Mehr Sicherheit für PDA-Benutzer

Handheld? Aber Sicher!

Thomas Fritsch, Frank Pallas, Torsten Pehl

Handhelds verschiedener Fabrikate kommen in nahezu jedem Unternehmen zum Einsatz – doch was ist für einen sicheren Einsatz der kleinen Alleskönner zu beachten?

Nach der Cebit wird es wieder so weit sein: Die Damen und Herren aus dem Management bringen die neuen PDAs vom Messebesuch mit. Und da mit aktuellen Geräten nahezu „alles machbar“ ist, wollen ihre Eigentümer sie so intensiv wie möglich nutzen. Die Vorstellung, die wichtigsten Informationen wie PIM-Daten (Personal Information Manager), Mails oder ausgewählte Dokumente immer und überall in der Westentasche parat zu haben, überzeugt zwar Viele auf den ersten Blick. Wenn die Hersteller mittlerweile sogar Mobilfunkfähigkeiten integrieren und die Geräte mit VPN-Clients für den sicheren Fernzugriff ins Firmenintranet ausstatten, leuchten die Augen nahezu jedes TCO- und ROI-Rechners.

Handhelds besitzen jedoch, ähnlich wie Mobiltelefone, die unangenehme Eigenschaft, leicht verloren zu gehen. Den Verlust bemerkt man meist erst, wenn es zu spät ist und das aus der Tasche gerutschte Gerät im kurz zuvor verlassenen Taxi längst hinter der nächsten Ecke verschwunden ist. In so einem Fall ist die Aufregung (früher oder später) groß: Was, wenn der aktuelle Vertragsentwurf mit dem frisch akquirierten Großkunden oder die Gehaltslisten der oberen Managementebene in die falschen Hände gelangen? Und was ist mit der aus gutem Grund geheim gehaltenen Telefonnummer des Vorstandsvorsitzenden?

Eine nüchterne Betrachtung von Sicherheitsaspekten beim PDA-Einsatz bleibt angesichts der Euphorie über das mobile neue Wunderding oftmals aus. Das liegt auch daran, dass deren Beurteilung keinesfalls trivial ist. Denn anders als die seit Jahren in Unternehmen im Einsatz befindlichen Notebooks sind Handheld-Geräte nicht einfach kleine Computer, sondern eine völlig neue Geräteklasse. Sie besitzen eigene Systemarchitekturen sowie Betriebssysteme und basieren auf anderen Konzepten als die nahezu vollwertigen mobilen Arbeitsplätze in Form von Notebooks. Bleibt dann der kleine Liebling tatsächlich im Taxi liegen, ist es zu spät für ernsthaftes Nachdenken über Sicherheit. Dieser Artikel zeigt Problemfelder auf, die vor einem Einsatz der Geräte im Unternehmen unbedingt in der Planung Beachtung finden sollten.

Zugriff auf den Winzling einschränken

Schon das Beispiel des Geräteverlustes illustriert die grundlegenden Ansprüche an die Sicherheit. Abgelegte Daten sollten, ungeachtet ihrer tatsächlichen Brisanz, in jedem Fall vor den Augen des Taxifahrers oder anderer potenzieller Angreifer verborgen bleiben. Das betrifft die Sicherheit des Standalone-Geräts: Es darf einen Angreifer weder als autorisierten Nutzer einstufen, noch darf dieser Zugriff auf im Gerät lokal gespeicherte schützenswerte Daten bekommen.

iX 4/2004

Folglich fällt der erste Blick auf eine sichere Anmeldeprozedur. Die bei Auslieferung von Handhelds aktivierten Standardeinstellungen reichen in der Regel nicht aus oder verlangen überhaupt keine Anmeldung vom Nutzer. Die meisten Geräte bieten jedoch eine Aktivierung einer kurzen Zahlenkombination (PIN) oder eines Passwortes beliebiger Länge und Zusammensetzung als Zugangsschutz an. Vereinzelt existieren sogar Handheldmodelle mit eingebauten biometrischen Authentifizierungsmechanismen (wie Fingerabdruckscanner). Einige Produkte wie Utimacos Safeguard nutzen solche zusätzlichen Mechanismen. Andererseits bietet movianCrypt nur einfache Anmeldung per Passwort.

