Aktuelle Themen im Bereich der Netze

Wireless LAN (WLAN)

Sicherheit und Lösungen

Dr.-Ing. Kai-Oliver Detken
Private URL: http://www.detken.net
Business URL: http://www.decoit.de

Consultancy & Internet Technologies

Agenda

- Kurzvorstellung
- WLAN-Entwicklung
- Sicherheitslücken
- Lösungen
- Zusammenfassung

WLAN-Entwicklung

Definition

- Ein Wireless LAN (WLAN) ist ein drahtloses Netzwerk, welches für mobile Teilnehmer geeignet ist
- Drahtlos bedeutet: die Daten werden kabellos übertragen
- Mobil bedeutet: die benutzten Geräte sind nicht ortsgebunden einsetzbar
- Als Übertragungsmedium bedient man sich der „Luft”:
  - Funk
  - Infrarot

Unterschiedliche Funktechnologien (3)

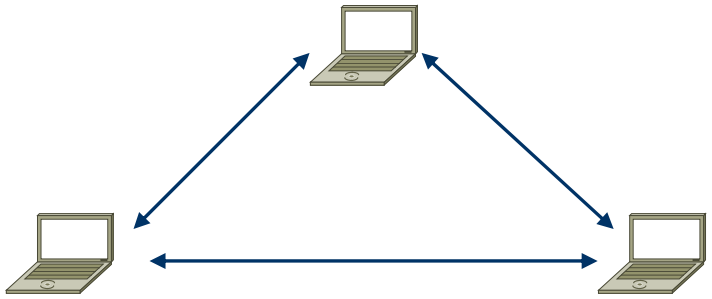
- WLAN
  - Übertragungsrate: bis 108 MBit/s
  - Reichweite: ca. 300 m im Freien / 30 m in Gebäuden
  - Frequenz: 2,4 und 5 GHz
  - Frequenzlizenz: nicht erforderlich
  - Für Übertragung von Daten entwickelt
  - Sprache ist per VoIP möglich
  - Standards: IEEE 802.11(a, b, g, h…)

Grundmerkmale

- WLAN-Technologie
  - Alle Standards im IEEE 802.11-Umfeld werden im allgemeinen als Wireless LAN bezeichnet
  - ISM Funktechnik (Industrial, Scientific, Medical)
  - Für ISM-Geräte reserviertes Frequenzband
  - Frequenzbereich ist lizenzfrei

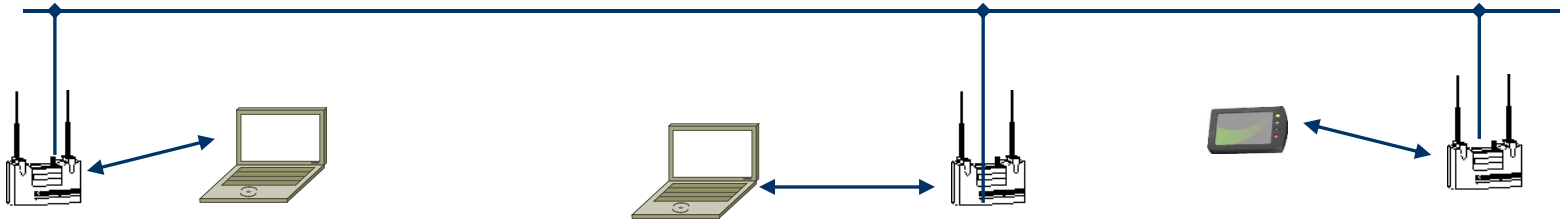
Grundlegende WLAN-Modelle (1)

- Ad-hoc Modus
  - Peer-to-Peer Netz in einer Zelle
  - Independent Basic Service Set
  - Einfach zu konfigurieren
  - Keine weitere Infrastruktur erforderlich
  - Beschränkte Reichweite
  - Beschränkte Funktionalität



