April 2025

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

KI-Manager – Skills für die Zukunft

von Laura Bies

In den letzten Jahren haben Large Language Models (LLMs) eine bemerkenswerte Evolution durchlaufen, die einen fundamentalen Wandel in der technologischen Landschaft markiert.

Seite 8

Neues Kompendium des BSI zur Absicherung organisationsinterner Telekommunikation

von Leonie Herden, Dr. Simon Hoff und Gaby van Laak

Seite 26

SD-WAN: Von Ausnahme zur Regel?

von Dr. Behrooz Moayeri

In einem Beitrag vom November 2024 habe ich mich dazu geäußert, in welchen Szenarien ein Software-Defined Wide Area Network (SD-WAN) sinnvoll ist. Auf den Punkt gebracht: SD-WAN bietet sich genau dort an, wo es im Vergleich zu klassischen Verfahren für Standort-Vernetzung mit entscheidenden Vorteilen hinsichtlich Verfügbarkeit, Leistungsfähigkeit, Flexibilität und Wirtschaftlichkeit verbunden ist.

Seite 2

Softwareeinkauf: Strategischer Erfolgsfaktor der digitalen Transformation

von Volker Lopp

Die digitale Transformation stellt Unternehmen vor immer komplexere Herausforderungen – insbesondere im strategischen Softwareeinkauf. Anders als bei der Hardwarebeschaffung müssen Unternehmen beim Softwareeinkauf deutlich vielschichtigere Aspekte berücksichtigen.

Seite 17

Webinar der Woche

Was stimmt hier nicht? Wolken über dem IT-Support

Seite 22

WPA3 – doch komplizierter als ursprünglich gedacht!

von Dr. Joachim Wetzlar

WPA3 ist inzwischen ein alter Hut, so sollte man meinen. Bereits 2018 habe ich über WPA3 in [1] berichtet, und mein Kollege Stephan Bien hat 2021 ein Webinar dazu gehalten. Nun, da es ein alter Hut ist, könnte ich ja mein WLAN im Homeoffice auf WPA3 umstellen – dachte ich mir.

Seite 23

SD-WAN: Von Ausnahme zur Regel?

von Dr. Behrooz Moayeri

In einem Beitrag vom November 2024 habe ich mich dazu geäußert, in welchen Szenarien ein Software-Defined Wide Area Network (SD-WAN) sinnvoll ist. Auf den Punkt gebracht: SD-WAN bietet sich genau dort an, wo es im Vergleich zu klassischen Verfahren für Standort-Vernetzung mit entscheidenden Vorteilen hinsichtlich Verfügbarkeit, Leistungsfähigkeit, Flexibilität und Wirtschaftlichkeit verbunden ist.

Braucht man überhaupt noch ein WAN?

Bevor ich auf die Gegenüberstellung von SD-WAN und klassischen WAN-Lösungen wie Multi-Protocol Label Switching (MPLS) eingehe, möchte ich auf eine Frage hinweisen, die in unserer Projektpraxis wiederholt aufgeworfen wird. Diese Frage lautet: Was ist der Unterschied zwischen Standorten eines Unternehmens und Homeoffices? Warum können für den Zugriff auf zentrale IT-Ressourcen nicht alle Arbeitsplätze dieselbe Lösung nutzen, unabhängig davon, ob es sich um Standorte einer Organisation oder Homeoffices ihrer Beschäftigten handelt? Auf Anhieb fällt einem diese Replik ein: Nicht alles an Arbeit ist vom Homeoffice aus zu leisten. Von der Fabrik bis zum Krankenhaus gibt es noch viele Arbeitsstätten, an denen Vor-Ort-Präsenz von Personal unerlässlich ist. An solchen Standorten müssen Maschinen und Dinge, Computer und Menschen interagieren. Diese Interaktion erfordert Lösungen über die direkte Internet-Verbindung jedes Endgerätes hinaus.