Mit den integrierten Mechanismen alleine lassen sich sensitive Daten jedoch nicht wirksam schützen – sie sind ähnlich wirksam wie die Schlösser von Tagebüchern. So ist ein unautorisiertes Login dank aktiviertem Passwort zwar ausgeschlossen, aber gebräuchliche Handheldgeräte legen die Daten ungeschützt im Speicher ab und ein Angreifer könnte diese – geeignete Ausrüstung vorausgesetzt - problemlos auslesen und auf alle gewünschten Daten zugreifen, ohne das Gerät anzuschalten.

Damit wird die aktivierte Login-Prozedur als einzige Sicherheitsmaßnahme sinnlos; sie erfordert unbedingt die Ergänzung durch eine Verschlüsselung der relevanten Daten. Besonderes Augenmerk sollte den PIM-Daten und potenziell sensiblen Dateien wie Office-Dokumenten gelten. Je nach Einsatzszenario fallen weitere zu schützende Daten an. Die Ideallösung schützte zwar den kompletten Speicher mit einem leistungsfähigen Chiffrieralgorithmus, wäre aber in der Praxis bei Handhelds momentan nicht einsetzbar.

X-TRACT

- PDAs bieten von Hause kaum Schutz vor unberechtigter Benutzung oder Datendiebstahl.
- Geeignete Zusatzprodukte schaffen mehr Sicherheit, indem sie Passwörter erzwingen und Dateien auf dem Gerät verschlüsseln.
- Im Unternehmen müssen solche Lösungen in Administrationswerkzeuge integriert sein, die unter anderem firmenweite Richtlinien umsetzen können.

Das liegt unter anderem daran, dass das Betriebssystem niemals komplett ausgeschaltet ist, sich also immer zumindest ein Teil von ihm im Speicher befindet. Außerdem widerspräche eine komplette Ver- und Entschlüsselung der „Schnell mal eben nachgucken"-Arbeitsweise. Wenn die Datensätze des Stadtplanes unverschlüsselt vorliegen, erscheint dies jedoch als weniger riskant als ein von jedem lesbarer Vertragsentwurf. Bis auf movianCrypt bieten alle Produkte das wahlweise Kodieren einzelner Dateien, aller PIM-Daten oder des gesamten Informationsbestandes an.

Ziffern, Buchstaben und Bilder

Sicherheitslösungen ersetzen im Regelfall zumindest die Anmeldeprozedur der Handhelds, kombinieren dies jedoch häufig mit verschiedenen Möglichkeiten zur Verschlüsselung sensitiver Daten. Die angebotenen Mechanismen und zu Grunde liegenden Algorithmen unterscheiden sich allerdings stark voneinander. Hier reicht es nicht, nur auf den Namen verwendeter Algorithmen und den angebotenen Leistungsumfang zu schauen. Nur Trustdigitals Produkt bietet überhaupt mehr als einen Verschlüsselungsalgorithmus an, alle anderen setzen auf das aktuelle AES. Die Implementierung der angebotenen Verschlüsselungsalgorithmen sollte beispielsweise nach FIPS 140 oder den Common Criteria zertifiziert sein und auf Standardbibliotheken beruhen. Einige neuere Betriebssysteme für Handhelds bieten hier bereits integrierte Schnittstellen für Entwickler.

