ComConsult Research

Der Netzwerk Insider

Oktober 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Authentifizierung und Single Sign On in Cloud-Umgebungen

von Dipl.-Math. Cornelius Höchel-Winter

Die Flut an Cloud-Angeboten nimmt täglich zu und es ist heutzutage nicht nur im privaten Umfeld kaum vorstellbar ohne Software oder Infrastruktur-Produkte aus der Cloud auszukommen. Die Nutzung von Software im Allgemeinen muss aber einfach und intuitiv sein, und dies gilt im Besonderen für Aspekte, die vom Benutzer als eher lästige Randerscheinungen wahrgenommen werden. Hierzu zählt an erster Stelle der Anmeldevorgang.

Hinzu kommt, dass kaum ein Anwender dazu in der Lage ist, sich ohne zusätzliche Hilfsmittel eine Vielzahl verschiedener

Passwörter in der nötigen Komplexität zu merken – und das gängige Hilfsmittel hierfür ist nach wie vor der Zettel in der oberen Schreibtischschublade.

Die Lösung hierfür heißt Single Sign On, das heißt der Aufbau oder die Nutzung einer Authentisierungs- und Autorisierungsarchitektur, bei der sich der Benutzer nur ein einziges Mal anmeldet (authentisiert) und die dann im Hintergrund und transparent für den Benutzer dafür sorgt, dass er die Anwendungen, die für ihn freigegeben sind, so nutzen kann wie sie für ihn freigegeben sind.

weiter auf Seite 6

Zweitthema

Strukturierte Verkabelung für Technische Gebäudeanlagen

von Dipl.-Ing. Hartmut Kell

Vor über 20 Jahren wurde in der EN 50173 die „Anwendungsneutrale Kommunikationskabelanlage“ in ihrer ersten Version spezifiziert, trotz anfänglicher Skepsis und durchaus vieler Optimierungspunkte hat sie sich durchgesetzt, ein Gebäude mit Büroarbeitsplätzen ist ohne informationstechnische Verkabelung und damit ohne Anwendung der EN 50173 nicht mehr vorstellbar.

Die Nutzbarkeit und Akzeptanz dieser ersten Version führte dazu, dass auch eine Standardisierung der IT-Verkabelung in Gebäuden ohne Büroarbeitsplätze sukzessive erfolgte. Ob Rechenzentrum oder Industriegebäude, für alles gibt es eine europäische oder nationale Verkabelungsnorm. Ganz zum Schluss erst aber wurde in den Normungsgremien die Notwendigkeit gesehen auch eine anwendungsneutrale Kommunikationsverkabelung für Geräte zu definieren, die selbstverständlich in jedem Gebäude zu finden ist, die aber bisher klassisch mit Netzwerk oder ähnlichem nichts zu tun hatte und damit mit eigenen Strukturen, Materialien und Techniken versorgt wurde. Bei der Planung von Gebäuden wird diese Form der Technik mit dem Begriff der „Technischen Gebäudeanlage“ oder abgekürzt TGA beschrieben und es war abzusehen, dass auch in diesem speziellen Umfeld eine andere Art der Kommunikationsverkabelung mehr und mehr Einzug halten wird. Der nachfolgende Artikel geht auf diese Art der Verkabelung ein und analysiert die im Jahr 2014 verabschiedete Norm, die aus Sicht des Autors auch nach 2 Jahren noch nicht im Bewusstsein der Fachplaner angekommen ist.

weiter auf Seite 21

Geleit

Herausforderung Agilität

auf Seite 2

Standpunkt

„Alle Räder stehen still, wenn dein starker Arm es will“ oder das unterschätzte Angriffspotential von DDoS

auf Seite 16

Aktuelle Kongresse

ComConsult Technologie-Tage 2016 UC-Forum 2016

auf Seite 4/5 und Seite 14/15

Aktuelle Sonderveranstaltung

Wireless und Mobility

auf Seite 17/18

Zum Geleit

Herausforderung Agilität

Wer kennt sie nicht, die Erzählungen über Projekte, die Wochen oder Monate auf einen Server oder mehr Netzwerk-Kapazität warten mussten. Aber diese Zeiten sind vorbei. Wenn es ein einzelnes herausragendes Kriterium gibt, an dem sich die IT-Infrastruktur-Planung in Zukunft orientieren muss, dann ist es die schnelle Bereitstellung von Kapazitäten. Und der Begriff Agilität beschreibt genau dies, also eine IT-Infrastruktur, die agil und flexibel ist.

Warum ist dies das dominante Kriterium für eine Zukunfts-orientierte IT? Dafür gibt es mehrere Gründe.