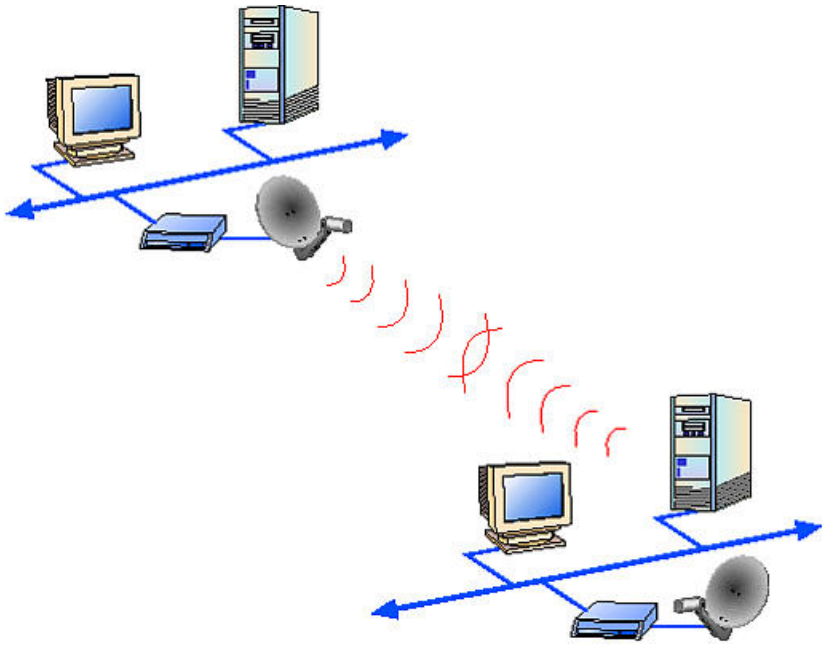
Grundlegende WLAN-Modelle (2)

- Infrastruktur Modus
  - Über Access Points
  - Konfiguration erforderlich
  - Verbundenes Netz = Extended Service Set
  - Wandern möglich
  - Zugang zum Festnetz mit allen Funktionen
  - Hohe Nutzerdichten über Load Balancing möglich



Grundlegende WLAN-Modelle (3)

- Bridging Modus
  - Direkte Kopplung von Access Points
  - Verbindung von Gebäudekomplexen (Hot-Spot-Erweiterung)
  - Reichweite: mehrere Kilometer sind möglich



Kollisionserkennung

- Bei drahtlosen Systemen ist keine direkte Kollisionserkennung möglich, da das Sendesignal das fremde Empfangssignal überdeckt!
- Folgende Verfahren zur Kollisionsumgehung werden genutzt:
  - CSMA-CA (Carrier Sense Multiple Access/Collision Avoidance)
    - Jedes gesendete Frame, wird vom Empfänger bestätigt
    - Ein Ausbleiben dieser Bestätigung bedeutet, dass es zu einer Störung (Kollision) gekommen ist
  - Virtual Carrier Sense
    - Anmelden einer bevorstehenden Übertragung
    - Dauer der anstehenden Übertragung wird mit gesendet und ist für alle anderen Teilnehmer ersichtlich

Übertragungsverfahren

Für Wireless LANs existieren drei Verfahren zur drahtlosen Datenübertragung:

- FHSS (Frequency Hopping Spread Spectrum)
  - Aufteilung des Bereichs in 79 Kanäle mit jeweils 1MHz Bandbreite
  - Automatisches Wechseln der Kanäle nach vereinbartem Muster
  - Viele Teilnehmer können parallel arbeiten
- DSSS (Direct Sequence Spread Spectrum)
  - 9 (13) Kanäle zu je 11 MHz Bandbreite
  - Teilweises überlappen der Kanäle
  - Ermöglicht höhere Geschwindigkeiten
- (Infrarot)

WLANs: von „b“ bis „h“

- 1999:
  - 802.11b: Weltweiter Standard (2.4 GHz)
  - 802.11a: 5 GHz, 54 MBit/s, in Deutschland legalisiert
- 2002:
  - 802.11g: Hohe Geschwindigkeiten für 802.11b
  - 802.11h: als 802.11a in Europa legalisiert (h-Standard selbst liegt bisher nur als Draft vor!)
- 2003
  - Dual-Mode/Dual-Band 802.11g/h

Arbeitsgruppe	Arbeitsgebiet
802.11a	54-Mbit/s-WLAN im 5 GHz-Band
802.11b	11-Mbit/s-WLAN im 2,4-GHz-Band
802.11c	Wireless Bridging
802.11d	"World Mode", Anpassung an regionsspezifische Regulatorien
802.11e	QoS- und Streaming-Erweiterung für 802.11a/g/h
802.11f	Roaming für 802.11a/g/h (Inter Access Point Protocol IAPP)
802.11g	54-Mbit/s-WLAN im 2,4-GHz-Band
802.11h	54-Mbit/s-WLAN im 5-GHz-Band mit DFS und TPC
802.11i	Authentifizierung/Verschlüsselung für 802.11a/b/g/h (AES, 802.1x)

