Dezember 2025

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Lizenzmodelle der Netzwerkausrüster

von Felix Gilleßen und Michael Schneiders
Das Thema Lizenzen hat nicht erst seit der umfassenden Änderung des Modells bei VMware an Bedeutung gewonnen. Ob im operativen Tagesgeschäft, in der strategischen Planung oder in der Administration – für alle IT-Verantwortlichen spielt die Lizenzierung eine wichtige Rolle.

Seite 8

Netz und Security: Aktuelle Aussagen der Hersteller

von Dr. Behrooz Moayeri
Am 07. Oktober 2025 lud ComConsult zur Veranstaltung „Hersteller-Roundtable Netz und Security“ ein. Sie fand im Online-Format statt und war gut besucht. Ich gehe im Folgenden auf einen kleinen Teil der Erkenntnisse ein, die ich von dem Tag mitgenommen habe, und bedanke mich insbesondere bei allen Referenten der Hersteller, die ihre Themen kompetent vertreten haben.

Seite 2

Der Fluch des Wissens: Warum du als Expert:in manchmal nicht verstanden wirst

von Steffen Moll
Viele IT-Profis kennen das: Man hat hohe Expertise und erklärt komplexe Themen präzise – und trotzdem kommt wenig an. Der „Fluch des Wissens“ sorgt dafür, dass wir vergessen, wie es ist, nichts zu wissen. In diesem Beitrag geht es darum, wie Inhalte verständlich und wirksam vermittelt werden können.

Seite 17

Webinar der Woche

Standards zum AI Act

Seite 27

Wie ComConsult die Tour de France gewinnt

von Dr. Joachim Wetzlar
Viele meiner Kollegen trainieren fleißig: Mal eben am Samstag nach Luxemburg und zurück, 24-Stunden-Rennen auf dem Nürburgring [1], und so fort. Und natürlich ist es ihr Traum, schließlich einmal bei der Tour de France mitfahren zu können.

Seite 29

Netz und Security: Aktuelle Aussagen der Hersteller

von Dr. Behrooz Moayeri

Am 07. Oktober 2025 lud ComConsult zur Veranstaltung „Hersteller-Roundtable Netz und Security“ ein. Sie fand im Online-Format statt und war gut besucht. Ich gehe im Folgenden auf einen kleinen Teil der Erkenntnisse ein, die ich von dem Tag mitgenommen habe, und bedanke mich insbesondere bei allen Referenten der Hersteller, die ihre Themen kompetent vertreten haben.

Neues von HPE

Nach der Juniper-Übernahme durch HPE gibt es „HPE Juniper Networking“ und den uns schon vertrauten Unternehmensbereich „HPE Aruba Networking“. Es darf darüber spekuliert werden, wie der Netzbereich bei HPE künftig heißen wird: HPE Networking?

Passend zum Titel der Veranstaltung war die Information über einen Top-of-Rack-Switch (ToR) mit Firewall-Funktionalität. Schließlich sind wir alle auf der Zero-Trust-Reise. Sie führt von offenen internen Netzen über segmentierte Netze bis zu dem Zustand, in dem jede Ressource so geschützt sein wird, als ob sie an das Internet angeschlossen wäre. Das Reiseziel ist somit gleich dem Ausgangspunkt, was die Netze betrifft. So weit sind wir aber nicht, weshalb wir den Schutz so nah wie möglich an die zu schützenden Ressourcen bewegen müssen, in diesem Fall also in den Rack, nah bei den Servern.

In der Veranstaltung war viel von KI-gestütztem Betrieb (AI-Ops) die Rede. Die ehrliche Aussage von HPE: Eigentlich braucht man gewerkübergreifende AI-Ops, vom Server und Storage über das Netz bis zum Endgerät. Das ist Zukunftsmusik. Es wird gerade mit AI Ops für Netze begonnen.

Die NAC-Lösung von HPE ist vielen bekannt. Es klang bei HPE so, dass NAC aus der Cloud möglicherweise OnPrem-NAC ablösen kann. Ich gehe jedoch nicht davon aus. Selbst bei KI sagt HPE, dass die mit KI-Funktionen versehene Management-Plattform „Central“ auch OnPrem realisierbar ist. Dafür werden 3 bis 7 Server gebraucht. Mich hat das nicht überrascht. Kleine KI-Modelle sind der Renner, erst recht nach dem DeepSeek-Schock. IBM macht Werbung für kleine LLM, auch in den Massenmedien.

Angereichert wurde der HPE-Vortrag mit einer Demonstration in einem Netz mit 311 Devices. Highlights: Insights mit AI-Empfehlungen, z. B. Erkennung von WPA3-fähigen Clients, damit man weiß, wann man die Access Points auf den bessern Sicherheitsstandard umstellen kann (wenn nämlich alle angezeigten Clients WPA3-fähig sind).

Die schlechte Nachricht: Auch HPE hat die Subscription-Lizenzen lieb gewonnen. Mit der Netz-Hardware kann man die Foundation oder die Advanced Subscription kaufen.

Arista überwacht Transceiver

Viele Netzprobleme lassen sich auf Transceiver-Ausfälle zurückführen. Bisher ist das Vorgehen überwiegend reaktiv: Der Link fällt aus, und der Transceiver muss ausgetauscht werden. Der Hersteller verspricht, dass die KI aufkommende Transceiver-Probleme im Vorfeld erkennen kann, etwa durch die Langzeitüberwachung der Temperatur und die Analyse der Entwicklung.

Wer wie Arista ein kleineres Produktspektrum als zum Beispiel Cisco oder HPE hat, kann dasselbe Betriebssystem (Extensible Operating System, EOS) auf allen Modellen laufen lassen. So wird es auch für das zentrale Management (Cloud Vision, CV) leichter, alle Komponenten zu verwalten.

Die WLAN-Lösung kommt ohne Controller aus, da die Access Points über eine vollwertige Control Plane verfügen, jedoch

selbstredend nicht ohne Management. Dieses gibt es in zwei Varianten: OnPrem oder in der Cloud.

Software-Updates sollen laut Anbieter im laufenden Betrieb mit einer Unterbrechung von weniger als 100 Millisekunden in der Data Plane (der Paketweiterleitung) möglich sein.

Es gab einige Momente in der Veranstaltung, wo ich dachte: allein dafür hat es sich gelohnt, dabei zu sein. So ein Moment war bei mir, als Arista ankündigte, statt „Spaghetti Code“ besser strukturierte Ensembles von Software-Modulen zu nutzen. Wer als zweiten Gang Spaghetti Code konsumiert, hat sicher als ersten Gang Kabelsalat genossen.

Wenn Sie bei diesem oder anderen Herstellern auf den Begriff NetDL stoßen, hier die Erklärung: Network Data Lake. Aus dem NetDL wird Input für KI generiert.

Bereits verfügbar ist AVA (Autonomous Virual Assistant), der in natürlicher Sprache spricht. Künftig soll es die Insights geben, mit denen man nicht nur die besagte Transceiver-Überwachung bekommt.

Der NAC-Bestandteil von Arista CV heißt AGNI (Arista Guardian for Network Identity) und ist sowohl OnPrem als auch in der Cloud verfügbar.

Die Arista ZTX Appliance wird zur Erfassung des Verkehrs und darauf basierend für Empfehlungen genutzt. ZTX greift den Datenverkehr zum Beispiel durch klassische Mirror Ports ab.

Über die Velocloud-Akquisition, mit der Arista seit Juli 2025 die SD-WAN-Sparte von VMware (Broadcom) übernommen hat, haben wir aufgrund der Kürze der Zeit in der Veranstaltung wenig erfahren. Ich habe jedoch an anderer Stelle diese Übernahme (positiv) bewertet.

Cisco: Smart Switches

Natürlich waren bei Cisco die neuen Smart Switches ein Thema. Mit diesen neuen Produkten und den darin verbauten Chips lassen sich Applikationen erkennen – kein Wunder, denn die DPU-Chips müssen ebenfalls die Intelligenz für statusbewusste Mikrosegmentierung mitbringen. Laut Angaben lassen sich 80-90% der Applikationen automatisch erkennen.

Mit der Lösung Firepower Threat Defense (FTD) lässt sich ein SD-WAN realisieren. Damit wird die Nahtstelle zwischen LAN und WAN zu einer intelligenten Komponente, die sich vielschichtig einsetzen lässt.

Daneben gibt es das SD-WAN auf Catalyst-Basis (die Router heißen nun auch Catalyst) sowie natürlich das Meraki SD-WAN.

Für die WAN-Verschlüsselung wird neben IPsec auch MACsec unterstützt, mit dem Vorteil, dass MACsec hardwarebasiert arbeitet und somit Wire Speed halten kann.

Cisco ist nicht der einzige Hersteller, dessen KI-Roadmap dreistufig ist. Hier heißen die Stufen so: Assurance (einfache ML-Funktionen), AI Assistant und Agentic AI.

Mit dem AI Assistant kann man bereits kontextabhängige Views generieren – anstelle der bisherigen statischen Dashboards.

Für das SD-WAN wird u.a. mit der Funktion „predictive path recommendations“ geworben, frei nach dem Motto: Diese Verbindung ist schon beinahe ausgelastet.

Der AI Assistant soll die Übernahme einer Konfiguration von einem alten zu einem neuen Switch erleichtern.

Die meisten AI-Funktionen sollen bei Cisco auch mit OnPrem-Servern möglich sein.

Extreme automatisierte und wurde doch von der Komplexität überholt

Ich danke ausdrücklich Extreme für einen weiteren jener Momente, die das Zuhören lohnenswert machten. Originalton der ehrlichen Aussage: „Die Komplexität ist schneller gewachsen als die Hersteller mit Automatisierung Abhilfe geschaffen haben“.

Das KI-fähige Management heißt ExtremeCloud IQ Site Engine. Die Entwicklung dient Zielen wie weniger manuelle Arbeit, kürzere Entstörungszeit, kürzere Downtimes und niedrigere Kosten. Abgedeckt werden die Produkte in den Bereichen LAN und WLAN inkl. der SPB-M-basierenden Fabric-Lösung.

Und auch hier durfte das duale Cloud-OnPrem-Portfolio nicht fehlen. Die „CloudIQ“ läuft entweder in AWS, Google Cloud Platform bzw. Azure (insgesamt an fast 30 Standorten) oder in kundeneigenen virtuellen Umgebungen bei AWS oder als Cloud Edge (OnPrem) mit Serverpaketen (3, 6, 9, 12 Server) auf Kubernetes-Basis.

Nach Unternehmensangaben wurde die OnPrem-Variante beispielsweise für sämtliche Schulen einer deutschen großen Stadt realisiert.

Für die Cloud-Variante wurde die C5-Zertifizierung angekündigt, die voraussichtlich in 2025 abgeschlossen sein wird.

Wie bei Cisco spricht der Hersteller von drei Phasen der AI-Entwicklung: AI Expert, AI Canvas, AI Agents. AI Expert wurde als eine Art Suchmaschine für Dokumentation beschrieben, die man etwa fragen kann: Wie konfiguriere ich OSPF? Dabei handelt sich um eine Explainable AI, die – anders als ChatGPT – nie halluziniert, sondern Quellen angibt wie zum Beispiel im zugehörigen Handbuch.

AI Canvas liefert eigene Dashboards (vgl. Cisco). Und zurzeit noch in der Implementierung: AI Agents (Agentic AI). Der Service-Agent hilft, mögliche Fehlerursachen auszuschließen.

Derzeit geht Extreme davon aus, dass in den meisten Fällen HITL (Human in the Loop) erforderlich bleibt – die KI macht Vorschläge, der Mensch nimmt sie an oder nicht.

Auch das bei Kunden ungeliebte Lizenzmodell war ein Thema. Wir haben gelernt, dass es die Lizenzen Pilot und Copilot gibt, wobei die Pilot-Lizenz für Cloud-Management erforderlich ist. Und schon wieder: Mit Platform ONE wird die Lizenzpolitik geändert. Wenn ich mich recht entsinne, soll es dabei vier Stufen geben.

Fortinet zapft fremde Gewässer an

Wir wissen längst, dass Fortinet nicht nur Firewalls verkauft, sondern auch Switches und WLAN-Komponenten. Mit den FortiGate-Firewalls lässt sich zudem SD-WAN bauen.

Damit können viele Logs gesammelt und zu einem Data Lake gemacht werden. Auch fremde Data Lakes können angezapft werden, etwa die Splunk/Cisco-SIEM-Lösung. Wo viele Daten vorhanden sind, kann es auch maschinelles Lernen und KI geben.

In einigen Komponenten kommen eigene ASICs zum Einsatz, die für Content Processing oder Beschleunigung genutzt werden können.

Und Sie dürfen raten, wie die Fortinet-KI heißt: FortiAI. Die dem Leser jetzt schon vertrauten drei Stufen heißen hier: Machine Learning (Deep Learning), GenAI, Agentic AI.

Das lässt sich zum Beispiel auf den Betrieb eines Security Operations Center wie folgt anwenden: Unified SOC, AI-driven SOC, Automated SOC.

Vielen ist schon bekannt, dass ein FortiGate nicht nur Wireless- und Switch-Controller, sondern auch ein Authentisierungsserver mit Basic NAC sein kann. Als kostenpflichtige Ergänzung steht außerdem FortiNAC zur Verfügung.

Auf meine Frage, ob das Unternehmen SASE auch ohne SD-WAN ermöglicht, erfuhr ich, dass fast alle Fortinet-Kunden die Fortinet-Lösungen für SD-WAN und SASE kombiniert einsetzen.

Alcatel-Lucent Enterprise als europäischer Hersteller

Interessant war für mich, von Alcatel-Lucent Enterprise (ALE) sowohl über die Zusammenarbeit mit Celona im Bereich Privates 5G-Netz als auch über die fortgesetzte Zusammenarbeit mit Nokia als weiterem europäischen Hersteller zu erfahren. In der Kürze der Zeit konnte jedoch nicht auf die schon sehr etablierten Core-Router von Nokia eingegangen werden. Das „E“ bei ALE heißt natürlich, dass Unternehmenslösungen von ALE selbst kommen, während Nokia eher als Ausrüster von Service-Providern (und teils auch Flughäfen) gesehen wird.

Das ALE-Betriebssystem AOS unterstützt mit MPLS, SPB und EVPN drei Plattformen für skalierbare und mandantenfähige Netze.

Ebenfalls interessant: der Industrieswitch OS6575-P12 mit Perpetual PoE (PoE geht weiter, während der Switch bootet).

Omnivista Cirrus ist die Bezeichnung für das Cloud-basierende Management von ALE.

Der Begriff AI Agent durfte auch hier nicht fehlen: der OmniVista AI Agent, der für Konfiguration oder Fehlersuche genutzt werden soll. Diverse Management-Funktionen wurden genannt, etwa Blockieren eines Endgeräts auf allen Access Points anhand von dessen MAC-Adresse, Fleet Supervision als Sicht auf Produkte und Service-Stände, Schwachstellen, Servicestände, Fälle von RTF (Return to Factory) etc.

Mit OmniVista Terra (OnPrem) auf Kubernetes-Basis lässt sich wie bei anderen Herstellern das Cloud-Management vermeiden.

LANCOM: Made in Germany

LANCOM hat natürlich als deutscher Hersteller für sich geworben. Seit nunmehr 7 Jahren ist das Unternehmen Bestandteil von R&S (100%-Tochter).

LANCOM ist ebenfalls in den Produktbereich Core Switches eingestiegen. Die Management-Cloud LMC ist eine Ergänzung für die Hardware, die jedoch auch weiterläuft, wenn die Cloud gerade nicht erreichbar ist.

Laut Hersteller werden zwei Drittel der installierten Managed-Device-Basis in der deutschen Public Cloud verwaltet. Wir kennen zum Beispiel den Cloud-Provider SysEleven (Teil der Secunet AG). Auch StackIT (Schwarz-Gruppe) ist ein bekannter Name.

LANCOM hat Enginesight als SIEM-Lösung genannt und ARP Guard als NAC-Lösung. Der Hersteller hat eine API-first-Strategie bei der Integration von Drittlösungen.

Für das Management wird Push gegenüber Pull bevorzugt – das Gerät initiiert die Verbindung zum Management, nicht umgekehrt.

ChatBots werden auch ohne LMC für Firewalls, Switches, Router und WiFi angeboten (die letzten beiden noch als Beta-Lösung).

An der OnPrem-KI arbeitet das Unternehmen noch.

Interesse an einer Neuauflage des Events?

Wenn Sie diesen Text gelesen und Interesse an einer Neuauflage des Events in 2026 haben, teilen Sie es ComConsult bitte unverbindlich mit. Wir werden die Veranstaltung für 2026 planen, wenn wir von einem signifikanten Interesse ausgehen.

Im Netzwerk Insider vor 20 Jahren: Zentralisierte Netzwerk-Sicherheit

von Dr. Markus Ermes

Vor 20 Jahren wurden im Netzwerk Insider das Thema Netzwerk-Sicherheit und die zur damaligen Zeit verfügbaren Werkzeuge und Management-Lösungen angesprochen. Wie war die Situation damals? Wie sieht es heute aus?

Die Situation vor 20 Jahren

Vor 20 Jahren wurde im Geleit des Netzwerk Insiders über die zunehmende Verfügbarkeit von Werkzeugen für die Netzwerk-Sicherheit berichtet. Dabei wurde die grundlegende Idee, Netzwerke mithilfe solcher Tools besser zu schützen, zwar als gut betrachtet, doch wurde auch auf die Hindernisse eingegangen, die mit der Einführung einer solchen Lösung einhergehen können. Dazu gehörten auf der einen Seite die zur damaligen Zeit noch sehr heterogen aufgebauten Lösungen aus verschiedenen Teilkomponenten. Diese waren weder optimal integriert noch in der Oberfläche ähnlich, was die Arbeit damit erheblich erschwerte. Auf der anderen Seite wurde auf viele organisatorische Herausforderungen eingegangen, insbesondere im Bereich der Zuständigkeiten. Hier waren Netzwerk, Clients und Server sehr streng getrennt und somit eine einfache Zusammenarbeit in vielen Fällen nicht möglich. Was hat sich hier getan?

Die Situation heute

Heute hat sich die Situation in einigen Bereichen verbessert, während in anderen leider nur wenig Veränderung zu erkennen ist. Durch die Verbreitung von RESTful APIs ist eine wesentlich bessere Integration verschiedener Werkzeuge möglich. Viele Unternehmen bleiben jedoch nach wie vor im Dunstkreis eines einzigen Herstellers. Dadurch entsteht inzwischen in vielen, wenn auch nicht in allen Fällen eine einheitlichere Oberfläche.

Bei den Verantwortlichkeiten hat sich nicht ganz so viel geändert. Immer noch sind strikt getrennte Abteilungen eher die Regel als die Ausnahme. Damit ergeben sich ähnliche Herausforderungen wie vor 20 Jahren. Trotzdem sieht man vermehrt, dass verschiedene Abteilungen konstruktiv zusammenarbeiten und gemeinsam den Mehrwert von zentralisierten Sicherheitslösungen (insbesondere Security Information and Event Management – SIEM) erkennen.

