

Sicherheit im Umgang mit mobilen Daten

Mit Sicherheit unterwegs

Mobile Geräte unterliegen gerade auf Reisen besonderen Risiken. Unterbinden Sie den unerwünschten Datenzugriff bei gestohlenen oder verloren gegangenen Geräten schon vorab. **Jörg M. Freiberger**

Auf einen Blick

Inhalt

Daten werden auf stationären PCs und häufig zusammen mit Servern und mobilen Endgeräten (etwa Notebooks, Laptops, Smartphones oder PDAs) eingesetzt. Unabhängig davon, auf welchem Gerät Sie die Daten letztendlich bearbeiten, müssen Sie für einen einfachen Datenaustausch sorgen und die Daten im Nachhinein wieder durch eine Datensynchronisation angleichen. Doch welche Bedeutung hat dabei die Datensicherheit? Dieser Artikel widmet sich genau diesem Thema und bietet eine allgemeine Diskussion mit dem Fokus auf der Datensicherheit bei mobilen Endgeräten.

Schwerpunkt

Tools und Verhaltensweisen, Sicherheit mit .NET und dem Compact Framework

Voraussetzungen

Grundlagen .NET, Mobile Geräte

Autor

Dipl.-Ing. Jörg M. Freiberger ist Leiter des Competence Center .NET bei der MT AG in Ratingen. Darüber hinaus beschäftigt er sich seit mehr als neun Jahren als Autor und Dozent mit technischen und projektorientierten Themen im Software Engineering auf der Microsoft-Plattform.



Laptops, Mini-Laptops, Pocket PCs oder Smartphones machen Daten mobil (Bild 1)

Mobile Versionen der Betriebssysteme für PDAs, Smartphones & Co. kommen schon fast an das Niveau und den Leistungsumfang von Betriebssystemen der Desktop- und Notebook-Varianten zum Jahrtausendwechsel heran (Bild 1). Die kleinen Helferlein stecken in unseren Taschen, weil wir immer und überall online sein wollen. WAP, EDGE, GPRS, HSCSD und wie sie alle heißen – Netzwerkverbindungen sind prinzipiell überall möglich. Doch wie steht es mit der Sicherheit der sensiblen Datenträger? Neben E-Mail, Adressbuch und Kennwörtern sind auch die (sensiblen) Anwendungsdaten auf mobilen Geräten zu schützen. Dieser Artikel beschäftigt sich zum einen mit speziellen Tools zur Verschlüsselung. Zum anderen bietet er einen Überblick über die Sicherheitsfunktionen bei der Anwendungsprogrammierung mit dem .NET Framework.

Gefahr und Abwehr

Natürlich machen Sie sich in der heutigen Zeit mehr und mehr Gedanken über die Sicherheit Ihrer Daten. Denn es vergeht mittlerweile kaum

eine Woche, in der nicht schon wieder der Diebstahl von Kreditkarteninformationen oder Bankdaten in die Schlagzeilen kommt, weil irgendjemand diese hochsensiblen Daten aus einer Datenbank gezogen und auf eine CD gebrannt hat. Eine Meldung wie „Übers Internet ersteigert: Festplatte mit Konteninformationen zehntausender Bürger aufgetaucht“ ist dementsprechend nur eine Nachricht unter vielen, die auf Lücken im Bereich der Datensicherheit hindeuten.

Gegen solche Fälle kann man als Normalbürger kaum etwas ausrichten. Was allerdings zum Selbstschutz wesentlich beitragen kann, ist die Verschlüsselung von Daten im – nennen wir es einmal – persönlichen Einflussbereich. Hierzu gehören beispielsweise die heimischen PCs oder die mobilen Geräte, die Sie ständig bei sich tragen und die über Netzwerkverbindungen (beispielsweise WLAN, Bluetooth) Daten mit anderen Geräten oder auch über das Internet austauschen.

Bei einer Verbindung mit einem Netzwerk sollte die Kommunikation optimal geschützt sein. Je nach Verbindungsart kommen dazu ver-

schiedene Technologien wie WEP/WPA, VPN oder SSL zum Einsatz. Was passiert allerdings, sollte das Gerät verloren gehen? Wie sind die Anwendungsdaten auf mobilen Geräten vor unerwünschtem Zugriff Dritter zu schützen?

