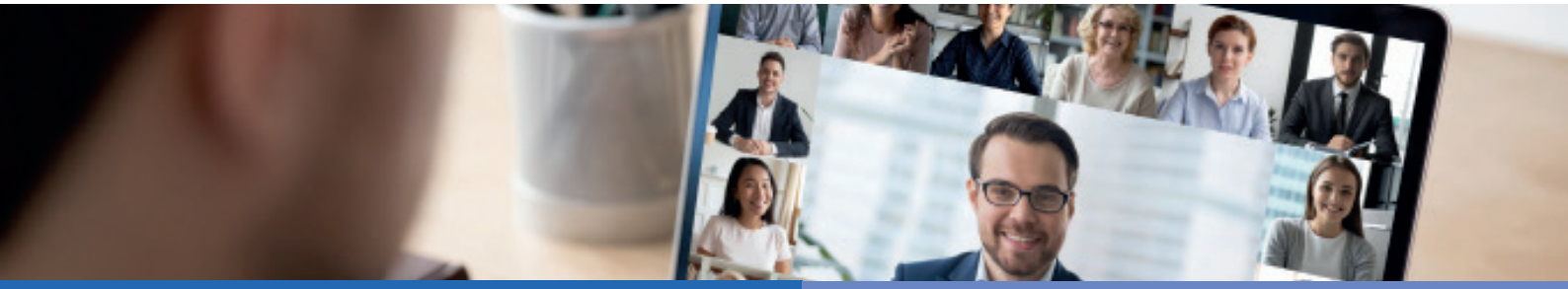
März 2024

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider



No more Death by Online Presentation

von Steffen Moll

"Stell dir vor, du nimmst an einer Online-Präsentation teil. Draußen strahlt die Sonne, dein Schreibtisch biegt sich unter dem Berg an Aufgaben und dein E-Mail-Postfach quillt über. Und dann ist da diese Präsentation: inhaltlich irrelevant ... eine Person, die monoton von Folien abliest, ohne einen Funken Interaktion oder Engagement. Und du wünschst dir, es gäbe einen Straftatbestand mit dem Namen: „Aktive Zuhörer-Sterbehilfe“.

Seite 10

Sichere Kommunikationsprotokolle in der Gebäudeautomation – im Fokus: BACnet Secure Connect

von Dr. Andreas Kaup

Die Gebäudeautomation wird immer wichtiger und ist für einen effizienten Gebäudebetrieb unerlässlich. Tatsächlich wird die Gebäudeautomation für eine Vielzahl von Nichtwohngebäuden durch das Gebäudeenergiegesetz (GEG) bis Ende 2024 sogar verpflichtend [1].

Seite 32

Unternehmens-IT nach dem Modell Internet und große Clouds

von Dr. Behrooz Moayeri

Eine Unternehmens-IT, die nach den Modellen Internet, Clouds und Providernetze konzipiert ist, kann große Vorteile hinsichtlich Robustheit bieten. Sowohl beim Routing als auch bei Standort-Redundanz gibt es von den großen Providern und Cloud-Betreibern einiges zu lernen.

Seite 2

Schadensersatz und Bußgelder wegen Datenschutzverletzungen

von Sabine Sobola

Die Datenschutzgrundverordnung (DSGVO) wurde im Mai 2018 verabschiedet und wird seitdem von Behörden und Unternehmen mehr oder weniger gut umgesetzt.

Seite 27

Webinar der Woche

KI-Einsatz in der Projektwirtschaft

Seite 26

Der Bootloader als Sicherheitslücke

von Dr. Markus Ermes

Vor wenigen Tagen wurde eine Sicherheitslücke in einem weit verbreiteten Bootloader für Linux bekannt. Diese lässt sich interessanterweise auch remote ausnutzen. Aber Moment mal: Wofür braucht ein Bootloader einen Netzzugriff?