Die damals aufgeführten Beispiele für den Zugriff eines Clients auf ein Netzwerk sind dagegen auf technischer Ebene gelöst. Durch IEEE 802.1X (Netzwerkzugangskontrolle, NAC) ist die Zuordnung von Endgeräten zu Netzwerken mittlerweile kein Problem mehr. Auch die Überprüfung des Zustands ist mit Endpoint Detection and Response (EDR) möglich, wobei Betrieb und Komplexität hier nicht unterschätzt werden sollten – Netzwerkzugangskontrolle ist leider noch nicht so verbreitet, wie man es in der IT-Sicherheit gerne sehen würde!

Fazit

Es gibt gute und schlechte Nachrichten im Bereich der Netzwerk-Sicherheit. Die guten: Auf technischer Ebene hat sich viel getan. Die meisten technischen Herausforderungen sind heute lösbar. Die schlechte Nachricht: Organisatorisch ist bei vielen Unternehmen noch Luft nach oben.

Zum Geleit

Netzwerk-Sicherheit: Hype oder Nutzen?

Die großen Hersteller von Netzwerk-Komponenten überschlagen sich mit immer neuen Konzepten und Produkten zur Netzwerk-Sicherheit. Auf den ersten Blick wirken diese Angebote durchaus überzeugend, doch auf den zweiten und intensiveren Blick offenbaren sich einige massive Mängel sowohl in den Produkten als auch in den Konzepten:

- Zum Teil werden isolierte Tools wild unter einem Marketing-Namen gemischt. Es gibt weder einen Zusammenhang in der Bediensystematik, noch ein gemeinsames Konfigurationstool, noch überhaupt ein passendes Rahmenkonzept. Das gemeinsame Element ist der Name, allerdings ist diese Vorgehensweise gerade bei Management-Tools nicht neu (siehe nahezu alle großen Management-Plattformen)

- In fast allen Produkten wird implizit unterstellt, dass sich der Bereich Client-Sicherheit dem Netzwerk unterzuordnen hat. Netzwerk-basierte Lösungen entscheiden, wann ein Client als sicher anzusehen ist. In der Praxis scheitert diese Sichtweise schon an der Zuständigkeit für den Client, die nun einmal nicht in der Netzwerk-Abteilung liegt

- Visualisierungskonzepte skalieren zum Teil nicht. In Präsentationen wird an einfachen und kleinen Umgebungen gezeigt, wie ein Angreifer versucht, auf einen Server zuzugreifen. Dabei ist die Erkennungsmethode so ausgelegt, dass in der Praxis im Zweifelsfall Hunderte von Flows darzustellen wären, was nun einmal nicht geht

Netzwerk-Sicherheit ist ohne Frage ein Fortschritt! Aber jeder akzeptable und sinnvolle Lösungsansatz setzt ein geeignetes Konzept voraus, das einige Bedingungen erfüllen muss:

- Das Konzept zur Netzwerk-Sicherheit muss ohne Brüche in ein Gesamtkonzept zur IT-Sicherheit einbindbar sein, die Schnittstellen zwischen den verschiedenen Systembereichen müssen klar definiert und in der täglichen Praxis handhabbar sein

- Der zu wählende Lösungsansatz muss auch organisatorisch ins Unternehmen passen, er darf keine Zuständigkeiten voraussetzen, die es in der Praxis in vielen Fällen nicht gibt. In Summe wird

ein Sicherheitskonzept nur funktionieren, wenn für ein Unternehmen auch eine geeignete organisatorische Lösung gefunden wurde. Dazu ist mindestens ein Abteilungs-übergreifendes Element, im Idealfall eine Stabsstelle Sicherheit mit Weisungsbefugnis erforderlich. Ohne den organisatorischen Gesamtzusammenhang entstehen in den Abteilungen Insellösungen, die zum einen nicht alle Gefahrenbereiche abdecken und die vor allem an den Schnittstellen nicht kompatibel zueinander sind

- Der gesamte Bereich der Netzwerk-Sicherheit sollte unter einer zentralen Oberfläche mit einem leicht zu handhabenden Bedienprinzip konfiguriert werden können. Die einzelnen Module dürfen nicht wild zusammengewürfelt sein

- Die Umsetzung eines Konzepts zur Netzwerk-Sicherheit darf nicht zu einer verstärkten Abhängigkeit vom Komponenten-Hersteller führen. Es darf dabei nicht übersehen werden, dass die Hersteller mit dem Thema Netzwerksicherheit für sich zwei Kernziele verfolgen. Zum einen sollen bestehende Netzwerk-Komponenten durch neue abgelöst werden, zum anderen soll dabei eine möglichst langfristige Bindung entstehen

Betrachtet man die aktuellen Trends im Bereich Netzwerk- und System-Management, dann drängt sich auf der Konzeptebene sofort ein zentraler Bereich auf:

- Alle sinnvollen und modernen Management-Ansätze, dazu zählt auch der Bereich Netzwerk-Sicherheit, basieren auf einer herstellerneutralen und zentralen Configuration Management Data Base CMDB. Dementsprechend gilt:

  - Eine zentrale Datenbank mit allen vorhandenen Endgeräten und deren Identitäten muss vorausgesetzt werden. Alle Zugangserlaubnisse für Geräte basieren auf Einträgen in dieser zentralen Datenbank. Es werden keine Individualschnittstellen zwischen Einzeltools aufgebaut, alles orientiert sich an der zentralen CMDB

  - Eine zentrale Benutzerverwaltung mit allen im Unternehmen vorhandenen Benutzern und deren Rechten muss unterstellt werden. Authentifizierungen erfolgen immer gegen diese zentrale Benutzerverwaltung oder eine damit synchronisierte Teilverwaltung

Weiterhin ist die zentrale Frage, ob folgende Annahmen getroffen werden können:

- Es gibt im Unternehmen ein Konzept zur Client-Sicherheit mit Virenschutz und Personal Firewall (letzteres zum Verhindern des Netzzugangs von nicht autorisierten Applikationen schon von der Client-Seite aus)

- Es gibt im Unternehmen ein Konzept zur Zugangssicherung auf zentrale Daten- und Applikations-Server

Können diese Annahmen getroffen werden, dann stellt sich die Frage, welcher Mehrwert durch Netzwerk-Sicherheit entsteht. Im Endeffekt kann man dies unterteilen in:

- Ein zulässiger und korrekt konfigurierter Client wurde durch einen Angriff übernommen und stellt nun selber eine Bedrohung dar. Er hat einen aktuellen Virenschutz und eine aktive Personal Firewall. Sollte der Angriff erfolgreich an der Personal Firewall (durch Nutzung einer zugelassenen Applikation) oder dem Mail-Virenschutz (durch keine geeignete Signatur im Virenscanner) vorbei kommen, dann stellt er natürlich eine Bedrohung dar. In der Praxis kann dieser Client nur durch ein abnormales Verhalten im Netzwerk identifiziert werden. Dies fällt dann in den Bereich Intrusion Detection/Prevention. Die damit verbundene Problematik der sichere-

Sonderveranstaltung: Server der Zukunft 25.02.2026 online

Neue Sonderveranstaltung

Die Sonderveranstaltung „Server der Zukunft“ wird von der ComConsult Akademie mit hervorragenden Referenten besetzt, um die Sicht führender Hersteller mit der Perspektive von unabhängigen Experten zu kombinieren. Genau diese Kombination ist erforderlich, um den Server- und RZ-Verantwortlichen die Informationen zu bieten, die sie für ihre Vorhaben der nächsten Jahre benötigen.

Warum Sie diese Schulung besuchen sollten:

Der KI-Boom zeigt deutlich, was RZ-Designer bereits seit über einem Jahrzehnt erkennen: RZ-Infrastrukturen für Energieversorgung und Kühlung müssen mit dem rasanten Innovationstempo im Server-Bereich Schritt halten. Dabei ist die Kühlleistung der bestimmende Faktor. Hersteller wie Nvidia bringen zunehmend leistungshungrige Chips auf den Markt, die wenige Monate später in Produkten führender Server-Anbieter eingesetzt werden. Rechenzentren müssen diese Produkte aufnehmen, ihren steigenden Energiebedarf abdecken und für einen stabilen Server-Betrieb sorgen. Dazu gehört, die Server zu kühlen.

Die reine Luftzirkulation reicht in Rechenzentren für Server mit höchster Leistungsdichte nicht mehr aus. Immer mehr Rechenzentren werden daher mit Technologien ausgestattet, die sich bereits in Supercomputer-Rechenzentren bewährt haben. Es genügt nicht mehr, Kühlflüssigkeiten nur in der zentralen Kälteerzeugung einzusetzen. Die Flüssigkeitskühlung durchdringt ganze Rechenzentren und muss zunehmend Server versorgen, die direkt in den RZ-Kühlkreislauf eingebunden sind.

Neben den Herausforderungen für Energieeffizienz und Kühlung sind für die Sever der Zukunft sämtliche Kriterien relevant, die das Open Compute Project (OCP) definiert hat, darunter die Orientierung an herstellerübergreifenden Standards und Interoperabilität. Steigende Sicherheitsanforderungen wirken sich ebenfalls auf das Server-Design aus: Alle kryptografischen Verfahren der Zukunft, auch für die Integrität von Firmware, müssen Quantumsafe sein. Nicht zu vergessen ist der Anschluss der Server an RZ-Netze, die an der Schwelle zur Terabit-Ära angelangt sind. Antworten auf diese Herausforderungen stehen auf der Agenda der Sonderveranstaltung Server der Zukunft.

Folgende Vorträge erwarten Sie:

Entwicklung, Trends und Herausforderungen der Server- und RZ-Kühlung
Dr. Markus Ermes, Dr. Philipp Rüßmann
Competence Center Cloud und Data Center, ComConsult GmbH

Das Open Compute Project – Hyperscale Innovation for All
Dr. Markus Ermes, Dr. Philipp Rüßmann
Competence Center Cloud und Data Center, ComConsult GmbH

Serverarchitekturen für KI und klassische Workloads: vom Allzweckgerät für Außenstandorte zum Rack Scale-Design
Dr. Stefan Muthmann, AI-Solutions-Teams bei Dell Technologies

Zukünftige Serveranforderungen, heute verfügbar
Florian Bettges Hybrid Cloud Category Manager, HPE

Weitere Inhalte folgen in Kürze

Schulungsdauer: 6 Stunden
Preis: 1.090,- €

Ihr Moderator
Dr. Markus Ermes hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau, Nutzung und Betrieb von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage, Servern, Virtualisierung und cloudbasierten Diensten sowie deren Absicherung liegen.

Lizenzmodelle der Netzwerkausrüster

von Felix Gilleßen und Michael Schneiders

Das Thema Lizenzen hat nicht erst seit der umfassenden Änderung des Modells bei VMware an Bedeutung gewonnen. Ob im operativen Tagesgeschäft, in der strategischen Planung oder in der Administration – für alle IT-Verantwortlichen spielt die Lizenzierung eine wichtige Rolle. Wir beobachten einen Wandel von klassischen, dauerhaften Modellen hin zu Abos mit wiederkehrenden Zahlungen. “Subscriptions” sind auch außerhalb der IT-Welt allgegenwärtig.

Doch was ist eine Lizenz genau? Sie ist eine rechtsgültige Erlaubnis, die einem Nutzer (Lizenznehmer) vom Inhaber eines Schutzrechts (Lizenzgeber) erteilt wird, um dessen immateriellen Rechte innerhalb definierter Grenzen wirtschaftlich zu nutzen. Diese Nutzungsrechte sind im entsprechenden Vertrag geregelt, der unter anderem Umfang, Laufzeit, Entgelt und Vertragsstrafen regelt. Der Lizenznehmer darf die Rechte des Lizenzgebers nutzen, ohne Eigentümer zu sein. Als Gegenleistung werden in den meisten Fällen Gebühren fällig.

Dabei beschränkt sich die Thematik nicht auf den Netzwerk-Bereich. Nahezu jede Software ist an Lizenzbedingungen geknüpft – auch dann, wenn sie kostenlos genutzt oder als Open-Source-Projekt angeboten wird. Bezogen auf die Betriebssoftware der Netzwerkkomponenten heißt das, dass der Hersteller, neben dem Verkauf der Hardware, eine (kostenpflichtige) Nutzung der Software regelt.

Dieser Artikel fokussiert sich auf die praktische Seite der Lizenzierung im Netzwerk-Umfeld und klammert eine tiefe rechtliche Analyse bewusst aus. Stattdessen beleuchten wir praxisrelevante Aspekte wie unterschiedliche Typen, Laufzeiten, das Management und typische Fallstricke bei Beschaffung und Umgang mit Lizenzen. Ein für die Betriebskosten entscheidender Punkt ist hierbei die oft übersehene Trennung zwischen Funktion, Support und Updates. Hier wurde lange Zeit zwischen dauerhaften und laufzeitbasierten Lizenzen (Subscriptions) unterschieden. Doch diese Abgrenzung wird zunehmend aufgeweicht. Es gibt immer weniger Netzkomponenten, für die keine Lizenz erworben werden muss oder für die keine Subscriptions abgeschlossen werden können bzw. müssen. Das Modell und die benötigten Lizenzen haben eine unmittelbare Auswirkung auf die Auswahl der infrage kommenden Komponenten und die Betriebskosten über die Lebenszeit der Hardware. Eine unvollständige Bestellung, Unwissen über Folgekosten nach der Erstlaufzeit sowie umständliches und zeitintensives Handling sind typische Herausforderungen im Betriebsalltag.

Basierend auf den Erfahrungen aus zahlreichen Projekten der vergangenen Jahre beobachten wir, dass der Anteil an Subscriptions weiter zunimmt. Ein Grund für diese Zunahme ist sicherlich, dass die Hersteller von dem kontinuierlichen Cashflow profitieren und die Kunden über einen längeren Zeitraum an sich binden als bei einem Einmal-Kauf. Damit vergrößert sich auch der durch laufende Kosten entstehende Anteil an den Gesamtkosten eines IT-Systems.

Am Beispiel eines Campus-Access-Switches eines europäischen Herstellers wird das schnell deutlich: Bezogen auf die Gesamtkosten beträgt der Anteil der Management-Lizenzen nach einer Laufzeit von 8 Jahren ca. 30%. Dabei bietet der Hersteller hinsichtlich des Managements gute Alternativen, mit deren Hilfe man, wenn auch verbunden mit einem gewissen Komfort-Verlust, auf das Cloud-Management verzichten könnte.

An einem anderen Beispiel wird der Unterschied zwischen den Kosten für die Hardware und die für den Betrieb notwendigen Lizenzen noch deutlicher: Bei einem renommierten Firewall-Hersteller beträgt der Anschaffungspreis für die Firewall-Hardware 6.200,00 €. Die Kosten für die notwendigen Features einschließlich einer Hardware-Wartung für 5 Jahre belaufen sich auf ca. 26.300 €. Damit betragen die Hardwarekosten gerade mal 20% der Gesamtkosten. Zudem kann die Firewall ohne eine Verlängerung nach Ablauf der 5 Jahre kaum sinnvoll weiterbetrieben werden.

Arten von Lizenzen

Im Folgenden gehen wir auf die verschiedenen und verbreiteten Arten von Lizenzen im Netzwerk-Bereich ein. Typischerweise werden in der Praxis mehrere Arten miteinander kombiniert, sodass für ein Produkt oft mehrere erforderlich sind. Zudem kann es vorkommen, dass nicht alle davon für ein Produkt relevant sind bzw. dass sie bereits im Hardwarepreis oder in anderen Vereinbarungen enthalten sind.

Feature- und Funktions-Lizenzen

Klassische Feature-Lizenzen sind häufig anzutreffen. Hier werden bestimmte Funktionalitäten der Komponenten an den Erwerb einer entsprechenden Lizenz gekoppelt. Eine Grund-Funktionalität ist durch eine Basis-Lizenz abgedeckt, die beim Kauf bereits enthalten ist oder zwingend gekauft werden muss. Bei einem Switch sind beispielsweise grundlegende Layer-2-Funktionen enthalten, was für viele Anwendungsfälle bereits ausreicht. Erweiterte Funktionen, wie Routing-Fähigkeit oder erweiterte Analyse-Funktionen, müssen hingegen über eine zusätzliche Funktions-Lizenz freigeschaltet werden.

Ein weiterer Ansatz ist, den Datendurchsatz von Geräten anhand verschiedener Stufen zu regulieren – ein typischer Fallstrick bei der Bestellung von Routing-Hardware. Auch wenn die Ausstattung einer Komponente einen hohen Durchsatz vermuten lässt (z.B. durch SFP28-Interfaces für 25 Gbit/s), bedeutet das nicht, dass dieser ohne eine passende Kapazität erreicht wird. Hier ist die Aufteilung in Stufen noch klarer abgegrenzt. Oft ist im Basisumfang nur ein geringer Durchsatz freigeschaltet, der durch höhere Stufen erweitert werden muss. Diese Lizenz kommt dann zusätzlich zu den ohnehin erforderlichen Funktionen für Protokolle wie BGP oder IPsec hinzu.

Da die Auswahl einzelner Lizenzen sehr anspruchsvoll sein kann, bieten Hersteller nicht selten gebündelte Pakete an. Dabei werden die für einen Anwendungsfall benötigte Einzellizenzen zusammengefasst, was die Bestellung vereinfacht. Diese Pakete folgen meist einer „Tiering-Logik“ mit Stufen wie „Basic“ oder „Advanced“, wobei höhere Stufen die Funktionen der darunterliegenden inkludieren. Eine Mischung verschiedener Level auf einem Gerät ist in der Regel nicht möglich. Der Vorteil liegt in der Einfachheit. Der Nachteil: Benötigen Sie nur eine einzige Funktion aus einem teureren Paket, müssen Sie oft die gesamte höhere Stufe erwerben und bezahlen für viele Features, die ungenutzt bleiben. Dies reduziert die Flexibilität und kann die Kosten ohne realen Mehrwert erhöhen. Dieser Umstand ist beabsichtigt, da Hersteller ein Interesse daran haben, die teureren Pakete zu verkaufen und die notwendigen Informationen in unübersichtlichen Dokumenten “verstecken”. Aus Sicht des Technikers führt dies in der Praxis dazu, dass man „zur Sicherheit“ eine zu große Lizenz bestellt, um nachträgliche und aufwändige Nachbestellungen sowie unangenehme Rückfragen zu vermeiden.

Positiv zu bewerten und von den jeweiligen Herstellern entsprechend beworben sind Komponenten, bei denen alle verfügbaren Leistungsmerkmale im Grundpreis enthalten sind. Auf diese Weise entfällt zumindest die Auswahl der passenden Feature-Lizenz.

Management-Lizenzen

Während sich Funktions-Lizenzen auf die Funktion des Gerätes selbst beziehen, ermöglichen Management-Lizenzen die zentrale Verwaltung von Geräten über eine herstellerspezifische Cloud- oder On-Prem-Plattform. Typ und Kosten hängen oft direkt vom Gerät und dessen zugewiesener Funktion ab. So ist eine Management-Lizenz für einen Switch mit Basisfunktion in der Regel günstiger als für einen mit stärkerer Hardware und erweitertem Funktionsumfang.