WLAN-Überblick

	802.11a	802.11h	802.11g	802.11b
Status	Standard	Standard	Standard	Standard
Frequenzband (MHz)	5150-5350, 5725-5825	5150-5350, 5725-5825	2400,0-2483,5	2400,0-2483,5
Datenrate brutto (MBit/s)	54	54	54	11
Datenrate netto (MBit/s)	32	28	32	5
Sendeleistung [RegTP] (mW)	30	200	100	100
Reichweite (ca., m)	10 bis 15	30 bis 50	30 bis 50	30 bis 50
Einsatz [RegTP]	Indoor	Indoor	Indoor, Outdoor	Indoor, Outdoor
Spektrum	300 MHz	300 MHz	83,5 MHz	83,5 MHz
Kanäle [RegTP]	8	8	3	3
Zugriffsverfahren	CSMA/CA	CSMA/CA RTS/CTS	CSMA/CA RTS/CTS	CSMA/CA
Multicasting	ja	ja	ja	ja
QoS	zukünftig	zukünftig	zukünftig	nein
PHY	OFDM	OFDM mit DFS	CCK/OFDM CCK/DSSS	CCK/DSSS
Link-Kontrolle	nein	TPC	nein	nein

WLAN-Anwendungen

- Mobile Arbeitsplätze
- Schulungseinrichtungen
- Vernetzung von Home Offices
- Vernetzung von geschützten Gebäuden
- Mobile Datenerfassung
- Hot-Spots
- Externe Vernetzung
- Ad-hoc-Networking

Sicherheitslücken

Sicherheitsgrad

- Die aktuellen standardkonformen Funk-LAN-Systeme bergen bzgl. der Sicherheit große Schwachstellen, die aktive wie passive Angriffe erlauben und damit zu einem Verlust in folgenden Bereichen führen können:
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- Zudem sind Funk-LAN Komponenten im Auslieferungszustand oftmals so konfiguriert, dass keine oder nur einige der Sicherheitsmechanismen aktiviert sind

Sicherheitslücken (1)

- **SSID Broadcast:** Einige APs bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden, um das Funk-LAN vor Unbefugten zu verstecken (so genanntes „Closed System“).
- **Manipulierbare MAC-Adresse:** MAC-Adressen der Funk-Clients können relativ einfach abgehört und manipuliert werden.
- **Fehlendes Schlüsselmanagement:** Schlüssel werden selten oder überhaupt nicht gewechselt. Die Offenbarung eines Schlüssels, z.B. durch Verlust eines Clients oder mittels frei verfügbarer Tools, kompromittiert das gesamte Funk-LAN.
- **Schwachstellen in WEP:** Das Ziel mittels WEP Vertraulichkeit, Integrität und Authentizität im Funk-LAN zu sichern, kann eindeutig als nicht erreicht eingestuft werden, denn WEP ist mittlerweile vollständig kompromittiert.

Sicherheitslücken (2)

- **Bedrohung der lokalen Daten:** Lokale Datei- bzw. Druckerfreigaben im Betriebssystem erlauben in der Grundeinstellung meist auch über das Funk-LAN Zugriffe auf diese Ressourcen.
- **Unkontrollierte Ausbreitung der Funkwellen:** Auch über die spezifizierte Reichweite von 10-150 Metern hinaus, breiten sich die Funkwellen der Funk-LAN-Komponenten aus und können von anderen genutzt werden.
- **Bedrohung der Verfügbarkeit:** Störung durch andere Funksysteme wie Bluetooth, andere WLANs und Mikrowellen.
- **Erstellung von Bewegungsprofilen:** Da die Hardwareadresse einer Funk-LAN-Karte, die sog. MAC-Adresse, bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen MAC-Adresse des Funk-Clients, Ort und Uhrzeit der Datenübertragung herstellbar.

