Bild: Fujitsu Siemens

Lauschangriff auf den PDA

Von Thomas Fritsch, Bernd Lutterbeck, Torsten Pehl und Frank Pallas

Auf PDAs werden Termine verwaltet, Kontakte gespeichert und E-Mails gelesen. Eine neue Studie zeigt gravierende Sicherheitsmängel beim Einsatz von Handhelds – insbesondere bei der Verwendung von Microsoft Pocket PC 2002.

Microsoft bietet mit Windows CE auf dem Markt ein weit verbreitetes Betriebssystem für mobile Geräte an, das in Form von Pocket PC 2002 (Windows CE 3.0 mit Applikationen wie Pocket Word und Outlook) für PDAs vorgesehen ist und inzwischen von vielen Herstellern genutzt wird. Dazu gehören Firmen wie Acer, Fujitsu Siemens, HP, NEC, Packard Bell, Viewsonic und Yakumo.

Im Vergleich zur Geräteklasse der Notebooks gibt es für PDAs bisher noch keine etablierten und erprobten Verfahren am Markt, um hohen Sicherheitsansprüchen gerecht zu werden. Ist schon die Sicherheit eines einzelnen PDAs ein nicht zu unterschätzendes Problem, stehen Unternehmen für gewöhnlich vor massiven Schwierigkeiten, wenn sie viele PDAs verwalten und sicher administrieren wollen. Aus diesem Grund untersuchte die Forschungseinheit „Informatik und Gesellschaft“ der TU Berlin im Auftrag des Bundesministerium des Innern (BMI) die Pocket-PC-Plattform am Beispiel von zwei repräsentativen Geräten aus der iPAQ-Serie von HP. Im Zentrum der Untersuchungen stand die Fähigkeit der Geräte zur mobilen Synchronisation von PIM-Daten, E-Mails und Dokumenten mit einen im Firmenintranet postierten Exchange Server. Dabei wurden die Geräte unter den Aspekten Sicherheit, Administration, Synchronisation, Usability und Kosten betrachtet. Ziel war es, eine Einschätzung auf dem Markt verfügbarer Softwareprodukte zu gewinnen und ein mögliches Gesamtsystem zu skizzieren, das auf Pocket-PC-2002-basierende Handhelds sicher in eine bestehende Firmeninfrastruktur integriert.

Dieser Artikel basiert auf dem zweiten Teil der Studie „Mobiler Zugang zu gesicherten Netzen – Lösungen für die Zukunft“ (www.ig.cs.tu-berlin.de/forschung/Mobile/index. html) der Forschungseinheit Informatik und Gesellschaft an der TU Berlin. Die Einheit Informatik und Gesellschaft (www.ig.cs.tu-berlin.de) unter Leitung von Prof. Dr. iur. Bernd Lutterbeck ist eine selbstständige Forschungseinheit am Institut für Wirtschaftsinformatik der TU Berlin. Sie beschäftigt sich schwerpunktmäßig mit Datenschutz, Informationsrecht, geistigem Eigentum, IT-Sicherheit und Open Source.

Die Ergebnisse im Überblick

Die Ergebnisse der Untersuchung zeigen bereits im rein funktionalen Bereich der Synchronisation Probleme der Pocket-PC-2002-Plattform auf. So gelingt es keiner Synchronisationslösung mit den komplexen Exchangestrukturen umzugehen. Dies liegt zum größten Teil an den geringen Möglichkeiten des PDA-Betriebssystems und den fehlenden Schnittstellen in den Microsoft-Komponenten. So können öffentliche Ordnerstrukturen nicht synchronisiert werden und verschiedene Terminkalender vermischen sich auf dem PDA untrennbar miteinander. Unterordner im Posteingang werden nicht synchronisiert und viele von dem Arbeitsplatz gewohnte Features funktionieren auf dem kleinen PDA mangels des Funktionsumfangs der dortigen Anwendungen wie Pocket Outlook überhaupt nicht.

Ein aufwendiges „Herunterbrechen“ des gewohnten Arbeitsumfeldes nur für die Synchronisation auf den PDA erscheint unvermeidbar. Hier muss das Unternehmen massive Anstrengungen aufbieten und etliche technische Hürden überwinden, bis zumindest eine Synchronisation gewisser Basisdaten am Arbeitsplatz möglich wird. Daher kann im Bereich der mobilen Synchronisation momentan nur von einem Einsatz von PDAs abgeraten werden.