Auch bei Management-Lizenzen sind verschiedene Stufen verbreitet. Während eine Basis-Stufe die grundlegende Konfiguration und Überwachung abdeckt, schalten höhere Tiers erweiterte Funktionen wie tiefgehende Analysen, KI-gestützte Fehlerbehebung (Assurance) oder komplexe Automatisierungsfunktionen frei.

Lizenzen für Wartung und Support

Wartungs- und Support-Lizenzen sichern den Zugang zu Software-Updates und Herstellerunterstützung über die gesamte Produktlebensdauer der Komponenten und gewährleisten damit Stabilität und Sicherheit im Betrieb.

Die Wartungskomponente einer Lizenz sichert primär die laufende Softwarepflege. Für den lizenzierten Geräte- oder Softwarebestand stehen Software-Downloads, Dokumentationen, Versionsinformationen und „Release Notes“ bereit. Zwar stellen Hersteller besonders kritische Sicherheitsupdates auch ohne Wartungs-Lizenz zur Verfügung, doch sind für einen verlässlichen, stabilen Betrieb essenzielle, regelmäßige Bugfixes, Kompatibilitätsanpassungen und Qualitätsverbesserungen typischerweise an die Wartung gebunden.

Wartungs-Lizenzen werden oft mit einer Support-Lizenz gekoppelt. Support-Lizenzen gewähren je nach Stufe oder Service-Level den Zugriff auf Herstellersupport und ermöglichen den Austausch defekter Hardware – über eine gegebenenfalls eingeräumte Basis-Garantie hinaus. Häufig sind konkrete Reaktions- und Lösungszeiten sowie die Verfügbarkeit von Austausch-Hardware vorgegeben. Erst mit einer Support-Lizenz kann auf das Ticket-System des Herstellers oder Partners zugegriffen werden und Unterstützung bei Fehlern, Konfigurations- oder Hardware-Problemen angefragt werden. Insbesondere bei zeitkritischen Störungen oder einem vermuteten Hardware-Defekt kann der Herstellersupport Ausfallzeiten deutlich reduzieren und damit Produktivitätsverluste minimieren. Durch schnellen Expertenzugang, Diagnose und Ersatzteilmanagement verkürzen sich Reaktions- und Wiederherstellungszeiten spürbar. Eine entsprechende Bereitschaft ist natürlich nicht preisgünstig, sodass gerade im Bereich Support genau überlegt sein muss, welche Geräte mit welchem Level ausgestattet werden, oder wo Ausfallzeiten im Zweifelsfall verkraftbar sind.

Grundsätzlich gilt es zu klären, wie groß die Auswirkungen einer Nicht-Verfügbarkeit des jeweiligen Systems ist und wie viele Bereiche und Mitarbeiter betroffen wären. Hierzu müssten sowohl unmittelbare Produktivitätsverluste als auch Auswirkungen auf Kunden, Compliance und Reputation geprüft werden. Der Herstellersupport ist dabei nur ein Baustein einer belastbaren und re-

silienten Infrastruktur. Weitere Maßnahmen wie Redundanz auf Hardware-Ebene, Cold- bzw. Hot-Standby, protokollbasierte Redundanz und passende organisatorische Maßnahmen gilt es ebenfalls zu berücksichtigen. Entscheidend ist das abgestimmte Zusammenspiel dieser Elemente.

Die genauen Leistungen werden durch SLAs (Service-Level-Agreements) definiert. Typische SLAs legen Reaktionszeiten des Herstellersupports und die Dauer für die Bereitstellung von Ersatzteilen fest. Den Einstieg bietet hier oft der „8 x 5 x Next Business Day“-Service.

- 8 x 5: Zeitraum zur Unterstützung Montag-Freitag (an 5 Tagen/Woche) in einem Zeitfenster von 8 Stunden, typischerweise 9-17 Uhr. Anfragen, die außerhalb dieses Zeitraums eingehen, werden erst am nächsten Tag bearbeitet und getrackt.
- NBD: Ein Service vor Ort oder ein Ersatzteil steht am nächsten Geschäftstag („Next Business Day“) zur Verfügung, sofern die Anfrage und Bearbeitung im 8x5-Zeitfenster erfolgt ist.

Ausgehend von diesem Zeitfenster ist eine Erweiterung der Service-Zeiten möglich. Typische Kombinationen sind 8x7xNBD, oder für kritische Komponenten 24x7x4, an denen eine Ersatzlieferung innerhalb von 4 Stunden nach Klassifizierung erfolgt. Hierbei sollte beachtet werden, dass nicht alle Hersteller alle Service-Level anbieten. Insbesondere 24x7x4 setzt eine Ersatzteilvorhaltung und entsprechende Logistik voraus.

Die benötigten Service-Level sollten schon bei der Evaluation möglicher Hersteller in Betracht gezogen werden. Gleichzeitig muss beachtet werden, dass auch interne Prozesse zu den ausgewählten SLAs passen. Kann der Mitarbeiter dem Herstellersupport auch die benötigten Informationen außerhalb der Kernarbeitszeiten zur Verfügung stellen? Wer tauscht das defekte Netzteil an einem Samstag vor Ort aus? Wie ist die Zutrittskontrolle außerhalb der Geschäftszeiten geregelt?

Für diejenigen, die mit weniger auskommen, verbinden viele Netzwerkausrüster eine Limited Lifetime Warranty (LLW) mit ihren Netzkomponenten. Die bereits im Grundpreis enthaltene LLW bietet herstellerabhängig eine Garantieverlängerung bis zum Erreichen des Status End of Life, einschließlich Hardware-Austausch bzw. Reparatur und Versorgung mit Sicherheitspatches. Darüber hinaus versprechen die Hersteller die kostenlose Bereitstellung von Funktions-Updates für zwei Jahre nach dem Erreichen des Status End of Sale. Natürlich gibt es mit einer LLW keine garantierte Lieferzeit, die an NBD oder 24x7x4 herankommt. Es empfiehlt sich dann zusätzlich eine Ersatzteilebevorratung vor Ort.

Bündelung verschiedener Lizenz-Typen

Die unterschiedlichen Lizenz-Typen können separat und in unterschiedlichen Stufen (“Lizenz-Tier”) erworben werden. Die richtige Zusammensetzung des Bündels ist teilweise aufwändig und erfordert Fachwissen über die jeweilige Bündelung.

Um dem entgegenzuwirken, verbinden Hersteller die klassischen Funktions-, Management- und Support-Lizenzen zu einem "All-in-One"-Paket, was die Grenzen zwischen den verschiedenen Typen aufhebt. Hierbei gilt es jedoch wieder zu unterscheiden:

- Freiwillige Bündelung: Hier werden typische Kombinationen von Einzellizenzen zusammengefasst und bieten oft einen Preisvorteil gegenüber dem Einzelkauf. Der Hersteller bündelt sinnvolle Funktionen in einem Gesamtpaket.
- Verpflichtende Bündel (meist Subscriptions): Der klare Trend geht jedoch zu untrennbaren (meist laufzeitbasierten) Lizenzen hin. Hier sind keine Einzellizenzen erhältlich, nur noch das verpflichtende “Gesamtpaket", wenn auch häufig in verschiedenen Stufen (z.B. Basic und Advanced).

Open-Source-Lizenzen

Open-Source-Software spielt in der Netzwerkwelt eine Doppelrolle: Einerseits ist sie eine für den Nutzer unsichtbare, aber essenzielle Grundlage vieler kommerzieller Produkte. Andererseits ist sie als eigenständige Alternative zu den Lösungen der großen Hersteller möglich.

Open-Source als Komponente in kommerziellen Produkten

Auch wenn die Verbreitung als eigenständige Lösung im Endkundenbereich eher ein Nischendasein führt, nutzen alle großen Hersteller mittlerweile Open-Source-Software in ihren Produkten. Die verschiedenen Lizenz-Arten von quelloffener Software wäre schon genug Stoff für einen weiteren Artikel. Häufig genutzte Pakete wie OpenSSL oder iptables unterliegen entweder strengen Copyleft-Lizenzen oder permissiven Lizenzen, die geringere Auflagen stellen. Die GNU Public License GPL Version 2 verpflichtet die Hersteller, die den Linux-Kernel in ihrer Firmware nutzen, zu Transparenz. Quellcode und Lizenzinformationen müssen in sogenannten „Third-Party-Notices“ offengelegt werden. Cisco bietet hierfür beispielsweise eine öffentlich zugängliche Dokumentation an, in der die verwendeten Open-Source-Projekte pro Produkt und Firmware-Version aufgelistet sind [1].

Open Source als Alternative zu kommerziellen Lösungen

Projekte wie die Firewalls pfSense und OPNsense oder die Routing-Distribution VyOS haben im Unternehmensumfeld durchaus ihre Berechtigung. Richtig konfiguriert und auf passender Hardware eingesetzt können sie mit Grundfunktionen kommerzieller Lösungen mithalten und bieten eine hohe Flexibilität im Einsatz. Der professionelle Einsatz setzt jedoch ein tiefes Fachwissen über die jeweilige Lösung voraus. Nicht selten erfordert die Fehlersuche auch Kenntnisse aus anderen Bereichen, zum Beispiel wenn innerhalb des Systems Inkompatibilitäten auftreten.

Für die meisten Projekte gibt es weder garantierten Herstellersupport sowie definierten Produktlebenszyklus noch eine verbindliche Zusage für zeitnahe Sicherheitsupdates. Bei Problemen oder Ausfällen fehlt ein zentraler Ansprechpartner, und die Wartung hängt meist vom freiwilligen Engagement der Community oder einzelner Entwickler ab.

Diese Einschränkung gilt jedoch nicht für alle Open-Source-Projekte. Für viele erfolgreiche Projekte haben sich spezialisierte Unternehmen gegründet, die Support, Wartung und sogar darauf abgestimmte Hardware anbieten. Ein prominentes Beispiel ist die Firma Netgate, die mit pfSense Plus eine kommerziell unterstützte Software-Version und mit ihren Appliances eine passende Hardware-Plattform vertreibt.

Die entfallenden Lizenzkosten durch den Einsatz von Open-Sour-

ce-Projekten sind erst einmal verlockend. Das ist aber zu kurz gedacht. Die Kosten verlagern sich vom Kaufpreis auf interne Ressourcen und stellen ein potenzielles Betriebsrisiko da. Bevor Sie eine Open-Source-Lösung in einer produktiven Umgebung einsetzen, sind die folgenden Fragen zu klären:

- Expertise: Verfügt das Team über das nötige Fachwissen, um die Lösung nicht nur zu installieren, sondern auch sicher zu betreiben und im Fehlerfall systematisch zu entstören?
- Kritikalität und Risiko: Wo und für welchen Zweck wird die Lösung eingesetzt? Welche geschäftlichen Auswirkungen hat ein Ausfall des Systems, und kann das Risiko des möglicherweise fehlenden Herstellersupports intern getragen werden?
- Support: Gibt es eine kommerzielle Variante mit Support oder ein Unternehmen, das Unterstützung bei Inbetriebnahme und Entstörung anbietet?
- Kontinuität: Wie kann die Lösung ersetzt werden, wenn sie nicht weiter gepflegt wird?

Die Entscheidung für Open Source sollte nie als reine Sparmaßnahme gedacht, sondern immer eine bewusste Abwägung sein. Es ist nicht zu unterschätzen, dass die Verwendung von Open Source in vielen Fällen einen guten Ausweg aus einem Hersteller-Ökosystem eröffnet.

Nutzung von Lizenzen

Die Nutzung wird in den Nutzungsbedingungen geregelt. Mit Erwerb und Nutzung einer Lizenz stimmt der End-Nutzer den Vertragsbedingungen zu. Die genauen Bedingungen finden sich meist im Endbenutzer-Lizenzvertrag (End User License Agreement, EULA) oder in speziellen Geschäftsbedingungen, also im “Kleingedruckten”.

Typischerweise sind Lizenzen gerätegebunden. Für jedes Gerät wird eine Lizenz (oder mehrere) benötigt, die dann für das Gerät reserviert ist. Um ein zweites Gerät zu lizenzieren, ist eine weitere erforderlich. Hierbei sind die Lizenzen nicht portabel. Wird für das erste Gerät z. B. ein Feature nicht mehr benötigt und damit auch eine Lizenz, bleibt diese trotzdem dem Gerät zugeordnet und die Funktionen freigeschaltet.

Genau diese starre Bindung stellt einen der größten Nachteile dar, da sie oft nicht zu den dynamischen Anforderungen moderner Infrastrukturen passt. Als Reaktion drauf etablieren sich zunehmend flexible Modelle.

Flexible Verwaltung durch Lizenz-Pooling

Ein Beispiel hierfür ist das Pooling. Die Lizenzen sind nicht mehr fest an Hardware gebunden, sondern werden in einem zentralen durch den Hersteller bereitgestellten System verwaltet. Das System erlaubt es, weitere Unterteilungen zu erstellen (virtuelle Accounts), um eine Organisationsstruktur (z. B. für verschiedene Abteilungen, Kunden oder Standorte) abzubilden. Aus diesem zentralen Pool können Administratoren die Lizenzen dann flexibel einzelnen Geräten zuweisen und die Nutzung aller verwalteten Geräte an einer zentralen Stelle einsehen. Die Zuweisung ist nicht endgültig und kann geändert werden.

Wird auf einem Gerät eine Lizenz nicht mehr benötigt, z. B. durch veränderte Anforderungen, kann diese vom Gerät entfernt und auf einem anderen wieder zur Verfügung gestellt werden.

Floating-Lizenzen

Floating-Lizenzen sind im Netzwerk-Bereich eher selten vertreten, kommen aber zum Beispiel bei VPN-Systemen zum Einsatz. Hier sind sie auch als Concurrent-User-Lizenzen bekannt. Das Prinzip ist einfach: Statt für jeden potenziellen Nutzer eine Lizenz zu kaufen, wird nur die maximale Anzahl gleichzeitiger Nutzer lizenziert. Ein Pool von Lizenzen steht allen Nutzern zur Verfügung. Bei Verbindung wird eine Lizenz aus dem Pool verwendet und bis zum Beenden der Verbindung belegt.

Der große Vorteil hierbei ist, dass eine Überbuchung der Lizenzen erfolgen kann. Beim Beispiel VPN-System ist es unwahrscheinlich, dass alle berechtigten Nutzer das System gleichzeitig nutzen. Dies führt zu erheblichen Kosteneinsparungen, da nur für die tatsächliche, gleichzeitige Nutzung bezahlt wird und nicht für jeden einzelnen potenziellen Anwender.

Laufzeit von Lizenzen

Lizenzen weisen unterschiedliche Laufzeiten auf. Einfach gesagt lässt sich zwischen permanent und laufzeitbasiert unterscheiden.

Permanente Lizenzen (perpetual licences) werden, wie der Name bereits sagt, nur einmal zusammen mit der Netzkomponente erworben. Im Wesentlichen waren und sind die zuvor beschriebenen Feature-Lizenzen häufig permanente Lizenzen. Ein prominentes Beispiel sind die beiden Lizenz-Stufen Enhanced Mulitlayer Image und Standard Multilayer Image bei Cisco-Switches älterer Bauart, etwa bei der 3550-Familie. Unter gewissen Umständen konnte die Lizenz-Stufe durch den Erwerb einer passenden Lizenz von “Standard” auf “Enhanced” angehoben werden. Interessanterweise taucht in den alten Datenblättern der 3550-Serie das Wort “License” zunächst überhaupt nicht auf. Erst mit der Nachfolge-Serie aus dem Jahr 2014 wurde dem Thema “Licensing” ein extra Kapitel gewidmet. Auch Management-Lizenzen waren in der Vergangenheit oftmals permanent. Sie mussten einmalig zusammen mit der Netzwerkmanagement-Software erworben werden und standen für eine festgelegte Anzahl von Geräten zur Verfügung, etwa für das Management von 50, 100 oder 500 Geräten, und eben permanent.

Die Nutzung laufzeitbasierter Lizenzen ist zeitlich begrenzt, weshalb sie regelmäßig erneuert werden müssen. Meist werden solche Lizenzen für unterschiedliche Laufzeiten angeboten, beispielsweise für 1, 3, 5 und 7 Jahre. Diese Art der Lizensierung verbreitete sich insbesondere mit dem Aufkommen von Cloud-Management-Systemen zunehmend. Hersteller von Netzwerk-Komponenten bewarben diese Modelle oftmals unter dem Begriff “pay as you grow”: Für jede Komponente wurde eine Lizenz erworben, wodurch der vermeintliche Nachteil entfiel, Bündel für eine feste Anzahl an Geräten gleich mit dem Erwerb einer Management-Software anschaffen zu müssen.

Befindet man sich noch in einer Entscheidungsphase und ist sich unsicher, ob eine neue Komponente tatsächlich beschafft werden soll, bieten viele Hersteller kostenlose Test-Lizenzen an. Mit deren Hilfe können die mit der Lizenz verbundenen Funktionalitäten für eine gewisse Zeit, beispielsweise für 90 Tage, genutzt werden. Diese Lizenzen sind besonders nützlich, wenn eine IT-Komponente für die Durchführung von Tests virtualisiert werden kann, da auf diese Weise auch die Beschaffung einer Testhardware entfällt. Beispielhaft seien hier Firewall-Hersteller genannt,

die ihre Produkte als virtuelle Maschinen zum Download und anschließender Installation auf einem Virtualisierungs-Host bereitstellen. Um zu verhindern, dass diese Evaluierungs-Lizenzen für einen Produktivbetrieb genutzt werden, schränken Hersteller teilweise den Leistungsumfang oder die Leistungsfähigkeit der Komponenten ein, etwa durch Begrenzung des Durchsatzes oder der Anzahl an Filterregeln.

In diesem Zusammenhang sind auch sogenannte Inbetriebnahme-Lizenzen positiv zu erwähnen, idealerweise ohne zusätzliche Kosten. Sie haben in der Regel eine eingeschränkte Laufzeit, die für den Zeitraum der Inbetriebnahme, etwa im Rahmen eines Rollouts, vollkommen ausreichend sind. Auf diese Weise fallen keine Kosten an, solange die Komponenten noch nicht eingebaut sind und möglicherweise nur im Lager auf ihren Einsatz warten.

Spätestens nach der Inbetriebnahme und Integration der Komponenten beginnt die Laufzeit der Management-Lizenz und somit auch die ständige Überprüfung der Restlaufzeiten. Kompliziert wird es, wenn nach einiger Zeit Komponenten – beispielsweise für eine Erweiterung des Netzes – nachgeordert und lizensiert werden müssen. Besteht dann nicht die Möglichkeit, Lizenzen mit granular abgestimmten Laufzeiten zu erwerben, kann es passieren, dass beim Erreichen des Lebensendes der Komponenten nicht alle Lizenzen am selben Tag oder zumindest im selben Monat enden. Um dieses Problem zu adressieren, bieten Hersteller häufig die sogenannte Co-Termination an. Dabei werden alle Lizenzen in einem gemeinsamen Pool verwaltet, und es wird ein gemeinsames Ablaufdatum berechnet. Unterschiedliche Stufen, z. B. basic und advanced, fließen entsprechend gewichtet in die Berechnung ein. Werden Geräte außer Betrieb genommen oder hinzugefügt, berechnet sich automatisch ein neues Enddatum. Zu beachten ist, dass Verfahren zur Co-Termination bei jedem Hersteller unterschiedlich und nur schwer miteinander vergleichbar sind.