Der sicher dominierende Grund ist, dass viele Branchen und Unternehmen sich in einer Wettbewerbs-Situation befinden, die es nicht mehr erlaubt, Projektzeiten von 12 bis 24 Monaten für eine zentrale Lösung zu haben. Die Liste der Unternehmen, die in den letzten 10 Jahren gescheitert sind, weil sie sich nicht schnell genug anpassen konnten, ist lang. Und dies wird sich in den kommenden Jahren weiter verschärfen. Fortschritte auf der Technologieseite (zum Beispiel im Bereich Artificial Intelligence), die Notwendigkeit einer neuen und verbesserten Kunden-Ansprache und ein zunehmender internationaler Konkurrenzdruck erzeugen einen exponentiell wachsenden Druck auf einzelne Branchen. Nicht alle werden davon betroffen sein, aber wen es trifft, den trifft es hart. Die IT-Abteilung ist dabei in der Regel gar nicht der Kern des Problems. Ein Unternehmen muss sich in seiner Gesamtheit an die veränderten Marktgegebenheiten anpassen. Und dabei gibt es viele interne Widerstände. Diese führen aber auch dazu, dass häufig ein Sündenbock gesucht wird. Und IT ist prädestiniert dafür.

Der zweite und sehr ernst zu nehmende Grund ist die veränderte Architektur von Anwendungen. Die betrifft zwar nicht alle Anwendungen, aber sicher mehr als 90%. Anwendungs-Architekturen sind heute stark parallelisiert und erlauben damit eine schnelle Anpassung an wechselnde Last-Anforderungen. Dies passt wiederum sehr gut zu modernen Virtualisierungs-Architekturen, die Lastanpassung über die Anzahl paralleler virtueller Maschinen umsetzen. Und es gibt eindrucksvolle Beispiele dazu, wie gut solche Architekturen skalieren.

Der dritte Grund liegt in einem Umdenken in Benutzer-Schnittstellen. Vor allem Web-Applikationen, die auf eine bestimmte Art der Bedienung ausgelegt sind, haben Benutzerschnittstellen in eine bestimme Richtung verschoben. Ein Beispiel sind Dashboards in ERP-Anwendungen, die flexibel angepasst werden können und aus denen heraus ein schneller Drill-Down in die Details möglich ist. Diese Art der Anwendung sehen wir heute in der gesamten Breite von CRM bis hin zur Buchhaltung.

Der vierte Grund ist die Weiterentwicklung von Artificial Intelligence AI. Hier werden wir aller Voraussicht nach in den nächsten drei bis fünf Jahren eine signifikante Änderung beobachten. Neben IBM mit dem schon alten Bekannten Watson sind auch Google und Microsoft aggressiv an den Markt gegangen. AI wird vor allem die Interaktion mit Benutzern verändern, indem das System quasi ahnt was der Benutzer will und die entsprechende Funktionalität anwendet oder bereit stellt. Das ist nicht neu und alle neueren Buchhaltungssysteme wenden eine einfache Regel-basierte Form davon an (mit einer dramatischen Reduzierung der notwendigen Zeit bei der Eingabe und einer Reduzierung der Fehlerquote), aber es nimmt an Geschwindigkeit zu. Tatsächlich kann dieser vierte Bereich dazu führen, dass Unternehmen viel schneller als erwartet wesentliche Anwendungen neu programmieren müssen, wollen sie nicht zurück fallen.

Wo liegt jetzt aber das Problem für die IT-Abteilung? Nun, zum einen ist nicht jede Infrastruktur-Lösung skalierbar. Wir haben in der Vergangenheit häufig auf den besseren und schnelleren neuen großen Server gesetzt. Das dies nun keine Rolle mehr spielt, da nur die Zahl der parallelen virtuellen Server entscheidet, erfordert ein Umdenken. Damit ist auch ein Umdenken in den Betriebsprozessen verbunden, da sich die Zahl der Betreuungspunkte erhöht und formal ein Problem im Operating entsteht, wenn Applikationen nicht mehr statisch den Betriebsmitteln zugeordnet werden. Das ist aber nicht das zentrale Problem. Das zentrale Problem ist, dass isolierte Lösungen keinen Sinn machen. Wenn ich Kapazität skalieren will, dann muss das für die Gesamtheit aus Server, Speicher, Netzwerk, Sicherheit gelten. Kombiniert man das mit dem Anspruch von Verfügbarkeit und im Extremfall von Georedundanz, dann wird die Aufgabe komplex (auch weil dies über ggf über Abteilungs-Grenzen hinaus geht). Und damit ist man dann je nach Unternehmensgröße bei der Diskussion von Automatisierung. Für kleinere Unternehmen kann dies mit den bestehenden Möglichkeiten der einzelnen Plattformen abgedeckt werden, aber für größere Lösungen wird ein umfassender Ansatz erforderlich. Den liefert im Moment nur OpenStack. Und wie schon häufiger an dieser Stelle erwähnt, ist OpenStack kein Trivialprojekt und dementsprechend teuer.

