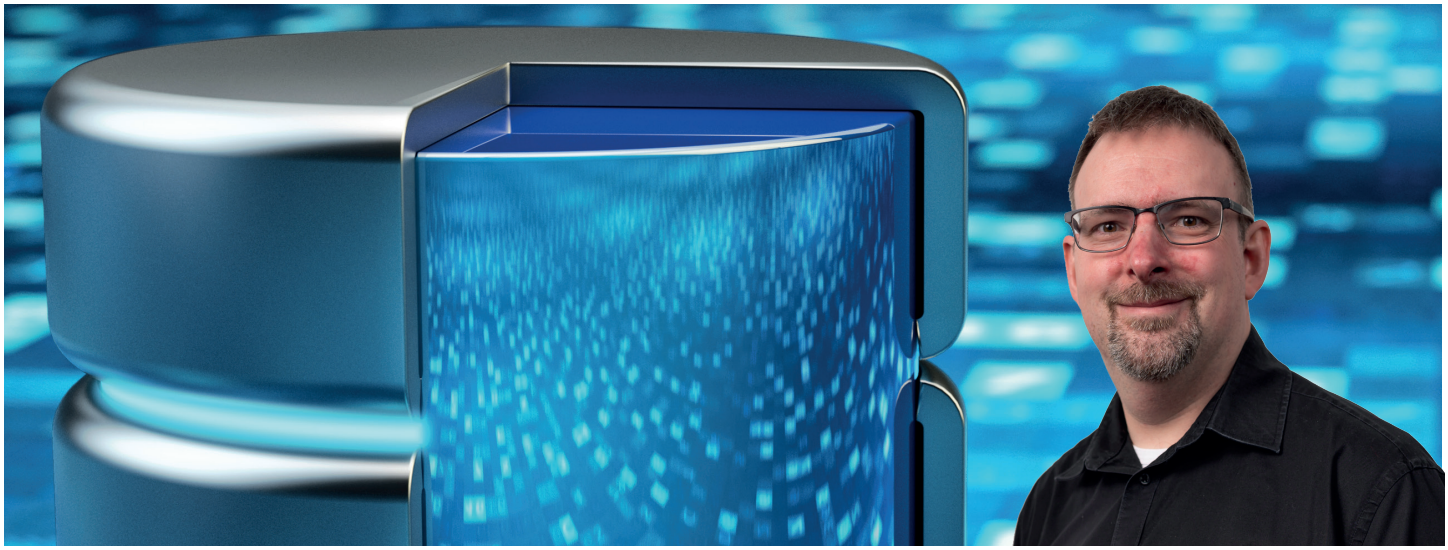
**15:15 - 16:00 Uhr**
**Security Service Edge**
- Überblick der Funktionalitäten von Security Service Edges
- Security Service Edge: Notwendigkeit in heutigen IT-Architekturen
- Techniken zur Kontrolle von Kommunikation mit und in der Cloud

*Simon Oberem, ComConsult GmbH*

**Pausenzeiten**

**Montag**
11:00 - 11:15 Uhr Kaffeepause
12:45 - 13:45 Uhr Mittagspause
15:15 - 15:30 Uhr Kaffeepause

**Dienstag**
10:30 - 10:45 Uhr Kaffeepause
12:30 - 13:30 Uhr Mittagspause
16:00 Uhr Ende der Veranstaltung



# Object Storage – Grundlagen und Use Cases

von Dr. Markus Ermes

Das Thema Object Storage begegnet mir im Projektgeschäft aktuell immer häufiger. Neu ist die Technologie dabei nicht. Besonders bekannt ist diese Art von Storage vor allem aus der Cloud, mit AWS S3 als vielleicht prominentester, aber auch sehr komplexer Object Storage.

Warum also erst jetzt ein Artikel? Object Storage kommt mittlerweile immer häufiger auch on Premises zum Einsatz, mit sehr unterschiedlichen Use Cases. Daher soll in diesem Artikel ein grundlegendes Verständnis für Object Storage als Technologie und einige Use Cases vermittelt werden, denn: Object Storage ist nicht gleich Object Storage.

Es werden zunächst die Grundlagen und Ähnlichkeiten mit anderen Technologien beschrieben. Danach sollen die verbreitetsten Arten von Object Storage dargestellt werden, nicht alle sind dabei überall verfügbar. Und da keine Technologie ein Selbstweck ist, werden für verschiedene Use Cases gezeigt, ob und warum Object Storage dafür (nicht) gut geeignet ist.

## Grundlagen von Object Storage

Object Storage unterscheidet sich sowohl in der Architektur als auch bei der Nutzung stark von traditionellen Storage-Technologien wie Block-Storage, z. B. in der Form von iSCSI oder Fibre Channel oder Fileservern. Fangen wir mit dem Zugriff auf die Daten an. Eine schematische Darstellung findet sich in Abbildung 1.

Der vielleicht größte Unterschied zu klassischem Storage: Es gibt keine Ordner, wie wir alle sie seit Jahrzehnten kennen. Ein Object Storage ist in sog. Buckets – Eimer – aufgeteilt, in denen Daten abgelegt werden können. „Alles in einen Eimer schmeißen“ ist also bei Object Storage kein reines Sprichwort. Das mag nach einem Rückschritt in die altehrwürdigen Zeiten von Multics und OS/360 aussehen. Aber das Fehlen von Ordnern wird durch andere Mechanismen ersetzt.