Bei unseren Recherchen sind wir bei einem großen Netzwerkausrüster auf ein interessantes punktbasiertes Modell gestoßen: Je nach Modell, z. B. Layer-2-Switch oder Access Point, und einer Feature-abhängigen Stufe konsumieren die Komponenten unterschiedlich viele Lizenzpunkte pro Tag. Einmal täglich wird dann der Verbrauch an Punkten berechnet und im Management-System dargestellt. Sobald der Vorrat an diesen Punkten aufgebraucht ist, beginnt ein dreimonatiger Kulanzzeitraum (Grace Period), innerhalb derer Punkte nachgeordert werden können. Im Gegensatz zu anderen Herstellern entstehen somit nur Kosten für Komponenten, die im Management-System verwaltet werden.

Was eigentlich selbstverständlich sein sollte, sieht leider in der Realität oft anders: Die Laufzeit beginnt nicht mit der Aufnahme der Komponente in das Management-System, sondern mit dem Lieferdatum gemäß Lieferschein.

Lizenz-Management

Mit dem Erwerb laufzeitbasierter Lizenzen eng verbunden ist ein aufwändiges Management. Bei vielen unterschiedlichen Komponenten, die in einem Unternehmen betrieben werden müssen, kann die Verwaltung von Lizenzen einen erheblichen Arbeitsaufwand mit sich bringen. In der Regel bleibt diese Aufgabe beim Endkunden oder beim beauftragten Dienstleister hängen. Diese Aufwände sollten beim Erwerb von IT-Komponenten auf jeden Fall in eine Gesamtkostenrechnung einbezogen werden. Die Arbeit beginnt meist mit der Aktivierung einer Feature-Lizenz auf den Komponenten selbst. Je nach Hersteller ist dies mehr oder weniger aufwändig und erfordert beispielsweise eine Aktivierung über die Command Line der Komponente. Im schlimmsten Fall ist zudem eine Online-Aktivierung erforderlich, d.h. die Netzkomponente muss über das Internet mit einem Lizensierungssystem beim Hersteller kommunizieren können, oder es muss ein Verwaltungsdienst beim Kunden installiert werden, der für diese Funktion als Proxy bzw. Rendezvous-Point fungiert. Für den Betrieb einer IT-Komponente über ein (Cloud-) Management-System kann die feste Verbindung der Seriennummer des Geräts mit einer Management-Lizenz erforderlich sein. Ein zusätzliches Eingreifen wird nötig, wenn eine Komponente aufgrund eines Hardware-Defekts ersetzt werden muss, da die Lizenz in diesem Fall auf die Ersatzkomponente übertragen werden muss.

Bei der IT-Beschaffung positiv zu bewerten sind sogenannte Trust-License-Modelle. Hierbei entfällt das Einspielen von Schlüsseln, die Zuordnung zu einer Komponente und die Herstellung einer Internetverbindung zum Server des Herstellers. Dieser behält ohnehin den Überblick darüber, wie viele Lizenzen und Komponenten erworben wurden.

Lizenz-Durchsetzung (Enforcement)

Mit dem Zwang zur Aktivierung ist in der Regel auch ein License Enforcement eng verbunden. Wird keine Feature-Lizenz oder Management-Lizenz für eine Komponente aktiviert oder läuft der Nutzungszeitraum ab, stehen die verbundenen Funktionen entweder sofort oder nach einer gewissen Zeit – der sogenannten Gnadenfrist oder Grace Period – nicht mehr zur Verfügung. Die Grace Period beträgt herstellerabhängig zwischen 30 und 60 Tagen, sodass noch ausreichend Zeit bleibt, eine neue Lizenz zu erwerben bzw. zu aktivieren.

Fallstricke in der Praxis

In unserer täglichen Arbeit mit Kunden, sei es bei der Auswahl neuer Komponenten oder im laufenden Betrieb, begegnen uns die unterschiedlichsten Modelle der Hersteller. Aus dieser Erfahrung haben wir die häufigsten und zugleich teuersten Fallstricke identifiziert.

1. **Versteckte Gesamtkosten: Die Subcsription-Falle**
   Oftmals werden die Gesamtkosten der Lösung (Total Cost of Ownership, TCO) unterschätzt. Der Hardware-Preis scheint recht günstig und passt damit ins Budget. Die wahren Kosten entfalten sich über den Lebenszyklus durch laufzeitbasierte Lizenzen für Features, Management und Support. Ein auf den ersten Blick günstiges Angebot kann sich über drei oder fünf Jahre als teuer erweisen.

2. **Überlizenzierung aufgrund unklarer Anforderungen: Der Preis der Sicherheit**
   Sind die zukünftigen Anforderungen an eine Komponente unklar oder die Dokumentation des Herstellers zu intransparent, bestellen viele "aus Sicherheit" die höchstmögliche Lizenz-Stufe.

   Damit sollen bürokratische Hürden für Nachbestellungen und unbequeme Rückfragen vermieden werden. Am Ende steht eine Überlizenzierung: Es wird für unzählige Premium-Funktionen gezahlt, die nie genutzt werden.

3. **Aufwändiges Handling: Zeitfresser Lizenz-Verwaltung**
   Ein kompliziertes Lizenzmodell verursacht nicht nur bei der

Bestellung, sondern auch im laufenden Betrieb erheblichen Mehraufwand. Das Verwalten in verschiedenen Herstellerportalen, das Zuweisen und Freigeben von Berechtigungen sowie das Nachverfolgen von Aktivierungen dauert meist länger als vermutet und vom Hersteller versprochen.

Zusätzlich erschweren die unzähligen Änderungen, die teilweise im Lebenszyklus einer Komponente eintreten, den Administratoren das Leben. Ein Gerät, das unter einem bekannten Lizenzsystem gekauft wurde, erfordert nach einem Update ein anderes Vorgehen. Für neue Produkte hat sich der Hersteller ein "überarbeitetes" System ausgedacht, und das Chaos ist perfekt:

- Auf bestehenden Geräten müssen ggf. Konfigurationsänderungen eingespielt werden.
- Die internen Prozesse für Beschaffung, Aktivierung und Verwaltung müssen angepasst werden.
- Neue Portale und Oberflächen erfordern erneut Einarbeitungszeit.

Deswegen gilt meist: Je einfacher das Lizenzsystem, desto einfacher das Handling.

4. **Teure Support-Verträge, langsame interne Prozesse: SLA-Mismatch**
   Ein teurer 24x7-Support-Vertrag mit 4-Stunden-Austauschservice ist wenig wert, wenn die internen Prozesse nicht ebenfalls entsprechend schnell sind. Was nützt ein Ersatzteil, das Sonntagmorgen geliefert wird, wenn niemand vor Ort ist, um den Techniker ins Rechenzentrum zu lassen oder das defekte Teil zu tauschen? Support-Level müssen immer realistisch an die internen Prozesse angepasst werden.

5. **Fehlende Übersicht bei Subscriptions: Verloren im Lizenz-Dschungel**
   Mit der Zunahme von laufzeitbasierten Lizenzen geht die Übersicht schnell verloren. Unterschiedliche Komponenten diverser Hersteller mit verschiedenen Paketen, die jeweils zu unterschiedlichen Zeiten für ein, drei oder fünf Jahre gekauft wurden – hört sich kompliziert an, und genau das ist es auch. Ohne eine zentrale, herstellerübergreifende Verwaltung ist es fast unmöglich, den Überblick zu behalten. Verpasste Erneuerungen können im schlimmsten Fall zum plötzlichen Ausfall von wichtigen Funktionen oder zum Verlust des Herstellersupports führen.

   In der Praxis wird diese Aufgabe meist zusätzlich dem Techniker-Team "zugeschoben", während Bestellungen in größeren Unternehmen über andere Abteilungen erfolgen, die wiederum keine Informationen über Bedarfe oder die Ablaufdaten haben. Unsere Empfehlung: Ein Kompetenz-Team aus Einkauf und Technik, in dem beide Parteien genau wissen, was wann erforderlich ist. Denn nichts ist schlimmer als eine ausgelaufene Funktion (siehe Punkt 7), die auf langsame Prozesse großer Unternehmen trifft.

   Fatal wird die fehlende Übersicht, wenn sich die Produkte dem Ende ihrer Lebenszeit nähern. Typischerweise können Lizenzen nach End-of-Life-Ankündigung nur bis zu einem festgelegten Datum verlängert werden. Wird dieses versäumt, ist eine Verlängerung nicht mehr möglich, und man steht mit Hardware ohne Support da, die dann vor dem eigentlichen End-of-Life, meist mehrere Jahre früher, ausgetauscht werden muss.

6. **Abhängigkeit vom Management-System: Der goldene Käfig**
   Moderne Netzwerkinfrastrukturen werden zunehmend über zentrale, herstellereigene Management-Plattformen (Cloud oder On-Prem) verwaltet. Oft ist die Lizenz für diese Plattform an den Kauf der Hardware gekoppelt und zu Beginn kostenlos oder stark rabattiert. Das Problem: Ohne Verlängerung der teuren Management-Lizenz verliert die Hardware nach Ablauf der Frist ihre zentralen Verwaltungsfunktionen. Diese Abhängigkeit sollte Ihnen von Beginn an bewusst sein. Entscheidet man sich für das herstellereigene System, müssen die Kosten hierfür in die TCO-Rechnung aufgenommen werden!

7. **Funktionsverlust bei auslaufender Lizenz: Wenn die Firewall zum Briefbeschwerer wird**
   Während Funktions-Lizenzen früher einmalig erworben wurden und permanent gültig waren, ändern immer mehr Hersteller ihre Modelle. Läuft die Subscription für Firewall oder Switch aus, stellt die Komponente wesentliche Kernfunktionen komplett ein. Die teure Hardware wird damit im Extremfall nutzlos, bis man den Vertrag verlängert. Gerade in Verbindung mit einer fehlenden Übersicht (siehe Punkt 5) oder bei Migrationen (siehe Punkt 8) hat dieser Umstand ein mögliches, betriebskritisches Fehlerpotenzial.

8. **Die Migrationsfalle: Wenn die Uhr schneller tickt als die neue Lösung**
   Ein gerne übersehener Fallstrick tritt am Ende des Lebenszyklus einer Infrastruktur ein. Die TCO wurde auf fünf Jahre berechnet, und im vierten Jahr beginnt die Planung der Ablösung.

   Doch die Praxis zeigt: Ausschreibungen, Lieferzeiten für die neue Hardware und der Rollout an vielen Standorten dauern oft deutlich länger als die Restlaufzeit der alten Verträge. Kurz vor Ablauf der fünf Jahre steht man vor einem Problem: Die neue Infrastruktur ist noch nicht vollständig betriebsbereit, während die Lizenzen der alten auslaufen.

   Nun muss eine Verlängerung für die alte Hardware gekauft werden, meist für mindestens ein weiteres Jahr. Der Schock bei der Preisabfrage: Die Kosten für eine einjährige Verlängerung sind nicht selten unverhältnismäßig hoch.

Zusammenfassung und Empfehlung

Die Auseinandersetzung mit dem Thema Lizenzen hat sich zu einem immer größeren, komplexen Thema entwickelt. Basierend auf unseren Praxiserfahrungen haben wir die folgenden Anforderungen an ein nutzerfreundliches Modell definiert:

Anforderungen an Feature-/Funktions-Lizenzen

Grundlegende Hardware-Funktionen sollten nicht zeitbasiert "gemietet" werden. Eine einmal gekaufte Funktion, wie der Datendurchsatz eines Routers, muss dauerhaft und ohne Folgekosten genutzt werden können. Eine Hardware darf nicht durch eine ausgelaufene Lizenz unbrauchbar werden.

Eine Ausnahme sehen wir hier bei Diensten, die dauerhaft Leistungen des Herstellers oder eines Dritten abrufen: beispielsweise die Aktualisierung von Signaturen eines Intrusion Prevention System (IPS) oder eines URL-Filters, der tagesaktuell vom Hersteller gepflegt wird. Hier wird eine laufende Dienstleistung bezahlt.

Anforderungen an Management-Lizenzen

Subscription-Lizenzen für eine Cloud-Management-Plattform sind fair. Hier wird die laufende Service-Infrastruktur des Herstellers genutzt, der für Betrieb und Wartung sorgt.

In diesem Zusammenhang ist es aus unserer Sicht essenziell, dass eine IT-Komponente auch ohne das vom Hersteller angebotene Cloud-Management-System betrieben werden kann. Betrieb umfasst dabei ein vollständiges Monitoring und Konfigurations-Management über einen alternativen Weg, beispielsweise mittels passender Open-Source-Produkte oder herstellerunabhängiger Management-Produkte eines alternativen Anbieters. Bei abgelaufener Management-Lizenz muss die gemanagte Hardware folglich ihre volle lokal konfigurierbare Funktionalität behalten oder alternativ mit einer anderen Firmware lokal nutzbar sein.

Anforderungen an Wartungs- und Support-Lizenzen

Ein laufzeitbasierter Vertrag für den Zugang zum Support-System des Herstellers und die Bereitstellung von neuen Features durch Updates ist ein faires und etabliertes Modell. Der Zugang zu kritischen Sicherheitspatches, die Schwachstellen in der Firmware beheben, sind aus unserer Sicht keine optionale Zusatzleistung, sondern eine Pflicht des Herstellers. Sie müssen bis zum offiziellen End-of-Life einer Komponente auch ohne laufenden Support-Vertrag bereitgestellt werden.

Anforderungen an ein modernes Lizenz-Management-System

Eine Subscription darf erst dann beginnen, wenn die Leistung tatsächlich genutzt wird, d.h. wenn ein Gerät zum ersten Mal in das Management-System aufgenommen wird, nicht am Tag des Kaufs oder der Lieferung. Erfahrungsgemäß vergehen zwischen Bestellung und Staging der Hardware teilweise Monate.

Eine laufzeitbasierte Management-Lizenz sollte ebenfalls pausiert werden können, wenn Komponenten temporär außer Betrieb genommen werden und keine Hersteller-Ressourcen nutzen. Das ist zum Beispiel bei einem Umbau oder bei nur zeitweise genutzten Komponenten (etwa für Veranstaltungen, Messe-Stände etc.) der Fall.

Lizenzen sollten automatisch vom Netzwerk-Gerät aktiviert werden können. Das Einspielen von gerätespezifischen Schlüsseln ist lange überholt. Geräte müssen ihre Berechtigungen in Echtzeit aus dem zentralen Pool des Unternehmens beziehen können. Eine zentrale Übersicht über alle genutzten Lizenzen muss jederzeit möglich sein. Zudem sollte jede Lizenz einem Gerät zugeordnet sein. Angesichts der Vielzahl verwalteter Geräte und Bestellungen im Unternehmen lassen sich Bestellungen und deren Bereitstellung im virtuellen Account nicht immer lückenlos nachverfolgen. Dadurch kann es vorkommen, dass Geräte die Lizenzen anderer Geräte beanspruchen. Grundsätzlich soll das zwar möglich sein, jedoch muss die Nutzung nachvollziehbar und steuerbar bleiben.

Eine Co-Termination muss möglich sein. Hersteller müssen die Möglichkeit bieten, die Laufzeiten von gleichen Lizenzen bzw. Lizenz-Gruppen im Unternehmen auf ein einziges, gemeinsames Enddatum zu synchronisieren. Dies vereinfacht die Budgetierung und Verwaltung und schafft einen einzigen, planbaren Erneuerungszeitpunkt für z. B. die gesamte WLAN-Infrastruktur des Unternehmens oder des Standortes.

Das Ablaufen einer Lizenz darf niemals zu einer sofortigen Funktionseinschränkung führen. Ein Kulanzzeitraum (Grace Period) von mindestens 30 Tagen muss dem Kunden gewährt werden. Ebenfalls sollte der Kunde vor Ablaufen mehrfach, beispielsweise per E-Mail oder durch eine Meldung im Management-System, informiert werden.

Für die Hersteller sind Lizenzen zu einem zentralen Geschäftsmodell geworden. Dieser Wandel folgt dem globalen, übergreifenden Trend zu einer “Subscription Economy”, etwa auch bei Produkten der Automobilindustrie. Der Trend ist aus unserer Sicht kritisch zu sehen. Die strategische Investition in Netzwerk-Hardware ist eine Entscheidung über viele Jahre. Aus diesem Grund sollte jede Entscheidung bewusst getroffen und durch sorgfältige TCO-Analyse über die gesamte Lebensdauer durchgeführt werden.

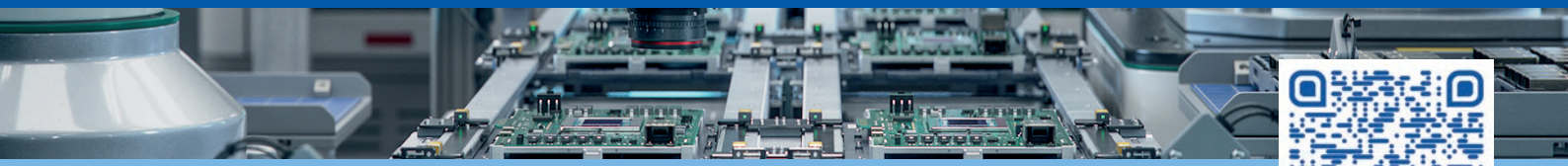
Hierbei geht es nicht darum, die Bezahlung für legitime Leistungen zu verweigern. Die Arbeit von Programmierern und Support-Teams muss bezahlt werden. Der Wechsel auf Open-Source-Hardware verlagert hier nur die Kosten. Vielmehr geht es darum, eine bewusste Entscheidung zu treffen, bei der das Lizenzmodell neben anderen wichtigen Kriterien, wie die technische Leistungsfähigkeit einer Lösung, in Betracht gezogen werden muss.

Zusammengefasst: Man das Rad nicht zurückdrehen. Wir müssen wohl oder übel mit Subscription-Modellen umgehen. Daher ist zu empfehlen, die Lizenz-Bedingungen für die Nutzung von IT-Produkten genau zu prüfen und insbesondere die Gesamtkosten über den zu erwartenden Nutzungszeitraum im Auge zu behalten. Achten Sie darauf, dass Sie sich nicht zu tief in eine Abhängigkeit eines Herstellers begeben und entwickeln Sie rechtzeitig eine Exit-Strategie.

