November 2024

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Erhöhte RZ-Verfügbarkeit – aktuelleres vom BSI

von Oliver Flüs
„Die Informationssicherheit“ ist ein wichtiger Stakeholder, den RZ-Planer und -Betreiber berücksichtigen müssen. Wie helfen aktuelle BSI-Veröffentlichungen, mit konkretem Bedarf und konkreten Rahmenbedingungen sinnvoll umzugehen?

Seite 11

Künstliche Intelligenz im Contact Center

von Nils Wantia
Kaum ein Technologiethema bewegt die Welt derzeit so sehr wie die Künstliche Intelligenz. Das geht mittlerweile seit Jahren so, und wir haben uns inzwischen an das dazugehörige Buzzword-Bingo gewöhnt: Häufig wird der Begriff der Künstlichen Intelligenz auf alles Neue und Beeindruckende angewendet, um mehr Aufmerksamkeit zu erregen.

Seite 29

Ist Netzmanagement aus der Cloud sinnvoll?

von Dr. Behrooz Moayeri
Der Cloud-Hype hat längst auch die Netzsparte erfasst. Einige Hersteller von Netztechnologie wollen ihre Kunden für das Netzmanagement aus der Cloud gewinnen. Einige Produkte kann man nur mit einem Cloud-basierenden Management betreiben. Ist damit die Zeit für OnPrem-Lösungen im Bereich Netzmanagement abgelaufen? Wird Cloud-based Management bald unumgänglich?

Seite 2

GA-IT-Infrastruktur – Nachrüsten und Modernisierung der Gebäudeautomation gemäß GEG und EPBD

von Dr. Andreas Kaup
Die gesetzlichen Anforderungen für Klimaschutz im Gebäudesektor steigen. Die zeitlichen Zielvorgaben in Deutschland und der EU werden mit ausschließlich baulichen Maßnahmen kaum umsetzbar sein.

Seite 33

Webinar der Woche

Berücksichtigung PoE-basierter Stromversorgung in der Infrastrukturplanung

Seite 25

Spectre nach fast 7 Jahren und kein Ende in Sicht

von Dr. Markus Ermes
Anfang 2018 schien das Ende der IT gekommen: Mit Spectre und Meltdown wurden zwei Schwachstellen in modernen Prozessoren gefunden, die ihre Ursache in den Chips selbst hatten und sich nicht mit dem x-ten Windows-Update beheben ließen.

Seite 26

Ist Netzmanagement aus der Cloud sinnvoll?

von Dr. Behrooz Moayeri

Der Cloud-Hype hat längst auch die Netzsparte erfasst. Einige Hersteller von Netztechnologie wollen ihre Kunden für das Netzmanagement aus der Cloud gewinnen. Einige Produkte kann man nur mit einem Cloud-basierenden Management betreiben. Ist damit die Zeit für OnPrem-Lösungen im Bereich Netzmanagement abgelaufen? Wird Cloud-based Management bald unumgänglich?

Wo Cloud-Lösungen sinnvoll sind

Ungeachtet der Motive der Hersteller, die auf Cloud-Lösungen für Netzmanagement setzen, sind solche Lösungen in bestimmten Szenarien sinnvoll. Denken Sie zum Beispiel an eine kommunale Verwaltung, die Schulen mit dem Internet verbinden muss. Die Netze der Schulen müssen dabei aus Sicherheitsgründen vom internen Verwaltungsnetz getrennt sein. In den Schulen werden WLAN Access Points und Switches genutzt. Diese sollen zentral verwaltet werden. In diesem Beispiel ist Cloud-basierendes Management durchaus sinnvoll. Denn sonst hätte man einen großen Aufwand, eine zentrale Management-Lösung mit einer Vielzahl von Netzen zu verbinden, die zwar mit dem Internet verbunden, jedoch vom internen Netz der kommunalen Verwaltung getrennt sind. Mit Cloud-based Management greift der kommunale Administrator auf eine Lösung in der öffentlichen Cloud des Herstellers der Netzkomponenten zu. Darüber sind die Netzkomponenten der Schulen administrierbar.

Es gibt etliche Analogien zu diesem Beispiel. Ein weiterer Anwendungsfall ist eine Verwaltung auf der Ebene eines Bundeslandes, die eine Netzlösung mit Internet-Zugang in Heimen für Geflüchtete administrieren muss.