Dabei drängt sich natürlich der Gedanke an die Cloud auf. Und tatsächlich werden wir genau diesen Aspekt auf unseren Technologietagen vertiefen. Wir sind davon überzeugt, dass es eine sinnvolle Strategie für ein Rechenzentrum für eine erfolgreiche Zukunft gibt. Dabei muss niemand vor der Cloud Angst haben. Aber die Forderung nach Agilität ist völlig unabhängig von einer Cloud-Diskussion zu sehen. Es gibt genügend Anwendungen, die nie in der Cloud landen werden. Und trotzdem muss auch für diese Anwendungen eine agile und flexible Lösung gefunden werden.

Ist der schwarze Peter dabei bei den Basis-Infrastrukturen? Nur wenn sich die Betreiber dumm anstellen. Die Bereitstellung von Rechenleistung, von Speicher, von Netzwerk und Sicherheit muss heute im Stundenbereich möglich sein. Auch wenn die Anforderung völlig unerwartet kommt. Die Betreiber haben schlicht keine andere Wahl und müssen dieses leisten. Wer dies nicht kann, der wird nicht überleben. Tatsächlich wird sich damit aber das Problem verschieben. Der Programmierer der Applikation oder der Datenbank-Planer wird in der Praxis große Probleme haben, neue Funktionalität im Stundenrhythmus anzubieten. Aber hier muss man die Kirche im Dorf lassen. Wir sind historisch gesehen zum Beispiel daran gewöhnt auf neue Funktionen im Banken und Versicherungsbereich Monate und Jahre zu warten. Wenn wir hier eine Lösung schaf-

Schwerpunktthema

Authentifizierung und Single Sign On in Cloud-Umgebungen

Fortsetzung von Seite 1

Dipl.-Math. Cornelius Höchel-Winter ist Leiter des Testlabors der ComConsult Research GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungstests neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von Windows- und Unixnetzen; so hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben.

Nun ist Single Sign On (SSO) bei weitem nichts Neues und keineswegs auf die Cloud fokussiert. Gerade in Windows-Domänen haben Datenbank-Server oder andere Systeme mit eigenen Benutzer- und Rechtedaten in der Regel schon „immer“ ein Single Sign On unterstützt. (siehe Abbildung 1)

Aber gerade bei der Integration von mehreren Cloud-Produkten im Unternehmen spielt Single Sign On eine wichtige Rolle. Denn Cloud-Anwendung haben spezielle Eigenschaften, die letztlich dem Anspruch geschuldet sind, ohne besondere Anforderungen an die Umgebung, in der sie gestartet werden, zu funktionieren (anywhere, anytime, any device):

Separate Benutzerbasis: „Any Device“ wird typischerweise dadurch erreicht, dass auf Web-Technologien und Zugriff via Browser gesetzt wird. In der Regel startet der Zugang zu einer Cloud-Anwendung über eine einfache Login-Seite, wo man Benutzername und Passwort eingeben muss. Diese auf den ersten Blick recht einfache Zugangsmethode impliziert jedoch, dass jeder Cloud-Provider und damit fast jede Cloud-Anwendung mit einer eigenen Benutzerdatenbank und oft zusätzlich mit einem eigenen Rechtekonzept daherkommen.