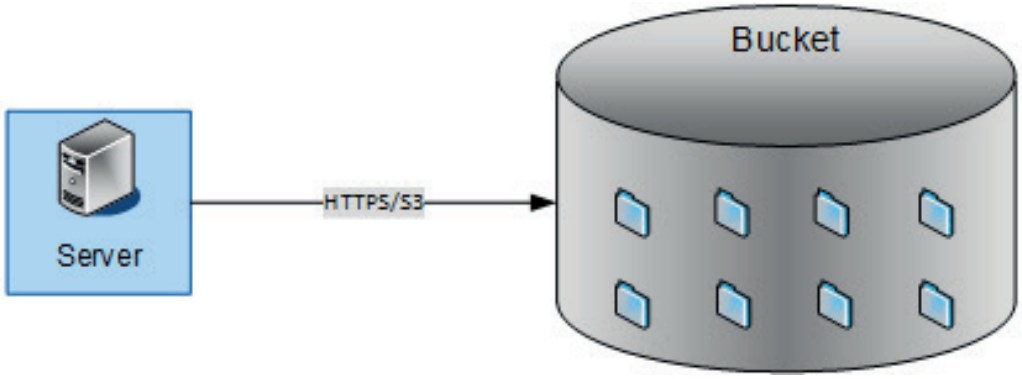



Abbildung 1: Zugriff auf einen S3-Bucket per HTTPS

Statt in Dateien mit einer begrenzten Zahl von Dateisystem-abhängigen Metadaten werden in Object Storage, wie der Name es schon andeutet, Daten in „Objekten“ abgespeichert. Die Identifikation innerhalb der oben genannten Buckets erfolgt anhand eines 128-bit-Identifiers, der sogenannten UUID, die typischerweise in hexadezimaler Form mit Bindestrichen dargestellt wird, z. B. 11223344-5566-7788-99aa-bbccddeeff00. Werden keine weiteren Funktionen genutzt, sollte man sich also eine Methode überlegen, wie man sich merkt, welche Daten zu welcher UUID gehören.

Aber genau hier kommen die weiteren Funktionen von Object Storage zum Einsatz: Vor allem die diversen Metadaten, die man an ein Objekt anhängen kann, sind dabei hilfreich. Diese können eine Vielzahl von Eigenschaften festlegen und auch bei der Suche helfen. Beispiele für mögliche Metadaten sind:

- Tags zur Sortierung und Organisierung
- Zugriffsrechte auf Nutzer- oder IP-Basis
- Ein Ablaufdatum, ab welchem Daten nicht mehr benötigt werden
- Ein Datum, ab dem die Daten verändert werden können – hierauf wird im Bereich der besonderen Funktionen noch genauer eingegangen
- Sprechende Namen

Durch diese in sich geschlossene Natur der Objekte ergibt sich auch eine große Herausforderung: Um einen Teil der Daten zu verändern, muss eine wesentlich größere Menge an Daten komplett neu hochgeladen und abgelegt werden. Das bedeutet entweder einen neuen Upload des gesamten Objekts oder zumindest eines Teils. Hierfür gibt es eine eigene Funktion, die jedoch eine Minimalgröße für den zu ändernden Teil hat sowie eine maximale Anzahl von Teilen für ein Objekt. Bei AWS S3 zum Beispiel ist die minimale Größe 5 MB und eine Aufteilung auf maximal 10.000 Teile möglich. Wird ein Objekt größer, bedeutet dies irgendwann unweigerlich größere Teile für das Objekt und längere Änderungszeiten. Für kleinere Objekte mag der Overhead sich in Grenzen halten. Bei größeren Objekten kann die Änderung eines einzelnen Bits aber zu enorm langen Schreibvorgängen führen. Zwar mag damit Object Storage für kleinere Datenmengen attraktiv wirken, jedoch wird der Overhead durch die Metadaten und die einzelnen Netzwerk-Verbindungen für jedes Objekt schnell signifikant. Und damit zeigt sich ein erster und vielleicht der wichtigste Use Case, den wir später genauer betrachten werden: Die Ablage von Daten, auf die fast nur lesend zugegriffen wird.

Der Zugriff auf die Daten erfolgt auch anders als im Bereich von klassischem Storage, wo entweder ein Protokoll wie NFS oder SMB für den Zugriff auf Dateisysteme oder Block-Storage-Protokolle gesprochen werden. Der Zugriff auf die Daten, ob lesend oder schreibend, erfolgt über HTTPS, also verhält sich, überspitzt dargestellt, der Storage wie eine Web-Anwendung oder eine REST-API.

Und hier kommt, auch für Nutzer die erste Komplikation ins Spiel: Zwar ist der Zugriff per HTTPS eigentlich standardisiert, es kann aber auf zwei Ebenen zu (teilweise großen) Unterschieden kommen:

- Zum einen ist S3 zwar für Object Storage der verbreitetste „Dialekt“, aber nicht der einzige.
- Zum anderen unterstützt auch nicht jeder S3-konforme Object Storage alle Funktionen und Befehle.

Auf diese Unterschiede wird weiter unten noch genauer eingegangen.

Die Grundlagen zu den Objekten und dem Zugriff darauf ist jetzt bekannt. Wie genau werden die Daten im Hintergrund abgelegt?

## Die Verteilung von Daten

Schauen wir uns also als nächstes an, wie Daten verteilt werden und welche Redundanz-Mechanismen zum Einsatz kommen (können):

Ein Hinweis vorweg: Bei der eigentlichen Verteilung der Daten auf verschiedene Datenträger oder Systeme sind die Details natürlich nur für On-Permises-Lösungen zu betrachten. Was genau bei Cloud-Anbietern eingesetzt wird, ist für den Nutzer nicht ersichtlich.

Bei den verbreitetsten On-Premises-Lösungen findet die Verteilung der Daten auf zwei Ebenen statt:

- Zum einen auf Ebene der Datenträger der beteiligten Systeme
- Zum anderen die Verteilung der Daten auf verschiedene Systeme, falls mehr als ein System zum Einsatz kommt.

Damit ergeben sich im Großen und Ganzen drei Möglichkeiten, Object Storage im eigenen Rechenzentrum zu betreiben:

- Ein System mit einem einzelnen Datenträger zur Ablage der Objekte (Single Node Single Disk):
  Die vielleicht einfachste Realisierung eines Object Storage. Diese Lösung ist eigentlich nur in Eigenarbeit mit Software-Lösungen denkbar. Kommerzielle Hersteller von Object-Storage-Appliances liefern zumeist größere Systeme, die unter die nächsten beiden Kategorien fallen. Trotzdem haben Single-Node-Single-Disk-Storages ihre Daseinsberechtigung: In Test- und Entwicklungsumgebungen ist ein einfacher Storage sinnvoll, da ein Datenverlust häufig verkraftbar ist und es sich auch nur um Testdaten handelt. Hier für einzelne Anwendungen komplette Object-Storage-Cluster aufzubauen, ist in vielen Fällen zu kostenintensiv.