Die Vielfalt der vorhandenen Sicherheitsprodukte zwingt zu genauen Vorüberlegungen über den gewünschten Grad der Sicherheit und die wichtigsten zu erfüllenden Anforderungen. Reichen zum Beispiel kurze PINs oder müssen es komplexe alphanummerische Passwörter sein? Was passiert, wenn der PDA in der Kaffeepause eingeschaltet liegen bleibt? Welche Daten sind zu schützen? Verlängert sich durch die Ver- beziehungsweise Entschlüsselung der Datenbanken die Zeit bis zur Betriebsbereitschaft? Sollen die Verfahren kombiniert werden (etwa PIN und Fingerabdruckscanner oder PIN und Hardware-Token)?

Eine sinnvolle Alternative zu den gebräuchlicheren Anmeldeverfahren mittels PIN oder Passwort können Verfahren sein, die auf Bildfolgen oder Symbolen beruhen. Dadurch vermögen sich Anwender Passwörter leichter zu merken, etwa anhand von kleinen Geschichten als visuelle Gedankenstützen, sodass sie sie nicht auf der Rückseite der Geräte notieren oder auf einem Zettel in der Brieftasche spazieren tragen. Drei der Produkte in der Tabelle „PDA-Sicherheitslösungen" bieten solche Login-Prozeduren per Bild. Lassen sich die verwendeten Bilder bei jeder Anmeldung unterschiedlich auf dem Bildschirm positionieren, vermeidet man zudem, dass ein Angreifer aus einiger Entfernung lediglich die Handbewegungen des Benutzers beobachten muss und daraus auf das Zugangspasswort schließen kann. Bei Geldautomaten begegnen die Aufsteller dieser Gefahr durch Sichtblenden – wenig praktikabel für Handhelds. Auch alternative Verfahren, zum Beispiel Handschriftenerkennung, sind einsetzbar und eine Überlegung wert.

Rechte des Benutzers einschränken

Was geschieht jedoch, wenn der Benutzer der eingebauten hochmodernen und sicheren Anmeldeprozedur oder der Performance zehrenden Verschlüsselung überdrüssig wird? Was passiert, wenn er ein neues Programm aus dem Netz auf dem Handheld installiert haben möchte?

Unterliegt bei Arbeitsplatzrechnern und Notebooks jeder Wunsch nach der neuesten Softwareversion oder kleinen nützlichen Tools für die tägliche Arbeit unweigerlich dem strengen Blick des Benutzerservice, so lockt die mobile bunte Welt moderner Handhelds mit vielen kleinen Miniprogrammen. Dank ihrer in der Standardausstattung uneingeschränkten Zugriffsmöglichkeiten können Anwender diese Programme nach Belieben selbst aufspielen und entfernen. Handheldbetriebssysteme sind nicht Multiuser-fähig, deshalb fehlen Rechte- und Nutzerverwaltung und damit die von Notebooks bewährten Kontrollmöglichkeiten. Im Auslieferungszustand, sogar mit Datenverschlüsselung und Zugangsschutz, hat der autorisierte Nutzer Zugriff auf alle Funktionen des Gerätes und kann nach Belieben das Passwort zum Login deaktivieren sowie eigene Programme installieren.

