ComConsult Research

Der Netzwerk Insider

Mai 2010

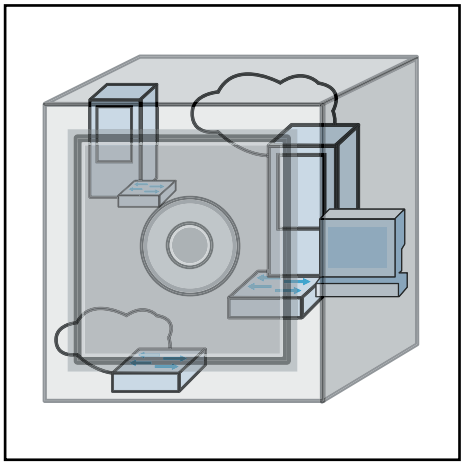
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Kommt der Durchbruch für die Netzzugangskontrolle mit IEEE 802.1X-2010?

von Dr. Simon Hoff

Ende Februar 2010 wurde die lang erwartete Neuauflage des Standards IEEE 802.1X zur Port-basierten Netzzugangskontrolle verabschiedet. Mit dieser Neuauflage sind Lücken in der Fassung von 2004 geschlossen und entscheidende Funktionen ergänzt worden. Mit IEEE 802.1X-2010 hat der Werkzeugkasten für die Absicherung von LANs im Campus- und Datacenter-Bereich endlich eine Form angenommen, die den extrem hohen Anforderungen an Leistung und Skalierbarkeit effektiv begegnen kann.



1. Netzzugangskontrolle mit IEEE 802.1X im Überblick

Der Standard IEEE 802.1X spezifiziert eine Methode zur Port-basierten Netzzugangskontrolle (Network Access Control, NAC) für Ethernet nach IEEE 802.3 und WLAN nach IEEE 802.11. IEEE 802.1X definiert verschiedene Rollen der beteiligten Netzelemente (siehe Abbildung 1)

weiter auf Seite 16

Zweitthema

Microsoft Exchange 2010: Hochverfügbarkeit On-Premise oder als Hosted-Service

von Dipl.-Inform. Nick Schirmer, Dr. Frank Imhoff, Dominik Zöller

Flexibilität, kürzere Reaktionszeiten und laufende Prozessoptimierung bei stetig steigendem Kommunikationsbedarf sind die Ziele einer verbesserten Unternehmensstrategie. Mit zunehmender Verbreitung IP-basierter Kommunikationslösungen unter dem Begriff Unified Communications / Collaboration (UCC) gewinnen auch E-Mail, Kalender, Kontakte und andere klassische Kommunikationswerkzeuge weiter an Bedeutung. IBM und Microsoft bieten mit ihren Messaging-Lösungen mehr als nur Bindeglieder zu UCC-Installationen. Vielmehr haben sich Exchange und Notes fast schon zu ausgewachsenen Groupware-Lösungen entwickelt.

Mit Exchange 2010 will Microsoft mithilfe verbesserter Fernzugriffsmöglichkeiten, erhöhter Sicherheit und deutlichen Erleichterungen bei der Bedienung und dem Management eine „strategische Waffe“ zur Optimierung der Prozessgestaltung liefern. In Abhängigkeit von der zugrundeliegenden Kommunikationsstruktur und der jeweiligen Unternehmensgröße ergeben sich mit diesen Neuerungen unterschiedliche Vorteile und Einsparpotenziale, auf die wir im Folgenden eingehen.

weiter auf Seite 9

Aktueller Kongress

ComConsult Wirless-Forum 2010

ab Seite 8

Geleit

Das Netzwerk wird zum Systembus: hin zur Matrix der kürzesten Wege!

ab Seite 2

Reportneuerscheinung

100G und 100G Ethernet

auf Seite 15

Zum Geleit

Das Netzwerk wird zum Systembus: hin zur Matrix der kürzesten Wege!

Letzte Woche ging das ComConsult Netzwerk-Redesign Forum 2010 zu Ende. Die starke Veränderung der Anforderungen an Netzwerke und die damit verbundenen Auswirkungen auf die Eignung von Komponenten stand im Mittelpunkt des Forums. Viele neue Switching-Standards sind momentan in Bearbeitung. Auf dem Forum gab es klare Bekenntnisse der anwesenden Hersteller in Richtung dieser Standards und ihrer Umsetzung in 2010 und 2011. Dabei wurde auch deutlich, dass einige dieser Standards Hardware-abhängig sind, also in bestehenden Netzwerk-Komponenten nicht nachgerüstet werden können. Auch beim Neukauf ist momentan Vorsicht geboten, da je nach Hersteller die nächste Generation von Komponenten, die alle diese Standards erfüllt, erst stufenweise in den nächsten 12 bis 18 Monaten auf den Markt kommen wird. Einige wenige existierende Produkte erfüllen alle Anforderungen bereits jetzt.

Ein gutes Beispiel für die ablaufenden Veränderungen ist das Rechenzentrum. Hier prägt der Satz „das Netzwerk wird zum Systembus“ die Diskussion seit Monaten. Doch ist wirklich jedem klar, was damit gemeint ist und wo die Begründung für diese Aussage liegt? Auf dem Netzwerk-Redesign Forum haben wir die aktuelle Entwicklung von IT-Architekturen und die resultierenden Anforderungen an Netzwerke diskutiert. Vertiefend wird auch die Sommerschule 2010 darauf eingehen. Vereinfacht kann man sagen, dass die Kommunikation im Rechenzentrum von 3 neuen Verkehrsströmen geprägt wird:

- Kommunikation zwischen virtuellen Maschinen als Teil von verteilten (Web-) Architekturen
- Systemkommunikation aus dem Umfeld der Virtualisierung, Beispiele sind das Wandern von virtuellen Maschinen, High Availability und Fault Tolerance
- Verlagerung von Plattenspeicher aus dem Direct Attached Bereich hin zu Storage Area Networks

Diese 3 Entwicklungen generieren sehr unterschiedliche Anforderungen an Netzwerke, die im Rahmen dieses Geleitworts nur kurz dargestellt werden können. Für Details wird auf die Sommerschule verwiesen. Im einzelnen können folgende Anforderungsbereiche benannt werden, die den Begriff „Netzwerk als Systembus“ auch klar machen:

- Es entstehen große Mengen von Transaktionen, die in verteilten Webarchitekturen Hauptspeicher-zu-Hauptspeicher über das Datennetz hinweg ablaufen. Hier entsteht eine Kommunikations-Matrix zwischen den Servern im Rechenzentrum (dieser Begriff und sein Verständnis sind sehr wichtig). Kommunikations-Transaktionen laufen in dieser Matrix zwischen beliebigen Paaren von Servern (virtuellen Maschinen auf Servern). Für die Server muss es dabei in der Performance egal sein, ob diese kommunizierenden virtuellen Maschinen auf einem physikalischen Server sind oder ob sie verteilt über das Netzwerk sind. Das Netzwerk bekommt also den Charakter einer Systembus-Verlängerung. Dies generiert keine besondere Anforderung an Bandbreite, aber eine klare Anforderung an Latenz (Verzögerungszeit Prozess-zu-Prozess).
- In der Systemkommunikation aus dem Umfeld der Virtualisierung tritt dem gegenüber eine Mischung aus Latenz und Bandbreite auf. Die System-Synchronisation im Rahmen von HA und FT ist Latenz-sensitiv, die Verschiebung von virtuellen Maschinen erfordert erhebliche Bandbreite, wenn dies unbemerkt für den Endanwender erfolgen soll. Dazu ist es unbedingt erforderlich, dass diese Mechanismen verstanden werden, um die negativen Folgen von zu wenig Bandbreite verstehen zu können. Wir haben das auf dem Forum ausreichend diskutiert.
- Die Verlagerung von Plattenspeicher ist ein spannender Vorgang. Im Rahmen der Konsolidierung von Servern durch Virtualisierung wird der bisherige Direct Attached Storage DAS durch Storage Area Networks SAN abgelöst. Der davon betroffene Speicher ist kein High-End-Datenbank-Speicher sondern Massenspeicher, der eine kostenoptimale Umsetzung erfordert. Wir haben auf dem Forum die Prognose von ComConsult Research präsentiert, die unterstreicht, dass wir an dieser Stelle iSCSI als Hauptinstrument dieser Umsetzung erwarten. Gegebenenfalls bekommt auch das neue parallele NFS eine hohe Bedeutung. Damit wird auch der Standpunkt von ComConsult Research klar, dass wir die Diskussion über Fibre Channel over Ethernet für fehlgeleitet halten. Wir sehen den weit stärkeren Bedarf in der Umsetzung von iSCSI. Dies generiert erhebliche Anforderungen an Bandbreite, wenn man diese Entwicklung im Rahmen von Server-Konsolidierung einmal durchrechnet. Dazu muss eigentlich nur die Anzahl der in den nächsten Jahren zu konsolidierenden Server und deren jetziger Plattenspeicher bekannt sein. 10 GbE mag der aktuelle Standard für RZ-Netzwerke sein, aber man kann leicht ausrechnen, dass das für die nächsten Jahre zu wenig ist. Wer daran zweifelt, sollte sich für sein Unternehmen dringend mit der Umsetzung von Speicher-Technologien in Netzwerken auseinander setzen.

Stark vereinfacht formuliert entstehen im Rechenzentrum Anforderungen aus einer Kombination aus Latenz und Bandbreite. Dabei ist wichtig, zu verstehen, dass mehr Bandbreite nicht auch mehr Latenz produziert. Dies ist ein im Markt weit verbreitetes Missverständnis (so im Sinne von „100 GbE ist schneller als 1GbE“, was aber natürlich Unsinn ist). Wir haben auf dem Forum einfache Beispielrechnungen mit 1GbE, 10 GbE und 100 GbE-Netzwerken vorgelegt, die sofort klar gemacht haben, dass die Leistung der einzelnen Switch-Systeme selber und die Art ihrer Verschaltung eine entscheidende Rolle für Latenz spielen. Die aus dieser Analyse resultierenden Anforderungen sind relativ einfach zu formulieren:

Das Netzwerk wird zum Systembus: hin zur Matrix der kürzesten Wege!

- Die Switchlatenz pro Switch muss möglichst niedrig sein, hier gibt es bei den Highend-Systemen erste Produkte, die mit 5 Mikrosekunden switchen.

- Die Anzahl der in der Kommunikation zu durchlaufenden Switch-Systeme muss minimal sein. Es muss eine Matrix der kürzesten Wege geben. Tatsächlich ist der Begriff „Matrix der kürzesten Wege“ der Schlüssel zum Verständnis des Netzwerk-Designs im Rechenzentrum der Zukunft.

Steigt man hier tiefer ein (das sprengt den Rahmen dieses Geleits), dann wird klar, dass hier neue Switching-Verfahren gefordert sind, um diese Matrix der kürzesten Wege umzusetzen. Dies wird auch zwangsläufig mit Redundanz kombiniert werden, wobei die Redundanz-Performance selber nicht im Vordergrund steht sondern die Optimierung der System-Latenz.

Wir haben auf dem Forum die beiden in der Entwicklung befindlichen Standards für Shortest Path Bridging der IETF und der IEEE diskutiert und diese auch gegenüber gestellt. Die IETF hat momentan mit dem TRILL-Verfahren die Nase deutlich vorne. Bei der IEEE haben wir die Situation, dass die sehr langsame Arbeit an dem Standard gut dazu führen kann, dass dieser Standard zu spät kommt. Auf dem Netzwerk-Redesign Forum 2010 haben sich dann auch alle anwesenden Hersteller klar zu TRILL bekannt. Cisco betreibt eine proprietäre Form von Shortest Path Bridging bereits jetzt, hat sich auf dem Forum aber auch klar zu TRILL bekannt (was nicht wirklich überraschend ist) und den Upgrade seiner jetzigen Lösung auf TRILL angekündigt (TRILL wurde im April 2010 weitestgehend verabschiedet).

Shortest Path Bridging und das Streben nach der Matrix der kürzesten Wege führen zu neuen Netzwerk-Designs, zu einer neuen Form der Verschaltung von Switch-Systemen. Frau Borowka und Herr Pflüger (Cisco) haben auf dem Forum sehr interessante Denkanstöße in diese Richtung gegeben.

Die sinnlose Auseinandersetzung zwischen der IETF und IEEE ist für den Endanwender ärgerlich, im Endeffekt wird sie auch von Hersteller-Interessen produziert. Wie auch immer, mit dieser Entwicklung ist die Zeit von Spanning Tree endgültig vorbei. Das neue Verfahren ist deutlich besser, deutlich flexibler und skaliert bis in mittelgroße Layer-2-Netzwerke gut. Im Kern arbeitet es wie die MESH-Netzwerke aus den Wireless LANs mit IS-IS.

Da TRILL mit einer Header-Erweiterung arbeitet, entsteht die Frage der Hardware-Kompatibilität mit vorhandenen Komponenten. Diese Frage konnte auf dem Forum nicht geklärt werden, wir arbeiten aber für die Sommerschule an der Klärung dieser sehr wichtigen Frage. Es kann auch gut sein, dass vorhandene Hardware aufgerüstet werden kann, dabei aber etwas an Leistung verliert (weil in der Verarbeitung ein weiterer Zugriff auf den Header erforderlich wird, vergleichbar mit dem Problem der IPv6-Performance).

Die Frage der Hardware-Kompatibilität ist eine der Kernfragen für alle Anwender. Neben TRILL stellt auch DCB erhebliche Anforderungen an die Hardware, speziell um Priority Based Flow Control durch eine Switching Fabric zu signalisieren. Hier wurde auf dem Forum deutlich, dass viele der im Markt vorhandenen Produkte nicht auf DCB aufgerüstet werden können.

Diese Diskussion ist symptomatisch für die aktuelle Entwicklung im Netzwerk- und Switching-Markt. Mehr als 20 neue Standards sind in der Entwicklung. Der Bedarf für diese Standards und die Auswirkung auf vorhandene und zukünftige Netzwerk-Komponenten muss dringend geklärt werden. Ich habe an dem Beispiel der „Netzwerk wird zum Systembus“ Diskussion in diesem Geleit versucht, diese Kausalitätskette ausgehend vom Bedarf und endend bei einem zwangsläufigen Netzwerk-Matrix Design klar zu machen. Aber dies ist nur ein Beispiel, eine umfassende Diskussion und Klärung der Bedeutung aller neuen Standards ist in den Unternehmen erforderlich. Wie immer wird die Betroffenheit sehr von den individuellen Rahmenbedingungen geprägt sein.

Wir helfen bei dieser Diskussion, indem die Sommerschule 2010 diese Entwicklungen aufgreift, analysiert und diskutiert. Dort stellen wir noch einmal alle aktuellen Entwicklungen, den dahinter stehenden Bedarf und die Auswirkungen auf die Netzwerke vor. Im Prinzip vertiefen wir dort die Diskussion, die wir auf dem Netzwerk-Redesign Forum 2010 begonnen haben.

Die nächsten 12 bis 18 Monate werden ohne Frage spannend. Es wird eine Reihe von Veränderungen in der Netzerk-Technologie-Landschaft geben. Bis Ende 2011 entsteht eine neue Situation mit vielen neuen Möglichkeiten.

Wir leben in einer spannenden Zeit,
in diesem Sinne

Ihr
Dr. Jürgen Suppan

Intensiv-Seminar

Sommerschule 2010 - Intensiv-Update auf den letzten Stand der Netzwerktechnik

Die ComConsult Akademie veranstaltet vom 05.07. - 09.07.10 ihr Inteniv-Seminar „Sommerschule 2010“ in Aachen.

Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Neue Standards zur Gestaltung von Netzwerken im Rechenzentrum und im Backbone sind gute Beispiele dafür. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen. Die ComConsult Sommerschule 2010 analysiert und diskutiert diese Änderungen und ihre Auswirkungen speziell auf die Netzwerk-Infrastrukturen.

Die Sommerschule hat folgende Themenschwerpunkte:

- Das Netzwerk wird zum Systembus: was bedeutet das?
  - Anforderungs-Analyse Rechenzentrum
  - Anforderungs-Analyse Backbone/ Campus
  - Anforderungs-Analyse Clients
  - Latenz und Bandbreite: wie hängt das zusammen?
  - Latenz-Anforderungen: wo, wie viel?
  - Bandbreiten-Bedarf: wo, wie viel?
  - Die neue Kommunikations-Matrix im Rechenzentrum
  - Warum wir neue Switching-Standards brauchen
- Speicher im Netzwerk: warum und für wen, ist Fibre-Channel over Ethernet ausgereift genug für den Praxiseinsatz?
  - iSCSI und NFS kontra Fibre Channel: wer gewinnt?
  - iSCSI und NFS im Netzwerk: Bandbreitenbedarf
  - Fibre Channel over Ethernet
  - Ergebnisse einer Analyse: FC-BB-5, Grenzen und Möglichkeiten einer neuen Technologie
- Neue Netzwerk-/Switching Standards
  - Verfügbare Verfahren und ihre Schwächen
  - Layer-2-Multipath, Shortest Path Bridging: IEEE kontra IETF
  - TRILL: der neue Stern am Horizont, was TRILL wirklich leistet
  - Was macht die DCB-Gruppe?
  - IEEE 802.1Qau: Congestion Notification
  - IEEE 802.1Qbb: Priority Based Flow Control
  - IEEE 802.1Qaz: Enhanced Transmission Selection
  - DCB Capability Exchange
  - Virtuelle Bridges
- Wireless LANs nach der Verabschiedung von IEEE 802.11n
  - Was bringt der Standard?
  - Wie sehen zukünftige Produkte aus, was leisten sie?
  - Auswirkungen auf die Planung
  - Leistungsengpässe bei Wireless Switching: skaliert das Verfahren nicht?
  - CAPWAP, das Herz des Wireless Switching: Status
  - Trouble Shooting: was kann passieren, was ist zu tun?
- IPv6: mehr als nur Adressen
  - Motivation: warum es jetzt endlich passiert
  - Basis Konzepte
  - Welche Komponenten sind kritisch?
  - Stateless, stateful, hybrid: warum und für wen?
  - DNS und DHCP: was muss sich ändern?
  - Migrations-Verfahren und ihre Tücken
- Der Netzwerk-Markt: wichtige Bewegungen
  - Wo sind die Grenzen bestehender Produkte?
  - Neue Standards und Produkte: wo sind mögliche Probleme?
  - Wie wichtig wird Bandbreite?
  - Was werden neue Produkte leisten?
  - Was passiert auf der Herstellerseite?
- Netzwerk-Sicherheit: ein neuer Meilenstein mit IEEE 802.1X-2010
  - Warum die bisherige Form von IEEE 802.1X im Kabel-basierten Netzwerk nicht brauchbar ist
  - Was der neue Standard leistet
  - Was das im Alltag bedeutet
  - Wie die Hersteller sich verhalten
- Voice und Video im Netzwerk
  - Warum Codecs wichtig sind
  - Voice im LAN im Umfeld von Unified Communications
  - Voice im WAN: brauchen wir Call Admission Control und wenn ja, wie?
  - Video: Bandbreitenbedarf und Integration externer Kommunikations-Partner

Wir bieten Ihnen bei Buchung dieses Seminars zwei Reports zu einem Sonderpreis an.

