ComConsult Netzwerk Forum

ComConsult Akademie

Programmübersicht

Montag 25.03.19

Vision

9:30 Uhr

Die Top-Trends der IT: was müssen Netzwerke in 5 Jahren leisten

- Welche Endpunkte müsse in Zukunft vernetzt werden
- Applikationen und ihre Infrastrukturen: wohin geht der Trend
- Das Rechenzentrum und seine Position in der IT der Zukunft
- Die technische und juristisch sinnvolle Positionierung der Cloud
- Resultierende Anforderungen an die Planung und den Betrieb von Netzwerken

Dr. Jürgen Suppan, ComConsult Research GmbH

10:30 Uhr Kaffeepause

11:00 Uhr

Gebäude-Automation und die Auswirkung auf IT-Infrastrukturen

- Was bedeutet Gebäude-Automation? Welche Gewerke sind betroffen?
- Typische Projektbeispiele und Erkenntnisse daraus
- Welche Infrastrukturen werden benötigt und wer plant die?
- Wie verändert sich dadurch die Schnittstelle zwischen IT und TGA?
- Netzwerke und Sicherheit müssen neu positioniert werden

Dipl.-Inform. Thomas Steil, ComConsult Beratung und Planung GmbH

11:45 Uhr

Künstliche Intelligenz und ihr Einfluss auf unsere Arbeit

- Was ist künstliche Intelligenz?
- Welche Anwendungsfälle ergeben sich?
- Welchen Mehrwert kann KI schaffen?
- Welche Produkte gibt es bereits?

Dipl.-Ing. Nils Wantia, ComConsult Beratung und Planung GmbH

12:30 Uhr Mittagspause

Campus/Edge

14:00 Uhr

Overlays und der Vorsatz im Netzwerk

- Grundlagen der Overlays und Fabrics im Campus
- Absicht und Vorsatz als nächsten Schritt im Netzwerk
- Das Netzwerk als Business-Case?

Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

14:45 Uhr

Planung der Datenverkabelung mit BIM

- BIM, was ist das? Warum braucht man das und wer braucht es?
- Konsequenzen für die Planung: Alles wird anders!
- Praxiserfahrungen
- Schwieriges und Nachdenkliches

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

10:30 Uhr Kaffeepause

16:00 Uhr

Das neue Smart OmniEdge von Extreme

- Wie bekommen wir den Edge sicherer?
- Wie bekommen wir den Edge intelligenter?
- Wie bekommen wir den Edge flexibler?

Dipl.-Ing. Olaf Hagemann, Extreme Networks GmbH

16:45 Uhr

Fluch und Segen der Künstlichen Intelligenz für die Informationssicherheit

- KI zur Erkennung von Malware, Spam- und Phishing-Mails und Angriffsmustern in Netzwerken
- KI zur automatisierten Klassifikation von Daten für Data LossPrevention (DLP)
- KI zur Schwachstellenanalyse und zur Fehlersuche in Diensten und Anwendungen mit Code-Analysen und Blackbox-Tests auf Schnittstellenbasis
- Kehrseite der Medaille: KI als Angriffswerkzeuge
- Systematische Ausnutzung von Fehlern in einer KI und Provokation von Fehlentscheidungen einer KI
- Notwendigkeit von Sicherheitskonzepten für KI

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Dienstag 26.03.19

9:00 Uhr

Software Defined Access (SDA) – Wie gehen wir mir den Massen an Endegeräten um – so geht die Lösung!

- Installation, Austausch und Umzug von Endgeräten
- Nutzer zu Applikation, was ist wichtig, wie kann man Fehlerquellen minimieren
- Mehr als nur PC, Laptop und Drucker – IoT Geräte wie zB LEDs
- Wie löst man mit DNA Center mit SDA das Problem der Automatisierung

Markus Harbeck, Cisco Systems GmbH

Cloud

9:45 Uhr

Aufbau und Anforderungen hochskalierbarer Cloud-Anwendungen an das Netzdesign

- Welche Anforderungen haben Clients an die Cloud? Gibt es einen Unterschied zwischen den Anforderungen von IoT-Geräten und GUIs an die Kommunikations- und Serverinfrastruktur?
- Immer mehr User und Geräte greifen auf Cloudanwendungen zu: wie werden hochskalierbare Anwendung in der Cloud realisiert? Autoscaling vs. Container vs. Serverless Architecture
- Welche Anforderungen haben die verschiedenen Varianten an das Design in Bezug auf Georedundanz und weltweiter Verfügbarkeit
- Wie können Cloudanwendungen durch Netzwerkfunktionen abgesichert werden?

Markus Schaub, ComConsult-Study.tv

10:30 Uhr Kaffeepause

11:00 Uhr

Der Weg in die Cloud

- Ein Cloud Starter Kit
- Basiskomponenten und Auswahlkriterien von SaaS (Dokumentenkollaboration)
- Welche Rolle spielt Office 365?

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

11:45 Uhr

SIP Trunk & UCaaS Connect

- Welche WAN Optionen gibt es? Welche technischen Bedingungen müssen eingehalten werden? Ist QoS im WAN noch wichtig? • 4G/5G Backup Option
- Internet Telefonie als Standard?