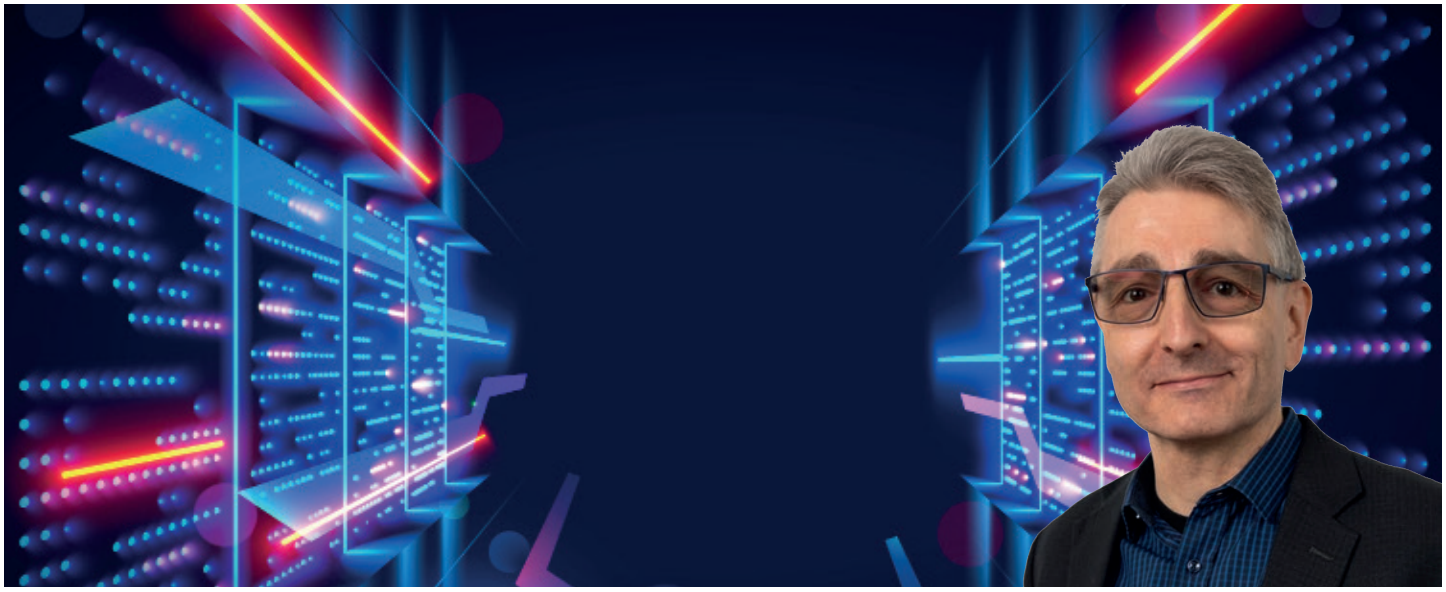
Auch in der Privatwirtschaft wird darüber nachgedacht, lokale Netze an Bürostandorten als Internet-Verlängerungen zu realisieren. Wenn die Endgeräte der Benutzer ohnehin zeitweise für mobiles Arbeiten genutzt werden sollen, kann man den Bürostandort quasi als großes Home Office behandeln. Die Maßnahmen zur Absicherung des Endgerätes sind angesichts der Nutzung unsicherer Netze in Home Offices und Service-Provider-betriebenen Umgebungen ohnehin erforderlich. Wenn immer mehr Büroapplikationen in öffentliche Clouds wandern, wird ein Schuh daraus. Der auf bestimmte Weise abgesicherte Zugriff auf Anwendungen im eigenen Rechenzentrum des Unternehmens wird auch möglich sein, jedoch bestimmt Cloud Computing als das überwiegende Nutzungsszenario die Gestaltung der Netzlösung.

Zusammengefasst gilt, dass das Cloud-basierende Netzmanagement immer dann interessant ist, wenn zentral eine Mehrzahl von lokalen Netzen zu betreiben ist, die mit dem Internet verbunden und von den internen Netzen einer Organisation getrennt sind.