Aktuelle Netzwerkstandards in der Analyse

Viele aktuell betriebene Netzwerke stehen vor einem Redesign, da sowohl für den Access / Front End als auch den RZ / Back End Bereich neue Anforderungen entstehen. Dieser aktuelle Report von ComConsult-Research analysiert neue Standards in der Entwicklung bei IEEE, IETF und ANSI/INCITS, die diese Anforderungen abdecken werden, unter funktionalen, designtechnischen und zukunftsstrategischen Gesichtspunkten. Er bildet eine ideale Basis für die Weiterentwicklung bestehender Netzwerke, aber auch eine optimale Grundlage für zukunftsgerichtete Planungen und Ausschreibungen.

Autorin:
Dipl.-Inform. Petra Borowka-Gatzweiler
Veröffentlicht: März 2010
Umfang: 93 Seiten

Netzwerk-Redesign 2010 - Neue Anforderungen, Technologien und Strukturen

Die Anforderungen an Corporate Networks wachsen permanent in jeder Dimension. Neue Technologien wie Virtualisierung vom Server bis zum Desktop erzeugen Abhängigkeiten zwischen Systemen und Netz, die sich nicht nur mit einer reinen Steigerung der Bandbreite beantworten lassen. Wünsche wie Multi-Mandantenfähigkeit, Hochsicherheit, unterbrechungsfreier Betrieb und Reaktionsfähigkeit treiben die Aufgaben eines Corporate Networks vom RZ über den Backbone bis hin zum Access-Bereich exakt in die Nähe der Aufgaben, die ein Provider-System heute hat. Also ist es legitim, über die Frage zu diskutieren, ob man Corporate Networks überhaupt noch so wie gewohnt weiterentwickeln kann oder ob man nicht auch im Corporate Network Provider Technologie einsetzen sollte, um auf die „Provider-Anforderungen“ zu reagieren. Das ist technisch möglich und wirtschaftlich durchaus vertretbar.

Autor: Dr. Franz-Joachim Kauffels
Veröffentlicht: April 2010
Umfang: 213 Seiten

Sommerschule 2010 - Intensiv-Update auf den letzten Stand der Netzwerktechnik

Frühbucherrabatt bis 31.05.10

Sommerschule 2010

05.07. - 09.07.10 in Aachen

Für Besucher unserer bisherigen Kongresse/Seminare bzw. für die Teilnehmer am VIP-Verteiler bieten wir Ihnen exklusiv eine Vorbuchungsphase für die Sommerschule 2010 bis zum 31.05.2010 für eine rabattierte Teilnahmegebühr an.

Sommerschule 2010
zum Preis bei Buchung bis 31.05.10 von € 2.090,-- zzg. MwSt.
statt regulär € 2.290,-- zzg. MwSt.

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sommerschule 2010

Ich buche das Seminar
Sommerschule 2010

☐ 05.07. - 09.07.10 in Aachen
zum Preis von € 2.090,--* zzgl. MwSt.
* gültig bis zum 31.05.10

☐ inkl. Report „Aktuelle Netzwerk-standards in der Analyse“
zum Sonderpreis von € 210,--

☐ inkl. Report „Netzwerk-Redesign 2010“ zum Sonderpreis von € 210,--

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 10

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2010

Die ComConsult Akademie veranstaltet vom 07.06. - 08.06.10 ihren Kongress „ComConsult IT-Sicherheits-Forum 2010“ in Königswinter.

Schwerpunktthema des diesjährigen IT-Sicherheits-Forums ist die Sicherheit im Rechenzentrum. Der massive Einsatz der Server-Virtualisierung erfordert neue Sicherheitskonzepte für den Umgang mit der Dynamik und Mobilität von VMs und für den Aufbau von Sicherheitszonen im Rechenzentrum. Damit einhergehend drohen Cloud-Konzepte in das Rechenzentrum einzuziehen und eine neuartige Risikolage zu schaffen.

Das aktuelle Redesign im Rechenzentrum steht häufig im krassen Gegensatz zu klassischen Konzepten der IT-Sicherheit. Beispielsweise ist die Vorgabe, dass VMs mit einem unterschiedlichen Sicherheitsniveau nicht auf einem gemeinsamen physischen System laufen dürfen, in der Praxis immer schwerer durchsetzbar. Im Sinne eines möglichst hohen Konsolidierungsgrads wird nicht selten sogar der Wunsch geäußert, selbst eine Internet DMZ innerhalb der gleichen Virtualisierungsumgebung abzubilden, wie die internen Serverbereiche. Dem steht eine erschreckend lange Liste mit gemeldeten Sicherheitslücken in Virtualisierungs-Produkten gegenüber. Aus einer Sicherheitsperspektive muss man hier nicht nur die Herstelleraussagen kritisch prüfen, sondern auch darüber nachdenken, wie ein Patch-Management für Virtualisierungslösungen angesichts der extrem hohen Verfügbarkeitsanforderungen noch sinnvoll gestaltet werden kann.

Diese Trends haben auch Auswirkungen auf die Sicherheit in SAN und NAS. Hier stellt sich zunächst die Frage, wie konsequent die Zonierung in Server-Bereich und LAN auch im SAN fortgesetzt werden muss und ob die Mittel der logischen SAN-Zonierung ausreichen.

Wir erleben im Moment einen konsequenten Umschwung weg von einer an Fat Clients orientierten IT hin zur Anwendungs- und Desktop-Virtualisierung. Aus einer Sicherheitsperspektive ist hier entscheidend, dass Ressourcen, die bisher im Campus-LAN verteilt waren, plötzlich zentral in das Gehirn der IT-Infrastruktur - das RZ - rücken. Eine Infektion eines Clients mit einer schadenstiftenden Software breitet sich plötzlich nicht mehr im Campus-LAN aus, sondern würde direkt in zentralen Komponenten im RZ wirken. Hier müssen für die verschiedenen in Frage kommenden Techniken die Gefährdungslage analysiert und die bestehenden Maßnahmenkataloge für die Endgerätesicherheit angepasst werden.

Die Entwicklung zur Desktopvirtualisierung stellt auch fundamentale Konzepte der LAN-Sicherheit in Frage. Wenn Clients zentral im RZ laufen bzw. Anwendungen nur noch zentral zur Verfügung gestellt werden, muss beispielsweise diskutiert werden, ob überhaupt noch eine Notwendigkeit für eine Netzzugangskontrolle besteht. Denn letztendlich bedeuten diese Entwicklungen, dass sich das für das Intranet zu schaffende Sicherheitsniveau immer mehr reduziert und sich dafür wesentliche Aspekte der IT-Sicherheit in das RZ verlagern.

Auf eine Sicherheit für die physischen Endgeräte wird jedoch nicht verzichtet werden können, denn Fat Clients werden uns mit Notebooks zunächst in der klassischen Art erhalten bleiben und müssen entsprechend abgesichert werden. Interessant ist in diesem Zusammenhang aber die Frage, wie sich Smartphones weiter entwickeln werden, denn dass diese ein ausgesprochen interessantes Angriffsziel darstellen, auf dem vertrauenswürdige Daten lagern können und das sich vorzüglich als Transportwirt für schadenstiftende Software eignet, ist keineswegs neu. Neu ist die Tatsache, dass Smartphones der Normalfall geworden sind und ein fast unüberschaubarer Zoo an Anwendungen sich explosionsartig entwickelt hat.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult IT-Sicherheits-Forum 2010

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2010

☐ 07.06. - 08.06.10 in Königswinter
zum Preis von € 1.690,-- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis _____ 10

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

ComConsult IT-Sicherheitsforum 2010 - Programmübersicht

Montag, den 07.06.2010

9:30 - 10:30 Uhr

Keynote: RZ im Wandel - Herausforderung an die IT-Sicherheit

- Konsequenzen der Virtualisierung für Sicherheitskonzepte und -prozesse
- Geänderte Rolle des Intranet angesichts Desktop- und Anwendungsvirtualisierung: Brauchen wir noch eine Netzzugangskontrolle?
- Aufbau von Sicherheitszonen im RZ jenseits von 10 Gbit/s: Hochleistungs-Appliances, MACsec und Co.
- Sicherheit auf Ebene der Anwendung oder Pauschalmaßnahmen auf Netzebene?
- Risiko Kurzschluss von Sicherheitszonen im Storage-Bereich

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 12:00 Uhr

Methodische RZ-Sicherheit mit den BSI IT-Grundschutz-Katalogen

- Umbruchphase: Sicherheitskonzepte für das moderne RZ
- RZ-Sicherheit: bestehende und geplante relevante Bausteine der IT-Grundschutz-Kataloge
- Umgang mit der Dynamik und Mobilität der Virtualisierung in den Prozessen zur IT-Sicherheit
- Was thematisiert der neue Baustein zur Virtualisierung?

Oliver Flüs, ComConsult Beratung und Planung GmbH

12:00 - 12:45 Uhr

Auswirkungen der Desktop- und Anwendungsvirtualisierung auf die IT-Sicherheit

- Gefährdungen durch Zentralisierung von Clients
- Sind neue Konzepte beispielsweise für den Virenschutz erforderlich?
- Wie sicher sind Terminal Server wirklich?
- Vergleich der Herstellerkonzepte zur Desktop-Virtualisierung

Matthias Egerland, ComConsult Beratung und Planung GmbH

12:45 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr

Sorgenkind Datenbanksicherheit

- Datenbank-Hacking, SQL-Injection und andere Gefährdungen
- Sicherheitsmaßnahmen für Datenbanken
- Sichere Datenbankzugriffe über Portal-Architekturen: erfolgreiche Risikoverlagerung?
- Schatten-Datenbanken

Oliver Flüs, ComConsult Beratung und Planung GmbH

14:45 - 15:30 Uhr

Sicherheit von Web-Anwendungen

- Verbreitete Schwachstellen und Angriffstechniken
- Herangehensweisen zur Absicherung von Web-Anwendungen
- Best-Practices und Hilfe zur Selbsthilfe (BSI, OWASP)
- Automatische Sourcecodeanalyse
- Einsatzvarianten von Web Application Firewalls (WAFs)

Thomas Schreiber, SecureNet GmbH

15:30 - 16:00 Uhr Kaffeepause

16:00 - 16:45 Uhr

Konzepte für den Aufbau von Sicherheitszonen im RZ

- Zwiebelschalenmodell: Wie praxistauglich ist ein mehrschichtiger Zonenaufbau?
- Kriterien für die physikalische Trennung und die Virtualisierung von Netzen und Servern
- Umgang mit Administrationsbereichen und Konsolennetzen
- Anforderungen an Firewalls, Intrusion-Prevention-Systeme und Security Gateways
- Verschlüsselung mit 10 GBit/s und mehr: Technologien und Hersteller
- Link Layer Encryption: Proprietäre Produkte oder wo steht MACsec?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:45 - 17:30 Uhr

Unified Communications über Vertrauensgrenzen hinweg

- Virtualisierung von Unified Communications (UC) aus dem Blickwinkel der IT-Sicherheit
- Problem Firewalling von VoIP und Unified Communications (UC)
- VoIP und UC im WAN
- Umgang mit Verschlüsselung von Medienstrom und Signalisierung in Firewall-Architekturen
- Rolle von Session Border Controllern
- Einbindung mobiler Nutzer und Heimarbeitsplätze

Axel Borchers, Siemens Enterprise Communications

ab 18:00 Uhr Happy Hour

Dienstag, den 08.06.2010

9:00 - 10:00 Uhr

Sicherheit in SAN und NAS

- Welche Gefährdungen sind in SAN und NAS relevant?
- Maßnahmen zur Absicherung von SAN und NAS-Elemente einer SAN-Sicherheitsrichtlinie • Konzepte für eine Zonierung im SAN
- Wann sollte verschlüsselt werden?
- Projekterfahrungen zur Verschlüsselung im SAN

Matthias Egerland, ComConsult Beratung und Planung GmbH

10:00 - 10:45 Uhr

Infrastruktur-Sicherheit im RZ

- Was passiert, wenn die Zutrittskontrolle streikt und den Zugang zum RZ verweigert?
- Zutrittskontrolle, Vereinzelungsanlagen, Video-Überwachung, etc.: Auch die Infrastruktur-Sicherheit braucht aktive Komponenten, die angemessen abgesichert werden müssen
- Elektromagnetische Verträglichkeit: ein unterschätztes Risiko?
- Stromausfall: immer noch der Präzedenzfall für die Notfallvorsorge

Hartmut Kell, ComConsult Beratung und Planung GmbH

10:45 - 11:15 Uhr Kaffeepause

11:15 - 12:30 Uhr

Security Appliances, Firewalls und IPS im Hochleistungsbereich

- Load-balancing und Load Sharing: Was geht wirklich?
- Wie sinnvoll sind Layer 2 Firewalls?
- Ist ein Durchsatz von 10 Gbit/s und mehr tatsächlich bei einem produktiven Regelwerk noch realistisch?
- Einsatzmöglichkeiten virtueller Firewalls
- Leistungsgrenzen von Intrusion- Prevention-Systemen
- Hersteller im Vergleich (Juniper, Checkpoint, Tipping Point)

Andreas Meder, ComConsult Beratung und Planung GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr

Sicherheit und Nachvollziehbarkeit administrativer Zugriffe

- Identity Management für privilegierte administrative Zugriffe
- Protokollierung von Adminstrationssitzungen auf Servern und Netzkomponenten
- Verfügbare Lösungsansätze und ihre Grenzen
- Marktüberblick und Auswahlkriterien

Stefan Strobel, Cirosec GmbH

14:45 - 15:30 Uhr

Grenzen der Protokollierungim Netz

- Folgen der Verfassungsgerichtsentscheidung zur Vorratsdatenhaltung
- Änderungen am Datenschutzgesetz
- Empfehlungen zur Protokollierung in Netzkomponenten und Servern
- Neue Regeln zur Auftragsdatenverarbeitung

Ulrich Emmert, e/s/b Rechtsanwälte

Ende der Veranstaltung 15:30 Uhr

Aktueller Kongress

ComConsult Wireless-Forum 2010
Early-Bird-Phase bis zum 30.06.2010

Die ComConsult Akademie veranstaltet vom 04.10. - 06.10.10 ihren Kongress „ComConsult Wireless-Forum 2010“ in Königswinter.

Wireless LANs (WLANs) sind erwachsen geworden, und der Aufbau für Produktion, Logistik und Büro ist scheinbar Routine. WLANs werden auch zunehmend für kritische Anwendungen eingesetzt und spätestens seit der Verabschiedung von IEEE 802.11n wird sogar die Frage gestellt, ob WLAN bereits eine echte Alternative zur kabelbasierten Endgeräte-Anbindung darstellen.

WLANs unterliegen dabei einer permanenten Weiterentwicklung und Veränderung. Hier müssen wir diese Entwicklungen einschätzen:

- IEEE 802.11n
  - Welche Produkte gibt es bereits mit 450 Mbit/s und wann kommen Produkte mit vier Spatial Streams, d.h. 600 Mbit/s auf den Markt?
  - Welcher Durchsatz kann tatsächlich erreicht werden?
  - Wie beeinflusst IEEE 802.11n tatsächlich das WLAN-Design und welche Auswirkungen bestehen auf das Controller-basierte WLAN-Design?
  - Stromversorgung der Access Points: Bewährt aber mit Einschränkungen über IEEE 802.3af, Einsatz proprietärer Techniken oder kann schon auf IEEE 802.3at gebaut werden?
- Controller-basiertes WLAN-Design
  - Wie unterscheiden sich die Konzepte der Hersteller für ein Controller-basiertes WLAN-Design - konsequente CAPWAP-Nutzung oder herstellerspezifische Funktionen?
  - Aufbau von hochverfügbaren Controller-Systemen
- Sinn und Unsinn von Local Bridging
  - Absicherung der Kommunikation zwischen Thin AP und WLAN Controller: Authentisierung, Verschlüsselung von Kontroll- und Datenkanal
- Frequenzmanagement
  - Notwendigkeit eines Frequenzmanagements
  - Strategien für die Zuteilung bei 2,4 GHz und bei 5 GHz
  - Kostbare Kapazität: Die unteren 100 MHz bei 5 GHz
- Sicherheit
  - Wie unsicher ist TKIP wirklich und welche Maßnahmen sollten ergriffen werden?
  - Notwendigkeit der Migration von TKIP zu CCMP: Warum höhere Datenraten bei IEEE 802.11n den Einsatz von CCMP erfordern
- Ortung - Die Ortung von Geräten hat sich als wichtige WLAN-Anwendung herauskristallisiert.
  - Welche Genauigkeiten können unter welchen Rahmenbedingungen mit den verschiedenen Systemen realisiert werden?
  - Müssen für Ortungssysteme spezielle Vorgaben an die Ausleuchtung berücksichtigt werden und wie kann dies mit der Zellplanung für die Datenkommunikation harmonisiert werden?
  - Mesh-Netze - Mesh-Netze versprechen den WLAN-Einsatz für Bereiche, in denen kein kabelbasierter Anschluss von Access Points sinnvoll möglich ist.
  - Welche Einsatzszenarien sind relevant?
  - Was wird mit IEEE 802.11s kommen und wie unterscheiden sich derzeit die Produkte der Hersteller?
  - Welche Leistung kann erreicht werden und wie plant man Mesh-Netze?
- Recht
  - Gastzugang über WLAN: Immer noch (oder schon wieder) in der Grauzone der Rechtssprechung?
  - Welche Daten sollten protokolliert werden und wann ist Vorsicht geboten?
- Trends
  - Welche neue Anwendungsbereiche von WLAN zeichnen sich ab, z.B. die Nutzung von WLAN für die Verkehrstelematik?
  - Welche drahtlosen Kommunikationstechniken spielen neben WLAN eine Rolle?

Hier setzt das ComConsult Wireless-Forum 2010 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Design drahtloser Kommunikationsnetze und deren zukunftsorientierter Auslegung für einen stabilen und zuverlässigen Betrieb.

Fax-Antwort an ComConsult 02408/955-399

über 15% Rabatt

Anmeldung
ComConsult Wireless-Forum 2010

über 15% Rabatt

Ich buche den Kongress
ComConsult Wireless-Forum 2010

☐ 04.10. - 06.10.10 in Königswinter
zum Preis von € 1.590,--* zzgl. MwSt.

* gültig bis zum 30.06.10

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 10

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Zweitthema

Dipl.-Inform. Nick Schirmer ist bei der ComConsult Beratung und Planung GmbH auf Unified-Communications- und Fixed-Mobile-Convergence-Lösungen spezialisiert. Darüber hinaus konnte er in zahlreichen Projekten Erfahrungen bei der Planung und Implementierung von komplexen Kommunikationslösungen sammeln. Weitere Schwerpunkte seiner Arbeit liegen in der Konzeption von Test-Umgebungen sowie in der Durchführung von umfangreichen Produkttests im ComConsult-eigenen Test-Center.

