

Dreamlab IT-Security Bulletin – Juni 2008

Funktechnologien: So sicher wie der verwendete Schlüssel

Drahtlose Kommunikation liegt im Trend und ist vermehrt in jedem Haushalt anzutreffen. Die Liste der Geräte mit Funktechnologie ist umfangreich: Handys, Headsets, Drucker, Mäuse und Tastaturen sind nur ein paar wenige Beispiele. Hardware- und Softwarehersteller verkünden die kabellose Freiheit und propagieren den Hochleistungsarbeitsplatz. Egal ob am Schreibtisch oder unterwegs, überall und jederzeit sei müheloses arbeiten möglich. Doch kabellose Kommunikation birgt Risiken. Funktechnologien sind angreifbar und nur so sicher wie die angewandte Verschlüsselung. Immer wieder gelingt es Hackern, die digitalen Schlüssel aufzudecken. Sie verschaffen sich Systemzugriff, schneiden die Kommunikation mit und können ganze Systeme manipulieren.

Viele User sind sich der allgegenwärtigen Sicherheitslücken von Funkverbindungen nicht bewusst und bezahlen das Leben ohne Kabelsalat mit Unsicherheit. Der IT-Security Provider Dreamlab Technologies zeigt, wie einfach Mitlauschen der Tasteneingaben ist. Microsoft wirbt auf ihrer Website für seine Optical Desktop Serie mit den Worten „geniessen Sie die kabellose Freiheit bei Maus und Tastatur“ bei „einem Maximum an Sicherheit“. Dreamlab Technologies hat die Funk-Kommunikation der Microsoft Wireless Optical Desktop Modelle 1000 und 2000 analysiert. Während der Analyse gelang es Max Moser und Philipp Schrödel von Dreamlab Technologies mittels eines einfachen Funkempfängers aus bis zu zehn Meter Entfernung Daten mitzulesen und zu entschlüsseln. Mit entsprechender technischer Ausrüstung sind grössere Distanzen realisierbar.

Unzureichende Verschlüsselung bei Microsoft

Obwohl der Trend in der kabellosen Kommunikation bei Peripheriegeräten wie PC-Tastaturen und -Mäusen in Richtung Bluetooth geht, setzen Marktleader wie Logitech und Microsoft auf die kosteneffiziente und bewährte 27-MHz-Funktechnologie. Das Frequenzband um 27MHz ist kostenlos und steht jedermann zur freien Sprach- und Datenübertragung zur Verfügung. Die Kommunikation zwischen den Funktastaturen und dem Basisempfänger ist verschlüsselt. Per Tastendruck synchronisiert und authentifiziert der User die Verbindung zwischen Sender und Empfänger. Als Schlüssel verwendet Microsoft ein 8-Bit langen Code.

Der digitale Schlüssel ist mit Hilfe eines einfachen Funkequipments und nach nur 20 bis 25 Tasteneingaben dechiffriert. Dazu führten Max Moser und Philipp Schrödel lediglich eine erweiterte Brute Force Attacke auf den abgehörten Funkverkehr durch. Bei einer Brute Force Attacke werden alle möglichen Tastenkombinationen systematisch getestet. Ein 2⁸-Bit langer Schlüssel ergibt 256 verschiedene Kombinationsmöglichkeiten und ist innert Millisekunden entziffert. Das gilt auch für Computer mit geringer Rechenleistung. Ist der Angreifer erst einmal im Besitz des geheimen Verbindungsschlüssels, kann er sämtliche Zeicheneingaben einer solchen Funktastatur aufzeichnen und entschlüsseln. Usernamen, Passwörter, Bankverbindungen oder vertrauliche Korrespondenz werden auf diesem Weg sehr einfach mitgeschnitten. Neben den getesteten Microsoft Wireless Optical Desktops 1000 und 2000 übertragen und verschlüsseln auch die Modelle 3000 und 4000 derselben Serie nach gleichem Muster. Dreamlab Technologies stuft diese Modelle deshalb ebenfalls als unsicher ein.