Weitere Vorteile des Cloud-basierenden Netzmanagements

Neben der Möglichkeit der zentralen Administration von Netzen, die nur mit dem Internet und nicht mit dem internen Netz verbunden sein sollen, hat Cloud-basierendes Netzmanagement mit jeder anderen Software as a Service (SaaS) den Vorteil gemeinsam, dass der Netzadministrator von einigen aufwändigen Arbeiten entlastet wird, als da wären:

- Bereitstellung und Pflege einer Hardware, auf der die Netzmanagementlösung läuft
- Gegebenenfalls Betrieb einer Virtualisierungslösung für die Bereitstellung der für das Netzmanagement benötigten Virtuellen



Erhöhte RZ-Verfügbarkeit – aktuelleres vom BSI

von Oliver Flüs

„Die Informationssicherheit“ ist ein wichtiger Stakeholder, den RZ-Planer und -Betreiber berücksichtigen müssen. Wie helfen aktuelle BSI-Veröffentlichungen, mit konkretem Bedarf und konkreten Rahmenbedingungen sinnvoll umzugehen?

Maßnahmenlisten gemäß veralteter BSI-Grundschutzkataloge, speziell zum RZ-Baustein, die man früher abarbeiten konnte, sind abgelöst worden. Jetzt sind Anforderungen gemäß modernisiertem Grundschutz maßgeblich, siehe Grundschutzkompendium.

Den Bänden des BSI-HV-Kompendiums, die Architekturen, Maßnahmenempfehlungen usw. spezifiziert haben, ist es ähnlich ergangen. Sie wurden wegen Veralterung zurückgezogen und bedingt durch aktuellere BSI-Dokumente ersetzt. Zudem ist eine Benchmarking-Basis im Aufbau, die einen gestuften Umgang mit erhöhtem RZ-Sicherheitsbedarf erleichtern soll (HV-Kompendium, Kompaktversion dazu).

Was bietet das aktualisierte Angebot an Anforderungsspezifikationen und Arbeitshilfen des BSI? Wie ist dieses „BSI-konform“ in Zusammenhang mit technischen Standards, Normen und Vorschriften zu RZ-Ausstattung und RZ-relevanter Technik zu sehen?

Der vorliegende Artikel will zunächst das Verständnis für die aktuelle „BSI-Denke“ erleichtern. Die Abkehr von detaillierten BSI-Vorgaben zum „Wie“ und die verschiedenen Veröffentlichungen zum „Was wird erwartet“ sollen verstanden werden. Vom BSI vorgesehene größere Gestaltungsfreiheit bedeutet einen bedingten Wegfall von Rechtfertigungszwang bei der Lösungsauswahl zu Basis- und Standardschutz.

Die Herausforderung beim nachvollziehbaren, angemessenen Umgang mit erhöhtem Sicherheitsbedarf wird dadurch allerdings nicht geringer. Der Aspekt der Verhältnismäßigkeit wird durch die zunehmende Komplexität und Abhängigkeit von IT-Lösungsangeboten schwieriger zu bewerten. Der zugehörige Stand der vom BSI unter „RZ-Sicherheit und Hochverfügbarkeit“ herausgegebenen Dokumente und Hilfen ist entsprechend wissenswert. Er wird ebenfalls vorgestellt und aus Praxissicht eingeordnet.

BSI-Anforderungen an die RZ-Gestaltung – wozu?

Der Name sagt es klar und deutlich: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschäftigt sich schwerpunktmäßig mit Informationssicherheit. Wenn vor diesem Hintergrund BSI-Anforderungen an die Absicherung von Anwendungen, Systemen und Netzwerken erhoben werden, überrascht das niemanden.

Das BSI-IT-Grundschutzkompendium formuliert entsprechende Anforderungen in Form von Bausteinen, die nach einem Schichtenmodell organisiert sind. Passend zu den eben genannten Maßnahmen der Absicherung gibt es dabei unter anderem die Schichten APP, SYS und NET. Bei diesen Schichten dürfte auch für in die Grundschutz-Praxis Einsteigenden sofort „klar und deutlich“ sein, dass sich das BSI für eine Spezifikation von Anforderungen zuständig sieht.