Dr. Frank Imhoff ist Technischer Direktor der ComConsult Beratung und Planung GmbH. Er leitet dort den Bereich Applikationen. Unter seiner Verantwortung sind bereits zahllose Beratungsprojekte zu den Themen Voice, Unified Communications, Collaboration, Messaging, Mobilfunk etc. erfolgreich durchgeführt worden.

Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich bereits auf moderne Kommunikationsnetze und Betriebssysteme. Zu seinen Spezialgebieten gehören jetzt u.a. die Konzeption und Ausschreibung professioneller Unified-Communications- und Kollaborations-Systeme sowie Microsoft-Lösungen.

Microsoft Exchange 2010: Hochverfügbarkeit On-Premise oder als Hosted-Service

Fortsetzung von Seite 1

Schon mit Exchange 2007 wurde deutlich, dass der Fokus von Microsoft zunehmend auf große Installationen gerichtet ist. Gleichzeitig wurde der zunehmenden Bedeutung von Messaging in den Unternehmen Rechnung getragen, indem höhere Zuverlässigkeitswerte angestrebt wurden. Exchange 2010 setzt diese Entwicklung konsequent fort und geht noch ein Stück weiter: Mit der neuesten Version von Exchange erhalten Benutzer mehr Möglichkeiten, Inhalte bereitzustellen, eine laut. Microsoft deutlich gesteigerte Benutzerfreundlichkeit sowie integrierte Funktionen zur Vermeidung von Informationslücken und zur Gewährleistung von Compliance. Damit wird Exchange auch für sehr große Konzerne immer interessanter, die heute häufig noch IBM Lotus Notes nutzen.

Hochverfügbarkeitskonzept

Mit der Einführung von Database Availability Groups (DAG) wird die Exchange 2007 Logik von Cluster Continuous Replication (CCR), Standby Continuous Replication (SCR) und Local Continous Replication (LCR) wieder abgeschafft (siehe Abbildung 1). Exchange 2010 führt stattdessen Cluster- und Standby Continous Replication innerhalb der DAG unter Verwendung unterschiedlicher Server zusammen und bietet so die Möglichkeit, auf eine zusätzliche LCR zu verzichten. Die Unterstützung von bis zu 16 Servern im Windows Cluster mit bis zu 100 Datenbanken pro Server bietet eine enorme Sicherheit, da jede Datenbank auf mehrere Server repliziert wird.

Mittels einer geeignet geplanten Verteilungsstrategie ist es möglich, auf eine lokale Absicherung der Festplatten per Disk-RAID zu verzichten, da im Fehlerfall die auf einem anderen Server ebenfalls vorhandene Datenbank aktiviert und weiter betrieben werden kann. Durch die Verteilung mehrerer einzelner Datenbanken auf verschiedene Server ist bei Ausfall einer oder mehrerer Datenbank bzw. eines Servers nicht die Aktivierung eines ganzen Servers, sondern lediglich die Aktivierung der betroffenen Datenbanken auf einem bereits laufenden Server notwendig. Da nun ein Failover nicht mehr je Server, sondern je Datenbank durchgeführt wird, liegt hier ein klarer Performance-Vorteil. Weitere Vorteile ergeben sich aus der einfachen Möglichkeit zur Lastverteilung und der Option, durch bewusste Verwendung von Verzögerungen in der Replikationsstrategie mehrere Versionen eines Datenbestandes vorzuhalten. Auf diese Weise sind kleinere Rückschritte bei Inkonsistenz von Datenbeständen auch ohne großen Aufwand zu realisieren.

Bereits mit der letzten Version von Exchange 2007 wurde durch Einführung der Client-Access-Server-Rolle (CAS) der

Microsoft Exchange 2010: Hochverfügbarkeit On-Premise oder als Hosted-Service

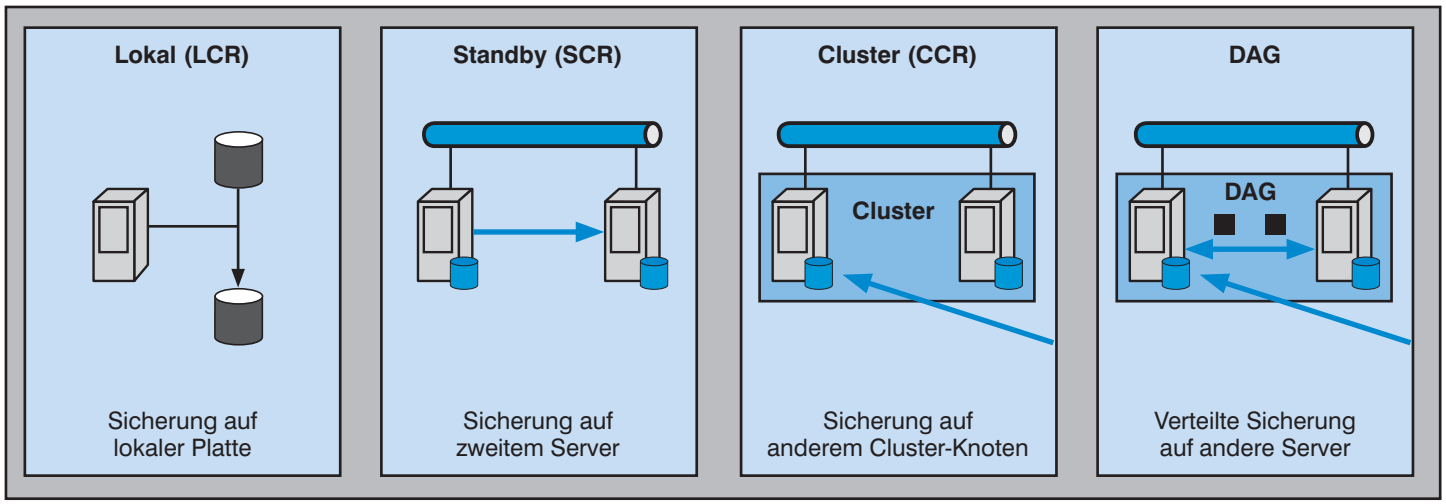


Abbildung 1: Replikations-Mechanismen

Client-Zugriff für Outlook-Web-Access (OWA), ActiveSync, POP3, IMAP4, RPC/HTTP und - mittels HUB/Transport-Rolle - auch SMTP zur Erhöhung der Sicherheit explizit über diese Access Server umgeleitet und in MAPI-Zugriffe auf den Postfachserver umgesetzt. Mit Exchange 2010 benötigt auch Outlook keine direkte Verbindung zum Postfachserver mehr, was bei der Dimensionierung der CAS-Server zu beachten ist. Auf diese Weise werden alle Client-Zugriffe zu einem oder einer Gruppe von CAS-Servern geleitet, die dann stellvertretend die Zugriffe auf den aktuellen Postfachserver durchführen.

Speicherflexibilität

Aufgrund der hohen Datenzugriffsraten der bisherigen Exchange-Versionen mussten höhere Mindestanforderungen an Daten- und Arbeitsspeicher gestellt werden. Nur auf diesem Weg konnte Exchange noch mit akzeptabler Performance seine Dienste erbringen. Durch eine Reduzierung der benötigten Input/Output-Operationen mit jeder neuen Exchange-Version konnten diese Anforderungen weiter gesenkt werden (vergleiche Abbildung 2).

Diese Entwicklung ermöglichte Exchange eine höhere Flexibilität in der Auswahl des zu verwendenden Speichers. Exchange 2010 unterstützt nun neben den bisherigen Speichermöglichkeiten Storage Area Network (SAN) und direkt angeschlossene Serial-Attached-SCSI-Disks (SAS) auch direkt angeschlossene SATA-Festplatten und Just a Bunch Of Disks (JBOD) ohne Performance einbußen.

Exchange out of the Cloud

Zunehmende Verfügbarkeit und sinkende Kosten für höhere Bandbreiten sowie eine verbesserte Ausfallsicherheit haben dazu geführt, dass immer mehr Dienste zum Beispiel als Hosted Services ausgelagert werden können. Neben der lokalen Installation bietet Exchange 2010 die Möglichkeit, Postfächer nicht mehr selbst verwalten zu müssen, sondern diese Tätigkeit an Dienstleister zu übertragen. Microsoft selbst bietet mit Exchange Online gehostete Postfächer für seine Kunden an. Die neue Version von Exchange bietet im Sinne verbesserter Föderations-Möglichkeiten auf diesen Zweck hin abgestimmte Verwaltungswerkzeuge innerhalb seines Exchange Control Panels an. So bleibt, trotz des eingeschränkten Server-Zugriffs der lokalen IT, ein gewisser Grad an Konfigurationsmöglichkeit erhalten. Die von Microsoft bewusst eingeplanten engen Verknüpfungsmöglichkeiten von gehosteten und lokalen Postfächern ermöglichen eine kosten- und funktionsorientierte Mischlandschaft.

Das Angebot attraktiver Lizenzmodelle als Alternative zu einer selbst betriebenen Lösung und der Kostendruck, der Firmen zum Outsourcing von Lösungen veranlasst, bieten Anlass, eine vollständig gehostete oder die Koexistenz einer gehosteten und einer lokalen Installation von Exchange 2010 als zusätzliche Option in Betracht zu ziehen (siehe Abbildung 3). Fraglich ist, ab welcher Nutzerzahl und welchem Funktionsumfang sich welches Modell tatsächlich rechnet. Aber es ist eine Option, die man bei zukünftigen Mi-

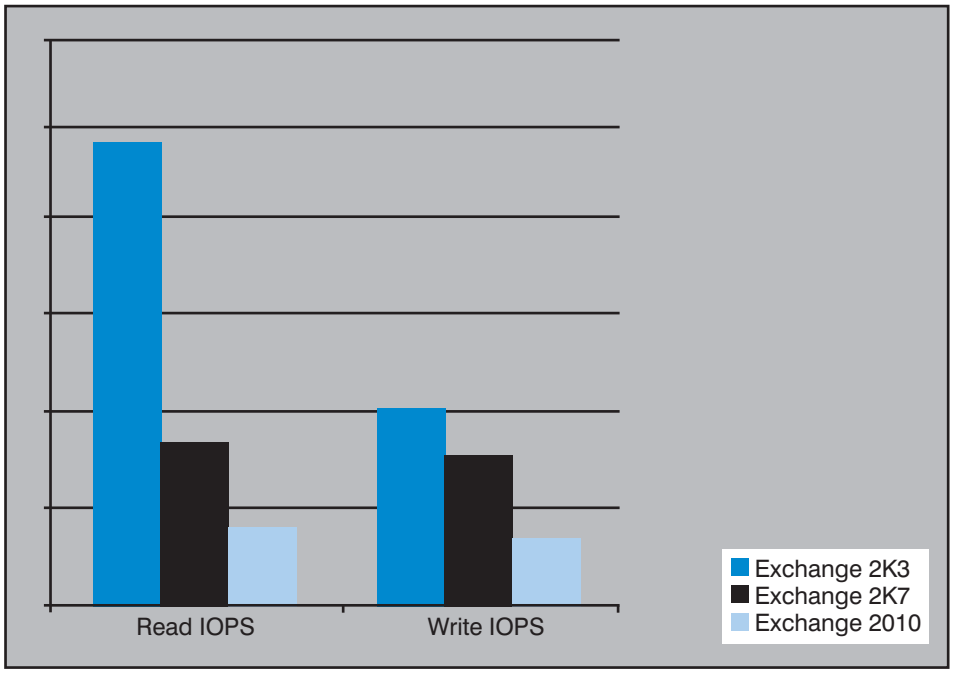


Abbildung 2: Vergleich notwendiger Zugriffsoperationen Quelle: Microsoft

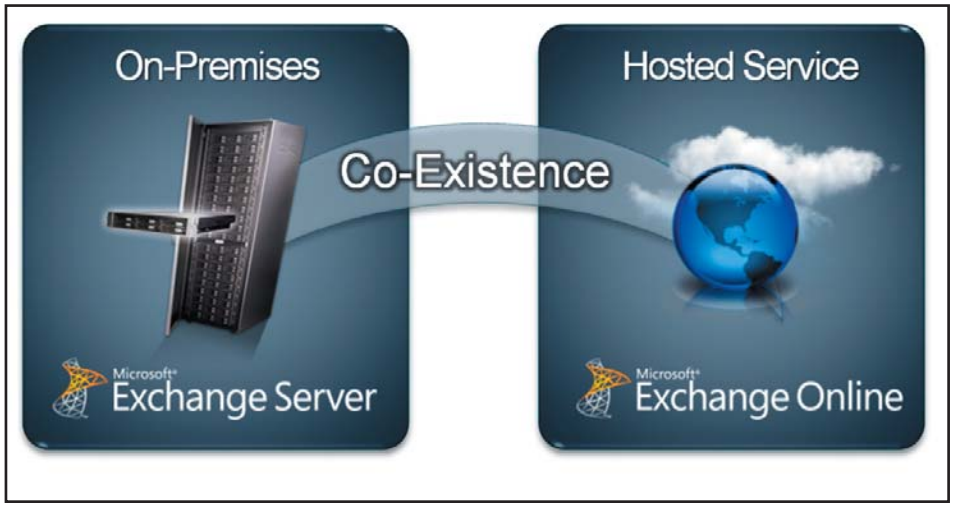


Abbildung 3: Lokaler und Hosted Exchange können koexistieren Quelle: Microsoft

grationsszenarien sicherlich nicht außer Acht lassen sollte.

Man sollte allerdings nicht allein die Kosten für Anschaffung, Installation und Betrieb eines eigenen Exchange Servers gegen die Angebote von externen Dienstanbietern rechnen. In jedem Fall muss der eventuell eingeschränkte Funktionsumfang einer Lösung in der Cloud berücksichtigt werden. Da die eigene IT nur noch begrenzt Zugriff auf die Server hat, ergeben sich eventuell Einschränkungen relevanter Funktionen, die eine gehostete Lösung für einige Firmen uninteressant machen könnte.

Dementsprechend sind die jeweilig zutreffenden Aspekte im Einzelfall zu prüfen und die damit verbundenen Konsequenzen in die Betrachtung mit einzubeziehen. Aus diesem Grund sollen hier exemplarisch einige Denkanstöße aufgelistet werden:

- Funktionseinbußen durch Installation von Exchange und OCS in unterschiedlichen Forrests
- Fehlende Möglichkeiten zur Integration eigener Dienste in Exchange (z.B. Transport Regeln)
- Maßgeschneiderte Anbindung, Zugriff von Anwendungen wie ERP, CRM, usw.
- Schutz und Verschlüsselung - Beim Provider müssen Konten mit entsprechenden Rechten vorhanden sein, um weiterhin Zugriff auf alle E-Mails zu haben

Sicherlich kann man im Hinblick auf den Zugriffsschutz den Einwand erheben, dass Exchange 2010 die Möglichkeit bietet, eingehende Mails mit Rights Management Services (RMS) zu sichern, so dass nur noch berechtigte Kreise Zugriff erhalten. Hier sollte man jedoch bedenken, dass beispielsweise das Archivkonto und der Virenscanner ebenfalls diese E-Mails lesen können müssen, da sie ansonsten ihre Funktion nicht erfüllen können und das Management der Rechte in der Hand des Administrators der Lösung liegt.

Bedienung

Die Exchange 2010 Microsoft Management Console (MMC) wurde um einige neue Funktionen erweitert, ist aber dennoch auch für weniger versierte Administratoren übersichtlich geblieben. Ein Großteil der erweiterten Funktionen ist auch diesmal nur über die Powershell, bzw. die Remote-Powershell zu erreichen. Einige der neuen über das Graphical-User-Interface (GUI) zu bedienenden Funktionen sind:

- Anwendung von Änderungen auf mehrere markierte Objekte gleichzeitig (Massenänderungen)
- Organisationsübersicht (Anzahl Server, Anzahl Empfänger und Anzahl der erforderlichen Lizenzen)
- Management der Database Availability Groups (DAGs)
- Management der integrierten Archivierungsfunktion
- Management von Zertifikaten
- Management über mehrere Exchange Organisationen hinweg

Auch wenn es nicht zu den häufigsten Aufgaben eines Administrators gehört, das Postfach eines Nutzers von einem Server auf einen anderen zu verschieben, so ist das neue Feature des Online-Mailbox-Movements sicherlich eine zu begrüßende Verbesserung. Gerade in Anbetracht der wachsenden Größe der Postfächer war die benötigte Zeit zum Verschieben des Postfachs und die damit verbundene Offline-Zeit des jeweiligen Nutzers unerträglich lang. Beim Verschieben eines Postfachs zwischen zwei Exchange 2010 Servern kann dies nun durch den Verwaltungsserver als „Job“ im Hintergrund durchgeführt werden. Dabei werden die Daten erst kopiert und im Anschluss synchronisiert, weshalb das Postfach des Nutzers lediglich für den Zeitraum der Synchronisation und somit eine deutliche geringere Zeitspanne als bisher offline ist.

Eine weitere nützliche Erweiterung ist die integrierte Archivierungsfunktion. Sie bietet zwar nicht denselben Leistungsumfang wie darauf spezialisierte Lösungen von Drittherstellern, deckt aber die wichtigsten Aspekte ab. So können Archivierungsregeln sowohl auf die gesamte Mailbox, einzelne Ordner, einzelne Nachrichten oder ganze lokale persönliche Outlook-Dateien (PST-Dateien) angewendet werden. Bei ausreichender Berechtigung besteht nun mit der erweiterten Suche von Exchange 2010 die Möglichkeit, die Suche nach E-Mails auf mehrere Postfächer auszudehnen. Die neuen Funktionen erleichtern die Einhaltung von Vorgaben und Richtlinien im Rahmen der Aufbewahrungsvorgaben sowie das Auffinden von Nachrichten z.B. als Nachweis im Rahmen eines Rechtstreits.

Um einen zuverlässigeren Versand einer E-Mail vom Absender bis zum Empfänger zu ermöglichen, verwendet Exchange 2010 ein Bestätigungsverfahren zwischen den Station auf dem Weg der Nachricht. Dabei durchläuft die E-Mail wie gewohnt den Weg vom Exchange Server über einen oder mehrere Hub-/Transport-Server zu internen Empfängern oder über Gateways zu externen Postfächern, wird aber nicht wie bisher nach erfolgreichem Versand einer Station dort direkt gelöscht. Durch die Übermittlung von SMTP-Nachrichten zwischen benachbarten Servern werden Statusmeldungen zum Versand der E-Mail ausgetauscht. Ein Hub-/Transport-Server behält die E-Mail auch nach der Weiterleitung an die nächste Station in seinem Transport-Cache, bis er vom nachfolgenden Server die Mitteilung erhält, dass dieser die Nachricht ebenfalls erfolgreich zugestellt hat. Bleibt die Bestätigung z.B. aufgrund des Ausfalls eines Transport-Servers aus, so hat die vorherige Station die E-Mail noch gespeichert und kann diese entweder über einen anderen Weg oder den wieder hergestellten Server erneut versenden.

