Rundschreiben Nr. 20/2012 des Landeskirchenamtes an die Kirchengemeinden, Kirchenkreise und kirchlichen Verbände betreffend kirchlicher Datenschutz: Sicherheitslücken bei Schnurlostelefonen und Mobiltelefonen[1]

Vom 03.07.2012 (Az.: 610.215/07)

Das Abhören von mit Schnurlostelefonen und Mobiltelefonen geführten Gespräche wird immer einfacher. Dies liegt darin begründet, dass zum einen die Kosten für die zum Abhören erforderliche Hardware gefallen sind (bereits ab 30,00 € über das Internet erhältlich) und zum Anderen die dafür benötigten Programme über das Internet heruntergeladen werden können. Das Abhörverbot des Telekommunikationsgesetzes (TMG) und die Regelungen des Strafgesetzbuches (StGB) schrecken hierbei vermutlich kaum ab, auch wenn das Abhören mit Freiheitsstrafe bis zu drei Jahre oder mit Geldstrafe bedroht ist (§ 89 TMG; § 201 StGB).

1. Welche Sicherheitsrisiken bestehen bei Schnurlostelefonen?

Mit Rundschreiben vom 27. März 2003 (Az.: A 14-03/01.09; im Fachinformationssystem-Kirchenrecht z. Z. noch unter der Nr. 855.5 aufrufbar) hatten wir bereits ausgeführt, dass vertraulich geführte Gespräche mit schnurlosen Telefonen, die mit der älteren analogen Übertragungstechnik betrieben werden, ohne großen Aufwand abgehört werden können. Derartige Telefone, die z. B. mit dem Standard „CT1+“ arbeiten, sind seit dem 01.01.2009 nicht mehr zugelassen, aber zum Teil noch im Einsatz.

Damals hatten wir ausgeführt, dass schnurlose Telefone, die die Sprache digital mit dem DECT-Standard (Digital Enhanced Cordless Telecommunication) übertragen, einen gewissen Schutz über einen Verschlüsselungsmechanismus bieten. Spätestens seit 2009 ist bekannt, dass über DECT geführte Telefonate mit geringem Kostenaufwand und verhältnismäßig geringen Vorkenntnissen von Hackern abgehört werden können. Ein Problem hierbei ist auch, dass einige Hersteller aktueller DECT-Produkte die optional standardisierte Verschlüsselung nicht einsetzen. Für die Personen, die mit Schnurlostelefonen kommunizieren, ist es dabei nicht erkennbar, ob das verwendete Gerät die Verschlüsselungsmöglichkeiten von DECT nutzt oder ob die Daten völlig unverschlüsselt übertragen werden. Auch ist es für Hacker verhältnismäßig leicht, Telefonate auf ihre Basisstation umzuleiten oder kostenlos zu telefonieren, wenn es ihnen gelingt, das Mobilteil der kirchlichen

1 Redaktioneller Hinweis: Am 24. Mai 2018 ist das neu gefasste EKD-Datenschutzgesetz vom 15. November 2017 (Nr. 850) in Kraft getreten. Es wird zurzeit geprüft, ob und inwieweit eine Aktualisierung der Regelungen des Rundschreibens an das neue kirchliche Datenschutzrecht erforderlich ist.

Stelle bei ihrer Basisstation anzumelden. Auch bei mustergültig verschlüsselten Gesprächen sind Sicherheitslücken gefunden worden, so gibt es Schnurlostelefone, bei denen der Hacker jede gewählte Rufnummer direkt mitlesen kann.

1.1 Welche Schnurlostelefone sind betroffen?

In einem aufwendigen Test[1] wurden im Jahr 2009 fünfzig Schnurlostelefone auf Sicherheitslücken überprüft. Jedes Schnurlostelefon hatte mindestens eine Sicherheitslücke, manche auch mehrere, so dass keines der eingesetzten Telefon als sicher einzustufen war.

1.2 Welche Empfehlungen sollten bei der Nutzung von Schnurlostelefonen beachtet werden?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist bereits seit 2003 auf Sicherheitsrisiken beim Einsatz von DECT-Telefonen hin[2].

Bei der Benutzung von Schnurlostelefonen wird Folgendes empfohlen:

1. *Schnurlostelefone sollen bei Gesprächen mit sensiblen Inhalten (z. B. Seelsorgegesprächen) nicht mehr verwendet werden.*
2. *Analoge Schnurlostelefone sollten kurzfristig ersetzt werden.*

Stattdessen sollten schnurgebundene Telefone eingesetzt werden, die normalerweise als sicher gelten, da der Telefon-Hausverteiler in der Regel nicht frei zugänglich sein wird, um dort ein Messtelefon zum Abhören der Gespräche anstöpseln zu können.