Seite 23

Unternehmens-IT nach dem Modell Internet und große Clouds

von Dr. Behrooz Moayeri

In der letzten Insider-Ausgabe des Jahres 2023 ging ich auf folgende Netztrends ein, die aus meiner Sicht zu den wichtigsten im Jahr 2024 gehören:

- Ausfallsicherheit nicht nur mittels Hardware-Redundanz, sondern durch Segmentierung und damit Verkleinerung von Fehlerdomänen, sowie Einfachheit des Netzdesigns
- Vorausschauende Wireless-Planung
- Externe Anbindung aller Standorte über Glasfasern

Im Folgenden möchte ich auf den Zusammenhang des erstgenannten Themas mit den zunehmenden Verfügbarkeitsanforderungen an die IT von Unternehmen eingehen. Ich möchte darlegen, was man beim Aufbau und der Weiterentwicklung einer Unternehmens-IT vom Modell Internet sowie dem Modell großer Clouds lernen kann. Mir ist bewusst, dass ebenfalls die Betreiber großer Clouds nur mit Wasser kochen. Auch in großen Clouds der sogenannten Hyperscaler wie Microsoft kommt es zu schmerzhaften Ausfällen. Meine persönliche Erfahrung ist jedoch, dass die Verfügbarkeit großer Clouds höher ist als die durchschnittliche Verfügbarkeit der von den Unternehmen für den eigenen Bedarf betriebenen IT-Infrastruktur. Deshalb bin ich der Meinung, dass eine Unternehmens-IT nach dem Modell Internet sowie dem Modell großer Clouds für die meisten Unternehmen wesentliche Verbesserungen insbesondere hinsichtlich der Robustheit und Ausfallsicherheit bedeuten kann.

Das Modell Internet

In meinem oben genannten Beitrag im Insider 12/2023 bin ich auf das Modell Internet näher eingegangen. Ich habe darauf hingewiesen, dass ein wie das Internet als Verbund verschiedener Fehlerdomänen gestaltetes Netz robuster ist als eine einzelne Fehlerdomäne mit mehr Abhängigkeiten zwischen den Komponenten. Das Internet lebt davon, dass die verschiedenen Autonomen Systeme (AS) auch Fehlerdomänen in dem Sinne sind, dass ein Fehler, Problem oder Ausfall selten mehr als ein AS betrifft.

Der lose Verbund Internet besteht auf Routing-Ebene aus verschiedenen AS, die mittels Border Gateway Protocol (BGP), speziell eBGP (mit „e“ für „exterior“, d.h. AS-übergreifend) Erreichbarkeitsinformationen austauschen. eBGP hat sich als extrem robust erwiesen. Das zum Beispiel bei Multi-Protocol Label Switching (MPLS) oft genutzte interior BGP (iBGP, innerhalb eines AS) hat etwas mehr Abhängigkeiten zwischen Komponenten als das eBGP. Will man zum Beispiel, dass in einem AS alle BGP-Router dieselben Routing-Informationen haben, setzt man häufig sogenannte Route Reflectors (RR) ein, die als Drehscheibe für BGP-Updates fungieren. Man muss auch an RR-Redundanz denken.

Robustheit auf reiner IP-Ebene ist jedoch nicht das einzige Erfolgsrezept im weltweiten Internet. Ein weiteres äußerst robustes Internet-Gebilde ist das weltweite Domain Name System (DNS). Wir sind mittlerweile von der Namensauflösung mittels DNS genauso abhängig wie von der IP-Konnektivität. Das weltweite DNS hat sich wie das weltweite IP-Routing ebenfalls als sehr ausfallsicher erwiesen. Auch beim DNS gilt das Prinzip der verteilten administrativen Hoheiten. DNS ist als hierarchischer Baum aufgebaut. Auf höheren Ebenen gibt es sogenannte Delegationen zu

No more Death by Online Presentation

von Steffen Moll

"Stell dir vor, du nimmst an einer Online-Präsentation teil. Draußen strahlt die Sonne, dein Schreibtisch biegt sich unter dem Berg an Aufgaben und dein E-Mail-Postfach quillt über. Und dann ist da diese Präsentation: inhaltlich irrelevant ... eine Person, die monoton von Folien abliest, ohne einen Funken Interaktion oder Engagement. Und du wünschst dir, es gäbe einen Straftatbestand mit dem Namen: „Aktive Zuhörer-Sterbehilfe“.