Das Exchange Control Panel (ECP) bietet dem Administrator die grundlegenden Konfigurations- und Delegations-Möglichkeiten. So kann ein Administrator damit Benutzern die Berechtigung erteilen, eigene Verteilerlisten und deren Mitglieder selbstständig über Exchange zu verwalten. Zudem bietet das ECP den Anwendern eine Reihe nützlicher neuer Möglichkeiten, wie die Nachverfolgung des Übermittlungszustands ihrer Nachrichten mittels Message Tracking und Delivery Report. Weiterhin bietet das ECP den Anwendern die Möglichkeit, unter dem Punkt SelfService bestimmte Felder ihres Active-Directory-Eintrages (wie z.B. die Eintragung im Feld Mobilfunknummer) selbst zu aktualisieren. Dieses Feature kann zwar zur Entlastung des jeweiligen IT-Supports beitragen, fordert aber von den Nutzern ein gewisses Maß an Zuverlässigkeit.

Die durch Exchange 2010 erzeugten Mail-Tipps, die beim Erstellen - also vor dem Versand einer E-Mail in Outlook 2010 - bereits im Kopf der E-Mail angezeigt werden, sollen ebenfalls eine sichere und fehlerfreie Übermittlung einer E-Mail begünstigen (vergleiche Abbildung 4). Beispiele für Mailtipps sind:

- Hinweise auf eingestellte automatische Antworten von Absendern (Abwesenheitsnotiz)
- Hinweis auf verbotene Empfänger
- Hinweis auf ungültige Mailadressen
- Hinweis auf eine zu große E-Mail
- Hinweis auf die Verwendung zu vieler Empfänger
- Hinweis auf den Versand an Externe Empfänger

Es bleibt abzuwarten, welche weiteren Tipps im Zusammenspiel mit Office 2010 beim endgültigen Release zur Verfügung stehen werden und ob man diese einzeln aktivieren kann. Auch wenn einige der Hinweise sicherlich als sehr hilfreich einzustufen sind, kann man doch davon ausgehen, dass der normale Nutzer dazu neigt, Informationen, die sich als für ihn unwichtig erwiesen haben, dann auch im Ausnahmefall zu ignorieren. Außerdem werden einige der Tipps nur unterstützt, wenn das Postfach des Empfängers ebenfalls von Exchange 2010 verwaltet wird.

Zusätzliche Verbesserungen für Nutzer sind sicherlich die funktionalere Unterstützung weiterer Browser für OWA 2010 und die nun auch hier integrierte Konversationsansicht. Somit wird der Ansatz, das Aussehen von Outlook 2010 möglichst detailgetreu im Browser abzubilden, auch auf Firefox und Safari angewendet. Durch die erweiterte Kompatibilität stellt der Server nun auch für andere Browser als den Internet Explorer eine deutlich leistungsfähigere, übersichtlichere und funktionalere Bedienoberfläche zur Verfügung. Thematisch zusammengehörende Nachrichten werden Newsgroup-ähnlich gruppiert dargestellt. Um auch namentlich die Zugehörigkeit zu Microsofts Web Apps 2010 zu demonstrieren, wurde die Bedeutung, die sich hinter der Abkürzung OWA verbirgt, von „Outlook-Web-Access“ in „Outlook-Web-Apps“ umgetauft. Zusätzlich können bei Verwendung von Microsofts Sharepoint Foundation (ehemals Sharepoint Services) die Office Anwendungen Word, Excel, PowerPoint und OneNote als Office Web Apps im Browser dazu verwendet werden, entsprechende Dokumente nicht nur anzuzeigen, sondern auch direkt im Browser zu bearbeiten.

Unified Communications & Collaboration

Wie anfangs erwähnt erhalten die Groupware-Systeme nicht zuletzt aufgrund der sich verbreitenden Unified-Communications-Lösungen erhöhte Aufmerksamkeit. Aus eigener Erfahrung sei hier angemerkt, dass die Unified-Messaging-Kopplung von Exchange 2007 und Microsoft Office Communications Server R2 zwar den Umfang an Unified-Messaging-Features deutlich erweitert, die dafür durchzuführenden Integrationsschritte aber nicht gerade als selbsterklärend und benutzerfreundlich zu bezeichnen waren. Dementsprechend erfreulich ist, dass Microsoft auch diesen Aspekt in der neuen Version berücksichtigt und die Unified-Messaging-Kopplung von Exchange 2010 deutlich benutzerfreundlicher gestaltet hat. So wird deutlich, dass Exchange 2010 das Unified-Communicati-

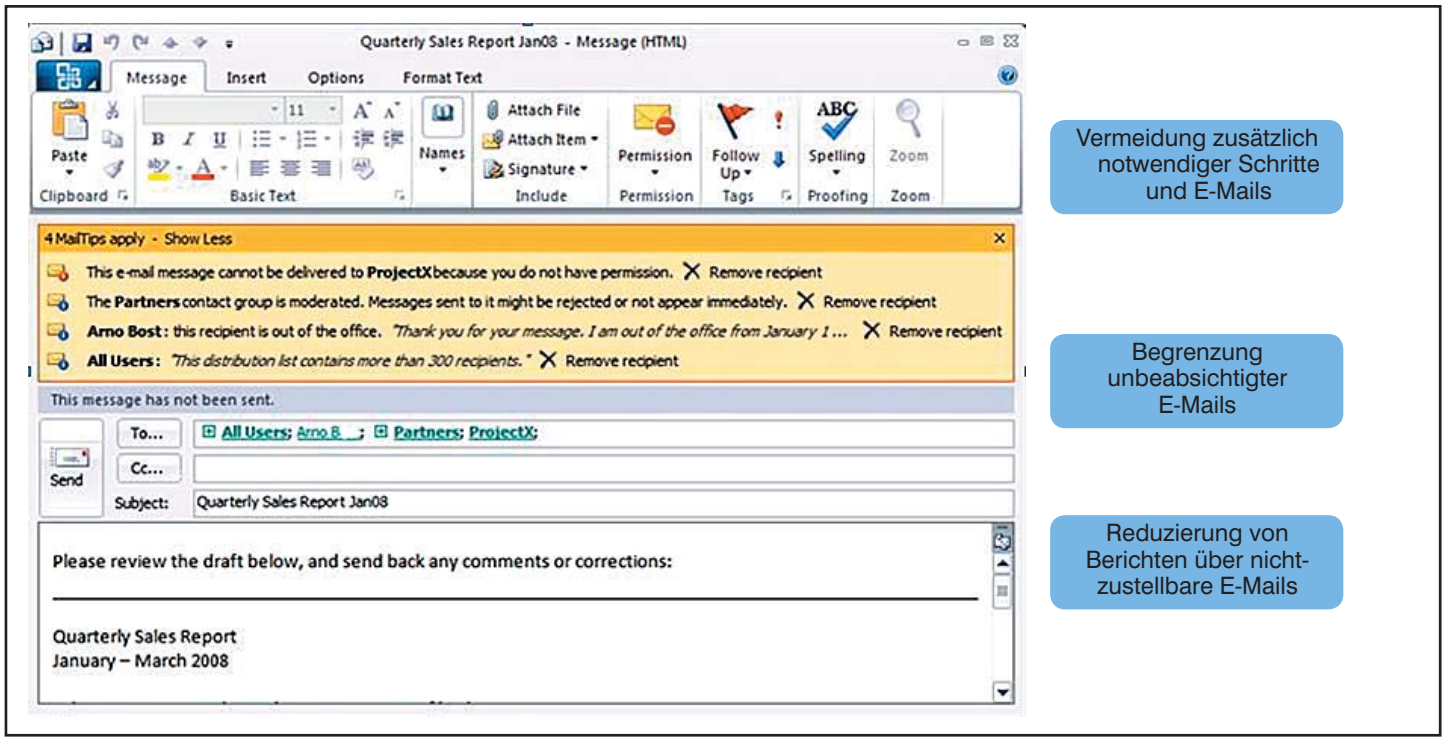


Abbildung 4: Outlook Mail-Tips

Quelle: Microsoft

ons-Paket von Microsoft ergänzen soll bzw. sogar als zentrale UC-Komponenten dient.

Es gibt aber auch funktionale Neuerungen die dem Nutzer und Administrator einer Microsoft-basierten Unified-Communications-Lösung das Tagesgeschäft erleichtern. Als Gegenstück zum bereits vorhandenen Text-to-Speech-Feature steht nun nach Installation der Unified Messaging Rolle auch der umgekehrte Weg zur Verfügung. Die Umsetzung einer Sprachnachricht (Voicemail) in ein Textdokument macht – ebenso wie die umgekehrte Richtung – nur in bestimmten Situationen Sinn. Grundsätzlich ist die Nachricht in Textform allerdings deutlich schneller zu erfassen und zu verarbeiten (auch durchsuchen und weiterleiten) als ein Audiofile, welchen man sich gegebenenfalls mehrfach anhören muss. Während Exchange 2007 nur die einfache Umleitung auf die Voicemail-Box zuließ, können bei Exchange 2010 nun auch Regeln zur Klassifizierung von Anrufern in Abhängigkeit von z.B. Uhrzeit oder Anrufer definiert werden.

Mit Exchange 2010 beendet Microsoft den kurzzeitigen Ausflug in die Welt der Fax-Verarbeitung von Exchange 2007. Die neue Version wird ein Fax noch erkennen und mittels SIP an einen anderen Server, z.B. den Fax-Server eines Drittherstellers weiterleiten, aber nicht mehr selbst verarbeiten oder in eine E-Mail umwandeln. Eine neue Funktion bietet Exchange 2010 mit der Integration des Short Message Services (SMS). In Zusammenarbeit mit ActiveSync und Windows Mobile 6.5 kann das Mobiltelefon selbst als SMS-Gateway für den SMS-Versand aus Outlook heraus fungieren. ActiveSync übernimmt dabei die Kommunikation zwischen Outlook und dem Mobiletelefon sowie den Abgleich der Ordner für gesendete und empfangene Objekte. Bei diesem Verfahren entstehen die Kosten für den SMS-Versand direkt auf dem Mobilfunkvertrag des verwendeten Mobiltelefons, dessen Rufnummer auch als Absender der Nachricht angezeigt wird.

Hinter dem Schlagwort „Federation“ verbirgt sich die Kollaboration zwischen unterschiedlichen Organisationen und Partner. Microsoft hat Exchange 2010 um einige Funktionen im Bereich Föderationen ergänzt. Mit Exchange 2010 können unter anderem Kontakte und Kalender von mehreren Organisationen gemeinsam genutzt und organisationsübergreifend frei gegeben werden. Ein Grund für die Erweiterung der Funktionalität der Föderation ist schnell gefunden, denn wenn man neben einer gehosteten Exchange-Lösung noch eine lokale betreiben möchte, so handelt es sich bei den beiden Instanzen um zwei unterschiedliche Exchange-Organisationen. Damit diese beiden aber möglichst übergreifend zusammenarbeiten können, musste die Federation-Funktionalität entsprechend erweitert werden.

Mit Microsoft Exchange 2010 besteht zudem die Möglichkeit, Kalender für Benutzer außerhalb des Unternehmens freizugeben. Selbstverständlich können diesen Nutzern dann auch entsprechende Berechtigungen zugewiesen werden. Dadurch kann sicheres Messaging auch mit externen Benutzern durchgeführt werden, so dass eine sichere Kommunikation mit Zulieferern, Geschäftspartnern oder Kunden möglich wird, für die bislang Lösungen von Drittanbietern oder eine separate Kontoverwaltung notwendig waren.

Exchange-Migrationspfade

Während man bei älteren Versionen (z.B. Exchange 2000 nach Exchange 2003) noch die Möglichkeit hatte, die Migration zu einer direkten Folgeversion, ähnlich einem Update auf demselben Server durchzuführen, ist dies seit Exchange 2007 nicht mehr möglich. Exchange 2010 setzt wie bereits die 2007er Version die Installation eines neuen Servers unter Verwendung eines 64-Bit-Betriebssystems mit anschließender Migration der Postfächer voraus. Im Gegensatz zu 2007 arbeitet 2010 jedoch ausschließlich unter Windows Server 2008 bzw. 2008 R2. Ein einfaches Update von einer früheren Version ist aufgrund der Änderungen, die Exchange 2010 an der zugrundeliegenden Datenbank vornimmt, nicht möglich.

Grundsätzlich gilt, dass Exchange 2010 nur die Möglichkeiten der Koexistenz mit vorhergehenden Versionen bis Exchange 2003 unterstützt. Eine direkte Migration ist demnach bei Neu-Installation mit Datenmigration auch von Exchange 2003 auf Exchange 2010 möglich. An dieser Stelle muss jedoch darauf hingewiesen werden, dass bei einer Migration von Exchange 2003 auf 2010 keine Möglichkeit mehr besteht, Exchange 2007 zu installieren. Das ist auf die bei der Installation durchgeführten Schema-Änderungen zurückzuführen, die eine spätere Installation eines Exchange 2007 und damit z.B. die Konsolidierung mit der Exchange 2007-Umgebung einer anderen Niederlassung unmöglich machen. Im Hinblick auf zukünftige Kopplungsmöglichkeiten ist daher unter Umständen ein Migrationspfad über Exchange 2007 zu empfehlen.

Für wen lohnt sich der Umstieg?

Wie bereits angesprochen ist Exchange 2010 - wie auch die für Produktiv-Umgebungen freigegebene Version des Vorgängers - lediglich als 64-Bit-Version erhältlich. Hinzu kommt, dass zur Installation ein Server mit mindestens Windows Server 2008 und Service Pack 2 benötigt wird, was bei einigen Interessenten die Umstellung der bisherigen Server-Plattform voraussetzen wird. Unabhängig von der bisher eingesetzten Exchange Version gibt es keinen direkten Upgradepfad, so dass auf jeden Fall eine Neu-Installation mit anschließender Migration der Daten durchgeführt werden muss.

Diese technischen Aspekte, sowie die mit Exchange 2010 eingeführten Neuerungen, wie beispielsweise Hochverfügbarkeit mittels Database Availability Group und der dafür benötigten unterschiedlichen Exchange- und Windows Server 2008 Server-Rollen, werden für viele kleinere Umgebungen sicherlich ein Hindernis darstellen. Hinzu kommt die Optimierung von Exchange 2010 als Software-as-a-Service in seiner gehosteten Version.

Dementsprechend zeigen Anforderungen und die Fokussierung auf Leistungsmerkmale wie Hochverfügbarkeit und effektiveres Management großer Datenmengen, dass Microsoft den Schwerpunkt für die vor Ort Installation bewusst auf große Unternehmen und Hoster gelegt hat. Es ist daher davon auszugehen, dass im ersten Schritt lediglich Unternehmen und Hoster, die große Installationen verwalten müssen, eine Umstellung auf Exchange 2010 in Erwägung ziehen werden.

Dennoch bedeutet die Veröffentlichung von Exchange 2010 sicherlich nicht das gleichzeitige Ende der Vorgängerversionen. Diese haben in Abhängigkeit von den Anforderungen der jeweiligen Umgebung auch weiterhin ihre Daseinsberechtigung. Im Mittelstand und bei KMUs, die derzeit größtenteils noch Exchange 2003 einsetzen, spricht sicher nichts gegen die weitere Verwendung ihrer Groupware-Umgebung. Dies bedeutet aber nicht, dass alle Mittelständler und KMUs den Umstieg völlig ausschließen sollten. Auch bei ihnen ergeben sich z.B. durch Expansion oder fehlende Funktionalität Aspekte, die eine Erweiterung oder ein Upgrade der bisherigen Exchange-Umgebung begründen können. Man sollte sich auch darüber im Klaren sein, dass man bei Verwendung einer älteren Version zwangsläufig früher oder später aus dem Fokus des Herstellersupports und der Entwickler von Drittlösungen läuft. Ebenfalls gilt es zu bedenken, dass bei einem zu großen Versionsunterschied die Koexistenz mit der gehosteten Version nicht unterstützt wird.

Microsoft Exchange 2010: Hochverfügbarkeit On-Premise oder als Hosted-Service

Für Betreiber anderer Groupware-Lösungen bietet Microsoft mit Exchange 2010 zwar einige Anreize über einen Wechsel nachzudenken. Diese können allerdings nur dann wirklich in Betracht gezogen werden, wenn die zugrundeliegende Umgebung ebenfalls Microsoft-basiert ist und die Einführung des Microsoft Office Communications Servers 2007 die Unified-Communications-Lösung als Ganzes abrunden würde. Die zunehmende Verbreitung von Microsofts Office Communications Server und die aus der einfacheren Kopplung mit Exchange resultierende Prozessoptimierung durch Bündelung der Kommunikationswege wird ebenfalls eine Entscheidungshilfe für die Einführung von Exchange 2010 darstellen.

Unabhängig ob lokal installiert oder gehostet bietet Exchange 2010 eine Option für Unternehmen, die ohnehin eine Änderung Ihrer Groupware- oder UC-Lösung planen. Allen anderen gibt eine individuelle Prüfung von Anforderungen, Kosten und Aufwand im Vergleich mit den zu erwartenden Vorteilen Aufschluss über Sinnhaftigkeit und Zeithorizont einer möglichen Migration, um diese rechtzeitig in das jeweilige IT-Budget einplanen zu können.

Exchange 2010 vs. Lotus Notes

In den vergangenen Jahren hat Microsoft Stück für Stück Marktanteile von IBM Lotus Notes übernommen. Vor allem in großen Konzernen ist aber nach wie vor noch häufig Notes vorzufinden. Selbst in ansonsten fast lupenreinen Microsoft-Landschaften kommt das vor. Grund dafür ist vor allem die Sorge vor einer hochkomplexen Migration und Applikationen, die speziell für Notes entwickelt und implementiert wurden. Diese Gründe lassen sich auch mit Exchange 2010 nicht wegdiskutieren. Lange Zeit standen zudem aber noch begrenzter Speicherplatz, vergleichsweise schlechte Verfügbarkeitswerte und eine eingeschränkte Skalierbarkeit einem Umstieg auf Exchange im Weg. Nun hat Microsoft jedoch einen Großteil dieser Probleme beseitigt. Mit Exchange 2010 wird ein Höchstmaß an Zuverlässigkeit und Leistung erzielt. Mithilfe neuer Funktionen wird die Verwaltung vereinfacht und die Kommunikation geschützt. Microsoft entspricht darüber hinaus dem zunehmenden Bedarf nach mehr Mobilität bei geschäftlichen Aktivitäten.

Mit Microsoft Exchange 2010 können Nutzer von nahezu allen Plattformen, Browsern und Geräten auf sichere Weise und mithilfe von Standardprotokollen auf ihre gesamte Kommunikation zuzugreifen. Dazu gehört auch die OWA-Unterstützung für noch mehr Browser (z. B. Apple Safari und Mozilla Firefox). Bei der umfangreichen Unterstützung für Windows Mobile Endgeräte wird es selbstverständlich bleiben. Lediglich bei anderen mobilen Endgeräten beispielsweise mit dem Symbian-Betriebssystem oder dem inzwischen weit verbreiteten iPhone wird es nach wie vor Einschränkungen geben. Im Gegensatz dazu bietet Lotus Notes als mobilen Nutzern lediglich „Traveler“ als Anwendung für Domino mit grundlegenden Funktionen und eingeschränkten Sicherheits- und Verwaltungsmöglichkeiten.