Soweit Schnurlostelefone mit der DECT-Technik für Gespräche mit nicht sensiblen Inhalten verwendet werden, ist zu berücksichtigen, dass sich die DECT-Sicherheitslücken nicht abstellen lassen. In der Anlage 1 sind einige Maßnahmen aufgeführt, die einfach umzusetzen sind und es Gelegenheitshackern schwerer machen sollen, die Sicherheitslücken für sich auszunutzen.

2. Welche Sicherheitsrisiken bestehen beim Mobiltelefon?

Im Mobilfunk ist die Sicherheitslage erst seit kurzer Zeit als kritisch einzustufen. Zwar wird beim Mobilfunk flächendeckend die Verschlüsselung eingesetzt, aber der verwendete einfache Algorithmus stammt aus den 80er Jahren und genügt nicht mehr den aktuellen Ansprüchen an die Abhörsicherheit. Hacker sind zwischenzeitlich in der Lage, mit Mobiltelefonen geführte Gespräche abzuhören und SMS- oder E-Mail-Daten mitzulesen. Zum Teil ist es auch möglich, Aufenthaltsorte eines Mobilfunkteilnehmers innerhalb bestimmter Grenzen zu ermitteln und sogenannte Bewegungsprofile zu erstellen[3].

2.1 Wie werden Sicherheitslücken von Hackern genutzt?

---

1 Computerbild 6/2009 S. 88 ff.; Testergebnis vom BSI grundsätzlich bestätigt.

2 siehe auch BSI-Sicherheitshinweis vom 24.02.2009, im Internet aufrufbar unter: https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/sicherheitsberatung_node.html

3 siehe auch BSI-Sicherheitshinweis vom 10.07.2009, im Internet aufrufbar unter: https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/sicherheitsberatung_node.html

In GSM-Netzen authentifiziert sich nur das Mobiltelefon gegenüber dem Mobilfunknetz (aber nicht umgekehrt), so dass unter Verwendung sogenannter mobil einsetzbarer IMSI-Catcher die GSM-Verschlüsselung deaktiviert werden kann. Der UMTS-Standard bietet nur einen eingeschränkten Schutz, da die Technik oft einen Wechsel zur Kommunikation über GSM erforderlich macht, wenn beispielsweise der Standort gewechselt wird. Sicherheitslösungen, die am Markt bereits erhältlich sind, setzen aber voraus, dass sowohl die Anruferin oder der Anrufer systemgleiche Telefone nutzen, die beispielsweise über eine zusätzliche Smartcard die Verschlüsselung von Sprache und Daten mit eindeutiger Authentifizierung ermöglichen (Ende-zu-Ende-Verschlüsselung mit 128-Bit-AES - Advanced Encryption Standard -, ein von der Nato geprüfter und zugelassener sicherer Algorithmus für die symmetrische Verschlüsselung von Daten und Sprache). Derartige Sicherheitslösungen sind nur bei dienstlichen Mobiltelefonen denkbar, die von einer kirchlichen Stelle eingesetzt werden (nur die Gespräche zwischen diesen Mobiltelefonen sind als sicher einzustufen). Bei Gesprächen mit Dritten, beispielsweise Gemeindegliedern, steht diese Lösung nicht zur Verfügung.

2.2 Welche weiteren Gefährdungen bestehen bei „modernen“ Mobiltelefonen?

Mobiltelefone sind oft als kleine Computer (iPhone von Apple, Smartphones von anderen Herstellern) anzusehen, die den normalen Gefährdungen aus der IT-Welt ausgesetzt sind. Die Sicherheitsmechanismen bei dem iPhone und den Smartphones sind oft unzureichend, z. B. können über die Geräte- oder SD-Karten-Schnittstellen bzw. durch das Laden von Programmen (Apps) Manipulationen am Mobiltelefon selbst und an der dort eingesetzten Software vorgenommen werden. Die Funkschnittstellen, z. B. Bluetooth oder WLAN, sind oft nur unzureichend abgesichert. Hacker haben die Möglichkeit, das Mobiltelefon per Software zu manipulieren oder über diese Funkschnittstellen die Gespräche abzuhören oder die Daten abzufangen. Den Hackern werden die Angriffe auf mobile Endgeräte verhältnismäßig leicht gemacht, da die unterschiedlichen Betriebssysteme der Geräte in der Regel nur bei schwerwiegenden Sicherheitsmängeln ein Update erhalten und den Nutzerinnern und Nutzern das Gefährdungsbewusstsein oft fehlt.