iX 4/2004

PDA-SICHERHEIT

Produkt	SafeGuard PDA	movianCrypt	Pointsec	PDA Secure + Trusted Mobility Server
Hersteller	Utimaco Safeware AG	certicom	Pointsec Mobile Technologies	Trust Digital
unterstützte PDAs	Pocket PC 2002, Windows Mobile 2003	Palm OS 3.x, 4.x, PocketPC 3.0, 2000/2002	Pocket PC, PalmOS, Windows Mobile 2003, SymbianOS (UIQ)	PalmOS, PocketPC , SymbianOS
Authentifizierungsmethoden				
Ziffern-PIN	✓	–	✓	✓
erweiterte PIN (grafische Symbole etc.)	✓[1]	–	✓	✓
Passwort/-phrase	✓	✓	✓	✓
Mindestanforderungen an das Passwort	✓	–	✓[6]	✓
Handschrifterkennung	✓	–	–	–
Fingerabdruckscan	✓[2]	–	–	–
Zeitpunkt der Authentifizierung				
beim Einschalten	✓	✓	✓	✓
regelmäßige Abstände	–	✓	–	nur für PocketPC
nach Inaktivität	✓	–	optional	✓
bei der Synchronisierung	✓	✓	✓	✓
bei IR/BT/WLAN/GSM/GPRS-Verbindung	–	–	–	✓
beim Aktivieren von Anwendungen	–	✓	–	✓
beim Ändern von Einstellungen der Sicherheitssoftware	✓[3]	✓	–[7]	k. A.[9]
bei verlorengegangenem Passwort				
Freischaltung durch Anwender	✓[4]	✓	–	✓[10]
Freischaltung durch Admin/Dritte	✓	–	✓[8]	✓
Schutz gegen Brute-Force-Attacken				
Sperre nach mehrmaligen Fehlversuchen	✓, Anzahl konfigurierbar	✓	✓, Anzahl konfigurierbar	✓, Anzahl konfigurierbar
Sperre nach Fehlversuchen mit Hard-Reset und Löschen aller Daten	✓	–	–	✓
Sperre mit Löschen des Speichers und aller Anwendungen durch sicheres Überschreiben	✓	–	–	✓
Fehler verlängert Wartezeit zwischen Eingaben	✓	–	–	✓
Sperrungen nur duch Master-Key aufhebbar	✓	–	✓[7]	✓
Benutzereinfluss auf Authentifizierung				
kein Einfluss	✓[5]	–	✓	✓
Passwort, PIN etc. wählbar	✓[5]	✓	✓	✓
Art der Authentifizierung wählbar	✓[5]	–	vom Administrator konfigurierbar	–
Einstellungen modifizierbar	✓[5]	✓	–	–
Authentifizierung abschalt- oder deinstallierbar	✓[5]	✓	–	–
Krypto-Algorithmen				
RC4/AES/Twofish/Blowfish/TEA/XOR	AES	AES	AES	alle +3DES (Schlüssellänge wählbar)
sicheres Löschen durch Überschreiben	✓	–	–	✓, 4-fach überschreiben
Schutz vor Desinstallation	✓	–	✓	✓
Was wird verschlüsselt?				
PIM/Mail/Externe Medien/individuell festgelegte Daten/Backup-Daten/Mail-Attachments/komplettes Dateisystem	✓/✓/✓/✓/✓/✓/–	–/–/–/–/–/–/✓	✓/✓/✓/✓/✓/✓/–	✓/✓/✓/✓/✓/✓/✓
Dokumentation (Sprache, Format, Umfang)	D/E/F; PDF + online auf PDA	E	E; PDF; 94 Seiten	E;PDF
Kosten pro Client	ca. 30 € (Personal Edition), ca. 76 € (Enterprise Edition)	ab 20 €	83 € bei einer 5-jährigen Laufzeit	ab 23 €
Wartungs/Updatekosten	auf Anfrage	ab 6 € nach dem ersten Jahr	15 % des Lizenzpreises pro Jahr	20 % des Lizenzpreises
Demoversion erhältlich	✓	✓	Evaluation der Vollversion	✓
Kontakt/Website	www.utimaco.de info.pds@utimaco.de	www.webtogo.de dberinger@webtogo.de kpalestis@webtogo.de	www.pointsec.com	www.ubitexx.com

[1] eigene Symbole definierbar [2] auf IPAQ 545x/555x [3] zentral einstellbar für jeden Wert [4] Master-Passwort bei Personal-Edition; telef. Challenge/Response-Verfahren bei Enterprise-Edition [5] Einflussmöglichkeiten des Benutzers zentral konfigurierbar [6] vom Administrator konfigurierbar (min./max. Länge, History, Fehlversuche) [7] Anwender kann Einstellungen nicht ändern [8] Nach telefonischem Challenge-Response Austausch mit Helpdesk
[9] Benutzer kann keine Änderungen vornehmen [10] nur in Verbindung mit der Administrator-Konsole Alle Preise zzgl. MwSt.
✓ vorhanden – nicht vorhanden k. A. keine Angaben