Standortvernetzung beschränkt sich nicht auf Arbeitsstätten, in denen die Natur der Beschäftigung die körperliche Präsenz des Personals erfordert. Auch einige reine Büroumgebungen müssen Anforderungen erfüllen, die es in Homeoffices nicht gibt. Zum Beispiel können in einem Bürogebäude verschiedene Gruppen von Endgeräten betrieben werden, die sich hinsichtlich ihrer Nutzungsart, ihrer Kommunikationsbeziehungen und ihres Schutzbedarfs unterscheiden. Typischerweise baut man an einem Unternehmensstandort verschiedene physisch oder virtuell (logisch) getrennte Netze, mit denen Endgeräte verschiedener Gruppen verbunden werden. Damit die Zuordnung eines Endgeräts zu einer Gruppe automatisch erfolgt, benötigt man an einem Firmenstandort Network Access Control (NAC). Das alles ist im Homeoffice nicht erforderlich. Das Local Area Network (LAN) ist daher in einer Liegenschaft des Unternehmens komplexer als das Netz im Homeoffice. Gleiches gilt für die WAN-Anbindung des Firmenstandorts.

Defizite klassischer WAN-Lösungen

SD-WAN kann einige Defizite klassischer Lösungen beheben. Eine MPLS-Lösung ist mit folgenden Nachteilen verbunden:

- Internationale MPLS-Lösungen sind in der Regel sehr teuer. Im Vergleich dazu kann SD-WAN wirtschaftlicher sein, wenn als Basis (Underlay) des SD-WAN das Internet genutzt wird, das als ein und dasselbe internationale Netz überall auf der Erde existiert.
- Eine MPLS-Plattform wird fast immer von einem Provider betrieben, dem auch Fehler unterlaufen können, die trotz kanten- und knotendisjunkter Wegeführung zum Ausfall einer Standortanbindung führen. Dagegen kann ein SD-WAN mit Provider-Diversität kombiniert werden.
- Verschlüsselung von Datenströmen muss in einem klassischen MPLS-Netz als separate Lösung betrieben werden, während im SD-WAN in der Regel Datenströme verschlüsselt werden.
- Viele MPLS-Lösungen haben nur wenige, wenn nicht sogar nur einen zentralen Übergang zum Internet und zum Zugriff auf externe Clouds, Backhauling genannt. Insbesondere bei internati-

KI-Manager – Skills für die Zukunft

von Laura Bies

In den letzten Jahren haben Large Language Models (LLMs) eine bemerkenswerte Evolution durchlaufen, die einen fundamentalen Wandel in der technologischen Landschaft markiert. Führende Modelle wie GPT-4o von OpenAI und vergleichbare KI- Systeme wie Claude 3.5 Sonnet von Anthropic haben nicht nur die theoretischen Grenzen des Machbaren verschoben, sondern auch konkrete Veränderungen in der Geschäftswelt und gesellschaftlichen Wahrnehmung bewirkt. Besonders der Mittelstand profitiert von dieser technologischen Revolution, da LLMs als vielseitige Werkzeuge weit über die reine Text- und Bildgenerierung hinausgehen. Sie fungieren als strategische Partner bei der Prozessoptimierung, Kostensenkung und Effizienzsteigerung. Vergleichbar mit einem digitalen Schweizer Taschenmesser bieten sie eine breite Palette an Funktionen, die sich nahtlos in bestehende Geschäftsabläufe integrieren lassen.

Die Evolution der generativen KI von einfachen Textgeneratoren zu hochkomplexen Sprachmodellen spiegelt sich eindrucksvoll in Systemen wie GPT-4o wider. Sie beherrschen nicht nur die Kunst der menschenähnlichen Konversation und Textproduktion, sondern exzellieren auch in technischen Bereichen wie der Programmierung und wissenschaftlichen Dokumentation. Ihre analytischen Fähigkeiten erstrecken sich über ein breites Spektrum: Sie führen präzise Datenanalysen durch, decken komplexe Zusammenhänge auf und generieren wertvolle neue Erkenntnisse. In der strategischen Planung unterstützen sie Unternehmen durch zukunftsweisende Innovations- und Prognosemodelle, während ihre kontextbezogenen Analysen und Empfehlungen intelligente Entscheidungsprozesse ermöglichen.