Anwendungssicherheit

Wie bei lokalen Anwendungen sollte ein Benutzer authentifiziert werden, wenn er mit sensiblen Daten auf mobilen Geräten arbeitet (vergleiche [1]). Deshalb sollten mobile Applikationen eine Benutzeranmeldung anbieten. Auch dann, wenn dies für den Endbenutzer eines mobilen Geräts (beispielsweise eines Smartphones) mit zusätzlichem Aufwand verbunden ist.

Geht das mobile Gerät verloren, lassen sich so zumindest die lokalen Daten schützen. Doch in der Regel werden die Anwendungen derart programmiert, dass Benutzername und Kennwort einmalig eingerichtet werden und so bei jedem Start der Anwendung die Anmeldung des Benutzers automatisch erfolgt. Besser wäre eine Abfrage der Kombination Benutzer/Kennwort (User/Passwort) bei jedem Start.

Datenspeicherung

Eine recht einfache Lösung zum Schutz sensibler Daten – zumindest bei einem Verlust des Geräts – ist die Speicherung der sensiblen Daten nicht auf dem Gerät direkt, sondern auf einer zusätzlichen Hardware, beispielsweise einer SD-Karte oder einem Memorystick. Voraussetzung ist natürlich, dass die Karte beziehungsweise der Stick nicht gleich zusammen mit dem mobilen Gerät verloren geht!

Eine andere Vorgehensweise ist, Daten nicht lokal, sondern in einer zentralen Instanz abzulegen, die per Netzwerk zu erreichen ist. Eine solche zentrale Datenhaltung bietet darüber hinaus den Vorteil, dass die Daten von unterschiedlichen Geräten aus zugänglich sind und demnach nicht (!) redundant vorliegen oder gar bearbeitet



MicroSD-Karte von Certgate (Bild 2)

Synchronisierung mit dem Backoffice

Mit den Microsoft-Dienstprogrammen ActiveSync und Mobile Device Center richten Sie auf mobilen Geräten mit den Systemen Windows CE oder Windows Mobile Partnerschaften ein.

Bei Verbindung mit entsprechenden Entitäten werden (Unternehmens-)Daten synchro-

nisiert. Hierzu gehören beispielsweise ein Datenabgleich bei Outlook-Kontakten mit dem Exchange-Server oder eine Dateisynchronisierung und eine Nutzung von Zertifikaten. Für Lotus-Produkte gibt es zum Beispiel XTNDConnect PC von Sybase, um unter anderem Kontakte, Kalender und E-Mails abzugleichen.

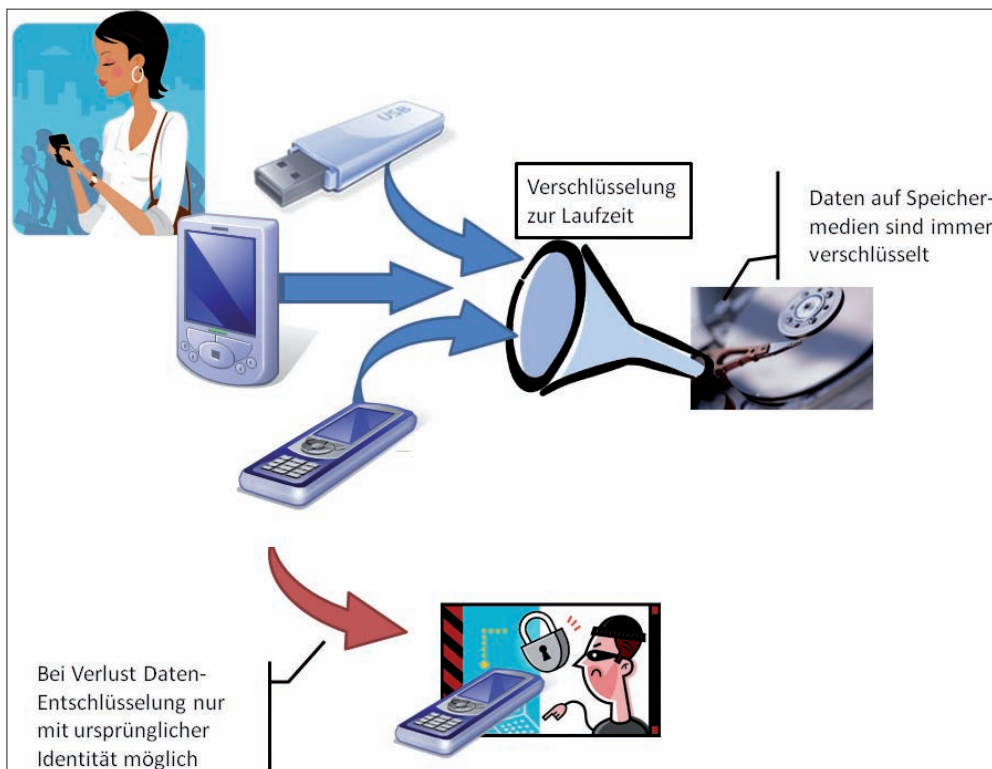
werden müssen. Daten müssen aber nicht zwangsläufig auf einem Datenspeicher in einem lokalen Netzwerk abgelegt werden (zum Beispiel auf einem Dateiserver oder einem NAS-Server), auch das Internet stellt zunehmend Datenspeicher über Webserver bereit, um Daten weltweit ohne Wechselmedium verfügbar zu machen (Cloud Computing). Einen Schritt weiter geht die Datenhandhabung dann, wenn bei zentraler Datenhaltung von Zeit zu Zeit ein Abgleich mit dem mobilen Gerät stattfindet. Dies geschieht im Alltag beispielsweise bei der Arbeit mit E-Mails und Kontakten. Unter Windows-Systemen kann dort mit ActiveSync oder Mobile Device Center eine Synchronisierung dieser Daten wahlweise mit dem eigenen PC oder mit dem Backoffice-Server erfolgen (siehe Textkasten „Synchronisierung mit dem Backoffice“). Für den Datenabgleich mit Webservern oder auch FTP-Servern kommen spezielle Synchronisationstools zum Einsatz, die die URL-Adressierung und die Internetprotokolle entsprechend beim Datenabgleich unterstützen.