IT-Sicherheit in der Gebäude-automation und Gebäudetechnik

Mit Dr. Andreas Kaup sprach Christiane Zweipfennig

Die IT-Sicherheit ist mit der ansteigenden Vernetzung von Geräten und Systemen zur entscheidenden Komponente geworden, um moderne Gebäude vor potenziellen Bedrohungen zu schützen. Planer, Errichter und Betreiber von Gebäuden sehen sich zunehmend damit konfrontiert, Maßnahmen für die IT-Sicherheit von neuen oder schon errichteten Systemen in der Gebäudeautomation und Gebäudetechnik zu entwickeln und umzusetzen.

Dr. Andreas Kaup ist im Competence Center Smart Technologis bei ComConsult tätig. Dort berät er Kunden zum Thema Smart Buildings. Zusammen mit den Kunden definiert er im Projekt die Nutzeranforderungen, konsultiert zum aktuellen Stand der Technik und erarbeitet Smart-Building-Konzepte, auf deren Basis die entsprechenden ComConsult Competence Center IT-Infrastruktur-Lösungen und -Konzepte entwickeln. Momentan erarbeitet er in mehreren Projekten IT-Sicherheitsrichtlinien und -konzepte für die Gebäudetechnik und Smart Buildings seiner Kunden, über die er in diesem Interview berichtet.

In den letzten Jahren hat das Thema IT-Sicherheit in der Gebäudetechnik und in der Gebäudeautomation an Bedeutung gewonnen. Warum?

> Vernetzte Gewerke erhöhen das Sicherheitsrisiko.

Während früher die einzelnen Gewerke eines Gebäudes Insellösungen waren, sind heute in einem Smart Building möglichst alle technischen Gewerke wie Heizung, Klima, Lüftung, Licht, Aufzüge und Sicherheitstechnik miteinander verknüpft und kommunizieren in der Regel auf der Automationsebene IP-basiert. Durch die erhöhte IP-Kommunikation und die wachsende Zahl an gewerkeübergreifenden Schnittstellen in der Gebäudetechnik und im Smart Building entstehen in der Theorie und in der Praxis vermehrt Einfallstore für Cyberverbrechen.

Welche Normen, Richtlinien und Regelwerke zur IT-Sicherheit sind für die Gebäudeautomation und die Gebäudetechnik relevant?

> Die Bedeutung der IT-Sicherheit scheint immer mehr in der GA-Branche anzukommen.

Im Jahr 2021 hat das Bundesamt für Sicherheit in der Informationstechnik im IT-Grundschutz-Kompendium die neuen Bausteine INF.13 und INF.14 veröffentlicht. Das Kompendium bildet zusammen mit den BSI-Standards die Basis für die Informationssicherheit in Organisationen und Unternehmen. Damit gab es erstmalig Bausteine zu Sicherheit im technischen Gebäudemanagement und in der Gebäudeautomation. Vermutlich haben die verschiedenen Branchenverbände dies zum Anlass genommen, auf der Grundlage dieser BSI-Bausteine als „Inspirationsquelle“ weitere IT-Si-

Spectre nach fast 7 Jahren und kein Ende in Sicht

von Dr. Markus Ermes

Anfang 2018 schien das Ende der IT gekommen: Mit Spectre und Meltdown wurden zwei Schwachstellen in modernen Prozessoren gefunden, die ihre Ursache in den Chips selbst hatten und sich nicht mit dem x-ten Windows-Update beheben ließen. Stattdessen musste der Microcode der CPUs aktualisiert werden. Dann kamen neue Ausprägungen von Spectre ans Licht, die wieder behoben wurden. Seitdem wurde es um diese Lücken still. Die befürchtete Sicherheits-Apokalypse blieb (glücklicherweise) aus. Spectre und Meltdown stellten sich als Sturm im Wasserglas heraus. Oder etwa nicht?

Spectre – eine kurze Wiederholung

Doch was genau war noch mal die Grundlage von Spectre? Ich hatte hierzu schon vor einiger Zeit einen ausführlichen Artikel geschrieben. Zur Wiederholung: Moderne Prozessoren können „raten“, in welche Richtung sich eine „Wenn-Dann“-Abfrage entwickelt und im Voraus ausrechnen, was dann passieren sollte. Dabei können Daten gelesen werden, die eigentlich nicht erreichbar sein sollten.