- Ein System mit mehreren Datenträgern (Single Node Multiple Disks):
  Hier können wir das erste Mal von einem auch für Produktivsysteme geeigneten Object Storage reden, da der Ausfall von Datenträgern nicht zu Datenverlust führt. Viele andere Komponenten, wie Netzteile, Lüfter etc. sind typischerweise auch redundant ausgelegt. Für unternehmenskritische Anwendungen ist diese Lösung aber auch nicht optimal. Bei „klassischem“ Storage kommen nicht umsonst Multi-Controller-Lösungen oder sogar synchrone Spiegelung über mehrere Standorte zum Einsatz.

- Mehrere Systeme jeweils mit mehreren Datenträgern (Multiple Nodes Multiple Disks):
  Hier ergibt sich die optimale Redundanz: Egal ob einzelne Datenträger oder ganze Systeme ausfallen: Die Daten werden (entsprechende Konfiguration vorausgesetzt) so verteilt, dass sie immer noch verfügbar sind. Dies ist die für Produktivsysteme optimale Architektur. Ein weiterer Vorteil: Eine Erweiterung der Kapazität ist einfach durch Hinzufügen weiterer Node möglich.

Natürlich gäbe es theoretisch noch die Möglichkeit, mehrere Systeme mit jeweils einem Datenträger zu nutzen. Der Overhead ist jedoch in diesem Fall nicht vertretbar und wird daher nicht weiter betrachtet.

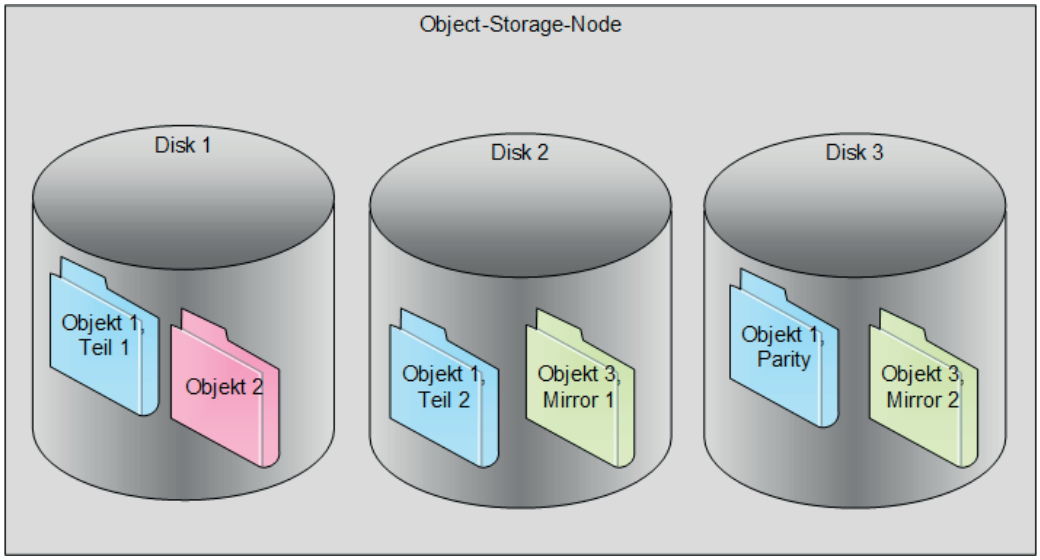



Abbildung 2: Aufteilung von Objekten innerhalb eines Nodes. Buckets und deren Objekte können unterschiedliche Redundanzen bieten. Hier: Einfache Parität (Objekt 1, blau), keine Redundanz (Objekt 2, rot) oder Spiegelung (Objekt 3, grün). Bei mehreren Nodes oder zusätzlichen Disks auch Mehrfach-Parity möglich.

Auch eine Replikation über verschiedene Standorte ist möglich. Ob man dabei eine synchrone oder asynchrone Replikation nutzt, hängt von vielen Faktoren ab, die den Rahmen dieses Artikels sprengen.

Die Aufteilung innerhalb eines Nodes ist in Abbildung 2 dargestellt, die Kopplung mehrerer Systeme und Standorte in Abbildung 3.

Wie viel Redundanz – aka wie viel Spiegelung oder Parität – pro Objekt benötigt wird, lässt sich bei On-Premises-Lösungen ebenfalls konfigurieren, meistens auf Bucket-Ebene. Ebenso werden die Objekte je nach Lösung in unterschiedlich große Teile aufgeteilt, für die dann die geforderte Redundanz greift.

