ComConsult Research

# Der Netzwerk Insider

Mai 15

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

## IT-Sicherheit im Zeitalter der Cyberangriffe

**von Dr. Melanie Winkler**

**Jedem Nutzer elektronischer Daten sollte mittlerweile klar geworden sein, dass alle Informationen, welche über ein öffentliches Netz übertragen werden, generell durch Unbefugte abgegriffen werden können. Dies gilt umso mehr seit den Enthüllungen durch Edward Snowden und die dadurch öffentlich bekannt gewordenen Angriffe auf vertrauliche Daten unterschiedlicher Art durch große Hackerangriffe. Daher wird natürlich schon seit einiger Zeit, zum Beispiel durch das BSI, die Empfehlung ausgesprochen, vertrauliche Daten ausschließlich verschlüsselt zu übertragen und zu speichern.**

Im Rahmen der Enthüllungen durch Edward Snowden ist jedoch auch bekannt geworden, dass zumindest einige große Hackergruppen - häufig mit staatlicher Unterstützung - über weitere Methoden verfügen, an Informationen zu gelangen, welche für sie von Interesse sind. Es stellt sich Unternehmen und Privatanwender daher immer mehr die Frage, wie sicher ihre Daten wirklich noch sind. Lohnt es sich beispielsweise als Endanwender überhaupt noch Daten zu verschlüsseln oder können diese nicht sowieso mit vergleichbar geringem Aufwand entschlüsselt und gelesen werden?

weiter auf Seite 6

Zweitthema

## High Performance Storage

**von Dr. Joachim Wetzlar**

**Die Diskussion Fiber Channel versus Fibre Channel over Ethernet (FCoE) ist inzwischen ein alter Hut. Die FCoE-Euphorie vom Anfang dieses Jahrzehnts ist verflogen; ungeachtet dessen werden heute beide Techniken eingesetzt.**

Network Attached Storage (NAS) ist bei vielen unserer Kunden auf dem Vormarsch – auch in Bereichen, die aus Performance-Gründen traditionell mit Fibre Channel SAN betrieben wurden. Die Rede ist z.B. von Datenbanken oder Data Stores der Server-Virtualisierung. Auf der anderen Seite werden die Speicher immer schneller; Storage Tiering mit schnellen Solid State Disks (SSD) in der höchsten Speicherklasse wird zu einer Selbstverständlichkeit. Wenn aber der Speicher hohe Datenraten und Unmengen von Input/Output Operations pro Sekunde (IOPS) unterstützt, muss das auch für die Schnittstellen zu diesem Speicher gelten. Ja, Fibre Channel und geswitchtes Multi-Gigabit Ethernet sind bereits sehr schnell. Wie wäre es also, wenn man nun auf der Betriebssystemseite optimierte? Ein vielversprechender Ansatz dafür ist Remote Direct Memory Access (RDMA). Hier hat es in jüngster Vergangenheit einige interessante Neuentwicklungen gegeben. Sogar (und gerade) Microsoft ist auf den Zug aufgesprungen. Und auch eine altbekannte Nischentechnologie aus dem High Performance Computing kommt wieder zu ihrem Recht, das Infiniband.

weiter auf Seite 16

Geleit

## Bandbreite erschlägt alles: gilt das immer noch?

auf Seite 2

Aktuelle Veranstaltung

## Sommerschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

ab Seite 4

Standpunkt

## Monitoring von Voice- und Video-Strömen!

auf Seite 14

Aktuelle Sonderveranstaltung

## Voice und Video im WAN

ab Seite 15

Zum Geleit

# Bandbreite erschlägt alles: gilt das immer noch?

Wir hatten in der Vergangenheit viele Diskussionen über die Notwendigkeit von Quality of Service in Netzwerken. Und meine Haltung war, dass ein solide geplantes und aufgebautes Netzwerk mit ausreichend Bandbreiten-Reserven keine QoS benötigt. Das wurde auch durch diverse Messungen und Tests in zum Teil sehr großen Kundennetzen immer wieder bestätigt. Insbesondere das Argument, dass VoIP QoS im LAN benötigt, hat sich aus meiner Sicht als nicht belegbar herausgestellt (ich will die Diskussion hier nicht wieder starten, mir ist klar, dass es ganz verschiedene Motivationen für den Einsatz von QoS geben kann).

Nun haben wir ja mit moderner Netzwerk-Technologie sehr viel Bandbreite, seien es 10, 40 oder 100 Gigabit-Ethernet im LAN. Dann hat sich das Thema jetzt ja wohl erledigt, oder?

Tatsächlich hat sich Netzwerk-Technologie zusammen mit den typischen Nutzungs-Situationen in den letzten Jahren verändert. Es gibt dabei mindestens drei Bereiche, die einer besonderen Beachtung bedürfen:

- Der Ost-West-Verkehr zwischen virtuellen Servern und zentralen Speichersystemen stellt hohe und vor allem schwer vorhersehbare Anforderungen an Netzwerke. Auch wenn FCoE nicht in dem prognostizierten Ausmaß gekommen ist, haben wir mit iSCSI und NFS oder ähnlichen Verfahren Datenströme, die ein erhebliches Ausmaß annehmen können. Und was besonders wichtig ist: das kann sich sehr schnell ändern, je nachdem was auf der Speicherseite passiert.

- Der Wunsch, automatisch Anwendungen aus einem Service-Katalog wie aus der Public Cloud bekannt auch im lokalen Umfeld starten zu können, verändert unsere Netzwerk-Welt. Persönlich bin ich zwar sehr skeptisch, ob wir diesem Wunsch wirklich folgen sollten, aber wir reden hier auch über ein politisches Thema, das nicht immer nach rein technischen Kriterien entschieden wird. Die Umsetzung dieses Wunsches erfordert programmierbare und vor allem virtualisierte Netzwerke im Rahmen einer Open Stack-Realisierung.

- Im Umfeld dynamischer virtueller Architekturen gibt es ähnlich dem Konstrukt,

das wir bei der automatischen Inbetriebnahme von Anwendungen haben, den Bedarf, die virtuellen Elemente, die zu einem Service gehören, durch ein abstraktes Netzwerk miteinander zu verbinden. Dieses Netzwerk integriert auch Netzwerk-Elemente wie Switches, Router, Load-Balancer als Software-Elemente. Der Grund für diese Architektur liegt in der Skalierbarkeit durch Parallelisierung von virtuellen Maschinen und der damit verbundenen Beweglichkeit der einzelnen virtuellen Elemente. Die damit erreichte Ortsneutralität hat zudem eine ganze Reihe weiterer Vorteile. Da dabei u.a. Layer-2-Verbindungen über Layer-3-Grenzen hinweg geschaltet werden müssen und Technologien wie LISP hier ein Overkill sind (auch wenn ich persönlich ein LISP-Anhänger bin), brauchen wir Technologien, die Netzwerk-neutral einen solchen Service-Verbund umsetzen.

Was hat das nun mit QoS zu tun? Bitte warten Sie noch einen weiteren Gedankengang, bevor ich darauf zurück komme.

Aus meiner Sicht brauchen wir für die Zukunft der LANs Edge/Core-Technologien, die die Intelligenz mit den Service-Definitionen am Rand umsetzen und den Kern relativ einfach gestalten. Ich habe große Befürchtungen, dass Technologien, die es erfordern Service-Anforderungen in jedem Switch zu programmieren zu einem Komplexität-Desaster führen. Aus diesem Grund bin ich auch von CISCO ACI nicht überzeugt (und bitte, kann endlich mal jemand das CLI-Interface aus solchen Lösungen entfernen? In welchem Jahrhundert leben wir denn eigentlich?).

Edge/Core-Lösungen sind aber direkt mit zwei Fragen verbunden:

1. Ist der Edge immer Software? Also immer eine Software-Switch in einem Hypervisor?

2. Was gilt eigentlich im Core, wie kann oder muss dieser gestaltet werden?

## Bandbreite erschlägt alles: gilt das immer noch?

Meine persönlichen Antworten:

Zu 1: Nein, sowohl als auch. Ich kann den Edge nicht auf Software reduzieren und in jedem Fall sollte die Software Virtualisierungs-neutral sein, also zum Beispiel nicht an VMWare gebunden sein. Es gibt in jedem Fall auch Situationen, in denen das Edge-System Hardware sein muss. Ich brauche also sowohl Software als auch Hardware als Edge-System. Dies wiederum kann nur auf der Basis eines internationalen Standards geleistet werden. Jede hersteller-spezifische Lösung greift hier zu kurz. Und mein persönlicher Favorit ist hier ganz klar SPB. Da auch zunehmend ASIC-Hersteller SPB-Funktionalität in den ASIC aufnehmen, ist es hoffentlich nur eine Frage der Zeit bis wir eine breitere Unterstützung dieses Verfahren erreichen.

Zu 2: Die Frage nach QoS oder nicht reduziert sich für mich dann auf das Core-Design. Ich habe noch keine abgeschlossene Meinung, ob ich IS-IS für ausreichend halte. Aber im Kern bin ich davon überzeugt, dass wir einen Core wieder nach den Prinzipien der ausreichenden Bandbreite planen können (in bestimmten Situationen werden wir nicht an DCB vorbei kommen).

Ich hoffe, dass damit klar geworden ist, dass die Frage nach QoS für mich gar nicht so entscheidend ist, die Probleme im Design eines LAN sind eben anders gelagert. Meine Kernfragen sind:

- brauchen wir programmierbare Netzwerke mit Abstrahierung?
- brauchen wir Service-Orientierung im Netzwerk?

Im Gegensatz zu früher sehe ich aber durchaus Themenbereiche, wo ich QoS beachten muss. Dies ist der Bereich Ost-West-Verkehr und möglicherweise die Frage, was wir in einem Schrank zwischen den vielen virtuellen Maschinen in Zukunft machen.

Aber wo wir gerade bei dem Thema QoS sind: wir haben natürlich einen Bereich, in dem das Thema explodiert und entscheidend wird. Dies ist der WAN-Bereich. Wir werden spätestens mit der Ablösung von ISDN und vermutlich auch schon deutlich früher eine deutliche Zunahme von Sprache und Video im WAN haben. Zum einen glaube ich, dass wir ernsthaft schon auf der Endgräteseite über Shaping nachdenken müssen. Speziell bei mobilen Endgeräten im WLAN halte ich eine Begrenzung der Auswirkung von YouTube oder ähnlich gelagerten Nutzungen für unvermeidbar. Die WLAN-Hersteller bieten auch zunehmend solche Mechanismen an (siehe Aruba als Beispiel). Aber wir haben dann immer noch den eigentlich unvermeidlichen Sprach und Video-Verkehr, der ein normal designtes WAN schnell überfordern kann. Hier müssen wir sowohl die Frage nach der ausreichenden Dimensionierung als auch nach der geeigneten Balance zwischen anderen Anwendungen und dem Sprache-/Video-Bereich finden.

Ihr
Dr. Jürgen Suppan

Aktuelles Seminar

# Sommerschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

## 22.06. - 26.06.15 in Aachen

## Frühbucherphase bis zum 31.05.2015

Die Sommerschule 2015 bringt Sie in 5 Intensiv-Tagen auf den letzten Stand der Netzwerk-, Kommunikations- und Infrastruktur-Technik.
Wir analysieren für Sie:

- Wie verändern sich IT-Architekturen?
- Welche neuen Technologie-Ansätze gibt es bei Netzwerken?
- Welche Auswirkungen hat das auf Netzwerke, Kommunikations-Technik und Infrastrukturen in der täglichen Praxis?
- Welche Änderungen und Investitionen sind auf Ihrer Seite in der nächsten Zeit erforderlich?

### Programmübersicht Sommerschule 2015

#### Montag, der 22.06.15 - IT-Architekturen und Auswirkungen auf auf LAN und WAN

IT-Architekturen sind geprägt von Endgeräten, die lokale Anwendungen ausführen und auf Applikationen auf Server zugreifen. Im Moment ändert sich hier alles. Unser Verständnis von Endgerät, Betriebssystem und Server muss auf den Prüfstand. Ohne Zweifel wird unsere IT-Landschaft in fünf Jahren dramatisch anders aussehen als heute. Und Netzwerke haben die zentrale, tragende Rolle für diese Entwicklung. Wir analysieren wo es hingeht und wie Netzwerke aussehen müssen, um diesen Weg zu unterstützen.

**9:30 - 17:00 Uhr**
Wir analysieren für Sie:

- Wie ändert sich IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerk-Seite, um diesen Anforderungen zu entsprechen?
- Welche neuen Technologien müssen speziell bei den Planungen für die nächsten Jahre beachtet werden?

*Dr. Franz-Joachim Kauffels, unabhängiger Technologie- und Industrie-Analyst*

Das WAN gewinnt mit den Entwicklungen im IT-Architektur-Bereich immer mehr an Bedeutung. Gleichzeitig entstehen Nutzungssituationen, die wirtschaftlich nicht immer abgedeckt werden können.

Wir analysieren für Sie:

- Welchen Stellenwert haben aktuelle WAN-Technologie für eine moderne IT
- Internet versus WAN: was ist besser?
- Ist Mobilfunk die Zukunft? Taugt es als Ersatz für terrestrische Leitungen?
- Anforderungen von Voice und Video: B2B und B2C puschen den Video-Anteil in bisher unerreichte Höhen, wie kann das WAN damit umgehen?
- QoS im WAN: unlösbarer Widerspruch oder wie weit gehen die vorhandenen Lösungen?

*Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH*

**11:00 - 11:15 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:00 - 15:15 Uhr Kaffeepause**
**ab 19:00 Uhr Happy Hour**

#### Dienstag, der 23.06.15 - LAN-Technologien: aktuelle Entwicklungen

LAN-Technik wird im Moment neu erfunden. Neue Anforderungen erfordern neue Lösungen. Programmierbare Netzwerke als Teil des Software Defined Data Center und als Teil von Software Defined Infrastrukturen sind ein Beispiel dafür. Neue Fabric-Konzepte, ein Umdenken bei VLAN-Technik, eine Neupositionierung von QoS und neue Nutzungsformen im Rahmen von Audio-/Video-Bridging sind herausragende Beispiele. Wir erklären, was im Moment passiert und wie Sie sich auf die Zukunft vorbereiten.

**9:00 - 17:00 Uhr**
Sie lernen in diesem Themenblock:

- Welche neuen LAN-Technologien gibt es, welche Konsequenzen hat das?
- Netzwerk-Design mit 10/40/100 Gigabit, wie sehen Anforderungen und Planungs-Ansätze aus?
- Fabric-Konzepte verdrängen traditionelle Architekturen: was leisten sie und wie können sie sinnvoll eingesetzt werden?
- Edge/Core-Architekturen mit neuen Formen von Label-Switching: ist hier die Zukunft?
- Quo Vadis VLAN-Technik: werden VLANs durch Edge-Provisioning und Overlays verdrängt?

*Dipl.-Inform. Petra Borwoka-Gatzweiler, Planungsbüro UBN*

**10:30 - 10:45 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:00 - 15:15 Uhr Kaffeepause**

#### Mittwoch, der 24.06.15 - Sicherheit / Unified Communications: wo stehen wir?

Sicherheit in der IT wird zum dominierenden Thema der nächsten Jahre. Aber hier geht es nicht um hochfliegende Träume, sondern um ein solides Fundament aus Basis-Sicherheits-Funktionen. Dies ist das Thema des Bereichs Sicherheit in der Sommerschule:

**9:00 - 12:30 Uhr**

- Sicherheit im LAN: neueste Entwicklungen
- Sicherheit und mobile Endgeräte: haben wir noch eine Chance unsere Sicherheit zu retten?
- Sicherheit und UC: immer offener und immer sicherer, ist das ein unlösbarer Widerspruch?