Administrationslösungen zeigen Schwächen

Auf dem Gebiet der Administration ist das Bild ebenfalls ernüchternd. Zwar existiert eine Administrationslösung, die tatsächlich den benötigten Funktionsumfang aufweist (Afaria vom Hersteller Xcellenet). Jedoch bietet der Hersteller keine Proxykomponente an, die eine klare Schicht-7-Trennung der Kommunikation in der DMZ (Demilitarisierte Zone) ermöglichen würde. Der Proxy trennt die Anfrage auf OSI-Schicht 7 (Application Layer) und erzeugt eine neue, sichere Anfrage auf den Server im Intranet. Stattdessen wäre es beim Einsatz von Afaria nötig, eine durchgehende Verbindung direkt in das Intranet aufzubauen – ein schwer wiegendes zusätzliches Sicherheitsproblem. Andere Lösungen, wie der XTND Connect Server oder der Mobile Information Server (MIS) in Kombination mit dem Internet Security & Acceleration Server als Proxykomponente, verfügen zwar über eine solche Proxykomponente, bieten aber entweder ungenügende oder gar keine Administrationsmöglichkeiten.

PDAs – kein Sicherheitsrisiko für Firmennetze

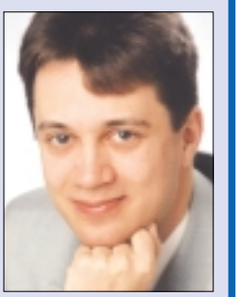
Bild: Pointsec

Heinz Kraus ist Geschäftsführer von Pointsec Mobile

Heinz Kraus, Geschäftsführer von Pointsec Mobile: „Handheld-Computer haben Charme und sind nützlich. Mitarbeiter können sie vielseitig – wann, wo und wie auch immer sie wollen – als mobiles Büro einsetzen. Eine aktuelle Studie des Bundesinnenministeriums macht jedoch darauf aufmerksam, dass PDAs für den Einsatz im Unternehmen nur bedingt geeignet seien. Aus Sicherheitsgründen sollte eine solche Plattform nicht ohne Zusatzsoftware genutzt werden. Was ist also zu tun?
Um rundum Sicherheit zu schaffen – hierzu bedarf es unter anderem auch einer Personal Firewall und Virenschutzprogrammen –, ist vor allem der Einsatz professioneller Authentisierungs- und Verschlüsselungs-Software notwendig. Werden diese Produkte unternehmensweit eingesetzt, sorgen sie für eine automatische Echtzeit-Verschlüsselung sämtlicher Daten. Die Pointsec-Lösung für Windows Pocket-PCs chiffriert dabei außer Windows und den Temp-Dateien alle Informationen auf den PDAs sowie auf sämtlichen Wechselspeichermedien. Anwender, die zudem bei der Datenübertragung mit einer Verschlüsselung arbeiten, haben einen Rundumschutz, wie er besser nicht sein kann. Als kostengünstige und komfortable Ergänzung zu Notebooks sind PDAs, sicherheitsbewusst eingesetzt, eine sinnvolle mobile Plattform.“ *(SW)*

Neue Versionen bereits am Markt

Bild: Utimaco



Richard Aufreiter ist Produkt Manager Personal Device Security bei Utimaco

Richard Aufreiter, Produkt Manager Personal Device Security bei Utimaco: „Eine der Hauptaussagen dieser sehr umfangreichen und gut recherchierten Studie ist, dass die angebotenen Sicherheitsprodukte für persönliche digitale Assistenten (PDA) kaum ausreichenden Schutz bieten. Zu den vielen im Test als ungenügend bewerteten Lösungen gehört auch die bereits im Frühjahr 2002 bereitgestellte Safeguard PDA – Version 1.0 Personal Edition.
Bei Safeguard PDA 1.0 Personal Edition führte die fehlende PIM-Verschlüsselung sowie die fehlende Möglichkeit einer zentralen Administration zur Abwertung. Die Safeguard-PDA-Lösungen bieten aus gutem Grund bisher keine PIM-Verschlüsselung an: Bis zur neuesten Betriebssystem-Version Windows Mobile 2003 (Release: Sommer 2003) wurden von Microsoft keine Schnittstellen für die Verschlüsselung der PIM-Daten in PDA-Betriebssystemen angeboten.
Inzwischen ist einiges geschehen. Wir bieten das Produkt Safeguard PDA 2.0 Enterprise Edition an und bringen demnächst die für Windows Mobile 2003 konzipierte Lösung Safeguard PDA Version 3.0 auf den Markt, welche die Aspekte PIM-Verschlüsselung und sichere Administration voll berücksichtigt. Eine ausführliche Version unseres Kommentars erhalten Sie auf Anfrage unter info@utimaco.de.“ *(SW)*