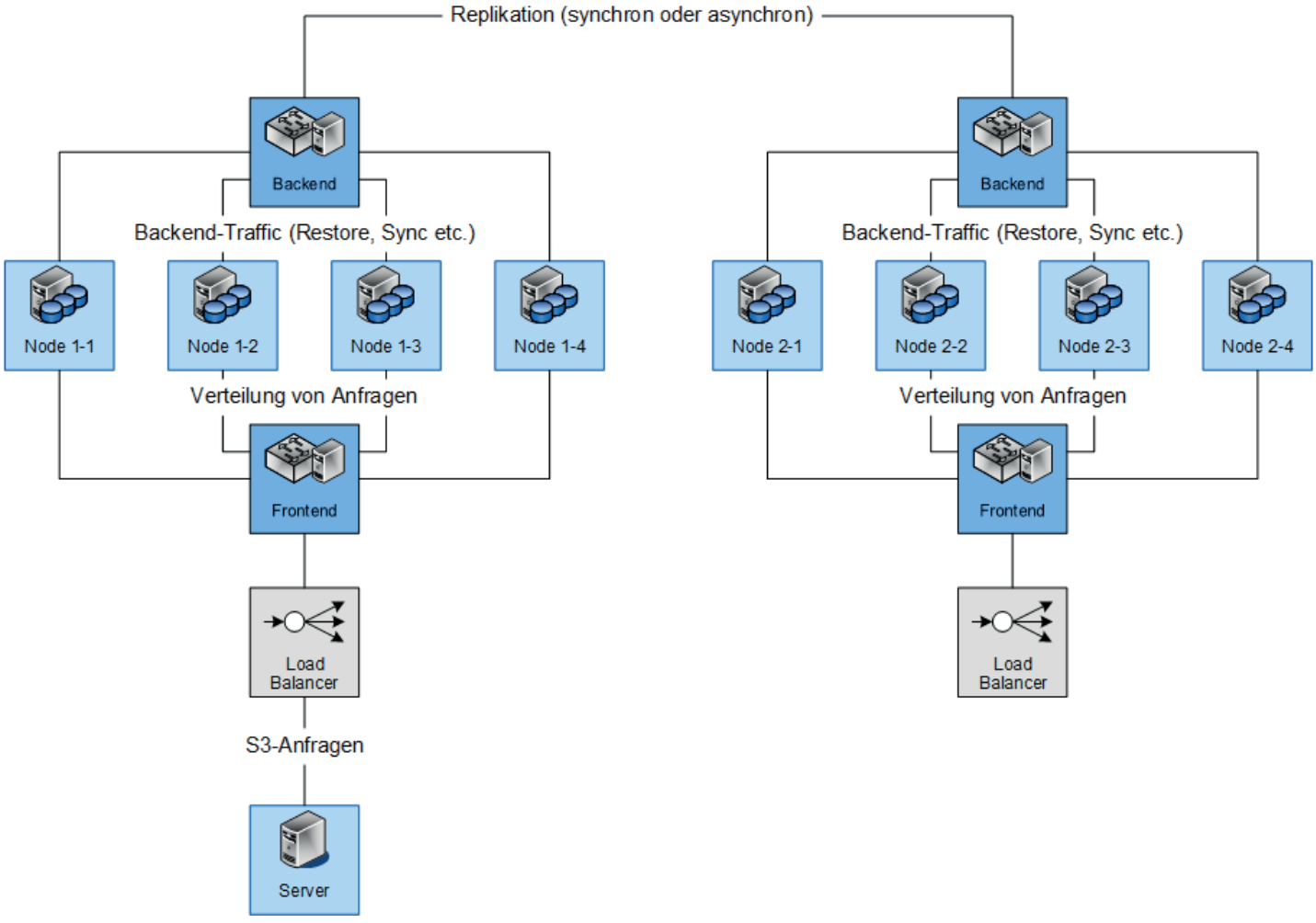



Abbildung 3: Beispielhafte Netzwerk-Topologie für einen Multi-Site, Multi-Node Object Storage

Sobald man mehrere Datenträger in einem System einsetzt, muss man auch noch weitere Vorgaben beachten. Im Gegensatz zu einem klassischen zentralen Storage müssen die Datenträger in einem Node oder Disk-Shelf immer die gleiche Größe haben. Ist dies nicht der Fall, werden normalerweise alle Datenträger identisch zum kleinsten Datenträger behandelt. Was man in der Darstellung der Architekturen und in diesem Abschnitt vielleicht auch schon zwischen den Zeilen lesen konnte: Ein klassisches RAID ist für den Ablageort der Objekte üblicherweise nicht vorgesehen und auch nicht empfohlen. Hier greift der Object Storage selbst ein und verteilt die Daten selbständig. Da das System weiß, welche Daten wo liegen und welche Bereiche der Datenträger noch frei sind, ist eine Wiederherstellung nach einem Ausfall einfacher: Es müssen nur die genutzten Bereiche wiederhergestellt werden. Eine Warnung an dieser Stelle: Besteht ein Zugriff auf das zugrundeliegende Betriebssystem, z. B. beim Einsatz von Open-Source-Software, so sollten die für den Object Storage genutzten Datenträger für nichts anderes verwendet werden!

Sobald mehr als ein Node zum Einsatz kommt, ist ein Object Storage ähnlich aufgebaut wie ein verteilter Storage. Mit dieser Ähnlichkeit kommt eine ganze Reihe von Vorteilen, gerade was Redundanz, Wiederherstellung und Skalierbarkeit angeht. Man bezahlt aber auch einen Preis dafür: Bei Ausfall eines Datenträgers oder Nodes erfolgt eine schnelle und gezielte Wiederherstellung der Daten an anderen Orten, um die Redundanz wieder herzustellen. Dies ist aber mit einer erheblichen Auslastung des Netzwerks und der Datenträger verbunden, was einen Einfluss auf den regulären Zugriff auf die Daten haben kann.

Damit kommen wir zu einem weiteren Thema, das beim Einsatz von Object Storage nicht außer Acht gelassen werden darf: Die Planung und Dimensionierung des Netzwerks. Dadurch, dass Object Storage vor allem für große Datenmengen geeignet ist, sollte auch eine entsprechende Netzwerk-Bandbreite zur Verfügung stehen. Die beste Technologie für die Ablage von Objekten im Terabyte-Bereich nutzt einem nichts, wenn das Netzwerk nur 100 Mbit/s liefert.

Auch das ist prinzipiell nichts neues: Ein klassischer Storage bietet normalerweise mehrere Ports mit hoher Bandbreite, die in Summe ein Vielfaches der Bandbreite der möglichen Clients liefern. Bei Object Storage kommt hier jedoch die Ähnlichkeit zu verteiltem Storage zum Tragen: Im Hintergrund oder bei einem Restore müssen die Daten auf mehrere Systeme verteilt werden, also erzeugt ein Object Storage auch viel Backend-Traffic. Zwar ist es grundsätzlich möglich, diese beiden Traffic-Arten über gemeinsame Netzwerk-Interfaces zu führen, es bietet sich aber an, den Backend-Traffic zu trennen. Mindestens über eigene Netzwerk-Interfaces der Nodes, im Optimalfall durch eigene Switches. Das führt insgesamt zu mehr Performance und ist deterministischer.

Damit sind die grundlegenden Aspekte von Object Storage geklärt: Was ist es? Wie benutze ich es? Wie werden die Daten im Hintergrund organisiert?