Angriff auf RC4-Algorithmus (1)

- Benötigte Datenmenge in Abhängigkeit von der durchschnittlichen Paketgröße und Paketanzahl:

Anzahl der Pakete	Paketgröße		
	512 Byte	1024 Byte	2048 Byte
2.000.000	0,95 GByte	1,91 GByte	3,81 GByte
4.000.000	1,91 GByte	3,81 GByte	7,53 GByte
6.000.000	2,86 GByte	5,72 GByte	11,44 GByte
8.000.000	3,81 GByte	7,63 GByte	15,26 GByte

Angriff auf RC4-Algorithmus (2)

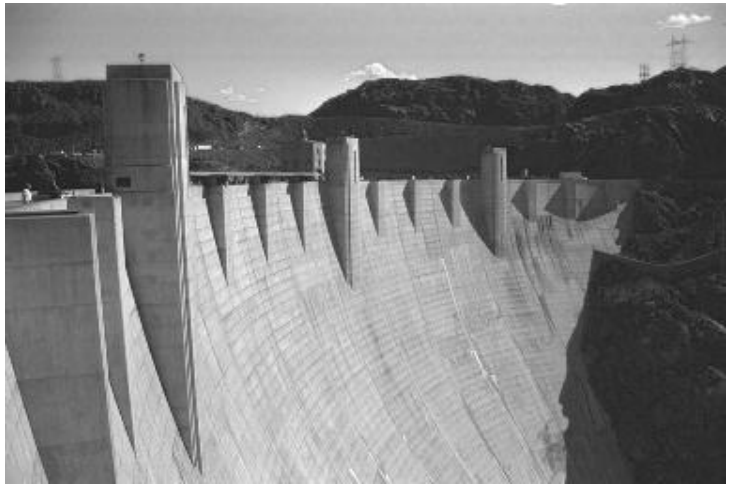
- Benötigte Angriffszeit in Abhängigkeit von der Datenmenge und der durchschnittlichen AP-Auslastung:

Datenmenge	Auslastung		
	5 MBit/s	1 MBit/s	0,1 MBit/s
0,95 GByte	25 Minuten	2,11 Stunden	21,11 Stunden
0,91 GByte	50 Minuten	4,24 Stunden	42,44 Stunden
2,86 GByte	1,27 Stunden	6,36 Stunden	2,65 Tage
3,81 GByte	1,7 Stunden	8,47 Stunden	3,53 Tage
5,72 GByte	2,54 Stunden	12,71 Stunden	5,3 Tage
7,63 GByte	3,39 Stunden	16,96 Stunden	7,06 Tage
11,44 GByte	5,08 Stunden	25,42 Stunden	10,59 Tage
15,26 GByte	6,78 Stunden	33,91 Stunden	14,13 Tage

Angriff auf RC4-Algorithmus (3)

- Gemäß beider Tabellen sind beispielsweise bei einer durchschnittlichen Paketgröße von 1.024 Byte und geschätzten 4 Millionen benötigten Paketen insgesamt 3,81 GByte an abgehörten Daten notwendig, um den Angriff auf RC4 durchführen zu können
- Bei einem AP mit mittlerer Auslastung, also z. B. bei einer durchschnittlichen Auslastung von 1 MBit/s benötigt der Angriff demnach ca. 8,4 Stunden
- Obwohl schon bei nur mäßiger durchschnittlicher Auslastung des Funk-LANs der Schlüssel in relativ kurzer Zeit ermittelt werden kann, ist ein regelmäßiger Schlüsselwechsel (so oft wie praktikabel) trotzdem sinnvoll
- Bei Systemen nach den Standards 802.11a und 802.11g verringert sich die benötigte Zeit entsprechend

Lösungen



Erhöhte Sicherheitsmechanismen

- Im Sommer 2003 hatte die WiFi-Alliance, in der sich fast 200 WLAN-Herstellern organisiert haben, mit WPA-Bestandteile von 802.11i vorweggenommen
  - WPA (WiFi Protected Access) sieht eine bessere Verschlüsselung vor, da es das so genannte Temporal Key Integrity Protocol (TKIP) verwendet
  - Ferner werden Pre-shared Keys verwendet sowie das RADIUS-basierte 802.1X
  - Mit diesem kann man Benutzer eindeutig identifizieren
  - Das Wi-Fi-Konsortium hat damit eine eigene Art der WLAN-Verschlüsselung etabliert