Kennst du das? Diese Momente, in denen du dir wünschst, es gäbe eine bessere, spannendere Art, Informationen online zu vermitteln? Die gute Nachricht: Die gibt es. Doch zunächst stellt sich die Frage: Warum scheitern Online-Präsentationen so oft?

Als Präsentationstrainer, der bereits unzählige Präsentationen erlebt hat – und teilweise auch ertragen musste – habe ich drei Hauptprobleme identifiziert:

1. **Mangelnde Relevanz:** Zu oft sind die Inhalte nicht auf die Erwartungen, Wünsche, Ziele und Probleme der Zuhörenden abgestimmt. Eine Präsentation, die keinen Bezug zum Publikum hat, ist wie ein Schiff ohne Kurs – es kommt nirgendwo an. Also stell dir die Frage: Kennst du die Erwartungen und Probleme deines Publikums? Bietest du passende und relevante Inhalte und Lösungen an?

2. **Langeweile:** Stundenlange Vorträge, Textfolien-Fluten, keine Abwechslung – das ist der Stoff, aus dem die Langeweile gemacht ist. Das Publikum schaltet mental oft schon nach den ersten Minuten ab. Ohne die Dynamik einer Präsenzveranstaltung fällt es schwer, den Funken überspringen zu lassen. Ein Funke entzündet sich jedoch nur, wenn er zuerst im Sprecher lodert. In dir muss brennen, was du in anderen entzünden möchtest. Frag dich also: Wie ansteckend ist deine Begeisterung?

3. **Einbahnstraßenkommunikation:** Viele Präsentationen gleichen einer Einbahnstraße, bei der die Informationen nur in eine Richtung fließen. Es mangelt an Interaktion, an einem echten Dialog mit dem Publikum. Dadurch entsteht keine wirkliche Verbindung oder Engagement. Die Teilnehmenden könnten genauso gut eine E-Mail lesen oder ein Video anschauen, bei dem sie die Freiheit haben, Teile zu überlesen oder zu überspringen. Stell dir daher die Frage: Wie kannst du deine Online-Präsentation so gestalten, dass die Teilnehmenden regelmäßig ihre Fragen, Themen und Wünsche einbringen können?

Wie du dich gut in Szene setzt

„Man kann nicht nicht kommunizieren“. Das gilt auch für den ersten Eindruck, den du innerhalb von Sekunden erweckst, nachdem deine Teilnehmenden deinen Ausschnitt sehen, den deine Web-

Herausforderungen einer Projektleiterin

Mit Leonie Herden sprach Christiane Zweipfennig

Nur eine effiziente Projektleitung bringt Projekte erfolgreich ins Ziel. Projektleiter sind für die operative Planung und Steuerung des Projekts verantwortlich. Sie sind der organisatorische und kommunikative Dreh- und Angelpunkt des Projektes und kümmern sich um die Einhaltung von Terminen und Deadlines, das Erreichen von Etappenzielen, die Einhaltung des Kostenrahmens und die Qualitätssicherung der Arbeit.

Leonie Herden begleitet seit über 10 Jahren Kunden von ComConsult bei der Konzeption und Umsetzung moderner Kommunikationslösungen. In diesem Interview berichtet sie davon, wie sie es als Projektleiterin schafft, alle Fäden im Projekt fest in der Hand zu halten und mit Weitblick und stetiger Kontrolle Projekte erfolgreich zum Abschluss zu führen.

Leonie, wie hat sich dein Tätigkeitsfeld bei ComConsult von den Anfangszeiten bis zur ersten eigenen Leitung eines Projektes entwickelt?