iX 4/2004

Und warum sollte er denn nicht aus Bequemlichkeit der Datenbestand des PDAs neben dem gesicherten Arbeitsplatzrechner am heimischen PC synchronisieren? Dumm nur, wenn Sohnemann den ganzen Tag auf dem Computer im Internet gedaddelt und sich dabei den neuesten Virus eingefangen hat. Die dienstliche Dockingstation stellt kaum ein Hindernis dar. Allzu schnell ist eine eigene private bestellt, die zu Hause die Verbindung zwischen Privatrechner und Handheld herstellen kann. Mit deren Hilfe landet der frische Virus erst auf dem PDA und bei der nächsten Synchronisierung in der Firma in deren Netz.

Richtlinien definieren und durchsetzen

Eine zentrale Anforderung an den Einsatz von Handhelds im Unternehmen ist deshalb die Kontrolle der Nutzung und die Verwaltung des eingesetzten Geräteparks. Der Einsatz von Administrationslösungen geht damit über das Verwalten und Inventarisieren mobiler Devices hinaus und ist wesentlicher Faktor bei der Sicherheit im Unternehmenseinsatz.

Gängige Verschlüsselungsapplikationen gibt es oftmals neben der Endkunden- in einer kostspieligen Enterprise-Version, die beispielsweise die zentrale Verwaltung von Richtlinien (Policies) für Passwortlänge und -zusammensetzung oder für zu verschlüsselnde Datenbereiche (ausgewählte Verzeichnisse oder Dateitypen) erlauben. Der Benutzer kann bei diesen Produkten, anders als in den meisten Standardversionen, die Verschlüsselung und die Anmeldeprozedur nicht komplett deaktivieren. Und auch der Taxikunde, der den verlorenen Handheld findet, kann selbst mit Cracker-Werkzeug nicht mehr ohne weiteres auf die nun vor üblichen Crackern geschützten Datenbestände zugreifen. Zwar gibt es spezialisierte Entschlüsselungsverfahren, die auf der Wärmeverteilung auf der CPU oder der Analyse von Antwortzeiten beruhen, aber diese sind bislang eine Domäne des Militärs.

Solche Policies müssen Teil der Administration sein und sich von den dafür benutzten Werkzeugen auf die Handhelds verteilen und dort durchsetzen lassen. Allerdings sind sie nur eine Notlösung für den Ersatz einer echten Rechteverwaltung und die Fähigkeiten eines Mehrbenutzer-Betriebssystems.

Zudem darf die Kontrolle der Sicherheitssoftware und damit der Anmeldeprozedur und Verschlüsselung auf dem Handheld nur ein Aspekt der Nutzung von Policies sein. Denn die unerlaubte Synchronisation am heimischen Arbeitsplatz lässt sich so in der Regel nicht verhindern. Die vielen Möglichkeiten der Handhelds, auf unterschiedlichen Wegen Verbindung zu anderen Geräten aufzunehmen, erfordern gesonderte Betrachtung.

VPN hängt von Infrastruktur ab

Bei der Kommunikation zwischen Handheld und Firmennetz erledigen oft VPN-Clients und -Server die sichere Verbindungsaufnahme und -verschlüsselung. Hier gibt es unzählige Varianten mit unterschiedlichen Vor- und Nachteilen. Viele VPN-Lösungen und Verbindungsoptionen (RAS-Einwahl, GPRS et cetera) ermöglichen flexible Konfigurationen, die nicht immer einfach zu integrieren sind, aber bei entsprechendem Kosten- und Zeitaufwand zumindest realisierbar erscheinen. Die Wahl konkreter VPN-Produkte hängt vor allem von der bestehenden Infrastruktur im Unternehmen ab. Wo es nur um gelegentliche gesicherte Verbindungen geht, können die bei einigen Betriebssystemen mitgelieferten PPTP- oder L2PT-Clients hilfreich sein.

