



**Der Landesbeauftragte für den
Datenschutz Niedersachsen**



Sichere Funknetzwerke

CeBIT 2004

Thomas Brosig

Mitarbeiter der Geschäftsstelle des
Landesbeauftragten für den Datenschutz Niedersachsen

Was erwartet Sie?

- Grundlagen
- Sicherungs- und Gestaltungsziele
- Gefahren
- Schutzmaßnahmen
- Fazit

Sichere Funknetze

Technische Grundlagen

Agenda

Grundlagen

Sicherungs-
ziele

Gefahren

Schutz-
maßnahmen

Fazit

Drahtlose Netze nach IEEE Standard 802.11 werden als
Wireless Local Area Networks (WLAN) bezeichnet.

- Anbindung an kabelgebundene Netze durch einen Access Point
- Übertragungsraten zwischen 11 Mbps und 54 Mbps erreichbar
- Verschiedene Betriebsarten möglich (Ad Hoc, Infrastruktur,...)
- Funkübertragung ist genehmigungsfrei und weltweit einsetzbar
- Herstellerseitig werden verschiedene Sicherheitskomponenten auf den Access Points implementiert

Sichere Funknetze

Unterschied LAN / WLAN

Agenda

Grundlagen

Sicherungs-
ziele

Gefahren

Schutz-
maßnahmen

Fazit

LAN:

- Traditionelle Netzwerke haben eine klar definierte Ausbreitung.
- Der Angreifer muss physikalischen Zugang zu einem Netzwerkanschluss haben, um angreifen zu können.

WLAN:

- Funknetzwerke breiten sich auch über Gebäudegrenzen hinweg aus und sind nur schwer einzugrenzen.
- Die Netzwerk-Infrastruktur wird von innen angegriffen.

Sichere Funknetze

Ausbreitung von Funkwellen

Agenda

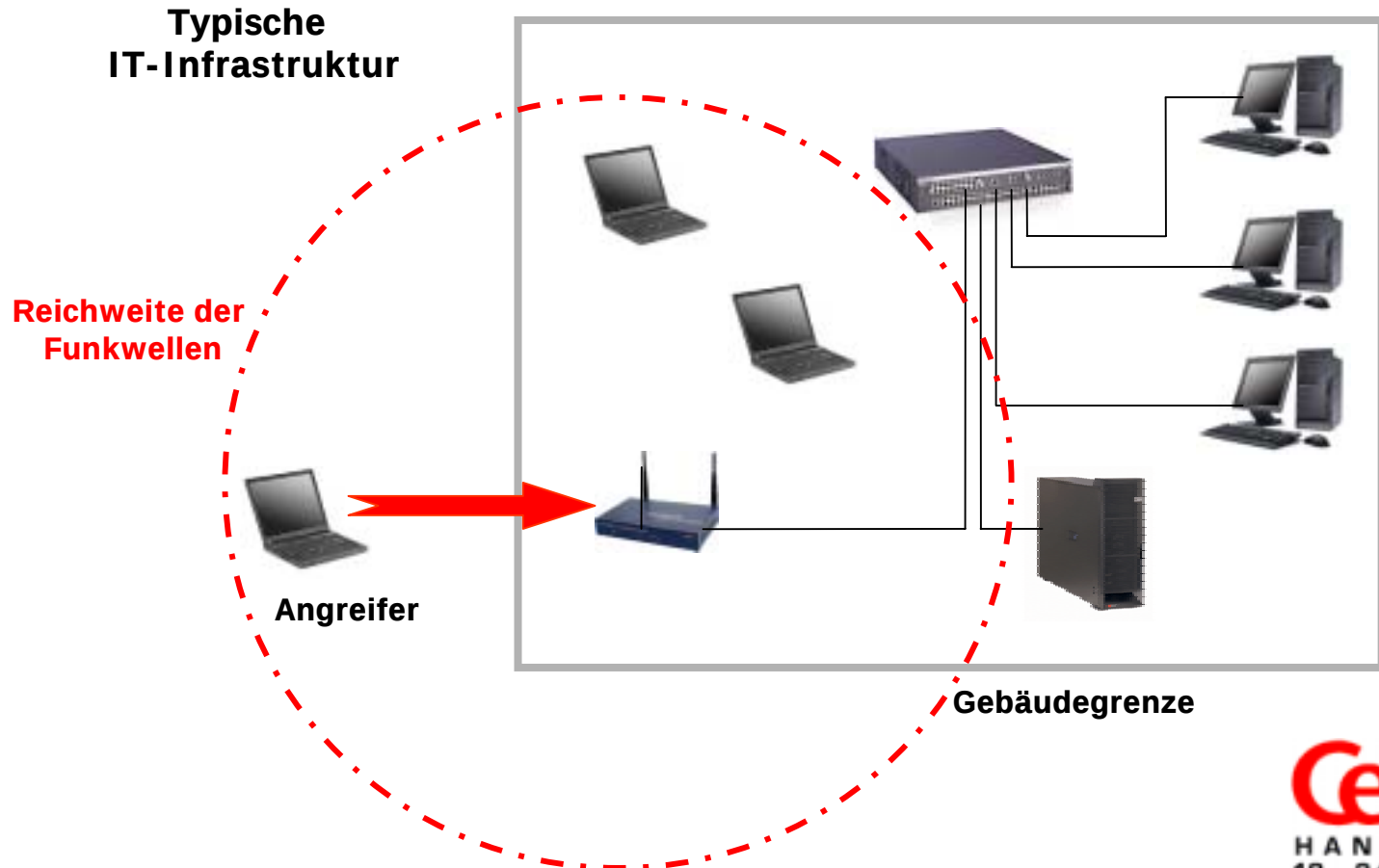
Grundlagen

Sicherungs-
ziele

Gefahren

Schutz-
maßnahmen

Fazit



Sichere Funknetze

Sicherungs- und Gestaltungsziele

Agenda

Grundlagen

**Sicherungs-
ziele**

Gefahren

Schutz-
maßnahmen

Fazit

Welche Ziele sollte ein sicheres Funknetzwerk erfüllen?

- **Vertraulichkeit** der Kommunikation bewahren
- **Integrität** der Daten gewährleisten
- **Verfügbarkeit** der IT-Infrastruktur und der Daten sicherstellen
- **Authentizität** der Benutzer verifizieren

Sichere Funknetze

Sicherungs- und Gestaltungsziele

Agenda

Grundlagen

**Sicherungs-
ziele**

Gefahren

Schutz-
maßnahmen

Fazit

Grundsätzlich gilt...

- Jedes lokale Netzwerk muss gegen Angriffe gesichert werden.
- Durch die Angriffsmöglichkeit von innen erhöht sich der dafür notwendige Aufwand bei Betrieb eines WLAN.
- Die geeigneten Maßnahmen sind individuell für jedes Netzwerk zu bestimmen (Risikoanalyse, Sicherheitskonzept).

Möglichkeiten eines Angreifers

- Internetnutzung (Authentizität)
- Datenverkehr abhören (*Vertraulichkeit*)
- Datendiebstahl (*Vertraulichkeit*)
- Datenmanipulation (*Integrität und Authentizität*)
- Vandalismus (*Verfügbarkeit*)

Bekannte Schwächen von WLAN Access Points

- SSID Broadcast
- Manipulierbare MAC-Adressen
- Fehlendes Schlüsselmanagement für WEP
- Technische Schwachstellen in WEP

Bekannte Schwächen von WEP Sicherheit

- WEP ist in jeder Schlüssellänge unsicher
- Keine Benutzerauthensierung möglich
- Keine gegenseitige Authentisierung
- Fehlende Schlüsselverwaltung auf Clients und AP

Das bedeutet...

... WEP ist auf keinen Fall eine Einrichtung für die absolute Sicherheit, aber kann einen gewissen Grundschutz bieten.

Sichere Funknetze

Schutzmaßnahmen

Agenda

Grundlagen

Sicherungs-
ziele

Gefahren

Schutz-
maßnahmen

Fazit

Grundschutz

Obwohl feststeht, dass die herstellerseitig implementierten Schutzmechanismen in WLAN-Komponenten nur einen bedingten Schutz gegen Angriffe bieten, sollten sie aktiviert werden.

Nachfolgend werden diese Schutzmaßnahmen für die sichere Konfiguration und den sicheren Betrieb vorgestellt.

Sichere Konfiguration

- ✓ Standard SSID ändern (kein Rückschluss auf Betreiber)
- ✓ SSID Broadcast am Access Point abschalten
- ✓ Standard Kennwort für die Access Point Konfiguration ändern
- ✓ Konfiguration des AP sollte nur von Clients aus dem LAN möglich sein
- ✓ MAC Adress-Filterung am Access Point einschalten

Sichere Konfiguration

- ✓ WEP Verschlüsselung aktivieren (möglichst 128 Bit oder höher)
- ✓ WEP-Authentifikationsmethode von „Shared Key“ auf „Open“ wechseln
- ✓ Deaktivieren des DHCP-Servers am Access Point
- ✓ Aufstellungsort und Antennencharakteristik des AP optimieren
- ✓ Reichweitenbeschränkung des AP durch Reduzierung der Sendeleistung

Sichere Funknetze

Schutzmaßnahmen

Agenda

Grundlagen

Sicherungs-
ziele

Gefahren

Schutz-
maßnahmen

Fazit

Sicherer Betrieb

- ✓ Regelmäßiger Wechsel der WEP-Schlüssel
- ✓ Sicherheitsrelevante Firmware-Upgrades durchführen
- ✓ WLAN nur bei Bedarf einschalten
- ✓ Protokollierung der WLAN-Kommunikation und regelmäßige Protokollauswertung

Sichere Funknetze

Schutzmaßnahmen

Agenda

Grundlagen

Sicherungs-
ziele

Gefahren

Schutz-
maßnahmen

Fazit

WICHTIG !

Neben den vorgestellten Schutzmaßnahmen sollten insbesondere bei der Verarbeitung personenbezogener Daten weitere Absicherungen getroffen werden, um zielgerichteten Attacken standhalten zu können.

Zusätzliche Absicherung

- ✓ Verwendung kryptographischer Verfahren für die Kommunikationsabsicherung (VPN/IPSec)
- ✓ Zertifikatsbasierte Authentisierung der Nutzer (Chipkarte, Token)
- ✓ Anbindung der Access Points über eine Firewall mit Intrusion Detection System
- ✓ Absicherung der mobilen Endgeräte (Virenschutz, Personal Firewall, lokale Datenverschlüsselung, etc.)

Sichere Funknetze

Schutzmaßnahmen

Agenda

Grundlagen

Sicherungs-
ziele

Gefahren

Schutz-
maßnahmen

Fazit

Fazit und Ausblick

- ✓ Bei der Beschaffung von WLAN-Komponenten sollte darauf geachtet werden, dass die aufgeführten technisch-organisatorischen Maßnahmen umgesetzt werden können.
- ✓ Soweit verfügbar sollte WPA der WEP-Verschlüsselung vorgezogen werden.
- ✓ Eine Vorabkontrolle bzw. ein Sicherheitskonzept sollte für das spezielle Einsatzszenario erstellt werden.
- ✓ Für die Verarbeitung von personenbezogenen Daten ist eine zusätzliche Absicherung (VPN, IPSec) erforderlich.

Wenn Sie mehr wissen wollen...

Der Landesbeauftragte für den Datenschutz Niedersachsen

Schreiben	Postfach 221, 30002 Hannover
Anrufen	(0511) 120-4500
Faxen	(0511) 120-4599
Surfen	www.lfd.niedersachsen.de
E-mailen	poststelle@lfd.niedersachsen.de