> Vom Konzepte erarbeiten im Hintergrund zur Projektleitung in der 1. Reihe

Als ich bei ComConsult eingestiegen bin, waren meine Kollegen an vorderster Front beim Kunden als Projektbegleiter tätig und ich habe im Hintergrund Dokumente gesichtet und bearbeitet. Die Kollegen haben die Gespräche mit den Kunden geführt und ich habe dabei oft Protokoll geführt und anschließend Excel-Tabellen bearbeitet und Konzepte erarbeitet. Je länger ich dabei war, umso mehr Verantwortung habe ich übernommen. Ich fing an, selber Workshops beim Kunden durchzuführen und hielt Vorträge in unseren offenen Seminaren. Vor drei Jahren brauchte ein Kollege Unterstützung in einem Projekt und bat mich, das Projekt zu leiten. So bin ich nach und nach in die Rolle der Projektleiterin hineingewachsen.

Was ist deine Hauptaufgabe als Projektleiterin?

> Kompletter Überblick und Dokumentation des Projektfortschrittes

Das Wichtigste bei der Leitung eines Projektes ist es, den Überblick über alle Tätigkeiten zu behalten, alle Listen und Pläne kontinuierlich zu kontrollieren und den Projektfortschritt sorgfältig zu dokumentieren. Ich erstelle am Anfang eines Projektes einen Plan, in dem sämtliche Aufgaben aufgeführt sind. Die einzelnen Schritte bringe ich in eine zeitliche Abfolge. Ich lege zum Beispiel für ein Migrationsprojekt fest, welche Arbeiten für die organisatorische und welche für die technische Vorbereitung nötig sind. Danach definiere ich, welche einzelnen Schritte für die Umsetzung und am Schluss für die Nachbereitung wichtig sind. Nachdem ich den Projektplan aufgestellt habe, stimme ich ihn mit dem Kunden und weiteren Dienstleistern ab. Oft sind es mehrere Dienstleister, die mit im Boot sitzen, und meine Aufgabe ist es, alle Mitwirkenden zu koordinieren.

Der Bootloader als Sicherheitslücke

von Dr. Markus Ermes

Vor wenigen Tagen wurde eine Sicherheitslücke in einem weit verbreiteten Bootloader für Linux bekannt. Diese lässt sich interessanterweise auch remote ausnutzen. Aber Moment mal: Wofür braucht ein Bootloader einen Netzzugriff?

In diesem Standpunkt sollen kurz der Bootloader, sein Ursprung und die Funktionen dargestellt werden, die zu der Sicherheitslücke geführt haben, sowie die Sicherheitslücke selbst.

Der Linux-Bootloader „shim“

Schon seit einiger Zeit benötigt Linux ein Stück zusätzliche Software, um auf aktuellen Systemen starten zu können. Dies betrifft insbesondere physische Systeme mit Secure Boot. Dazu kommt bei vielen verbreiteten Distributionen das Werkzeug „shim“ zum Einsatz, mit dem ein Linux gestartet werden kann, auch ohne sich groß um Secure Boot Gedanken machen zu müssen.

Doch was hat es mit Secure Boot auf sich? Es handelt sich dabei um eine Technik, die nur das Starten von als vertrauenswürdig eingestuften Betriebssystemen erlaubt. Wie aber weiß die Hardware, dass das Betriebssystem vertrauenswürdig ist? Über hinterlegte Signaturen im UEFI des Motherboards. Für weit verbreitete Betriebssysteme, allen voran die (mehr oder weniger) aktuellen Versionen von Microsoft Windows, ist das relativ einfach. Es gibt einen Hersteller, der den Bootloader signiert, und diese Signatur kann einfach überprüft werden.

Bei weniger verbreiteten und besonders anpassbaren Betriebssystemen, hier in Form von Linux, ist dies schwieriger. Ja, man kann eigene Signaturen hinzufügen, doch das ist kompliziert und fehleranfällig. Das würde in letzter Instanz bedeuten, dass man Secure Boot abschalten müsste, um ein Linux zu installieren. Und wirklich toll ist die Idee nicht, eine Sicherheitsfunktion abzuschalten. Das war übrigens einer der wichtigsten Punkte, warum Secure Boot zu Anfang von der Linux-Community sehr kritisch gesehen wurde und häufig auch heute noch gesehen wird.