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

UC-Projekte haben in den letzten Jahren deutlich an Komplexität gewonnen. Zwar haben sich die Produkte weiter entwickelt, doch gleichzeitig hat sich ein neues Verständnis von Kommunikation mit einer gleichzeitigen Verschiebung der Funktionsbereiche ergeben. Moderne Browser beinhalten heutzutage die komplette Funktionalität eines UC-Clients für Sprache und Video und generieren die Frage nach der Zukunft des Telefons.

**14:00 - 17:00 Uhr**
In diesem Themenblock lernen Sie:

- Wo steht UC heute?
- Wie sieht die Zukunft des Clients aus?
- Wird das Telefon als Endgerät verdrängt?
- Was kommt nach ISDN?
- UC und Kollaboration: Gibt es überhaupt noch eine Abgrenzung? Wie sieht die Zukunft aus?
- Welche Rolle werden Produkte wie Cisco Project Square oder Unify Circuit für den Markt haben?
- Was bedeutet diese Entwicklung für Infrastrukturen?

*Dipl.-Inform. Petra Borwoka-Gatzweiler, Planungsbüro UBN*
*Markus Geller, ComConsult Research GmbH*

**10:30 - 10:45 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:00 - 15:15 Uhr Kaffeepause**

## Programmübersicht Sommerschule 2015

### Donnerstag, der 25.06.15 - WLAN und Mobilfunk / IPv6: aktueller Stand bei Unternehmen

Mit der rasanten Zunahme mobiler Endgeräte bekommt der Zugang dieser Geräte zu den Unternehmens-Infrastrukturen eine zentrale Bedeutung. In Zukunft werden deutlich mehr Endgeräte diesen Zugang wählen als die Kabel-basierte Alternative. Denkt man einen Schritt weiter zum Internet of Everything, dann wird die zukünftige strategische Bedeutung des Zugangs über WLAN und Mobilfunk deutlich. Sowohl die schiere Anzahl der Teilnehmer als auch der damit verbundene Schutz- und Kontrollbedarf machen Änderungen an der Netzwerk-Infrastruktur erforderlich.

**9:00 - 12:30 Uhr**
In diesem Themenblock lernen Sie:
- Welche Optionen Ihnen das moderne WLAN bietet
- Wie sich Mobilfunk-Alternativen demgegenüber positionieren

*Dr. Franz-Joachim Kauffels, unabhängiger Technologie- und Industrie-Analyst*

IPv6 Projekte sind angelaufen. IPv6 existiert nicht mehr nur in Forschungsumgebungen, bei den Providern und in Testnetzen von Unternehmen. Immer mehr Firmen haben mit der Migration begonnen, von DAX 30 bis Mittelständler, von Finanzinstituten bis zur Fertigung. Nicht nur der Internet-Auftritt, der Provider-Anschluss und die Homeoffice VPNs werden migriert. Auch in den Unternehmen selbst hat die Migration begonnen.

**14:00 - 17:00 Uhr**
In diesem Themenblock lernen Sie:
- Welche Entscheidungen wann getroffen werden müssen
- Wie man ein IPv6 Projekt planerisch und organisatorisch umsetzt
- Wie man die IPv6 Migration in den Lifecycle von Hard- und Software integriert
- Warum ein Migrationsprojekt nicht so teuer ist, wie viele annehmen
- Wo mit Schwierigkeiten zu rechnen ist und wo nicht
- Wie man die Internet-Präsenz schrittweise migriert
- Worauf bei Software und Appliances in Bezug auf IPv6 zu achten ist

*Markus Schaub, ComConsult Study.tv*

**10:30 - 10:45 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:00 - 15:15 Uhr Kaffeepause**

### Freitag, der 26.06.15 - Rechenzentren: neue Arten von Infrastrukturen gefordert

Rechenzentren sind von allen Seiten unter Druck:
- Die Cloud generiert einen direkten Kostenvergleich und puscht das Thema Wirtschaftlichkeit im RZ noch weiter als bisher
- Infrastrukturen für mobile Endgeräte erfordern den Aufbau einer private Cloud und setzen neue Anforderungen an Infrastrukturen
- Server- und Speicher-Konsolidierungen gehen permanent weiter, neue Perspektiven entstehen und stellen alle traditionellen Ansätze in Frage
- Virtualisierung geht in die nächste Runde, leistet noch mehr, stellt aber auch immer mehr und immer schwierigere Anforderungen an die Infrastrukturen

Angesichts dieser Entwicklungen brauchen Rechenzentren eine neue und Zukunftsorientierte Infrastruktur-Strategie.

**9:00 - 15:30 Uhr**
Sie lernen in diesem Themenblock:
- Was passiert im RZ, welche neuen Anforderungen entstehen?
- Wo stehen Server und Speicher?
- Welche Anforderungen generiert Virtualisierung?
- Dienstneutralität im Netzwerk: geht das noch im RZ der Zukunft? Brauchen wir ein neues Verständnis von Netzwerken?
- Open Stack und SDN: das Fundament für das Software Defined Data Center, Provider-Technologien oder eine neue Chance für Unternehmen?

*Dipl.-Math. Cornelius Höchel-Winter*
*ComConsult Research GmbH*
*Dr. Joachim Wetzlar,*
*ComConsult Beratung und Planung GmbH*

**10:30 - 10:45 Uhr Kaffeepause**
**13:00 - 14:00 Uhr Mittagspause**
**15:30 Uhr Ende der Veranstaltung**

## Frühbucherphase bis zum 31.05.2015

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

## Sommerschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

Ich buche das Intensiv-Seminar
**Sommerschule 2015**

☐ vom 22.06. - 26.06.15 in Aachen
zum Preis € 2.290,-- netto*

*Preis gültig bis zum 31.05.15 - danach 2.490,- netto. Anmeldungen innerhalb der Frühbucherphase sind verbindlich und können nicht storniert werden. Gerne akzetprieren wir aber einen Ersatzteilnehmer.

**Zur Anmeldung**
**www.comconsult-akademie.de**

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Schwerpunktthema

# IT-Sicherheit im Zeitalter der Cyberangriffe

Fortsetzung von Seite 1

Dr. Melanie Winkler ist als Beraterin bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Dort beschäftigt sie sich besonders mit Sicherheitskonzeptionen nach ISO 27001 und BSI Grundschutz und deren Umsetzung.

In diesem Artikel werden die wesentlichen der aktuell bekannten Gefährdungen dargestellt und es wird aufgezeigt, wie man sich zumindest gegen einige dieser Bedrohungen schützen kann und welche Grenzen hier aktuell bestehen.

### 1.1 Zugriff auf Daten

**1.1.1 Zugriff durch Abfangen von Daten**
In vielen Fällen durchlaufen Daten zu einem Zeitpunkt während ihrer Übertragung ein öffentliches Netz und können dann von einem Angreifer an einem Punkt der Verbindung abgefangen und ausgewertet werden. Werden die Informationen unverschlüsselt übertragen, so können diese direkt vom Angreifer abgehört oder umgeleitet, gespeichert und genutzt werden. Ein Abfangen übertragener Daten ist in allen Bereichen von Kommunikationsverbindungen möglich.

Beispielsweise werden bei jedem normalen Telefonat Daten über ein öffentliches Netz übertragen. Dabei handelt es sich hauptsächlich um Sprachdaten, welche zwischen den Teilnehmern ausgetauscht werden sollen. Bei Telefonaten werden die Sprachdaten normalerweise (zumindest auf Teilen der Gesamtübertragungsstrecke) unverschlüsselt übertragen. Das bedeutet, dass ein Angreifer, welcher die Leitung abhört oder ein Gespräch mitschneidet, dieses unmittelbar verstehen kann.

Auch für Informationen, welche über das Internet verschickt werden, ist es möglich, diese mit geeigneten Werkzeugen abzufangen. Dies ist beispielsweise gegeben, wenn per E-Mail kommuniziert wird oder im Internet Daten ausgetauscht werden. Es werden aber auch Daten übers Internet übertragen, wenn ein Mitarbeiter von außerhalb des Büros auf ein Firmennetz zugreift (VPN Zugriff) oder einen Rechner von Extern administriert (Zugriff über SSH).

Darüber hinaus kann auch auf Daten zugegriffen werden, welche lediglich auf dem System gespeichert sind, aber nicht über das Netz übertragen werden. Ein solcher Zugriff ist dann durchführbar, wenn über Schadsoftware, Sicherheitslücken oder sogenannte Backdoors auf ein System und die darauf befindlichen Daten zugegriffen werden kann. Außerdem existiert auch Schadsoftware, welche Daten des Systems direkt an einen Angreifer überträgt. Ein Beispiel für eine solche Schadsoftware ist „EquationDrug“. Mit Hilfe dieser Software können die Personen, welche die Software auf den Rechner eingeschleust haben, Daten vom Rechner abziehen. Sie können so beispielsweise Informationen darüber erhalten, was auf der Tastatur getippt wird oder welche Seiten im Browser geöffnet wurden.

Die hier beschriebenen Zugriffe auf Informationen sind jedoch bei immer weiter steigenden Datenmengen sehr mühsam. Die Größenordnung sowohl der gespeicherten Daten, als auch der übertragenen Daten steigen von Tag zu Tag. Daher sind derartige Vorgehensweisen des Abfangens sehr aufwendig und erfordern einen hohen Einsatz an Zeit und Ressourcen zur Speicherung und Auswertung der abgefangenen Daten.

**1.1.2 Gezielte Angriffe auf Systeme**
In der Vergangenheit ist es bereits vorgekommen, dass Certificate Authorities, welche die privaten SSL Schlüssel vieler bekannter Hersteller verwalten, durch externe Angreifer attackiert und dabei private Schlüssel gestohlen wurden. Somit ist jede SSL Kommunikation, welche mit den zugehörigen öffentlichen Schlüsseln kodiert wurde, ohne viel Aufwand mit den gestohlenen privaten Schlüssel in Echtzeit zu entziffern. Eine andere Methode verschlüsselte Kommunikation zu entschlüsseln benötigt Eingriffe auf die kommunizierenden Komponenten.

Angriffe auf solche Komponenten zielen beispielsweise darauf ab, die Konfigurationen der Verschlüsselung zu modifizieren. Dabei kann eine Verschlüsselungsart eingestellt werden, die der Angreifer ohne privaten Schlüssel entschlüsseln kann. Solche Modifikationen können an den Konfigurationen der E-Mail Clients, Router oder VPN-Clients vorgenommen werden. Daher gehören Benachrichtigungen und Logging im Falle von Konfigurationsänderungen an Software und Hardware zu wichtigen Sicherheitsfeatures.

Die Angriffe auf Endpunkte sind jedoch wesentlich aufwendiger als Eingriffe in die Kommunikation. Viele der bekannten Angriffe auf Endpunkte benötigen physikalischen Zugriff zum Endpunkt (z.B. USB-Stick in Laptop einschieben). Solche Angriffe können jedoch auch über Backdoors in auf dem Endpunkt installierten Programmen initiiert werden, z.B. durch böswillige E-Mail Anhänge und modifizierte Update-Pakete für das Betriebssystem oder einzelne Programme.

Eine weitere Methode gezielt auf Daten zuzugreifen ist heutzutage weit verbrei-

tet. Sie wird „Advanced Persistent Threat“ (APT) genannt. Ein APT besteht meist aus mehreren aufeinander abgestimmten Angriffsformen und verfolgt ein festumrissenes Angriffsziel (z.B. Industriespionage). Ein APT lässt sich in 5 verschiedene Phasen unterteilen:

1. Auskundschaften / Zielerfassung:
   Bevor ein erster Angriff auf das System erfolgt, informiert sich der Angreifer möglichst genau über den Aufbewahrungsort (z.B. Server, Rechenzentrum, Laufwerk, …) der Daten. Hierzu kann er sowohl auf öffentlich zugängliche Informationen zugreifen (z.B. eine unsicher konfigurierte Fehlermeldungswebseite eines Apache Servers) als auch gezielt Informationen erfragen (Social Engineering, Spear Phishing, …).

2. Eindringen und Erstinfektion:
   Nachdem der Angreifer die gesuchten Informationen grob lokalisiert hat, versucht er gezielt an diese heranzukommen. Ziel dieser Phase ist es als Vorbereitung für einen Zugriff auf die gewünschten Daten, unentdeckt in das System einzudringen. Dies erfolgt beispielsweise darüber, dass im ersten Schritt auf dem Zielsystem installierter Schadcode gezielt weitere Software auf dem System installiert. Bei dieser handelt es sich häufig um einen speziellen Trojaner, der oft ironisch als Remote Administration Tool (RAT) bezeichnet wird und welcher mit dem Command and Control Server (C&C) kommuniziert.

3. Folgeinfektion (en):
   Sollte der Angreifer nach der Erstinfektion noch nicht auf alle für ihn wünschenswerten Daten zugreifen können, dann wird er von seinem ersten Einfallstor aus weitere Systeme infizieren. Dieser Schritt ist häufig wesentlich leichter als die Phase der Erstinfektion, da die Sicherheit nach Außen bei den meisten Systemen wesentlich besser ist als die interne Sicherheit. Dieser Schritt ist auch notwendig, wenn im ersten Schritt zwar eine Infektion eines Systems im Zielnetzwerk (z.B. ein normaler PC), aber keine direkte Infektion des Zielsystems (z.B. Administrations-PC, Server…) möglich war.

4. Datendiebstahl / Sabotage:
   In dieser Phase beginnt die Übertragung interessanter Daten in großen Mengen. Bis zu dieser Phase hat der Eindringling noch keine Daten abgegriffen und keine großen Datenmengen kopiert, um nicht aufzufallen. Diese Phase birgt das größte Risiko entdeckt zu werden, da hier Anomalien in Bezug auf den Datenverkehr und die durchzuführenden Aktionen (Datenbank-Dump, Kopieren von Dateien, …) gemessen werden können. Nach Abschluss dieser Phase hat der Angreifer die gewünschten Daten abgegriffen und der Schaden ist vollständig verursacht.

5. Verwischen von Spuren:
   Sollte der Angriff nicht aufgefallen und unmittelbar blockiert worden sein, so hat der Angreifer noch die Möglichkeit Spuren zu verwischen. Hierzu gehört das Löschen von Log-Dateien, Verbindungsinformationen und des Terminalverlaufs. Außerdem löscht sich die Schadsoftware selbst oder sie löscht einen Teil von sich und wird inaktiv. Wird diese Phase ebenfalls erfolgreich abgeschlossen, so fällt es den Geschädigten wesentlich schwerer den Angreifer und das Ausmaß des Schadens zu bemessen.

#### 1.1.3 Zugriff auf rechtlichem Wege

Ein wesentlich angenehmerer und weniger aufwendigerer Weg an Informationen zu gelangen, ist mit der Unterstützung der Informationshalter. Wenn also Hersteller dazu gebracht werden können, Zugang zu ihrer Software / Firmware bereitzustellen, dann spart dies Zeit gegenüber der Informationsbeschaffung durch Angreifer. Außerdem können die Grenzen, die durch andere Beschaffungsmöglichkeiten vorhanden sind, gegebenenfalls aufgehoben werden. So muss beispielsweise bei einem Abtransport von großen Datenmengen durch die Angreifer nicht vermieden werden, dass der Datenfluss auf Ebene des Netzwerkverkehrs auffällt.

Eine Grundlage für einen solchen rechtlich legitimen Zugriff auf sensible Informationen bietet den Geheimdiensten der USA der Foreign Intelligence Surveillance Act (FISA). Dieses Gesetz regelt insbesondere Fragen zur Auslandsaufklärung und Spionageabwehr. Es beschreibt unter anderem, dass Informationen von verdächtigen Personen, die bestimmten Kriterien entsprechen, für die Regierung der Vereinigten Staaten von Amerika zugänglich gemacht werden müssen. Zu diesen Kriterien gehören beispielsweise, dass die Person kein US-Bürger ist und sich nicht auf dem Territorium der USA aufhält. Jedoch können unter bestimmten weiteren Auflagen auch US-Bürger mit dem FISA durchleuchtet werden.