Neuer Standard 802.11i

- Der Wireless-Standard IEEE 802.11i ist seit Juni 2004 vom IEEE ratifiziert
- Beinhaltet sind die seit längerem erwarteten Sicherheitsspezifikationen für Funknetze, insbesondere was Verschlüsselung betrifft
- 802.11i ersetzt das unsichere Verschlüsselungsverfahren WEP durch WPA
- Darüber hinaus schreibt der Standard vor, wie Advanced Encryption Standard (AES) zur Verschlüsselung von Daten zu verwenden ist
- Damit genügt er den Vorschriften des Federal Information Standards (FIPS) und ist somit auch behördentauglich
- Allerdings erfordert die AES-Umsetzung kompatible Hardware, es sei denn, der Anbieter hat schon vorsorglich 802.11i in seine Komponenten integriert

WiFi Protected Access (WPA)

- WPA ist vom IEEE-Projekt 802.11i abgeleitet und aufwärtskompatibel
- WPA nutzt ausgewählte Bestandteile von 802.11i wie beispielsweise
  - einen erweiterten Initialization-Vector
  - Re-Keying
  - Message-Integrity-Check
- WPA verwendet Authentifizierung mittels IEEE 802.1x und EAP (Extensible Authentication Protocol), die auf einen vorhandenen RADIUS-Server für die Nutzerverwaltung zurückgreifen
- WiFi-zertifizierte WLAN-Geräte lassen sich per Software-Aktualisierung mit WPA ausrüsten

EAP/802.1X

- IEEE 802.1X wurde mit dem Ziel entwickelt, möglichst viele Sicherheitslücken aus 802.11 zu schließen (z.B. fehlendes Schlüsselmanagement, fehlende Benutzeridentifikation und -Authentisierung)
- In 802.1X kommt eine Port-basierende Authentisierung zum tragen
- Das Extensible Authentication Protocol (EAP) soll im Zusammenspiel mit einem Authentisierungsserver das Sicherheitsniveau erhöhen
- 802.1x basiert auf EAP: Die EAP-Messages werden hierzu in 802.1X-Nachrichten verpackt (EAP over LAN - EAPOL)
- An einer solchen portbezogenen Authentifizierung sind drei Elemente beteiligt:
  - der Client (Supplicant), der sich in einem Netzwerk authentifizieren möchte (z.B. Laptop)
  - der Authentifizierer (Authenticator), der den Authentifizierungsvorgang mit dem Client durchführt (z.B. WLAN AP)
  - der Authentifizierungs-Server (Authentication Server), der dem Authentifizierer die zur Authentifizierung erforderlichen Informationen zur Verfügung stellt (z.B. RADIUS Server)