Dass die zahlreichen Zugriffsmöglichkeiten zugleich auch immer sicherheitskritischer werden, erklärt sich von selbst. Hinzu kommen regulatorische Aspekte sowie sich ständig verschärfende Vorschriften und Gesetze, nicht zu vergessen natürlich auch Unternehmens-interne Aspekte, denen Exchange 2010 mithilfe von speziellen Funktionen zur E-Mail-Archivierung und Compliance entgegen kommt, die bislang bei Notes nur rudimentär zu finden sind.

Der wichtigste Punkt ist aber die Bereitstellung von mehrinstanzenfähigen, hoch skalierbaren Architekturen und Speichervarianten (DAS, SATA, JBOD), die vor allem im Hinblick auf die Total Costs of Ownership (TCO) Vorteile für die Unternehmen bringen. Eine solche Skalierbarkeit bei gleichzeitiger Bereitstellung unterschiedlichster Plattformen und Speichervarianten ist bei Notes, wenn überhaupt, nur mithilfe von Outsourcing-Lösungen möglich. Hinzu kommt dann natürlich immer die tiefe Integration in die übrige Microsoft-Welt, was beispielsweise bei der Nutzung des Active Directory erst für die Version 8.5 von Notes vorgesehen ist.

Für die Nutzer ist Exchange 2010 sicherlich ebenfalls eine Bereicherung, weil es Unified Messaging, E-Mail, Voicemail, IM, SMS und Mobilitätsverwaltung in einer einzigen Applikation mit dem typischen Microsoft Look & Feel bereitstellt. Dazu sind bei IBM mehrere Produkte und Lösungen erforderlich. Die Möglichkeit, Kalender für Benutzer außerhalb des Unternehmens freizugeben, spezielle Berechtigungen zuzuweisen etc. entspricht darüber hinaus dem Anspruch, Kommunikation auch über die Unternehmensgrenzen hinaus von Medienbrüchen frei und durchgängig zu machen. Insofern ist Microsoft mit Exchange 2010 sicherlich einen großen Schritt auf die derzeitigen Nutzer von Lotus Notes zugegangen und wird an vielen Stellen den ohnehin schon vorhandenen funktionalen Vorsprung ausbauen. Für überzeugte Nutzer von Unified Communications und Collaboration ist daher ein Umstieg von Notes auf Exchange kaum noch zu umgehen.

Neuer Report

Reportneuerscheinung:
100G und 100G Ethernet
Anwendungen, Technik, Standards, Produkte

Mitte Juni erscheint der neue Report „100G und 100G Ethernet: Anwendungen, Technik, Standards, Produkte“ von Dr. Franz-Joachim Kauffels bei ComConsult Research.

Der Report von Dr. Franz-Joachim Kauffels verdeutlicht, wieso es Sinn machen kann, direkt auf 100 G zu gehen, wenn sich im 10 G-Bereich Engpässe ergeben könnten. Von der Anwendung her spielen hier vor allem die hohen möglichen I/O-Datenraten Virtualsierter Server und die Problematik der Energieeffizienz eine wesentliche Rolle. Wichtig ist vor allem, darauf zu achten, dass neu anzuschaffende Core-Switches „100 G-ready“ sind. Letztlich führen die neuen Anforderungen und Möglichkeiten zu einer Weiterentwicklung des möglichen Netzdesigns.

Die Leistungsexplosion Virtueller Server bei der I/O durch Virtual I/O und SR-IOV sowie die allgemeine Speicherproblematik und der Wunsch nach höherer Grundqualität nicht nur hinsichtlich der Leistung, sondern auch des Delays eines RZ-Netzes werfen verschiedene neue Fragen auf:

- Wie kann man z.B. Blade-Systeme, in denen jedes einzelne Server-Blade schon 10 Gb I/O kann, sinnvoll an Netze anschließen?
- Welche Qualität müssen Netze haben, wenn sie zum Systembus Virtualisierter Systemumgebungen werden?
- Wie kann man unter diesem Qualitätsanspruch Konvergenz von Ethernet- und FC-Speicherverkehr realisieren?
- Wir können die Inter Switch Links für die neu aufkommenden „Virtual Chassis“, bei denen mehrere Hochleistungs-Switches zu einem einzigen logischen Switch zusammengeführt werden, sinnvoll realisiert werden?
- Wie steht es um die Energieeffizienz und generelle Wirtschaftlichkeit neuer Lösungen?
- Welche Implikationen ergeben sich aus den neuen Anforderungen und Möglichkeiten hinsichtlich des Gesamt-Designs eines RZ-Netzes?

In diesem Report werden allgemeine Motivationen zur Einführung von 100 G, der aktuellen Entwicklungsstand bei der Transceivertechnologie und deren Weiterentwicklung, Einzelheiten des Standards IEEE 802.3ba sowie der speziellen 100 G-Varianten sowie Produktlage und Planungsempfehlungen gegeben. Auch wenn Sie heute das Problem nicht sofort haben, liefert der Report wesentliche Aussagen, die einem Verantwortlichen dabei helfen, zukunftsfeste Entscheidungen bei der Entwicklung Ihres RZ-Netzes zu treffen. Verschiedene Hersteller liefern schon heute Switches, die man als „100 G-ready“ bezeichnen kann. Insgesamt geht es neben den Leistungsaspekten auch darum, Kosten zu senken. 100 G spart gegenüber multiplem 10 GbE oder 40 GbE Adapter, Strom, je nach Version ToR-Switches, Kabel und vor allem Wartungspunkte. Darüber hinaus ist einzig 100 G in der Lage, die Anforderungen an ein Netz auch dann zu erfüllen, wenn man es zum Systembus einer Virtuellen Umgebung macht. In der Providertechnik ist es für ein 10, 40 oder 100 G-Signal gleichgültig, ob die Information, die übertragen wird, vorher ein Ethernet-Paket, ein FC-Frame, ein OC-Container oder ein FICON-Strom war. Von daher lässt 100 G auch elegantere Lösungen für die Konvergenz erwarten, als dies z.B. FCoE darstellt.

Fax-Antwort an ComConsult 02408/955-399

Bestellung
100G und 100G Ethernet

Ich bestelle den Report
☐ **100G und 100G Ethernet**
zum Subskriptionspreis von nur
€ 318,--* zzgl. MwSt. und Versand

*gültig bis zum 30.05.10 - dann regulärer Preis € 398,-- zzgl. MwSt. und Versand

Der Report ist ab Juni 2010 verfügbar.

Bestellen Sie über unsere Web-Seite
www.comconsult-research.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Schwerpunktthema

Kommt der Durchbruch für die Netzzugangskontrolle mit IEEE 802.1X-2010?

Fortsetzung von Seite 1

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

- Der Supplicant ist eine Software-Komponente, die den Netzwerkzugang anfordert.
- Der Authenticator bietet eine Schnittstelle, über die der Supplicant authentisiert werden kann und stellt den gewünschten Netzwerkzugang her. Im LAN liegt diese Funktion typischerweise in demjenigen Switch an den das Endgerät unmittelbar angeschlossen ist. Im WLAN wird diese Funktion vom Access Point bzw. WLAN Controller wahrgenommen.
- Der eigentliche Authentisierungsdienst wird zentral über den Authentication Server bereitstellt. Der Authentication Server ist typischerweise ein RADIUS-Server (siehe RFC 2865).

Der Austausch der Authentisierungsinformationen läuft über das Extensible Authentication Protocol (EAP, siehe RFC 3748) ab. Dabei erfolgt die Kommunikation über die LAN- bzw. WLAN-Schnittstelle zwischen Supplicant und Authenticator über das Layer-2-Protokoll EAP over LAN (EAPOL). Auf diese Weise wird eine Authentisierung am Netzzugangspunkt ermöglicht, bevor eine Kommunikation auf IP-Ebene und höheren Protokollebenen stattfindet. Die Kommunikation zwischen Authenticator und Authentication-Server geschieht meist über RADIUS, wobei die EAP-Nachrichten als RADIUS-Attribute übertragen werden. Für die Verwaltung der Daten der Geräte oder Nutzer, die sich mit IEEE 802.1X authentisieren, wird oft ein Verzeichnisdienst (Directory Service) wie z.B. LDAP verwendet, der vom RADIUS-Server angesprochen wird. Abbildung 2 zeigt die genutzten Protokolle im Überblick. Wichtig ist dabei, dass es keine direkte Kommunikation des Supplicant mit dem Authentication Server gibt. Der Authenticator ist der einzige für den Supplicant sichtbare Kommunikationspartner, der sich also quasi wie ein Authentisierungs-Proxy verhält.

IEEE 802.1X wurde 2001 erstmalig verabschiedet. Die aktuell in der Praxis relevante Version ist die Überarbeitung von 2004. (siehe Abbildung 2)

Authentisierungsmethoden

EAP ist ein generisches Protokoll, über das die eigentlichen Authentisierungsverfahren, die sogenannten EAP-Methoden, kommunizieren. Es gibt eine ganze Reihe von EAP-Methoden.

Beispielsweise verwendet EAP-TLS Zertifikate zur gegenseitigen Authentisierung von Supplicant und Authentication Server. Bei der EAP-Methode Protected EAP (PEAP) werden Zertifikate nur zur Authentisierung des Servers genutzt. Anschließend wird ein TLS-Tunnel zwischen Server und Supplicant aufgebaut, in dem dann geschützt die Authentisierung des Supplicant durch eine andere EAP-Methode erfolgt. In Microsoft Windows-Umgebungen wird PEAP mit EAP-MSCHAPv2 zur Authentisierung des Supplicant verwendet. Über EAP-MSCHAPv2 werden die für eine Domänenanmeldung üblichen Credentials genutzt, sodass diese Methode sehr gut zur Benutzerverwaltung in Windows-Lösungen passt.

Autorisierung

IEEE 802.1X gestattet in der Fassung von 2004 nach einer erfolgreichen Authentisierung eine Autorisierung, die über eine simple Türöffnerfunktion hinausgeht. Der Authentication Server kann bei der Erteilung der Zugangserlaubnis zusätzlich eine Information für die Zuweisung eines VLANs oder einer Access Control List (ACL) für den Port, an dem der Supplicant angeschlossen ist, übertragen. Auf diese Weise kann dynamisch und individuell bzw. in Abhängigkeit von der Gruppenzugehörigkeit des Supplicant (der dabei ein Gerät oder einen Nutzer repräsentieren kann) eine Autorisierung der Kommunikation vorgenommen werden.

Compliance Checks: Weitere Anwendungen von EAP und IEEE 802.1X

Neben Authentisierungsinformationen können mit EAP grundsätzlich auch andere Daten übertragen werden. Hierzu kann etwa ein Agent auf dem Endgerätesystem Parameter der Endgerätekonfiguration auswerten (z.B. Version des Viren-Pattern-File) und eine entsprechende Prüfsumme über EAP an die Infrastruktur schicken. Diese wird dann ausgewertet und das Endgerät hinsichtlich der Konformität zu den Vorgaben (also hinsichtlich des Gesundheitszustands) bewertet. Je nach Ergebnis kann dann über die eben erwähnten Autorisierungsmechanismen der gewünschte Netz-

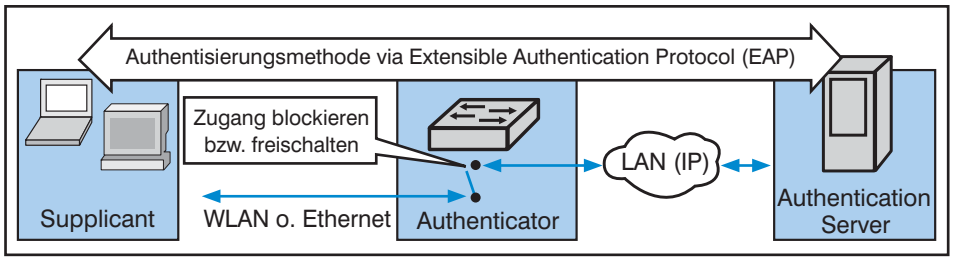


Abbildung 1: Rollen in IEEE 802.1X

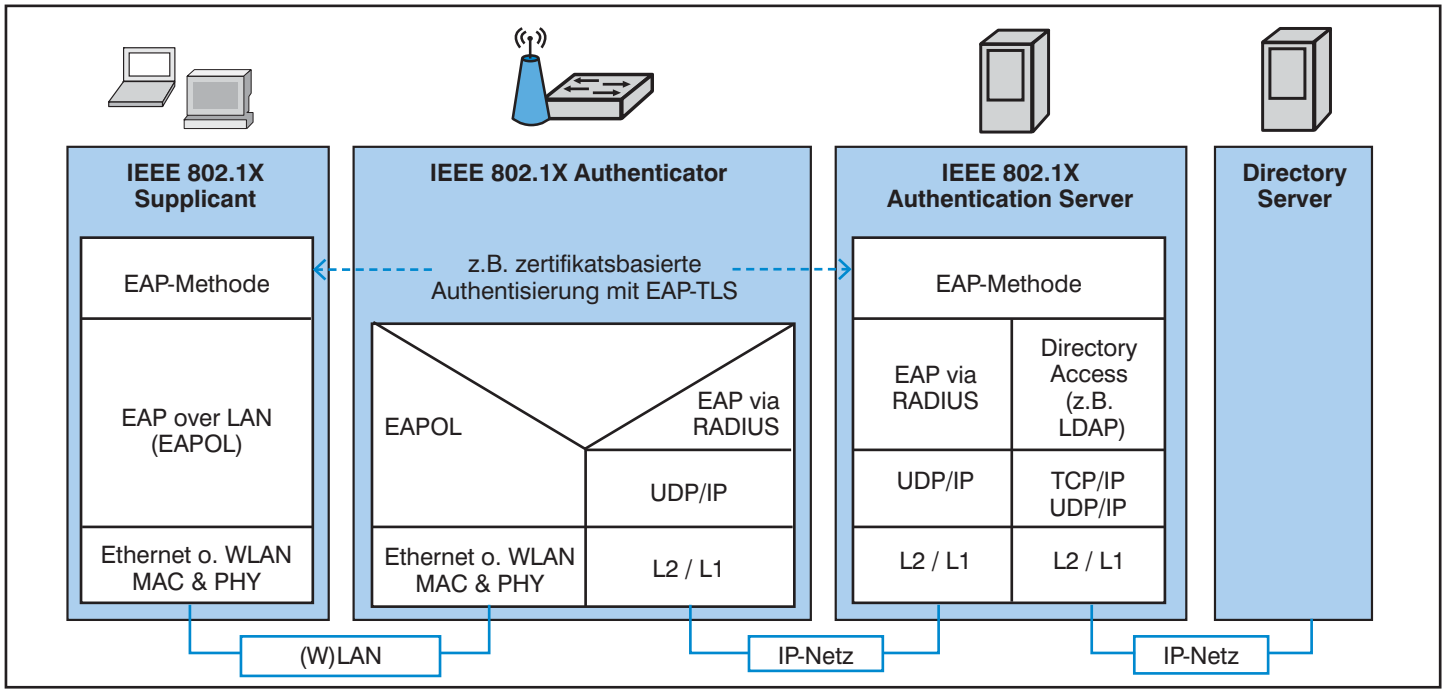


Abbildung 2: Protokolle in IEEE 802.1X

zugang gewährt oder das Gerät in eine Quarantäneumgebung gesetzt werden.

Neben Trusted Network Connect (TNC) der Trusted Computing Group (TCG) sind insbesondere die proprietären Lösungen Network Access Protection (NAP) von Microsoft und Cisco Network Admission Control (CNAC) zu erwähnen.

Für TNC und den unter der Bezeichnung Network Endpoint Assessment (NEA) laufenden Aktivitäten der IETF hat es im Februar 2010 eine entscheidende Vereinbarung gegeben, auf deren Basis eine Harmonisierung der Arbeiten stattfindet und die Industriestandards der TCG für TNC sukzessive als RFCs der IETF aufgelegt werden. Produkte werden dabei wie bisher von der TCG zertifiziert.

2. Problembereiche und Grenzen von IEEE 802.1X-2004 im kabelbasierten LAN

Der Standard IEEE 802.1X-2004 wird inzwischen von sehr vielen Produkten unterstützt und für WLAN hat sich IEEE 802.1X auch in der Praxis massiv durchgesetzt. Es gibt kaum noch WLAN-Installationen auf Enterprise-Niveau, die für die Authentisierung auf IEEE 802.1X verzichten. Das Sorgenkind ist, obwohl die Anzahl der Implementierungsprojekte für IEEE 802.1X signifikant steigend ist, das kabelbasierte LAN. Die Ursachen liegen in den im Folgenden beschriebenen Problembereichen.

Die Anwendung von IEEE 802.1X hat zunächst das generelle Problem, dass zwar grobe allgemeingültige Design-Konzepte genutzt werden können, im Detail aber die Unterschiede zwischen Installationen erheblich sind. Weiterhin sind für die Anpassungen der Betriebsprozesse stets aufwendige individuelle Betrachtungen erforderlich. Die Gründe liegen dabei zunächst in der Komplexität des technischen Apparats für IEEE 802.1X und in der Größe der Wirkkette, die bei IEEE 802.1X vom Endgerät über das Netzwerk bis hin zu zentralen Komponenten reicht.

Das wesentliche Problem bei der Einführung von IEEE 802.1X ist daher zunächst organisatorischer Natur. Erschwerend ist zudem, dass die aktuell in der Praxis relevante Version des Standards von 2004 Schwachstellen hat, die in der Umsetzung für das kabelbasierte LAN notgedrungen zu Kompromissen führen. Wesentliche Punkte sind dabei:

- Kommunikation mit nicht authentisierten Systemen
- Simultane Authentisierung mehrerer Endgeräte an einem Port
- Anfälligkeit gegenüber MAC-Adress-Spoofing

Kommunikation mit nicht authentisierten Systemen: Default Policy und adaptive Authentisierung

Die Forderung, dass über einen Port im nicht autorisierten Zustand ausschließlich EAPOL erlaubt ist und erst nach erfolgreicher Authentisierung Nutzverkehr über den Port geleitet werden darf, ist in der Praxis in den allermeisten Fällen zu scharf. Es kann notwendig sein, auch für nicht gemäß IEEE 802.1X authentisierte Systeme rudimentäre Kommunikationsmöglichkeiten anzubieten.

Wenn das Preboot Execution Environment (PXE) genutzt werden soll, um z.B. das Betriebssystem über das Netz zu laden, und auf Ebene der Firmware kein Supplicant zur Authentisierung zur Verfügung steht, muss zunächst die PXE-Boot-Sequenz über den Port im nicht autorisierten Zustand ablaufen können. Erst wenn das Betriebssystem im Anschluss startet, steht ein Supplicant für IEEE 802.1X zur Verfügung. Diese PXE-Boot-Sequenz erfordert neben DHCP auch die Kommunikation mit dem PXE-Boot-Server (TFTP), die der Port im nicht autorisierten Zustand gestatten muss.