Laut amerikanischer Rechtsprechung unterliegen dem FISA alle auf amerikanischem Boden agierenden Unternehmen. Hierzu gehören unter anderem Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube und Apple. Somit kann beispielsweise bei einem terroristischen Verdacht auf rechtlichem Wege Einsicht in die E-Mail-Konten von verdächtigen Personen erlangt werden.

Um solche Informationen von den betroffenen und interessanten Unternehmen zu erhalten, gab es laut den Dokumenten von Edward Snowden mehrere Treffen zwischen Regierungsvertretern (NSA, CIA, FBA, …) und Vertretern der Unternehmen (inklusive CEOs). Diese Treffen wurden unter der Enduring Security Framework (ESF) Initiative abgehalten. Dabei wurden angeblich sowohl die Art der benötigten Informationen, als auch die Übermittlungswege für Daten besprochen.

Aber nicht nur amerikanische Geheimdienste und damit auch die amerikanische Regierung können auf diesem Weg an Informationen gelangen. Durch Weitergabe können die so erlangten Informationen auch von anderen Geheimdiensten und Regierungen genutzt werden, welche mit der USA zusammenarbeiten. Laut den Dokumenten von Edward Snowden muss mindestens mit einer Weitergabe an die Geheimdienste und Regierungen verbündeter Staaten der USA gerechnet werden. Allerdings ist auch zu beachten, dass es sich hierbei um einen sehr speziellen Weg der Informationsgewinnung handelt. Auf diese Art Informationen zu erlangen können zwar einige der Geheimdienste zurückgreifen, jedoch außerhalb dieser Kreise ist dies nicht möglich. Maßnahmen zu ergreifen, welche gegen diese Art von Angriff nicht schützen können, sind daher trotzdem sinnvoll, um sich vor sonstigen Hackerangriffen zu schützen.

Die Art der Informationen, welche über diesen Weg erlangt werden können, hängen vom jeweiligen Anwendungsfall und von der ausgespähten Applikation ab. So wird in manchen Veröffentlichungen behauptet, die abgegriffenen Informationen würden sich auf Metadaten beschränken. Diese Datensätze beinhalten beispielsweise Informationen darüber, wer mit wem, wann und wie lange kommuniziert hat. Andere Veröffentlichungen beschreiben jedoch die Übertragung vollständiger Datensätze, also auch die Inhalte von E-Mails, Facebook-Profilen, Skype-Kommunikationen und Kalendereinträgen.

Die Wege über welche ein Angreifer an Informationen gelangen kann, hängen von den Applikationen und Szenarien ab. Im Folgenden geben wir einen Überblick.

### 1.2 Übertragungswege von Daten

Für die Übertagungswege von Informationen an unberechtigte Dritte gibt es unterschiedliche Möglichkeiten. Zum

einen ist eine Übertragung über bestehende Sicherheitslücken und einen darüber erfolgenden Datenabgriff möglich. Andererseits können auch Daten auf unterschiedlichen Ebenen (siehe dazu auch Abbildung 1) bewusst übertragen werden. Dies beinhaltet auch einen Vollzugriff für bestimmte Parteien auf alle Daten eines Unternehmens. Ein wissentlich (z.B. unter dem FISA) genehmigter Vollzugriff auf alle Informationen wird allerdings bisher von keinem Unternehmen zugegeben.

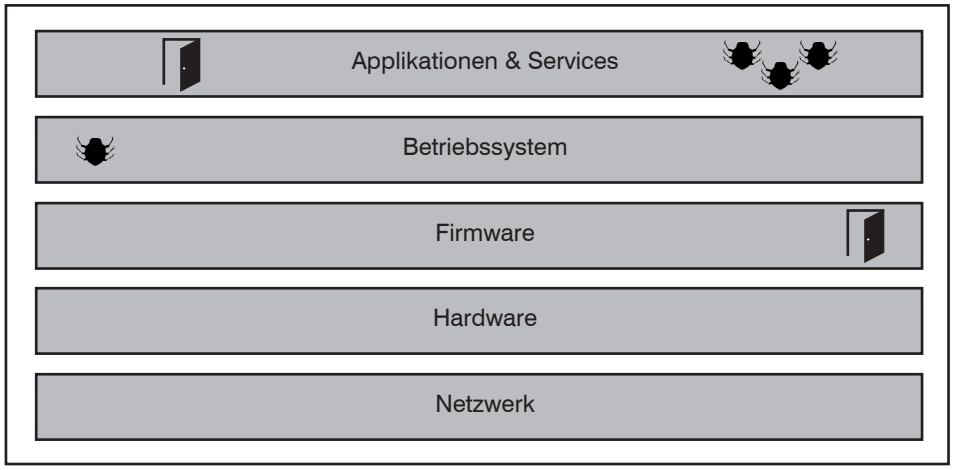


Abbildung 1: Ebenen eines IT-Systems aus der Angreiferperspektive

- **Applikationsebene**
  Auf Applikationsebene werden Datensätze aus Anwendungen wie Facebook oder Google explizit beim Unternehmen angefragt. Falls diese Anfragen akzeptiert und Daten an den Antragsteller übermittelt werden, so verwendet man für die Übergabe der Informationen dafür definierte Prozesse.

  In diesen Prozessen spielen Übergabeportale eine entscheidende Rolle. Das Unternehmen stellt die von der Regierung angefragten Datensätze in einem solchen Portal (beispielsweise eine Anwendung oder Webseite) zur Verfügung. Zugriff auf das Portal hat ausschließlich der Antragsteller (z.B. ein Regierungsvertreter). Nachdem die Daten von dem Antragsteller eingesehen (und ggf. kopiert) wurden, werden diese aus dem Portal gelöscht.

  Weitere Dokumente beschreiben eine andere Art der Informationsbeschaffung. Hierbei platzieren Regierungsvertreter unter Absprache mit den Unternehmen Personal in den Räumlichkeiten des Unternehmens mit entsprechenden Zugriffsrechten. Diese Personen können dann die Anfragen seitens der Regierung vor Ort abarbeiten.

  The Guardian beschreibt, dass die Zugriffe der NSA auf Microsoft Freemail-Dienste wie beispielsweise Outlook vor der Verschlüsselung der Inhalte geschehen. Auch auf die verschlüsselten Chats über Outlook.com hat die NSA seitens Microsoft Zugriff. Und seitdem Microsoft Skype gekauft hat, wird angeblich nicht mehr nur das Audio-Signal aufgenommen, sondern auch Video. Skype hat weltweit ca. 660 Mio. Nutzer. Daher gehen Kritiker davon aus, dass Microsoft mit Updates für seine Software und Services auch neue Instrumente ausliefert, um auch zukünftig den Anforderungen seitens Gesetzgeber gerecht werden.

  Weiterhin ist auch eine Ausnutzung von Schwachstellen auf Applikationsebene möglich. So kann ein Angreifer über Fehler in der Implementierung auf Daten zugreifen, welche von der jeweiligen Applikation verarbeitet werden. In manchen Fällen kann über Schwachstellen der Applikationen auch die Kontrolle über das zugrunde liegende System erlangt werden. Andere Applikationen des Angreifers (Schadsoftware) können auf diese Weise vom Nutzer unbemerkt installiert werden, um darüber wiederum Daten des Systems abzufangen oder auf das System selbst zuzugreifen.

  Es gibt auch Berichte über eingebaute Backdoors in kommerziellen Kryptoalgorithmen. Hierbei werden die Verschlüsselungsverfahren bewusst weniger gut umgesetzt. Häufig ist es ausreichend den Zufallszahlengenerator deterministischer zu machen als er eigentlich ist. Wenn die Anzahl der generierten Zufallszahlen überschaubar und dem Angreifer bekannt ist, dann sind Angriffe wesentlich schneller erfolgreich.

- **Betriebssystemebene**
  Eingriffe auf Betriebssystemebene erreichen nicht nur eine Anwendung oder einen Hersteller, sondern ermöglichen häufig den Zugriff auf alle Anwendungen und Daten, die auf diesem Betriebssystem (auf einem Client) installiert sind.

  Zu den wichtigsten Betriebssystemen aus der Perspektive eines Geheimdienstes (oder eines ähnlich versierten Angreifers) mit der Absicht, einen Verdächtigen zu beobachten, gehören bei den Desktopsystemen heutzutage Windows und OS X. Bei den mobilen Endgeräten sind insbesondere die Betriebssysteme Android, iOS und Windows Phone weit verbreitet. Alle Hersteller dieser Betriebssysteme (Apple, Microsoft und Google) sind den Dokumenten von Edward Snowden zufolge durch Gesetze wie FISA zur Kooperation mit den vereinigten Staaten verpflichtet.

  So ist es theoretisch möglich, dass Smartphones mit den oben erwähnten Betriebssystemen Backdoors haben oder Exploits (programmtechnische Möglichkeiten zur Manipulation von PC-Aktivitäten) erlauben, die auf Betriebssystemebene Zugriff auf die Inhalte und Kommunikation des Smartphone-Nutzers ermöglichen. Jedoch können auch Sicherheitslücken, welche unabsichtlich in einem Betriebssystem enthalten sind, Möglichkeiten für einen solchen Angriff bieten.

  Aus diesem Grund ist die Anzahl von Sicherheits-Features bei Smartphones in den vergangenen Jahren rapide gestiegen. So gehören beispielsweise Verschlüsselungen des internen und externen Speichers mittlerweile zur Standardausstattung eines Smartphones. Das iPhone 6 verschlüsselt beispielsweise seinen internen Speicher mit AES 256 Bit. Zudem wird der Schlüssel zum Entschlüsseln des Speichers bei jedem Herunterfahren des Gerätes gelöscht. Der Schlüssel kann nur durch die Eingabe der PIN wiederhergestellt werden. Zusätzlich kann der Benutzer ein Feature aktivieren, mit welchem bei 10-facher Falscheingabe der PIN der gesamte interne Speicher des iPhones gelöscht wird. Ähnliche Mechanismen kommen auch bei anderen Smartphones zum Einsatz oder sind zumindest für die Zukunft geplant.

  Diese Art der Verschlüsselung, welche vom Endbenutzer immer häufiger als Schutz vor unberechtigtem Zugriff genutzt wird, wurde in letzter Zeit schon

häufiger kritisiert. So seien beispielsweise in Fällen von Kidnapping direkte Maßnahmen, welche die Entschlüsselung eines gefundenen iPhones als Grundlage haben, nicht mehr möglich. NSA-Chef Michael Rogers hat daher laut einem Bericht der Washington Post angeregt, dass Hersteller Zugriffscodes für verschlüsselte Smartphones und Computer erstellen sollen, welche den Zugriff auf diese Geräte ermöglichen. Die Zugangscodes sollen dann in einzelnen Teilen bei unterschiedlichen Institutionen hinterlegt werden. Bei Bedarf können sich die Institutionen dann ihre Schlüssel kombinieren und auf das entsprechende Gerät zugreifen.

- **Firmware**
  Ein Eingriff auf Firmware- / Treiber-Ebene ermöglicht das Abgreifen von Informationen unabhängig vom Betriebssystem. Solche Eingriffe können sowohl über ungewollt auftretende Sicherheitslücken, als auch über bewusst eingebaute Backdoors erfolgen. So können beispielsweise Backdoors im BIOS angelegt werden, die nach einem PC-Start auf Betriebssystem- und Applikationsebene ausgenutzt werden können.

  Den Dokumenten von Edward Snowden zufolge war eine solche Backdoor im BIOS verschiedener Systeme (u.a. von Dell PowerEdge Servern) der NSA zuzuordnen. Software, um diese Backdoor im BIOS zu implementieren, wird im NSA ANT Katalog unter der Bezeichnung DEITYBOUNCE aufgeführt. Der NSA ANT (Advanced Network Technology) Katalog ist ein angebliches Dokument der NSA, welches sowohl Hardware als auch Software auflistet, mit der Spionage auf IT-Ebene betrieben werden kann. Die dort gelisteten Elemente können von der NSA selbst als auch von ausgewählten verbündeten Staaten erworben werden.

  Zu solcher Hardware gehören auch kleine Hardwarekomponenten, welche beispielsweise in Routern von Nerzwerkausrüstern implementiert werden. Laut den Snowden-Dokumenten werden hierzu Bestellungen von großen Netzwerkausrüstern gezielt abgefangen, mit entsprechenden Hardwarekomponenten ausgestattet (verwanzt) und anschließend wieder versiegelt und weiterversandt. Ein solches Vorgehen spielt sich vermutlich ohne das Wissen der Hersteller ab und scheint nicht durch Gesetze wie FISA abgedeckt zu sein.

- **Netzwerkebene**
  Daten, welche über ein Netz übertragen werden, können von einem Angreifer abgegriffen werden. Ein Angreifer kann alle Daten, welche über eine bestimmte Verbindung gesendet werden, abfangen und auf einem eigenen System speichern.

  Auf Grund der hohen Datenmenge, die heutzutage über das Internet versandt wird, ist es in der Regeln nicht praktikabel alle Informationen abzufangen und zu speichern. Bei einem Angriff auf Netzwerkebene können daher zwei Strategien verfolgt werden. Es können blind Nachrichten abgefangen und ausgewertet werden. Die Speicherung interessanter Daten erfolgt dann nach Auswertung der Daten. Diese Art des Abfangens von Informationen ist allerdings sehr mühsam und es ist nicht garantiert, dass die Informationen, welche man auf diesem Weg erhält für den Angreifer sinnvoll sind.

  Alternativ können gezielt Nachrichten abgefangen werden, welche von einem bestimmten Router aus oder an einen bestimmten Server gesandt werden, indem der Angreifer gezielt diese Verbindung abhört. Auf diese Art sind Angriffe auf bestimmte Personen (falls bekannt ist, von wo aus diese kommunizieren) oder auf bestimmte Dienste (abhören der entsprechenden Server) möglich.

  Staaten und Hackergruppen können bei Angriffen auf Kommunikationswege wesentlich mehr Daten von unterschiedlichen Quellen abfließen lassen. Diese werden zunächst in Data Centern gespeichert und bei Bedarf mit Big Data-Ansätzen analysiert. Bei solchen Angriffen sind die angreifenden Gruppen beispielsweise an den Meta-Informationen interessiert. Hieraus lässt sich ohne große Aufwände rekonstruieren, wer mit wem zu welcher Zeit kommuniziert. Allerdings ist das Abfangen von Daten auf Netzwerkebene mit sehr hohem Aufwand verbunden, da die abgefangenen Daten insbesondere gezielt nach den gewünschten Informationen durchsucht werden müssen.

### 1.3 Schutzmaßnahmen

Um die eigenen Daten bei der Aufbewahrung, Verarbeitung und Kommunikation zu schützen, kann man unterschiedliche Maßnahmen umsetzen. Einige dieser Maßnahmen und die Grundlagen zu diesen stellen wir im Folgenden vor.

#### 1.3.1 Grundlagen zur Verschlüsselung und Tor-Verbindungen

- **Verschlüsselung**
  Eine einfache Möglichkeit zur Verschlüsselung bieten symmetrische Verschlüsselungsalgorithmen. Bei der symmetrischen Verschlüsselung wird der gleiche Schlüssel zur Ver- und Entschlüsselung genutzt. Das bedeutet, dass der Schlüssel, wenn er zweimal auf den gleichen Text angewandt wird, wieder den ursprünglichen Text ergibt. Das hat jedoch den Nachteil, dass der Schlüssel auf sicherem Weg ausgetauscht werden muss, da jeder, der Kenntnis über den Schlüssels erlangt, in der Lage ist, den Text wieder zu entschlüsseln.