Verweis

[1] https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html#~documentation1

Erfolgreiche IT-Strategien für Produktion 4.0 22.01.2026 online



Neues Seminar

Die Anforderungen an zukunftsorientierte IT-Konzepte für die Produktion (OT, Operational Technology) werden mit Praxisbeispielen erläutert. Bei Auswahl und Umsetzung digitaler Produkte und Lösungen im Shopfloor unterstützt die IT das Produktionsteam. Dafür ist Verständnis für das Produktionsumfeld ein entscheidender Faktor. Der Produktionsablauf muss mit den Anforderungen der IT in einen sinnvollen Zusammenhang gebracht werden.

Warum Sie diese Schulung besuchen sollten:

Eine erfolgreiche Umsetzung digitaler Konzepte gelingt nur durch Zusammenarbeit. Daher ist es wichtig, das Verständnis für die Anforderungen der kooperierenden Bereiche IT und OT zu verbessern. Nur wenn man weiß, was für die Produktion wichtig ist, können gemeinsam passende Lösungen erarbeitet und umgesetzt werden.

In diesem Seminar vertiefen Praxisbeispiele aus verschiedenen Industriebereichen den Einblick der IT in die Rahmenbedingungen in der Produktion.

Folgende Inhalte erwarten Sie:

Optimierung durch Digitalisierung
- Produktion und Digitalisierung
- Aktuelle Technologien und Trends
- Innovationen durch smarte Produkte

Umsetzung in der Fertigung
- Produktionsoptimierung durch IT und OT
- Auswahl und Implementierung von Tools
- Rahmenbedingungen im Shopfloor

Kompetente Nutzung von Daten
- Datenmanagement im Shopfloor
- Einsatzbereiche von digitalen Tools und KI
- Verteilung der Datenströme

Digitalisierungs-Strategie im Shopfloor
- Strategie-Entwicklung
- Ziele einer Digitalisierungs-Strategie
- Erstellung einer Roadmap für die Produktion

Sie lernen in diesem Seminar:

- Datenmanagement im Shopfloor
- Randbedingungen des Datentransfers aus Produktionssicht
- Use-Case-orientierte IT-Architektur
- Zielorientierte Projektarbeit in gemeinsamen Teams
- Einflussfaktoren der Produktion

Dieses Seminar richtet sich an IT-Verantwortliche, Projektleiter und alle, die mit OT-Aufgaben befasst sind. Melden Sie sich jetzt an und sichern sich Ihr Wissen für die Zukunft!

Schulungsdauer: 6 Stunden
Preis: 1.090,- €

Ihr Referent
Ullrich Möllmann war seit 2008 in einem internationalen Anlagenbau-Konzern für den Aufbau eigener digitaler Lösungen zur Produktionssteuerung (MES) und die entsprechenden Plattform-Aktivitäten verantwortlich. Seit 2018 arbeitet er als freier Consultant und begleitet Unternehmen beim Aufbau einer digital gesteuerten Produktion.

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

NW
NETZWERK

ComConsult GmbH
Beratung + Planung + Schulung

NETZWERKDESIGN IM CAMPUS

FLEXIBLE UND ZUKUNFTSFÄHIGE NETZE IM CAMPUS

NETZWERK-DESIGN | LAN | WLAN | IT-ARCHITEKTUREN | SOFTWARE-DEFINED NETWORKS

NW

In einer Zeit, in der die Anforderungen an Campus-Netzwerke rapide steigen, ist ein durchdachtes Netzwerkdesign unerlässlich. Moderne Anwendungen von klassischer Büro-Kommunikation und Medientechnik bis hin zu smarten Gebäudetechnologien sollen sich nahtlos in Ihre Campus-Infrastruktur integrieren. Gerne stehen wir Ihnen bei einem möglichen Redesign Ihres Netzwerks zur Seite. Dabei ist es wichtig, flexible Strukturen, Mandantenfähigkeit und betreibbare Netzwerkarchitekturen zu planen. Mit einem Blick auf bewährte Technologien und innovative Ansätze wie Software-Defined Networks garantieren wir eine zukunftssichere Lösung.

OFFENE STELLEN

Sie suchen eine neue Herausforderung -
wir suchen neue Mitarbeiter

https://karriere.comconsult.com/

Der Fluch des Wissens: Warum du als Expert:in manchmal nicht verstanden wirst

von Steffen Moll

Viele IT-Profis kennen das: Man hat hohe Expertise und erklärt komplexe Themen präzise – und trotzdem kommt wenig an. Der „Fluch des Wissens“ sorgt dafür, dass wir vergessen, wie es ist, nichts zu wissen. In diesem Beitrag geht es darum, wie Inhalte verständlich und wirksam vermittelt werden können. Aus meinen Trainings weiß ich: Schon kleine, gezielte Hebel verändern die Wirkung sofort.

Bist du auch verflucht?

In einem Experiment der Stanford-Forscherin Elizabeth Newton wurden zwei Gruppen gebildet: sogenannte „*Klopfer*“ und „*Zuhörer*“.

Die Klopfer trommelten den Rhythmus eines bekannten Liedes – etwa *Happy Birthday* – mit den Fingern auf den Tisch. Die Zuhörer mussten das Lied erraten.

Erstere schätzten, dass etwa 50 % das richtige Lied erraten würden. Tatsächlich lag die Trefferquote bei nur 2,5 %. Die Klopfer hörten die Melodie klar in ihrem Kopf, doch die Zuhörer hörten nur das rhythmische Klopfen.

Die Klopfer konnten sich nicht mehr vorstellen, wie es ist, das Lied nicht zu kennen. Genau darin liegt der Fluch des Wissens: Wer etwas sehr gut weiß, kann sich kaum noch vorstellen, wie es ist, es *nicht zu wissen*.

Damit wird Wissensvermittlung zur Herausforderung – egal ob im Meeting, in einer Präsentation oder in einem Training. Die entscheidende Frage lautet also: Wie gehst du damit um?

Wenn dein Wissen zur Barriere wird

Je mehr wir wissen, desto schwerer fällt es, die Perspektive anderer einzunehmen. Unser Gehirn vergisst, wie es ist, etwas nicht zu wissen.

In der Psychologie nennt man das den „*Curse of Knowledge*“ – den Fluch des Wissens.

Bei Themen über Firewalls, APIs oder Cloud-Architekturen siehst du Zusammenhänge, Abhängigkeiten und Fachbegriffe sofort. Dein Gegenüber aber nicht – ihm fehlt der Kontext, die Landkarte im Kopf. Und genau dort entstehen Missverständnisse: Was für dich logisch ist, wirkt auf andere abstrakt oder überfordernd.

Typische Situationen:

- Du erklärst etwas zum dritten Mal – und trotzdem bleibt es unklar.
- Während deiner Präsentation wirken einige Teilnehmende unaufmerksam oder abgehängt.
- Du bekommst Rückfragen zu Punkten, die du für selbstverständlich hältst.

Der Fluch des Wissens wirkt also nicht, weil du zu wenig erklärst, sondern weil du zu viel über dein Thema weißt und dir nicht mehr vorstellen kannst, wie es ist, dieses Wissen nicht zu haben.

Die gute Nachricht: Dieser Fluch lässt sich mit ein paar gezielten Techniken brechen.

Wie du den Fluch des Wissens brichst

Der erste Schritt, den Fluch zu brechen, besteht darin, dein Wissen bewusst zu steuern, statt es einfach weiterzugeben. Bevor du Inhalte erklärst oder präsentierst, frag dich:

Was sollen die anderen am Ende wirklich können, verstehen oder anwenden?

Viele Fachleute starten direkt mit Inhalten, Folien oder Demos – ohne sich klarzumachen, wo ihr Publikum eigentlich steht. Das ist wie eine Route zu planen, ohne Start oder Ziel. Wer Wissen aufnehmen möchte, begibt sich auf eine Lernreise mit unterschiedlich herausfordernden Zielen.

Das Modell von Benjamin Bloom macht Lernziele sichtbar – von Erinnern, Verstehen, Anwenden bis hin zu *Analysieren, Bewerten* und *Erschaffen*. Wenn du deine Lernziele auf einer dieser Stufen festlegst, kannst du dein Wissen gezielter portionieren:

- Soll dein Publikum Begriffe erkennen (*Erinnern*)? → Dann nutze klare Definitionen und Wiederholungen.
- Soll es Zusammenhänge verstehen (*Verstehen*)? → Verwende Metaphern oder einfache Visualisierungen.
- Soll es etwas umsetzen (*Anwenden*)? → Plane eine kleine Übung oder ein Beispiel aus seinem Alltag ein.

Nur wer weiß, wo die anderen stehen und wohin sie sollen, kann sie auch wirklich mitnehmen.

Ebenso wichtig: Kenne dein Publikum. Erfrage das Vorwissen aktiv – durch Fragen wie:

- „Wer hat das schon mal gemacht?“
- „Wie würdet ihr das aktuell erklären?“
- „Was interessiert euch am meisten?“

So findest du heraus, wo du ansetzen kannst – und wo es besser ist, einen Schritt zurückzugehen. Nachdem du weißt, wo deine Zielgruppe steht und auf welche Erkenntnisstufe du sie nach Bloom heben möchtest, folgt ein entscheidender Schritt: Mach den Nutzen deiner Inhalte klar, bevor du inhaltlich wirst.

Wir nennen das in unseren Train-the-Trainer-Seminaren „Sell the Value“. Es ist ein psychologischer „Vertrag“: „*Ich zeige euch, was euch wirklich weiterbringt – und ihr schenkt mir dafür eure Aufmerksamkeit*“.

So sagt das Publikum innerlich „ja“, bevor du in Details gehst. Die Teilnehmenden verstehen, warum sich Zuhören lohnt, wohin du sie führst und welchen persönlichen Nutzen sie haben. Wer zuerst den Wert vermittelt, macht das Publikum bereit für fachlichen Input.

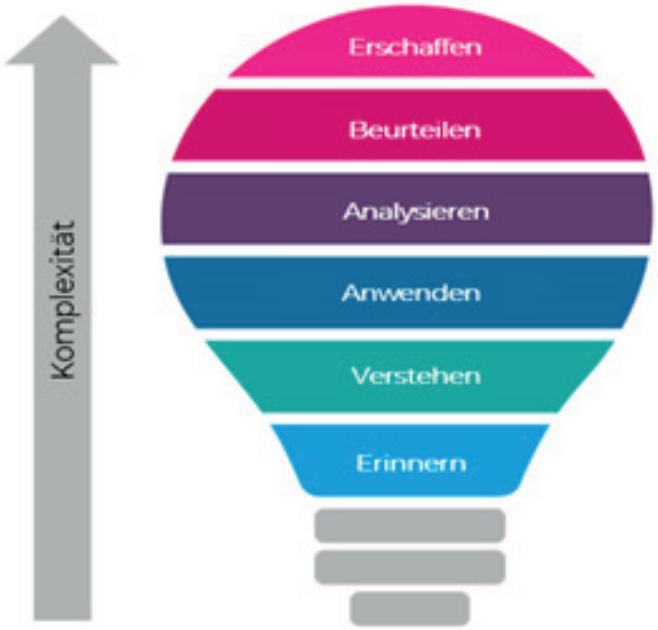


Abbildung 1: Das Modell nach Benjamin Bloom – die sechs Lernstufen
Quelle: Die sechs Lernstufen nach Bloom

Nutze Verständlichmacher in deinen Erklärungen

Nachdem du den Nutzen klargemacht und dein Publikum innerlich „an Bord“ geholt hast, geht es um die Sprache. Viele Erklärungen, Präsentationen und Trainings scheitern nicht am Inhalt, sondern an der Verständlichkeit.

Fachsprache darf nicht zur Fremdsprache werden. Wer verstanden werden will, braucht Übersetzerqualitäten – von der komplexen Fachwelt in die Denkweise der Zuhörenden. Fachleute sprechen oft, als würden sie mit ihrer Software reden: präzise, korrekt, aber ohne Anschluss an die Denkweise des Publikums.

Setze bewusst **Verständlichmacher** ein – kleine sprachliche Werkzeuge mit großer Wirkung:

- **Sprachliche Verständlichmacher:** „Lasst es mich ganz einfach sagen“ oder „Um es auf den Punkt zu bringen“.
- **Aktiv statt passiv:** Nicht „Das wird konfiguriert“, sondern „Wir konfigurieren das jetzt.“ Aktivsprache bringt Energie und Nähe.
- **Bilder und Vergleiche:** Eine Datenbank ist wie eine Bibliothek mit unendlich vielen Regalen, ein Proxy wie die Empfangsdame im Netzwerk, ein Backup wie eine Zeitmaschine für Daten,

ein VPN wie ein geheimer Tunnel durch das Internet. Solche Metaphern machen Abstraktes verständlich.

- **Pausen einbauen:** Kurze Denkpausen geben Zeit, das Gehörte zu verarbeiten. Gerade online oft besonders wirksam.

- **Struktur:** Sag, was kommt – sag es – und fass es zusammen. Das gibt Sicherheit und Klarheit, besonders in virtuellen Settings.

Merke: Verständlichkeit ist kein Stilbruch, sondern ein Zeichen von Souveränität. Nur wer Komplexes einfach erklären kann, beherrscht es wirklich.

Strukturiere dein Wissen – weniger ist mehr

Wer viel weiß, will oft alles teilen. Zu viele Informationen überfordern, das Publikum schaltet ab oder behält nur Bruchstücke.

- **Begrenze dich auf drei Kernaussagen:** Mehr Punkte merkt sich kaum jemand. Drei ist die magische Zahl für unser Gehirn.

- **Klare Zwischenstopp:** Kurze Pausen, neue Folien, Überschriften oder Beispiele signalisieren neue Gedankenabschnitte.

- **Regelmäßig zusammenfassen:** Wiederholung ist kein Zeichen von Schwäche, sondern von Professionalität. Kurze Rückblick wie „Was haben wir bisher gelernt?“ verankern Wissen langfristig.

Denn unser Gehirn liebt Wiederholung, aber nicht alles auf einmal. Lernen ist nachhaltiger, wenn Wissen in **kleinen Portionen über Tage oder Wochen** verteilt wird (Spacing Effect). Häufige Aktivierung stärkt das Gedächtnis, macht Zusammenhänge sichtbar und verwandelt Komplexität in Klarheit.

Ich bevorzuge Lernreisen über längere Zeit statt Einzeltrainings. Denn Lernen braucht Zeit: Studien zeigen, dass **achtmal eine Stunde zu lernen effektiver ist als acht Stunden am Stück**.

Storytelling – von der trockenen Theorie zur lebendigen Geschichte

Fakten überzeugen den Kopf – Geschichten erreichen das Herz. Wissen nur zu erklären bleibt abstrakt. Erzählst du es, wird es erlebbar und merkfähiger. Gerade in der IT oder im technischen Umfeld hilft Storytelling, komplexe Inhalte greifbar zu machen. Nutze dabei diese einfachen Prinzipien:

- **Relevanz erzeugen:**
  Statt mit der Lösung zu starten, zeig zuerst den Schmerzpunkt, der relevant ist. Zum Beispiel: „Viele Unternehmen verlieren täglich wertvolle Zeit, weil ihre Systeme nicht miteinander sprechen. So auch Kunde XYZ, als …“ So erzeugst du Relevanz – und dein Publikum erkennt sich wieder.

- **Drei Schritte:**
  Situation – Challenge – Solution (SCS): Ein Klassiker aus dem Consulting und Tech-Storytelling:

  - **Situation**: Ausgangslage oder Kontext
  - **Challenge**: Das Problem oder Hindernis, das sich zeigt
  - **Solution**: Wie du (oder dein Team, dein Produkt) das Problem löst

  Beispiel: „Unsere Infrastruktur war verteilt (Situation). Die Updates dauerten ewig (Challenge). Durch eine Automatisierung der Deployments konnten wir die Rollout-Zeit um 60 % verkürzen (Solution).“

- **Menschen einbauen:**
  Sag nicht: „Das System reagiert nicht mehr“, sondern: „Peter klickt – und nichts passiert.“ So werden technische Zusammenhänge emotional und nachvollziehbar.

- **Persönliche Anekdoten nutzen:**
  Keine Heldengeschichte nötig – oft reicht eine persönliche Geschichte wie: „Ich erinnere mich an ein Projekt, in dem wir genau diesen Fehler gemacht haben.“ Das schafft Nähe, Glaubwürdigkeit und Verbundenheit. Und ganz nebenbei kannst du das komplexe Problem beschreiben und dabei dein Fachwissen vermitteln, wie du es gelöst hast. Wenn Inhalte mit Geschichten verbunden werden, erinnert sich das Publikum nicht nur an Fakten, sondern an Erlebnisse. Das bedeutet, Wissen wird nicht nur verstanden, sondern bleibt im Kopf.

- **Klare Botschaft führt zu Lernerkenntnis:**
  Im Kontext der Wissensvermittlung erzählst du Geschichten nicht zum Selbstzweck, sondern damit dein Publikum eine neue Erkenntnis gewinnt. Deshalb braucht jede gute Story ei-

ne Lernerkenntnis – also einen Satz, der beschreibt, was dein Publikum aus deiner Geschichte mitnehmen soll.

Tipp: Formuliere sie als Satz mit „Deshalb …“ oder „Daraus erkennen wir …“. Beispiel: „Deshalb ist es besser, erst die Bedürfnisse der User zu verstehen, bevor man die Lösung baut.“ Oder: „Und da wurde mir klar: Wir waren plötzlich so viel effizienter, als wir die Systeme miteinander kommunizieren ließen.“

Extra-Tipp: Vermeide Formulierungen wie „Daraus lernen wir …“. Viele verbinden Lernen oder Lehrer mit negativen Erfahrungen. Solche Begriffe aktivieren alte Muster – das willst du vermeiden.

Nutze Storytelling, damit deine Inhalte ankommen. Du erzeugst Emotion und leitest eine Erkenntnis ab, die hängen bleibt. Eine gute Lernerkenntnis sorgt dafür, dass das Publikum die Geschichte versteht, sich erinnert und später anwendet.

Machen ist wie Zuhören – nur krasser

„Sage es mir – und ich vergesse. Zeig es mir – und ich verstehe. Lass es mich tun – und ich behalte es.“ Verstehen entsteht nicht durch Zuhören, sondern durch eigenes Tun. Im Training, Präsentationen oder Meetings solltest du das Publikum aktiv einbinden: mitdenken, mitreden, mitmachen. So wird aus Konsum Beteiligung und aus Wissen Verständnis.

Hier sind einfache, wirkungsvolle Wege, dein Publikum zu aktivieren:

- **Fragen stellen, statt alles zu erklären:**
  Zum Beispiel: „Wie würdet ihr das lösen?“ oder „Was vermutet ihr, passiert als Nächstes?“ Fragen öffnen Denkräume – und erzeugen Verbindungen im Gehirn deiner Zuhörenden.

- **Teilnehmende selbst erklären lassen:**
  Eigene Worte verknüpfen neues Wissen mit vorhandenem – ein stabiles Wissensnetz entsteht.

- **Mini-Übungen oder Quizzes:**
  Kurze, interaktive Aufgaben erzeugen Erfolgserlebnisse, aktivieren, ohne zu überfordern, schaffen Selbstwirksamkeit und festigen Wissen durch Wiederholung.