Um dem entgegenzuwirken, gibt es das oben genannte „shim“. Hierbei handelt es sich um ein Stück Software, das von Microsoft signiert ist und den eigentlichen Linux-Bootloader (in den meisten Fällen GRUB) laden kann, ohne dass Secure Boot Probleme bereitet.

Der Bootloader mit Netzwerk-Zugriff

Auch wenn es sich angeblich um ein einfaches Stück Software handelt, so kann shim doch sehr viel mehr, als man auf den ersten Blick vermuten würde. Eine besonders interessante Funktion: shim kann auch ISO-Dateien per HTTP herunterladen und diese starten wie ein lokales Betriebssystem oder einen lokalen USB-Stick. Für Experimentierfreudige durchaus eine interessante Funktion, jedoch auch eine, die man nicht mit einem „minimalen“ Bootloader in Verbindung bringen würde.

Und genau bei dieser Funktion gab es eine Sicherheitslücke, über die ein Angreifer mittels präparierter HTTP-Antworten ein System übernehmen und somit Secure Boot ad absurdum führen konnte,

Schadensersatz und Bußgelder wegen Datenschutzverletzungen

Wichtige Gerichtsurteile des Europäischen Gerichtshofs

von Sabine Sobola

Die Datenschutzgrundverordnung (DSGVO) wurde im Mai 2018 verabschiedet und wird seitdem von Behörden und Unternehmen mehr oder weniger gut umgesetzt. Dabei spielt immer wieder die Frage nach Bußgeldern der Aufsichtsbehörden und Schadensersatzforderungen von betroffenen Personen eine zentrale Rolle. Fast 6 Jahre nach Geltungsbeginn der DSGVO sind mittlerweile einige Urteile des Europäischen Gerichtshofs zu beiden Themenkomplexen gefällt worden, die einige Fragen dazu beantworten. Bereits an dieser Stelle muss jedoch ebenfalls festgehalten werden, dass viele Themen immer noch offen sind, insbesondere die Frage nach der angemessenen Bußgeld- bzw.- Schadensersatzhöhe.

Im vorliegenden Beitrag wird der Fokus auf die Fragen gelegt, die vom EuGH bereits verbindlich beantwortet wurden. Diese sind zum Thema Bußgeld folgende:

1. Muss bei Bußgeldverfahren immer festgestellt werden, dass es eine natürliche oder juristische Person war, die die Ordnungswidrigkeit tatsächlich begangen hat, oder kann ein Bußgeldverfahren auch direkt gegen ein Unternehmen geführt werden?

2. Falls ein solches Bußgeldverfahren auch direkt gegen ein Unternehmen geführt werden kann: Muss das Unternehmen den durch einen Mitarbeitenden vermittelten Verstoß schuldhaft begangen haben, oder reicht für eine Bestrafung des Unternehmens per Bußgeld im Grundsatz bereits ein ihm zuzuordnender objektiver Pflichtenverstoß gegen die DSGVO aus („strict liability“)?

Zum Thema Schadensersatz betroffener Personen wurden unter anderem folgende Fragen vom EuGH beantwortet:

3. Begründet ein bloßer Verstoß gegen die DSGVO bereits einen Schadensersatzanspruch?

4. Muss der erlittene Schaden eine gewisse Erheblichkeit oder Bagatellgrenze überschreiten?

5. Unter welchen Bedingungen kann eine Person, deren personenbezogene Daten sich im Besitz einer öffentlichen Agentur befinden, welche nach einem Angriff von Cyberkriminellen im Internet veröffentlicht wurden, Ersatz des immateriellen Schadens verlangen?