Verschlüsselung: Das A und O

Funk ist vielseitig einsetzbar und verschafft in vielen Anwendungen Vorteile gegenüber Kabellösungen. Je nach Produkt und Bedürfnis kommen unterschiedliche Funktechnologien und Standards zum Einsatz. Handy-Zubehör funktioniert mit dem Kurzstreckenfunk Bluetooth, der Internetzugang über Wireless LAN erlaubt Mobilität und Garagentore sowie Autoverriegelungen lassen sich mit RFID (Radio Frequency Identification) per Knopfdruck schliessen. Für alle Funktechnologien gilt jedoch, dass das Mitschneiden der übertragenen Daten mit entsprechender Ausrüstung einfach ist. Ohne entsprechende Verschlüsselung ist Funk offen für Mitlauscher. Sind die Daten jedoch verschlüsselt, kann der Angreifer den Datenverkehr mitschneiden, im Idealfall den Code jedoch nicht entschlüsseln.

Brute Force Attacks gehören zu den häufigsten Angriffsmethoden. Verschlüsselungsverfahren werden gegen Brute Force Attacks gewappnet, indem die Schlüssellänge erhöht wird. Mit zunehmender Schlüssellänge wächst die Anzahl an Schlüsselkombinationen und der Rechenaufwand für einen Brute Force Angriff nimmt exponentiell zu. Nach den zurzeit auf dem Markt gängigen symmetrischen Verschlüsselungsverfahren wie AES (Advanced Encryption Standard) gelten Schlüssel ab einer Länge von 256 Bit als sicher. Der mit 256 Bit erreichte Schlüsselraum lässt sich mit heutigen Methoden per Brute Force nicht absuchen. Unabhängig von der verwendeten Technologie gilt aber für alle Funktechnologien derselbe Grundsatz: Das Sicherheitslevel hängt von der Schlüssellänge und dem verwendeten Algorithmus ab.

Schutzmassnahmen gegen den Datenklau

Da die für eine qualitativ hochwertige Verschlüsselung benötigte Rechenleistung beträchtlich ist, wird diese in den für den Gebrauchsmarkt konzipierten Geräten häufig nicht zur Verfügung gestellt. Bei geringer Rechenleistung sind jedoch nur unzureichende Algorithmen oder zu kurze, vorhersehbare Schlüssel einsetzbar. Bislang existiert abgesehen von der Nichtverwendung solcher Funktastaturen keine hundertprozentige wirksame Schutzmassnahme.

Es steht aber dem Benutzer frei eine andere Technologie, wie zum Beispiel Bluetooth zu nutzen. Diese bietet zwar bessere Verschlüsselungsmöglichkeiten, besitzt aber ebenfalls Schwächen. Im Gegensatz zu den 27MHz-Funktastaturen hängt bei Bluetooth der Erfolg stark vom Angriffszeitpunkt ab, da der Verbindungsaufbau mitgeschnitten werden muss.

Für Anwendungen bei denen die Mobilität entscheidend ist, erwartet Dreamlab Technologies einen Trend hin zur Funkübertragung. Davon betroffen sind beispielsweise die Maschinenindustrie und der Home-Office Bereich: Drucker, Kamera oder Audio-Equipment funktionieren künftig per Funk und Schleppkabel für die Systemsteuerung von beweglichen Maschinenteilen verschwinden. Ein weiteres Beispiel für den sich abzeichnenden Trend sind intelligente Infrastrukturen in Fahrzeugen und Gebäuden. Da Funktechnologien gänzlich unterschiedliche Eigenschaften und Verhaltensweisen besitzen, ist auch in naher Zukunft mit unterschiedlichen Funksystemen zu rechnen.

Verantwortungsvolle Offenlegung durch Dreamlab Technologies

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“.

Weitere Informationen und eine Videodemonstration zu den Sicherheitslücken bei den 27-MHz-Funktastaturen von Microsoft finden Sie auf <http://www.dreamlab.net/news>.

Autorin:

Claudia Stahel
Dreamlab Technologies AG
Monbijoustrasse 36
CH-3011 Bern
contact@dreamlab.net
<http://dreamlab.net>

Die Publikation dieses Artikels ist unter Angabe der Quelle und Zusendung eines Belegexemplars ausdrücklich gestattet.