

Medienmitteilung

Bern, 30. November 2007

Weltneuheit: Dreamlab Technologies Schweiz knackt Funktastatur

Auf immer mehr Schreibtischen stehen Funktastaturen und –mäuse. Doch kabellose Hardware birgt grosse Risiken. Das Schweizer IT-Security Unternehmen Dreamlab Technologies AG zeigt, dass ein Mitlauschen der Tasteneingaben möglich ist. Usernamen, Passwörter, Bankverbindungen oder vertrauliche Korrespondenz können sehr einfach mitgeschnitten werden.

Obwohl der Trend in der kabellosen Kommunikation bei Peripheriegeräten wie PC-Tastaturen und -Mäuse in Richtung Bluetooth geht, setzen Marktleader wie Logitech und Microsoft auf die kosteneffiziente und bewährte 27-MHz-Funktechnologie. Dreamlab Technologies hat nun mit einem einfachen Funkempfänger, einer Soundkarte und der entsprechenden Software die Radiofrequenzen zwischen Tastatur und PC/Notebook abgefangen und decodiert. Zwar erschweren die Hersteller von Funktastaturen das Abfangen von Daten teilweise mit einer Verschlüsselung - diese zeigt jedoch gravierende Mängel und bietet somit keinen echten Schutz. Dazu Max Moser von Dreamlab Technologies: „Kabellose Kommunikation ist nur so sicher wie die benutzte Verschlüsselungstechnologie und auf Grund ihrer Natur mit wenig Aufwand abhörbar.“

Dreamlab Technologies hat die Verschlüsselung der Microsoft Wireless Optical Desktop 1000/2000 Tastaturen geprüft und erfolgreich entschlüsselt. Da die meisten Produkte der Wireless Desktop Serie von Microsoft auf derselben Technologie beruhen, hält Dreamlab Technologies diese Produkte ebenfalls für nicht sicher. Während der Analyse gelang es Max Moser und Phillipp Schrödel von Dreamlab Technologies mittels eines einfachen Funkempfängers aus bis zu zehn Meter Entfernung Daten mitzulesen. Mit entsprechender technischer Ausrüstung sind grössere Distanzen realisierbar.

Als Kompetenzzentrum für IT Security ist für Dreamlab Technologies eine verantwortungsvolle Offenlegung von Sicherheitslücken (Responsible Vulnerability Disclosure) oberstes Gebot. Der betroffene Hersteller wurde umgehend über die bestehende Sicherheitslücke informiert. Die Fehlerbehebung ist für die betroffenen Hersteller aufwändig und langwierig. Dementsprechend veröffentlicht Dreamlab Technologies zum aktuellen Zeitpunkt weder das entwickelte Angriffswerkzeug noch die exakten Details. Dazu führt Nicolas Mayencourt, CEO Dreamlab Technologies, aus: "Um echte Sicherheit produzieren zu können, müssen Unsicherheiten geortet und thematisiert werden. Eine Sicherheitslücke ethisch thematisieren heisst, das Publikum und den Hersteller korrekt informieren. Dem Hersteller muss die Möglichkeit geboten werden, sein Produkt zu verbessern und dem Konsument sein Sicherheitslevel zu korrigieren. Nur so entsteht echte Sicherheit“.

Dreamlab Technologies ist auf IT Sicherheit spezialisiert und ein international ausgerichtetes Unternehmen mit Standorten in der Schweiz, Deutschland und Frankreich. Seit 1997 führt Dreamlab High-End-Sicherheitstests, Beratungen und Schulungen durch und realisiert Lösungen basierend auf "best-in-class" Open Standard Technologien. Als Vorstandsmitglied von ISECOM.org arbeitet Dreamlab Technologies nach dem OSSTMM-Manual, der heute am meisten verbreiteten Methodik für umfassende Sicherheitsaudits.

Dreamlab Technologies pflegt strategische Partnerschaften mit den renommiertesten, internationalen Open Source Projekten, führenden technischen Hochschulen und wegweisenden Normeninstituten (W3C). Es ist das Ziel von Dreamlab Technologies seinen Kunden und Partnern zu ermöglichen, von diesem Erfahrungsschatz direkt zu profitieren.

Weitere Informationen und eine Videodemonstration des Angriffes finden Sie auf <http://dreamlab.net>

Allgemeiner Kontakt	Nicolas Mayencourt, CEO Dreamlab Technologies AG CH – 3011 Bern / Switzerland	+41 31 398 66 66 nicolas.mayencourt@dreamlab.net http://dreamlab.net
Technischer Kontakt	Max Moser, Senior Security Spezialist Dreamlab Technologies AG CH – 3011 Bern / Switzerland	+41 31 398 66 66 max.moser@dreamlab.net http://dreamlab.net