

NACHRICHTEN

Vorsicht bei DECT-Telefonie!



28.01.2009 - Sicherheitsexperten des **Chaos Computer Club (CCC)** demonstrierten den interessierten Teilnehmern des **25. Chaos Communication Congress** in Berlin, wie sich Telefonate auf Basis des weit verbreiteten Standards für Schnurlostelefone „Digital Enhanced Cordless Telecommunication“ (DECT) abhören und mitschneiden lassen.

Der DECT-Standard wurde Ende der 80er Jahre als europaweit einheitlicher Standard konzipiert, um die bis dahin vorhandenen verschiedenen analogen schnurlosen Telefonsysteme wie etwa CT1 und CT1+ zu ersetzen. Der im Jahre 1992 vom European

Telecommunications Standards Institute (ETSI) verabschiedete DECT-Standard spezifiziert ein vollständig digitales Mobilfunknetz zur Übertragung von Sprache und Daten, das sich im Vergleich zu analogen Schnurlostelefon-Standards durch eine hohe Sprachqualität und Optionen für eine höhere Abhörsicherheit auszeichnet. Als typische Einsatzorte von DECT sind in erster Linie Bürogebäude und Firmengelände sowie Heimbereiche zu nennen. Gerade in Privathaushalten erfreuen sich DECT-Telefone einer hohen Beliebtheit.



Lauschangriff für 23 Euro

Zum Belauschen der DECT-Gespräche verwendeten die an der Entdeckung beteiligten Forscher von der TU Darmstadt ein Notebook mit Linux, eine manipulierte PCMCIA-Karte des Herstellers Dosch Amand (links oben) - der Straßenpreis dafür beläuft sich auf etwa 23 Euro - und einer Weiterentwicklung des bekannten WLAN-Sniffers Kismet (links unten).



„Bei Analysen“, so die Sicherheitsexperten, „sei aufgefallen, dass es bei DECT-Geräten zuweilen keinen Authentisierungs- oder Verschlüsselungsprozess zwischen der Sendestation und dem Handgerät gibt. In den meisten Fällen authentisiert sich das Schnurlostelefon nur gegenüber der Basisstation, auch wenn der DECT-Standard grundsätzlich eine gegenseitige Authentifikation der Gerätschaften vorsehe“. Bei anderen Anlagen erfolge zwar eine Authentisierung der Station, allerdings ohne die zu diesem Zweck vorgesehene Verschlüsselung. Die Sicherheitsexperten führten fort, dass man in all diesen Fällen aktive Gespräche, die über DECT-Telefone geführt werden, aufspüren und mitschneiden

könne, eine vertrauliche Kommunikation über DECT-Gerätschaften somit nicht gewährleistet sei.

Stellungnahme vom DECT Forum

Das **DECT Forum**, der internationale Verband der Home-Communication-Industrie, versucht zu beschwichtigen und stuft das Abhörrisiko von DECT-Telefonaten als gering ein. Die **Stellungnahme des DECT-Forums** wirkt hierbei jedoch alles andere als überzeugend: So wird vom Verband argumentiert, dass das Abhören von Telefongesprächen eine Straftat darstelle und es nicht möglich sei, Telefongespräche zufällig abzuhehren. Der Verband führt weiterhin fort, dass „nur Personen, die mit krimineller Energie und Absicht handeln sowie über detaillierte technische Kenntnisse und Ausstattungen verfügen, überhaupt in der Lage seien, Gespräche abzuhehren“. Der Verweis auf die Strafbarkeit hilft Betroffenen, deren DECT-Telefonate von einem Unbekannten abgehört werden, jedoch recht wenig: Wie bei WLAN können DECT-Gespräche aus der Entfernung abgehört werden. Die Wahrscheinlichkeit, den passiv durchgeführten Lauschangriff zu entdecken, ist somit extrem unwahrscheinlich.

Einschätzung vom Bundesamt für Sicherheit in der Informationstechnik (BSI)

„Die Tatsache, dass DECT-Gespräche durch minimalem Invest unbemerkt belauscht werden können, kommt für uns nicht überraschend“, beschreibt Vincenzo Abate, Director der auf Informationssicherheit spezialisierten buw consulting GmbH die aktuelle Entwicklung. „So hat beispielsweise das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** in der Vergangenheit bereits mehrfach darauf hingewiesen, dass bei DECT – als funkbasiertes Verfahren – grundsätzlich die Gefahr besteht, dass „unberechtigte“ DECT-fähige Geräte die DECT-Kommunikation mithören oder sich aktiv in die Kommunikationsverbindung einschalten“. „Ausschlaggebend für die frühen Sicherheitsbedenken der Behörde“, führt Vincenzo Abate fort, „sind seit jeher die geringe, von Experten allenfalls für ein mittleres Sicherheitsniveau als ausreichend angesehene Schlüssellänge, als auch der verwendete und nicht-öffentliche Verschlüsselungsalgorithmus DSC (DECT Standard Cipher). Kunden, die vertrauliche Gespräche über DECT-Telefone führen wollten, hatte die buw consulting GmbH schon seit jeher von diesem Vorhaben abgeraten“.

IT-Bedrohungen nicht isoliert betrachten

Aktuelle Bedrohungen wie die Schwächen beim DECT-Standard zeigen erneut, wie bedeutsam ein

ganzheitlicher Ansatz für ein effektives Sicherheitsmanagement ist: Nicht nur die IT-Prozesse selbst, sondern auch infrastrukturelle, personelle und organisatorische Aspekte der gesamten IT-Umgebung müssen berücksichtigt werden – um beispielsweise auch unscheinbare Sicherheitsrisiken durch den Einsatz von DECT-Telefonen, die in der Vergangenheit nur zu oft als verlässlicher Träger einer vertraulichen Kommunikation fehleingeschätzt wurden, aufzudecken und bewerten zu können. Für ein nachhaltiges Informationssicherheitsmanagementsystem (ISMS) empfiehlt die buw consulting GmbH eine Orientierung an internationalen anerkannten Standards, wie beispielsweise der ISO 27001 auf der Basis von BSI IT-Grundschutz. Die Methodik nach IT-Grundschutz und der damit einhergehende Lebenszyklus des Sicherheitskonzepts bietet Unternehmen die Möglichkeit, typische Gefährdungen aufzudecken und mittels Standardsicherheitsmaßnahmen ein ganzheitliches Sicherheitsmanagement umzusetzen – potentielle Gefährdungen durch schnurlose Verbindungen inbegriffen, beispielsweise in Form einer Risikoanalyse.

© GWV Fachverlag

**Über den Autor:**

Andreas G. Weyert ist lizenziertes BSI IT-Grundschutz-Auditor und Security Consultant bei der **buw consulting**.

Autor(en): *Andreas G. Weyert*