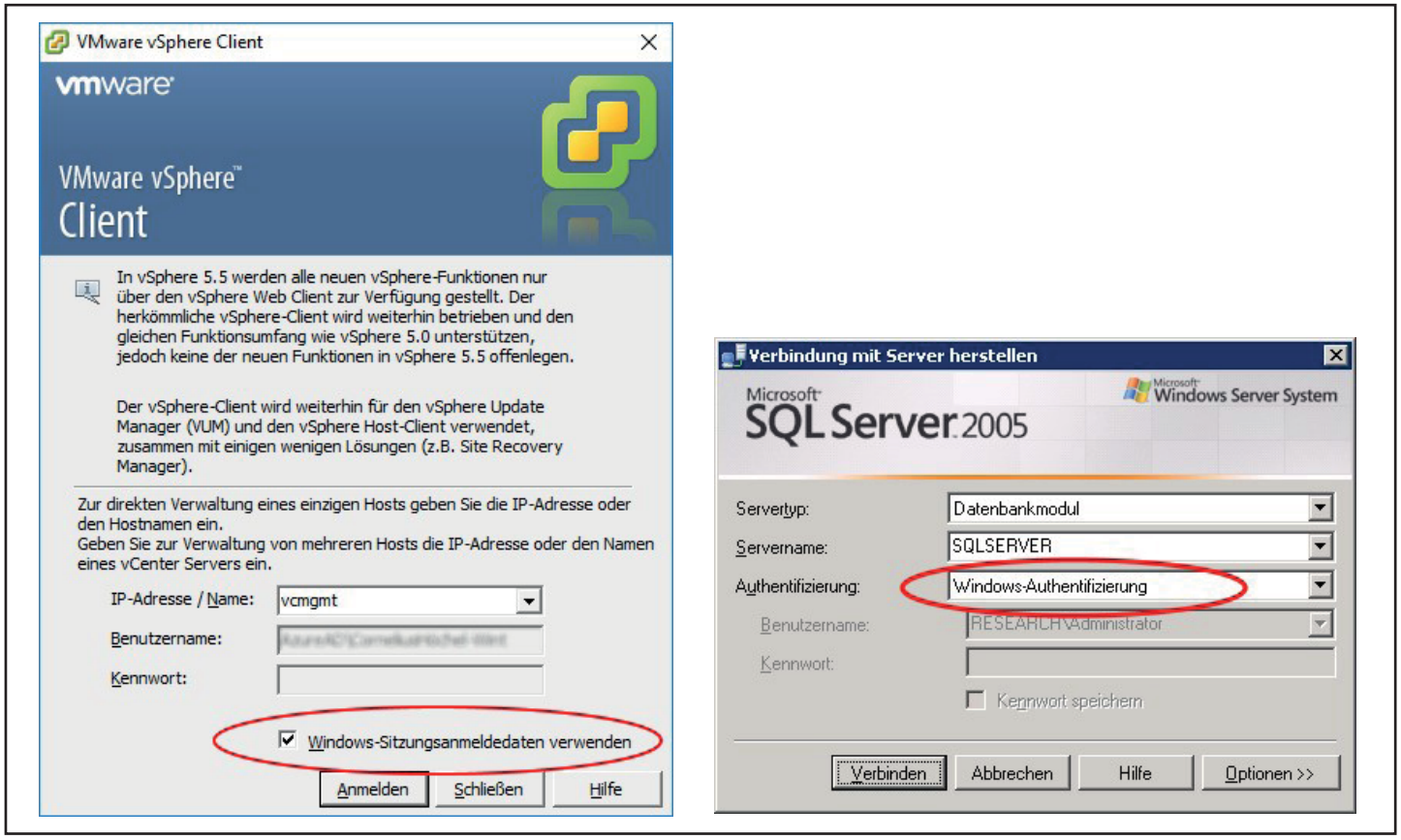

Abbildung 1: Integrierte SSO-Funktionalität in einer Windows-Domäne am Beispiel des vSphere Clients und des Verwaltungstools für Microsoft SQLServer.

Authentifizierung und Single Sign On in Cloud-Umgebungen

Hohe Sicherheitsanforderungen: „Anywhere“ bedeutet, dass die Anwendungen über das Internet mehr oder weniger öffentlich erreichbar sind und damit natürlich hohen Sicherheitsanforderungen unterliegen: Jeder Zugriff muss authentifiziert werden und gerade für die Zugangspasswörter muss eine ausreichende Komplexität gefordert werden.

Daraus ergeben sich auf mehreren Seiten nicht zu unterschätzende Probleme:

1. Die Benutzer selbst müssen sich eine Vielzahl von Benutzernamen-Passwort-Kombinationen merken, die Passwörter sollen möglichst komplex sein und die Idee, für alle Zugänge dasselbe Passwort zu nutzen, ist einerseits aus Sicherheitsüberlegungen eigentlich abzulehnen (lässt sich aber gerade in der Cloud nicht unterbinden) und scheitert andererseits ganz oft an der Realität: Die Provider haben einfach unterschiedliche Vorgaben für Passwörter. Die einen akzeptieren kein Leerzeichen, die andern keinen Schrägstrich, bei wiederum anderen wird der Komplexitätsindikator erst ab 16 Zeichen grün, während die andere Cloud nur maximal 12 Zeichen akzeptiert. Und dann kommen noch diverse Vorgaben für die maximale und minimale Nutzungszeit von Passwörtern hinzu.