Desktop-PC und mobile Geräte

Viele Überlegungen, die für die Anwendungssicherheit auf Desktop-Maschinen oder bei Webanwendungen gemacht werden, gelten ebenso bei mobilen Anwendungen. Zum Beispiel sollten Anwendungen nach einem Timeout gesperrt und Passwörter auf keinen Fall im Klartext abgelegt werden. Konfigurationseinstellungen in einer XML-Datei sind einfach auszulesen und Benutzereingaben sind in der Regel nicht vertrauenswürdig, zumindest nicht, wenn Sie dies nach Sicherheitsaspekten beurteilen.

Authentifizierung und Autorisierung

Die Autorisierung ist der Vorgang, bei dem die Entscheidung getroffen wird, ob eine Identität die aktuell geforderte Operation ausführen darf, oder es handelt sich um die ►



Bei Verlust ist eine Entschlüsselung der Daten nicht möglich (Bild 3)

Überprüfung von Zugriffsrechten auf Ressourcen. Zuvor ist eine Authentifizierung durchzuführen, wobei eine Überprüfung einer behaupteten Identität erfolgt. Die Authentifizierung des Endbenutzers am mobilen Gerät erfolgt in aller Regel überhaupt nicht. Das kaum vorhandene Sicherheitsbewusstsein ist häufig sogar so stark eingeschränkt, dass kaum jemand sein Firmen-Handy mit der PIN schützt. Sicher ist es eine etwas umständliche Prozedur, sich zuerst am Handy anzumelden und dann auch noch in eine Anwendung einzuloggen. Aber dies könnte dann wiederum recht komfortabel gestaltet werden, wenn in beiden Fällen lediglich eine PIN einzugeben wäre. Das Verfahren PIN/PUK hat sich bei SIM-Karten zum Telefonieren bereits seit langem etabliert. Heutzutage ist bei smarteren mobilen Geräten immer wieder von einer 2-Faktor-Authentifizierung die Rede, bei der eine Kombination aus zwei Verfahren zum Einsatz kommt (vergleiche Textkasten „2-Faktor-Authentifizierung“).