Die auf den Pocket PCs in der Standardausstattung angebotenen Sicherheitsfeatures hielten sogar eine böse Überraschung parat. So konnte eines der Geräte, der iPAQ h5450 mit seiner eingebauten biometrischen Zugangskontrolle in Form eines thermischen Fingerabdruck-Scanner nicht überzeugen: Im Labor ließ sich der Scanner rund zwölfmal erfolgreich täuschen. Ein katastrophales Ergebnis für ein Biometrieverfahren, das beim Nutzer erhöhte Sicherheit suggeriert.

Unzureichende Verschlüsselung

Die Softwareprodukte von Drittanbietern fallen größtenteils auf Grund massiver Probleme im Bereich der Verschlüsselung durch. Die häufig fast gänzlich fehlenden Administrationsmöglichkeiten beziehungsweise Schnittstellen können selbst durch Einsatz von Afaria nur ungenügend ausgeglichen werden. Außerdem existieren Kompatibilitätsprobleme auf dem iPAQ h5450, auf dem nur wenige Produkte fehlerfrei zu betreiben waren. Die Zahl technischer Probleme und Fehler war generell zu hoch. Viele Produkte lagen während der Tests allerdings lediglich in einer der ersten Versionen für den Pocket PC vor und verursachten derart viele Fehler, dass ein reibungsloser Betrieb nicht möglich war – die Hersteller kämpfen offenbar massiv mit „Kinderkrankheiten“. Bei abschließenden Tests konnte das Produkt Filecrypto von F-Secure soweit überzeugen, dass ein Einsatz zu empfehlen ist, auch wenn im Bereich der Verschlüsselung noch einige Mängel bestehen bleiben.

Darüber hinaus zeigt sich das untersuchte Gesamtsystem vom PDA bis ins Firmennetz, inklusive aller Komponenten zur Steuerung des Verbindungsaufbaus, der Administrations- und Synchronisationssoftware und der empfohlenen Sicherheitssoftware, als nahezu unbedienbar für die mobile Synchronisation. Ein Nutzer müsste für einen vollständigen Synchronisationsvorgang bis zu sieben Passwörter in unterschiedlichsten Dialogmasken eingeben. Ein unzumutbarer Zustand, der auch durch aufwendiges Scripting oder Programmieren auf der Pocket-PC-2002-Plattform kaum zu lindern ist.