Hinweis: Von der Firma Intel wird seit Intel AMT Firmware Version 2.5 ein Supplicant auf Ebene der Firmware unterstützt. Dabei kann unter anderem auch PEAP verwendet werden. Die Konfiguration von IEEE 802.1X erfolgt über Intel SCS (Setup and Configuration Service).

Ein weiteres Beispiel ist der Anschluss eines erlaubten Endgeräts, das sich (z.B. bedingt durch eine Fehlkonfiguration oder ein abgelaufenes Zertifikat) nicht oder nicht erfolgreich authentisieren kann. In

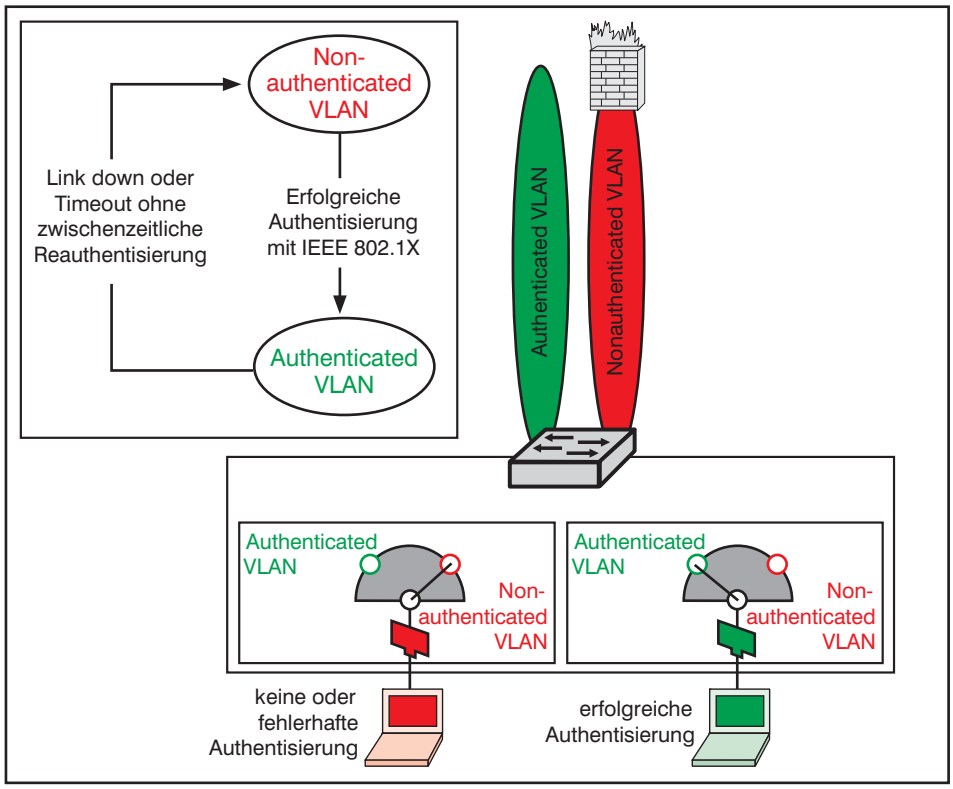


Abbildung 3: Default Policy

diesem Fall wäre es zweckmäßig, wenn der User Helpdesk (UHD) auf das Gerät zugreifen könnte. Der Port würde dies aber nicht zulassen, da das Gerät sich nicht authentisieren kann. Ein Teufelskreis.

Für solche und ähnliche Situationen gestattet der Standard IEEE 802.1X eine sogenannte Default Policy, die den Zustand eines Ports im nicht autorisierten Zustand bestimmt. In der Default Policy wird dem Port ein spezielles VLAN zugeordnet (in Abbildung 3 als Non-authenticated VLAN bezeichnet). In diesem VLAN sollten dem angeschlossenen Gerät natürlich nur eingeschränkte Kommunikationsmöglichkeiten gewährt werden (was durch ACLs oder Firewall-Techniken erzwungen werden kann). Die Entscheidung, welche Kommunikationsziele im Non-authenticated VLAN erreichbar sind, muss im Einzelfall getroffen werden. Beispielsweise können über die Default Policy gewisse Server, wie DHCP Server und PXE Boot Server, erreichbar sein.

Wenn ein Gerät sich an dem Port erfolgreich authentisiert, wird der Port in den autorisierten Zustand gehoben und dem Port ein entsprechendes VLAN (in Abbildung 3 als Authenticated VLAN bezeichnet) zugeordnet. In diesem Zustand wird typischerweise eine uneingeschränkte Kommunikation erlaubt.

Wenn der Link nicht mehr besteht oder bei Ablauf des Reauthentisierungs-Zeitintervalls ohne erfolgreiche Neuauthentisierung, fällt der Port wieder auf die Default Policy zurück.

In der Praxis ist die Default Policy für den Einsatz von IEEE 802.1X ein unverzichtbares Gestaltungsmittel.

Eine Default Policy wird in dieser oder einer ähnlichen Form von den meisten Herstellern unterstützt. In diesem Zusammenhang muss aber betont werden, dass der Standard IEEE 802.1X in der Fassung von 2004 eine solche Default Policy zwar in einem informellen Anhang gestattet (siehe Anhang C.2.1 „Manageability of end stations“ von IEEE 802.1X-2004), die Funktion aber nicht normativ standardisiert. Es handelt es sich hier also um eine Funktion, die von Herstellern unterschiedlich gestaltet wird und daher im Einzelfall geprüft werden muss.

Die Default Policy kann in den Switches typischerweise um eine MAC-Adress-Authentisierung ergänzt werden. Das Ergebnis ist eine mehrstufige adaptive Authentisierung, wie exemplarisch in Abbildung 4 gezeigt.

Eine solche adaptive Authentisierung ist immer dann sinnvoll, wenn Geräte berücksichtigt werden müssen, die keinen IEEE 802.1X Supplicant unterstützen und die trotzdem nicht ohne Authentisierung einen Netzzugang rein über die Default Policy erhalten sollen. Ein solcher Mechanismus hat sich in vielen NAC-Projekten als essentiell erwiesen.

Die kombinierte Authentisierung mit IEEE 802.1X und als Fallback mit MAC-Adresse ist nicht im Standard IEEE 802.1X (auch in der aktuellsten Fassung) beschrieben und als herstellerspezifisch einzustufen. Daher können sich die Implementierungen der Hersteller entsprechend deutlich unterscheiden und es ist zur Bewertung stets eine Einzelbetrachtung erforderlich.

Simultane Authentisierung mehrerer Endgeräte an einem Port

Größtes Problem in IEEE 802.1X-2004 ist die Limitierung der Spezifikationen im Standard für das kabelbasierte LAN auf eine strikte 1-zu-1-Beziehung zwischen Supplicant und Authenticator, d.h. ein Gerät pro Port.

Dummerweise fällt unter diese Einschränkung neben dem Anschluss eines Hubs oder eines Desktop-Switches an einen

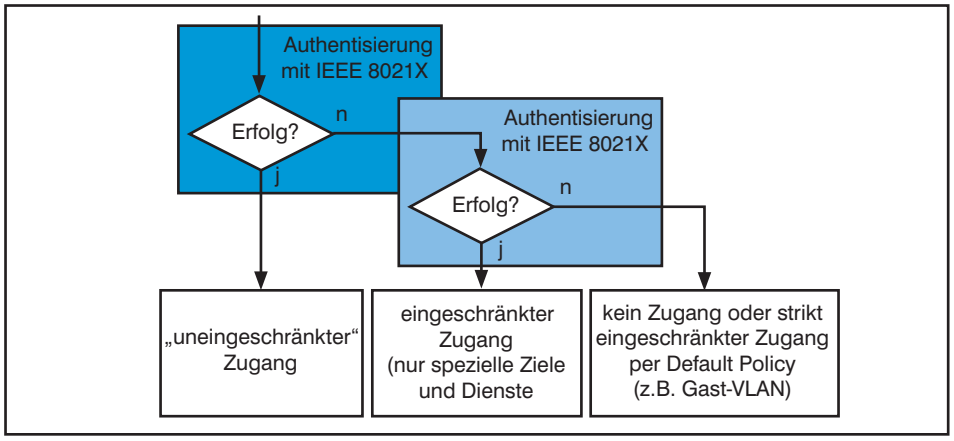


Abbildung 4: Typisches Beispiel einer adaptiven Authentisierung

Port, der IEEE 802.1X aktiviert hat, auch der kaskadierte Anschluss von IP-Telefon und PC am PC-Port des IP-Telefons sowie die Nutzung von VMs im Bridged-Modus auf einem PC.

Die Netzwerkausrüster haben daher in ihren Implementierungen den Standard durch proprietäre Funktionen ergänzt, die zwar im Grundsatz recht ähnlich sind, im Detail aber erheblich voneinander abweichen können. Das Prinzip ist dabei recht einfach: Für jede an einem Switch-Port neu gelernte MAC-Adresse instanziiert der Switch eine neue NAC-Sitzung für den Port, die per IEEE 802.1X oder per MAC-Adresse authentisiert wird (siehe Abbildung 5 und Abbildung 6). Nur diejenigen MAC-Adressen, die einer authentisierten Sitzung zugeordnet werden können, erhalten einen Zugang.

Es ist einleuchtend, dass eine dynamische VLAN-Zuweisung für einen Port, an dem mehrere Endgeräte angeschlossen sind, fragwürdig ist, denn welches der Endgeräte soll die VLAN-Zugehörigkeit entscheiden, das zuerst oder das zuletzt angeschlossene? Es wird sich immer ein Szenario finden lassen, das hierbei keinen Sinn ergibt. Eine etwas andere Situation ergibt sich beim Anschluss eines PCs über ein IP-Telefon. Das Voice-VLAN (mit IEEE 802.1Q Tag) wird entweder über LLDP-MED oder CDP übermittelt oder ist statisch konfiguriert. Das native Daten-VLAN kann dann dynamisch per RADIUS

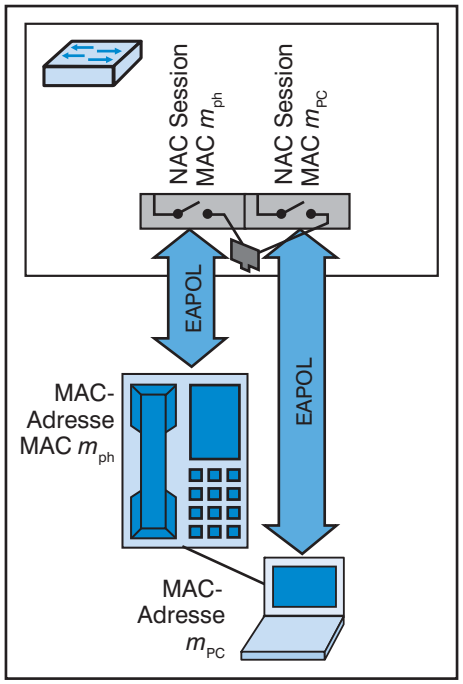


Abbildung 5: Simultane Authentisierung mehrerer Endgeräte an einem Netzwerk-Port am Beispiel von IP-Telefon und PC

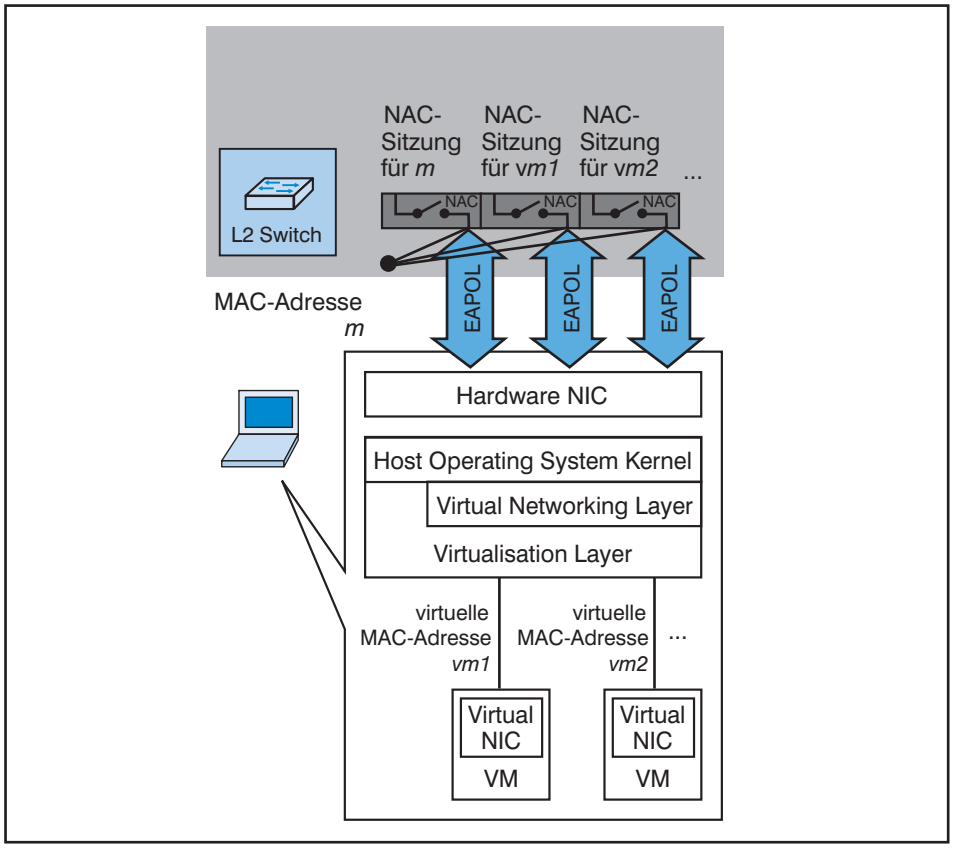


Abbildung 6: Beispiel Simultane Authentisierung mehrerer Endgeräte an einem Netzwerk-Port bei Verwendung von VMs mit virtuellen MAC-Adressen

zugewiesen werden.

Anfälligkeit gegenüber MAC-Adress-Spoofing

Über IEEE 802.1X ist zwar die Authentisierung eines Systems bzw. eines Nutzers am System möglich. Es erfolgt aber keine Authentisierung der über einen autorisierten Port übertragenen Pakete eines Endgeräts. Insbesondere findet keine Prüfung statt, ob die Pakete auch tatsächlich von dem Gerät stammen, auf dem der Supplicant, der sich authentisiert hat, läuft.

Ein Angreifer könnte unter der MAC-Adresse eines authentisierten Supplicant einen Dialog mit der Infrastruktur führen, solange der Port autorisiert ist (siehe Abbildung 7). Er benötigt hierzu allerdings einen Helfer, der sich erfolgreich authentisieren kann. Sobald dies geschehen ist, ist an dem entsprechenden Netzwerk-Port die MAC-Adresse des Helfers – zumindest bis zum Ablauf des Reauthentisierungsintervalls - frei geschaltet. Wenn der Angreifer jetzt seinen Adapter mit der MAC-Adresse des Helfers konfiguriert, hat er automatisch dieselben Kommunikationsmöglichkeiten wie der Helfer.

Wenn eine NAC-Lösung basierend auf der Version von 2004 des Standards IEEE 802.1X aufgebaut werden soll, muss diese Gefährdung bewertet werden. Entweder das Risiko wird eingegangen oder IEEE 802.1X-2004 macht an dieser Stelle keinen Sinn. Wenn die beschriebene Gefährdung als nicht akzeptabel eingestuft wird, bleibt in dieser Situation aktuell nur der Einsatz konventioneller VPN-Techniken zur Absicherung der Datenübertragung oder es müssen Funktionen in IEEE 802.1X ergänzt werden, womit wir automatisch bei einer Neuauflage von IEEE 802.1X wären.

3. IEEE 802.1X-2010: Revolutionär oder Papiertiger?

Die Zusicherung von Vertraulichkeit und Integrität der über einen autorisierten Port übertragenen Pakete ist zunächst nicht Aufgabe eines Authentisierungsverfahrens. Hierzu muss generell die Sicherheitsarchitektur um eine Komponente für Verschlüsselung und/oder Integritätsprüfung erweitert werden. Für die verbindungslose Kommunikation in LAN/MAN werden diese Mechanismen in dem im August 2006 verabschiedeten Standard IEEE 802.1AE MAC Security (kurz: MACsec) beschrieben.

Das hierzu notwendige Schlüsselmanagement für den Aufbau von gesicher-

Kommt der Durchbruch für die Netzzugangskontrolle mit IEEE 802.1X-2010?

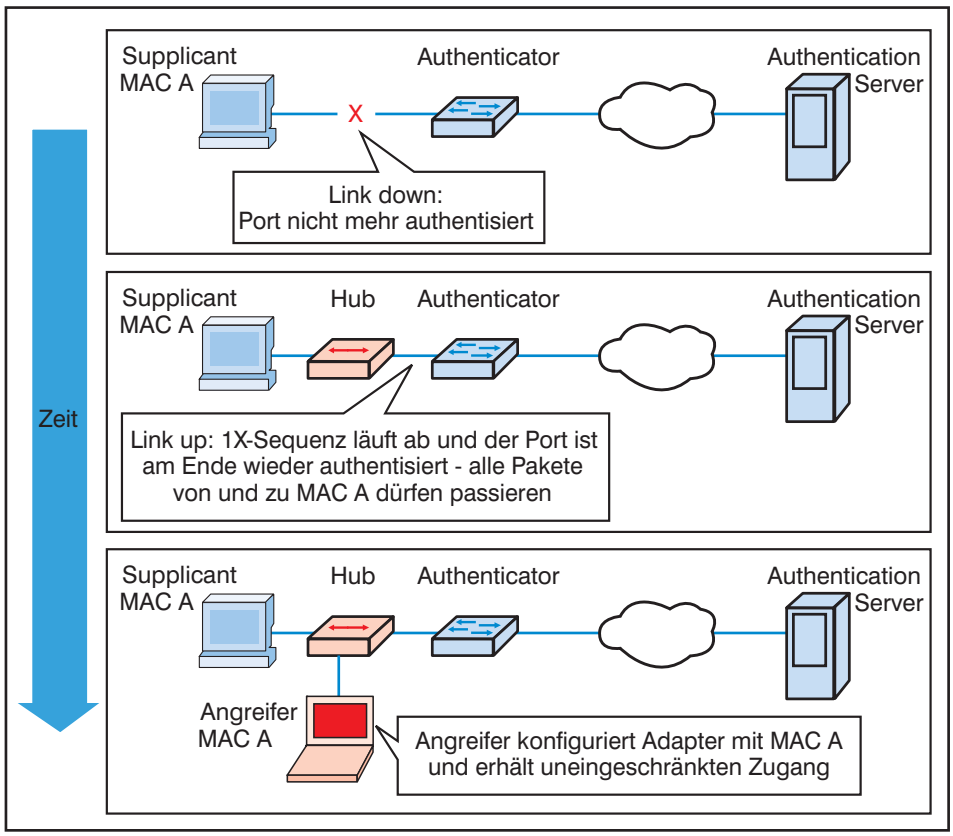


Abbildung 7: Umgehung von IEEE 802.1X-2004

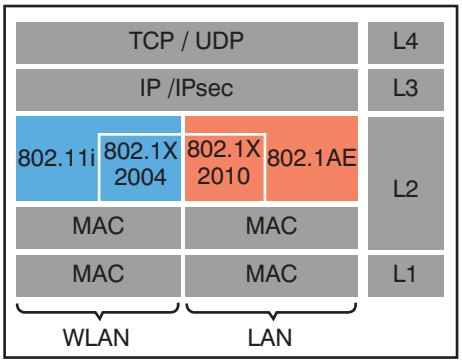


Abbildung 8: Einordnung von IEEE 802.1AE und IEEE 802.1X-2010 in den Protocol Stack

ten Kommunikationsbeziehungen ist das wesentliche Element der Neuauflage von IEEE 802.1X, die Ende Februar 2010 verabschiedet worden ist. IEEE 802.1AE und IEEE 802.1X-2010 bilden dabei zusammen für das kabelbasierte LAN das konzeptionelle Pendant zur Absicherung von WLAN mit IEEE 802.11i, wie in Abbildung 8 gezeigt.

