softScheck
we identify vulnerabilities others don't

Pressemitteilung:

Mythos 'Sichere Kommunikation'

Keine Sicherheit für das Kanzler-Handy!

Sankt Augustin, 30. Juni 2014

Der Hinweis aus den Reihen der NSA ist korrekt und wissenschaftlich nachvollziehbar: Das Handy der Kanzlerin ist längst geknackt:

Entscheidend sind die in der Hardware und der Software des Handys enthaltenen Sicherheitslücken! Denn auch das Kanzlerinnen-Handy kann nur dann ausspioniert werden, wenn es eine Sicherheitslücke gibt. Und die gibt es, und diese Sicherheitslücken sind nachgewiesen. Das heißt aber auch: Nur wenn die entscheidenden Sicherheitslücken in dem Handy korrigiert (gepatcht) wären, wäre das Handy tatsächlich angriffssicher!

Dazu müssen die folgenden 5 Fragen gestellt werden:

- Wer hat die Software des Handy systematisch und methodisch auf Sicherheit geprüft: Anwendungssoftware, Betriebssystem, Dateiverwaltung … Das Handy enthält ja einen vollständigen Computer! Und hier gibt es mehrere bekannt Sicherheitslücken.
- Wer hat mit welchen Methoden das Verschlüsselungsprogramm Sicherheits-geprüft? Die Mathematik ist dabei nur ein (kleiner) Teil. Entscheidend ist die entwickelte Software mit allen Sicherheitslücken. Hier können Fehler auftauchen wie seltener Schlüsselwechsel oder eine unzureichende Schlüssellänge. Solche Fehler sind unter Experten lange bekannt und tauchen nicht nur beim Handy der Kanzlerin auf.
- Wer generiert die Schlüssel zur Verschlüsselung? Ist der Hersteller und sind die Tools Sicherheits-geprüft? Werden die Schlüssel zum Handy sicher transportiert? Darauf haben bisher weder der Bundesnachrichtendienst noch das Bundesamt für Verfassungsschutz eine Antwort gegeben.
- Bei einer soliden Sicherheitsprüfung müssen auch alle nicht-dokumentierte Funktionen identifiziert werden. Über eine Hintertür können Nachrichtendienste und Hacker in ein Handy eindringen und mitlesen bzw. mithören, bevor verschlüsselt wird und ohne dass der Nutzer etwas merkt.
- Schließlich muss das Bundesamt für die Sicherheit in der Informationstechnik darüber Auskunft geben, ob und wie verdeckte Kanäle (covert channels) untersucht und identifiziert wurden. Darüber können z.B. die verwendeten Schlüssel offen gelegt werden. Auch hier schweigen die Sicherheitsbehörden. „Schweigen ist aber fatal", meint Prof. Hartmut Pohl, Geschäftsführer der IT-Sicherheitsberatung softScheck GmbH. „Denn nur wenn solche Sicherheitslücken transparent beseitigt werden, kann das Handy der Kanzlerin sicher gemacht werden. Die deutschen Sicherheitsbehörden handeln hier nach dem Urteil vieler Sicherheitsexperten fahrlässig.

Über softScheck

Die IT-Sicherheitsberatung softScheck GmbH identifiziert seit mehr als 10 Jahren bislang nicht-erkannte Sicherheitslücken (Zero-Day-Vulnerabilities) in Software (und auch Hardware).

softScheck führt regelmäßig Sicherheitsprüfungen von Software und Hardware durch. Daneben bietet softScheck selbstverständlich auch die klassische IT-Sicherheitsberatung an vom Grundschutz (ISO 27000-Familie) bis hin zur Hochsicherheit in der Informationsverarbeitung (Redundanz und Diversität) – auch mit Consulting, Coaching und Forensics.

Kontakt

Anja Wallikewitz
Tel.: 02241 – 255 43 – 11
Fax: 02241 – 255 43 – 29
anja.wallikewitz@softScheck.com

softScheck GmbH
Bonner Straße 108
53757 Sankt Augustin
www.softScheck.com