Markus Geller, ComConsult Research GmbH

12:30 Uhr Mittagspause

14:00 Uhr

Sicherer Zugang zu externen Cloud

- Differenzierung zwischen verschiedenen Cloud-Typen
- Zugang zu SaaS anhand des Beispiels Office 365
- Sicherer Cloud-Zugriff: On-premise Proxies versus Web Security Cloud •SD-WAN • Netzzugang zur Cloud: Internet vs. dedizierte Verbindungen • Auswirkungen von IaaS und SaaS auf die unternehmensinterne IT-Infrastruktur • Netz- und Security-Design in der Cloud

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

14:45 Uhr

Einführung von Cloud-Proxies am Beispiel von Zscaler

- Motivation für den Einsatz von Sicherheitskomponenten aus der Cloud
- Anbindung von lokalen Infrastrukturen und Nutzung von Anwendungen im Internet, insb. Office 365
- Praxisdemo

Friedrich Eltester, ComConsult Beratung und Planung GmbH

15:30 Uhr Kaffeepause

Wireless

16:00 Uhr

5G: Anwendungsbereiche, Standards, Technologie, Einführung

- Erweiterter Mobilfunk, Massives IoT, Missionskritische Anwendungen • Grundsätzliche Technologien fortgeschrittener drahtloser Systeme
- Die Software-basierte Gesamtarchitektur von 5G
- 5G New Radio: die Vielfalt der Funkschnittstellen
- 5G und Zellentechnologien
- 5G Feldversuche, Chiptechnologie, Einführung

Dr. Franz-Joachim Kauffels, unabhängiger Technologie-Analyst

16:45 Uhr

Quo vadis Wireless-LAN?

- Cloud-Managed WLAN/SD-WLAN oder noch Wireless LAN Controller?
- Hat 802.11ac (Wave 1 and Wave 2) geliefert, was erwartet wurde?
- Erweiterung des Spektrums bis 6 GHz, was geschieht in den USA und was in Europa, bzw. Deutschland?
- 802.11ax und 5G; wo sind sie gleich und was macht sie einzigartig?
- Friedliche Koexistenz multipler drahtloser Lösungen

Jan Buis, LANCOM Systems GmbH

ComConsult Netzwerk Forum

ComConsult Akademie

Programmübersicht

Mittwoch 27.03.19

9:00 Uhr

Funknetze für das IoT
- Warum andere Funktechniken? Tut es WLAN nicht auch?
- Bluetooth und BLE – mit kleinen Sprüngen ans Ziel
- ZigBee und Zwave, geeignet auch für Enterprise-Umgebungen?
- Was tun, wenn man keine eigene Infrastruktur installieren kann?
- Die zukünftige Rolle des Mobilfunks bei der IoT-Vernetzung

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

9:45 Uhr

WLAN und der Arbeitsplatz der Zukunft
- Was kommt mit 802.11ax auf uns zu?
- Technologie-Überblick und der aktuelle Stand der Erfahrungen mit 802.11ax
- Das WLAN als Ersatz fürs Kabel im Büro
- Auswirkungen auf Anforderungen und Planung

Dr. Joachim Wetzlar, Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

10:30 Uhr Kaffeepause

Data Center

11:00 Uhr

RZ-Netzdesign für Private Cloud
- EVPN-VXLAN mit MP-BGP
- Designvarianten
- Einsatz von 100G/400G im RZ

Thomas Sillaber, Arista Networks GmbH

11:45 Uhr

Absicherung moderner Applikationen
- Erzielen Sie agile, nachhaltige Sicherheit mit VMware
- Lernen. Beschützen. Anpassen.
- Intelligentes und Einfaches lernen schafft die Vorrausetzungen, um effektives Anpassen zu ermöglichen
- Ost-West-Verschlüsselung in der modernen Applikationswelt
- Ändern Sie die Art und Weise, wie wir Daten sichern

Christoph Buschbeck, VMware Global Inc.

12:30 Uhr Mittagspause

13:45 Uhr

RZ-Georedundanz
- Georedundanz versus RZ-Auslagerung
- DWDM versus IP-Kopplung
- Synchrone und asynchrone Datenhaltung
- Layer-2/3-Design für georedundante RZ

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

14:30 Uhr

OpenStack Neutron: Netzwerk in der Cloud
- Anforderungen an das physische Netz
- Switching, Routing Load Balancing: Was kann Neutron
- Sicherheitsfeatures
- Anbindung an die externe Welt

Dr. Stefan Muthmann, ComConsult Beratung und Planung GmbH

15:15 Uhr

VMware NSX in Theorie und Praxis
- Möglichkeiten und Einschränkungen
- NSX-V vs. NSX-T
- Unterschiede zwischen NSX und physischer Infrastruktur
- Praxisbeispiele und Fallstricke