2.3 Welche Empfehlungen sollten bei der Benutzung von Mobiltelefonen beachtet werden?

Die nicht mehr ausreichende Verschlüsselung, die unsichere Konfiguration der Endgeräte und die mangelnde Sensibilität der Nutzerinnen und Nutzer lässt eine Kommunikation mit Mobiltelefonen ohne ausreichende Sicherheitsmaßnahmen nicht mehr zu. Das BSI und die Datenschutzbeauftragten halten angemessene Schutzmaßnahmen[1] für dringend notwendig.

Bei der Benutzung von Mobiltelefonen (iPhones, Smartphones) wird empfohlen,

---

1 siehe Broschüre des BSI „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen“, im Internet aufrufbar unter https://www.bsi.bund.de/ContentBSI/Publikationen/Broschueren/mobile/index_htm.html

1. Gespräche mit sensiblen Inhalten (z. B. Seelsorgegespräche) über Mobiltelefone nicht mehr zu führen oder bei Anrufen auf die technisch nicht gesicherte Vertraulichkeit hinzuweisen;

2. die notwendigen Maßnahmen zum Umgang und Schutz mit mobilen Telefonen im Rahmen des IT-Sicherheitskonzeptes festzulegen, zum Beispiel

- *für die Kommunikation (Datenübertragung, -speicherung) mit den Mitarbeitenden der kirchlichen Stelle sind hinreichend abgesicherte Endgeräte und Infrastrukturen erforderlich (z. B. zusätzliche Ende-zu-Ende-Verschlüsselung durch Einsatz zusätzlicher Hard- und Software, VPN-tunnel, Verschlüsselung der mobilen Speicher);*
- *zusätzlicher Zugriffsschutz zur Deaktivierung der Displaysperre, Möglichkeit zum Orten, (Fern)Sperren und (Fern)Löschen der Daten bei Verlust oder Stilllegung des Gerätes, ggf. Einsatz von Virenscannern;*
- *Regelungen zur Installation von Anwendungen (Apps) und deren Sicherheitspatches/ Updates (z. B. Ausgabe einer Liste von geprüften Apps);*
- *zentrale Administration der Mobiltelefone (Authentisierung im Rahmen der Passwortrichtlinie, automatische Sperre bei Inaktivität durch Bildschirmschoner oder ähnliche Zugriffssperren, restriktives Rechtemanagement, Backup-Konzept, zentrale Datensicherung);*
- *den installierten Anwendungen nur die Rechte einräumen, die unbedingt erforderlich sind (insbesondere bei kostenlosen Apps werden oft umfangreiche Daten an Dritte übermittelt);*
- *keine Übermittlung personenbezogener Daten an die Gerätehersteller oder an die Hersteller von Apps;*

3. die Nutzerinnen und Nutzer regelmäßig über die Risiken und die festgelegten Sicherheitsmaßnahmen zu informieren;

4. bei dienstlich angeschafften Mobiltelefonen nur die dienstliche Nutzung zuzulassen und die private Nutzung zu untersagen.

Anlage 1

Soweit Schnurlostelefone mit DECT-Standard für Gespräche mit nicht sensiblen Inhalten verwendet werden, sollten folgende Maßnahmen umgesetzt werden:

1. Das Schnurlostelefon sollte nicht im sogenannten Repeater-Modus laufen. Dieser Modus dienst normalerweise zur Reichweitenvergrößerung, aber damit sendet das Schnurlostelefon unverschlüsselt.
2. Die PIN von DECT-Telefonen ist regelmäßig zu ändern, da der Übergabe-PIN oft „0000“ lautet. Eine andere PIN erschwert das unbefugte Anmelden von Mobilteilen.
3. Um weitere Schnurlostelefone anzumelden, muss oft an der Basisstation ein Knopf gedrückt werden. Daher sollte die Basisstation für unbefugte Personen nicht zugänglich sein.
4. Die Inbetriebnahme des Schnurlostelefons an der Basisstation sollte ganz dicht an der Basisstation vorgenommen werden, damit es für Hacker schwieriger wird, sich auf die Basisstation einzuwählen.
5. Sofern auf dem Schnurlostelefon keine Telefonate mehr eingehen, könnte es von Hackern „entführt“ worden sein (Gesprächsumleitung). Wenn das Schnurlostelefon beim Drücken der Suchtaste („Paging“) an der Basisstation klingelt, dürfte dieser Fall ausgeschlossen sein.
6. Im Öko-Modus (Eco-Mode) wird die Sendeleistung auf ein Minimum reduziert. Sofern das Schnurlostelefon in der Basisstation liegt, stoppt der Sender ganz und das Schnurlostelefon ist für Hacker viel schwerer zu orten.