

[Über den Sicherheitsmelder](#)

[Inhalt](#)
[Index](#)
[Schnellsuche](#)
[Recherche](#)
[Alle Fachbeiträge](#)
[Freie Fachbeiträge](#)

[Unsere Autoren](#)
[Unsere Partner](#)
[Impressum](#)
[Kontakt](#)
[AGB](#)
[Bewerten Sie uns!](#)

[Anmeldung](#)
[Einstellungen](#)

Kompromittierende Strahlung macht Computer abhörbar

07.10.08

Autor: [Christian Schaaf](#)
Anlass: [Kompromittierende Strahlung](#)
Abstract: [Kompromittierende Strahlung](#) ist die elektromagnetische Strahlung von Computer-Komponenten, die mit geeigneter Empfangs-Technik aus einer Entfernung von bis zu 150 Metern abgehört werden kann. Vor allem durch die Strahlung der Bildschirme, egal ob LCD, TFT oder CRT, können damit vertrauliche Informationen reproduziert werden. Eine technische Lösung schützt Computer und Peripherie-Geräte.
Sachbereich: [\[A.2\] Allgemeine Themen - Sicherheitsrisiken/Bedrohung](#)
Schlagwörter: [Industriespionage](#), [Kompromittierende Strahlung](#)

Kompromittierende Strahlung

Viele [Unternehmen](#) sind sich des Risikos von [Industriespionage](#) bereits bewusst und stellen ihre Computer-Bildschirme vor allem im Erdgeschoss [so](#) auf, dass sie durch die [Fenster](#) nicht abgelesen werden können. Was aber, wenn der Angreifer gar nicht auf den [PC](#) blicken muss, sondern bequem aus 100 Meter Entfernung den Bildschirm mitlesen kann? Jedes vertrauliche Dokument und jede brisante Information wären damit offen zugänglich.

Abschirmung von Computern

Komponenten sind umso sicherer, je besser sie geschirmt sind. Die Strahlung kann nicht nach außen dringen, ähnlich wie bei einem Faradayschen Käfig. Daher sollten [PC](#) und die verbindenden [Kabel](#) doppelt metallisch ummantelt sein, um eine möglichst hohe Abschirmung zu erreichen. Man spricht in diesem Zusammenhang von Tempest (Temporary Emanation and Spurious Transmission) festen Computern.

Schwierig wird die Situation bei Steckern, Bildschirmen und Peripherie-Geräten. Stecker sind häufig aus Kunststoff und damit unzureichend abgeschirmt. Sie geben die Strahlung genauso ab wie z.B. Modem oder Drucker. Bildschirme sind deshalb besonders gefährdet, weil sie nur unzureichend abgeschirmt werden können, das Bild muss ja noch lesbar sein.

Angriffsmethoden

Potenzielle Angreifer können die hochfrequente elektromagnetische Strahlung mit einem Breitbandempfänger und einer speziellen Log-Periodic-Antenne empfangen. Ähnlich einem schlecht empfangenen und deshalb rauschenden Fernsehbild, besteht die Schwierigkeit darin, das Bild zu synchronisieren, um es überhaupt sichtbar zu machen. Mit speziellen technischen Geräten ist dies aber möglich.

Die Empfangstechnik ist zwar ein wenig aufwändig und liegt bei ca. 30.000 bis 40.000,- Euro, für Geheimdienste und technisch versierte Täter stellt dies jedoch kein Hindernis dar.

Das nötige Equipment, einschließlich des Bildschirms, auf dem das Bild dupliziert wird, passt in einen Pilotenkoffer. Es kann somit überall leicht hintransportiert und auch unauffällig verwendet werden. Nur die spezielle Antenne, die auf den anzugreifenden Computer ausgerichtet werden muss, ist bei höheren Reichweiten relativ groß. Sollte das Ziel, z.B. ein [Laptop](#) im [ICE](#) oder am Flughafen, jedoch in unmittelbarer Nähe sein, kann die Antenne klein sein und sogar ebenfalls im Pilotenkoffer untergebracht werden. Der [Angriff](#) erfolgt somit ganz unauffällig.

Technische Lösung

Sicherheitskonzepte sollten [so](#) effektiv und diskret sein, dass ihre Existenz am besten gar nicht wahrgenommen wird. Corporate Trust, der strategische Partner namhafter [Unternehmen](#) im Risiko- und [Krisenmanagement](#), bietet Anfang 2009 ein neu entwickeltes spezielles Gerät an, mit dem die [kompromittierende Strahlung](#) jedes [PC](#) [so](#) verfälscht wird, dass sie nicht mehr dupliziert werden kann.

Diese neue Komponente schützt sämtliche Computer und deren Peripherie-Geräte in einem Radius von ca. 5 Metern und kostet 1.700,- Euro und ist gesundheitlich unbedenklich, da es nur eine geringe Strahlung im Milliwatt-Bereich abstrahlt.

Zum [Vergleich](#): Handelsübliche Schnurlostelefone, sog. DECT-Telefone, haben eine sechs- bis achtfach höhere Strahlung. Das Gerät hat die Baugröße einer Zigarrenschachtel und verfügt über einen Akku mit ca. 4 Stunden Laufzeit. Es bietet sich daher auch für den mobilen Einsatz an, z.B. Verwendung eines Laptops. Der [Betrieb](#) über ein Netzteil bzw. am USB-Anschluss jedes Computers (Leistungsausgang 500 mA) ist möglich.

Praxishinweise

- [Unternehmen](#) sollten ihre [Mitarbeiter](#) über den richtigen Umgang mit der IT und dem vertraulichen Firmen Know-how sensibilisieren. Das Risiko der [Industriespionage](#) ist durch die große Innovationsfähigkeit in Deutschland sehr hoch.
- Jedes [Unternehmen](#) sollte seine Schwachstellen durch [kompromittierende Strahlung](#) kennen. Hierfür eignet sich eine Basis-Messung, bei der ein Strahlungsdiagramm erstellt wird. Es wird aufgezeigt, welche Computer von außerhalb des Unternehmens abgelesen werden können. Die duplizierten Bildschirminhalte können dabei live vor Ort mit angesehen werden.