  In der Praxis werden häufig Verschlüsselungsalgorithmen genutzt, welche ein Public-Key-Verfahren zur Ver- und Entschlüsselung nutzen. Bei der Public-Key-Verschlüsselung (asymmetrische Verschlüsselung) hat jeder Teilnehmer einen öffentlichen Schlüssel, welchen er nach außen hin bekannt gibt, und einen privaten Schlüssel, welcher nur dem Teilnehmer selbst bekannt ist.

  Zwischen dem öffentlichen und dem privaten Schlüssel besteht ein mathe-

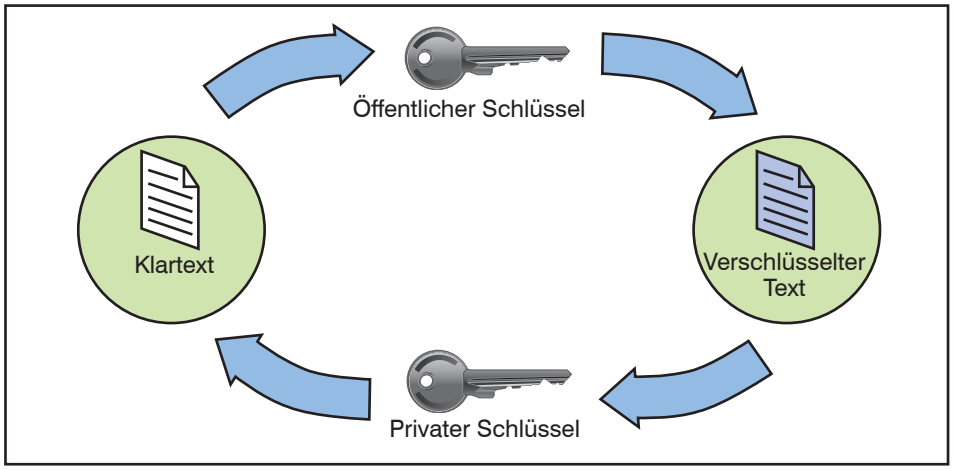


Abbildung 2: Asymmetrische Verschlüsselung

matischer Zusammenhang. Jedoch kann man, wenn man einen der beiden Schlüssel kennt, den anderen ohne Kenntnis der dahinter liegenden Formel nicht berechnen. Der öffentliche Schlüssel kann zur Verschlüsselung einer Nachricht an den Teilnehmer verwendet werden. Die Entschlüsselung ist dann nur mit dem privaten Schlüssel des Teilnehmers möglich.

Zur schnelleren Berechnung wird normalerweise nicht die ganze Kommunikation mittels asymmetrischer Verschlüsselung verschlüsselt, da die Berechnung dieser sehr langsam ist. Asymmetrische Verschlüsselung wird lediglich genutzt, um einen zufällig erzeugten symmetrischen Schlüssel zu verschlüsseln. (siehe Abbildung 2)

Voraussetzung, um die Sicherheit einer mittels asymmetrischer Verschlüsselung verschlüsselter Nachricht zu garantieren, ist allerdings, dass die Schlüssel sicher verwaltet werden.

- **Tor**
  Bei Tor handelt es sich um einen Anonymisierungsdienst, welcher Datenströme verschleiert. Bei der Nutzung von Tor wird der Datenverkehr nicht direkt vom Start zum Ziel geroutet, sondern die Route wird über zufällige Zwischenziele geroutet.

  Der Client muss dabei eine entsprechende Software installieren. Über diese Software werden verfügbare Tor-Knoten ermittelt. Sie verbindet sich dann mit einem Tor-Knoten und handelt mit diesem eine verschlüsselte Verbindung aus. Dieser Tor-Knoten wiederum handelt dann mit dem nächsten Tor-Knoten eine verschlüsselte Verbindung aus. Dies wird fortgesetzt, bis drei Zwischenserver gewählt wurden, um eine möglichst gute Anonymität zu erreichen, dabei die Übertragung aber nicht unnötig zu verzögern.

  Die Übertragung vom Client zum ersten Tor-Knoten und zwischen den Tor-Knoten erfolgt dabei verschlüsselt. Nur die Verbindung zwischen dem letzten Tor-Knoten und dem Ziel erfolgt unverschlüsselt. Es ist einem Angreifer so möglich, die Kommunikation zwischen dem letzten Tor-Knoten und dem Ziel-Server abzuhören. Allerdings ist das Netzwerk so aufgebaut, dass es einem Angreifer nicht möglich ist, die Kommunikation zum Startpunkt zurück zu verfolgen. (siehe Abbildung 3)

**1.3.2 Maßnahmen in der Praxis**

Möchte man sensible Informationen vor Angriffen schützen, so ist die sicherste Schutzmaßnahme nach wie vor ein klassischer „Air Gap“. Hierbei werden die sensiblen Informationen auf Systemen hinterlegt, welche keinen Zugriff auf das Internet haben und an kein Netzwerk angebunden sind (weder kabelgebunden noch kabellos). Komponenten zur Anbindung an ein Netzwerk sind dabei entweder gar nicht erst installiert oder deaktiviert. Der Austausch von Informationen mit diesen Systemen geschieht über externe Datenträger (z.B. USB-Sticks). Dabei werden die Daten häufig verschlüsselt zwischen den Systemen übertragen. Dies ist bis heute die einzige Maßnahme um einen Angriff auf die Daten fast vollständig auszuschließen.

In der Praxis ist ein solcher „Air Gap“ allerdings meist nicht praktikabel. Im Folgenden werden daher verschiedene Maßnahmen aufgelistet, welche zu einer erhöhten Sicherheit von Informationen beitragen können. Diese können zwar das Risiko eines Angriffs bzw. der Folgen durch einen Angriff verringern, sie bieten jedoch keinen absoluten Schutz vor Angriffen:

- **Verwendung von Anonymisierungsdiensten:** Durch die Verwendung von Anonymisierungsdiensten (wie Tor) wird der Kommunikationsdatenstrom verschleiert und bei jedem Verbindungsaufbau über ein anderes Gateway ins Internet gleitet. Somit kann der Angreifer den interessanten Datenstrom schwer identifizieren.

- **Verschlüsselung der Datenströme:** Die Datenströme sollten stets verschlüsselt sein (z.B. Verwendung von TLS und IPSec). Obwohl auch solche Datenströme gegebenenfalls entschlüsselt werden können, so ist der Aufwand doch wesentlich höher als unverschlüsselte Daten zu lesen. Je aufwendiger die Entschlüsselung von Daten ist, desto unwahrscheinlicher ist es, dass ein Angreifer diese einsehen möchte und kann. Dabei sollten so viele Datenströme verschlüsselt werden, wie möglich / sinnvoll. So gibt es beispielsweise HTTPS-Everywhere Browser Addons, welche bei Webseiten, die es sowohl verschlüsselt als auch unverschlüsselt gibt, stets den verschlüsselten Zugang wählen.

- **Nutzung von Browser in a Box:** Browser in a Box ist eine Lösung um ge-

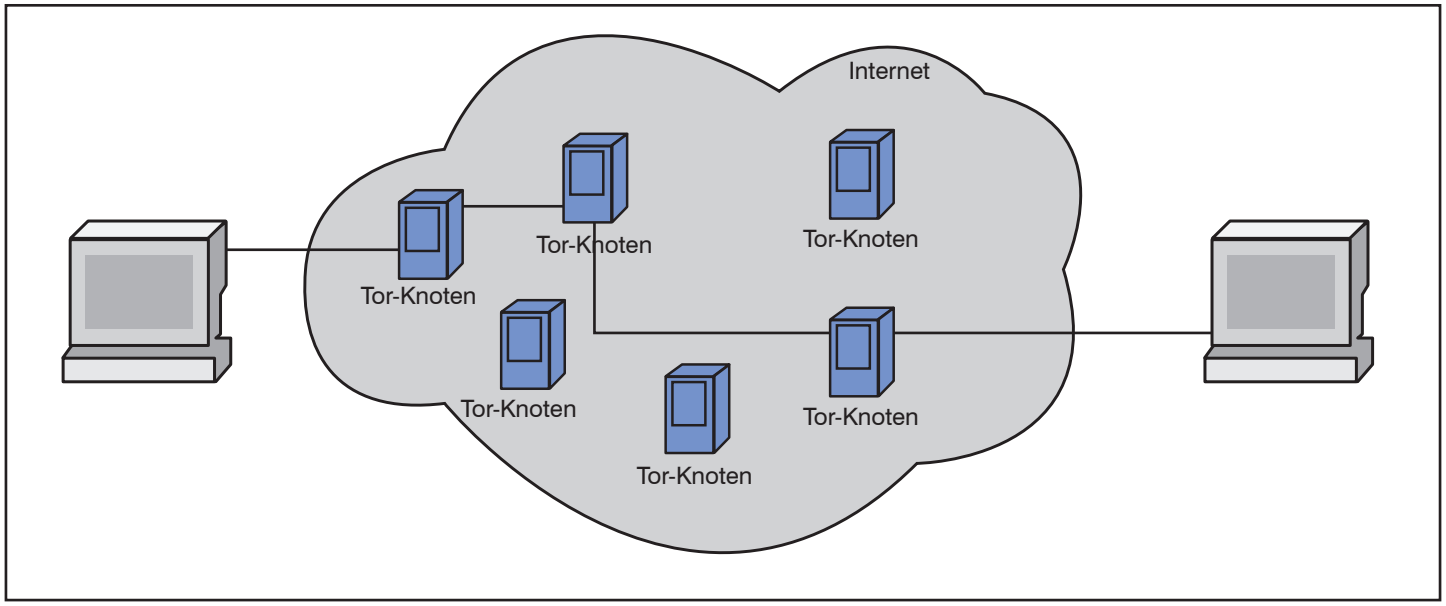


Abbildung 3: Zufällige Wahl einer Route über Tor-Knoten

schützt im Internet zu Surfen und E-Mails zu empfangen. Bei Browser in a Box Lösungen wird ein Browser auf einem reduzierten Betriebssystem in einer virtuellen Maschine gekapselt. Malware, welche beim Surfen im Internet oder durch Öffnung des Anhangs einer E-Mail auf das Betriebssystem gelangt, kann sich durch die Kapselung nicht weiter auf das Hostsystem ausbreiten. Kommuniziert das Hostsystem ausschließlich über den Bowser in a Box mit dem Internet, ist vor Angriffen durch Schadsoftware weitgehend geschützt. Das Betriebssystem, auf welchem der Browser läuft, kann bei einer Infektion jederzeit auf einen definierten Ausgangszustand zurückgesetzt werden.

Ein Beispiel für einen Browser in a Box ist BitBox, welches im Auftrag des BSI entwickelt worden ist. Hinsichtlich der Praktikabilität solcher Ansätze ist jedoch anzumerken, dass für viele Anwendungsfälle die Box für einen Datenaustausch kontrolliert geöffnet werden müsste (z.B. zur Datenübertragung an das Hostsystem), was die Sicherheit oder die Nutzbarkeit deutlich reduzieren kann oder bei entsprechend starker Reglementierung der Öffnung der Box die Nutzbarkeit der Lösung einschränkt.

- **Kritische Analyse bei der Softwarebeschaffung:** Viele Berichte deuten darauf hin, dass große Softwareunternehmen für die Regierungen der Länder, in denen sie wirtschaften, Backdoors einbauen müssen. Dies trifft sowohl für Unternehmen zu, die Betriebssysteme verkaufen als auch für solche, die Antivirenprogramme, Verschlüsselungs- und Router-Software bereitstellen. Diese Backdoors können auch von anderen Angriffsgruppen als der landeseigenen Regierung ausgenutzt werden. Wenn eine solche Backdoor bekannt wird, vertuschen viele Unternehmen dies häufig als Versehen und veröffentlichen einen entsprechenden Patch.

  Häufig kann es daher sinnvoll sein auch die Nutzung von Open Source Software zu prüfen. Da diese öffentlich entwickelt und geprüft werden kann, ist es bei dieser Art von Software deutlich unwahrscheinlicher, dass in diese Software Backdoors eingebaut worden sind.

- **Ende-zu-Ende Verschlüsselung verwenden:** Bei Kommunikation über öffentliche Netzwerke sollte stets Ende-zu-Ende Verschlüsselung verwendet werden. Es ist generell darauf zu achten, dass der private Schlüssel nur dem Eigentümer bekannt ist. Bei Ende-zu-Ende Verschlüsselung werden die Daten vom Sender der Daten verschlüsselt. Die kodierten Daten werden anschließend übertragen und können nur vom Empfänger wieder entschlüsselt werden. Es erfolgt keine Entschlüsselung der Daten auf dem Transportweg.

  Ein Beispiel für eine Ende-zu-Ende Verschlüsselung mittels Public-Key-Verfahren ist die Verschlüsselung von E-Mails mittels PGP (Pretty Good Privacy) oder S/MIME (Secure / Multipurpose Internet Mail Extensions). S/MIME wird mittlerweile von den meisten E-Mailprogrammen nativ unterstützt. Für die Verwendung von PGP ist hingegen meist die Installation eines Plug-Ins erforderlich. Kürzlich wurde bekannt gegeben, dass De-Mail PGP nun über ein Browser-Plugin nativ unterstützt.

  Da E-Mails bei der Ende-zu-Ende Verschlüsselung jedoch verschlüsselt versandt und gespeichert werden, ist es nicht mehr möglich, diese einfach auf dem Webserver zu lesen oder von einem beliebigen Endgerät abzurufen. Dies ist nur noch von Endgeräten aus möglich, welche diese Verfahren unterstützen und welchen, der der persönliche Schlüssel des Empfängers bekannt ist. Aus diesem Grund werden in der Praxis viele Mails immer noch unverschlüsselt versandt.

  Eine weitere Anwendung für die Ende-zu-Ende Verschlüsselung ist die Verschlüsselung von Telefonaten oder Textnachrichten mittels Verschlüsselungsapplikationen. Dies setzt allerdings voraus, dass beide Gesprächspartner die gleiche Applikation installiert haben. Beispiele für Applikationen zur Verschlüsselung von Telefonaten sind Red Phone (Android), Signal (iPhone) oder Cellcrypt (für unterschiedliche Betriebssysteme). Textnachrichten können über Applikationen wie Cryptochat und Red Phone ausgetauscht werden.

- **Datenspeicher verschlüsseln:** Bei einem unbefugten Zugriff auf ein System(PC, Server, Datenbanken, etc.) ist es wesentlich schwieriger Informationen zu extrahieren, wenn die dort hinterlegten Daten verschlüsselt sind. Viele Betriebssysteme, auch von mobilen Endgeräten (iOS, Android, Windows Phone, …), bieten bordeigene Mittel zur Verschlüsselung des Speichers an.

- **Angemessene Passwortrichtlinien bzw. Wahl eines angemessenen Passworts:** Um die Sicherheit eines Passwortes zu gewährleisten, sollte dieses ausreichend komplex und lang sein. Hierzu gibt es zahlreiche Richtlinien im Internet, aktuelle Empfehlungen dazu können beispielsweise auf den Internetseiten des BSI gefunden werden. Wenn das Passwort anderweitig beschafft werden kann, dann bringt diese Maßnahme keinen Schutz. Daher ist zusätzlich - soweit möglich - sicherzustellen, dass Unbefugte keinen Zugriff auf das Passwort erhalten. Die angemessene Wahl eines Passworts ist vor allem bei Dictionary und Brute Force Angriffen essentiell.

- **Zwei-Faktor-Authentisierung:** Für den Zugang zu besonders sensiblen Bereichen sollte ausschließlich eine Zwei-Faktor-Authentisierung genutzt werden. Diese besteht aus einer fixen Anmeldeinformation (z.B. ein selbst gewähl-

tes Passwort) und einer variablen Anmeldeinformation (z.B. ein temporärer Code den man zu jeder Anmeldung auf sein Smartphone erhält).