   Hier öffnet sich schnell ein riesiges Sicherheitsproblem, da die Benutzer anfangen, sich ihre Passwörter aufzuschreiben, nach Ablauf von Passwörtern nur an der letzten Stelle einen Zähler zu erhöhen etc. pp.

   Wenn sich dann auch noch die Benutzernamen bei verschiedenen Produkten unterscheiden, ist die Akzeptanz bei den Mitarbeitern schnell völlig am Ende. Und der direkt beim Passwort notierte Benutzername führt jedes Sicherheitskonzept ad absurdem.

   Und Nein: Passwort-Safes sind keine geeignete Lösung für die Mehrzahl der Endbenutzer. Unserer Erfahrung nach kommen damit nur IT-affine Benutzer zurecht.

2. Aber auch für die Benutzeradministration explodieren plötzlich die Probleme. Nicht allein deswegen, weil die Benutzer nach mehrfachen Falscheingaben jetzt nicht nur im lokalen Active Directory gesperrt und wieder freigeschaltet werden müssen, sondern eben bei vier, fünf, sechs verschiedenen Cloud-Providern.

   Ein großer Teil zusätzlicher Arbeit entsteht dadurch, dass bei den verschiedenen Providern Benutzerkonten für neue Mitarbeiter angelegt und – ganz wichtig – für ausgeschiedene Mitarbeiter gelöscht oder gesperrt werden. Vergessen Sie nicht, wir sprechen hier über Cloud-Anwendungen! Das heißt, der ausgeschiedene Mitarbeiter hat in der Regel auch außerhalb des Unternehmens Zugriff auf die Anwendung.

3. Speicherdienste in der Cloud, aber auch komplexere Cloud-Anwendungen wie CRM oder Finanz- oder Buchhaltungsdienste nutzen – genauso wie übrigens ihre lokalen Pendants – anwendungsspezifische Rechtekonzepte. Lokale Anwendungen sind aber oft enger in das lokale Betriebssystem integriert als das mit Cloud-Anwendungen möglich ist und haben damit die Möglichkeit beispielsweise lokale Sicherheitsgruppen für ihr eigenes Rechtekonzept zu nutzen. Das macht vieles einfacher.

   Bei der Einführung von Cloud-Anwendungen mit eigenem Rechtekonzept muss dieses selbstverständlich an die Unternehmensanforderungen angepasst werden. Das eigentliche Problem besteht aber wiederum darin, dieses anwendungsspezifische Konzept – oder diese unterschiedlichen Konzepte bei verschiedenen Cloud-Diensten – immer wieder aktuell zu halten.

   Ein typisches Beispiel: Speicherdienste wie Box, Dropbox oder andere bietet den unbestritten großen Vorteil, zum Beispiel projektspezifische Daten auf Verzeichnis- oder sogar Dateiebene für externe Mitarbeiter freizugeben. Wer sorgt aber dafür, dass diese Freigaben auch wieder zurückgenommen werden, wenn sie nicht mehr benötigt werden?

Es ist offensichtlich, dass diese Probleme nicht durch schärfere Passwort-Policies und Mehrfaktor-Authentifizierung entschärft werden können – eher im Gegenteil.

Microsoft zeigt mit der Einführung einer PIN-basierenden Anmeldeoption mit einem Microsoft-Account bei Windows 10 übrigens durchaus überzeugend, dass Einfachheit und Sicherheit sich nicht zwangsläufig widersprechen:

- Für die regelmäßige Anmeldung am Arbeitsplatz-PC wird eine einfache und verglichen zum Passwort deutlich kürzere PIN genutzt. Da diese PIN gerätespezifisch festgelegt ist und daher nur am eigenen PC verwendet werden kann, ist das Missbrauchsrisiko deutlich geringer als das des Passworts, das von überall auf der Welt genutzt werden kann.

- Für das Passwort selbst, das weiterhin für alle verbundene Microsoft-Dienste gilt, kann so eine hohe Komplexität, gegebenenfalls sogar eine Zwei-Faktor-Authentifizierung gefordert werden.

Protokolle

Es gibt eine ganze Reihe standardisierter und auch proprietärer Protokolle zur verteilten Benutzerauthentifizierung.

Die zugrundeliegende Architektur ist dabei meist sehr ähnlich. Unterschieden werden drei Rollen:

- der Benutzer, der einen bestimmten Dienst nutzen will,
- der Dienstanbieter, der den gewünschten Dienst zur Verfügung stellt,

Zweitthema

Strukturierte Verkabelung für Technische Gebäudeanlagen

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH vermittelt er sein Fachwissen aus umfangreichen Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken in Form von Publikationen und Seminaren.