Darüber hinaus glänzen moderne LLMs mit beeindruckenden multimodalen Fähigkeiten: Sie übersetzen mühelos zwischen verschiedenen Sprachen, generieren und analysieren realitätsnahe Bilder wie Flux 1.1 von Blackforest Labs und erreichen beinahe ein menschliches Niveau in natürlichen Konversationen wie mit dem Advanced Voice Mode von ChatGPT. Ihre Expertise erstreckt sich auch auf die Erkennung und Verarbeitung von Audio- und Videoinhalten wie bei Sora Turbo von OpenAI, die Automatisierung komplexer Workflows sowie die Unterstützung kreativer Prozesse in Design und Content-Erstellung. In der technischen Dokumentation und im Projektmanagement optimieren sie Arbeitsabläufe durch automatische Zusammenfassungen, Kategorisierungen und die Extraktion relevanter Informationen aus großen Datensätzen. Diese Systeme haben sich zu unverzichtbaren Werkzeugen entwickelt, die nicht nur operative Prozesse optimieren, sondern auch strategische Entscheidungsfindung in einer Zeit der digitalen Transformation auf ein neues Niveau heben. Ihre Fähigkeit, große Datenmengen zu verarbeiten und daraus wertvolle Erkenntnisse zu gewinnen, macht sie zu einem Katalysator für Innovation und Wettbewerbsfähigkeit in der modernen Geschäftswelt.

Aus eben diesen aufgeführten Gründen ist es essenziell für Unternehmen, ihre Mitarbeitenden zu effektiven „KI-Managern“ ausbilden zu lassen. Als KI-Manager bezeichnen wir hier eine Person, die in der Lage ist, mit verschiedenen KI-Tools zusammenzuarbeiten, um deren Potenzial für Effizienzsteigerung, Automatisierung und Innovation optimal für sich oder ihr Unternehmen zu nutzen. Was macht einen effektiven KI-Manager aus? Relevante Kriterien und Fähigkeiten teilen sich in folgende acht Kategorien auf: Wissen, Datenkompetenz, kritische Denk- und Analysefähigkeit, Kommunikationsfähigkeit, Prompt-Engineering, Erfahrung, Kreativität und Anpassungs- und Lernfähigkeit.

Softwareeinkauf: Strategischer Erfolgsfaktor der digitalen Transformation

von Volker Lopp

Die digitale Transformation stellt Unternehmen vor immer komplexere Herausforderungen – insbesondere im strategischen Softwareeinkauf. Anders als bei der Hardwarebeschaffung müssen Unternehmen beim Softwareeinkauf deutlich vielschichtigere Aspekte berücksichtigen: von komplexen Lizenzmodellen über langfristige Wartungsvereinbarungen bis hin zu potenziellen Herstellerabhängigkeiten. Ein professionell aufgesetzter Softwareeinkauf wird damit zum entscheidenden Erfolgsfaktor für die digitale Zukunftsfähigkeit von Unternehmen.

Die Grundlage jeder erfolgreichen Softwarebeschaffung bildet eine fundierte Bedarfsanalyse. Hier gilt es, die tatsächlichen Anforderungen des Unternehmens herstellerneutral zu spezifizieren. Allzu oft werden Anforderungen bereits auf bestimmte Produkte oder Hersteller zugeschnitten, was die späteren Auswahl- und Verhandlungsmöglichkeiten drastisch einschränkt. Ein professionelles Lastenheft sollte die funktionalen und technischen Anforderungen präzise, aber lösungsneutral beschreiben. Besonderes Augenmerk verdienen dabei die langfristigen Aspekte wie Skalierbarkeit, Integration in die bestehende Systemlandschaft und künftige Entwicklungsmöglichkeiten.

Die Total-Cost-of-Ownership-Analyse über einen Planungshorizont von mindestens 10 Jahren bildet die Grundlage für fundierte Investitionsentscheidungen. Dabei müssen sowohl externe Kosten wie Lizenzen, Implementation und Wartung als auch interne Aufwände für Schulung, Migration und Betrieb berücksichtigt werden. Moderne Lizenzmodelle ermöglichen dabei eine flexiblere Anpassung der Kosten an den tatsächlichen Geschäftsnutzen: Nutzungsbasierte Abrechnungen oder transaktionsabhängige Modelle erlauben eine dynamische Kostenentwicklung entsprechend der tatsächlichen Nutzungsintensität.