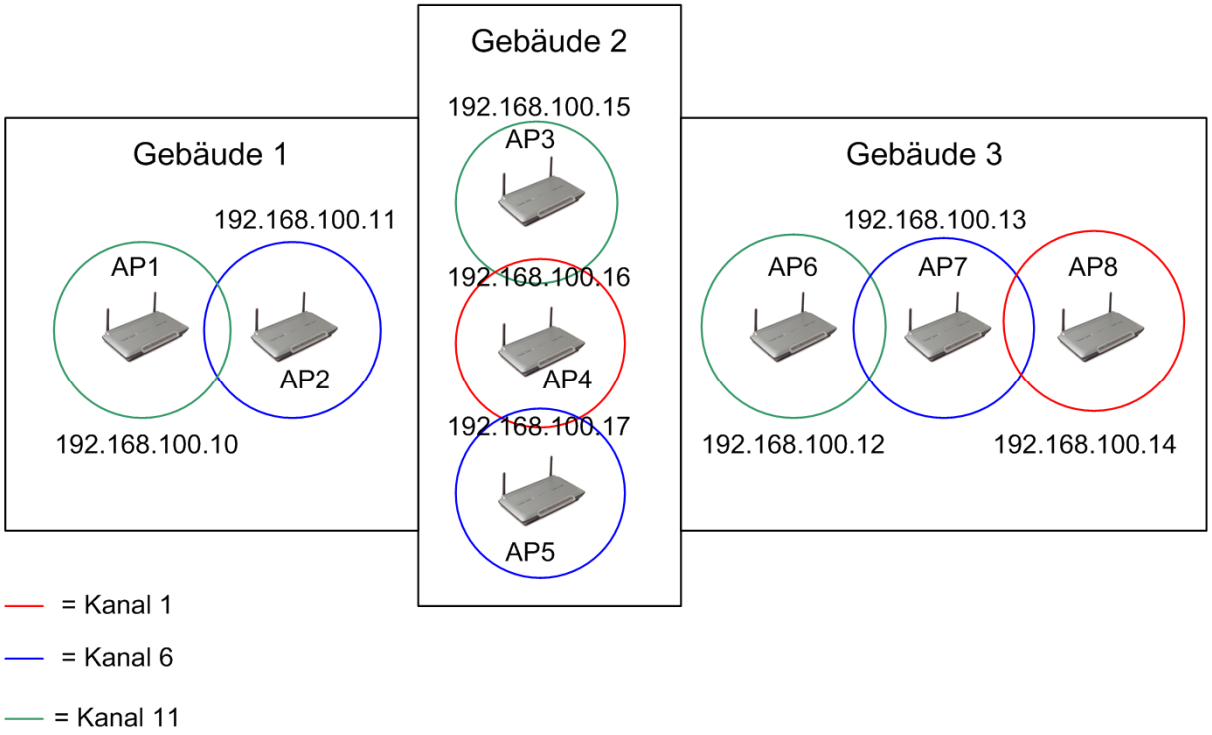
Auswahlkriterien

- Bei der Auswahl der geeigneten Komponenten ist es nicht mehr ausreichend, nur die vom Hersteller zur Verfügung gestellten Funktionen oder den Anschaffungspreis der Produkte als Auswahlkriterium heranzuziehen
- Heutzutage hat sich im IT-Bereich als Grundlage für Investitionsentscheidungen der Begriff der Total Costs of Ownership (TCO) etabliert, welcher zusätzlich zu den oben genannten Aspekten noch folgende Kriterien hinzufügt:
  - die Kosten für den Betrieb und den Support,
  - die Ausbau- und Erweiterungsfähigkeit einer Lösung sowie
  - ihre Integrationsfähigkeit in bestehende und zukünftige IT-Landschaften

Ausleuchtung der WLAN-Komponenten

- Besonders die Ausleuchtung ist bei Aufbau von WLAN APs zu beachten sowie die Überlappung von gleichen Kanälen
- Um Störungen zu vermeiden sollte jeder AP nur mit einem Kanal senden und einen anderen besitzen, als seine direkten Nachbarn
- Ein Abstand von 5 Kanälen stellt dabei ein Optimum dar
- Zusätzlich können manche APs noch durch zusätzliche Bridging-Funktionalität direkt miteinander verbunden werden, um ein unterbrechungsfreies Roaming zwischen den APs für die Endgeräte zu ermöglichen

WLAN-APs in verschiedenen Gebäuden



Weitere Anforderungen

- Weitere Anforderungen bei der Umsetzung und Implementierung sind:
  - Ausarbeitung eines WLAN-Konzepts (Ausleuchtung, Frequenzen etc.)
  - Vermessung des Funknetzes vor Ort (WLAN-Messung)
  - Dokumentieren der optimalen/möglichen Standorte der Access Points
  - Konfiguration der Basiseinstellungen (SSID und MAC-Zugriffsschutz)
  - Konfiguration der Sicherheitseinstellungen (WPA, RADIUS, AES)
  - Durchführen von Sicherheits-Checks zur Überprüfung der Einstellungen

Zusammenfassung

Fazit

- WLAN-Netze erweitern heutige Netzwerke, um so den Benutzern mehr Flexibilität und Mobilität zu verleihen
- Weiterentwicklungen, wie Mobile Broadband Wireless Access (IEEE 802.20), WiMAX ((IEEE 802.16) und Wireless Personal Area Networks (IEEE 802.15) werden den drahtlosen Technologien einen weiteren Schub bescheren und neue Einsatzgebiete ermöglichen
- Der Einsatz ist dabei heute, durch die neuen Sicherheitsstandards, auf einem sehr hohen Niveau möglich
- Neben der Sicherheit sind allerdings noch weitere Kriterien beim Aufbau zu betrachten und in einem Konzept einzubeziehen, um alle Vorteile wirklich nutzen zu können

Vielen Dank für Ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 1
D-28359 Bremen
Tel./Fax: +49-421-2208-185/-150
info@decoit.de

Consultancy & Internet Technologies