

## Sicherheit von Personal Digital Assistants (PDA)

Detlef Kraus, SRC Security Research & Consulting GmbH, Bonn  
(E-Mail: [detlef.kraus@src-gmbh.com](mailto:detlef.kraus@src-gmbh.com))

Die Funktionalität von Personal Digital Assistants (PDAs) hat sich innerhalb kürzester Zeit vom einfachen elektronischen Terminkalender zum Mini-Laptop gewandelt. PDAs sind frei programmierbar und für die Standard-Betriebssysteme PalmOS oder Windows CE ist eine Vielzahl von Programmen verfügbar, die zum großen Teil von der Nutzung am heimischen oder dienstlichen PC her bekannt sind. Anders als herkömmliche Mobiltelefone verfügen PDAs über ein grafisches Display, welche die Darstellung kleinerer Texte, Tabellen oder Bilder erlauben. Mittels eines Touch-Screens können Eingaben zur Steuerung der Programme oder zur Eingabe von Daten (tlw. über Mustererkennung) vorgenommen werden.

Zur Kommunikation mit der externen Welt werden neben den sogenannten Cradles, die eine feste Verbindung zum PC des Benutzers ermöglichen, Infrarot-, Bluetooth- oder GSM-Schnittstellen auf dem Markt angeboten. Mobiltelefone und PDAs wachsen so in ihrer Funktionalität zusammen, Kombinationsgeräte sind bereits am Markt verfügbar (z.B. Handspring Treo).

Mit diesen Eigenschaften erreichen PDAs zwar nicht die Leistungsfähigkeit eines Laptops; das Angebot und die Nutzung von Diensten im elektronischen Geschäftsverkehr auf Basis eines PDAs nimmt jedoch ständig zu. Geschäftsleute speichern vertrauliche Firmendaten und Adressinformationen, die Sie auf Reisen nachschlagen und/oder bearbeiten können. E-Mails lassen sich lesen und beantworten. Falls der PDA eine direkte Kommunikationsschnittstelle ins Internet hat, lassen sich die Nachrichten auch gleich versenden.

Einige Direktbanken und Sparkassen bieten Mobile-Banking und Brokerage mit dem PDA unter Nutzung des HBCI-Standards an. Auf der CeBIT 2002 waren Lösungen zu sehen, die ein sicheres Bezahlen (aus Sicht des Händlers **und** des Kunden) mit Chipkarten erlaubte, die auf dem Standard der Zahlungssysteme Europay, MasterCard und VISA (EMV) basieren. Für letztere Anwendung wurde der PDA mit einem Chipkartenleser ausgestattet, um einerseits den Benutzer zu authentisieren und andererseits kryptographische Funktionen von der Chipkarte ausführen zu lassen. (Eine ausführliche Beschreibung findet man als Download bei [www.src-gmbh.com](http://www.src-gmbh.com)).

PDAs werden aufgrund der Tatsache, dass sie vom Besitzer ständig bei sich getragen werden, als ‚sichere‘ Devices betrachtet. Der Schluss ist trügerisch, da insbesondere die geringe physische Größe die Gefahr eines schnellen Verlustes bergen; Studien gehen von einer Verlustrate von ca. 30% aus. Zusätzlich wird der PDA über die vorhandenen Kommunikationsschnittstellen den aus der PC-Welt bekannten Bedrohungen ausgesetzt. Bei allen Anwendungen ist zu prüfen, was der PDA schützen soll, und wie der Schutz der Daten gewährleistet werden kann. Man kann nicht a priori davon ausgehen, dass der PDA über Eigenschaften verfügt, die gespeicherten Daten zu schützen oder die Sicherheit auf die Hoffnung setzen, dass man ihn schon nicht verlieren wird.

## **Verlust des PDAs**

Der Verlust eines PDAs bedeutet für den Besitzer sicher mehr als nur den Verlust der Hardware. In den meisten Fällen ist die gespeicherte Information von sehr viel höherem Wert, als die Wiederbeschaffung des Geräts; dies wird unter Umständen sogar durch eine entsprechende Versicherung bezahlt; die Wiederbeschaffung der Daten ist in allen Fällen in den Versicherungsbedingungen explizit ausgeschlossen. Wie dramatisch die Auswirkungen eines Verlustes sein können, zeigte das Beispiel des Golfkrieg-Offiziers, dessen Laptop mit militärischen Plänen vom Rücksitz seines Wagens gestohlen wurde. Die Rückgabe des Laptops war nur dem glücklichen Umstand zu verdanken, dass der Dieb nicht in Spionageverdacht geraten wollte – was sehr viel höhere und drastische Strafen zur Folge gehabt hätte.

Unternehmensdaten wie z. B. Angebote, Konstruktionsunterlagen oder strategische Planungsdaten sind für eine Firma unter Umständen überlebenswichtig und sollten nicht in falsche Hände geraten.

Private Daten auf dem PDA, wie beispielsweise Zugangscodes zum Online-Banking, PINs oder Transaktionsnummern, Kreditkartennummern und Bankverbindungen sollten nur dem Eigentümer des Gerätes zugänglich sein. Die Folgen eines Verlustes sind vergleichbar mit dem Verlust einer Geldautomatenkarte - mit auf der Rückseite notierter Geheimzahl.