Bis jetzt haben wir nur ein paar „Eimer“, in die wir Daten einwerfen und aus denen wir sie wieder auslesen können. Was bietet uns Object Storage für weitere Möglichkeiten, gerade mit Blick auf die ganzen Zusatzinformationen, die an ein Objekt angehängt werden können?

## Besondere Funktionen

Bei den weiteren Funktionen kommen wir in einen Bereich, in dem sich nicht alle Lösungen gleich verhalten. Ich möchte an dieser Stelle die häufigsten Funktionen erwähnen.

Zunächst ist da der Umgang mit den vielen verschiedenen Redundanz-Mechanismen und -Ebenen, die ich oben beschrieben habe. Diese sind typischerweise auf verschiedenen Ebenen konfigurierbar. Meistens gilt dies auf Bucket-Ebene, teilweise kann die gewünschte Redundanz für ein Objekt auch als Metadatum an ein Objekt angehängt werden.

Zusätzlich ist eine Versionierung von Objekten sehr häufig möglich. Das heißt: Sollte ein Objekt überschrieben werden, werden alte Versionen noch vorgehalten und können über entsprechende Anfragen auch wieder ausgelesen werden. Das kostet Speicherplatz im Object Storage, weswegen man typischerweise eine begrenzte Anzahl von alten Versionen vorhält. Wie viele das sind, muss konfiguriert werden.

Zu den Komfort-Funktionen von Object Storage gehören Suchfunktionen und die mögliche Vorverarbeitung der Daten.

Die Suchfunktionen basieren dabei auf Tags und anderen Metadaten, die an das Objekt angehängt sind. Damit können Nutzer alle Daten zu einem bestimmten „Thema“ schneller finden und runterladen.

Die Vorverarbeitung von Daten ist für Datenanalysen oder Anonymisierung/Pseudonymisierung sehr nützlich, erfordert aber ein tiefes Verständnis der zu erwartenden Daten und Kenntnisse in der Programmierung von entsprechenden Interfaces. Hier sind Cloud-Dienste im Allgemeinen im Vorteil, da sie typischerweise auch für den Object Storage optimierte Dienste für die Vorverarbeitung anbieten, z. B. AWS Lambda oder Azure Functions.

Auch lassen sich Objekte individuell verschlüsseln und der Schlüssel vom Object Storage verwalten. Wie weit man einem Object Storage hier vertraut, muss man für sich entscheiden, gerade bei Cloud-basierten Lösungen.

Und wo wir schon mit Verschlüsselung anfangen: Es gibt noch einige weitere Funktionen, die im Bereich der IT-Sicherheit helfen können:

- Benachrichtigungen auf Bucket-Ebene:
  Viele Lösungen unterstützten eine Protokollierung und/oder Benachrichtigung bei bestimmten Ereignissen. Wird zum Beispiel immer wieder ein Objekt aktualisiert, dass eigentlich statisch sein sollte, kann das ein Indikator für einen Angriff sein.

- Object Lock:
  Bei der „Object Lock“-Funktion handelt es sich um eine Object-Storage-Version von „Write Once Read Many“ (WORM), wie man es vielleicht aus der Welt der Bandlaufwerke noch kennt: Daten können einmal geschrieben und beliebig oft gelesen, jedoch nicht mehr geändert werden. Markiert man ein Objekt in dieser Weise, wird es in keinem Fall geändert oder gelöscht und somit vor Manipulation, zum Beispiel durch Ransomware, geschützt. Im Gegensatz zu WORM-Tapes, die entsorgt werden, wenn sie nicht mehr benötigt werden, unterstützt Object Storage ein Ablaufdatum für die mit Object Lock versehenen Daten. Diess Ablaufdatum wird pro Objekt vergeben, und nach Ablauf dieses Datums können die Daten gelöscht und der Speicherplatz wieder anderweitig genutzt werden. Dabei wird zwischen zwei Modi unterschieden:

  - Governance: Hier können die Nutzer, die die Daten ablegen, diese vor dem Ablaufdatum nicht mehr verändern oder löschen, Administratoren aber haben diese Möglichkeit.

- Compliance: In diesem Fall ist auch für die Administratoren eine Veränderung oder Löschung der Daten nicht möglich.

Damit haben wir jetzt die wichtigsten und einige spannende, weitere Funktionen kennengelernt. Es wurde bereits darauf eingegangen, dass bestimmte Funktionen von der genauen Lösung abhängen. Daher sollen im nächsten Abschnitt die Unterschiede etwas genauer beleuchtet werden.

## Object-Storage-Varianten und ihre Unterschiede

Zuallererst soll hier noch mal wiederholt werden, was bereits weiter oben erwähnt wurde: Es gibt nicht „den einen Object Storage“, sondern verschiedene Varianten und Ausprägungen. Die vielleicht verbreitetsten Varianten dabei sind AWS S3 und Azure Blob Storage. Beide sind, wie der Name schon andeutet, von Cloud-Herstellern entwickelt worden und vor allem in der Cloud verfügbar.

Ein weiterer Object Storage, der bei einigen Kunden im Einsatz ist, ist Ceph. Dieser vor allem unter Linux verbreitete Object Storage wird typischerweise über Systeme angesprochen, die Ceph-spezifische Funktionen liefern und für Spezialaufgaben genutzt werden. Er bietet einige Funktionen, die für Object Storage untypisch sind, z. B. eine gezielte Änderung, dafür fehlen andere Funktionen. Man kann Ceph zwar über entsprechende Gateways über andere Protokolle ansprechen, darunter auch S3. Von den Vorteilen hat man dann aber nichts. Typische Beispiele für den Einsatz von Ceph sind hyperkonvergente Systeme (HCI – Hyper-Converged Infrastructure) und Supercomputing oder HPC (High Performance Computing).

Zusätzlich gibt es noch anderen Storage, der technisch gesehen zwar ein Object Storage ist, auf den aber immer nur über Abstraktionsschichten zugegriffen wird. Diese werden nicht weiter betrachtet.

Die Unterschiede zwischen den verschiedenen Versionen liegen vor allem in den genutzten Protokollen und – bei HTTPS-basiertem Object Storage – im genauen Format und dem Inhalt von Anfragen und Antworten.