Sinn der strukturierten Verkabelung

Errichter von Gebäuden wie z.B. Architekten müssen sich bei Bürogebäuden damit auseinandersetzen, wie die einzelnen Arbeitsplätze mit einer IT-Verkabelung auszustatten sind. Dies ist Standard jeder Planung neuer Gebäude und wird durch den Nutzer als bereitgestellte Infrastruktur, ähnlich der Stromversorgung, zwingend vorausgesetzt. Die auf diese passive Infrastruktur aufsetzende Kommunikationstechnik ist in den mit Abstand allermeisten Fällen eine Netzwerk/IP-basierende Technologie. Theoretisch könnte dieses Netzwerk auf Basis von unterschiedlichen Zugangstechnologien realisiert werden, doch faktisch ist dies Stand heute ausschließlich Ethernet nach IEEE802.3. Damit verliert die Anwendungsneutralität der Verkabelung an Bedeutung, in der Norm wird sie aber weiterhin als Anforderung aufrechterhalten. Dieses Ethernet ist letztendlich auch dafür verantwortlich, dass die EN 50173 im Laufe der 20 Jahre immer wieder angepasst werden musste, keine bzw. kaum eine andere leitungsgebundene Übertragungstechnik hat so großen Einfluss auf die Anpassungen und Erweiterungen genommen. Wurden neue Funktionen beim Ethernet-Zugangsverfahren entwickelt, so erfolgte zunächst die Prüfung, ob dies mit der vorhandenen Verkabelung möglich ist und mit welchen Konsequenzen. War es nicht möglich, wurde eine Überarbeitung der EN 50173 notwendig, sehr häufig mit einer Dauer der Normungsanpassung von mehreren Jahren (man erinnere sich an die gefühlte endlose Standardisierung der Klasse E).

Welche Konsequenzen hat dies für die Betrachtung einer anwendungsneutralen Kommunikationsverkabelung *„zur Unterstützung von Nutzer-unspezifischen Diensten..., von denen viele die Verwendung von ferngespeisten Geräten erfordern“* (Zitat aus der EN 50173-6)? Für den Fall, dass bei der Planung eines neuen Gebäudes eine TGA-Verkabelung für diese Nutzungsformen geplant wird, muss sich diese nach der höchsten Anforderungsklasse zum aktuellen Stand der verfügbaren Übertragungstechniken richten, und das ist weiterhin die Ethernet-Technologie. Warum? Zur Vermeidung von Neuverkabelung und unter Beachtung der allgemein üblichen Prognose, dass auch bei diesen „ferngespeisten“ Geräten im Laufe der Zeit Ethernet als Kommunikationstechnik zum Einsatz kommen wird, sollte die Verkabelung entsprechend eingerichtet sein, sprich sie sollte strukturiert und anwendungsneutral sein (man denke an die aktuelle Diskussion zum Thema Industrie 4.0).

Erste Anforderungsspezifikationen

Geht man davon aus, dass die Kommunikationsverkabelung zwischen den Verteilern weiterhin im Wesentlichen geprägt wird durch große Distanzen und höhere Datenraten, so kommt in erster Linie Lichtwellenleiter als Medium in Frage. Bei der physikalischen Anbindung der „TGA-Endgeräte“ an das Netzwerk dagegen dürfte bevorzugt gefordert werden,

- eine Datenrate von nicht weniger als 100 Mbit/s sicherzustellen
- eine Stromversorgung über die Datenleitung mit Hilfe von Power-over-Ethernet sicherzustellen.

Daraus resultiert Twisted Pair (in Deutschland als „symmetrische Verkabelung“ geführt) als bevorzugtes Übertragungsmedium, doch muss diese „Endgeräte“-Verkabelung auch

- so aufgebaut werden wie bisher (selbe Topologie bzw. Hierarchie)?
- mehr als 100 Mbit/s übertragen können?
- mehr als 100 MHz übertragen können?
- überall den RJ45-Steckverbinder bereitstellen?

Die Beantwortung dieser Fragen lässt sich nur sehr wenig auf Grundlage von Erfahrungen durchführen, dazu steht die Einführung der Netzwerk-Technik in diesen TGA-Bereichen noch viel zu sehr am Anfang. Wünschenswert wären also möglichst herstellerneutrale Standards oder Richtlinien, die Hilfe bei der Planung leisten könnten. Gibt es diese Richtlinien/Standards, sind diese ausreichend bzw. vollständig zur Durchführung der Planung bzw. was muss der Planer möglicherweise noch ergänzen?