Das Projekt: Mobiler Zugang zu gesicherten Netzen – Lösungen für die Zukunft

Im Auftrag des Bundesministerium des Innern untersuchte die Forschungseinheit „Informatik und Gesellschaft“ die Pocket-PC-Plattform am Beispiel von zwei repräsentativen Geräten aus der iPAQ-Serie von HP. Im Zentrum der Untersuchungen stand die Fähigkeit der PDAs zur mobilen Synchronisation von PIM-Daten, E-Mails und Dokumenten mit einen im Firmenintranet postierten Exchange Server.
Die Untersuchungen wurden im Rahmen eines Projektes im Wintersemester 2002/2003 durchgeführt. Dazu wurde in einem Testlabor eine Firmeninfrastruktur nachgebildet. Die Geräte und Lösungen wurden unter den Aspekten Sicherheit, Administration, Synchronisation, Usability und Kosten betrachtet. Zum Einsatz kamen die Synchronisationslösung Extended Connect Server (Extendended Systems), die Administrationslösung Afaria (Excellenet) sowie die Sicherheitsapplikationen Filecrypto Enterprise Edition (F-Secure), Moviancrypt (Certicom), PDA Defense (Asynchrony), PDA Secure Premium (Trust Digital), Pointsec for Pocket PC (Pointsec) und SafeGuard PDA Personal Edition (Utimaco) in den Ende 2002 verfügbaren Versionen. Mittlerweile existieren für nahezu alle aufgeführten Lösungen Nachfolgeversionen mit teilweise umfangreichen Funktionalitätserweiterungen. Einige Programme sind am Markt nicht mehr verfügbar, andere Wettbewerber sind hinzu gekommen.
Als Groupware im Firmenintranet kam ein Exchange 2000 Server zum Einsatz. Als Endgeräte dienten zwei Geräte aus der iPAQ-Serie von HP (h3970, h5450). Eines der Geräte verfügte dabei über einen zusätzlichen biometrischen Zugang mittels eines thermischen Fingerabdruckscanners. Es wurden zwei Möglichkeiten der Einwahl untersucht: Zum einen die Einwahl über das Internet durch die Firewall in die demilitarisierte Zone (DMZ) und zum anderen die direkte Einwahl über das Mobilfunk-Netz auf einen RAS Server (Remote Access Service) in der DMZ. Beide Zugangswege wurden durch ein VPN (Virtual Private Network) getunnelt.
Ein einheitlicher Evaluationsbogen inklusive eines transparenten und flexibel anpassbaren Konzeptes gewährleistet die Nachvollziehbarkeit der Ergebnisse. Soweit möglich wurden zudem anerkannte Verfahren und bestehende Normen berücksichtigt (zum Beispiel für die Usability die ISO 9241-10). Die ausgewählten Produkte wurden ebenso wie die Standardausstattung der beiden Handhelds gemäß dem in der Studie vorgestellten Evaluationskonzept getestet und bewertet.

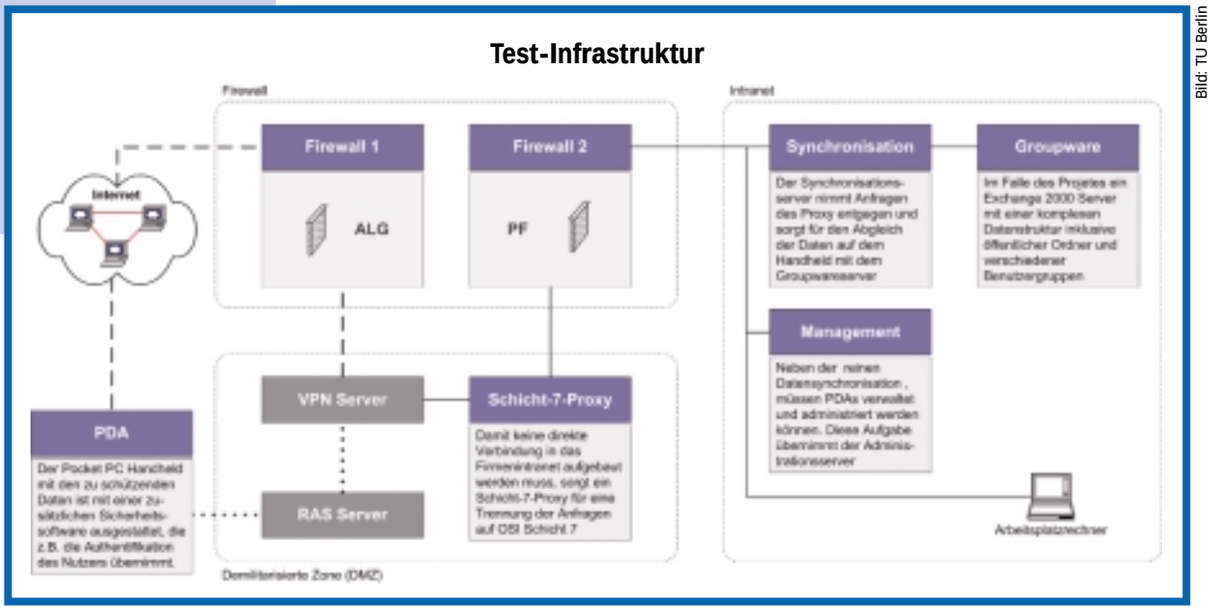


Bild: TU Berlin

Im Zentrum der Untersuchungen stand die Fähigkeit der Geräte zur mobilen Synchronisation von PIM-Daten, E-Mails und Dokumenten mit einen im Firmenintranet postierten Exchange Server. Dazu wurde in einem Testlabor eine Firmeninfrastruktur nachgebildet