Nicht alle Anbieter unterstützen dabei jeden „Dialekt“, und auch nicht jede Lösung ist on Premises verfügbar. Daher soll im nächsten Abschnitt betrachtet werden, wo und wie sich Cloud und on Premises unterscheiden.

## Object Storage in der Cloud vs. on Premises

Direkt vorweg: Azure Blob Storage von Microsoft ist nur in der Azure-Cloud verfügbar. Es gibt zwei Ausnahmen:

- Für Tests und für Entwickler gibt es den Microsoft Azure Storage Emulator, der jedoch weder im Bereich Performance noch bei der Redundanz die Anforderungen einer typischen Unternehmensanwendung erfüllen kann.

- Hat man Azure Stack Hub im Einsatz, bietet dieses natürlich auch Storage-Technologien aus der Azure Cloud, und damit auch Azure Blob Storage. Diese sind zwar direkt im eigenen Rechenzentrum verortet, aber stark an Microsoft gebunden.

Das heißt, egal wie man es dreht und wendet: Will man Azure Blob Storage einsetzen, ist man auf Microsoft beschränkt.

Ganz anders sieht es beim Platzhirsch im Bereich Object Storage aus: S3-Storage ist in vielen Farben und Formen sowohl in der Cloud als auch on Premises realisierbar. Natürlich denkt man bei S3 unweigerlich als erstes an AWS – daher kommt es schließlich auch. Aber auch andere Cloud-Anbieter bieten S3-kompatiblen Storage. Und damit nicht genug: Auch on Premises gibt es von allen namhaften (und einigen weniger namhaften) Herstellern und Entwicklern S3-basierten Object Storage. Auch kleinere Hersteller können hier einen Blick wert sein.

Eine Alternative zu großen Herstellern kann Open Source sein, vorausgesetzt, die Hardware ist vorhanden, und die Möglichkeit für eine Einarbeitung besteht. Hier ist vor allem minIO zu erwähnen, welches eine sehr weitgehende Unterstützung der Funktionen von S3 liefert.

## Open-Source-Beispiel: minIO

minIO ist die wohl verbreitetste Open-Source-Lösung für S3-basierten Object Storage. Es unterstützt alle oben genannten Architekturen (Single Node Single Drive, Single Node Multiple Drives, Multiple Nodes Multiple Drives) und bietet eine sehr umfangreiche und verständliche Dokumentation. Was besonders nützlich ist: minIO dokumentiert sehr offen, welche Funktionen von S3 nicht unterstützt werden und generell, welche Einschränkungen sonst bestehen. Auch ist die Dokumentation von minIO sehr deutlich darin, welche Szenarien nicht empfohlen werden, entweder aus Performance- oder aus Sicherheitsgründen.

Daher ist minIO gut dafür geeignet, erste Erfahrungen mit Object Storage zu sammeln und um Object Storage für Testzwecke bereitzustellen. Will man ein Produktiv-System für Object Storage auf Basis von minIO nutzen? Darauf gibt es die übliche Berater-Antwort: Es kommt darauf an. Technisch und hinsichtlich des Funktionsumfangs ist minIO gut aufgestellt, jedoch bedeutet ist es wahrscheinlich mit einem höheren Aufwand bei der Installation und beim Betrieb verbunden.

## (Do Not) Use Cases

Als nächstes soll betrachtet werden, wofür Object Storage (gut oder nicht so gut) geeignet ist. Ja, es ist eine interessante Technologie., Das heißt noch lange nicht, dass ich damit meinen bisherigen Storage ablösen kann.

Fangen wir zunächst mit Bereichen und Use Cases an, für die Object Storage gut geeignet ist. Einige dieser Use Cases waren sogar die ursprüngliche Motivation für die Entwicklung von Object Storage:

- Big Data und KI:
  Der erste Einsatzzweck von Object Storage war die Ablage großer Datenmengen, die sich selten bis gar nicht ändern, um diese dann auf leistungsstarken Servern zu analysieren. Hier war am Anfang „Big Data“ ein Kandidat für die Nutzung von Object Storage. Mittlerweile sind noch einige Use Cases hinzugekommen, die ähnliche Anforderungen stellenund andere Namen haben. Als aktuell prominentestes Beispiel sei hier Künstliche Intelligenz und insbesondere deren Training genannt. Hier werden Unmengen an Daten benötigt, die sich nicht ändern. Es werden lediglich weitere Daten in großen „Paketen“ hinzugefügt – die Paradedisziplin von Object Storage.

- Backup und Archivierung:
  Wenn man an große Datenmengen denkt, die selten geändert werden und bei denen die Performance nicht das Allerwichtigste ist, ergibt sich ein weiterer Use Case quasi von selbst: Backup und Archivierung. Man hofft, dass man eigentlich nur sichern und niemals wiederherstellen muss, also ist Object Storage ein vielversprechender Kandidat. In Verbindung mit der recht flexiblen WORM-Funktionalität, die nicht so endgültig ist wie bei WORM-Tapes, ergibt sich auch ein guter Schutz vor versehentlicher oder vorsätzlicher Manipulation und damit vor dem aktuellen Schreckgespenst der IT: Ransomware. Das haben auch die Entwickler von Backup-Software erkannt. Gerade die im professionellen Umfeld gängigen Backup-Lösungen unterstützen als Ziel Object Storage, egal ob on Premises oder in der Cloud.

- Auslagerung alter Daten (Tiering):
  Eine weitere Funktion, die Object Storage übernehmen kann, ist das Vorhalten alter Daten, die so selten genutzt werden, dass sie auf dem (teuren) Primär-Storage nur Platz wegnehmen, der eigentlich besser für andere Daten geeignet wäre. Damit sind wir in der auch nicht so neuen Welt des Storage-Tierings. Wo früher von SSD auf HDD ausgelagert wurde, bieten heute viele Storage-Systeme ein Tiering auf Object Storage an. Teilweise herstellerunabhängig, meistens jedoch mit einer optimierten Integration in die Object-Storage-Systeme des jeweiligen Herstellers. Ein kleiner Hinweis an dieser Stelle: Diese gute Integration lassen sich manche Hersteller in Form von zusätzlichen Lizenzen extra bezahlen!