Bei vielen Diensten ist es mittlerweile möglich eine Zwei-Faktor-Authentisierung zu wählen. Diese ist jedoch normalerweise nicht standardmäßig aktiviert, sondern sie muss vom Nutzer bewusst ausgewählt werden.

- **Antivirenprogramme regelmäßig aktualisieren:** Die Installation eines Antivirenprogramms, sowie einer Firewall sollten heutzutage für jeden selbstverständlich sein. Jedoch wird stets neue Schadsoftware entwickelt, welche Angreifern die Möglichkeit bietet unbefugt auf Daten eines Systems zuzugreifen. Daher ist es notwendig, auch die Programme, die diese Schadsoftware finden und entfernen sollen, regelmäßig zu aktualisieren. Nur so ist sichergestellt, dass die Antivirensoftware aktuelle Schadsoftware auch erkennt und diese vom System entfernen kann. Nur so ist gewährleistet, dass die Angriffsfläche eines Systems möglichst gering gehalten wird.

- **Aktuelle Sicherheits-Patches installieren:** Betriebssysteme und andere Software weisen häufig Sicherheitslücken auf, welche zum Zeitpunkt der Installation noch nicht bekannt waren. Über diese Sicherheitslücken ist es möglich ein System anzugreifen und Daten des betroffenen Systems abzufangen. Angriffe über öffentlich bekannt gewordene Sicherheitslücken, für welche aber bereits Patches existieren, treten vermehrt auf. Sicherheits-Patches, welche diese Sicherheitslücken schließen, sind daher umso notwendiger, um das Angriffsrisiko zu minimieren.

- **Standardisierte Produkte verwenden:** Cyberangreifer können, indem sie sich Zugriff auf den Quellcode verschaffen, Backdoors in Software einbauen. Da der Quellcode proprietärer Software (z.B. Bitlocker) nicht öffentlich zugänglich ist, fallen Backdoors in proprietärer Software deutlich seltener auf, als in öffentlicher (bspw. TLS-Implementierungen). Daher sind Implementierungen allgemeingültiger Standards (RFCs, IEEE Standards, etc.) häufig sicherer gegen Angreifer als proprietäre Software.

- **Übergreifende Analyse und Kontrolle zur Bekämpfung von Angriffen:** Durch den Einsatz einer Plattform-, System- und anwendungsübergreifenden Analyse und Kontrolle sollen auch neuartige Cyberangriffe wie APT-Angriffe oder Zero-Day-Exploits erkannt und gezielt bekämpft werden. Hierfür kommen in Ergänzung zu herkömmlichen Sicherheitssystemen, wie Firewalls, Intrusion Prevention Systemen (d.h. Systemen zur Abwehr von Angriffen, kurz: IPS), Data Loss Prevention (d.h. Systemen, zum Schutz vor unerwünschtem Datenabfluss, kurz: DLP) und Antivirenprogrammen, Sicherheits-Intelligenzen zum Einsatz.

  Traditionell wird dieses Themengebiet durch sogenannte Security Information und Event Management (SIEM) Systeme bedient, welche eine Analyse von Sicherheitsmeldungen verschiedener Komponenten in Echtzeit auswerten. Deren weitere Entwicklungsstufe ist nun Bedrohungs- und angriffsfokussiert. Solche 2nd Generation SIEM, oder auch Next-Generation-Threat-Protection (NGTP) Systeme wenden verschiedene (auch signaturunabhängige) Analysen an, um zielgerichtete und mehrstufige Angriffe zu erkennen. NGTP verfolgen das Ziel auch Schadsoftware und Angriffe zu erkennen, welche bisher unbekannt sind und durch herkömmliche Sicherheitssysteme daher noch nicht erkannt werden können.

  Um die notwendigen Informationen für solche Intelligenzen zu sammeln, werden Endgeräte (Clients, Server) aber auch Netzwerkkomponenten (insbesondere solchen mit Firewall-Funktion) mit einer Sensorik im Sinne von Intrusion Detection Systemen (IDS) ausgestattet. So kann ggf. der Angriff schon dort festgestellt werden, wo er geschieht. Außerdem werden die so erweiterten Komponenten befähigt ein kontextuelles Bewusstsein für die Nutzer, Anwendungen, Kommunikation u.Ä. zu entwickeln. Ein Bespiel für eine solche Sensorik sind die FirePOWER Produkte von Cisco und ein Beispiel für eine NGTP-Lösung ist die Threat Analytics Platform von FireEye.

- **Nutzung von Big Data zur Angriffserkennung:** Big Data bedeutet hier die Sammlung und Auswertung großer Datenmengen mit Relevanz in der Informationssicherheit, wie beispielsweise über traditionelle SIEM ausgewertete Daten, aber auch Netzwerkverkehr, Nutzeraktivitäten uvm. Big Data wird in der Informationssicherheit zur Analyse von Merkmalen bei zielgerichteten Angriffen genutzt. Big Data Tools helfen die vorhandenen Daten effektiv auszuwerten und ermitteln Muster bzw. anderen Indizien zur Identifizierung potentieller Angriffe. Auf diese Weise können Sicherheits-Intelligenzen wie NGTP auf ein mächtiges Analysewerkzeug zurückgreifen und aus der Masse der zur Verfügung stehenden Informationen potentielle Angriffe herausfiltern. Ein Beispiel für die Anwendung von Big Data in der Informationssicherheit ist die Nutzung von Daten aus IBM InfoSphere BigInsights im IBM Security QRadar.

- **Interagierende Plattformen:** Heutige Cyberangriffe zielen in der Regel nicht nur auf eine Komponente ab, sondern erstrecken sich über verschiedene Plattformen, Ebenen und Komponenten des angegriffenen Systems. Daher sind interagierende Plattformen, welche bei einem Angriff zur Erhöhung des Schutzes Informationen austauschen und sich organisieren, eine gute Methode Angriffen entgegenzutreten.

Hierbei bekommen diverse Netzwerkkomponenten neben einer Sensorik, um z.B. aus dem Datenverkehr die Art, den Nutzer, oder die Anwendung zu erkennen und zu melden, zusätzlich die Fähigkeit auf Ereignisse zu reagieren. Falls beispielsweise eine Sicherheits-Intelligenz eine verdächtige Verhaltensanomalie in der Infrastruktur feststellt, kann sie über einen Alarm hinaus aktiv werden. Sie kann beispielsweise die Firewall kontaktieren, damit diese den Verkehr von und zur Quelle des Angriffs blockiert.

Zudem könnte über die Sicherheits-Intelligenz die NAC-Lösung (z.B. RADIUS Server) informiert werden, damit diese das Endgerät, von dem ein Angriff ausgeht (z.B. ein Endgerät, dass mit einem RAT infiziert ist), vom normalen Netz abkoppelt und in Quarantäne ausgliedert. Damit wird verhindert, dass sich ein Angriff über das betroffene System hinaus ausbreitet. Ein Beispiel für ein Produkt, was eine solche Sicherheits-Intelligenz implementiert, ist Damballa Filesafe.

- **Nutzung von Endpoint Visibility, Access, and Security (EVAS) zur Netzzugangskontrolle:** NAC-Lösungen steuern den Zugriff von Endgeräten auf ein Netzwerk. Bei traditionellen NAC-Lösungen erfolgt der Zugang von Endgeräten zum Netz gemäß der Konfiguration des gewählten Zugangspunkts, wobei der gewünschte Zugriff jedoch nur nach erfolgreicher Authentisierung erfolgen darf. Mit EVAS wird die Steuerung des Zugangs zu einem Netz erweitert. Dies geschieht mithilfe einer detaillierten, kontextuellen Prüfung gemäß betrieblicher Anforderungen, wie beispielsweise der Rolle des Anwenders, des Orts und der Zeit des Zugriffs, Forderungen der Geschäftsprozesse etc. Über eine Überwachung der übertragenen Daten und einer Anbindung an bestehende Systeme wie SIEM, Next-Generation-Threat-Protection oder andere Präventionssysteme können außerdem Angriffe auf das Netzwerk frühzeitig erkannt und unterbunden werden.

### 1.4 Grenzen des Schutzes

Es gibt Möglichkeiten die hier vorgestellten Schutzmaßnahmen zu umgehen. So kann die Verschlüsselung von Nachrichten als Unbefugter beispielsweise umgangen werden, um Nachrichten trotz Verschlüsselung zu lesen. Eine dieser Möglichkeiten ist es die Nachricht auf dem System, von welchem sie gesendet wird, vor der Verschlüsselung abzufangen und an eine eigene E-Mail-Adresse oder einen eigenen Server weiterzuleiten. Dies ist beispielsweise über das Einschleusen von eigener Schadsoftware (z.B. über RAT wie „EquationDrug“) auf Rechnern von Personen, deren Nachrichten gelesen werden sollen, möglich.

Auch gibt es bisher keinen wirksamen Schutz gegen Angriffe, welche über Backdoors in Software erfolgen, bei denen der Hersteller die Daten an Dritte freigibt. Zwar kann in manchen Fällen das Risiko einer Backdoor durch geschickte Auswahl der eigenen Software minimiert werden, jedoch ist es nicht möglich, solche Angriffe vollständig zu vermeiden.

Um solche Angriffe in Zukunft besser erkennen zu können, werden übergreifende Analysen und interagierende Plattformen benötigt. Um konsistente und mächtige Schutzmaßnahmen im Rahmen von interagierenden Plattformen und Netzwerken mit Sicherheits-Intelligenz in heterogenen Umgebungen jedoch möglich zu machen, werden diesbezüglich neue und übergreifende Standards benötigt. Diese Standards müssen von den beteiligten Plattform-Herstellern dafür genutzt werden, die Inter-Plattform Kommunikation zu erlauben. So können unterschiedliche kommerzielle Lösungen von konkurrierenden Unternehmen in einem Kunden-Setup eine lückenlose und einheitliche Sicherheitskonzeption auf Ebene der interagierenden Plattformen ermöglichen. Eine Standardisierung dieser Art fehlt jedoch heute noch häufig.

Dieses Thema könnte bauartbedingt durch Software-Defined Networks (SDN) bedient werden. Sensoren für Bedrohungserkennungen im Sinne von IDS Systemen könnten über bereits vernetzte und interagierende Systeme in SDNs eine Bedrohung frühzeitig erkennen und mehrstufige Angriffe bekämpfen. Die SDN-Gemeinde greift das Thema der Informationssicherheit aber erst seit kurzem ernsthaft auf und dies spiegelt sich daher bislang auch kaum in Produkten wieder. Neue Entwicklungen in diesem Bereich sind daher mit Spannung abzuwarten.

### 1.5 Fazit

Eine Kombination der hier vorgestellten Maßnahmen kann nicht gänzlich verhindern, dass Daten abgegriffen werden können. Jedoch werden die Hürden und das Risiko für einen Zugriff durch Angreifer deutlich höher gesetzt. Ein Angriff auf ein gut gesichertes System kostet viel Zeit und Aufwand. Nur so wird auch die Möglichkeit gegeben einen Angriff zu erkennen, nachzuverfolgen und schnell darauf zu reagieren.

Da sich die Angriffsmethoden immer wieder verändern und vielschichtiger werden, müssen das auch die Abwehrmechanismen. Traditionelle und seit langem genutzte Sicherheitsmechanismen stellen heutzutage eine wichtige Basis dar und haben trotz immer neuer Angriffsformen auch weiterhin ihre Berechtigung. Sie müssen jedoch durch auf neue Angriffsformen angepasste Maßnahmen ergänzt werden, um weiterhin einen hohen Schutz gegen Angriffe sicherzustellen. So gehören Maßnahmen zur übergreifenden Kontrolle und Überwachung beispielsweise zu den unbedingt notwendigen Best Practices, wenn stark vernetzten Angreifern mit ihren weitreichenden Überwachungsmöglichkeiten ein Netzwerk an Angriffserkennung entgegengesetzt werden soll. Bei schützenswerten Daten sollten diese daher konsequent und unternehmensweit eingesetzt werden.

Standpunkt

# Monitoring von Voice- und Video-Strömen!

Der Standpunkt von Dr. Joachim Wetzlar greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Die Übertragung von Bildern und Sprache über LAN, WAN und WLAN ist inzwischen zum Standard geworden. Wohl kaum ein Unternehmen möchte wohl noch separate Netze für derlei Zwecke betreiben. Und dennoch – oder vielleicht gerade deshalb – entstehen immer wieder Probleme bei der Bild- und Tonübertragung. Nein, ich möchte mich in diesem Standpunkt nicht (schon wieder) über Quality of Service auslassen. Stattdessen möchte ich Ihren Blick auf Überwachung und Bewertung der Übertragungs-Qualität lenken.

Der Aufhänger ist mal wieder ein Erlebnis aus der Praxis. Einer meiner Kunden überträgt nicht nur Sprache und Bilder über seine Netze, sondern im großen Stil auch Faksimile-Nachrichten als „Fax over IP“. Dafür gibt es bekanntlich verschiedene Optionen. Die Varianten, bei denen das Fax mit eigens dafür konzipierten Protokollen über das Netz gesendet wird – die Rede ist von T.37 oder T.38 – gefallen mir am besten. Diese Protokolle sind robust gegen Paketverluste und Jitter. Allerdings lässt sich Fax over IP auch mit dem Real Time Protokoll (RTP) als Pulse-Code-modulierte Töne übertragen, so wie sie aus dem Fax-Modem herauskommen. Dieses „Fax Pass-through“ hat sogar Vorteile, denn es unterstützt z.B. Fax-Übertragungen mit mehr als 14.400 Bit/s.

Der besagte Kunde klagt über einen gewissen Prozentsatz fehlgeschlagener Telefax-Sendungen. Um der Sache auf den Grund zu gehen, hat er an verschiedenen Punkten seines Netzes Monitoring-Systeme installiert. Diese Systeme greifen den Datenverkehr per Port Mirror von Switches ab, eine altbekannte und kostengünstige Methode. Und tatsächlich, die Monitoring-Systeme zeigen einen konstanten Jitter im einstelligen Millisekunden-Bereich und auch Paketverluste an.

Die Frage war nun, in welchem Teil des Netzes Jitter und Paketverluste entstehen. Ist es ein bestimmter Teil des Backbones, ist es das Weitverkehrsnetz oder die Firewall? Zu diesem Zweck habe ich

mir „Traces“ angesehen, die der Kunde mit seinen Monitoring-Systemen aufgezeichnet hatte. In den Traces waren die RTP-Paketfolgen zu erkennen. Alle RTP-Ströme, die ich untersucht habe, zeigten vergleichbare Werte für Jitter und Paketverluste. Ich konnte sogar Ereignisse entdecken, bei denen alle RTP-Ströme fast gleichzeitig deutlich erhöhten Jitter und zum Teil auch Paketverluste zeigten. Die Pausen zwischen den RTP-Paketen betrugen zum Teil das Doppelte des normalen Wertes von 20 Millisekunden, danach folgten zwei Pakete unmittelbar aufeinander. Solche Effekte treten auf, wenn Pakete in Warteschlangen von Netzkomponenten aufgehalten werden. Aber in welcher?

Moment Mal, alle RTP-Paketfolgen waren betroffen? Das ist ungewöhnlich! RTP-Ströme sind nämlich unidirektional. Wenn also das Netz irgendwo einen Flaschenhals hat, sind davon aus Sicht des Messgeräts nur die RTP-Ströme betroffen, die zunächst den Flaschenhals passieren und dann den Messpunkt. Die RTP-Ströme der Gegenrichtung kommen dagegen am Messpunkt vorbei bevor sie den Flaschenhals passieren. Diese Ströme sollten also nicht von dem Effekt betroffen sein. Sie waren es aber! Die einzige Erklärung für meine Beobachtung ist, dass der Switch, an dem das Monitoring-System angeschlossen ist, selbst die Ursache für den Effekt war. Ein Messfehler also?