- **Lernpartner einsetzen:**
  Teilnehmende erklären sich gegenseitig – etwa in Breakout-Räumen oder Zweiergruppen. Oder wie sie das Wissen in ihrem eigenen Kontext anwenden würden. Das stärkt nicht nur das Verständnis, sondern auch die soziale Dynamik.

- **Mit Take-aways arbeiten:**
  Am Ende fragen: „Wenn du morgen nur eine Sache umsetzt – welche wäre das?“ So entsteht Commitment und Transfer in den Alltag.

Wissen entsteht, wenn Menschen aktiv werden – nicht, wenn einer redet und alle anderen abschalten. Bezieh dein Publikum ein, um Verstehen und Vertrauen in die eigene Kompetenz zu fördern. Das ist der Kern nachhaltiger Wissensvermittlung: Mach aus Teilnehmenden Mitgestaltende – sie lernen mit und nutzen das erworbene Wissen selbst.

Fazit: Entscheidend ist nicht, was du sagst – sondern was ankommt

Der Fluch des Wissens betrifft alle, die erklären, präsentieren oder vermitteln. Wer ihn erkennt, kann ihn brechen – mit Struktur, Lernmethoden und der Bereitschaft, die Perspektive der Lernenden einzunehmen. Wirklich gute Wissensvermittlung bedeutet, nicht alles zu sagen, was man weiß, sondern das zu vermitteln, was Lernende benötigen, um ein Ziel zu erreichen. Es geht nicht um Brillanz, sondern darum, verstanden zu werden.

Als Führungskraft, Trainer oder Experte gestaltest du so mehr als einen Lernmoment – du erzeugst Erkenntnis. Darin liegt der Unterschied zwischen Wissen weitergeben und Menschen weiterbringen.

Albert Einstein sagte dazu: „Wenn du es nicht einfach erklären kannst, hast du es selbst noch nicht gut genug verstanden.“

Virtuelle Präsentationen: So begeistern Sie Ihr Publikum!
11.03.2026 online

„Eine(r) redet, viele schlafen.“ So laufen leider zu viele Online-Präsentationen ab. Entdecken Sie in diesem Seminar die Vielfalt an Möglichkeiten, wie Sie Ihre virtuellen Meetings, Webinare und Präsentationen interessant gestalten.

Lernen Sie in diesem halbtägigen Seminar von unserem erfahrenen Experten, worauf es bei erfolgreichen Online-Präsentationen ankommt. Erfahren Sie, wie Sie durch Interaktionen für Abwechslung sorgen, Ihre Präsentation authentisch und lebendig gestalten und souverän Fragerunden moderieren.

Referent: Steffen Moll
Preis: 590,- €
Schulungsdauer: 3,5 Stunden

Online Wissen weitergeben – für Inhalte mit Aha-Effekt, die hängen bleiben 26.03.2026 online

Aktuelles Seminar

In diesem Seminar erhalten Sie die Fähigkeiten, nicht nur als Fachexperte, sondern auch als Präsentator und (interner) Trainer zu überzeugen. Sie lernen, wie man Präsentationen interaktiv, lebendig und wirkungsvoll gestaltet, um die Aufmerksamkeit des Online-Publikums zu gewinnen und Inhalte “gehirngerecht” zu übermitteln. Durch praktische Tipps und direkte Anwendungsbeispiele wird es Ihnen möglich sein, Ihr Wissen effektiv zu teilen und eine dauerhafte Wirkung zu erzielen.

Warum Sie diese Schulung besuchen sollten:

Verbessern Sie Ihre Kommunikations- und Lehrfähigkeiten, um Ihre Inhalte aktiv zu transportieren, sodass sie bei den Teilnehmern verständlich sind und hängen bleiben.

Folgende Vorträge erwarten Sie:

- Prinzipien der gehirngerechten Informationsverarbeitung verstehen
- Entwicklung und Gestaltung interaktiver Lerneinheiten
- Strategien zur Steigerung des Teilnehmerengagements
- Nutzung und Anwendung digitaler Ressourcen und Tools
- Feedback sammeln und in Echtzeit reagieren

In diesem Seminar lernen Sie:

- virtuelle Kommunikation zur Weitergabe von Inhalten effektiv zu nutzen,
- interaktive Elemente und Engagement-Techniken einzusetzen,
- Online-Trainings für maximalen Lernerfolg zu strukturieren,
- digitale Tools zur Unterstützung der Wissensvermittlung zu verwenden und
- Feedback für mehr Transferwirksamkeit zu nutzen.

Schulungsdauer: 3,5 Stunden
Preis: 590,- €

Dieses Seminar könnte Sie aus interessieren

Mastering Keynotes: Souverän präsentieren bei IT-Konferenzen & Co
10.03.2026 online

Das Seminar bereitet Sie darauf vor, beeindruckende Präsentationen zu liefern, die Ihr Publikum bei IT-Konferenzen nachhaltig begeistern – damit Ihre Inhalte ankommen und Ihre Botschaft überzeugt und in Erinnerung bleibt. Interaktive Techniken und gezielte Inhaltsgestaltung helfen dabei, die Zuhörer aktiv einzubinden und ihre Aufmerksamkeit zu gewinnen. Optimieren Sie die Fähigkeiten, damit die Keynotes besser ankommen und länger im Gedächtnis bleiben.

Warum Sie diese Schulung besuchen sollten:

Dieses Seminar ist unverzichtbar für alle, die ihre Präsentationsfähigkeiten verbessern möchten, um bei jeder Tech-Konferenz als Sprecher zu glänzen und in bester Erinnerung zu bleiben.

Schulungsdauer: 6,5 Stunden
Preis: 1.090,- €

Ihr Referent
Steffen Moll ist Coach und Trainer mit Leib und Seele. Der zertifizierte (Online-)Trainer begeistert mit inspirierenden Denkanstößen und Übungen. Seine Überzeugung: „Zum Dichter wird man geboren. Zum Redner wird man gemacht“. Zum Beispiel in seinen Trainings. Steffen Moll hat einen Master in Marketing und die Erfahrung aus unzähligen Präsentationen für Unternehmen, Videos und Vorträgen. Offline, online und hybrid. Neben Gruppen-Trainings ist er auch YouTuber, TEDx Speaker-Coach sowie Moderator der GABAL Webtalks.

IT-Strategie für einen öffentlichen Auftraggeber

Mit Dr. Philipp Rüßmann sprach Christiane Zweipfennig

Vor dem Hintergrund der digitalen Transformation ist die Entwicklung einer zukunftsorientierten IT-Strategie für öffentliche Auftraggeber von zentraler Bedeutung. Dabei treibt das zentrale Ziel, Verwaltungsprozesse effizient, sicher und bürgerfreundlich zu gestalten, Veränderungen und Neuausrichtungen an. Im Fokus steht dabei nicht nur die stetige Modernisierung der vorhandenen technischen Infrastruktur, sondern auch die strategische Ausrichtung auf Themen wie Informationssicherheit, Datenschutz, digitale Services und nachhaltige IT-Betriebsmodelle. Im öffentlichen Sektor ist dabei wesentlich, dass eine IT-Strategie die spezifischen Anforderungen und Rahmenbedingungen berücksichtigt: Sie muss gesetzliche Vorgaben erfüllen, den sparsamen Umgang mit öffentlichen Mitteln sicherstellen und gleichzeitig Innovationen ermöglichen. Eine erfolgreiche IT-Strategie verbindet langfristige Planung mit der Fähigkeit, flexibel auf technologische Entwicklungen und gesellschaftliche Anforderungen reagieren zu können.

Dr. Philipp Rüßmann arbeitete nach seinem Studium der Physik und seiner Promotion an einer nationalen Forschungseinrichtung zunächst in der Wissenschaft mit dem Fokus auf Materialforschung und Materialsimulationen auf modernen Supercomputern. Seit Anfang 2025 setzt er sein in der Forschung erworbenes Wissen bei ComConsult im Competence Center Cloud und Data Center für die berufliche Projektpraxis ein. Dort beschäftigt er sich unter anderem mit Themen zur IT-Strategie und mit der ganzheitlichen Betrachtung der Infrastruktur, ausgehend vom Rechenzentrum und den dazugehörigen Themenfeldern wie der IT-Sicherheit, und begleitet Kunden bei der Ausschreibung von Komponenten und Software.

ComConsult hat für einen öffentlichen Auftraggeber eine IT-Strategie entwickelt, um den Kunden in den nächsten Jahren zukunftsfähig aufzustellen. Was waren dafür die wesentlichen Treiber?

> Umzug in Neubau, IT-Fachkräftemangel, digitale Transformation von Verwaltungsprozessen

Zum einen war der bevorstehende Umzug unseres Kunden in ein neues Verwaltungsgebäude ein entscheidender Grund, eine IT-Strategie anzustoßen. Wenn sich Rahmenbedingungen ändern, dann können auch Strukturen, Abhängigkeiten und Perspektiven der IT beim Auftraggeber im Ganzen bewertet und der Unterbau der digitalen Transformation langfristig gestärkt werden. Zum anderen ist der Fachkräftemangel einer der wesentlichen Treiber der IT-Strategie, denn in der öffentlichen Verwaltung besteht grundsätzlich ein erheblicher Bedarf an Fachkräften, insbesondere vor dem Hintergrund der fortschreitenden Digitalisierung der Verwaltungsdienste und -angebote. In diesem Zusammenhang gilt es, veraltete Strukturen zu modernisieren und aufzubrechen. Daher erhielten wir den Auftrag, eine IT-Strategie zu entwickeln: in die Zukunft zu schauen, zu analysieren, was bereits gut läuft, was weitergeführt werden kann und wo Betriebsmodelle sowie Infrastruktur weiterentwickelt werden müssen, um für die Zukunft gewappnet zu sein.

Wie seid ihr bei der Strategieentwicklung vorgegangen?

Status-Quo-Analyse -> Strategische Ziele -> Handlungsfelder -> Maßnahmen

Bei der Strategieentwicklung wählten wir einen Bottom-up-Ansatz, bei dem die Lösungen und Systeme zunächst auf der Ebene der einzelnen Komponenten betrachtet wurden. Dazu erfassten und dokumentierten wir systematisch die gesamte IT-Infrastruktur – vom Rechenzentrum über die eingesetzten Server, Switches und Firewalls bis hin zur Nutzung der Fachverfahren in der Verwaltung. Darauf aufbauend führten wir eine Schwachstellenanalyse durch und ermittelten, wo konkret Handlungsbedarf bestand. In der Zusammenarbeit mit der Projektgruppe beim Kunden legten wir strategische Ziele und Handlungsfelder fest und leiteten daraus konkrete Handlungsmaßnahmen ab.

Insgesamt wechselten wir somit die Flughöhe von sehr tief (detaillierte Analyse des Status quo) zu hoch (übergeordnete Vision und Strategieentwicklung) und dann wieder runter (einzelne Maßnahmen zur Umsetzung der Strategie) und versuchten, eine gesunde Mischung aus langfristiger Vision und pragmatischer Umsetzbarkeit zu erreichen.

Was wurde bei der Ermittlung der Ist-Situation aufgenommen?

Wir begannen unsere Untersuchung im Rechenzentrum und schauten uns zunächst die Standorte an, die aus einem Betriebsverbund von zwei Rechenzentren bestanden. Dort analysierten wir die geographische Lage und prüften, welche Gefährdungen durch natürliche Ereignisse wie beispielsweise Hochwasser auftreten könnten. Anschließend untersuchten wir die vorhandenen Komponenten: die Server-, die Storage- und Backup- sowie die Netzwerk-Infrastruktur. Weiterhin beschäftigen wir uns mit den Sicherheitskomponenten wie Firewalls und weiteren Filtern, zum Beispiel für den E-Mail-Verkehr. Von der Infrastruktur aus richteten wir unseren Blick auf die Anwendungen und überlegten, welche Programme von unterschiedlichen Gruppen genutzt werden müssen, um die Dienstleistungen zu erbringen, und welche Anforderungen das Zusammenspiel zwischen Infrastruktur und Anwendungen prägen.

Lage der Rechenzentren, Server-, Storage-, Netzwerk-, Sicherheits-Infrastruktur, Anwendungen

Bei der betrachteten öffentlichen Verwaltung gibt es weit über 1.000 Dienstleistungsprozesse, die den Bürgern bereitgestellt werden. Das Spektrum reichte von Fällen im Jugendamt über die Finanzverwaltung und Wirtschaftsförderung bis hin zu alltäglichen Anfragen wie Sperrmüllabholung. Unsere Hauptansprechpartner auf Kundenseite waren drei Experten, die für die Infrastruktur zuständig waren und die Verantwortung für das Rechenzentrum sowie den gesamten Betrieb trugen. Zusammen verschafften wir uns in der Projektgruppe einen Überblick über die Prozesse. Bei spezifischen Detailfragen oder weiteren Themen unterstützten uns zusätzlich noch andere Beschäftigte des Auftraggebers.

Wie habt ihr den Status quo analysiert?

Die Bewertung der aktuellen Situation basierte auf einem Abgleich mit dem Stand der Technik und berücksichtigte aktuelle Entwicklungen. Dies trugen wir mittels einer sogenannten SWOT-Analyse zusammen. Sie gliederte sich in vier Teile: interne Faktoren wie Strengths (Stärken), Weaknesses (Schwächen) sowie externe Faktoren wie Opportunities (Möglichkeiten) und Threats (Bedrohungen).

SWOT-Analyse: Bestimmung der Stärken, Schwächen, Chancen und Bedrohungen

Beginnen wir mit den Stärken: Die bestehende IT-Infrastruktur unseres Auftraggebers ist für den aktuellen Bedarf gut ausgelegt, was für eine öffentliche Verwaltung nicht selbstverständlich ist. Wir konnten beobachten, dass die Fachkräfte eine hohe Kompetenz aufweisen. Die Altersstruktur der Mitarbeiter ist insgesamt ausgewogen, weshalb in den kommenden Jahren kein unerwartet starker Fachkräfteverlust zu erwarten ist. Gleichzeitig ist genügend Nachwuchs vorhanden, wodurch der Übergang planbar und stabil verlaufen sollte.

Im Bereich der Dokumentation der Infrastruktur und von Prozessen konnten wir einige Defizite feststellen. Wenn detaillierte und umfängliche Dokumentationen vorliegen, ist das Wissen im Unternehmen verankert, und neue Mitarbeitende können auch ohne Hilfe älterer Kollegen verstehen und nachvollziehen, wie die firmeninternen Systeme aufgebaut sind, wie sie miteinander interagieren und welche Standards gelten. Die fehlende und unzureichende Dokumentation stellt jedoch eine Schwäche dar und ist keine Besonderheit der öffentlichen Verwaltung: Dokumentationen und Prozesse sind häufig die Achillesferse – sowohl bei einem KMU als auch bei Großkonzernen.

Im ersten Teil unserer IT-Strategie diskutierten wir sämtliche Aspekte der aktuellen Situation ausführlich und schrieben sie nieder. Somit entstand ein sehr umfangreiches Dokument, das für die Zukunft Transparenz, Wiederholbarkeit und Nachhaltigkeit bringen wird. Eine weitere Schwäche bestand darin, dass sehr viele Vorgänge eigenständig erledigt wurden und der Grad externer Unterstützung relativ gering war. Hier sahen wir in dem Ausbau des IT-Outsourcing bzw. Outtasking Potenzial. Auch im Bereich der IT-Sicherheit konnten Mängel aufgedeckt werden.

Mögliche Bedrohungen, die in die Analyse mit einbezogen werden mussten, waren externe Faktoren, die zum Beispiel mit der gesamtgesellschaftlichen Lage zusammenhängen. Wir haben in

Deutschland einen umfangreichen Rechts- und Regulierungsrahmen, der gerade auch öffentliche Auftraggeber betrifft. Gleichzeitig wächst der Druck, stärker zu digitalisieren und neue Technologien zu nutzen. Es besteht ein Wettbewerb um Fachkräfte, die öffentliche Hand zahlt weniger als die freie Wirtschaft, was die Situation nicht vereinfacht. Trotz einer guten Altersstruktur gibt es erfahrene Kollegen, die Kernbereiche wie beispielsweise den Netzwerkbetrieb jahrzehntelang betreuen und altersbedingt ausscheiden werden. Auch darauf muss man vorbereitet sein.

Bedrohungen gibt es ebenso im Bereich der IT-Sicherheit, insbesondere für die Verfügbarkeit von Diensten, die über das Internet bereitgestellt werden. Das eröffnet grundsätzlich Möglichkeiten für Cyberangriffe. Unser Auftraggeber war bislang nicht betroffen; in der Region kam es jedoch vor einigen Jahren zu einem größeren Ransomware-Vorfall, der das Bewusstsein deutlich geschärft hat, sich auf Cyberbedrohungen hinreichend vorzubereiten. Wir haben daher eine Zero-Trust-Strategie empfohlen, deren Umsetzung angestoßen und schrittweise realisiert werden musste, um den Auftraggeber nachhaltig sicher für die Zukunft aufzustellen.

Durch den Neubau des Verwaltungsgebäudes eröffneten sich für den Auftraggeber zahlreiche weitere Möglichkeiten, insbesondere im Hinblick auf die Umsetzung eines Smart-Building-Konzepts. Dadurch konnte die Infrastruktur langfristig vernetzter, intelligenter und energieeffizienter gestaltet werden. Insgesamt entstand so ein wirtschaftlich und technologisch zukunftsfähiges Gesamtgebilde. Der Umzug in den Neubau bot zudem die Chance, bestehende Strukturen grundlegend zu überdenken und vollständig neu zu gestalten.

Wie habt ihr die strategischen Ziele entwickelt und welche waren es?

6 strategische Ziele: Stabiler IT-Betrieb, hohe IT-Sicherheit, moderne IT-Dienste, digitale Datenbereitstellung, IT-Neuerungen, Arbeitgeberattraktivität

Bei der Entwicklung der strategischen Ziele gingen wir pragmatisch vor und legten zunächst eine übergeordnete, langfristig ausgerichtete Vision fest. Aus dieser Vision leiteten sich die konkreten Ziele ab, die wir definierten. Bei der Zielentwicklung betrachteten wir, für wen welches Ziel relevant war – wer also beispielsweise von den Anwendern in der Verwaltung oder den Mitarbeitern im IT-Betrieb betroffen war. Anschließend legten wir das konkrete Ergebnis des jeweiligen Ziels fest. Schließlich klärten wir, welche Erfolgskriterien nötig waren, um die Erfüllung eines Ziels messen zu können. Wichtig bei der Erarbeitung strategischer Ziele war dabei der Dialog: Innerhalb der Projektgruppe brachten wir unsere Erfahrungen und Erkenntnisse ein und unterbreiteten Vorschläge. Da die Umsetzung der IT-Strategie letztlich beim Auftraggeber und dessen Personal lag, mussten zentrale Stakeholder (z.B. Fachpersonal aus dem IT-Betrieb) in die Diskussion, Abstimmung und Festlegung der strategischen Ausrichtung eingebunden werden. Der langfristige Erfolg einer IT-Strategie konnte nur gelingen, wenn Akzeptanz und Veränderungswille bei den Personen, die sie am Ende umsetzen mussten, geschaffen werden konnten.