Fazit

Daten werden nicht dadurch weniger schützenswert, dass sie statt auf einem Notebook auf einem PDA gespeichert liegen. Hier muss aus Sicht der Sicherheit das Unternehmen vergleichbare Anforderungen stellen, welche die deutlich leistungsschwächeren Handhelds vor große Probleme stellt.

Zum Zeitpunkt des Projektes (Anfang 2003) zeigte sich der Markt der Sicherheitssoftware für Pocket PC 2002 voller unausgereifter Produkte, die häufig in den ersten Versionen vorlagen. Der beste Kandidat Filecrypto wird zudem von F-Secure inzwischen in der untersuchten Enterpriseversion mangels Nachfrage nicht mehr vertrieben und löst auch nicht alle Sicherheitsprobleme der Pocket-PC-2002-Plattform. Ob der Vertrieb mit der jüngst verkündeten strategischen Partnerschaft zwischen den Unternehmen Pointsec und F-Secure wieder aufgenommen wird, bleibt abzuwarten.

Die größten Schwierigkeiten des Gesamtsystems manifestieren sich in den Bereichen Administration und Synchronisation. Zumindest die Administration lässt sich auf der funktionalen Ebene halbwegs zufrieden stellend von Afaria lösen, verursacht jedoch ein neues Sicherheitsproblem. Die mobile Synchronisation mit einem Exchangeserver kann angesichts der aufgetretenen Probleme nicht empfohlen werden. Eine einfache Arbeitsplatzsynchronisation

Systemeigene Security Features der Pocket-PC-Plattform

	Pocket PC 2002	Windows Mobile 2003
Authentifizierung	Power-on 4-stellig und stabil (7 oder mehr alphanumerische und Interpunktionszeichen); Passwort wird vor dem Speichern zerstückelt	
	Secure Socket Layer und Private Communications Technology ermöglicht sichere Website-Authentifizierung	
	Windows NT LAN Manager (NTLM) Challenge/Response dial-up Netzwerk Athentifizierung	
	Network file share password authentication im File Manager	
	CHAP, MS-CHAP Version 1 & 2, und PAP Virtual Private Networking Authentifizierung	
		RSA SecurID Support (Exchange Activesync unterstützt Authentifizierung in Verbindung mit RSA SecurID)
		WIFI Security 802.1x;systemeigener Support für viele Authentifizierungs-Algorithmen; EAP-TLS (Zertifikate), PEAP, und SSN
Verschlüsselung	Optional für Download und Installation: High Encryption Pack für Pocket PC für Anwendungen, die 128-bit Kryptographie und das Cryptographic Application Program Interface (CryptoAPI)	Native 128-Bit CAPI Verschlüsselung: (unterstützt 40-Bit, 56-Bit and 128-Bit symmetrische Verschlüsselung mit RC2, RC4, und DES. RSA encryption technology mit 16.384-Bit key lengths) wird auch unterstützt
	40-Bit SSL (https) und PCT-Verschlüsselung im Pocket Internet Explorer Web Browser. 128-Bit SSL optional mit High Encryption Pack für Pocket PC	Zusätzlich:SSL Inbox Support: Inbox unterstützt Secure Socket Layer (SSL) für IMAP- uns POP3--E-Mail, und für SMTP Server
	Virtual Private Networking (VPN) Point to Point Tunneling Protocol (PPTP) ist integriert im Pocket PC Connection Manager	Zusätzlich: Enhanced VPN Support: PPTP und IPSec Level 2 Tunneling Protocol (L2TP)
		Certificate Support für IPSec/L2TP VPN, 802.1x Authentifizierung, und Client Authentifizierung in Pocket Internet Explorer.
		WIFI Security: 802.1x systemeigener Support für viele Authentifizierungs-Algorithmen. EAP-TLS (Zertifikate), PEAP, and SSN
		Secure WAP with WTLS Class 2 support
Zusätzliche Security Services	Anti-Virus APIs für Anti-Virus Software Community	
	ActiveSync auf dem Pocket PC kann eine Sicherungskopie aller Daten erstellen und komplett wieder herstellen	
	Terminal Server client (RDP protocol) erhält Daten und Anwendungen auf dem Enterprise Server	
Security		Configuration Manager, damit Internet Service Provider Connectivity-Einstellungen für mobile Endgeräte programmatisch konfigurieren können (auch over-the-air, OTA)
		CAB Provisioning ermöglicht Provisioning von Compact Flash.- oder SD-Karten, etc., oder von einer Web-Seite