Ich habe das nachzuweisen versucht. Glücklicherweise konnte ich zwischen den RTP-Paketen auch solche des Real Time Control Protocol (RTCP) entdecken. RTCP gibt den Endgeräten die Möglichkeit, ihren Kommunikationspartnern eine Qualitäts-Rückmeldung zu geben. In den so genannten Sender Reports trägt das Endgerät ein, welchen Jitter es gemessen hat und wie viele Pakete verloren gingen. In den Sender Reports steht auch, auf welche Gruppe von RTP-Paketen sich die Werte beziehen. Ich konnte also aus dem Trace die RTCP Sender Reports isolieren, die sich auf den Zeitpunkt des Effekts bezogen. Und – oh Wunder – in den Sender Reports wurden weder Paketverluste noch Jitter gemeldet. Aus Sicht der Endgeräte scheint also alles in Ordnung zu sein. Der von mir beobachtete Effekt war also offensichtlich nicht die Ursache für die fehlgeschlagenen Fax-Sendungen.

Natürlich, auch das ist kein Beweis. Wer sagt mir denn, dass die Implementierung des RTCP auf den Endgeräten korrekt funktioniert. Vielleicht senden die Endgeräte nur „Dummies“ aus. Das wäre noch nachzuweisen, bevor man die RTCP-Pakete zur Quantifizierung von Übertragungs-Problemen verwendet. Aber so viel ist klar: Trauen Sie keiner Messung, deren Aussagekraft Sie nicht selbst verifiziert haben! Anders ausgedrückt, „wer misst, misst Mist“…

Sonderveranstaltung

# Sonderveranstaltung Voice und Video im WAN

## All-IP, B2B, B2C und Daten kämpfen um die Kapazität, wie kann das beherrscht werden?

# 22.06.15 in Köln

**Die ComConsult Akademie veranstaltet am 22.06.15 ihre neue Sonderveranstaltung "Voice und Video im WAN" in Köln.**

Die Zeiten von ISDN sind fast vorbei, parallel ändert sich unsere Art zu kommunizieren. Der Anteil von Sprach- und Video-Kommunikation im WAN nimmt deshalb permanent zu und wird in den nächsten Jahren mit der starken Zunahme von All-IP, B2B und B2C alle anderen Anwendungen an den Rand drängen. Die hoch dynamische Natur der Datenströme kann zudem zu temporären

Vollbelastungen Überlastsituationen führen. Die Herausforderung besteht nun darin, gleichzeitig den Bedarf von Sprache und Video zu erfüllen und dabei die anderen Nutzer des WAN und ihre geschäftskritischen Applikationen nicht zu beeinträchtigen.

Diese Sonderveranstaltung greift dieses drängende Problem auf und analysiert:

- wie können Sprache und Video optimiert werden ohne andere Anwendungen zu gefährden
- wie gehen wir mit einem immer höheren Anteil speziell von Video in zentralen

Geschäftsprozessen und speziell auch in der Kommunikation mit Kunden um
- wie können wir die extreme Dynamik der Verkehrslasten beherrschen
- wie können wir eine ausreichende Qualität gerade in sensitiven Nutzungen für Video sicher stellen
- welche Parameter stehen uns zur Verfügung, um die notwendige Optimierung durchzuführen
- welche Dimensionierung des WAN ist in Zukunft erforderlich
- wie können Betriebsprobleme erkannt, bearbeitet und eingeschränkt werden

In dieser Analyse werden die besonderen Eigenarten der WAN-Technologien den technischen Rahmenbedingungen der Sprach- und Video-Übertragung gegenüber gestellt. Dabei werden auch die Interaktionen zwischen beiden Technologien betrachtet, um zum Beispiel mögliche Optimierung durch Call Admission Control zu untersuchen.

Sprache und Video im WAN geht immer einher mit möglichen Betriebsproblemen. Dabei entstehen typische Störmuster, die dem Betreiber bekannt sein müssen. Diese Veranstaltung diskutiert diese Störmuster, ihre Erkennung und empfehlenswerte Reaktionen. Diese Sonderveranstaltung setzt dabei folgende inhaltliche Schwerpunkte:

Basistechnologien für Weitverkehrsnetze
- Anwendungsfall Multimedia-Kommunikation
- Voice- und Video-Codecs für das WAN
- Quality of Service im WAN
- Call Admission Control
- Troubleshooting von Voice und Video im WAN
- SIP-Trunking, NGN und das WAN

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

Ich buche die Sonderveranstaltung
**Voice und Video im WAN**

☐ am 22.06.15 in Köln
zum Preis von € 990,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

vom_____ bis_____15

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

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

Zweitthema

# High Performance Storage

Fortsetzung von Seite 1

Dr.-Ing. Joachim Wetzlar ist seit mehr denn 20 Jahren Senior Consultant der ComConsult Beratung und Planung GmbH und leitet dort das Competence Center „Data Center“. Er verfügt über einen erheblichen Erfahrungsschatz im praktischen Umgang mit Netzkomponenten und Serversystemen. Seine tiefen Detailkenntnisse der Kommunikations-Protokolle und entsprechender Messtechnik haben ihn in den zurückliegenden Jahren zahlreiche komplexe Fehlersituationen erfolgreich lösen lassen. Neben seiner Tätigkeit als Trouble-Shooter führt Herr Dr. Wetzlar als Projektleiter und Senior Consultant regelmäßig Netzwerk- WLAN- und RZ-Redesigns durch. Besucher von Seminaren und Kongressen schätzen ihn als kompetenten und lebendigen Referenten mit hohem Praxisbezug.

Storage Area Networks (SANs) sind von Natur aus auf hohe Bitraten und geringe Latenz getrimmt. Insbesondere die geringe Latenz ist eine Voraussetzung dafür, dass Leitungen überhaupt mit hoher Bitrate ausgelastet werden können. Und für schnelle Datenbanken ist die Latenz gar der einzige Hemmschuh. Dementsprechend besitzen SANs im Allgemeinen eine geringe Ausdehnung mit nach Möglichkeit nur einem Layer-2-Switch zwischen Host Bus Adapter (HBA) des Servers und dem Speicherprozessor.

### Data Center Bridging

Das gilt letztlich auch für Ethernet, wenn es für Storage-Zwecke eingesetzt wird. Data Center Switches sind auf geringe Latenzen getrimmt. Das Cut Through Switching der 90er Jahre, das Pakete bereits auszusenden begann, bevor sie vollständig empfangen waren, erlebt eine Renaissance. Und außerdem verfügen Data Center Switches über Techniken, die ein „Lossless Ethernet“ ermöglichen. Denn Paketverluste dürfen in SANs nicht auftreten da den Block-basierten Protokollen die Möglichkeit der Retransmissions fehlt. Und außerdem bremsen Retransmissions die Performance gnadenlos aus. Das kennen Sie von Ihren TCP-basierten Anwendungen in ausgedehnten LANs und WANs. Fibre Channel kennt dieses Problem nicht, hier sorgen eingebaute Layer-2-Flusskontrollmechanismen (insbesondere die Buffer Credits) für Verlustfreiheit.

Über „Lossless Ethernet“ wurde in den Netzwerk-Insidern der vergangenen Jahre bereits ausführlich berichtet. Ich beschränke mich daher an dieser Stelle auf eine kurze Zusammenfassung der drei Mechanismen des Data Center Bridging (DCB).

- Congestion Notification (IEEE 802.1Qau): In einem geswitchten Netz können grundsätzlich alle Switch Ports von einer Überlast betroffen sein, wenn nämlich die entsprechende Warteschlange voll ist. Dasselbe gilt auch für die empfangende Netzwerkkarte. Solche Ports sind Congestion Points (CP) im Sinne des Standards. Der CP meldet Überlast an den Verursacher, also an die sendende Netzwerkkarte, die im Sinne des Standards der Reaction Point (RP) ist. Der RP begrenzt daraufhin die Rate des verursachenden Datenstroms.

- Priority-based Flow Control (IEEE 802.1Qbb): Hierbei wird der im Ethernet altbekannte Mechanismus des Pause Frame gem. 802.3x (oft als „Flow Control“ bezeichnet) um Prioritäten erweitert. Der Switch kann damit die Überlast verursachende Warteschlange seines Nachbarn „bremsen“. Alle übrigen Warteschlangen bleiben davon unbeeinflusst.

- Enhanced Transmission Selection (IEEE 802.1Qaz): Dabei handelt es sich sozusagen um die Spezifikation von Differentiated Services (DiffServ) auf Layer-2. Datenverkehr wird anhand der Prioritäts-Markierung im VLAN Tag in eine Verkehrsklasse eingeordnet. Die entsprechende Wartschlange wird vom Switch auf konfigurierbare Weise bedient, beispielsweise als Priority Queue oder per Rate Queuing.

### Infiniband

Während das Data Center Bridging erst in den letzten Jahren entstanden ist, gibt es Infiniband bereits seit 15 Jahren. Die Infiniband Trade Association (IBTA, http://www.infinibandta.org/) wird von den Herstellern Cray, Emulex, HP, IBM, Intel, Mellanox, Microsoft und Oracle angeführt. Sie prüft Infiniband-Produkte auf Einhaltung der Spezifikationen und auf Interoperabilität, letzteres auf halbjährlich stattfindenden „Plugfests“. Die aktuelle Liste kompatibler Produkte („Integrators‘ List“) umfasst mehr als 400 Produkte. Damit spielt die IBTA für Infiniband eine ähnliche Rolle, wie die Wi-Fi Alliance für WLAN.

Infiniband dient – wie Fibre Channel – zur Verbindung zwischen Servern („Hosts“) und ihren Peripheriegeräten. Die Adapter auf Server-Seite heißen dementsprechend Host Channel Adapter (HCA) und die auf Peripherie-Seite Target Channel Adapter (TCA). Dazwischen befindet sich eine geswitchte Fabric, wie bei Ethernet oder Fibre Channel.

Infiniband zeichnet sich durch hohe Performance und sehr geringe Latenzen aus; Round Trip Times liegen bei vielen Produkten im einstelligen Mikrosekunden-Bereich. Dementsprechend lassen sich über ein Infiniband-Netz sehr hohe Befehls-Raten (I/O Operations per Second, IOPS) erzielen. Infiniband gibt es derzeit in verschiedenen Bitraten, beginnend bei der Single Data Rate (SDR) mit 2 Gbit/s über die Double Data Rate (DDR) und Quad Data Rate (QDR) bis zur Fourteen Data Rate (FDR) mit 14,0625 Gbit/s. Eine Enhanced Data Rate (EDR) mit 25 Gbit/s und High Data Rate (HDR) mit 50 Gbit/s sind in der Entwicklung. Außerdem ist in der Infiniband-Spezifikation bereits die Link Aggregation enthalten. Im Server-Bereich eingesetzte Adapter verfügen häufig über 4 parallele „Lanes“ („4x“), leisten also 56 Gbit/s bei FDR. Für Supercomputer gibt es sogar Adapter mit 12 Lanes.

Interessant an der Infiniband Link Aggregation ist, dass die Bits eines Paketes gleichmäßig auf alle verfügbaren Lanes aufgeteilt werden. Dadurch wird die Auslastung aller Lanes immer gleich groß. Und außerdem verringert sich die Zeitdauer zur Übertragung eines Pakets. Im Gegensatz dazu verteilt die Ethernet Link Aggregation die Last pro Paket. Schaltet man also 5 mal 10 Gigabit Ethernet zu einer Link Aggregation zusammen (um etwa die FDR mit 4 Lanes zu erzielen), ist die Bitrate zwar fünfmal so hoch, das einzelne Paket wird aber nach wie vor mit 10 Gbit/s ausgesendet. Demgegenüber sendet die 4xFDR das einzelne Paket de facto mit 56 Gbit/s in einem Fünftel der Zeit aus.

Wie kommt es, dass diese eigentlich so interessante Technik erst jetzt in den Fokus der RZ-Betreiber rückt? Ganz einfach: Die Technik wird nun von der Firma Microsoft eingesetzt, um den Windows Server richtig schnell zu machen. Der Anwender braucht nun nicht mehr auf leistungsfähige „Fremdprodukte“ zurückzugreifen, um z.B. große Farmen virtueller Server zu betreiben. Das Verfahren, das dieser Technik zu Grunde liegt, ist „SMB Direct“. SMB Direct basiert auf einer Technik, die sich „Remote Direct Memory Access“ (RDMA) nennt. Und das wiederum ist eine Erweiterung des schon lange bekannten DMA. SMB Direct benötigt außerdem „SMB Multichannel“. Fangen wir also ganz langsam und von vorne an.

### Direct Memory Access

Die Von-Neumann-Architektur, auf der letztlich alle unsere Computer basieren, verfügt bekanntlich über einen zentralen Speicher für Daten und Programme. Ein Prozessor greift auf diesen Speicher zu und verwendet dafür ein Bus-System, das aus Daten und Adressbus besteht. Auch Peripheriegeräte sind an dieses gemeinsame Bus-System angeschlossen. Empfängt ein Peripheriegerät Daten, liest der Prozessor diese Daten über das Bussystem in eines seiner internen Register ein und schreibt sie anschließend über das Bus-System an sinnvoller Stelle in den Speicher. Nehmen wir an, bei dem Peripheriegerät handelte es sich um eine Netzwerkkarte. Dann setzte der Prozessor solche Lese- und Schreibvorgänge dazu ein, um beispielsweise die einzelnen Segmente eines TCP-Datenstroms zusammenzusetzen.

Es ist offensichtlich, dass das Bus-System bei derlei Ein-/Ausgabeoperationen einem Flaschenhals gleichkommt. Direct Memory Access (DMA) schafft hier Abhilfe, indem er dem Peripheriegerät die Möglichkeit gibt, Daten unmittelbar in den Speicher zu schreiben bzw. daraus zu lesen. Die Netzwerkkarte aus dem Beispiel könnte also den gesamten TCP-Datenstrom im Speicher selber zusammensetzen, ohne dass der Prozessor dafür etwas tun müsste. Erst wenn alle Daten im Speicher liegen, läse der Prozessor sie und führte sie damit der Anwendung zu.

Das Peripheriegerät übernimmt beim DMA zeitweise die Kontrolle über das Bus-System. Da der Prozessor zu bestimmten Zeiten anderweitig beschäftigt ist und nicht auf das Bus-System zugreift, lässt sich DMA so gestalten, dass der Prozessor nicht ausgebremst wird. Letztlich steigt durch DMA die Effizienz des Bus-Systems.

### Remote Direct Memory Access

Stellen Sie sich nun zwei Netzwerkkarten vor, die über eine Infiniband Fabric gekoppelt sind. Beide Netzwerkkarten greifen per DMA auf einen Speicherbereich ihres Computers zu und kopieren die Daten. Der Prozessor von Computer 1 legt Daten im RDMA-Speicherbereich der Netzwerkkarte ab. Die Netzwerkkarte im Computer 1 holt diese Daten per DMA ab und sendet sie per Infiniband an die Netzwerkkarte im Computer 2. Diese legt die Daten per DMA im Speicher ab. Von dort kann sie der Prozessor des Computers 2 weiter verarbeiten. Die Abbildung 1 illustriert dieses Prinzip.

RDMA schöpft seinen Performance-Gewinn nicht nur aus der Tatsache, dass die Netzwerkkarten per DMA auf den Speicher zugreifen – in der Tat gibt es das schon sehr lange. Mit entsprechender Unterstützung des Betriebssystems kann dank RDMA die eigentliche Datenübertragung sogar ganz ohne Mitwirkung des Protokollstacks erfolgen. Die Anwendungen auf beiden Computern kommunizieren also direkt miteinander, indem sie auf einen gemeinsamen Speicherbereich schreiben bzw. davon lesen, der mittels RDMA quasi gespiegelt wird.