Normenübersicht

Herstellerneutrale Verkabelungsnormen existieren seit 1995, als weltweit gültige Normen (ISO/IEC 11801 plus weitere), als Europäische Normen (EN 50173) und als Deutsche Normen (DIN/EN 50173), welche weitestgehend eine Übersetzung EN 50173 mit geringfügigen nationalen Änderungen darstellt. Einen besonderen Fall stellen die amerikanische Normen der EIA/TIA dar, sie sind zwar kaum als Planungsrichtlinie in Deutschland zu nutzen, bilden aber sehr häufig bei neuen Technologien die ersten herstellerunabhängigen Richtlinien, welche anschließend in großen Teilen in den oben genannten internationalen und nationalen Normen einfließen. Bleiben wir aber bei den national wichtigen Normen, auch hier gibt es nicht die EINE Norm, in der alles enthalten ist, stattdessen gibt es neben der zentralen Normenreihe EN 50173 weitere bedeutende Normen. Als Beispiele sind zu nennen die EN 50346 in Zusammenhang mit den Messungen der Verkabelung, die EN 50288 in Zusammenhang mit der Spezifikation der Twis-

ted-Pair-Kabel oder die IEC 60603 in Zusammenhang mit der Spezifikation der Steckertechnologie bei Twisted-Pair.

Im vorliegenden Artikel liegt der Fokus auf der EN 50173-6 (Anwendungsneutrale Verkabelung für verteilte Gebäudedienste), deren letzte Überarbeitung im Mai 2014 erfolgt ist. Es wird notwendig sein, die wesentlichen Unterschiede

- zur EN 50173-1 (September 2011),
- zur EN 50173-2 (Anwendungsneutrale Verkabelung in Bürogebäuden; September 2011)
- und zur EN 50173-3 (Anwendungsneutrale Verkabelung in industriell genutzten Gebäuden; September 2011)

zu zeigen, denn nur die Berücksichtigung und Kenntnis der Basisnorm EN 50173-1 ist nicht ausreichend.

Die genannten ergänzenden Normen erläutern in der Einleitung den jeweiligen Anwendungsbereich:

EN 50173-2: Die Richtlinie beschreibt die IT-Verkabelung für Anwender in Büroumgebungen, die auf eine anwendungsneutrale Infrastruktur statt proprietärer Lösungen setzen.

EN 50173-3: Die Richtlinie beschreibt die IT-Verkabelung für Anwender mit industriell genutzten Kommunikationsanlagen, die auf eine anwendungsneutrale Infrastruktur statt proprietärer Lösungen setzen und die einen Schwerpunkt beim Zugangsverfahren Ethernet erwarten. Ziel ist die durchgängige Einbindung dieser Lösungen in vorhandene Unternehmensnetze/ -infrastrukturen der Bürobereiche. Wichtig ist die Abgrenzung: Sie betrachtet keine Kabelanlagen im Industrie-Bereich, die an den „Schnittpunkt“ der EN 50173-3 angeschlossen werden, z.B. Profinet-Verkabelungen.

EN 50173-6: Die Richtlinie beschreibt Kommunikationskabelanlagen für „nutzer-unspezifische Kommunikationsdienste“, welche auf ferngespeiste Geräte Zugriff haben wie z.B.

- Telekommunikation,
- Energiemanagement,
- Steuerung Umgebungsbedingungen,
- Zugangskontrolle,
- Alarmierung.

Interessant ist, dass der definierte Anwendungsbereich auch medizinische Bereiche umfasst, wie z.B. Schwesternrufanlage, Patientenüberwachung oder ähnliche. Im Prinzip würde dies bedeuten, dass kein modernes Krankenhaus mehr geplant werden dürfte ohne Beachtung der EN 50173-6. Ziel ist die Ablösung einer bedarfsorientierten Verkabelung und damit Vereinheitlichung der gesamten IT-Infrastruktur eines Gebäudes und, darauf wird besonders hingewiesen, die Verringerung der Verkabelung und damit eine Brandlastreduzierung. Auch in der EN 50173-6 werden nicht die Kabelanlagen betrachtet, die an den „Schnittpunkt“ der EN 50173-6 oder -3 angeschlossen werden (also z.B. keine Berücksichtigung von Spezialverkabelungen einer Evakuierungsanlage).