Der (bisherige) Fix

Genau an der oben beschriebenen Stelle setzte der erste Fix der CPU-Hersteller an: Die sog. „Indirect Branch Predictor Barrier“ (IBPB) soll verhindern, dass gelernte Vorhersagen weiter-geleitet werden.

Spectre zeigt sich wieder

Jedoch haben Forscher der ETH Zürich kürzlich herausgefunden, dass die IBPB nicht korrekt implementiert ist. Man kann sie umgehen und trotz allem auf Speicherbereiche zugreifen, die durch die IBPB gesperrt sein sollten. Der Angriff der Forscher ermöglichte nachweislich den Zugriff auf Daten eines anderen Prozesses als desjenigen, in dem die neue Spectre-Variante ausgenutzt wurde. Dabei stellten sie fest, dass die 12., 13. und 14. Intel-Core-Prozessorgenerationen, die 5. und 6. Intel-Xeon-Generation sowie Zen 2 von AMD angreifbar sind.

Und was jetzt?

Glücklicherweise haben sowohl Intel als auch AMD schon seit Längerem Updates bereitgestellt, die die neue Lücke schließen. Intel hat diese Updates im März dieses Jahres veröffentlicht, und AMD hat bereits Ende 2022 auf diese Lücke hingewiesen, mit einem Verweis, wie Betriebssystem- und Hypervisor-Entwickler damit umgehen können.

Wird die IT diesmal wirklich ihre Apokalypse erleben?

Vermutlich wird auch dieses Mal wieder relativ wenig passieren. Zur Einordnung: Es ist nach wie vor kein real durchgeführter Angriff bekannt, der auf Spectre und Meltdown basiert. Es existieren zwar viele Proof-of-Concepts, die hier ansetzen, doch muss man

Künstliche Intelligenz im Contact Center

von Nils Wantia

Kaum ein Technologiethema bewegt die Welt derzeit so sehr wie die Künstliche Intelligenz. Das geht mittlerweile seit Jahren so, und wir haben uns inzwischen an das dazugehörige Buzzword-Bingo gewöhnt: Häufig wird der Begriff der Künstlichen Intelligenz auf alles Neue und Beeindruckende angewendet, um mehr Aufmerksamkeit zu erregen.

Welche Technologie tatsächlich dahinter steckt, interessiert ohnehin kaum jemanden, und verraten muss man es ja auch nicht, ist schließlich alles geheim und neu. Oder auch nicht. Der Begriff der Künstlichen Intelligenz ist im allgemeinen Sprachgebrauch nicht wirklich definiert, warum also nicht auf den Hype-Zug aufspringen und von den Assoziationen profitieren?

Wenn es um konkrete Anwendungen geht, dreht sich die Diskussion allerdings häufig noch immer um Wunschdenken, Phantasie und Versprechen von künftigem Nutzen. Natürlich gibt es zahlreiche Meetings, Workshops, Projekte und mittlerweile in vielen Unternehmen auch Tests, Proofs of Concept, Testabos etc. pp. Man will schließlich nicht den Anschluss verpassen.

Doch was bedeutet das? Wie viele dieser Anwendungen sieht der durchschnittliche Angestellte davon in seinem Arbeitsalltag?

Meistens nicht so viele – jedenfalls nicht genug, um den anhaltenden Hype zu rechtfertigen. Zwar gibt es entsprechende Angebote, wie Microsofts Copilot, der Potenzial für spürbare Veränderungen hat, doch bislang wirkt es stellenweise eher unausgereift und ist zudem noch teuer. Daneben gibt es natürlich viele neue Webseiten, Apps und Services, sowohl von hippen Startups als auch von alten Bekannten, die jedoch in der Breite noch nicht angekommen sind.

Wer also nicht gerne zwischendurch mit den großen Sprachmodellen bzw. Large Language Models wie ChatGPT, Gemini, Llama und Konsorten spielt oder bereits einen Weg gefunden hat, sie produktiv zu nutzen, bleibt schnell als Beobachter am Rande des Geschehens zurück, mit mehr oder weniger Interesse am Thema.

Contact Center

Ein Bereich, in dem bereits einiges passiert und mit dem die meisten von uns - zumindest auf Kundenseite - regelmäßig Kontakt haben, ist der Kundenservice bzw. das Contact Center.