Zur ersten Frage, ob bei Bußgeldverfahren immer festgestellt werden muss, dass es eine natürliche oder juristische Person war, die die Ordnungswidrigkeit tatsächlich begangen hat, oder ob ein Bußgeldverfahren auch direkt gegen ein Unternehmen geführt werden kann, hat der EuGH im Dezember grundlegende Rechtsfragen in Zusammenhang mit der Bußgeldhandhabung

Sichere Kommunikationsprotokolle in der Gebäudeautomation – im Fokus: BACnet Secure Connect

von Dr. Andeas Kaup

Die Gebäudeautomation wird immer wichtiger und ist für einen effizienten Gebäudebetrieb unerlässlich. Tatsächlich wird die Gebäudeautomation für eine Vielzahl von Nichtwohngebäuden durch das Gebäudeenergiegesetz (GEG) bis Ende 2024 sogar verpflichtend [1]. In der GEG-Novelle von Oktober 2023 wurden in §71a erstmals Anforderungen an die Nutzung einer Gebäudeautomation definiert. Für eine effiziente Gebäudeautomation muss Kommunikation zwischen allen Systemen der Gebäudeautomatisierung und -steuerung stattfinden. Um diese Kommunikation gewerke- und herstellerübergreifend zu ermöglichen, wurden im Laufe der Zeit GA-Kommunikationsprotokolle entwickelt und auch normativ definiert. Eines der weitverbreitetsten Kommunikationsprotokolle ist BACnet. Für diesen Standard wurde die neue Protokollversion BACnet Secure Connect (SC) entwickelt, welche im Vergleich zu vorherigen Versionen eine sichere Netzwerkkommunikation ermöglicht.

BACnet ist ein herstellerneutraler Kommunikationsstandard für die Gebäudeautomation. Die erste Version von BACnet wurde bereits im Jahr 1995 veröffentlicht. BACnet Secure Connect (SC) ergänzt als neuer Protokoll-Layer den bisherigen BACnet-Standard. BACnet/SC wurde im Jahr 2019 von der ASHRAE im Addendum bj der Version 125-2016 veröffentlicht [2]. Normativ wird der BACnet-Standard in der DIN EN ISO 16484-6 definiert [3]. Die Ergänzung um BACnet/SC wurde im Jahr 2020 in dem Annex AB veröffentlicht. BACnet eignet sich als interoperabler Kommunikationsstandard in der Gebäudeautomation, um die gewerkeübergreifende Integration von HKLS-Anlagen (Heizungs-, Klima-, Lüftungs- und Sanitäranlagen), Lichtsteuerung, Verschattung, Sicherheit und Brandmeldetechnik zu realisieren. Eine zentrale Rolle spielen hierbei die intelligenten Automationsstationen, die ein einheitliches Gesamtsystem durch Vernetzung untereinander, mit Geräten aus der Feldebene und mit übergeordneten Management-Bedieneinrichtungen aufbauen. In Abbildung 1 ist ein schematischer Aufbau einer Gebäudeautomation unter Verwendung von BACnet als führendes Kommunikationsprotokoll visualisiert. In der Managementebene kann sich eine BACnet-Workstation oder eine Gebäudemanagementplattform befinden. In der Automationsebene werden die klassischen TGA-Anlagen über die Automationsstationen angebunden. In der Feldebene befinden sich die Raumautomationsstationen. An die Raumautomation können verschiedenste Aktoren und Sensoren mit unterschiedlichen Kommunikationsprotokollen angebunden werden.

Das BACnet-Kommunikationsprotokoll fungiert unabhängig von einer konkreten Anwendung und kann somit herstellerunabhängig für Komponenten der Gebäudeautomation genutzt werden. BACnet zeichnet sich weiterhin dadurch aus, dass es zu einer Vielzahl von Kommunikationsprotokollen kompatibel ist. Hierfür wurde der Standard stets so fortgeschrieben, dass die Kompatibilität zu älteren Protokollversionen gewahrt wurde. Das BACnet-Protokoll wurde in Anlehnung an das ISO/OSI-Schichtenmodell entwickelt. Der Aufbau wird auch in der Norm ISO 16484-5:2022 in Anlehnung an das ISO/OSI-Schichtenmodell definiert, siehe Abbildung 2. Gemäß dieser Abbildung bleiben der *BACnet Application Layer* und der *BACnet Network Layer* immer bestehen,