Beide dienen grundsätzlich den Errichtern von Gebäuden (z.B. Architekten) als Planungshilfen für eine IT-Verkabelung bevor die spezifischen Anforderungen der eingesetzten Übertragungstechniken bekannt sind, somit stellen sie im Grunde genommen ein „Muss“ für alle Gebäudeplaner dar. Aus Sicht des Autors ist gerade die EN 50173-6 aber noch nicht wirklich im Planungsdenken vieler Gebäudeplaner „angekommen“.

Grundnorm und Bürogebäudenorm

Alle drei Normen (-2, -3, -6) sind ohne gleichzeitige Beachtung der EN 50173-1 nicht anwendbar, denn sie weisen zumeist nur die Unterschiede zur Basisnorm EN 50173-1 aus. Geht es z.B. darum, in welchen Güteklassen die Materialien der symmetrischen Verkabelung (TP-Verkabelung) einzuteilen sind, so wird auf die Basisnorm verwiesen und es gelten exakt die gleichen Spezifikationen. In einem entscheidenden Punkt unterscheiden sich alle Normen, dies ist die empfohlene Topologie.

Die sternförmige „Rumpf-Topologie“ der Basisnorm EN 51073-1 sieht wie folgt aus: Mit Hilfe der Elemente Standortverteiler (SV), Gebäudeverteiler (GV) und Etagenverteiler (EV) wird eine 2-stufige Topologie realisiert. Die 2 Stufen sind:

- Primärverkabelung
- Sekundärverkabelung

Vor der Verabschiedung der EN 50173-2 wurde die Basisnorm noch in der bekannteren 3-stufigen Form geführt, in der es auch noch eine Tertiärverkabelung gab, die in den Teilnehmeranschlusseinheiten (TA) bzw. informationstechnischen Anschlüssen endete. Da diese dritte Stufe in Abhängigkeit der Nutzungsform des Gebäudes nicht immer identisch sein kann, wurde diese dritte Ebene aus der Basisnorm herausgenommen und in unterschiedlichen Formen in den Ergänzungsnormen für Bürogebäude, Industriegebäude und für verteilte Gebäudedienste spezifiziert. (siehe Abbildung 1)

Für jede Hierarchieebene können unterschiedliche Medien geplant werden mit unterschiedlichen Güteklassen, bei Kupfer werden die Begriffe „Kategorie“ (z.B. Kategorie 7) und „Klasse“ (z.B. Klasse E) verwendet, bei Lichtwellenleiter die Begriffe „OM“, „OS“, „OP“, „OH“ für die Fasertypen und „OF“ für die Streckenklasse (es gibt bis heute keine Güteklassen in diesen Normen für LWL-Stecker!).

In der Annahme, dass den meisten Lesern die Topologie der EN 50173-2 (Bürogebäude) bekannt ist, konzentrieren wir uns auf die beiden Alternativen, der EN 50173-3 und -6. Schauen wir uns zunächst die Topologie der „Industrieverkabelung“ einmal an, was fällt auf:

Industrieverkabelung

Die Ebene Primär- und Sekundärverkabelung wurde übernommen, dies vereinfacht die Anbindung von Industrieverkabelungen/-topologien an bereits vorhandene Topologien. Explizit wird darauf hingewiesen, dass auch Bus- und Ringtopologien unterstützt werden und damit vielfältige Möglichkeiten zur Bildung von redundanten Strukturen möglich sind.

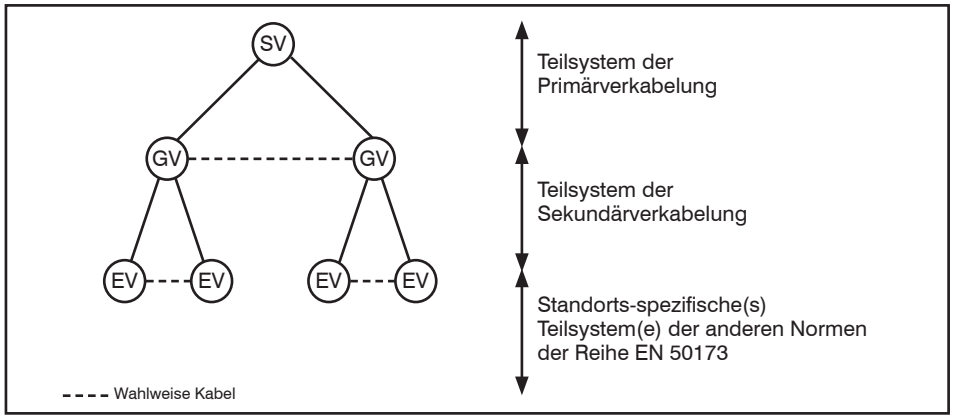

Abbildung 1: Sterntopologie nach EN 50173-1