Dr. Markus Ermes, ComConsult Beratung und Planung GmbH

Donnerstag 28.03.19
Optionaler Thementag „Netzwerk-Sicherheit“

Umgang mit zielgerichteten Angriffen
- Wie zielgerichtete Angriffe bzw. Advanced Persisten Threats (APTs) funktionieren und welche Bedrohungen davon ausgehen
- Welche Angriffsmethoden werden genutzt und wie sieht ein typischer Werkzeugkasten eines Angreifers aus?
- Analyse von bekannten Angriffen: Warum sind system-und anwendungsübergreifende Strategien notwendig?
- Wie können Symptome von Angriffen erkannt werden und welche Rolle spielen Protokollierung, 2nd Generation SIEM und Big Data?
- Sicherheitsgateways im Netzwerk zur Abwehr von Angriffen
- Notwendigkeit einer effektiven und effizienten operativen Informationssicherheit
- Entscheidende Grundlage: Security by Design
- Bedeutung eines Information Security Management System (ISMS) für den Umgang mit zielgerichteten Angriffe • Sensibilisierung der Nutzer und Administratoren

Elemente der operativen Informationssicherheit
- Anforderungen in Standards: ISO 27001 und BSI IT-Grundschutz-Kompendium
- Wie unterscheiden sich spezielle Bereiche wie z.B. Industrial IT und gibt es besondere Anforderungen für Kritis-Bereiche?
- Aufbau eines Security Operation Center (SOC)
- Prozesse der operativen Informationssicherheit
- Systematisches Schwachstellen-Management und zugehöriger Werkzeugkasten
- Integration der operativen Informationssicherheit in den Lebenszyklus von IT-Komponenten • Security Testing und Penetration Testing
- Kernelement Security Incident Management / Prozess zur Behandlung von Sicherheitsvorfällen
- Von Change Management über das Incident Management bis zum Notfallmanagement: Schnittstellen zu IT-Prozessen • Ohne Risikomanagement geht es nicht

Schwachstellen-Scanner und Angriffswerkzeuge
- Wie Schwachstellen-Scanner funktionieren und welche Möglichkeiten sie bieten
- Scanning auf Netzwerk-, Betriebssystem- und Anwendungsebene
- Scanning und Security Testing von Web-Anwendungen und Web-Services
- Compliance Checks: Möglichkeiten und Grenzen
- Produktbeispiele: Nessus, OpenVAS, Burp, ZAP und andere Werkzeuge
- Automatisiertes Schwachstellen-Scanning
- Integration von Schwachstellen-Scannern in internes Netz und in den DMZ-Bereich • Risiken beim Schwachstellen-Scanning und Penetration Testing
- Datenschutzaspekte
- Welche Anforderungen an Security Scans und Tests gibt es in Standards zur Informationssicherheit?
- Elemente eines Konzepts für Schwachstellen-Scanning, Security Testing und Penetration Testing
- Festlegung von Scan-Zielen und Vorgaben zu Scan-Methode, Testtiefe, Testfrequenz • Auswertung von Scan- bzw. Testergebnissen und zugehöriges Berichtswesen

Security Information and Event Management (SIEM)
- Architektur, Funktionsweise von SIEM-Lösungen und Abgrenzung zu Log Management
- Welchen Mehrwert bietet ein SIEM für den Nutzer?
- Typische Anforderungen an eine SIEM-Lösung
- Wie funktioniert die Anbindung der IT an ein SIEM?
- Schnittstellen zu Ticketing-Systemen und Systemen der operativen Informationssicherheit
- Wie funktioniert eine anwendungs- und systemübergreifende die Erkennung von Anomalien und Angriffen?
- Besondere Bedeutung von Künstlicher Intelligenz
- SIEM as a Service und Managed SIEM: Betriebsformen, Möglichkeiten und Grenzen des Outsourcing
- Welche Produkte sind am Markt verfügbar und was leisten sie?
- Ist ein SIEM nur passiv oder könnte auch aktiv und selbständig ein Sicherheitsvorfall beseitigt werden?
- Prozesse, typische Organisationsformen und notwendige Kompetenzen für Betrieb und Nutzung eines SIEM
- Datenschutz und Risiken: Worauf ist beim Betrieb eines SIEM zu achten?

Automatisierte Abwehr von Angriffen und anderen Sicherheitsvorfällen
- Network Access Control (NAC): Einsatz von Profiling-Techniken
- Next Generation NAC und Compliance Checks
- Dynamische Netzsegmentierung: SDN-basierte Konzepte, Mikrosegmentierung mit VMware NSX und Cisco SDA
- Interaktion zwischen Sicherheitskomponenten zur Erkennung und Abwehr von Angriffen • User and Entity Behavior Analytics in Verbindung mit dynamischen Policies auf Sicherheitskomponenten
- Beispiele Cisco Tetration und Aruba Introspect
- Auslösen von Aktionen auf Sicherheitskomponenten durch ein SIEM

Praxisdemonstrationen

Dr. Markus Ermes, Dr. Simon Hoff, Dipl.-Math. Simon Oberem, Dipl.-Inform. Daniel Prinzen, Benjamin Wagner B. Sc., ComConsult Beratung und Planung GmbH