Konkret formulierten wir sechs strategische Ziele, die in Summe dazu beitrugen, die langfristige Vision und Ausrichtung des Auftraggebers zu untermauern. Ein Schwerpunkt lag auf der Weiterentwicklung der IT-Infrastruktur und der Sicherstellung eines stabilen IT-Betriebs. Ebenso zentral war die dauerhafte Gewährleistung eines hohen IT-Sicherheitsstandards. Darüber hinaus galt es, Nachhaltigkeit und moderne IT-Dienste fest zu verankern. Ein weiteres Kernthema bildete die Verfügbarkeit, Verwaltung und Verarbeitung von Daten – insbesondere im Hinblick auf den Aufbau geeigneter Dateninfrastrukturen. Darauf aufbauend entwickelten wir digitale Zukunftsthemen, etwa Potenziale aus der Nutzung von Daten durch den Einsatz Künstlicher Intelligenz. Schließlich war es ein wichtiges Ziel, den Kunden als attraktiven Arbeitgeber zu positionieren, um dem Fachkräftemangel wirksam zu begegnen.

Welche Handlungsfelder und Maßnahmen habt ihr aus den Zielen abgeleitet?

Cloud-Entscheidungsbaum, nachhaltige IT, Datenstrategie, Zero-Trust-Architektur

Aus den Zielsetzungen ergaben sich Handlungsfelder, aus denen wir den erforderlichen Handlungsbedarf und konkrete Maßnahmen ableiteten. Um einen stabilen und sicheren IT-Betrieb zu gewährleisten, prüften wir, welche Komponenten unter welchen Rahmenbedingungen in die Cloud verlagert werden sollten, statt im eigenen Rechenzentrum betrieben zu werden. Dazu entwickelten wir einen Entscheidungsbaum, der bei der Betrachtung der Applikationen unterstützte. Er diente als Entscheidungshilfe, ob eine Anwendung in die Cloud verlagert werden durfte. Insbesondere bei der Übermittlung von sensiblen Bürgerdaten in Hyperscaler-Clouds waren Alternativen wie die Speicherung in einer privaten Cloud zu erwägen, damit die Daten in Deutschland oder im Rechtsraum der EU verblieben. Auch prüften wir die Möglichkeit eines öffentlich-rechtlichen Rechenzentrums, das von einem kommunalen Dienstleister betrieben wird und Ressourcen speziell für die öffentliche Verwaltung bereitstellt.

Ein weiteres Handlungsfeld betraf das Thema Nachhaltigkeit und knüpfte an die Dokumentation an. Im laufenden Betrieb sollten nicht nur Pläne zur IT-Infrastruktur entstehen, sondern auch Daten gesammelt und Logging- sowie Monitoring-Informationen zur Nachhaltigkeit, beispielsweise zum Stromverbrauch, erfasst werden. Dazu gehörten auch Aspekte, die den Betrieb nicht unmittelbar betrafen, wie Zertifizierungen, die Nachhaltigkeit bereits im Beschaffungsprozess belegen konnten. Hier galt es, bei der Anschaffung neuer Geräte deren Nutzungsdauer und die Dauer der Supportleistungen zu prüfen und zu optimieren.

Die Ausgestaltung von Dateninfrastrukturen und -Plattformen stellte als Zukunftsthema ein weiteres zentrales Handlungsfeld

dar, um die Digitalisierung voranzutreiben. Zunächst musste eine solide Datengrundlage geschaffen und eine Metadateninfrastruktur aufgebaut werden, um beispielsweise die Möglichkeiten von Künstlicher Intelligenz gewinnbringend nutzen zu können. In den Organisationen existierten große Datenmengen, die von unterschiedlichen Anwendungen genutzt wurden, auf unterschiedlichen Systemen lagen und vielleicht auch in unterschiedlichen Datenbanken verfügbar waren. Zur Erreichung eines Gesamtbilds über alle verfügbaren Daten galt es, ein Verzeichnis zu erstellen, das alle Informationen über den Ablageort und die Zugriffsmöglichkeiten der Daten abbildete. Ziel war die Schaffung eines Data Lakes, eines zentralen Speichers, der alle Daten zur Verfügung stellte – unabhängig davon, ob es sich um Datenbanken, Word-Dokumente oder andere Dateien handelte. Bereits zuvor kamen Data Lakes im Zusammenhang mit Big-Data-Analysen und maschinellem Lernen zum Einsatz. Doch zunächst musste der zentrale Speicherort geschaffen werden, um den Datenzugriff zu ermöglichen.

Im Bereich der Informationssicherheit identifizierten wir für unseren Auftraggeber Bausteine, die schrittweise implementiert werden konnten, um den Übergang zu einer Zero-Trust-Architektur zu realisieren. Gemäß dem Grundgedanken „Vertraue niemandem – überprüfe alles.“ wurden bei Zero Trust die Netzbereiche in möglichst kleine Abschnitte unterteilt, um sämtliche Zugriffe auf Daten oder Systeme ständig überprüfen, authentifizieren und autorisieren zu können. Diese Vorgehensweise der Mikrosegmentierung war eine Teilmaßnahme, mit der wir uns als einem der Bausteine auf dem Weg hin zu einer Zero-Trust-Architektur beschäftigten.

Welche weiteren Maßnahmen habt ihr empfohlen?

Mitarbeiterzufriedenheit fördern, Rechenzentrumsbetrieb auslagern, auf Kernkompetenzen fokussieren

Ein weniger technisches Handlungsfeld ist das Thema Arbeitgeberattraktivität. Diese spielt eine zentrale Rolle, um qualifizierte Fachkräfte langfristig zu binden und neue Talente zu gewinnen. Als eine wichtige Maßnahme sehen wir hierbei die kontinuierliche Aus- und Fortbildung. Sie ermöglicht es, sich in einem dynamischen von IT geprägten Umfeld stetig weiterzuentwickeln und den Wandel aktiv mitzugestalten. Darüber hinaus ist die Einführung geeigneter Instrumente zur regelmäßigen Erfassung der Mitarbeiterzufriedenheit und des Feedbacks von großer Bedeutung. Hierbei sollen Verfahren etabliert werden, die niedrigschwellige und zeitnahe Rückmeldungen ermöglichen – etwa durch kurze, themenspezifische Befragungen, die sich problemlos in den Arbeitsalltag integrieren lassen. Solche Formate fördern eine höhere Beteiligung und bieten die Möglichkeit, Entwicklungen und Stimmungen innerhalb der Belegschaft frühzeitig zu erkennen und gezielt darauf zu reagieren.

Ich komme noch einmal auf das Thema Rechenzentrum zurück. Hier lässt sich allgemein der Trend beobachten, dass ein direkter Umstieg in die Cloud nach dem sogenannten Lift-and-Shift-Prinzip – also die unveränderte Überführung bestehender Systeme in eine Public-Cloud-Umgebung – häufig nicht wirtschaftlich ist. Gleichzeitig steigen die Anforderungen an den Eigenbetrieb eines Rechenzentrums kontinuierlich. Aspekte wie Energieversorgung, Klimatisierung, physischer Zutrittsschutz und bauliche Sicherheitsmaßnahmen erfordern erhebliche Investitionen und sorgfältige Planung. Vor diesem Hintergrund bietet es sich an, die eigenen Server in einem externen Rechenzentrum zu betreiben und mit spezialisierten Dienstleistern zusammenzuarbeiten, beispielsweise sogenannten Housing- oder Colocation-Anbietern. Diese stellen die notwendige Infrastruktur und Umgebung bereit, während die eigene IT-Hardware weiterhin selbst betrieben wird. Auf diese Weise bleibt die volle Kontrolle über die Systeme und Daten – einschließlich der Datenhoheit – erhalten. Dies stellt aus unserer Sicht eine empfehlenswerte Option dar, um hohe Sicherheitsanforderungen zu erfüllen, gleichzeitig den wirtschaftlichen Aufwand im Rahmen zu halten und Kernkompetenzen im Haus zu behalten und damit einen (kleinen) Beitrag zur digitalen Souveränität leisten zu können.

Gibt es einen Zeitplan für die Umsetzung der Maßnahmen bis zum Wunschtermin des Kunden?

Maßnahmenumsetzung: Priorisierung, Rahmenbedingungen und Aufwandseinschätzung

Die Maßnahmen werden sich über mehrere Jahre erstrecken. Bei der Erstellung des Zeitplans für die Umsetzungsmaßnahmen prüften wir jeweils, wie dringlich die einzelnen Schritte waren. Maßnahmen, die insbesondere Schwachstellen in der Informationssicherheit betrafen, haben wir priorisiert und an den Beginn der Planung gestellt. Langfristig angelegte Themen wurden entsprechend nachgeordnet.

Teilweise war die Priorisierung auch von äußeren Rahmenbedingungen abhängig. So war es beispielsweise nicht möglich, bestimmte Maßnahmen vor der Fertigstellung des neuen Gebäudes umzusetzen. Diese Faktoren hatten den zeitlichen Rahmen maßgeblich beeinflusst.

Darüber hinaus bewerteten wir den geschätzten Aufwand für jede Maßnahme, um ein realistisches Verhältnis zwischen Dringlichkeit und Umsetzbarkeit herzustellen. Auf dieser Grundlage wurde die zeitliche Reihenfolge festgelegt. Bei der Aufwandsschätzung konnten wir auf die umfangreiche Erfahrung von ComConsult zurückgreifen. Ich konnte durch den fachlichen Austausch mit meinen erfahrenen Kolleginnen und Kollegen zusätzliches Expertenwissen in die Bewertung der einzelnen Themen einfließen lassen. Diese interne Expertise war für die Erstellung eines fundierten und ausgewogenen Zeitplans von großem Vorteil.

Ist das Projekt abgeschlossen? Was ist dein persönliches Fazit?

Vielfältiges Projekt mit konstruktiver, bereichernder Teamarbeit

Das gesamte Projekt erstreckte sich über einen Zeitraum von rund sechs Monaten und ist nun abgeschlossen. Unser Auftrag umfasste die Entwicklung der Strategie. Mit dem Abschluss der Erstellung der IT-Strategie begann erst die eigentliche Arbeit beim Kunden. Die Umsetzung und deren Begleitung war allerdings nicht mehr Bestandteil unserer Leistungen. Es gab jedoch Themenbereiche, bei denen wir potenziellen Unterstützungsbedarf auf Kundenseite identifiziert hatten. Hier könnten wir bei Bedarf weiter unterstützen.

Ich habe es als sehr positiv empfunden, im Rahmen des Projekts einen umfassenden Überblick zu gewinnen und den gesamten thematischen Querschnitt betrachten zu können. Die Zusammenarbeit mit dem Projektteam des Kunden war ausgesprochen angenehm und konstruktiv. Die regelmäßigen Treffen zum Austausch über den Fortschritt haben wesentlich zum Gelingen beigetragen. Besonders reizvoll fand ich die inhaltliche Vielfalt des Projekts, die unterschiedliche Perspektiven zusammengeführt und das Arbeiten daran besonders interessant gemacht hat.

Schwachstellenscanner – Grundlagen, Technik, Betrieb
04.05.2026 online

Dieses Seminar behandelt das Schwachstellenscanning auf verschiedenen Ebenen. Dazu werden zunächst die notwendigen Grundlagen vermittelt, beispielsweise die Einstufung von Schwachstellen nach dem „Common Vulnerability Scoring System“ (CVSS) sowie Arten von Schwachstellen und Informationsquellen wie die CVE-Datenbank.

Ausgehend davon werden technische sowie betriebliche Aspekte von Schwachstellenscannern erläutert. Diese umfassen die verschiedenen Betriebsmodi, Netzwerkaspekte sowie Vorteile, Nachteile, Möglichkeiten und Einschränkungen. Es werden ebenfalls die Herangehensweisen der verbreitetsten kommerziellen und freien Tools beschrieben.

Des Weiteren wird die Schwachstellenanalyse bei (individualisierten) Web-Anwendungen betrachtet. Diese verhalten sich anders als typische Services und erfordern spezielle Tools und weiteres Know-how. Die Auswirkungen dieses Verhaltens und die gängigen Tools werden näher untersucht.

Warum Sie diese Schulung besuchen sollten:

Erhalten Sie eine technische und betriebliche Einführung in das Thema Schwachstellenscanning auf unterschiedlichen Ebenen und mit verschiedenen Tools – von den wichtigsten Mechanismen und Begriffen bis zu den vielseitigen Werkzeugen inklusive einer Demonstration.

In diesem Seminar lernen Sie:

- welche Grundlagen und Begriffe für den Einsatz von Schwachstellenscannern wichtig sind,
- wie Schwachstellenscanner und Web-Application-Scanner funktionieren,
- welche sonstigen Tools und Frameworks verbreitet sind und
- welche Herausforderungen beim Betrieb solcher Lösungen auftreten.

Referent: Dr. Markus Ermes
Preis: 1.090,- €
Schulungsdauer: 6 Stunden

Kostenlose Webinare der Woche

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

Standards zum AI Act

04.12.2025 10:45-11:45 Uhr

Unternehmen können die Konformität zu europäischen Gesetzen über harmonisierte Europäische Normen nachweisen. Auch für den europäischen AI Act werden solche Normen zurzeit in der Europäischen Normungsorganisation CEN-CENELEC entwickelt.

In diesem kostenlosen Webinar erklärt Ihnen unser Referent die Bedeutung solcher Normen, gibt einen Überblick über die adressierten Themen und den Zeitrahmen ihrer Entwicklung. Weiterhin erläutert er, wie Unternehmen schon jetzt an der Gestaltung teilhaben können.

Zusammenfassung der Inhalte des Webinars:

- Was sind harmonisierte Europäische Normen und wie werden sie entwickelt?
- Themen: Die Standardisierungsanforderungen der Europäischen Kommission
- Stand der Arbeiten und Zeitrahmen
- Möglichkeiten zur Teilhabe

Dauer: 1 Stunde
Preis: kostenlos
Referent: Dr. Peter Deussen, Standardisierungsexperte

Notfallvorbereitung im Klartext: So erstellen Unternehmen ein professionelles IT-Notfallhandbuch

11.12.2025 10:45-11:45 Uhr

In diesem kostenlosen Webinar vermittelt Ihnen unser Referent, worauf es bei der Vorbereitung von Unternehmen auf potenzielle Risiken wie IT-Ausfälle und Cyber-Angriffe wirklich ankommt und wie Sie Schritt für Schritt zu Ihrem eigenen IT-Notfallhandbuch kommen. Damit haben Sie nicht nur das richtige Werkzeug an der Hand, um sich in Notsituationen schnell und effektiv wieder in einen Normalbetrieb zu bewegen, sondern schaffen auch ausreichend Einblicke, um Risiken im Vorfeld zu vermeiden.

Zusammenfassung der Inhalte des Webinars:

- Warum sich Unternehmen auf IT-Notfälle vorbereiten müssen
- Gesetzliche und unternehmerische Anforderungen an die IT-Notfallvorbereitung
- Worauf es bei IT-Notfällen in der Praxis wirklich ankommt
- Wie Sie zielgerichtet Ihr IT-Notfallhandbuch erstellen
- Welche Themen Sie behandeln sollten, um Ihre digitalen Geschäftsprozesse nachhaltig zu schützen
- Tipps, Tricks und Fallstricke in der Notfallvorbereitung

Dauer: 1 Stunde
Preis: kostenlos
Referent: Kevin Schneider, Dreamed IT

Gruppenrichtlinien in der Windows-Server-Umgebung 23.02.-24.02.2026 online

Neues Seminar

In diesem Seminar lernen die Teilnehmer, Gruppenrichtlinien professionell zu planen, zu implementieren, zu verwalten und zu analysieren. Neben den Grundlagen stehen praxisnahe Szenarien, Sicherheitsaspekte und Troubleshooting im Vordergrund. Nach dem Seminar sind die Teilnehmer in der Lage, Gruppenrichtlinien sicher und zielgerichtet in Unternehmensumgebungen einzusetzen.

Warum Sie diese Schulung besuchen sollten:

Gruppenrichtlinien sind der Hebel für sichere, einheitliche und automatisierte Windows-Umgebungen. Ohne klares Design wachsen GPOs jedoch an, werden widersprüchlich und bremsen den Betrieb – bis hin zu Sicherheitslücken, langen Anmeldezeiten und schwer nachvollziehbaren Seiteneffekten.

Dieses Seminar liefert einen strukturierten, praxiserprobten Ansatz: Von sauberer Planung über wartbare Strukturen, ADMX-Zentralablage und gezielte Filterung bis zum robusten Troubleshooting mit GPResult, GpLogView und Eventlogs. Sie gewinnen Entscheidungs- und Umsetzungssicherheit, reduzieren Komplexität und Risiken und erhöhen Stabilität sowie Compliance. So werden Gruppenrichtlinien vom Störfaktor zum produktiven Werkzeug – messbar im Alltag von IT-Teams.

Tag 1 – Grundlagen und Planung

- Einführung in das Konzept der Gruppenrichtlinien
- Aufbau und Funktionsweise von GPOs
- Active Directory und Gruppenrichtlinien – Zusammenspiel von Sites, Domains und OUs
- Verwaltung mit der Gruppenrichtlinienverwaltungskonsole (GPMC)
- Benutzer- vs. Computerrichtlinien
- Vererbung, Priorität und Verknüpfung von Richtlinien
- Blockieren, Erzwingen und Sicherheitsfilterung
- WMI-Filter – gezielte Anwendung von Richtlinien
- Planung einer sinnvollen GPO-Struktur in der Praxis

Tag 2 – Praxis, Sicherheit und Fehlerbehebung

- Gruppenrichtlinien in der Praxis: Beispiele aus typischen Unternehmensszenarien
- Administrative Vorlagen und zentrale Vorlagendateien (ADMX/ADML)
- Gruppenrichtlinien für Sicherheit und Hardening
  - Kennwortrichtlinien
  - Windows Defender und Firewall
  - Benutzerrechte, Skripte und Start-/Anmeldeskripte
- Gruppenrichtlinien mit PowerShell verwalten und auswerten
- Replikation und Caching von Richtlinien (SYSVOL, GPT.ini)
- Gruppenrichtlinien-Fehleranalyse:
  - GPResult, GpUpdate, GpLogView
  - Eventlogs und erweiterte Diagnose
- Best Practices, typische Fehlerquellen und Troubleshooting-Strategien

Methodik

- Theorie und Hintergrundwissen
- Live-Demonstrationen
- Praktische Übungen in einer Active-Directory-Testumgebung
- Erfahrungsaustausch und Diskussion

Schulungsdauer: 11,5 Stunden
Preis: 1.590,- €

Ihr Referent
Franz-Georg Clodt ist technischer Berater und IT-Trainer und blickt auf über 25 Jahre Berufserfahrung zurück. Zu seinen Spezialgebieten zählen Microsoft Exchange und Exchange Online, Powershell, Windows Serversysteme, Active Directory, Windows Clustering, PKI, Internet Information Server und Docker und Kubernetes. Herr Clodt ist seit 1994 durchlaufend zertifiziert als Microsoft Trainer.