In Abbildung 2 habe ich den Unterschied deutlich gemacht. Bei der herkömmlichen Kommunikation über TCP Sockets erledigt der Prozessor einen erheblichen Teil der Arbeit. Er muss die Daten der Anwendung in Segmente zerlegen und dabei die Sequenz- und Acknowledge-Nummern des TCP verwalten. Danach verpackt er die Segmente in IP-Pakete und übergibt diese dem Kartentreiber. Der ist aber auch nur ein Stück Software, das wieder vom Prozessor abgearbeitet wird. Letztlich werden die Ethernet-Pakete in Register auf der Netzwerkkarte geschrieben, die danach (ohne weiteres Zutun des Prozessors) für das Aussenden im Netz sorgt. Sicher, so genannte TCP Offload Engines erlauben die Auslagerung dieses Geschäfts auf die Netzwerkkarte. Allerdings habe ich noch keine wirklich gut funktionierende Implementierung von TCP Offloading gesehen. Zu eng ist doch die Abhängigkeit zwischen TCP Stack im Betriebssystem und TCP Stack auf der Netzwerkkarte.

Bei RDMA werden die Daten dagegen gänzlich ohne TCP kopiert. Eine Abhängigkeit zur TCP-Implementierung des Betriebssystems besteht also nicht. Die Anwendungen kommunizieren gleichsam am TCP Stack vorbei (rechte Seite der Abbildung 2). Da in diesem Fall offensichtlich die Fehlerkorrektur-Mechanismen des TCP nicht mehr wirken, muss die Fehlerfreiheit der Übertragung auf andere Weise sichergestellt werden. RDMA greift dazu auf die entsprechenden Mechanismen des Infiniband zurück. Infiniband ver-

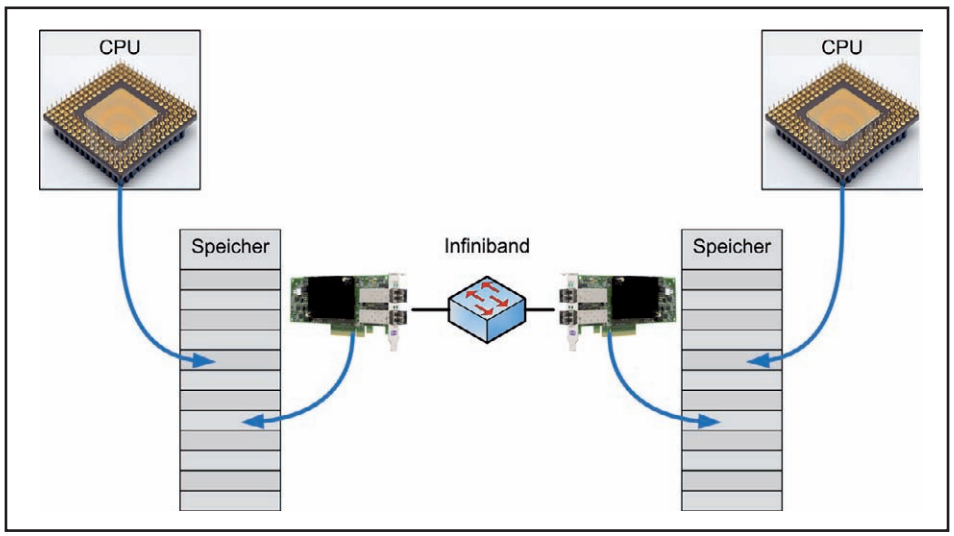


Abbildung 1: Zum Prinzip von RDMA

fügt nämlich über wirksame Flusskontroll-Mechanismen. So gibt es einerseits eine Flusskontrolle auf Layer 2 – vergleichbar zu den Buffer Credits des Fibre Channel – und andererseits eine Ende-zu-Ende Flusskontrolle zwischen den Adaptern.

### RDMA over Converged Ethernet

Eine Technik verkaufen zu wollen, die nur mit einem „Nischenprodukt“ wie Infiniband einzusetzen ist, könnte wohl als kurzsichtig bezeichnet werden. Ethernet ist nun mal der Stand der Technik, allen Nachteilen zum Trotz. Die Infiniband Trade Association hat daher RDMA auch für die Übertragung im Ethernet spezifiziert [1] und ihm dem Namen RDMA over Converged Ethernet (RoCE, gesprochen „Rocky“) gegeben. Infiniband-Pakete werden dabei einfach mit einem Ethernet MAC Header und entsprechender Prüfsumme versehen. Es handelt sich (wie bei IP) um Ethernet Frames des Typs 2. Als Typ Code wird der Wert 8915 hexadezimal verwendet.

Da sich Infiniband auf die Layer-2-Flusskontrolle seiner Fabrics verlässt, muss Ethernet für RoCE also Vergleichbares bereitstellen. RoCE kann letztlich nur mit einem Lossless Ethernet auf der Basis von Data Center Bridging (siehe oben) wirklich gut funktionieren. Interessanterweise verzichtet die Spezifikation explizit darauf, ein solches Lossless Ethernet zu fordern.

Seit einiger Zeit gibt es sogar eine Spezifikation[2] RoCEv2 zur Bereitstellung von RDMA über IP-Netze. RoCEv2 ermöglicht die Enkapsulierung der Infiniband-Pakete in UDP. Im Oktober des letzten Jahres wurde von der Internet Assigned Numbers Authority (IANA) dafür das UDP Port 4791 reserviert. Auch in IP-Netzen, insbesondere bei der Verwendung von UDP, stellt sich die Frage nach der Verlustfreiheit. RoCEv2 empfiehlt den Einsatz von Priority-based Flow Control (IEEE 802.1Qbb, siehe oben), lässt jedoch auch vergleichbare Verfahren zu. Darüber hinaus wird der Einsatz von Quality of Service (QoS) empfohlen, entweder IP-basiert oder mittels Enhanced Transmission Selection (IEEE 802.1Qaz, siehe oben). Und nicht zuletzt empfiehlt die IBTA den Einsatz von Explicit Congestion Notification (ECN) gemäß RFC 3168.

### SMB Multichannel

Der Begriff „Server Message Block“ (SMB) bezeichnet das Dateitransfer-Protokoll der Windows-Welt. Wie das entsprechende Network File System (NFS) aus der UNIX-Welt existiert SMB schon sehr lange. Microsoft hat es in den letzten Jahren immer wieder optimiert. SMB 2 – mit Windows Vista bzw. Server 2008 eingeführt – brachte ein gestrafftes Protokoll, das sich auf die Übertragung hoher Bitraten auf weiten Entfernungen fokussiert. Mit Windows 8 bzw. Server 2012 kommt nun SMB 3, das neue Features für den Einsatz im Rechenzentrum im Gepäck hat. Eines dieser Features ist „SMB Multichannel“.

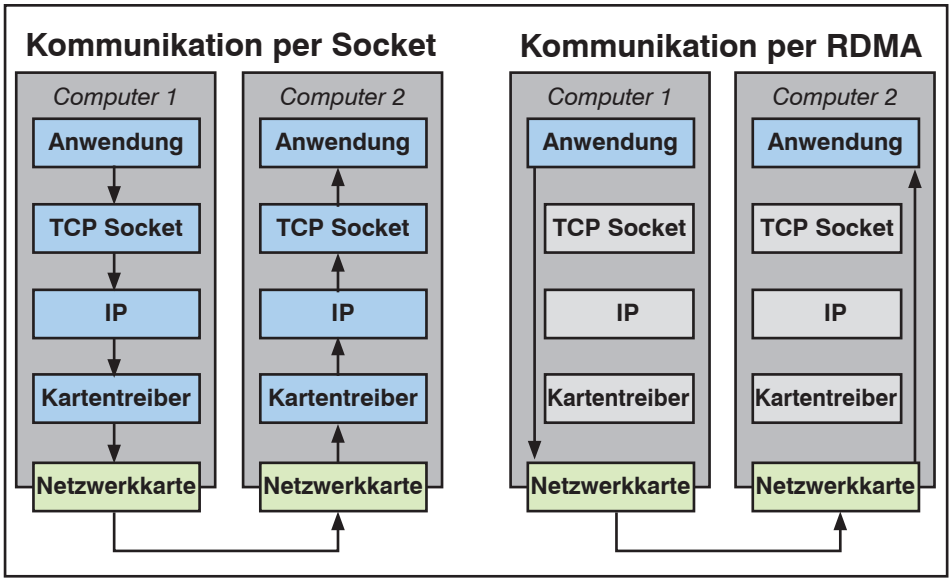


Abbildung 2: Anwendungs-Kommunikation ohne und mit RDMA

Die Idee hinter SMB Multichannel ist, einen Ersatz für die meist proprietären Techniken des Adapter Teaming zu bieten. Eine Freigabe (Share) auf einem SMB Server kann dank SMB Multichannel über mehrere Zieladressen erreicht werden. SMB Server werden dazu mit mehreren Netzwerkkarten ausgestattet, die sich in unterschiedlichen IP-Subnetzen befinden. Gleiches gilt auch für die SMB Clients. Typischerweise handelt es sich bei diesen „Clients“ um andere Server, die auf die File Server zugreifen, wie beispielsweise Datenbanken oder Virtualisierungs-Hosts. Der SMB Client kann jetzt mehrere TCP Sessions zum Server aufbauen und seine Zugriffe auf die Sessions verteilen. SMB Multichannel funktioniert sogar auf einzelnen Netzwerkkarten, wenn diese das so genannte Receive Side Scaling (RSS) unterstützen. In diesem Fall werden bis zu vier parallele TCP Sessions zu einer entsprechenden Netzwerkkarte im SMB Server aufgebaut. Der Geschwindigkeitsgewinn resultiert daraus, dass die TCP Sessions von unterschiedlichen Prozessorkernen verarbeitet werden können.

### SMB Direct

Setzt man im SMB Server und Client Netzwerkkarten ein, die RDMA bzw. RoCE unterstützen, kann SMB Multichannel in einer besonderen Spielart wirken: Zunächst baut der SMB Client per TCP die Verbindung zum SMB Server auf. Danach etablieren SMB Client und Server eine RDMA-Verbindung. Infolgedessen werden alle SMB-Befehle per RDMA übertragen, wodurch sich wegen der verringerten Laufzeit die Performance gegenüber der TCP/IP-basierten Verbindung erhöht. Das ist in Abbildung 3 skizziert. SMB Multicannel bezieht sich bei SMB Direct auf die Parallelität von TCP-Verbindung und RDMA. SMB Direct ist ohne SMB Multicannel nicht denkbar. Selbstverständlich lassen sich dafür beliebige RDMA-fähige Netzwerkkarten einsetzen, also Infiniband oder Ethernet mit RoCE bzw. RoCEv2.
Wer wird nun die bis hierher beschriebene

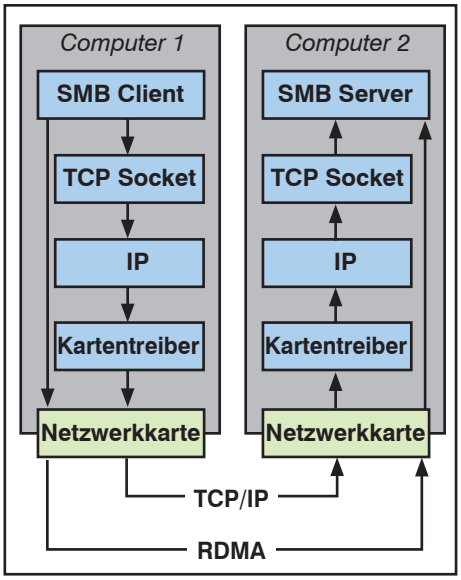


Abbildung 3: Zur Wirkungsweise von SMB Direct

Technik einsetzen wollen? Denn immerhin muss die hohe Performance mit entsprechenden Investitionen erkauft werden. Man benötigt RDMA-fähige Netzwerkkarten und eine dementsprechende Fabric, also Infiniband oder Ethernet mit Data Center Bridging. Microsoft hat hier insbesondere seine eigene Virtualisierungs-Lösung Hyper-V im Visier. Unzählige Virtuelle Maschinen laufen in großen Hyper-V-Clustern und benötigen entsprechende Performance auch im Backend Storage. Mehr noch, es wird eine Speicher-Virtualisierung benötigt, die einem virtuellen Server „seinen" Speicher bereitstellt, unabhängig vom physischen Ort, an dem der virtuelle Server gerade läuft. Verschiebt man den virtuellen Server auf einen anderen Hyper-V Host, so muss insbesondere der Data Store (also die VHDX-Datei) dort verfügbar sein, ohne langwierig Gigabytes Daten verschieben zu müssen. Hierfür bietet SMB eine ideale Plattform. Jeder Hyper-V Host eines Clusters sieht dieselben SMB Shares. Die SMB Server müssen zu diesem Zweck höchst performant und skalierbar sein.

### Microsoft Scale Out File Server

Dementsprechend heißt das neue Produkt „Scale Out File Server" (SOFS). Genau genommen handelt es sich dabei um eine zusätzliche Server-Rolle des Windows Server 2012 R2. Die Idee des SOFS ist einfach: Mehrere SMB Server stellen parallel dieselben Shares bereit. Zu diesem Zweck teilen sie sich dieselben Festplatten in einem „Shared Storage". Das können herkömmliche logische Laufwerke (Logical Units, LUNs) in einem Fibre Channel SAN sein. Das können aber auch Festplatten mit Serial Attached SCSI (SAS) in preiswerten Disk Shelves sein, die man gerne als „Just a Bunch of Disks" (JBOD) bezeichnet. Bis zu 8 Server lassen sich auf diese Weise zu einem SOFS kombinieren.

Stattet man alle Server mit RDMA-fähigen Netzwerkkarten aus, ist für die hohe Performance gesorgt. Die Hyper-V Hosts können dann SMB Direct nutzen. Baut man darüber hinaus zwei unabhängige Ethernet- bzw. IP-Netze auf (vgl. Abbildung 4), wird dank SMB Multichannel die erforderliche Verfügbarkeit auch bei Netzwerk-Störungen oder Adapter-Fehlern sichergestellt.

### Zusammenfassung

Remote Direct Memory Access (RDMA) über Infiniband und dessen Ethernet-basierende Variante RoCE sind Techniken, die hohe Bitraten mit geringen Latenzen miteinander verbinden. Diese Techniken erfahren nun Unterstützung durch die aktuellen Server-Produkte von Microsoft.