Zertifikate

Sehr wichtig in diesem Zusammenhang ist, dass alle Sicherheitsaspekte nicht nur für den Endbenutzer am mobilen Gerät Gültigkeit haben. Auch das Gerät selbst sollte beim Zugriff aufs Backend authentifiziert werden. Als Beispiel sei hier die Verwendung von digitalen Zertifikaten genannt. Diese zertifikatbasierte Authentifizierung stellt eine interessante Form dar, um Anmeldeinformationen zu übermitteln und die Identität von Endbenutzer und Gerät zu bele-

gen. Dies kann dann in Verbindung mit SSL eingesetzt werden und später beim Zugriff auf einen Exchange 2007 Server. Wenn Exchange entsprechend vorkonfiguriert ist, werden nur Geräte zugelassen, die ein gültiges Client-Zertifikat zur Benutzerauthentifizierung installiert haben und über ein vertrauenswürdigen Stammzertifikat für den Server verfügen.

Hardware

Bei der Arbeit mit hochsensiblen Daten in kritischen Umgebungen, wie zum Beispiel Behörden oder Krankenhäusern, ist eine hardwaretechnische Lösung zu empfehlen. Mittlerweile haben sich auch hier einige Hersteller etabliert. Ein Beispiel ist das SmartCard-System der Certgate GmbH [2]. Hier kommt eine MicroSD-Karte zum Einsatz, die Hardware-Zertifikate tragen kann und als sicherer Datenspeicher dient (Bild 2). Mithilfe dieser Lösung lassen sich Dateien und E-Mails verschlüsseln und sogar Manipulationen an Daten und Anwendungen verhindern. Der Zugang zum Gerät ist mit einer PIN geschützt, die Zertifikate werden für die anderen Leistungsmerkmale benötigt.

Ein weiterer bekannter Anbieter ist Pointsec [3], dessen Produkte Authentifizierungslösungen bieten und zuverlässig Smartphones sowie PDAs schützen. Unterstützung finden die Betriebssysteme Symbian, Pocket PC, Windows Mobile und Palm. Daten auf Gerät und Speicherkarten werden automatisch verschlüsselt. Hier erfolgt jedoch keine zusätzliche Unterstützung bei der Authentifizierung des Geräts ge-

2-Faktor-Authentifizierung

Die sogenannte 2-Faktor-Authentifizierung behebt Probleme, die sich bei der Verwendung einfacher Passwörter ergeben. Passwörter sind häufig zu schwach und daher ein hohes Sicherheitsrisiko. 2-Faktor-Authentifizierung ist einfach zu handhaben und gilt in Fachkreisen als bestmöglicher Schutz vor unbefugtem Zugriff. Wer Zugang zu einem System haben möchte, braucht zwei Dinge: etwas, was er besitzt, und etwas, was er weiß. Der Besitz ist beispielsweise eine Hardwarekomponente in Form einer SmartCard, einer SD-Karte oder eines USB-Sticks. Das Wissen ist nach wie vor ein Passwort oder eine PIN. Nur in Kombination beider Dinge können sich PC-Nutzer sicher authentifizieren, ihre Daten unabhängig von der Übertragung verschlüsseln und Dokumente signieren.

genüber dem Backend. Die Firma Charismathics bietet mehrere Lösungen im Umfeld von mobilen Geräten an. Dies beinhaltet sowohl softwareals auch hardwaretechnische Ansätze für Anwender und die Industrie [4]. E.siqia aus der Schweiz bietet gar eine SmartCard-Lösung (unter Verwendung der Certgate-Hardware) für mobile Geräte unter Linux an [5].

Verschlüsselung

Ein Denkansatz bei der Verschlüsselung von Daten, der sich in der Softwareindustrie in anderen Zweigen (zum Beispiel Webportalen oder klassischen Client-Server-Anwendungen) leider noch nicht durchsetzen konnte, ist im Gegensatz dazu bei mobilen Geräten schon lange bekannt: Die Verschlüsselung wird derart durchgeführt, dass bei Verlust des Gerätes kein Dritter Zugang zu den Daten hat.

Dieses Prinzip wird jedoch dadurch erschwert, dass die Bandbreite der in einem Unternehmen eingesetzten mobilen Geräte sehr groß ist. Neben Notebooks und Tablet-PCs kommen PDAs oder Smartphones sowie externe Speichermedien zum Einsatz. Des Weiteren werden Geräte wie MP3-Player, Handys oder Digitalkameras oftmals zweckentfremdet als Speicher für Unternehmensdaten genutzt. Deshalb ist es recht schwierig, zum einen überhaupt den Überblick zu behalten und zum anderen die Daten und damit gleichzeitig auch das Unternehmen zu schützen. Unter solch „modernen Umständen“ unterliegen Sie demnach ständig der Gefahr, dass Daten verloren gehen und in die falschen Hände geraten.