Die Herstellerkosten für eine weitere Softwarekopie liegen praktisch bei null, während die Gewinnmargen der Hersteller bis zu 40 % betragen. Dies eröffnet substanzielle Verhandlungsspielräume. Diese müssen jedoch strategisch genutzt werden. Erfahrene Einkäufer orientieren sich an den Verkaufszyklen der Anbieter: Zum Quartals- oder Geschäftsjahresende sind häufig deutlich bessere Konditionen erreichbar. Mehrjährige Vereinbarungen, Volumenversprechen oder die Positionierung als Referenzkunde können weitere Verhandlungshebel darstellen. Eine detaillierte Marktanalyse und die Evaluation mehrerer Anbieter schaffen die Basis für erfolgreiche Verhandlungen. Nach der Auswahl eines Anbieters entsteht oft eine brutal hohe Abhängigkeit – umso wichtiger ist es, bereits bei der Auswahl die Perspektiven und Ausbaustufen zu berücksichtigen.

Vertragsgestaltung und Risikomanagement bilden weitere zentrale Erfolgsfaktoren. Moderne Softwareverträge müssen klare Regelungen zu Nutzungsrechten, Wartungsumfang, Service-Levels und geografischen Nutzungsbeschränkungen enthalten. Bei Cloud-Lösungen sind zusätzlich Aspekte wie Datenschutz, Verfügbarkeit und Exit Management zu regeln. Eine sorgfältige Vertragsgestaltung minimiert spätere Risiken und schafft Planungssicherheit für beide Seiten.

Die Wartungsvereinbarungen haben besondere strategische Be-

WPA3 – doch komplizierter als ursprünglich gedacht!

von Dr. Joachim Wetzlar

WPA3 ist inzwischen ein alter Hut, so sollte man meinen. Bereits 2018 habe ich über WPA3 in [1] berichtet, und mein Kollege Stephan Bien hat 2021 ein Webinar dazu gehalten [2]. Nun, da es ein alter Hut ist, könnte ich ja mein WLAN im Homeoffice auf WPA3 umstellen – dachte ich mir. Wohlgemerkt, es geht um WLAN mit Pre-Shared Key (PSK), wie es die meisten von Ihnen zu Hause einsetzen werden. Doch auch in vielen Unternehmen werden WLANs mit PSK abgesichert.

Gesagt, getan. Und schon tauchte die erste Schwierigkeit auf: Bei der Konfiguration (ich nutze die Cloud-Lösung eines bekannten Netzwerk-Ausrüsters) war die Entscheidung zwischen „HNP“ oder „H2E“ oder einer Kombination aus beidem zu fällen. Was sollte ich wählen?

Dazu musste ich erst einmal lesen, und zwar meinen eigenen Standpunkt [1]. Das Neue an WPA3 ist insbesondere die erhöhte Sicherheit der „Personal“-Varianten von WPA, d.h. der Varianten mit PSK. Bei WPA2 wird im Rahmen des sogenannten 4-Wege-Handshakes Schlüsselmaterial ausgetauscht, das aus dem PSK abgeleitet wurde. Schneidet ein Angreifer diesen Austausch mit, kann er anschließend z. B. mittels eines Wörterbuchs in Ruhe ausprobieren, ob eines der Wörter genau dieses Schlüsselmaterial ergibt. Sobald er den PSK gefunden hat, kann der Angreifer anschließend allen aufgezeichneten WLAN-Verkehr entschlüsseln.

WPA3 setzt eine zusätzliche Authentisierung vor den 4-Wege-Handshake. Über ein Hash-Verfahren mittels Elliptischer Kurven ermitteln Access Point und Client aus den PSKs ein sogenanntes Passwort-Element (PWE), das anstelle des PSK im nachfolgenden 4-Wege-Handshake verwendet wird. Der Algorithmus zur Ermittlung des PWEs heißt „Dragonfly“ und wurde in RFC 7664 publik gemacht. Bei WPA3 heißt das Verfahren „Simultaneous Authentication of Equals“ (SAE). SAE soll robust gegen Wörterbuch-Attacken sein.

Doch wie schon des Öfteren in Zusammenhang mit WLAN, haben auch hier findige Köpfe Schwächen entdeckt. In [3] beschreiben die Autoren mehrere Schwachstellen von WPA3-SAE. Zugegeben, die Mathematik der Kryptographie ist mir zu hoch, um sie zu verstehen. Etwas verständlicher ist die Veröffentlichung [4].

