Van-Eck-Phreaking & Co

Verräterische Monitorstrahlung

Das Abhören von Bildschirminhalten funktioniert erstaunlich gut. Eine Methode ist Van-Eck-Phreaking, bei der elektromagnetische Störstrahlung mit einem Empfänger aufgenommen wird, um z.B. Bildschirminhalte heimlich sichtbar zu machen.

Der Name Van-Eck-Phreaking geht auf den niederländischen Wissenschaftler Wim van Eck zurück, der 1985 das Konzept dieser Technik erstmalig beschrieb und die Gefahren aufzeigte.

Jedes elektronische Gerät erzeugt eine elektromagnetische Störstrahlung. Die maximal zulässige Störstrahlung ist im Allgemeinen unter dem Aspekt gesundheitlicher Risiken gesetzlich geregelt; in Deutschland in dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG).

Daneben behandeln die Normen MPR-I/II, TCO 92/95/99 oder TÜV-Ergo die maximal erlaubte Stärke der Abstrahlung von elektronischen Geräten.

Der Gesundheitsschutz ist geregelt – der Abhörschutz nicht

Unter dem Gesichtspunkt Abhörsicherheit gibt es aber keine gesetzlichen Vorschriften. Lediglich das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschäftigt sich in den IT-Grundschutzkatalogen im Maßnahmenkatalog Infrastruktur (M4) im Unterabschnitt Hard- und Software mit Abstrahlsicherheit (M4.89).

Zum Abhören reichen aber Strahlungsstärken aus, die nicht als gesundheitsschädlich gelten. Ein nach den genannten Normen strahlungsarmes Gerät bietet keinen Schutz gegen Van-Eck-Phreaking!

Ein Abhören ist in bis zu 100 Metern Entfernung möglich

Elektromagentische Wellen breiten sich in der Luft aus, gedämpft durch Gebäudewände. Ein empfindlicher Empfänger kann die Störstrahlung eines Monitors aber auch noch in 100 Metern Entfernung auswerten.

Auf der CeBit 2006 demonstrierte Markus Kuhn von der Universität Cambridge mit relativ einfacher Elektronik das Abhören von Monitoren. Überzeugen Sie sich selbst von der Qualität im Internet (siehe Linktipps).

Auch Strahlung von Monitoren kann Geschäftsgeheimnisse verraten.

Leichtes Spiel bei metallischen Leitern

Darüber hinaus breiten sich elektromagnetische Wellen sehr gut entlang metallischer Leiter aus. Hierzu zählen Kabel, Lüftungsschächte und Heizungs- bzw. Wasserrohre.

Die Einspeisung kann direkt geschehen, z.B. über das Netzteil des Geräts in die Stromversorgungskabel, oder indirekt, weil eine Überkoppelung auf einem parallelen Leiter geschieht. Dies passiert, wenn z.B. ein Monitorkabel parallel zu einem anderen liegt.

Verräterisches Monitor-Flackern

Im Jahr 2002 stellte Markus Kuhn in seiner Doktorarbeit eine neue Abhörmethode vor. Da das Bild eines Monitors Punkt für Punkt und Zeile für Zeile geschrieben wird, flackert das Licht in einem halbdunklen Raum im Takt der Bildschirminformation. Ein entsprechend schneller und empfindlicher Photomultiplier (spezieller Lichtsensor) kann aus diesem Flackern den Bildschirminhalt rekonstruieren.

Bildschirminhalte sind selbst durch Glas abhörbar

Diese Methode funktioniert auch von der Straße durch das Fenster. In einem technischen Report zeigt Kuhn eindrucksvolle Demobilder von rekonstruierten Bildschirminhalten.

Gegen das Abhören helfen nur Abschirmen und spezielle Geräte

Die Abstrahlung lässt sich nur durch Abschirmung reduzieren. Das vom BSI entwickelte Zonenmodell hilft bei der Klassifizierung der notwendigen Maßnahmen. Die Abschirmung kann man dabei direkt am Gerät oder an der Umgebung (Gebäude) vornehmen.

Zudem gibt es etliche Hersteller, die spezielle, extrem strahlungsarme Geräte – sogenannte Tempest-Geräte – im Angebot haben.

Wägen Sie nach einer Risikoanalyse die notwendigen Maßnahmen ab

Ob Maßnahmen erforderlich sind oder nicht, muss eine detaillierte Risiko-Analyse für den eigenen Bereich ergeben. Hierbei helfen die IT-Grundschutzkataloge und das BSI.

Prof. Dr. Rainer W. Gerling

Linktipps

BSI: *http://www.bsi.bund.de*

Demonstration auf der CeBIT: *http://www.lightbluetouchpaper.org/2006/03/09/video-eavesdropping-demo-at-cebit-2006/*

Demobilder von rekonstruierten Bildschirminhalten: *http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-577.pdf*