Device Management ist Voraussetzung für Sicherheit


Bild: Extended Systems

Horst Lange ist Geschäftsführer von Extended Systems

Horst Lange, Geschäftsführer Extended Systems: „Die Ergebnisse der Studie 'Mobiler Zugang zu gesicherten Netzen – Lösungen für die Zukunft' der TU Berlin können wir nachvollziehen. Sicherlich ist es ein Horrorszenario für jedes Unternehmen, wenn ein Mitarbeiter seinen privat angeschafften PDA mit wichtigen unternehmenskritischen Daten abgleicht, und ihm dieser PDA abhanden kommt. Wenn die Daten dann nicht geschützt und die Verbindung zum Unternehmensnetz unverschlüsselt eingerichtet werden kann, liegt ein echtes Sicherheitsrisiko vor.
Dieses Szenario zeigt, warum Unternehmen mobile Geräte zentral verwalten müssen. Ausschlaggebend für den Kunden ist dabei nicht unbedingt das eingesetzte Endgerät und dessen Sicherheitsfunktionalitäten, sondern das reibungslose Zusammenspiel des Backend-Systems, der mobilen Lösung und des Endgerätes. Durch eine Lösung basierend auf der Onebridge-Plattform von Extended Systems werden diese Anforderungen unterstützt. Die Sicherheit steht dabei besonders im Vordergrund: Onebridge-Lösungen sind RSA- beziehungsweise AES-verschlüsselt mit einer Schlüssellänge von bis zu 1.024 Bit, FIPS-zertifiziert bieten diverse Authentifizierungen wie Two-Tiers, verbindungsbasierend oder Secure-ID, unterstützen DMZ Proxy und speichern keine Daten auf fremden Servern zwischen. Durch dieses Maximum an Sicherheit ist der mobile Zugriff auf Informationen aus einem CRM- oder ERP-System sowie auf wichtige Groupware-Daten innerhalb einer Anwendung absolut sicher." *(SW)*

Sicherheit lässt sich aus der Ferne herstellen


Bild: Xcellenet

Christoph Jung ist Sales Manager Germany bei Xcellenet

Christoph Jung, Sales Manager Germany von Xcellenet: „ Eine der entscheidenden Fragen bei der Absicherung mobiler Clients ist: Wie kommt Security auf das Gerät? Hier leistet Systemmanagement-Software wie Afaria von Xcellenet wertvolle Dienste. VPN-Clients, sichere E-Mail-Clients und vieles mehr lassen sich von einer zentralen Stelle aus auf jeden Client verteilen. Darüber hinaus lassen sich auf diesem Wege auch Software- und Virus-Patches automatisch aufspielen und ausführen. Sämtliche Datenübertragungen, beispielsweise bei der Synchronisation von Datenbanken oder Dokumenten, erfolgen über sichere und in der Zentrale überprüfte Verbindungen. Der Aspekt Fernwartung spielt eine Rolle beim Thema Sicherheit. Der Agent auf den Geräten, der zur automatischen Herstellung der Verbindung verwendet wird, kann so konfiguriert sein, dass er die Festplatte des Geräts automatisch formatiert, wenn die Verbindung aufgebaut wird. Meldet beispielsweise ein Mitarbeiter den Verlust oder Diebstahl des Device, kann dieser Mechanismus sofort beim nächsten Aktivieren des Client ausgelöst werden. Gleiches gilt, wenn jemand versucht die Festplatte oder andere Speichermedien auszubauen und anderweitig in Betrieb zu nehmen." *(SW)*