Sollte ich mich für einen Cloud-basierten Object Storage entscheiden und diesen auch von meinen lokalen Systemen aus benutzen wollen, muss ich daran denken, dass die Daten auch übertragen werden müssen. Nicht umsonst bin ich auf einen möglichen Flaschenhals im Netz eingegangen. Bei Cloud-basiertem Object Storage kann dieser noch viel unangenehmer werden. Nicht umsonst bieten die großen Cloud-Anbieter auch die Möglichkeit an, Daten per Post zu verschicken und in den jeweiligen Object Storage zu übertragen. Hier greift ein Zitat von Andrew S. Tanenbaum: „Never underestimate the bandwidtch of a station wagon full of Tapes hurtling down the highway.“ Oder, frei übersetzt: „Unterschätze niemals die Bandbreite eines Kombis voller Tapes auf der Autobahn.“

Ich möchte auch nicht verschweigen, für was ein Object Storage nicht gut geeignet ist:

- Sobald ein System, welches externen Storage nutzt, viele Änderungen an den Daten vornimmt, ist ein Object Storage nicht gut geeignet. Selbst bei einer Aufteilung in viele Teile kann dies für die Änderung eines Blocks einen Upload von mindestens 5 MB bedeuten. Und bei Objektgrößen jenseits von 50 GB werden die jeweiligen Teile der Daten unweigerlich größer. Bei Datenbanken zum Beispiel kann dies zu enormen Performance-Problemen führen.

- Bei der Ablage vieler kleiner Dateien/Objekte läuft man in eine andere Herausforderung: Jedes Objekt muss in einem eigenen Request hochgeladen werden. Der Overhead für den Verbindungsaufbau kann hier signifikant sein. Sind dann noch viele Metadaten an das Objekt angehängt, wird das Verhältnis zwischen zu übertragenden Daten und den eigentlichen Nutzdaten noch ungünstiger.

## Die Sicherheit von Object Storage

Ein weiteres Thema, das ich ansprechen möchte, ist die Sicherheit von Object Storage. Denn man liest immer wieder davon, dass S3 Buckets im Internet gefunden werden, auf denen vertrauliche Daten liegen, auf die komplett ohne weitere Authentisierung zugegriffen werden kann. Daraus könnte man schließen, dass Object Storage inhärent unsicher ist. Das ist nicht der Fall. Object Storage bietet viele Sicherheitsmechanismen, auch was die Zugriffsregelung angeht. Und wir haben mit dem Object Lock auch schon ein weiteres Puzzle-Stück gesehen, das sich positiv auf die Sicherheit auswirken kann. Woher kommen also diese ganzen Datenlecks, von denen man auf einschlägigen Newstickern immer wieder liest?

Ganz einfach: Die Sicherheitsmechanismen von Object Storage müssen auch konfiguriert und genutzt werden. Es nutzt mir nichts, ein großartiges RBAC zu haben, wenn ich keine Authentisierung verlange, sondern alle Anfragen beantworte!

Früher war die Situation bei AWS nicht ganz optimal, da viele Sicherheitsmechanismen für S3 Buckets im Standard deaktiviert waren. Hier hat sich einiges getan, und die wichtigsten Mechanismen inklusive Authentisierung sind mittlerweile per Default aktiviert. Das hilft jedoch nicht, wenn man die Mechanismen dann aus Bequemlichkeit wieder abschaltet!

Wie bei so vielen Systemen und Maßnahmen in der IT bedeutet das also: Ich kann es sicher betreiben, muss mir aber Gedanken dazu machen und die Mechanismen, die mir zur Verfügung stehen, auch konsequent einsetzen.

## Fazit

Zusammenfassend kann man über Object Storage sagen, dass es eine sehr interessante und nützliche Technologie ist. Object Storage insgesamt ist gekommen, um zu bleiben, denn es bietet eine einfache und vergleichsweise günstige Möglichkeit, mit großen Datenmengen umzugehen.

Wird Object Storage unseren bisherigen Storage ablösen? Definitiv nicht, denn die Art und Weise, wie Daten abgelegt und verarbeitet werden, passt einfach nicht zu allen Use Cases. Im Bereich Big Data, KI und Backup haben wir mit Object Storage etwas, was bisherige Technologien mindestens ergänzen und in einigen Fällen sogar ablösen kann.

Ist es sinnvoller, Object Storage aus der Cloud oder lokal zu beziehen? Das hängt maßgeblich davon ab, welche Datenmenge übertragen wird und wo meine „Clients“ für den Object Storage verortet sind. Habe ich alles in der Cloud, ist eine On-Premises-Lösung wenig sinnvoll. Umgekehrt bietet mir ein Object Storage in der Cloud, den ich von lokalen Systemen aus nutze, eine gewisse Redundanz und Standort-Unabhängigkeit. Hier muss auch die Bandbreite meiner Cloud-Anbindung mitspielen!

# Aktuelle Seminare

Cybersecurity: Vom Social Engineering zu erfolgreichen Awareness-Trainings
10.06.2024 online

✓ Sommerschule – Neueste Trends der IT-Infrastruktur
10.06.-14.06.2024 Aachen | online

Jira für Projektadministratoren
12.06.-13.06.2024 online

✓ IT-Sicherheitsrecht 3.0:Überblick über die neuen IT-Sicherheitsgesetze
13.06.2024 online

SIP-Trunk: Notruf, Fax und Netzdesign
13.06.2024 online

Datenschutz bei einer Videoüberwachungsanlage – Grundlagen (DSGVO und Co.)
13.06.2024 online

Unified Communiciations: Strategien für Ihr Unternehmen
17.06.2024 online

KI als GameChanger und die damit verbundene digitale Transformation
17.06.-18.06.2024 online