Im Klartext: Die Sicherheitslösung muss alle Geräte umfassen. Im Idealfall wird Hardware, die zum ersten Mal mit einem Unternehmens-Netzwerk oder einer anderen -Hardware in Verbindung gebracht wird, direkt in die Schutzmaßnahmen eingebunden. Das bedeutet, dass beispielsweise eine SD-Karte, die zum ersten Mal in ein Firmen-Smartphone eingesetzt wird, vor einer Datensynchronisierung automatisch aufgespürt werden muss. Die Sicherheitsinfrastruktur sollte in der Lage sein, anwender- und geräteabhängig die Benutzung des Speichermediums zu erlauben oder zu verbieten. Gleichzeitig muss eine Verschlüsselung der Daten auf dem Speichermedium erfolgen – bei zentralisierter Steuerung.

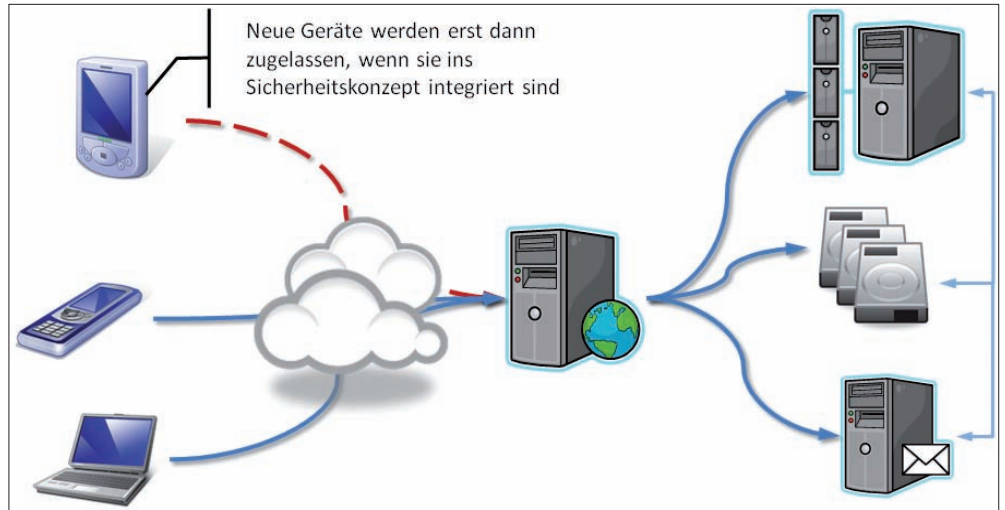
Dies hört sich zunächst „sicher“ an. Doch bei einem zweiten Blick und mit dem Gedanken im Hinterkopf, dass die meisten Angriffe intern erfolgen, zeigt sich ein weiteres Problem: Übergibt zum Beispiel der CFO (Chief Financial Officer – Finanzvorstand) eines Unternehmens sein Smartphone dem zuständigen Support-Mitarbeiter zwecks Upgrade, hat dieser voll-

ständigen Zugriff auf das Gerät und alle Daten, zumindest sofern er das Festplatten-Passwort kennt. Aus diesem Grund sollten auch die System- und die Sicherheitsadministration getrennt werden. Ein Verantwortlicher für die Sicherheit darf lediglich die Möglichkeit haben, Sicherheitsrichtlinien zu implementieren. Dies beinhaltet unter anderem eine benutzerspezifische Datenverschlüsselung auf mobilen Endgeräten und umfasst ganze Laufwerke oder einzelne Dateitypen. Auf diese Weise lassen sich gezielt für kritische Umgebungen Regeln aufstellen, die einen Datenzugriff für einen eingeschränkten Personenkreis oder Gruppen zulassen. Die Sicherheitsrichtlinien sollten möglichst auch die Nutzung externer Speichermedien betreffen, wobei alle Anwendungsdaten (etwa Kontaktlisten, E-Mails oder Tabellen mit Finanzdaten des Unternehmens) einschließlich der Anhänge oder Mediendateien zu verschlüsseln sind. Die Daten liegen immer verschlüsselt auf einem Speichermedium! Selbst dann, wenn das Gerät eingeschaltet wird und der Endbenutzer sich erfolgreich authentifiziert hat, bleiben die Daten verschlüsselt und werden erst bei Zugriff zur Laufzeit ent- und wiederverschlüsselt (Bild 3).