Ungewünschte Verbindungen abseits der Kontaktaufnahme zur mobilen Synchronisation mit dem Firmennetz unterliegen in der Standardausstattung keiner Einschränkung. Der Aussteller, der auf der Messe dem interessierten Manager per Infrarot den neuesten Prospekt oder die elektronische Visitenkarte überspielt, könnte jedoch genauso gut ein Angreifer sein oder einfach der unwissentliche Verbreiter eines Makrovirus, der später nach der Synchronisation am Arbeitsplatz das ganze Firmennetz lahm legen wird. Die vertrauensvoll in den Erweiterungsslot gesteckte Speicherkarte mit der Demoversion eines viel versprechenden Projektierungstools könnte in Wirklichkeit die Daten des Handhelds kopieren.

Autorisierung der Kommunikationspartner findet bei Handhelds bisher praktisch nicht statt. Zwar können ausgefeilte und teure Administrations- und Sicherheitslösungen zumindest Infrarotschnittstellen und ähnliches deaktivieren, scheitern jedoch oft an gesteigerten Ansprüchen, wenn zum Beispiel die Kontaktaufnahme mit dem unsicheren Privatrechner verhindert werden soll. Zwar gibt es Notlösungen; diese schaffen aber unter Umständen neuen Ärger. So können einige Produkte die eingebaute Synchronisationsschnittstelle (Hotsync oder Activesync) deaktivieren und durch einen spezialisierten Synchronisationsclient ersetzen, der dank geeigneter Policy nur Verbindung mit dem firmeninternen Synchronisationsserver aufnehmen kann. Das setzt den austauschbaren Daten und den Einsatzmöglichkeiten im mobilen Betrieb dem ohnehin eingeschränkten Funktionsumfang der Handhelds jedoch noch engere Grenzen. Erst in jüngster Zeit mehren sich die Ankündigungen, dass Konzepte und Erweiterungen in Softwareprodukte einfließen, die autorisierte und genau definierte Sync-Partnerschaften auch auf Handhelds ermöglichen.

Fazit

Viele bunte Werbeprospekte und glitzernde Messestände dürfen nicht darüber hinweg täuschen, dass der sichere Einsatz von PDAs in Unternehmen immer noch Risiken aufwirft. Ohne durchdachte Sicherheits- und Administrationskonzepte verursacht die Einführung der kleinen Rechner gerade in größerer Anzahl mehr Probleme als sie der Produktivität nutzt. Handhelds sind eine eigenständige Geräteklasse und verlangen derzeit noch umfangreiche Anpassungen bestehender Strukturen. Das erfordert Aufwand und Kosten, aber die Anstrengungen können sich durchaus auszahlen. Im Auslieferungszustand stellen die Geräte zudem ein hohes Sicherheitsrisiko dar. Das gewünschte Maß der Sicherheit hängt von verschiedenen Faktoren ab und beeinflusst insbesondere die Benutzbarkeit der Geräte. Wie stark die Fähigkeiten des PDAs aus Sicherheitsgründen beschnitten werden, muss dabei für den konkreten Einsatz genau abgewogen werden. (ck)

DIE AUTOREN

arbeiten an der Technischen Universität Berlin im Forschungsgebiet „Mobiles Arbeiten" und beschäftigen sich dabei insbesondere mit der Integration von Handhelds in bestehende Infrastrukturen.