Die TU-Studie weißt Defizite auf


Bild: Winlinx

Dr. Wolfram Knoblauch ist Senior Consultant bei Winlinx

Dr. Wolfram Knoblach, Senior Consultant bei Winlinx: „Wir befürworten sehr, dass Universitäten die Eignung von Produkten im IT-Umfeld untersuchen. Sie haben mehr Zeit für eine tief gehende technische Analyse und können kostengünstiger arbeiten. Bei eingehender Prüfung der Studie der TU Berlin stellten wir jedoch Defizite fest, die wir zur Diskussion bringen möchten. Die technische Einzelprüfung der untersuchten Produkte wurde meist sorgfältig durchgeführt und ausführlich dokumentiert, aber die daraus abgeleiteten Empfehlungen sind in ihrer Verallgemeinerung aus unserer Sicht nicht durchgängig haltbar. Das ist zum einen darauf zurückzuführen, dass die Marktanalyse unvollständig durchgeführt wurde und deshalb Produkte übersehen wurden, die die geforderte Leistung bieten. Außerdem wurden Produkte auch ohne explizite Prüfung auf Grund von 'Hören-Sagen' beurteilt, was zu inhaltlichen Fehlern in den Aussagen geführt hat. Wir wissen aus der Praxis, dass viele Unternehmen mit der untersuchten Pocket-PC-Plattform eine passende Lösung finden. Die Sicherheitsanforderungen der Unternehmen werden erfüllt und gleichzeitig ist die Lösung einfach zu bedienen und nachweislich mit hohem Nutzen verbunden. Für Außendienstmitarbeiter können PDAs durchaus als Ersatz für Laptops gelten. Wenn es um das Erfassen von komplexeren Dokumenten geht, muss der Einzelfall geprüft werden, egal um welchen Gerätetyp oder um welche Software-Plattform es sich handelt. Grundsätzlich gilt: Anforderungen müssen für jedes Unternehmen individuell analysiert werden. Eine ausführliche Kommentierung der Studie finden Sie unter: www.winlinx.de." *(SW)*

Windows Mobile 2003: Mehr Sicherheits-Features


Bild: Microsoft

Ulrich Keller ist Marketing Manager Business Group Mobility bei Mircrosoft Deutschland

Ulrich Keller, Marketing Manager Business Group Mobility bei Microsoft Deutschland: „Mit Pocket PC 2002 haben wir eine erfolgreiche mobile Software-Plattform im Markt. Unsere Partner entwickeln Security-Lösungen, die individuell an die Sicherheitsanforderungen der Unternehmen angepasst werden müssen. Mit Windows Mobile 2003 Software für Pocket PCs haben wir die Anregungen von Kunden und Partnern umgesetzt. Für Folgestudien der TU Berlin zu Windows Mobile 2003 stehen wir gern als Ansprechpartner zur Verfügung."

von Basisdaten ist möglich. Dafür erscheinen jedoch Pocket PC 2002 Handhelds zu teuer und überdimensioniert. Hier würden die seit längerer Zeit bereits auf dem Markt etablierten und preiswerteren Palm-PDAs völlig ausreichen und könnten zudem auf Softwareprodukte zurückgreifen, die bereits aus den Kinderschuhen herausgewachsen sind.

Reicht der eingeschränkte Funktionsumfang eines Basis-PDAs nicht aus, erscheint der Einsatz von Geräten der Subnotebook-Klasse mit vollwertigem Desktop-Betriebssystemen wie zum Beispiel Windows XP angeraten. Diese Klasse vereint die hohe Mobilität von PDAs durch geringe Größe und die Leistungsfähigkeit von Notebooks in einem Gerät. Zudem lassen sich bereits erprobte Sicherheits- und Administrationslösungen aus dem Notebook-Bereich anwenden.

Bei all den Überlegungen zur Sicherheit von IT-Systemen sollte ein Unternehmen einen Aspekt jedoch nie vergessen: Der klassische Papierorganizer verfügt weder über eine sichere Nutzer-Authentifikation noch über eine sichere Datenverschlüsselung. Es nützt nichts, sich in der Frage der Sicherheit nur auf die IT-Welt zu beschränken und die klassischen Medien zu ignorieren. Nur eine gesamtheitliche Sicherheitsstrategie kann die Sicherheit bieten, die man sich wünscht. *(SW)*