Microsoft 365 rechtssicher einführen
18.06.2024 online

Netzzugangskontrolle (NAC)
18.06.-19.06.2024 online

✓ SIP: Basistechnologie für VoIP und IP-Telefonie
18.06.-19.06.2024 online

✓ Hybrid Cloud: RZ der neuen Generation
18.06.-20.06.2024 online

Systematische Absicherung industrieller Automatisierungssysteme mit der IEC 62443
19.06.2024 online

Data Breach Notification: Datenschutzpannen nach der DSGVO
19.06.2024 online

✓ Kundenorientierte Kommunikation im IT-Support
19.06.2024 online

✓ Windows PKI und Zertifikatsverwaltung
19.06.-20.06.2024 online

Generative KI: Entwicklung und rechtliche Herausforderungen
20.06.2024 online

Modern Workplace: Konzepte und UCC-Lösungen
20.06.2024 online

Apple in die eigene IT integrieren – mit guter Planung kein Problem
20.06.2024 online

IT-Sicherheit und Compliance in der IT-Praxis
24.06.2024 online

✓ Garantietermin

# ComConsult Online-Veranstaltungskalender

**https://www.comconsult.com/kalenderuebersicht/**

# Zertifizierungen

## ComConsult Certified Network Engineer

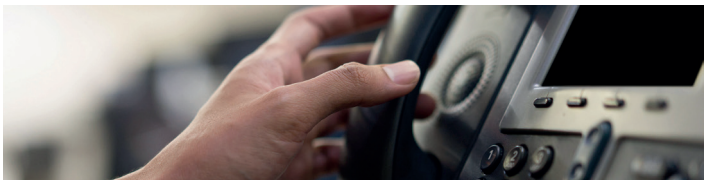
Lokale Netze für Einsteiger
02.09.-06.09.24 in Aachen
31.03.-03.04.25 in Aachen

TCP/IP-Netze erfolgreich betreiben
29.10.-31.10.24 in Aachen
13.05.-15.05.25 in Aachen

Switching und Routing: Optimales Netzdesign
24.09.-27.09.24 in Aachen
08.04.-11.04.25 in Aachen

Paketpreis für alle drei Seminare: € 6.273,--* statt € 6.970,--

## ComConsult Certified Voice Engineer



Unified Communications – von Grundlagen über Planung bis Umsetzung
25.06.-27.06.24 online
29.10.-31.10.24 in Aachen
18.03.-20.03.25 in Aachen

SIP: Basistechnologie für VoIP und IP-Telefonie
18.06.-19.06.24 online
05.11.-06.11.24 in Aachen

Sicherheitsmaßnahmen für VoIP und UCC
03.12.-05.12.24 in Bonn
08.04.-10.04.25 in Aachen

Paketpreis für alle drei Seminare: € 5.013,--* statt € 5.570,-

* Alle ausgewiesenen Preise sind Netto-Preise. Alle Paketpreise sind zzgl. abschließender Prüfung (Einzelpreis € 180,--).
Alle Seminare bieten wir auch als Online-Seminar an.

# Sparen Sie 20% bei jeder Buchung


## ComConsult Firmenkarte

- Die ComConsult Firmenkarte kostet 950,00 € netto.
- Die Gültigkeit des Rabatts beginnt mit dem Tag der Bestellung für 12 Monate. Rabattiert werden alle offen angebotenen Veranstaltungen, die in diesem Zeitraum liegen.
- Sie erhalten mit der Bestätigung Ihrer Bestellung einen Code, der bei jeder Veranstaltungsbuchung anzugeben ist. Wir gewähren Ihnen den Rabatt automatisch bei der Anmeldung.
- Der Rabatt gilt nicht für Inhouse-Schulungen.
- Der Rabatt ist nicht mit anderen Vergünstigungen wie Paketpreise für Zertifizierungen und Rahmenverträge kombinierbar.
- Bei Buchungen über andere Bildungsplattformen oder Seminarvermittler, die Provision berechnen, kann der Rabatt nicht gewährt werden.

# Die Autoren dieser Ausgabe

**Dr. Markus Ermes** hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau und Nutzung von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage und Cloud-basierten Diensten liegen. Seine Kenntnisse im HPC-Bereich geben zusätzlich Einblicke in modernste Hochleistungstechnologien (CPU, Storage, Netzwerke), die in Zukunft auch im Rechenzentrum Einzug erhalten können.
**Kontakt: ermes@comconsult.com**

**Dr. Behrooz Moayeri** blickt auf über drei Jahrzehnte Projekterfahrungen zurück. Er gehört der Geschäftsleitung der ComConsult GmbH an und ist Leiter der ComConsult Akademie. Darüber hinaus betätigt er sich als Berater, Autor und Seminarleiter.
**Kontakt: moayeri@comconsult.com**

**Thomas Steil** ist Geschäftsführer und Leiter des Competence Centers Smart Technologies. Neben seiner Tätigkeit als Berater und Projektleiter ist er Autor diverser deutscher und englischsprachiger Artikel.
**Kontakt: steil@comconsult.com**

**Dr. Joachim Wetzlar** ist seit mehr als 25 Jahren Senior Consultant der ComConsult GmbH und leitet dort das Competence Center „Tests und Analysen“. Er verfügt über einen erheblichen Erfahrungsschatz im praktischen Umgang mit Netzkomponenten und Serversystemen. Seine tiefen Detailkenntnisse der Kommunikations-Protokolle und entsprechender Messtechnik haben ihn in den zurückliegenden Jahren zahlreiche komplexe Fehlersituationen erfolgreich lösen lassen. Weiterhin führt er als Projektleiter und Senior Consultant regelmäßig Netzwerk- WLAN- und RZ-Redesigns durch.
**Kontakt: wetzlar@comconsult.com**

# Impressum

ComConsult GmbH - Pascalstr. 27 - 52076 Aachen
Amtsgericht Aachen HRB 6428 VAT ID no.: DE 811956504
Telefon: 02408/951-0 | E-Mail: kundenservice@comconsult.com
Web: www.comconsult.com

Herausgeber und verantwortlich:
ComConsult GmbH - Chefredakteur: Dr. Behrooz Moayeri
Erscheinungsweise: monatlich, 12 Ausgaben im Jahr
Bezug: kostenlos als PDF-Download