ADMINISTRATIONSSOFTWARE – FRAGEBOGEN

Produkt	Afaria 5.0	OneBridge Mobile Groupware	Manage Anywhere Studio
Hersteller	XcelleNet	Extended Systems	iAnywhere Solutions
Server-Plattformen (Hardware)	Intel	Intel	Intel
Server-Plattformen (Betriebssysteme)	Windows 2000/2003 Server	Windows NT/2000 Server	Windows NT 4.0 Server/2000/XP
unterstützte PDA-Betriebssysteme	Windows Mobile/PocketPC 2000/CE, Palm OS; SymbianOS; Java	Windows HPC/PocketPC/Mobile/ SmartPhone, PalmOS, SymbianOS, browser-basierte Geräte	Windows CE/Pocket PC 3.0/Mobile, PalmOS 3.x,BlackBerry
Größe Client/Serversoftware	< 1 Mbyte/abhängig von der Zahl der Clients	k. A.	k. A.
Funktionsumfang			
Daten-Synchronisierung	✓[1]	✓	✓.
Software-Synchronisierung	✓	✓	✓
Übernahme von Benutzern/Gruppen aus LDAP/ADS/NIS	✓[2]	✓	✓
Verwaltung von Benutzer-/Gruppen-einstellungen	✓[3]	✓	✓ [4]
Passwortverwaltung			
Administrator kann neues Passwort verlangen	✓	–	✓
Einschalt-Passwort auf PDA erzwingbar	✓	✓	✓
Verschlüsselung			
bei der Datenübertragung (wie)	SSL, Crypto-API	RSA OAEP 1024 Bit; AES 128 Bit; CFB-Modus mit 128 Bit basierend auf AES-Algorithmen	SSL
der Daten auf dem Server (wie)	über beliebige Verschlüsselungsdienste	keine Benutzerdaten auf dem Sync-Server	✓[5]>
Protokolle			
Ereignisprotokolle (auf Server, Endgerät)	detaillierte LOG-Dateien auf dem Server	Server: MMC-basierte Listen einschließlich parametrierbarer Event-Viewer-Protokolle Endgerät: Log-Protokoll des letzten Vorgangs	k. A.
Fehlerprotokolle (auf Server, Endgerät)	Auswertung der LOG-Dateien auf dem Server (in SQL-Datenbank gehalten) über beliebige, teils vordefinierte, teils selbst-definierbare Kriterien	Server: MMC-basierte Listen einschließlich parametrierbarer Event Viewer-Protokolle Endgerät: Log-Protokoll des letzten Vorgangs	k. A.
Dokumentation	Client; 7 Sprachen einschl. D, 66 S./ Server: E, einschließlich API-Referenz > 1000 S.	E, online	E, PDF, 394 S.
Kosten pro Server/Client	auf Anfrage	k. A.	Basispaket: 472 ?, Kosten je nach Gerät ab 28 ?
Wartungs/Updatekosten	20 % vom gezahlten Preis per anno	abhängig von Service- und Wartungsvertrag	Wartungs- und Updateverträge
Demoversion erhältlich	zeitlich beschränkte Vollversion	kostenfreie Testversion für 30 Tage	✓
Kontakt/Website	info.de@xcellenet.com, www.xcellenet.com	www.extendedsystems.de/ info@extendedsystems.de	www.ianywhere.com

[1] Anbindung an mehrere Datenbanken gleichzeitig möglich
[2] Anbindung, kein Import/Export
[4] auch geräteabhängig
[5] Verschlüsselung der Datenbank möglich

iX 4/2004

	PDA Secure + Trusted Mobility Server
	Trust Digital
	Intel
	Windows NT, 2000, 2003, XP-Pro
	Windows Pocket PC/CE, PalmOS, SymbianOS
	ca. 300 KByte / ca. 125 Mbyte
	Policy Push via TCP
	zentrale Verteilung der PDASecure Software + Policy
	LDAP / ADS / NIS
	✓ – hierarchisch strukturiert
	✓
	✓
	3DES
	✓[6]
	Eventlogs auf dem Server für jeden Nutzer abrufbar – Clientprogramm liefert die Daten
	Ablauf- und Ereignisprotokolle auf dem Server abrufbar – Cllientprogramm liefert die Daten
	E, PDF
	ab 3000 ??
	20 % Support und Wartung auf den Lizenzpreis
	✓: www.pdasecure.de
	www.ubitex.com

[3]über Verzeichnisdienst oder geräteabhängig
[6]abhängig von der Datenbank

iX 4/2004