Wie ComConsult die Tour de France gewinnt

von Dr. Joachim Wetzlar

Viele meiner Kollegen trainieren fleißig: Mal eben am Samstag nach Luxemburg und zurück, 24-Stunden-Rennen auf dem Nürburgring [1], und so fort. Und natürlich ist es ihr Traum, schließlich einmal bei der Tour de France mitfahren zu können.

Ich selber nutze das Fahrrad eher als Transportmittel. Hier im Norden gibt es nur plattes Land. Abgesehen vom ständigen Gegenwind ist das ideal (zumindest subjektiv gesehen gibt es immer Gegenwind, als ob sich die Naturkräfte gegen mich verschworen hätten). Daher nutze ich auch ein altmodisches Tourenrad mit Kettenschaltung und Felgenbremsen. Der gute alte Bowdenzug überträgt alle Bewegungen. Das ist wartungsarm, langlebig und sicher, auch bei Wind und Wetter.

Aktuelle Rennräder sind dagegen vollgestopft mit Elektronik. Wie sollte es anders sein, spielt auch beim Radrennsport das Smartphone eine zentrale Rolle. Es kommuniziert mit den Sensoren, Aktuatoren und Anzeigen am Rad. Sensoren sind z. B. Schalthebel, Nabentachometer und Kurbelgarnituren. Sie steuern Umwerfer, Schaltnaben, Federungen, etc. Fahr- und Leistungsparameter werden dem Fahrer angezeigt und mit dem Smartphone aufgezeichnet. Umgekehrt lassen sich mit der Smartphone-App individuelle Fahrprogramme auswählen oder die Firmware der Komponenten aktualisieren.

Alle genannten Komponenten – wer hätte es gedacht – kommunizieren drahtlos. Die Parametrierung der Fahrrad-Komponenten erfolgt i.d.R. mittels Bluetooth Low Energy (BLE), wodurch Interoperabilität zu Smartphones erreicht wird. Für Steuerungszwecke scheint BLE jedoch nicht robust genug zu sein.

Stattdessen kommt eine Funktechnik namens ANT zum Einsatz, die ich bislang noch nicht auf dem Schirm hatte. Sie wurde von Garmin entwickelt, um drahtlose Monitoring-Geräte untereinander zu vernetzen, also Smartwatches, Fitness-Tracker, GNSS-Empfänger, etc. Garmin hat es überdies vermocht, zahlreiche andere Hersteller von Sport-Zubehör davon zu überzeugen. Die Website [2] enthält ein „Product Directory“ mit mehr als tausend unterstützten Produkten. Eine Erweiterung von ANT um Anwendungsprofile ähnlich denen, die wir von Bluetooth kennen, bezeichnet Garmin als ANT+.

Schon vor längerer Zeit fragten mich meine Kollegen, wie sicher denn solche Funktechnik sei. Man könne sich doch am Fuß einer Bergetappe postieren und mit einem Störsender die Rennfahrer am Zurückschalten hindern. Sicher, erwiderte ich, das wäre möglich. Nur der ComConsult-Fahrer müsse dann mit herkömmlichen Bowdenzügen schalten.

Das Thema geriet wieder in Vergessenheit, bis ich neulich über einen Artikel [3] stolperte. Die Autoren beschrieben, wie sie das Anwendungsprotokoll eines Herstellers von Fahrradschaltungen analysiert haben. Sie kamen zu dem Schluss, dass die Kommunikation verschlüsselt ist.

Ungeachtet dessen war es ihnen möglich, einmal aufgezeichnete Kommunikation erneut auszusenden und damit die ursprünglichen Aktionen an den Schaltwerken erneut auszulösen. Diese Vorgehensweise bezeichnet man als „Replay-Attacke“. Das in [3] referenzierte Video zeigt ab Minute 12:20 eindrucksvoll die Auswirkung dieser Attacke.

Wollen Sie es selber einmal versuchen? Ich meine, digitalen Funk aufzeichnen, analysieren und wieder aussenden? Mal abgesehen davon, dass derlei Aussendungen grundsätzlich nicht zulässig sind, ist die erforderliche Technik für jedermann erschwinglich zu beschaffen. Als Basis dient ein sogenanntes Software-defined Radio (SDR). Entsprechende Produkte werden in [3] oder auch in unseren Seminaren benannt.

SDRs verfügen über USB- oder Ethernet-Schnittstellen zur Verbindung mit PCs. Entsprechende Treiber sind selbstverständlich zu installieren. Dann kann es losgehen, beispielsweise mit dem Universal-Baukasten „GNU Radio“, ein Standard-Werkzeug für SDR [4]. Auf einem graphischen Frontend lassen sich verschiedenste Module zu Empfängern oder Sendern zusammensetzen. Filterschaltungen, Oszillatoren, Mischer, analoge und digitale Modulatoren und Demodulatoren, Anzeigeelemente, Ausgaben auf Sound-Karte oder in Dateien – der Vielfalt sind kaum Grenzen gesetzt.

Auf der anderen Seite gibt es mit dem „Universal Radio Hacker“ ein fertiges Tool zur Aufzeichnung, Analyse und Aussendung digitaler Signale per SDR [5]. Ich habe es noch nicht probiert, doch die Tutorials sind vielversprechend.

Überhaupt werden Sie auf sehr viel interessante Veröffentlichungen stoßen, wenn Sie einmal in das Thema eintauchen. Ich wünsche Ihnen viel Spaß dabei. Währenddessen trainieren meine Kollegen weiter für die Tour de France.

Verweise

[1] https://radamring.de/
[2] https://www.thisisant.com/consumer/ant-101/what-is-ant
[3] „MakeShift: Security Analysis of Shimano Di2 Wireless Gear Shifting in Bicycles“, Maryam Motallebighomi (Northeastern University), Earlence Fernandes (UC San Diego), Aanjhan Ranganathan (Northeastern University), August 2024, abgerufen unter https://www.usenix.org/system/files/woot24-motallebighomi.pdf; Präsentation dazu anlässlich der Konferenz WOOT ’24, abgerufen unter https://www.youtube.com/watch?v=wQ00-Hig_Jc
[4] https://www.gnuradio.org
[5] „Universal Radio Hacker, Investigate Wireless Protocols Like a Boss“, Software Suite, abgerufen unter https://github.com/jopohl/urh

Aktuelle Seminare

- ✓ Erfolgreiches IT-Projektmanagement
  08.12.-09.12.2025 online
- ✓ Winterschule – Neueste Trends der IT-Infrastruktur
  08.12.-12.12.2025 online
- IT-Providermanagement in der Praxis
  09.12.2025 online
- ✓ Grundlagen von Storage-Systemen: Hardware, Netzwerk, Protokolle
  09.12.2025 online
- KI-gestützte Testfallerstellung mit ChatGPT
  10.12.2025 online
- Einführung der E-Akte: Praktische Umsetzung im Behördenalltag
  10.12.2025 online
- ✓ Quantum Computing und Post-Quanten-Kryptographie
  11.12.2025 online
- Storage: Neueste Trends, Technologien und Architekturen
  11.12.2025 online
- IT-Infrastrukturen für Smart Buildings
  15.12.-16.12.2025 online
- SIP-Trunk: Notruf, Fax und Netzdesign
  17.12.2025 online
- 404 Leadership not found? – Projektteams souverän führen
  17.12.-18.12.2025 online
- Der neue EVB-IT Rahmenvertrag – Effizienzboost für die digitale Transformation
  07.01.2025 online
- GENERATION X, Y und Z
  07.01.2026 online
- Geschäftliche E-Mails schreiben – möglich mit KI?
  08.01.2026 online
- ✓ Sonderveranstaltung: Netzwerkplanung im Smart Building
  13.01.2026 online
- IT-Admins aufgepasst: So vermeiden Sie rechtliche Stolperfallen im Alltag
  13.01.2026 online
- IT-Sicherheitsrecht 3.0: Überblick über die neuen IT-Sicherheitsgesetze
  13.01.2026 online
- IT-Outsourcing managen – Chancen und Risiken
  13.01.-14.01.2026 online
- IT-Verträge sicher verhandeln, gestalten und durchführen
  13.01.-14.01.2026 in Aachen

✓ Garantietermin

ComConsult Online-Veranstaltungskalender

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

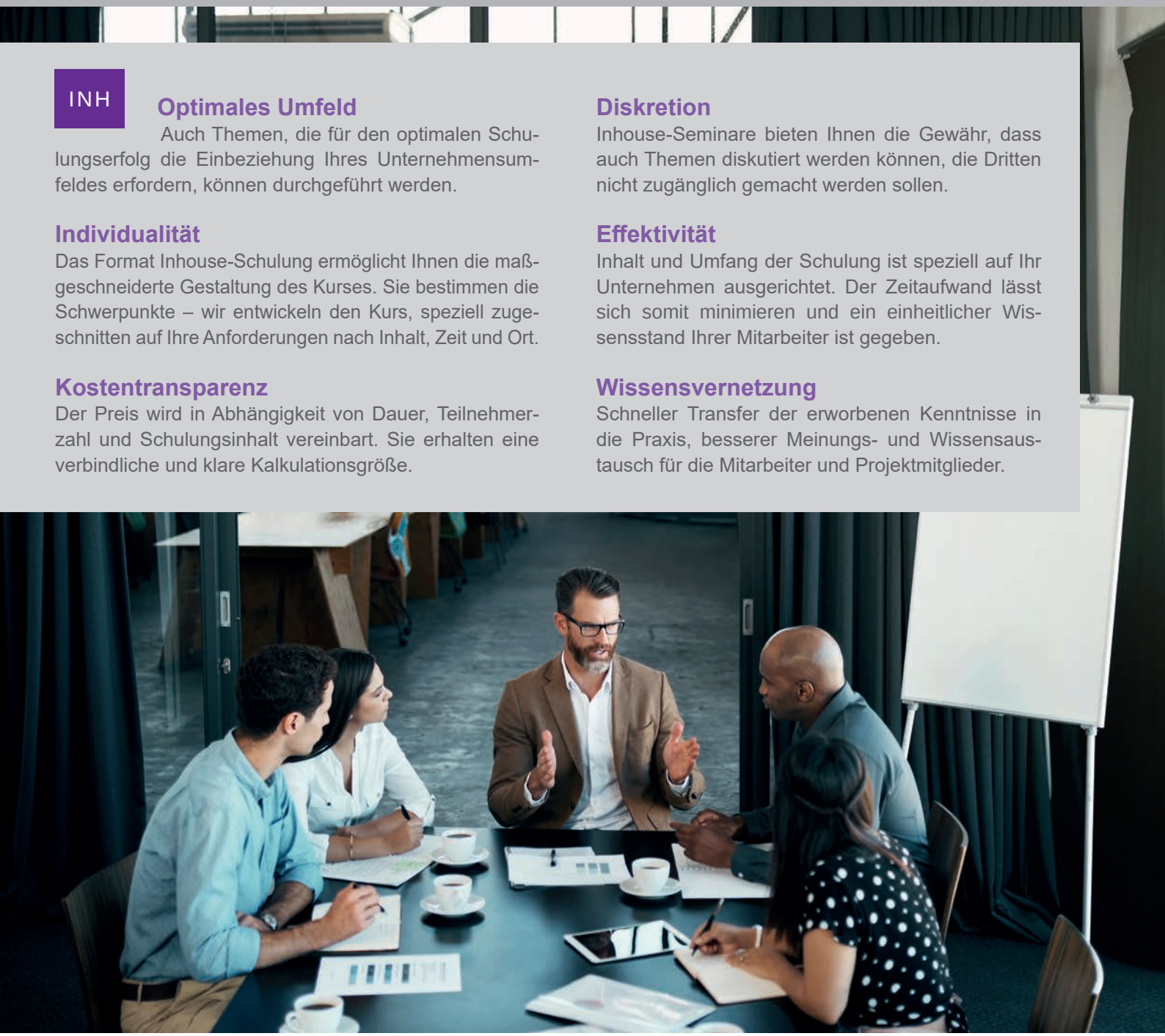
INH
INHOUSE-SCHULUNGEN

ComConsult GmbH
Beratung + Planung + Schulung

INHOUSE-SCHULUNGEN

IT-TRAINING NACH MASS

BUSINESS SKILLS / SOFTSKILLS| CLOUD UND DATA CENTER | FUNKNETZE | IOT / SMART TECHNOLOGIES | IT-INFRASTRUKTUREN | IT-MANAGEMENT | IT-RECHT | IT-SICHERHEIT | KI / DATA SCIENCE / MACHINE LEARNING | NETZE | SOFTWARE | UC / IT-ENDGERÄTE



INH

Optimales Umfeld

Auch Themen, die für den optimalen Schulungserfolg die Einbeziehung Ihres Unternehmensumfeldes erfordern, können durchgeführt werden.

Individualität

Das Format Inhouse-Schulung ermöglicht Ihnen die maßgeschneiderte Gestaltung des Kurses. Sie bestimmen die Schwerpunkte – wir entwickeln den Kurs, speziell zugeschnitten auf Ihre Anforderungen nach Inhalt, Zeit und Ort.

Kostentransparenz

Der Preis wird in Abhängigkeit von Dauer, Teilnehmerzahl und Schulungsinhalt vereinbart. Sie erhalten eine verbindliche und klare Kalkulationsgröße.

Diskretion

Inhouse-Seminare bieten Ihnen die Gewähr, dass auch Themen diskutiert werden können, die Dritten nicht zugänglich gemacht werden sollen.

Effektivität

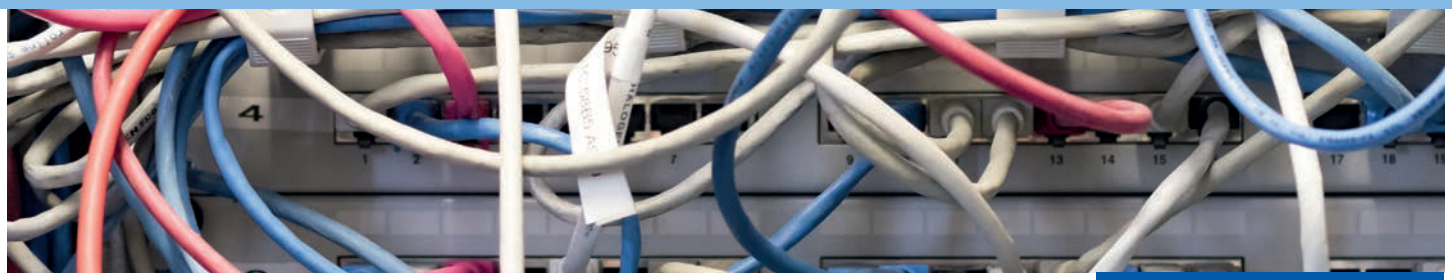
Inhalt und Umfang der Schulung ist speziell auf Ihr Unternehmen ausgerichtet. Der Zeitaufwand lässt sich somit minimieren und ein einheitlicher Wissensstand Ihrer Mitarbeiter ist gegeben.

Wissensvernetzung

Schneller Transfer der erworbenen Kenntnisse in die Praxis, besserer Meinungs- und Wissensaustausch für die Mitarbeiter und Projektmitglieder.

Zertifizierungen

ComConsult Certified Network Engineer



Lokale Netze für Einsteiger
02.03.-06.03.26 Aachen
07.09.-11.09.26 Aachen

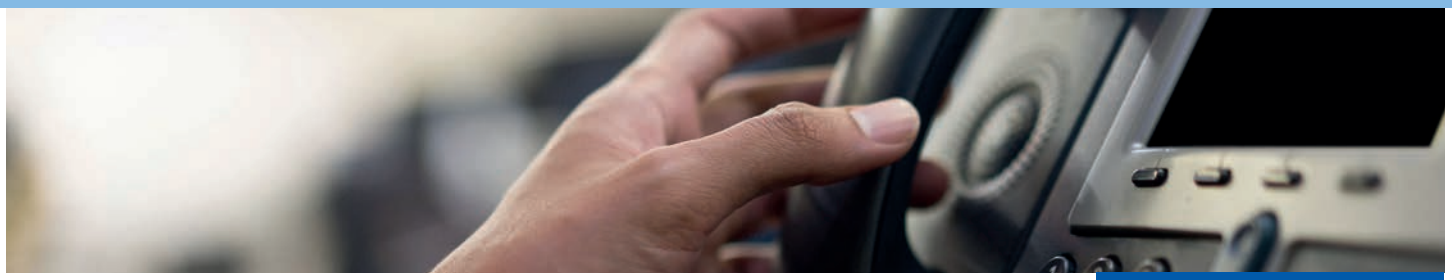
TCP/IP-Netze erfolgreich betreiben
05.05.-07.05.26 Aachen
03.11.-05.11.26 Aachen

Switching und Routing: Optimales Netzdesign
21.04.-24.04.26 Aachen
06.10.-09.10.26 Aachen

Paketpreis für alle drei Seminare:

€ 6.273,--* statt € 6.970,--

ComConsult Certified Voice Engineer



Unified Communications – von Grundlagen über Planung bis Umsetzung
10.03.-12.03.26 Aachen
23.06.-25.06.26 Aachen
03.11.-05.11.26 Aachen

SIP: Basistechnologie für VoIP und IP-Telefonie
21.04.-22.04.26 Aachen
24.11.-25.11.26 Aachen

Sicherheitsmaßnahmen für VoIP und UCC
05.05.-07.05.26 Aachen
08.12.-10.12.26 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.

Die Autoren

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

Felix Gilleßen ist seit 2017 Mitarbeiter im Competence Center Netze der ComConsult GmbH. Er unterstützt unter anderem bei Netzwerkplanungen und Konzepten, ist für die Konfiguration von Netzwerkkomponenten zuständig und begleitet die Inbetriebnahme und Umzüge von Netzwerken (Migration, Rollout, Patching). Ein weiterer Schwerpunkt seiner Arbeit liegt in der Durchführung von WLAN-Planungen und -Messungen.
Kontakt: gillessen@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

Steffen Moll ist Coach und Trainer mit Leib und Seele. Der zertifizierte (Online-)Trainer begeistert mit inspirierenden Denkanstößen und Übungen. Seine Überzeugung: „Zum Dichter wird man geboren. Zum Redner wird man gemacht“. Zum Beispiel in seinen Trainings. Steffen Moll hat einen Master in Marketing und die Erfahrung aus unzähligen Präsentationen für Unternehmen, Videos und Vorträgen. Offline, online und hybrid. Neben Gruppen-Trainings ist er auch YouTuber, TEDx Speaker-Coach sowie Moderator der GABAL Webtalks.

Michael Schneiders kann bis heute auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Mitarbeiter des Competence Center Rollout und Betrieb der ComConsult GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Implementierung von LAN- und WLAN-Infrastrukturen gesammelt.
Kontakt: schneiders@comconsult.com

Dr. Joachim Wetzlar ist seit mehr als 30 Jahren Senior Consultant der ComConsult GmbH. 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 und Cloudinfrastrukturen beschäftigt.
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