Das Grundprinzip für den Aufbau gesicherter Kommunikationsbeziehungen bei IEEE 802.1X-2010 besteht darin, dass im Rahmen der Authentisierung Schlüsselmaterial in Supplicant und Authenticator bereitgestellt wird, welches dann zum Aufbau einer gesicherten Kommunikationsbeziehung mit IEEE 802.1AE verwendet werden kann (Abbildung 9). Dabei kann (analog zu WLAN gemäß IEEE 802.11i) wahlweise ein Pre-Shared Key (PSK) oder eine dynamische Schlüsselaushandlung mit EAP genutzt werden.

Die Neuauflage IEEE 802.1X-2010 beinhaltet neben der bereits angesprochenen Nutzung von IEEE 802.1AE weitere wichtige Elemente. Dies sind insbesondere die Übernahme der Default Policy in den normativen Teil als erlaubte Option und die Möglichkeit der simultanen Authentisierung mehrerer Endgeräte an einem Port. Weiterhin ist die sichere Geräte-Identifizierung mit IEEE 802.1AR berücksichtigt worden.

Grundkonzepte in IEEE 802.1AE MACsec

MACsec ergänzt das MAC-Layer der Netzelemente eines LAN um eine Hop-by-Hop-Absicherung, die Daten-Vertraulichkeit, -Integrität, -Authentisierung für die verbindungslose Kommunikation in einem LAN schafft (Abbildung 10). Die Default Cipher Suite verwendet den Advanced Encryption Standard (AES) mit 128 Bit Schlüssel. Die Verschlüsselung ist dabei optional. Kernelement ist die Authentisierung der Daten, welche neben den Nutzdaten auch die MAC-Adressen berücksichtigt, was insbesondere die eben beschriebene Spoofing-Attacke automatisch aushebelt.

Neben Punkt-zu-Punkt LAN-Verbindungen werden Multi-Access LAN und Shared-Media LAN (exklusive IEEE 802.11 WLAN, denn hier wirkt IEEE 802.11i) berücksichtigt. Dabei geht es insbesondere um den kaskadierten Anschluss von PC und IP-Telefon an einen Port eines Access Switch und um die Behandlung von VMs mit virtuellen MAC-Adressen auf einem Endgerät.

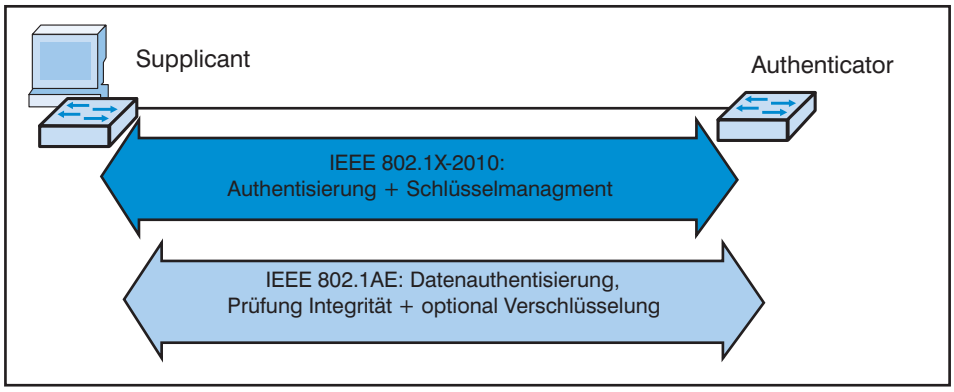


Abbildung 9: Beziehung zwischen IEEE 802.1X-2010 und IEEE 802.1AE

MACsec wurde für eine hohe Verschlüsselungsleistung konzipiert, die mit 40 Gbit/s und mehr weit über die aktuellen Anforderungen im Endgeräte-Anschlussbereich hinaus geht. Hintergrund ist hier der Einsatz von MACsec im Datacenter-Bereich, wo die Möglichkeit einer Verschlüsselung unter hohen Leistungsanforderungen (ohne unwirtschaftlich zu werden) immer mehr gefordert wird.

Durch diese Skalierbarkeit der Leistung setzt sich MACsec von Sicherheitsmechanismen auf höheren Protokollebenen wie IPsec und TLS, die bei den Leistungsanforderungen moderner LANs im Campus- und Datacenter-Bereich immer mehr an Grenzen stoßen, deutlich ab.

Aufbau sicherer Kommunikationsbeziehungen

Zwischen den Stationen eines Vertrauensbereichs in einem LAN kann mit MACsec der Aufbau einer sogenannten Secure Connectivity Association (CA) erfolgen, wie in Abbildung 11 gezeigt. Im einfachsten Fall sind dies zwei Parteien, etwa ein Endgerät und ein Switch oder zwei Switches. Über eine CA etabliert jede beteiligte Station mindestens einen Secure Channel (SC), d.h. einen unidirektionalen Point-to-Multipoint-Kanal. Über einen SC werden aufeinanderfolgende Security Associations (SAs) aufgebaut. Im Folgenden wird aus Gründen der Vereinfachung der Begriff CA allgemein für einen gemäß MACsec abgesicherten Kanal verwendet.

Für den Aufbau sicherer Kommunikationsbeziehungen muss MACsec notgedrungen das Layer-2-Frame-Format erweitern. Dabei kommt ergänzend ein Security TAG und ein Integrity Check Value (ICV) hinzu. Letzterer schützt im Wesentlichen die gesamten Layer-2-Daten, also nicht nur den Payload, sondern auch MAC-Quelladresse und -Zieladresse! Als Konsequenz muss hier zwingend neue Hardware eingesetzt werden. Die Migration zu IEEE 802.1AE hat daher zunächst einen langfristigen Charakter.

Ein Station, die ein Paket empfängt, kann die im Paket übertragene kryptographische Prüfsumme auswerten und so mit einer sehr hohen Wahrscheinlichkeit feststellen, ob das Paket tatsächlich von der angegebenen MAC-Adresse kommt und ob der Inhalt manipuliert worden ist (Abbildung 12).

Den grundsätzlichen Ablauf des Aufbaus einer abgesicherten Kommunikationsbeziehung zeigt zusammengefasst Abbildung 13. Im ersten Schritt erfolgt die Authentisierung mit EAP bzw. IEEE 802.1X, verbunden mit einer Autorisierung, die - wie bisher eine VLAN- oder ACL-Zuweisung beinhalten kann. Auf dieser Basis wird in einem zweiten Schritt das Schlüsselmaterial zwischen den beteiligten Port Access Entities (PAEs), d.h. zwischen Supplicant und Authenticator, verhandelt. Dieses Material wird zur jeweiligen MAC Security Entity übertragen, die hiermit die CA aufbauen kann (Schritte 3 und 3.1 in Abbildung 13). Im letzten Schritt kann dann der Port freigeschaltet werden.

Verschlüsselungsendpunkte bilden bei MACsec die Switches und die Endgeräte. Es gibt also keine Ende-zu-Ende-Absicherung wie etwa bei TLS. Den Switches muss also vertraut werden. Das ist nicht unbedingt nachteilig, denn in der Praxis gibt es beispielsweise auch das Problem, dass eine Ende-zu-Ende-Verschlüsselung aufgebrochen werden muss, damit ein Content Filter oder ein Intrusion Prevention System

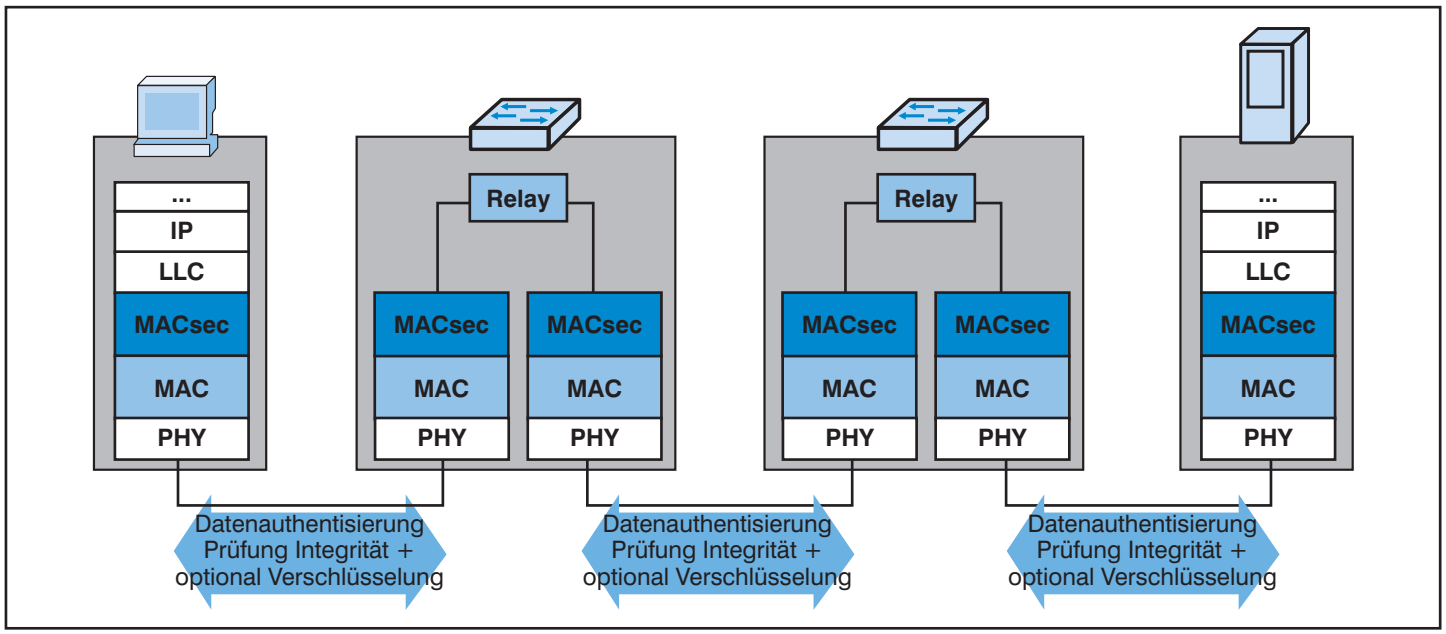


Abbildung 10: Hop-by-Hop-Sicherheit mit MACsec

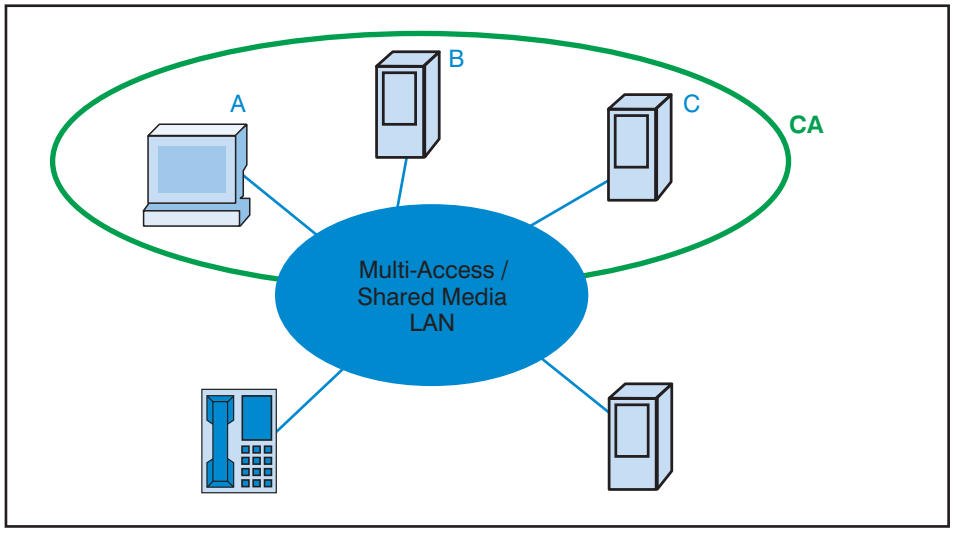


Abbildung 11: Secure Connectivity Association (CA) zwischen den Stationen eines Vertrauensbereichs

(IPS) den Verkehr analysieren kann.

Anbindung nicht authentisierter Geräte (Default Policy)

Die oben beschriebene Default Policy ist in Kapitel 7.1.3 „Connectivity to unauthenticated systems“ in den normativen Teil des Standards übernommen worden. Damit besteht zunächst die Hoffnung, dass sich die unterschiedlichen Interpretierungen dieser Funktion der Hersteller angleichen werden.

Weiterhin ist die Default Policy explizit um die Möglichkeit einer ACL ergänzt worden (im Standard als Selective Relay bezeichnet).

In der Fassung des Standards von 2004 gab es noch eine spezielle Funktion (Unidirectional Controlled Port), um einen Port im nicht autorisierten Zustand nur einseitig vom Supplicant in Richtung des Authenticator zu blockieren. In der anderen Richtung konnten unabhängig vom Autorisierungsstatus des Ports Pakete weitergeleitet werden. Hintergrund dieser Funktion war die Unterstützung von Wake on LAN (WoL), um eine Möglichkeit zu schaffen, das so genannte WoL Magic Packet zu einem schlafenden Endgerät zu transportieren, auch wenn sich der entsprechende Port im nicht autorisierten Zustand befindet.

Bei einem Port, der im nicht autorisierten Zustand beidseitig blockiert, sieht ein Angreifer lediglich ein EAPOL-Paket, das ihn zur Authentisierung auffordert. Wenn der Port nur einseitig blockiert, sieht der Angreifer stets zumindest alle Broadcasts in der Broadcast-Domäne, was ein geringeres Sicherheitsniveau bedeutet.

In der Neufassung von 2010 von IEEE 802.1X wurde die Funktion der einseitigen Blockierung wieder entfernt. Eine Unterstützung von WoL wird jetzt explizit durch die Default Policy erreicht.

Simultane Authentisierung mehrerer Geräte an einem Port

Die Möglichkeit der simultanen Authentisierung mehrerer Endgeräte wurde an zwei Stellen in die Neufassung des Standards aufgenommen: im normativen und im informellen Teil.

Im normativen Teil wird beschrieben, wie simultan mehrere gesicherte Kommunikationsbeziehungen von einem Port behandelt werden können. Idee ist dabei, dass jede MAC-Adresse über eine eigene MAC Security Entity (SecY) authentisiert wird und einen eigenen kryptographisch geschützten Kommunikationskanal erhält. Dies entspricht auch exakt dem Konzept in WLAN, wo ein Access Point simul-

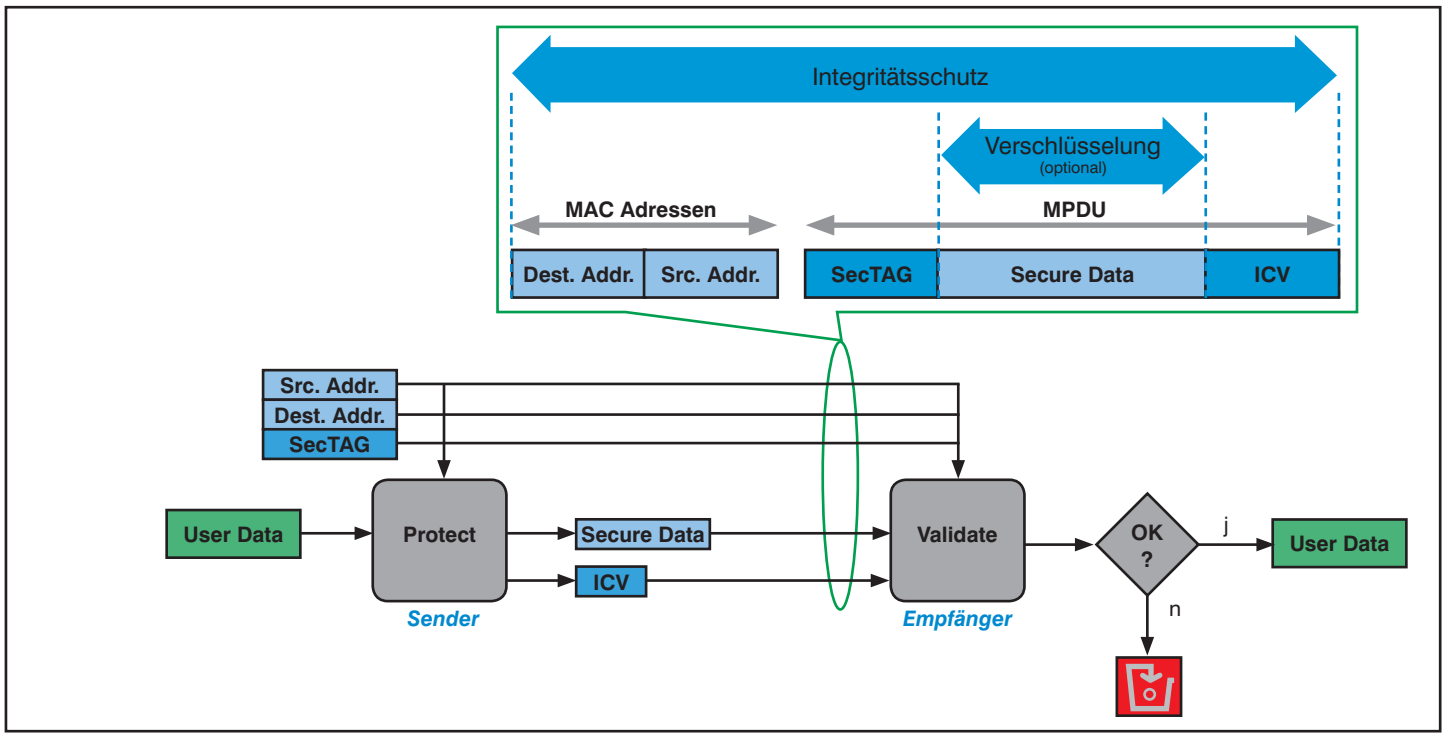


Abbildung 12: Sicherung der Übertragung mit MACsec

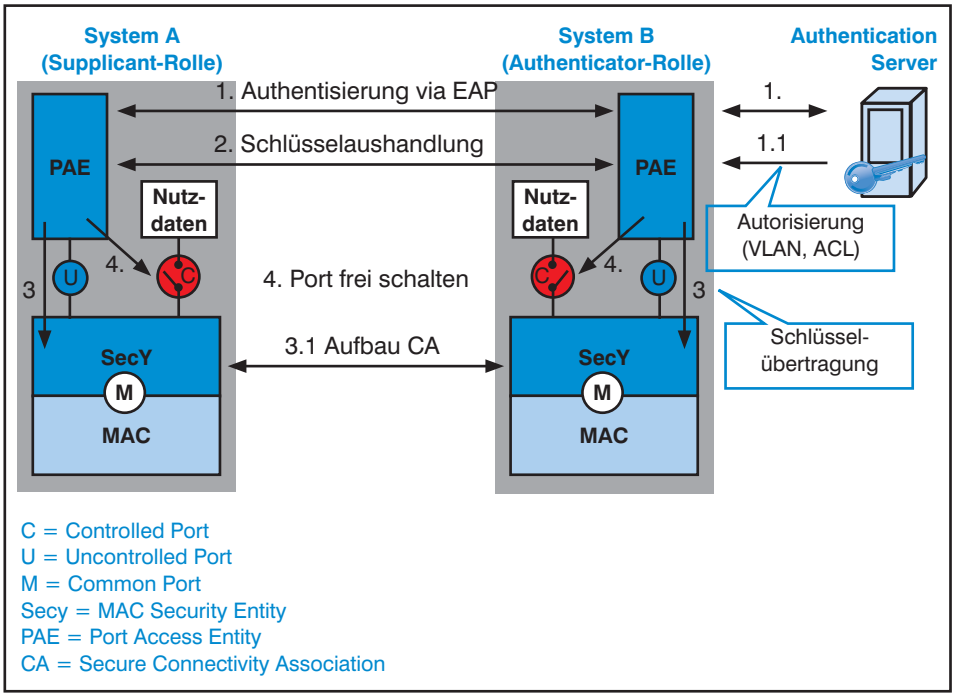


Abbildung 13: Schritte für den Aufbau einer abgesicherten Kommunikationsbeziehung mit IEEE 802.1X-2010

tan unterschiedliche verschlüsselte Kanäle zu den verschiedenen Stationen unterhält, die an ihm assoziiert sind.