Wie dies funktionieren kann, sei kurz am ►

Tabelle 1: Ausgewählte Sicherheitssoftware für mobile Geräte

Produkt	Beschreibung
Trend Micro Mobile Security	Das Produkt bietet unter anderem eine Echtzeit-Datenverschlüsselung für den Datenschutz bei Verlust eines Geräts. Daten sind auf dem Gerät und (externen) SD-Karten verschlüsselbar. Bei Nichteinhaltung von Authentifizierungsrichtlinien (Kennworthistorie, Timeout etc.) lassen sich automatisiert Daten löschen. Eine zentrale Verwaltung erlaubt die administrative Erstellung und Verteilung von Richtlinien und Einstellungen. Per Administration lassen sich auch Aktualisierungen (Updates) über eine drahtlose Datenverbindung (WiFi, GPRS, EDGE, EV-DO usw.) oder mittels ActiveSync übertragen [6].
Symantec Mobile Security	Auch dieses Produkt bietet zentrale Administrationsmöglichkeiten, um Leistungsmerkmale wie Verschlüsselung und Aktualisierungen zu verwalten. In Verbindung mit Symantecs Mobile VPN sind recht einfach sichere Verbindungen zwischen Gerät und Netzwerkressourcen herstellbar [7].
Utimaco Safeguard PDA	Utimaco ist ein Hersteller, der eine Softwarelösung zur Verschlüsselung anbietet. Die Lösung schützt mobile Geräte durch Authentisierung gegen unbefugte Inbetriebnahme. Daten lassen sich nicht nur verschlüsseln, sondern auch sicher per Mail übertragen. Auch hier gibt es wieder die Möglichkeit der zentralen Administration [8].
Sybase OneBridge Mobile Groupware	Dieses Produkt verspricht die sichere Übermittlung von E-Mails und Daten (Kalender, Kontakte, Notizen, Aufgaben) auf zahlreichen Plattformen (z. B. Windows Mobile und Palm OS) und unterschiedlichen Verbindungstechnologien (GPRS, UMTS etc.) zu verschiedenen Servern (u. a. Exchange und Lotus Notes) [9].



Übersicht über eine mobile Unternehmensstrategie (Bild 4)

Beispiel der bereits erwähnten Lösung von Certgate erläutert: Beim ersten Einsatz der MicroSD-Karte startet eine *autorun.exe*-Anwendung und installiert selbstständig Treiber und Anwendung. Der Treiber zur Verschlüsselung wird dann dynamisch geladen und ermöglicht die Verschlüsselung und Entschlüsselung einzelner Partitionen eines Flash-Speichers auf Basis eines Hybrid-Verfahrens mit AES 256/RSA 2048 Bit. Das Schlüsselpaar wird bei erstmaliger Verwendung auf der Certgate-SmartCard generiert oder ist wahlweise auch importierbar. Für ein Unternehmen gilt es also, nicht nur eine Verschlüsselung der Daten auf mobilen Geräten zu erreichen, sondern eine „mobile Unternehmensstrategie“ aufzustellen (Bild 4). Kein Anbieter von Antiviren- und „Anti-alles“-Softwarelösungen kommt an diesem Markt vorbei. In Tabelle 1 sind nur einige Softwareprodukte in diesem Umfeld zusammengestellt.

.NET Compact Framework

Wenn die Sicherheit, wie bisher beschrieben, bei mobilen Geräten im Nachhinein so einfach einzurichten ist, warum dann bei der Entwicklung von Anwendungen überhaupt darüber nachdenken? Tools und Hardware zur Verschlüsselung und Authentifizierung, deren Verwendung eine Architektur ohne Sicherheitsaspekte zulassen, existieren? Also: „Lasst uns einfach mal im-

plementieren, für die Sicherheit sorgen dann später die Administratoren!“

Diese Betrachtung stimmt nur in Teilen. Denn es ist ja nicht nur wichtig, die Daten auf einem mobilen Gerät zu schützen oder den Zugriff eines unbekanntes Geräts auf das (Firmen-)Netzwerk zu unterbinden. Wichtig ist auch ein Schutz des Geräts dahingehend, dass eine neue Anwendung lediglich diejenigen Ressourcen erhält, die aufgrund bestimmter Eigenschaften (der Anwendung) erlaubt sein sollten. Was nutzt eine Verschlüsselung der Daten auf einer Partition des eingesetzten Speichermediums, wenn eine fremde Anwendung auf dem Gerät diese Daten im laufenden Betrieb auslesen und versenden kann?