Im Contact Center liegen die Vorteile von KI-Anwendungen auf der Hand: In keinem anderen Bereich der Kommunikation lässt sich das kommerzielle Potenzial von Einsparungen derart gut nachvollziehen wie im Contact Center. Wenn zudem der Kundenservice verbessert wird, lohnt sich die Investition. Auf Kundenseite sind die Erwartungen häufig schon derart tief gesunken, dass man auch gerne bereit ist, sich mit einem Automaten abzugeben, da einem dann wenigstens zügig geholfen wird – sofern alles funktioniert. Man spricht hier von einem echten Win-Win und einem positiven Return of Invest.

Doch was kann Künstliche Intelligenz in dem Bereich überhaupt leisten? Ich möchte in der Folge einige Beispiele skizzieren. Was dabei unter den KI-Begriff fällt und was nicht, unterliegt dabei – ganz im Sinne des Zeitgeistes – keiner festen Definition oder zugrunde liegenden Technologie.

Künstliche Gesprächspartner

Das offensichtlichste Beispiel für Künstliche Intelligenz im Contact

GA-IT-Infrastruktur – Nachrüsten und Modernisierung der Gebäudeautomation gemäß GEG und EPBD

von Dr. Andreas Kaup

Die gesetzlichen Anforderungen für Klimaschutz im Gebäudesektor steigen. Die zeitlichen Zielvorgaben in Deutschland und der EU werden mit ausschließlich baulichen Maßnahmen kaum umsetzbar sein. Der große Hebel der technischen Möglichkeiten muss genutzt werden. Auf EU-Ebene gibt der Green Deal Klimaneutralität bis 2050 vor. In Deutschland definiert das Bundesministerium für Wirtschaft und Klimaschutz für 2045 den Anspruch auf Klimaneutralität. Dabei gilt das Zwischenziel, bis 2030 die Treibhausgasemission um 55 % im Vergleich zum Verbrauch von 1990 zu reduzieren. Teilweise gilt auf Länderebene, wie auch bei vielen Unternehmen, bereits das Jahr 2030 als Zieldatum für einen klimaneutralen Gebäudebestand. Ein Ziel, das vorraussichtlich nur mit Systemen für die Gebäudeautomatisierung und -steuerung sowie ergänzenden PropTech-Lösungen [1] realisierbar sein wird.

Die Gebäudeenergiegesetz-Novelle 2024 (GEG 2024) definiert erstmalig technische und terminliche Vorgaben bezüglich des Einsatzes von Gebäudeautomationssystemen in Deutschland. Die Einführung des neuen Paragrafen hat ihren Ursprung in der EU-Gebäuderichtline (European Performance of Building Directive, EPBD). Somit muss jetzt schon darauf geschaut werden, was in der EPBD-Novelle 2024 gefordert wird, um sowohl den diesjährigen als auch den zukünftigen Vorgaben an die Gebäudeautomation gerecht zu werden.

Das übergeordnete Ziel von GEG und EPBD ist es, die Energieeffizienz von Gebäuden zu erfassen und zu verbessern, wobei dieser Artikel sich nur auf die technischen Vorgaben zur Effizienzsteigerung konzentriert. Für die Bewertung der Energieeffizienz wird auf die GA-Effizienzklassen gemäß ISO 52120, den Automationsgrad gemäß DIN V 18599 und den Intelligenzfähigkeitsindikator eingegangen.

Grundlegende Informationen vorab

Die EU-Gebäuderichtline spielt eine entscheidende Rolle im „Fit for 55“-Ziel der Europäischen Union und wird in jeder Legislaturperiode fortgeschrieben. Sobald eine Novelle das EU-Parlament passiert und anschließend Zustimmung durch den Europäischen Rat erfährt, haben die EU-Staaten 24 Monate Zeit, um die EU-Richtlinie in nationales Recht umzusetzen.

Am 12. April 2024 hat der Europäische Rat der EPBD-Novelle final zugestimmt, womit die EU-Staaten nun zwei Jahre Zeit haben, die neuen Vorgaben umzusetzen.

Das jetzige Gebäudeenergiegesetz (GEG 2024) basiert noch nicht auf der zuvor erwähnten EPBD-Novelle, sondern auf der EPBD von 2018. Es wurde am 16.10.2023 beschlossen und im