Wird ein PDA wie hier skizziert genutzt, dann ist bzgl. der Sicherheit die Frage zu beantworten: „Wie werden die Daten auf meinem PDA geschützt, so dass sie auch bei Verlust des Gerätes nicht kompromittiert werden?“

## **Verschlüsselung und Zugriffsschutz**

Alle PDAs können so konfiguriert werden, dass man auf die Daten und Programme nach dem Einschalten nur nach Eingabe eines Passwortes zugreifen kann. Da sich die Geräte aus Gründen der Stromersparnis nach kurzer Zeit wieder ausschalten, wenn sie nicht benutzt werden, ist es ratsam, diese Möglichkeit zu nutzen. Ob diese Maßnahme einen wirkungsvoller Schutz der Daten garantiert, kann bezweifelt werden. Zum Vergleich: die Entwendung eines PCs mit eingestelltem BIOS Passwortschutz bietet auch keinen Schutz davor, dass niemand die auf der Festplatte gespeicherten Daten auslesen kann; im Gegenteil, nach Ausbau der Festplatte kann man sie auf einem dritten System verfügbar machen und alle gespeicherten Daten auswerten. Daher bieten – wie für Laptops auch – viele Hersteller bereits Verschlüsselungssysteme für PDAs an, die alle Kundendaten verschlüsseln. Damit kann man sicherstellen, dass der Schutz des PDA-Speichers der Güte des eingesetzten Verschlüsselungsverfahrens entspricht. Dies sollte aus heutiger Sicht äquivalent zu Triple-DES, IDEA oder Rijndael sein. Bei Verwendung eines solchen Verschlüsselungssystems für die Daten ist u.a. das Key Management zu prüfen, d.h. in welcher Weise wird der kryptographische Schlüssel vom Bediener eingegeben oder freigeschaltet. Hier bietet sich natürlich ein potenzieller Angriffspunkt: ein Angreifer wird versuchen in den Besitz des Schlüssels zu kommen, wenn er weiß, dass die Daten verschlüsselt sind. Dies kann z.B. über eine als ‚trojanisches Pferd‘ getarnte Software erfolgen. Dies ist besonders wirkungsvoll, wenn der PDA auch direkt über einen online-Zugang verfügt (beispielsweise via GSM, GPRS oder UMTS) und die maliziöse Software dem Angreifer die erforderlichen Informationen schon vor dem Diebstahl des Gerätes überträgt.

## Virenschutz

Die vorangegangenen Überlegungen legen es nahe, auch PDAs mit Virenschutzprogrammen auszustatten. Spätestens seit die ersten Viren für PDAs aufgetaucht sind, werden solche Virenschutzprogramme angeboten. Sie bieten zwar keinen Schutz vor trojanische Pferde, vielfach sind die oben beschriebenen schlechten Eigenschaften jedoch auch in selbstreproduzierenden Programmen vorhanden, die sich im Netz ausbreiten. Generell ist, insbesondere zum Schutz von Firmendaten darauf zu achten, dass auf den PDAs nicht beliebige Software aus dem Netz geladene oder von ‚Bekanntem‘ geschenkte Software installiert wird. Wie hoch jedoch die Motivation für die Installation von Software auf einem PDA sein kann, zeigen beispielsweise die kostenlosen CeBIT Kataloge. Diese wurden während der Messe auf mehreren tausend PDAs installiert. Für die Konkurrenz kann schon das Adressverzeichnis oder der Terminkalender wertvolle Hinweise bieten, um auf die Strategie eines Unternehmens zu schließen. Die Bedeutung anderer schützenswerter Firmen-Informationen, wie Konstruktionsunterlagen, Angebote, Preise etc. können einem Konkurrenten unmittelbar Wettbewerbsvorteile verschaffen.

Für Privatpersonen ist z.B. der Schutz der Daten wichtig, mit denen er seine Bankgeschäfte unter Nutzung des PDAs abwickelt. Auch hier können PIN-Eingaben und Transaktionsnummern ein lohnendes Ziel für einen Angreifer sein. In diesen Fällen muss ein Angreifer ggfs. nicht einmal in den Besitz des PDAs gelangen, um sich einen Vorteil zu verschaffen.

Gerade dieses Beispiel zeigt, dass man einem PDA nicht unbedingt alle Geheimnisse anvertrauen sollte. Wie eingangs erwähnt, ist es möglich PDAs mit Smartcard-Lesern auszurüsten. Auf den Chipkarten können dann beispielsweise kryptographische Schlüssel oder bankspezifische Informationen gespeichert werden. Dieses bietet jedoch nur dann einen zusätzlichen Schutz, wenn die zur Freischaltung der Chipkarte notwendige Geheimzahl nicht ausgespäht wurde und die Chipkarte nicht zugleich mit dem PDA abhanden kommt.

Wie bei allen Überlegungen zu einer Risikoanalyse ist vorab zu klären, welchen Wert die gespeicherten Informationen für den Besitzer (für das Unternehmen oder eine Privatperson) haben. Hieraus müssen sich die zu ergreifenden Maßnahmen ableiten. Generell kann jedoch festgehalten werden, dass für PDAs die gleichen Schutzmechanismen genutzt werden sollten wie für Laptops, Notebooks oder andere mobile Computer. Da der Anwender die Qualität der angebotenen Schutzmaßnahmen in den meisten Fällen jedoch nicht beurteilen kann, sollten auch hier Sicherheitsuntersuchungen und Zertifikate – etwa nach den Common Criteria – dem Anwender einen Hinweis darauf geben, was das eingesetzte Produkt tatsächlich leistet.