Nur so viel: Eine der Schwachstellen basiert darauf, dass SAE das Passwort-Element ursprünglich mit einer Iteration namens „Hunting-and-Pecking“ (HNP) berechnet. Die Antwortzeit eines Access Point auf die Authentisierungs-Anfrage des Clients hängt davon ab, wie oft die Iteration durchlaufen wird. Ein Angreifer bestimmt im Rahmen einer Wörterbuch-Attacke die Antwortzeiten für Gruppen von PSKs und vergleicht sie mit der Antwortzeit, die ein authentisierter Client erlebt.

Die genannte Schwäche des HNP wird durch ein neues Verfahren vermieden, bei dem das Passwort-Element durch einen direkten Hash entsteht. Es wird als „Hash-to-Element“ (H2E) bezeichnet. In IEEE 802.11-2020 sind entsprechende Definitionen bereits vorhanden. Insbesondere kann ein Access Point den Clients im Beacon Frame mitteilen, ob er eine SAE-Authentisierung mit H2E erwartet.

Neues Kompendium des BSI zur Absicherung organisationsinterner Telekommunikation

von Leonie Herden, Dr. Simon Hoff und Gaby van Laak

Am 05.03.2025 war es so weit: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte das „Kompendium für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf (KomTK)“, siehe [1]. Vor etwas mehr als 10 Jahren hatten wir im Netzwerk Insider einen Artikel, der ausgesprochen ähnlich anfing (siehe [2]). Damals wurde die „Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ (TLSTK II, siehe [3]) des BSI vorgestellt, und die TLSTK II hat jetzt mit KomTK einen Nachfolger bekommen. Gleichzeitig löst KomTK auch das „Kompendium Videokonferenzsysteme“ des BSI (siehe [4]) ab, dessen Inhalte hier auch aktualisiert mit einfließen.

Die organisationsinterne Telekommunikation nutzt die gesamte verfügbare Palette von modernen Anwendungs-, Dienst- und Kommunikationsplattformen. Dadurch entsteht eine übergreifende ganzheitliche Architektur, die durch folgendes Zitat aus KomTK sehr treffend beschrieben wird: „Ein Telekommunikationssystem ist hier quasi in der Rolle einer Spinne in der Mitte eines großen Netzes von Anwendungen und Systemen zu sehen“ (siehe [5]). Doch was bedeutet dies nun für die Informationssicherheit? Ein sicherheitsrelevantes Ereignis kann über das reine Telekommunikationssystem hinaus im gesamten „Spinnennetz“ eine erhebliche Wirkung entfalten. Dies muss entsprechend in der Informationssicherheit berücksichtigt werden. Dabei spielen auch weitere Aspekte eine Rolle, die sich aus dem Einsatz von Cloud Computing, Mobile Computing, Künstlicher Intelligenz (KI) und Internet of Things (IoT) in der organisationsinternen Telekommunikation ergeben. Bedenkt man nun noch, dass bei Telekommunikation oft erhöhter Schutzbedarf vorliegt, kumuliert sich dies zu einer besonderen Risikolage für die Informationssicherheit.

KomTK (siehe [5]) ist in drei Teile aufgeteilt, die im Folgenden genauer vorgestellt werden:

- Teil 1 - Gefährdungen, Anforderungen und Umsetzungshinweise
- Teil 2 - Beispiele für Sicherheitskonzepte
- Teil 3 - Beschaffungsleitfaden

Teil 1 - Gefährdungen, Anforderungen und Umsetzungshinweise

KomTK Teil 1 beschreibt die in der modernen Telekommunikation eingesetzten Techniken und deren Nutzung, analysiert die Gefährdungen und leitet auf Basis des IT-Grundschutz-Kompendiums des BSI entsprechende Anforderungen ab, deren Umsetzungsmöglichkeiten dann genauer beschrieben werden. Dabei wird der gesamte Lebenszyklus eines Telekommunikationssystems von Planung und Beschaffung über Betrieb und Revision bis zur Außerbetriebnahme adressiert.

Die Struktur vom KomTK orientiert sich an einem Haus (siehe Abbildung 1), dessen Etagen die verschiedenen Bestandteile der or-