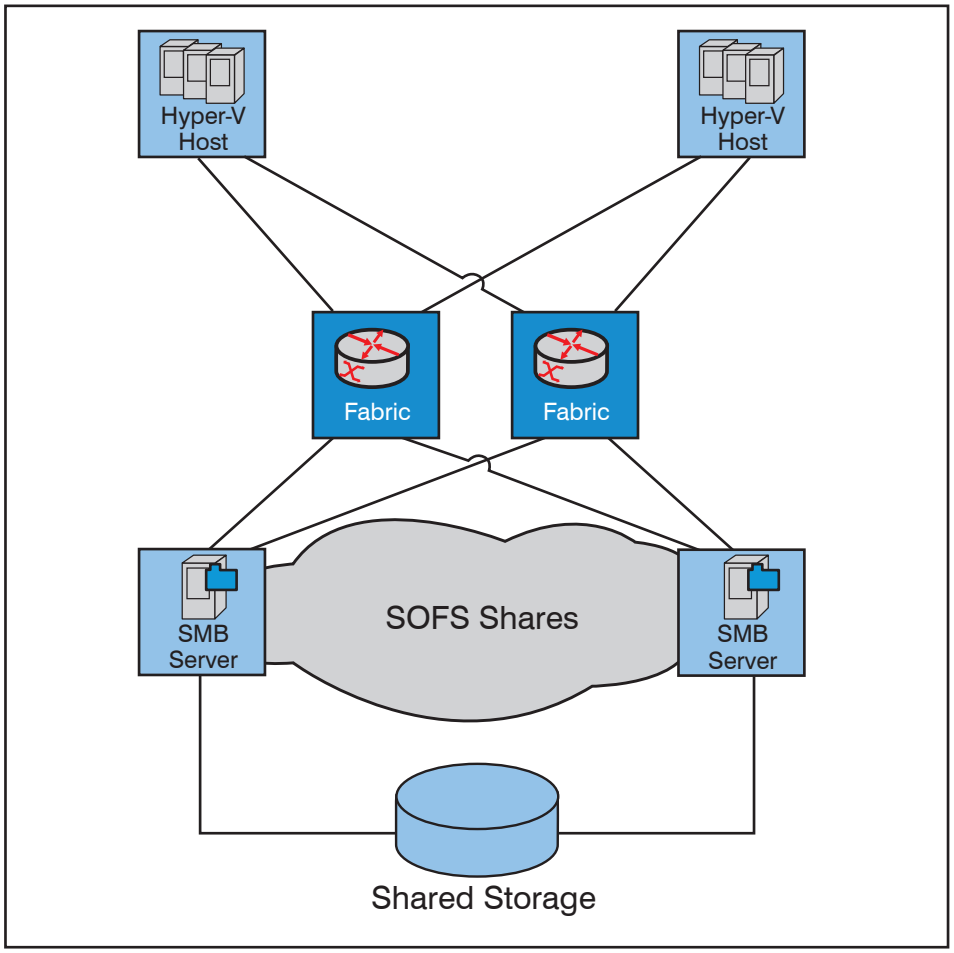


Abbildung 4: Scale Out File Server (SOFS)

SMB Multichannel und SMB Direct bieten einerseits höhere Performance als mit den herkömmlichen TCP/IP-basierten Zugriffen erreicht werden kann. Andererseits wird hohe Verfügbarkeit durch Redundanzmechanismen erzielt, die unabhängig von speziellen Techniken der Switch- und Adapter-Hersteller sind (sieht man einmal von RDMA ab, das natürlich eine „spezielle Technik" der Adapter-Hersteller ist).

Microsoft kombiniert diese Techniken zu einem neuen Produkt, dem Scale Out File Server (SOFS) als Teil von Windows Ser-

ver 2012 R2. Mit dem SOFS bekommt der Kunde eine Lösung zur Realisierung performanten virtuellen Speichers, der insbesondere im Zusammenhang mit der Server-Virtualisierung (Hyper-V) Vorteile bietet. Im SOFS mutiert der Windows Server quasi zu einem Storage Controller.

Letztlich versucht Microsoft mit dem SOFS in den Markt der Speicher-Systeme vorzudringen und den „Platzhirschen" der Branche Marktanteile abzunehmen. Für den Kunden ist damit die Hoffnung verbunden, zukünftig ein performantes Speichersystem preiswerter aufbauen zu können als es heute mit Fibre Channel SANs oder speziellen NAS Clustern möglich ist.

**Ausblick**

Wie oben bereits angedeutet, könnte die einstige Nischentechnologie Infiniband dank der Unterstützung von RDMA durch Microsoft eine gewisse Renaissance erleben. Jedoch funktioniert ein Infiniband HCA im Grunde nicht anders als eine Ethernet-Karte oder ein Fibre Channel HBA. Auf dem Adapter befindet sich ein Controller, der auf der einen Seite das entsprechende Protokoll bedient. Der Controller ist also dazu in der Lage, die Daten zu Paketen zusammenzuschnüren und mit den erforderlichen Header-Informationen zu versehen. Auf der anderen Seite verfügt dieser Controller über eine Schnittstelle zum Computer, in den der Adapter hineingesteckt wurde. Das ist heute im Allgemeinen der „Peripheral Component Interconnect Express", kurz PCIe.

Was ist PCIe eigentlich? Wie wir weiter oben gesehen haben, ist er die Verbindung an das Bus-System des Computers. Es lassen sich also Speicherstellen adressieren (Adressbus) und Daten von diesen Speicherstellen lesen bzw. darauf schreiben (Datenbus). Außerdem hat das Bus-System einige zusätzliche Funktionen wie die Möglichkeit Interrupts zu generieren oder eben DMA-Zugriff zu initiieren.

Frühe Bus-Systeme hatten für jeden der genannten Zwecke eigene Leitungen. Ein 32-Bit-Datenbus brauchte also 32 Drähte. Beim PCIe hat man sich stattdessen für eine serielle Übertragung entschieden. Adressen und Daten werden nacheinander übertragen und in Paketen zusammengefasst. Auch Interrupts und alle anderen Funktionen sind beim PCIe spezielle Pakete. Übertragen werden die Pakete mit vorgegebener Bitrate über Leitungen, die nun „Lanes" genannt werden. Bis zu 16 Lanes lassen sich über PCIe parallel bedienen, je nachdem wie die Steckplätze ausgestattet sind. Beim PCIe in der Version 4.0 leistet jede Lane 2 GByte/s, umgerechnet also 16 Gbit/s. Ein voll ausgestatteter Steckplatz schafft also sagenhafte 256 Gbit/s.

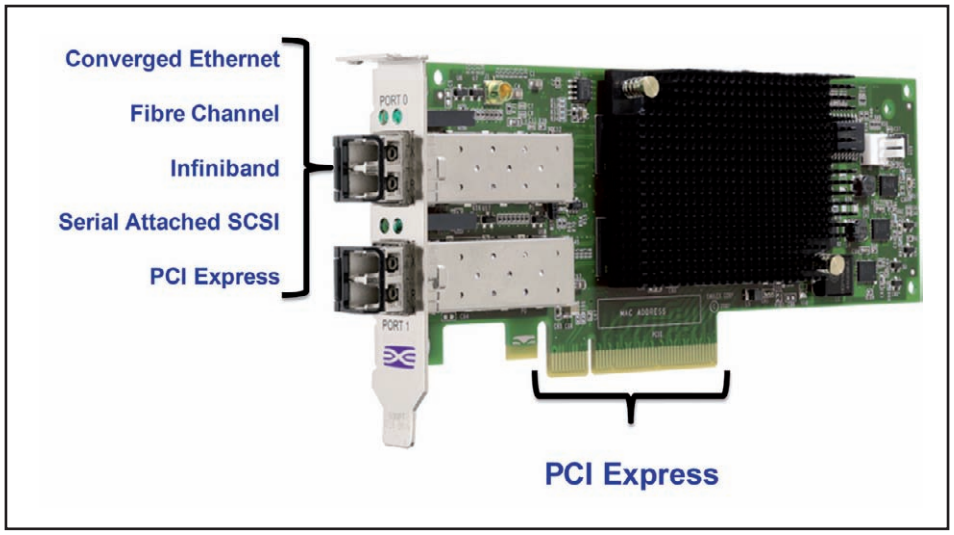


Abbildung 5: Schnittstellen eines Server-Adapters

Die Lanes der PCIe-Steckplätze werden im Computer über spezielle Bausteine mit den übrigen Komponenten verbunden, insbesondere also mit Prozessor und Speicher. Bei diesen Bausteinen – als „Southbridge" und „Northbridge" bezeichnet – handelt es sich genau genommen um Switches. Nur vermitteln diese nicht Ethernet oder Fibre Channel Frames sondern PCIe-Pakete. Was läge also näher als das Verlängern der PCIe Lanes aus dem Computer hinaus, etwa über Glasfasern. Verbände man auf diese Weise zwei Computer miteinander, ließen sich Speicher und Peripherie beider Computer direkt adressieren. Ein Prozessor wäre dann in der Lage, Speicher auf dem anderen Computer direkt zu beschreiben. Im Vergleich zu RDMA hätte man noch einmal Rechenzeit eingespart.

In der Tat hat man bereits in 2011 eine PCIe-Übertagung per Glasfaser demonstriert, immerhin mit 64 Gbit/s. Und auch erste PCIe Switches sind bereits gesichtet worden. Es bleibt abzuwarten, ob eines Tages einer der großen Hersteller diese Technik unterstützt und damit der Marktakzeptanz eine Chance gibt.

**Verweise**

[1] Spezifikation von RoCE:
**https://cw.infinibandta.org/document/dl/7148**

[2] Spezifikation von RoCEv2:
**https://cw.infinibandta.org/document/dl/7781**

ComConsult Veranstaltungskalender

## Lokale Netze für Einsteiger, 18.05. - 22.05.15 in Aachen

Garantietermin

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- netto

## Netzwerk-Design für Enterprise Netzwerke, 18.05. - 19.05.15 in Köln

Garantietermin

LAN-Technik wird im Moment neu erfunden. Neue Anforderungen erfordern neue Lösungen. Neue Fabric-Konzepte, ein Umdenken bei VLAN-Technik, eine Neupositionierung von QoS und neue Nutzungsformen im Rahmen von Audio-/Video-Bridging sind herausragende Beispiele. Das Seminar zum Thema Netzwerk-Design für Enterprise Netzwerke erklärt, was im Moment passiert und wie Sie sich auf die Zukunft vorbereiten. Es geht auf RZ- und Campus Design-Alternativen im Zeitalter neuer Layer-2 Technologien wie Fabrics, Multichassis-Link Aggregierung, Shortest Path Bridging und Hochgeschwindigkeits-Datenraten von 10/40/100 Gbit ein. Darüber hinaus werden Priorisierungs-Techniken wie AVB und DCB sowie der sinnfällige Einsatz von VLAN-Technik und VLAN-Overlays behandelt. Preis: € 1.590,-- netto

## Interne Absicherung der IT-Infrastruktur, 08.06. - 09.06.15 in Stuttgart

Garantietermin

In diesem Seminar lernen Sie wie man die Sicherheit von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN erreicht. Konkrete Beispiele aus der Praxis zeigen den Weg zu einer erfolgreichen IT-Sicherheits-Lösung.

Preis: € 1.590,-- netto

## Wireless LAN professionell, 08.06. - 10.06.15 in Stuttgart

Lernen Sie in diesem Seminar wie Sie eine WLAN-Lösung zukunftsorientiert und investitionssicher für die verschiedensten Endgerätetypen und Dichten aufbauen. Lernen Sie wie Sie Verfügbarkeit und Bandbreite optimieren. Verbessern Sie Ihr WLAN mit den verschiedensten Struktur-Elementen vom Access-Point bis zum WLAN-Controller. Erfahren Sie worin sich Produkte und Technologien führender Anbieter unterscheiden. Berücksichtigen Sie die neusten Entwicklungen zur Gestaltung einer WLAN-Lösung, die langfristig tragfähig und wirtschaftlich ist. Lernen Sie Vor- und Nachteile aller aktuellen Technologien kennen und vermeiden Sie Planungs-Fehler.

Preis: € 1.890,-- netto

## Internetworking: optimales Netzwerk-Design mit Switching und Routing, 08.06. - 12.06.15 in Aachen

Dieses Seminar vermittelt alles Wichtige, was Sie zum Thema LAN wissen müssen. Es werden unterschiedlichen Einsatzszenarien für Routing und Switching beleuchtet und das notwendige Wissen zur erfolgreichen Planung und dem Betrieb von Netzwerk Infrastrukturen vermittelt. Die Abdeckung der Themen erstreckt sich über Layer 2 Redundanzverfahren, Routing und Tunneltechnologien, sowie Netwerkmanagement Fragen. Einen weiteren Schwerpunkt bildet das Kapitel Office Network. Hier werden der Aufbau und die Integration von WLAN Strukturen detailliert beleuchtet. Abgerundet werden diese Informationen durch verschiedene praktische Übungen und einen Blick auf die aktuelle Markt- und Produktsituation der führenden Hersteller von Netzwerk-Komponenten.

Preis: € 2.490,-- netto

## Umfassende Absicherung von Voice over IP und Unified Communications, 08.06. - 10.06.15 in Stuttgart

Garantietermin

Dieses Seminar zeigt die Risiken beim Einsatz von Voice over IP und Unified Communications auf und gibt den Teilnehmern einen Überblick über die zu ergreifenden Sicherheitsmaßnahmen. Auf Grundlage von Best Practices aus dem Beratungsgeschäft sowie den marktrelevanten Standards, wie z.B. der „Technischen Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ (TLSTK II) des BSI, werden den Teilnehmern die Anforderungen an eine Sicherheitskonzeption für TK und UC vermittelt. Das Seminar richtet sich vorrangig an Sicherheitsverantwortliche, Planer, Architekten und Betreiber von TK- und UC-Systemen.

Preis: € 1.890,-- netto

## Trouble Shooting für Netzwerk-Anwendungen, 09.06. - 12.06.15 in Aachen

Garantietermin

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzten 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: € 2.290,-- netto

## RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 15.06.15 in Stuttgart

Rechenzentren in entfernten Standorten zu betreiben erfordert sich mit IT-Sicherheit, Desaster Recovery, Service Level Agreements und Hochverfügbarkeit auseinander zu setzen. Dabei sind zum Teil Vorgaben bspw. vom BSI zu beachten. In dieser Schulung werden die aktuellen Techniken erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 990,-- netto

## Das mobile Unternehmen, 15.06.15 - 16.06.15 in Stuttgart

Dieses 2-tägige Seminar gibt Ihnen einen umfassenden Überblick über Einsatzmöglichkeiten, Risiken und Chancen sowie Anforderungen und Auswirkungen mobiler Technologien im Unternehmen. Es werden die grundlegenden Veränderungen in Arbeitsweise und Arbeitsausstattung aufgezeigt, die die steigende Mobilität mit sich bringt und die Auswirkungen auf den IT-Betrieb, die Infrastruktur und das Management von mobilen Geräten diskutiert. Zum einen werden mögliche Gefährdungen aufgezeigt, die durch die zunehmende Konsumerisierung und den damit verbundenen Anstieg von privat genutzten Geräten entstehen. Zum anderen werden aber auch Möglichkeiten und Chancen, die mobile Applikationen und die lückenlose Vernetzung im „Internet of Things“ bieten, erläutert.

Preis: € 1.590,-- netto

Zertifizierungen

## ComConsult Certified Network Engineer

**Lokale Netze**
**18.05. - 22.05.15 in Aachen**
**28.09. - 02.10.15 in Aachen**

**TCP/IP-Netze erfolgreich betreiben**
**15.06. - 17.06.15 in Nürnberg**
**11.11. - 13.11.15 in Bonn**

**Internetworking**
**08.06. - 12.06.15 in Aachen**
**19.10. - 23.10.15 in Aachen**

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

## ComConsult Certified Trouble Shooter

**Trouble Shooting in vernetzten Infrastrukturen**
**27.10. - 30.10.15 in Aachen**

**Trouble Shooting für Netzwerk-Anwendungen**
**09.06. - 12.06.15 in Aachen**
**17.11. - 20.11.15 in Aachen**

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

## ComConsult Certified Voice Engineer

**IP-Telefonie und Unified Communications erfolgreich planen und umsetzen**
**28.09. - 30.09.15 in Köln**

**Session Initiation Protocol Basis-Technologie der IP-Telefonie**
**15.06. - 17.06.15 in Nürnberg**
**11.11. - 13.11.15 in Bonn**

**Umfassende Absicherung von Voice over IP und Unified Communications**
**08.06. - 10.06.15 in Stuttgart**
**19.10. - 21.10.15 in Bonn**

**Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter**
**14.09. - 15.09.15 in Bonn**

Wir empfehlen die Teilnahme an diesem Seminar **"IP-Wissen für TK-Mitarbeiter"** all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 5.100,-- netto statt € 5.670,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

Verlag:
ComConsult Research Ltd.
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