Weiterhin gestattet die Neufassung von IEEE 802.1X auch ohne die Verwendung von MACsec die simultane Authentisierung nach dem Schema, das auch heute von vielen Herstellern verwendet wird (siehe Abbildung 5 und Abbildung 6). Allerdings wurde diese Spezifikation bewusst in eine informellen Anhang des Standards gepackt (siehe Anhang G „Unsecured multi-access LANs“ von IEEE 802.1X-2010).

Wichtig ist, dass damit zumindest den bestehenden herstellerspezifischen Implementierungen der simultanen Authentisierung mehrerer Endgeräte an einem Port nicht mehr der Geruch einer bewussten Standardverletzung anhaftet.

Sichere Geräteidentifizierung mit IEEE 802.1AR

Der Standard IEEE 802.1AR „Secure Device Identity“ ist Ende 2009 verabschiedet worden und schließt eine wesentliche Lücke zur Absicherung von Netzen. In der Vergangenheit gab es als einheitliches Identifikationsmerkmal eines Endgeräts in einem LAN lediglich die MAC-Adresse, was aus einer Sicherheitsperspektive ausgesprochen schwach ist und nur in einem kryptographisch abgesicherten Kontext (etwa mit MACsec) sicher ist.

Natürlich haben Hersteller in ihren Lösungen spezifische Mechanismen eingesetzt, um sicherzustellen, dass sich ein Gerät (z.B. ein IP-Telefon oder ein WLAN Thin Access Point), das sich an eine zentrale Komponente (z.B. ein Telefonie-Server oder ein WLAN Controller) der jeweiligen Lösung anmelden möchte, auch authentisiert. Hier wird in der Praxis oft mit Zertifikaten gearbeitet, die im einfachsten Fall bereits auf den Geräten vorinstalliert werden und – je nach System – durch nutzerspezifische Zertifikate ergänzt werden können.

Um den damit verbundenen Wildwuchs unterschiedlicher Formen der Identifikation von Geräten zu bremsen, wurde IEEE 802.1AR spezifiziert. Es ist nicht überraschend, dass in IEEE 802.1AR die Nutzung von Zertifikaten und die Authentisierung mit EAP-TLS eine explizit erlaubte Betriebsform darstellt. Die Neufassung von IEEE 802.1X geht hier sogar soweit, dass ein Supplicant, der eine sichere Geräteidentifizierung gemäß IEEE 802.1AR anbietet, eine entsprechende Authentisierung mit EAP-TLS zwingend unterstützen muss.

Produktsituation

Der Standard IEEE 802.1X-2010 schließt entscheidende Lücken der Vorversion von 2004. Es bleibt die Frage, wie schnell sich dies auch in Implementierungen am Markt materialisiert. Besonders kritisch ist dabei die Verfügbarkeit von IEEE 802.1AE, da hier neue Hardware erforderlich ist.

Auf Seiten der NIC-Hersteller ist seit 2008 eine deutliche Bewegung sichtbar. Hersteller wie Intel, Marvell und SafeNet haben Chips mit IEEE 802.1AE im Programm. Auf Seiten der Netzwerkausrüster ist bislang Cisco am weitesten. In einem ersten Schritt hat Cisco mit TrustSec für die Nexus 7000 Serie eine Implementierung von IEEE 802.1AE herausgebracht. Hier wurde zunächst der Aufbau von hoch-performanten Sicherheitszonen im RZ adressiert. Konzeptionell sind mit TrustSec aber bereits alle wesentlichen Elemente von IEEE 802.1X-2010, insbesondere die Verwendung von IEEE 802.1X für das dynamische Schlüsselmanagement, umgesetzt worden. Schrittweise wird IEEE 802.1AE jetzt auch für kleinere nicht-modulare Switches angeboten. Seit Frühjahr 2010 gibt es beispielsweise Trustsec auf den Switches der Serie

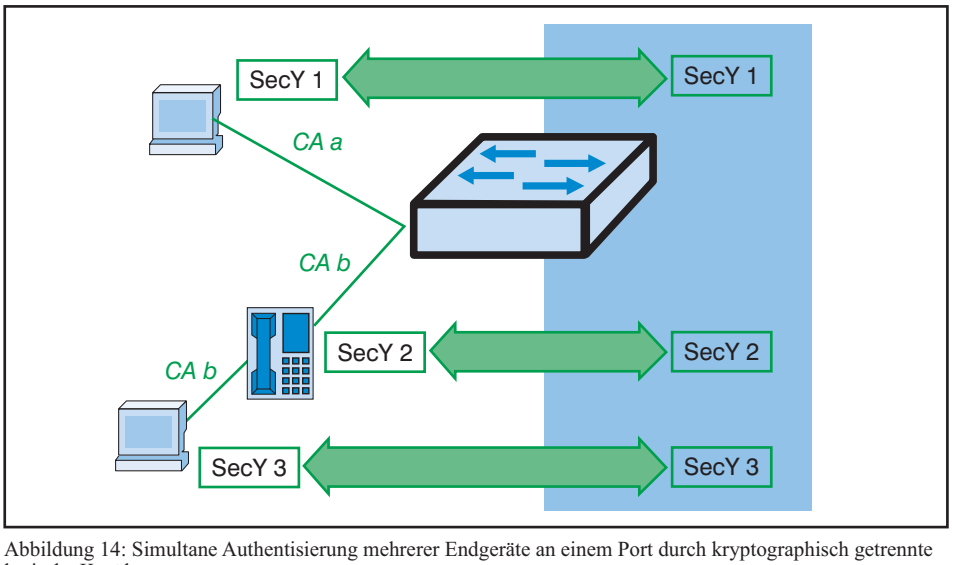


Abbildung 14: Simultane Authentisierung mehrerer Endgeräte an einem Port durch kryptographisch getrennte logische Kanäle

Catalyst 3750-X und 3560-X. Damit ist die Implementierung von IEEE 802.1AE endlich im Bereich des Endgeräteanschlusses angekommen.

Es fehlt noch die Unterstützung von IEEE 802.1AE auf Ebene der Betriebssysteme (z.B. Windows). Da hier erst die Verabschiedung von IEEE 802.1X-2010 abgewartet werden musste, besteht jetzt die Hoffnung, dass sich auch diese letzte Lücke bald schließt.

4. Fazit

Allen Unkenrufen zum Trotz ist IEEE 802.1X ein vitaler Standard für das kabelbasierte LAN, der auch immer stärker in der Praxis genutzt wird. Es gibt nun einmal keine Alternative. Auch der Trend zur Anwendungs- und Desktop-Virtualisierung ändert hier nichts. Die Notwendigkeit einer sicheren Geräteidentifizierung am Netzwerk wird bleiben, und IEEE 802.1X ist hier für Netzwerke das einzige standardisierte Instrument.

Mit der Neuauflage von IEEE 802.1X im Februar 2010 sind endlich die offenen Punkte der Fassung von 2004 adressiert worden, und es ist erstmals möglich, solide abgesicherte Kommunikationsbeziehungen in LANs im Campus- und Datacenter-Bereich ohne Leistungsverlust und skalierbar auch für große Netze zu gestalten. Die Standardfamilie IEEE 802.1X-2010, IEEE 802.1AE und IEEE 802.1AR hat für das kabelbasierte LAN einen strategischen Charakter, der für lange Zeit das LAN-Design beeinflussen wird.

Dass es sich dabei nicht um einen Papiertiger handelt, zeigen die aktuellen Produktentwicklungen.

5. Abkürzungen

ACL	Access Control List
AES	Advanced Encryption Standard
AMT	Active Management Technology
CA	Secure Connectivity Association
CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	IP Security
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
LLDPmed	LLDP Media Endpoint Discovery
MAC	Media Access Control
MAN	Metropolitan Area Network
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
NAC	Network Access Control
NAP	Network Access Protection
NEA	Network Endpoint Assessment
NIC	Network Interface Card
PAE	Port Access Entity
PEAP	Protected EAP
PXE	Preboot Execution Environment
RFC	Request For Comments
RADIUS	Remote Authentication Dial-In User Service
SA	Security Association
SC	Secure Channel
SCS	Setup and Configuration Service
SecY	MAC Security Entity
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TNC	Trusted Network Connect
UDP	User Datagram Protocol
UHD	User Help Desk
VLAN	Virtual LAN
VM	Virtual Machine
VPN	Virtual Private Network
WLAN	Wireless LAN
WoL	Wake on LAN

6. Literatur

[1] IEEE 802.1X-2004, „Port-Based Network Access Control", Dezember 2004; verfügbar unter http://www.ieee.org

[2] IEEE 802.1AE-2006, „Media Access Control (MAC) Security", August 2006, verfügbar unter http://www.ieee.org

[3] IEEE 802.1AR-2009, Secure Device Identity", Dezember 2009, verfügbar unter http://www.ieee.org

[4] IEEE 802.1X-2010, „Port-based Network Access Control", Februar 2010, verfügbar unter http://www.ieee.org

[5] RFC 2865, „Remote Authentication Dial In User Service (RADIUS)", IETF Standards Track, Juni 2000, http://www.ietf.org/rfc/rfc2865.txt

[6] RFC 3748, „Extensible Authentication Protocol (EAP)", IETF Standards Track, Juni 2004, http://www.ietf.org/rfc/rfc3748.txt

[7] RFC 3579, „RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", IETF Informational, September 2003, http://www.ietf.org/rfc/rfc3579.txt

[8] RFC 5216, „The EAP-TLS Authentication Protocol", IETF Standards Track, März 2008, http://www.ietf.org/rfc/rfc5216.txt

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001, 31.05. - 02.06.10 in Köln

Informationssicherheit ist heutzutage ein Muss, sei es aus rechtlichen oder wettbewerbstechnischen Gründen. Den vielfältigen „Compliance"-Ansprüchen gesellt sich der Aspekt einer Konformität zu BSI-Methodik bzw. ISO 27001 hinzu und die Anforderung, sich an den zugehörigen Kontrollfragen und Maßnahmenkatalogen erfolgreich messen zu können. Längst sind ISO 27001 und BSI-IT-Grundschutz nicht mehr nur eine Möglichkeit, sich „werbewirksam" zertifizieren zu lassen. Vielfach liefert ihre Anwendung die erwartet plausible Antwort auf die Frage nach Erreichung eines „best-practice"-Mindest-Sicherheitsniveaus oder nach angemessenem (!) Sicherheitsaufwand bei erhöhtem Sicherheitsbedarf. So nützlich diese Hilfestellung bei Aufbau und Aufrechterhaltung der nötigen Sicherheit sind, so sehr kann bei mangels Erfahrung „ungeschickter" Anwendung ein enormer, vermeidbarer Arbeitsaufwand entstehen. Erfahrungen aus ComConsult-Projekten zur Anwendung der Methoden und Werkzeuge, mit und ohne abschließender Zertifizierung, können und sollen hier helfen.

Preis: € 1.690,-- zzgl. MwSt.

Projekt-Erfahrungsbericht: Cisco CallManager Rollout und Migration CUCM Version 6, 07.06.10-08.06.10 in Königswinter

Dieses 2-tägige Seminar beschreibt Planung, Installation und den Betrieb einer großen verteilten IP-Telefonie-Lösung auf der Basis des Cisco CallManagers. Es macht deutlich, in welchem Umfang die Standard-Installation angepasst und erweitert werden musste, um den Anforderungen der Teilnehmer zu entsprechen. Auch die Umstellung traditioneller Betriebsabläufe im Änderungs-Management und deren Auswirkung auf die Konfiguration des CallManagers wird beschrieben. In diesem Zusammenhang werden insbesondere auf die Akzeptanz der Benutzer und die damit notwendigen Änderungen in der Bedienung der Telefone eingegangen. Preis: € 1.390,-- zzgl. MwSt.

E-Mail-Archivierung planen, evaluieren, umsetzen, 14.06.10-16.06.10 in Frankfurt a.M.

Dieses Seminar behandelt einerseits die rechtlichen Vorschriften zur Speicherung von E-Mails und anderen digitalen Dokumenten sowie die zahlreichen Regelungen zur Beschränkung des Zugriffs auf die Daten aus Gründen des Persönlichkeitsrechts, des Fernmeldegeheimnisses, des Schutzes von Betriebsgeheimnissen und des Datenschutzes.

Preis: € 1.690,-- zzgl. MwSt.

Virtualisierungstechnologien in der Analyse, 14.06.10-16.06.10 in Düsseldorf

Dieses Seminar analysiert die verfügbaren Virtualisierungstechnologien der führenden Anbieter. Sie lernen, welche Gestaltungselemente virtuelle Umgebungen haben, angefangen von einfachen und überschaubaren Lösungen bis hin zu komplexen und umfassenden Rechenzentrums-Gesamt-Architekturen. Dabei wird auch der Bedarf an Infrastruktur-Leistung insbesondere auf der Netzwerkseite untersucht.Dieses Seminar analysiert die verfügbaren Virtualisierungstechnologien der führenden Anbieter. Sie lernen, welche Gestaltungselemente virtuelle Umgebungen haben, angefangen von einfachen und überschaubaren Lösungen bis hin zu komplexen und umfassenden Rechenzentrums-Gesamt-Architekturen. Dabei wird auch der Bedarf an Infrastruktur-Leistung insbesondere auf der Netzwerkseite untersucht.

Preis: € 1.690,-- zzgl. MwSt.

Sicherheit im LAN mit IEEE 802.1X, 17.06. - 18.06.10 in Düsseldorf

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes.

Preis: € 1.390,-- zzgl. MwSt.

Ethernet Technologien neuester Stand, 21.06. - 22.06.10 in Bonn

Dieses Premium-Seminar bieten wir Ihnen mit multimedialem erweitertem Leistungsspektrum an:
Vorbereitungs-Videos im Vorfeld des Seminars, Live-Seminar, Vertiefungs-Videos zur Nachbereitung des Seminars, Volltext-Dokumentation über 480 Seiten in Report-Qualität.

Preis: € 1.590,-- zzgl. MwSt.

Unified Communications mit Siemens - HiPath 8000 & OpenScape im Überblick, 21.06. - 22.06.10 in Bonn

Mit der Zusammenführung der rein SIP-basierten TK-Lösung HiPath 8000 und der Applikation-Suite OpenScape präsentiert Siemens ein umfangreiches Kommunikationsprodukt, das verspricht, im Sinne von Unified Communications alle modernen Kommunikationstechnologien unter einer gemeinsamen Struktur für den Endanwender steuerbar und nutzbar zu machen. So wurden neben der in der Tradition der bekannten HiPath-Telefonanlagen stehenden Sprachlösung weitere Dienste und Leistungsmerkmale wie Präsenzanzeige, Erreichbarkeitsanzeige, regelbasierte automatische Steuerung der Erreichbarkeit, Instant Messaging, Fax und E-Mail sowie Webkollaboration und Videokonferenzsysteme integriert.

Preis: € 1.690,-- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 21.06. - 22.06.10 in Bonn

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,-- zzgl. MwSt.

Trouble Shooting für Netzwerk-Anwendungen, 22.06. - 25.06.10 in Aachen

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.190,-- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
13.09. - 17.09.10 in Aachen
22.11. - 26.11.10 in Aachen

TCP/IP und SNMP
27.09. - 01.10.10 in Stuttgart

Internetworking
25.10. - 29.10.10 in Aachen

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290,--)

ComConsult Certified Trouble Shooter

Trouble Shooting 1
21.09. - 24.09.10 in Aachen

Trouble Shooting 2
22.06. - 25.06.10 in Aachen
26.10. - 29.10.10 in Aachen

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 4.120.-- zzgl. MwSt.
(Seminar-Einzelpreis € 2.190,--, mit Prüfung € 2.370,--)

ComConsult Certified Voice Engineer

Session Initiation Protocol-Basis-Technologie der IP-Telefonie
28.06. - 30.06.10 in Bonn
22.11. - 24.11.10 in Hamburg

Sicherheitsmechanismen für Voice over IP
21.06. - 22.06.10 in Bonn
03.11. - 04.11.10 in Bonn

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
12.07. - 14.07.10 in Bonn
04.10. - 06.10.10 in Bonn
13.12. - 15.12.10 in Stuttgart

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
27.09. - 28.09.10 in Stuttgart
15.11. - 16.11.10 in Königswinter

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

ComConsult Zertifizierter Projektleiter

Projektmanagement I: Projekte aus IT und Kommunikationstechnik leiten und organisieren
08.11. - 12.11.10 in Aachen

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Teams führen
29.11. - 03.12.10 in Aachen

Paketpreis für beide Seminare € 4.090,-- zzgl. MwSt. (Einzelpreise: € 1.990,-- und € 2.290,--)

Impressum

Verlag:
ComConsult Technology Information Ltd.
ComConsult Research
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie