

## Newsletter 08.09

**DOK SYSTEME – 25  
Jahre Erfahrung,  
Qualität und  
Neutralität in der ITK  
Unternehmens- und  
Technologieberatung**

**Das Team des  
Newsletters  
DOKinfo!  
wünscht Ihnen  
viel Spaß beim  
Lesen. Für  
Anregungen  
sind wir dankbar  
und nehmen  
diese gern auf.  
Bitte richten Sie  
diese an Frau  
Melanie Bienek :  
bienek@doksysteme.de**

## Aktuelles

### 25 Jahre DOK SYSTEME GmbH

#### Inhalt:

**Datenschutz bei DECT**

**DOK SYSTEME unterstützt die  
EWE TEL von der Angebotserstellung  
bis zum Zuschlag für das neue Sprach-  
und Datennetz der Landesverwaltung  
Niedersachsen**

**Seminare und Veranstaltungen:  
Programm 02/2009**

**„Fach-Chinesisch“ und „Kürzelknacker“**

No-Spam-Policy: Sie erhalten diesen Newsletter, weil Sie sich für ihn registriert haben oder weil Sie mit der DOK SYSTEME GmbH in Korrespondenz oder Geschäftsverbindung standen oder stehen. Wir geben keine E-Mail-Adressen weiter. Falls Sie in Zukunft keinen Newsletter mehr erhalten möchten, können Sie sich [hier](#) abmelden oder uns eine E-Mail an [newsletter@doksysteme.de](mailto:newsletter@doksysteme.de) mit dem Text "unsubscribe" in der Betreffzeile zusenden.

## Newsletter 08.09



Dipl.-Ing. Dieter Steuer  
Gründungsgesellschafter

### **25 Jahre DOK SYSTEME GmbH** **- Ein Rückblick -**

1984 wurde die DOK SYSTEME Ingenieurgesellschaft für Kommunikationstechnik mbH mit dem Ziel der Kundenberatung gegründet, in den nachfolgenden Bereichen:

**D**atentechnik  
**O**rganisation  
**K**ommunikation

Durch die Entwicklung der Informations- und Kommunikationstechnik war die Zeit damals reif für unser Unternehmen.

1980 wurden die ISDN-Standards veröffentlicht und die Arbeitsgruppe IEEE 802 nahm ihre Arbeiten zur Standardisierung von Local und Metropolitan Area Networks auf.

1982 entschied sich die Deutsche Bundespost, ISDN als Basis für ihr digitales Netz einzusetzen.

1984 brachte Apple den Macintosh Computer und IBM den PC AT heraus. In Deutschland startete das erste Kabelfernsehpilotprojekt und die ersten privaten Fernsehsender nahmen ihren Betrieb auf. Gekennzeichnet war dieser Zeitraum durch die Umstellung von analogen auf digitale Technologien in der Kommunikationstechnik, durch die Migration von den zentralen Großcomputern auf dezentrale Personal Computer, die Entwicklung von Computernetzwerken und die Einführung neuer Medienangebote.

So konnte sich DOK SYSTEME innerhalb kurzer Zeit durch Fachkompetenz und methodisches Vorgehen Referenzprojekte schaffen, die die Basis für ein erfolgreiches Fortbestehen waren.

## Newsletter 08.09



Dr.-Ing. Jan Steuer  
Geschäftsführer

Die zweite Hälfte der 80er Jahre wurde maßgeblich durch den Bildschirmtext (BTX) geprägt. Diese Zeit kann man rückblickend als Einstieg zur Internetkommunikation werten; DOK SYSTEME war an vielen Projekten maßgeblich beteiligt.

Ein für DOK SYSTEME bahnbrechender Meilenstein war die Planung und Einführungsbegleitung der ersten in Deutschland an ISDN angeschlossenen TK-Anlage zur CeBIT 1989, nämlich die der Deutschen Messe AG in Hannover mit sofort 52 Anschlüssen PMX/1TR6 und ca. 10.000 Teilnehmern. Hierzu gab es kein Back-up und es ging gut!

Aber die technologische Entwicklung ging rasant weiter.

Etwa 10 Jahre später war der Markt geprägt durch die Deregulierung der Telekommunikation und den Aufbau der GSM-Netze.

Dementsprechend war DOK SYSTEME in den 90-er Jahren neben der Betreuung der privaten Wirtschaft und der öffentlichen Auftraggeber insbesondere bei den neuen Netzbetreibern aufbauunterstützend, beratend und planend tätig. Eine Vielzahl von Stadtnetz- und Regionalnetzbetreibern entstand mit Hilfe der DOK SYSTEME, die auf Basis der vorhandenen Netzinfrastruktur und des zu erwartenden Marktpotenzials die technische Planung und die betriebliche Organisation der neuen Netze erfolgreich begleitete.

Mit der Erfolgsstory des Internet stand die Informations- und Kommunikationstechnik weitere 10 Jahre später im Zeichen von „All-IP“.

Telekommunikationsanlagen wandeln sich von Hardware-lastigen zentralen Systemen in flexibel einsetzbare Kommunikationsserver in IP-Netzen mit Voice-over-IP-Endgeräten. Telefonie wird dadurch zu einer weiteren Applikation im Datennetz, die Verknüpfung von Sprache und Daten in spezifischen Applikationen zur Unterstützung der Geschäftsprozesse wird einfacher.

## Newsletter 08.09



Dr.-Ing. Andreas Rendel  
Geschäftsführer

Netzbetreiber stellen ihre Netzinfrastrukturen auf „Next Generation Networks“ um, Fest- und Mobilfunknetze wachsen zusammen. Für den Kunden entstehen dadurch neue Produktangebote und Lösungen, während alte vom Markt verschwinden.

Der Beratungsbedarf bei den Kunden nimmt also keineswegs ab. Neben der technischen Beratung und Planung auf dem Weg zur nächsten Netzgeneration sind es heute wirtschaftliche und betriebliche Fragestellungen, die in den Projekten der DOK SYSTEME eine zentrale Rolle spielen.

So hat sich DOK SYSTEME in den letzten Jahren zu einer ganzheitlichen Unternehmensberatung im Bereich der Informations- und Kommunikationstechnik gewandelt und ist mit diesem Ansatz weiterhin erfolgreich am Markt tätig. Bewährt hat sich insbesondere die stets neutrale und unabhängige Vorgehensweise.

DOK SYSTEME ist nunmehr in der zweiten Generation inhabergeführt; die Geschäftsführung ging 2005 vom Gründer und langjährigem Gesellschafter-Geschäftsführer Dieter Steuer auf die Geschäftsführer Dr. Jan Steuer und Dr. Andreas Rendel über.

Nach 25 Jahren fanden wir es an der Zeit, den Öffentlichkeitsauftritt der DOK SYSTEME neu zu gestalten, um auch ein optisches Zeichen für den Wandel zu setzen.

Wir freuen uns darauf, Ihnen auch in Zukunft unter neuem Logo unsere Beratungsleistungen in gleicher Kompetenz und Qualität erbringen zu können.

Auch unser Internetauftritt wird in diesem Zuge neu gestaltet.

## Newsletter 08.09



Dipl.-Ök. Michael Stalke

### Datenschutz bei DECT

#### 1 Einleitung

Die schnurlose Telefonie nach dem DECT-Standard galt bisher als sicher. Durch die ZDF-Sendung „Frontal 21“ im Januar 2009 wurde die Öffentlichkeit in Deutschland auf Sicherheitslücken in diesen Standard hingewiesen. So lassen sich nichtverschlüsselte DECT-Verbindungen mittels einer COM-ON-AIR PCMCIA Card (etwa 25 €), einem Laptop und einer frei im Internet erhältlichen Treibersoftware mithören. Insbesondere bei Endgeräten aus dem Heimbereich scheint dieses ein Problem zu sein, da viele ältere Endgeräte nicht verschlüsseln.

Darüber hinaus sind aber auch andere Angriffe möglich, die nachfolgend beschrieben werden.

Im Internet werden Anleitung und Software vom deDECTed.org Projekt ([dedected.org](http://dedected.org)) zur Verfügung gestellt. Ziel dieses Projektes ist das bessere Verständnis verschiedener DECT Implementierungen und das Erstellen einer Open-Source-Implementierung des DECT-Standards, um letztendlich auch auf Sicherheitslücken hinweisen und diese schließen zu können.

Das Projektteam setzt sich aus Mitgliedern der folgenden Organisationen zusammen:

- Chaos Computer Club,
- TU Darmstadt,
- University of Luxembourg,
- Bauhaus-Universität Weimar.

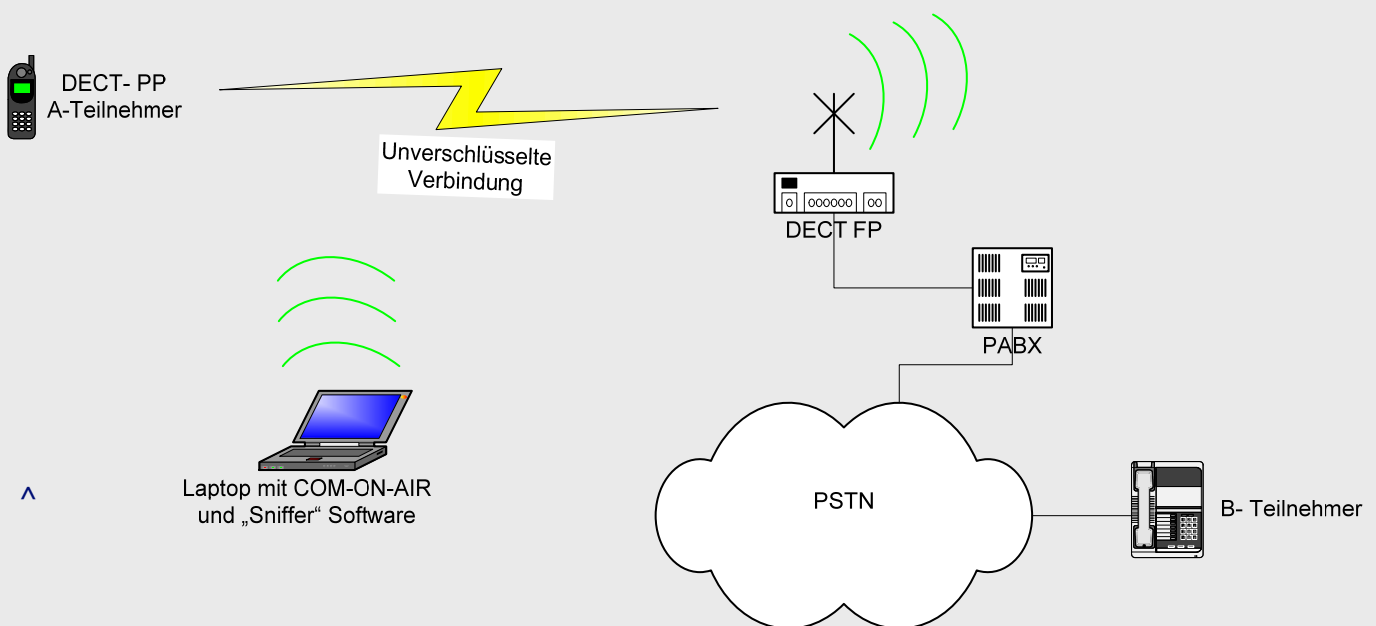
Im Folgenden werden einige der bestehenden Bedrohungen aufgeführt und im Anschluss die Auswirkungen auf DECT-Geräte und -Systeme betrachtet.

## Newsletter 08.09

### 2 Bedrohungsszenarien

#### 2.1 Abhören mittels COM-ON-AIR PCMCIA Card „laut Frontal 21“

Beim Abhören mittels COM-ON-AIR PCMCIA Card wird diese durch eine frei erhältliche Sniffer-Software umprogrammiert. Ein Angreifer ist damit in der Lage, im näheren Umkreis geführte DECT-Gespräche aufzuspüren und deren Inhalt aufzuzeichnen (siehe Abbildung). Voraussetzung hierfür ist, dass die Übertragung unverschlüsselt stattfindet. Viele DECT-Geräte nutzen per Default keine Verschlüsselung oder es sind erst gar keine Verschlüsselungsalgorithmen implementiert worden.



Abhören mittels COM-ON-AIR Sniffer

## Newsletter 08.09

Aus den „gesniffen“ Informationen kann nicht nur die Sprache extrahiert werden, sondern auch Daten zur Identität des Mobilteils. Mit diesen Angaben kann sich wiederum ein „gefälschtes“ Endgerät eines Angreifers in der Basisstation einbuchen und mit der gefälschten Kennung telefonieren. So können vom „gefälschten“ Endgerät aus:

- eingehende Anrufe angenommen;
- abgehende Anrufe im Namen (Nebenstellenummer) des angegriffenen Gerätes und auf Kosten des Angegriffenen geführt werden.

Um zu erfahren, ob die vorhandenen Endgeräte über Verschlüsselungsmöglichkeiten verfügen, stehen Listen von Herstellern oder unabhängigen Stellen zur Verfügung. Die Internetseite [deDECTed.org](http://deDECTed.org) hat dazu aufgerufen, ihr Geräte zum Testen zur Verfügung zu stellen. Die Zeitschrift ComputerBILD hat den Test von 40 Geräten gesponsort und die Ergebnisse in der Ausgabe vom 2. März 2009 veröffentlicht.

Die oben genannte PCMCIA-Karte wird laut neueren Internetbeiträgen nicht mehr produziert. Weltweit sollen 20.000 Stück im Umlauf sein. Es ist jedoch davon auszugehen, dass in kürzester Zeit Treiber für weitere Hardware zur Verfügung stehen werden.

### 2.2 Man-in-the-Middle Attacke

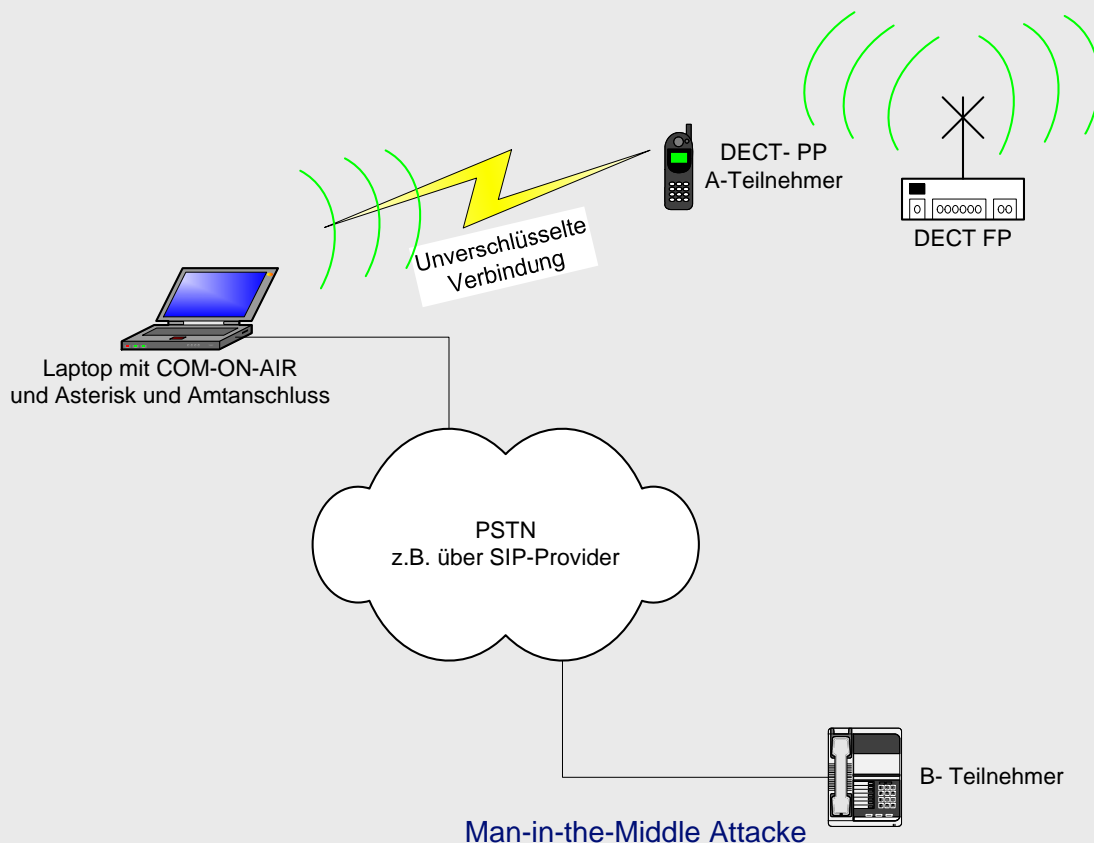
Man-in-the-Middle Attacken sind möglich, indem sich die Angreiferhardware gegenüber den angegriffenen Endgeräten als Basisstation „ausgibt“. Dafür sendet die Angreiferhardware die gleiche Identifizierung wie die der eigentlichen Basisstation aus.

Da die Endgeräte sich in die Basisstation mit den besten Empfangswerten einbuchen, muss seitens des Angreifers sichergestellt werden, dass die Angreiferstation mit einem höheren Empfangspegel als die ursprüngliche Basisstation am angegriffenen Mobilteil empfangen wird. Die angreifende Station muss sich also im Umkreis der eigentlichen Basisstation befinden und mit entsprechend hoher Sendeleistung (ggf. mehr als im DECT-Standard vorgesehen) senden. Reichweiten könnten hier bei gezielten Angriffen über Richtantennen vergrößert werden.

Bucht sich das Mobilteil in die angreifende Station ein, fordert diese es auf sich zu authentifizieren. Das Endgerät sendet seine Authentisierungsinformationen. Die angreifende Station akzeptiert diese (ohne Prüfung). Anschließend wird dem Endgerät signalisiert, dass die angreifende Station keine Verschlüsselung unterstützt und die Übertragung daher unverschlüsselt erfolgen muss. Das Endgerät wird nun unverschlüsselt kommunizieren, ein Knacken des Schlüssel ist somit nicht erforderlich.

Verfügt die Angriffshardware über eine Verbindung in das angegriffene TK-Netz, können so vom Mobilteil ausgehende Anrufe über die angreifende Station umgeleitet und unbemerkt mitgehört werden.

## Newsletter 08.09



Der angerufene Teilnehmer könnte nur anhand der CLIP-Informationen erkennen, dass der Anruf aus einem anderen Netz kommt als erwartet (vorausgesetzt der Angerufene verwendet ein CLIP-fähiges Endgerät). Auch bei Verwendung der CLIR-Funktion (Rufnummernunterdrückung) würde der angerufene Teilnehmer auf die fehlende Rufnummernanzeige aufmerksam werden. Es gibt aber auch bei einigen Anlagenanschlüssen die Möglichkeit, die Information zu überschreiben (CLIP-no screening).

Ein so angegriffenes Endgerät befindet sich quasi in einem anderen Netz, welches die gleiche RFPI (Netzkennung) ausstrahlt. Das Endgerät ist somit bei einem Anruf aus dem eigentlichen Netz (unter der regulären Rufnummer) nicht erreichbar. Mit der Man-in-the-Middle Attacke lassen sich also nur Anrufe abhören, die von dem betroffenen Endgerät initialisiert werden. Diese Attacke kann erkannt werden, wenn beim Anruf des betroffenen Endgerätes nur der Tischapparat „klingelt“ und das DECT Endgerät keine Reaktion zeigt.

## Newsletter 08.09

Laut telefonischen Aussagen von Mitarbeitern der TU Darmstadt soll es auch Möglichkeiten geben, Protokoll-Nachrichten in den Datenstrom mit einzuschleifen, um über diesen Weg die Verschlüsselung auszuschalten.

Zu verhindern ist dieser Angriff nur, wenn die Verschlüsselung per Firmware immer eingeschaltet ist und nicht abgeschaltet werden kann.

### 2.3 Sicherheitsrisiko Repeater

Beim Einsatz von DECT-Repeatern sind Verbindungen nicht verschlüsselt. Der Repeatermodus kann per Default bei vielen Basisstationen abgeschaltet werden. Bei einem Angriff von „Innen“ könnte der Repeatermodus am Telefon eingeschaltet werden.

### 2.4 Sicherheitsrisiko bei GAP

Generic Access Profile (GAP) bietet die Möglichkeit, Endgeräte anderer Hersteller an Basisstationen mit verringertem Leistungsumfang anzumelden. Verschlüsselung soll in diesem Fall optional sein, was noch im Standard zu prüfen wäre. Bei diesem Szenario wäre jedes eingebuchte GAP-Endgerät im Unternehmen zu prüfen.

### 2.5 Schwachstelle bei der Implementierung der Schlüssel

Bei einigen Implementierungen des Protokollstacks ist die Verschlüsselung laut telefonischer Aussage der TU Darmstadt so schwach, dass sie bereits mit einfachen Mitteln geknackt werden kann. Der ursprünglich 128 Bit lange Schlüssel hat nur eine netto Schlüssellänge von 23 Bit, die restlichen Schlüsselbits können anhand der vorhandenen Daten bestimmt (bzw. ausgerechnet) werden.

## 3 Auswirkungen auf die DECT-Nutzung in Unternehmen

Grundsätzlich ist es möglich, Gespräche die über DECT geführt werden, abzuhören. Je nachdem welche Sicherheitsmechanismen in den Geräten implementiert und auch aktiviert sind, können die oben genannten Attacken verhindert werden. Solche Angriffe erfordern zur Zeit noch tieferegehende IT-Kenntnisse, kriminelle Energie und relativ viel Aufwand.

Um das Risiko des Abhörens von DECT-Endgeräten zu minimieren, sollte überprüft werden, ob alle Endgeräte, die im Unternehmen im Einsatz sind, verschlüsselt übertragen. Bei neueren DECT-Endgeräten ist zusätzlich der so genannte Eco-Mode eine Möglichkeit den potenziellen Angreifern die Attacken zu erschweren. Die Endgeräte senden dann nur mit sehr geringer Leistung; Angreifer können die Endgeräte somit nur schwer erkennen.

## Newsletter 08.09

Die Firma Gigaset Communications GmbH hat eine Liste der Endgeräte veröffentlicht, bei denen werkseitig eine DECT-Verschlüsselung implementiert ist (siehe Tabelle 1). Ferner wurden an der TU Darmstadt einige DECT-Endgeräte auf Sicherheitslücken überprüft. Die Ergebnisse wurden in der ComputerBILD veröffentlicht. Es ist sinnvoll, künftig nur Endgeräte zu beschaffen, die über eine Verschlüsselung verfügen. Ältere Modelle, die aktuell im Einsatz sind und als unsicher eingestuft wurden, sollten in kritischen Bereichen wie Geschäftsführung beim Umgang mit personenbezogenen Daten oder in der Forschung/Entwicklung nicht weiter verwendet werden.

Im Folgenden die von der TU Darmstadt getesteten Endgeräte:

Nr.	Hersteller	Modell	ist sicher vorm Einbuch gefälschter Endgeräte	ist sicher vor "Man in the Middle" Attacken	verschlüsselt Gespräche	Angerufene Telefonnummer wird verschleiert gesendet
		<i>Spalte -&gt;</i>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
1	AEG	Colombo Coral	nein	nein	nein	nein
2	AEG	Crombo 3400	nein	nein	ja	ja
3	AEG	Fame 400	nein	nein	nein	ja
4	AEG	Fame 405	nein	nein	nein	nein
5	AEG	K125 AB	nein	nein	ja	ja
6	Audioline	Big Tel 100	nein	nein	ja	ja
7	Audioline	Slim DECT 500	nein	nein	ja	ja
8	AVM	7270 mit Fon MT-D	ja	nein	ja	ja
9	B&O	BeoCom 600	nein	nein	ja	nein
10	DeTeWe	Beetel 650 Eco	nein	nein	ja	ja
11	DeTeWe	Style 250	nein	nein	ja	ja
12	Doro	Phone Easy DECT315	nein	nein	ja	ja
13	Grundig	Calios 1	nein	nein	nein	ja
14	Grundig	Sinio 1	nein	nein	nein	nein
15	Hagenuk	Stick SR	nein	nein	nein	nein
16	iDECT	x2i	nein	nein	ja	ja
17	Loewe	Alphatel 5000	nein	nein	nein	nein
18	Medion	MD 81877	nein	nein	ja	ja
19	Motorola	D701	nein	nein	nein	nein
20	Motorola	D811	nein	nein	ja	ja
21	Orchid	LR 4610	nein	nein	ja	ja
22	Panasonic	KX-TG 8222	nein	nein	nein	nein

## Newsletter 08.09

Nr.	Hersteller	Modell	ist sicher vorm Einbuchen gefälschter Endgeräte	ist sicher vor "Man in the Middle" Attacken	verschlüsselt Gespräche	Angerufene Telefonnummer wird verschleiert gesendet
23	Philips	SE250/SE255	nein	nein	nein	nein
24	Philips	Zenia Voice	nein	nein	nein	nein
25	Sagem	D23XL	nein	nein	ja	ja
26	Siemens	Gigaset 3010	nein	nein	nein	nein
27	Siemens	Gigaset A260	ja	nein	ja	nein
28	Siemens	Gigaset A580	ja	nein	ja	nein
29	Siemens	Gigaset C450 IP	ja	nein	ja	nein
30	Siemens	Gigaset E360	ja	nein	ja	nein
31	Siemens	Gigaset S675 IP	ja	nein	nein	nein
32	Siemens	Gigaset S680	ja	nein	ja	ja
33	Siemens	Gigaset SL785	ja	nein	ja	ja
34	Swissvoice	Avena 357	nein	nein	ja	ja
35	Swissvoice	Eurit 577 ISDN	ja	nein	ja	ja
36	Swissvoice	Eurit 758 Duo	nein	nein	ja	ja
37	T-Home	Sinus 45	ja	nein	nein	nein
38	T-Home	Sinus 101/102	nein	nein	ja	ja
39	T-Home	Sinus 212	nein	nein	ja	ja
40	T-Home	Sinus 421	nein	nein	ja	ja
41	T-Home	Sinus 501	ja	nein	ja	ja
42	T-Home	Sinus 700 S	nein	nein	nein	nein
43	T-Home	Sinus 710 Komfort	nein	nein	nein	nein
44	T-Home	Sinus A301	ja	nein	ja	ja
45	T-Home	Sinus C31	nein	nein	nein	nein
46	TCM	219295	nein	nein	nein	nein
47	Tiptel	Decline	nein	nein	nein	nein
48	Topcom	Butler 800 Twin	nein	nein	ja	nein

## Newsletter 08.09

Erläuterungen zu den Tabellenspalten:

- Spalte 1 – Das „Fälschen“ von Endgeräten ist in 2.1 erläutert;
- Spalte 2 – die Man-in-the-Middle Attacke ist in 2.2 erläutert;
- Spalte 3 – Verschlüsselung von Gesprächen.

Die hier mit „nein“ markierten Geräte verschlüsseln die Übertragung gar nicht.

- Spalte 4 – Verschleierung von Telefonnummern.

Werden die Rufnummern unverschlüsselt übertragen, kann ein Angreifer (siehe Absatz 2.1) die angerufenen Rufnummern „sehen“.

Die in Unternehmen häufig verwendeten DECT-Headsets der Firmen

- Plantronics,
- GN Netcom

zählen nicht zu den getesteten Geräten. Beide Hersteller geben an, dass die Headsets verschlüsselt übertragen. Plantronics gibt an, dass ein 64-Bit Schlüssel eingesetzt wird. Sicherer als Schlüssel dieser Länge sind 128 Bit Schlüssel, deren alternativer Einsatz empfohlen wird. Bei GN Netcom liegen keine Informationen zum verwendeten Schlüssel vor.

#### **4 Fazit**

Das Gefahrenpotenzial des Abhörens von Gesprächen über DECT-Endgeräte ist grundsätzlich vorhanden. Hierbei sind insbesondere ältere Geräte und Geräte aus dem Heimnutzerebereich gefährdet.

Die Tabelle zeigt auch, dass keines der aufgelisteten Endgeräte über alle überprüften Eigenschaften im Sinne der Absicherung verfügt. Ob auch integrierte DECT-Systeme von den Attacken betroffen sind, konnte bisher nicht geklärt werden. Dieses sollte in Zusammenarbeit mit dem Lieferanten/Systemintegrator abgeklärt werden.

Grundsätzlich ist die Reichweite der DECT-Geräte begrenzt. Ein Angreifer müsste sich also in den meisten Fällen auf dem Gelände des Unternehmens befinden, um überhaupt ein DECT-Signal empfangen zu können.

## Newsletter 08.09

Der Einsatz von DECT-Telefonen am Arbeitsplatz in Bereichen, die einem besonderen Datenschutz unterliegen, sollte ohne detaillierte Prüfung der eingesetzten Geräte nicht vorgenommen werden.

Insgesamt scheint es ratsam zu sein

- sämtliche Endgeräte auf Verschlüsselung zu prüfen und ggf. auszutauschen;
- für sehr sensible Gespräche sollte DECT überhaupt nicht verwendet werden;
- Alternativ können Endgeräte, wie das DECT-Endgerät Gigaset SL965 (ehemals Siemens, heute Gigaset Communications) oder andere Alternativen, beispielsweise von Rohde&Schwarz, die eine Ende-zu-Ende-Verschlüsselung ermöglichen;

eingesetzt werden.

## Newsletter 08.09



Dr.-Ing. Jan Steuer  
Geschäftsführer

### **DOK SYSTEME unterstützt die EWETEL von der Angebotserstellung bis zum Zuschlag für das neue Sprach- und Datennetz der Landesverwaltung Niedersachsen**

Der niedersächsische Innenminister Uwe Schünemann hat im Rahmen der CeBIT 2009 bekannt gegeben, dass die oldenburgische Firma EWE TEL GmbH als Generalunternehmer die neue Telekommunikationsinfrastruktur in der niedersächsischen Landesverwaltung bereitstellen wird. Nachfolgend einige Auszüge aus der Pressemitteilung.

"Die Niedersächsische Landesregierung hat in den Jahren 2005 und 2006 die strategische Neuausrichtung des IT-Betriebes der Landesverwaltung beschlossen. Eine der Kernkomponenten ist die Zusammenführung der Informationstechnologie mit der Sprachkommunikation", sagte Schünemann in Hannover. Die neue Telekommunikationsinfrastruktur vereinige dann den Datenverkehr, zum Beispiel E-Mail oder Internet, und die Sprachkommunikation, das Telefon.

Für die Einführung ist ein Zeitraum von insgesamt drei Jahren bis Ende 2012 eingeplant. Angestrebt werden qualitative Verbesserungen und deutlich steigende Bandbreiten der Datenübertragung, die zur Bewältigung der immer weiter fortschreitenden "Datenflut" unabdingbar sind.

Nach einer europaweiten Ausschreibung, die der Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) im Auftrag des Innenministeriums durchgeführt hat, konnte sich die Firma EWE TEL GmbH als Generalunternehmer gegen fünf Mitbewerber durchsetzen. Die Firma EWE TEL wird für die Betreuung der Sprach- und Datenkommunikation des Landes Niedersachsen eine Projektgesellschaft gründet. Sie bindet unter anderem die Firmen BCC Business

## Newsletter 08.09

Communication Company GmbH (Braunschweig) für den Betrieb des Datennetzes und Nextira One Deutschland GmbH für den Bereich der Telefonie mit ein. Der Vertrag umfasst bei einer Laufzeit von sechs Jahren ein Gesamtvolumen von ca. 164 Mio. Euro. Es besteht eine Verlängerungsoption von zwei mal zwei Jahren. Die Vertragsunterzeichnung wird derzeit von beiden Partnern vorbereitet.

"Die gesamte Telekommunikationsinfrastruktur für die niedersächsische Landesverwaltung wird modernisiert und leistungsfähiger gemacht", so der Innenminister. So wird zum Beispiel künftig die Technologie Voice over IP, also das Telefonieren über die Datenleitung, eine zentrale Rolle spielen. Im Endausbau werden ca. 75.000 Anschlüsse in etwa 2.500 Liegenschaften einen Zugang zur neuen Netzinfrastruktur haben, inklusive Polizei, Justiz und Steuerverwaltung. Entsprechend aufwändig war das Ausschreibungsverfahren: Basierend auf einem Anforderungskatalog, der in einem über 600 Seiten starken Leistungsverzeichnis dargestellt wurde, hat die Auswahl über mehrere Verhandlungsrunden einen Zeitraum von mehr als eineinhalb Jahren in Anspruch genommen. Die Vorbereitungszeit betrug insgesamt drei Jahre."

DOK SYSTEME hat die EWE TEL bzw. das Konsortium im gesamten Angebotsprozess unterstützt. Schwerpunkte der Tätigkeit waren dabei die Angebots-Urkalkulation für alle Bereiche (LAN, WAN, Security, zentrales IP-TK-System, Security und Mobilfunk) für das Portmodell, Qualitätssicherung, Projektbüro, Dokumentenmanagement, strategische Beratung und Verhandlungsunterstützung.

## Newsletter 08.09

### Seminare und Veranstaltungen: Programm 02/2009

Titel	Termin
<b>NEU</b> <b>Intensiv Workshop Management, Kalkulation und Controlling von ITK-Projekten</b>	<b>19.-23.10.2009</b>
<b>KT</b> <b>Kommunikationstreff 2009</b>	<b>23.-24.09.2009</b>
T1        Hybride TK-Anlagen versus IP-Telefonie	16.08.2009
T2        Dienste und Anwendungen im TK-Umfeld (UMS, CTI, IVR, ...)	17.08.2009
N2        Einführung in die TCP/IP-Protokollwelt	22.08.2009
N4        Einführung in die SIP-Technologien	23.08.2009
N9        Prüfung von Netzen auf VoIP-Tauglichkeit	24.08.2009
M1/2     Funksysteme und Funkanwendungen im Überblick	29.-30.08.2009
MB3     Hürden in der Vergabe öffentlicher Aufträge zu IT-Leistungen, Schwerpunkt EU-weite Ausschreibungen	15.09.2009
G1        Gebäude-, RZ- und Objektsicherheit	01.10.2009
M3        Ablösung des analogen Betriebs- und Bündelfunks (TETRA, TETRAPOL, GSM-ASCI; DMR; Alternativen)	10.11.2009
TK2     Intensivkurs Telekommunikation	12.-13.11.2009 24.11.2009
MB2     Vergabe von IT- und TK-Dienstleistungen – Ausschreibungserfahrungen	25.11.2009
N6        Next Generation Networks (NGN) intensiv	26.11.2009

## Newsletter 08.09

### “Fach-Chinesisch” und „Kürzelknacker“

#### LTE

LTE steht für Long Term Evolution und bezeichnet den heute bereits absehbaren Nachfolgestandard von UMTS bzw. HSDPA /HASUPA, oder anders gesagt den Mobilfunkstandard der vierten Generation.

LTE zielt insbesondere auf eine für Mobilfunkprovider kostengünstigere Bereitstellung von breitbandigen Internetdiensten und Echtzeitapplikationen ab.

Technisch basiert LTE auf ähnlichen Verfahren wie UMTS. Durch verbesserte Antennentechnik, die so genannte MIMO-Technik (Multiple Input Multiple Output) und das Modulationsverfahren OFDM, (Orthogonal Frequency Division Multiplex) unterstützt LTE im Gegensatz zu UMTS verschiedene Übertragungsbandbreiten. Das Spektrum reicht von 1 MHz bis zu 20 MHz. Dadurch können kostbare Frequenzbandbreiten sehr flexibel genutzt werden. Die für LTE öffentlich kommunizierten maximalen Übertragungsraten in Downloadrichtung von theoretisch bis 300 Mbit/s und 75 Mbit/s beim Upload, sind nur mit der vollen Bandbreite von 20 MHz realisierbar. In Freilandversuchen in Deutschland wurden praktisch Datenraten von rund 175 Mbit/s nachgewiesen.

Ein weiterer Aspekt, der zur Attraktivität von LTE beiträgt, sind Überlegungen, die in Deutschland durch Abschaltung des analogen Fernsehens frei werdenden Trägerfrequenzbereiche zwischen 790 und 862 MHz für den neuen Mobilfunkstandard LTE frei zu geben. Im Gegensatz zu den heute für GSM und UMTS verwendeten Trägerfrequenzbereichen von 1.900 MHz bis 2.500 MHz ließen sich damit wesentlich größere Funkzellen realisieren.

Die Ansichten, wann LTE in Deutschland auf breiter Front verfügbar sein wird, gehen heute weit auseinander.

- Einerseits wurde aktuell LTE noch nicht als verbindlicher Standard verabschiedet, geplant ist dies jedoch bis Ende 2009.
- Andererseits ist für das Jahr 2010 die Inbetriebnahme der ersten kommerziellen Netze durch den japanischen Netz-Betreiber NTT DOCOMO angekündigt.

Zu diesem Zeitpunkt sind auch die ersten Markteinführungen im Endgerätesektor zu erwarten. In den USA wurde bereits 2008 ein Frequenzband für LTE zentral für 19,6 Milliarden Dollar versteigert. Der Betreiber Verizon Wireless wird hier ebenfalls 2010 mit dem großflächigen Roll-Out beginnen.

**Vielen Dank für Ihre Aufmerksamkeit und bis zur nächsten Ausgabe. Ihr DOKinfo!-Team**

#### Impressum / Herausgeber:

**DOK SYSTEME Ingenieurgesellschaft für Kommunikationstechnik mbH**

**Steinriede 7 • 30827 Garbsen**

**Tel.: 05131 / 4933-0 • Fax: 05131 / 4933-99**

**E-Mail: [info@doksysteme.de](mailto:info@doksysteme.de)**

Alle Rechte vorbehalten.

Die Urheberrechte dieser Publikation liegen vollständig bei der DOK SYSTEME GmbH.

Haftungsausschluss: Für inhaltliche Fehler wird keinerlei Haftung übernommen. Irrtümer sind vorbehalten.

Haftungshinweis: Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.