Ein weiteres Anwendungsbeispiel ist die Speicherung der Daten auf einer mobilen Version einer SQL-Datenbank. Automatisierte Tools wie die, die zuvor vorgestellt wurden, können nicht gezielt Tabellen verschlüsseln. Doch diese sollen möglichst anwendungs- und benutzerspezifisch auszuwerten sein. In solchen Szenarien ist es hilfreich, wenn sich ein Architekt oder Entwickler bereits beim Design der neuen Anwendung entsprechende Gedanken macht.

Die Programmierung mit dem Microsoft .NET Compact Framework, das seit Januar 2008 in der Version 3.5 verfügbar ist, erleichtert die Entwicklung von Sicherheitsfunktionen – jedoch nicht in allen Lebenslagen. Im Vergleich zum .NET Framework für Desktops enthält es lediglich abgespeckte Versionen der Namensräume und Klassenbibliothek, ist jedoch speziell für den Einsatz auf Geräten wie Pocket PCs, Smartphones und PDAs ausgerichtet. Bild 5 illustriert den Funktionsumfang des .NET Compact Framework. Für eine umfassende grafische Darstellung des .NET Framework, die auch die Unterschiede zwischen .NET Framework und .NET Compact Framework im Detail beinhaltet, folgen Sie bitte der Internetadresse [10]. Darüber

Code Access Security

Die Code Access Security (CAS) soll die Ausführung sicherheitskritischer Aktionen über .NET-Programmcode unterbinden.

Im .NET-CAS-System wird Code anhand von Eigenschaften der Zugriff auf angeforderte Ressourcen erlaubt oder verweigert. Per Konfiguration wird auf einer Windows-Maschine festgelegt, in welche Codegruppe eine An-

wendung einzustufen ist und welche Berechtigungen Anwendungen einer solchen Codegruppe haben. So lässt sich beispielsweise definieren, dass lokal installierte Programme auf ein bestimmtes Verzeichnis der Festplatte zugreifen dürfen, während aus dem Web heruntergeladenen Anwendungen keinerlei Festplattenzugriff gewährt wird. Dies funktioniert jedoch nur mit .NET-Anwendungen.

erhalten Sie ein vollständiges Klassendiagramm zum .NET Framework 3.5, in dem die Elemente des Compact Framework mit der Kennung „CF“ markiert sind. Im Bild werden lediglich die hell hinterlegten Namensräume im Compact Framework 3.5 unterstützt, und hiervon jeweils nur ein Teil aller darin enthaltenen Klassen. Dies macht etwa 30 Prozent des gesamten Frameworks aus. Sollen Ressourcen von mobilen Geräten, wie beispielsweise eingebauter Speicher oder eine WAN-Verbindung, geschützt werden, dann kann dies nicht mit .NET-Bordmitteln erfolgen. Die in .NET spezielle Code Access Security (kurz: CAS) wird im Compact Framework überhaupt nicht unterstützt. Allerdings ist diese Unterstützung für zukünftige Versionen geplant (siehe Textkasten „Code Access Security“).

Eine Verschlüsselung von Daten wird in der Compact-Framework-Klassenbibliothek unterstützt. Sollen Daten in einer mobilen Datenbank abgelegt werden, dann lassen sich diese aus der Anwendung heraus verschlüsseln. Dies kann auch benutzerspezifisch geschehen. Somit lassen sich Daten – zumindest unter mobilen Windows-Betriebssystemen – dann auch in einer für Tools von Drittanbietern nicht unterstützten oder zugänglichen Datensinke schützen. Auch die Handhabung von X509-Zertifikaten implementieren Sie mit dem Compact Framework. Aufgrund einiger Einschränkungen des Compact Framework treten gegebenenfalls die folgenden Probleme auf:

- Es gibt keine Unterstützung für CAS. Deshalb sollten Anwendungen, die mit der Desktop-Version von .NET entwickelt wurden, mit Vorsicht zur mobilen Version konvertiert werden. So sollten beispielsweise Sicherheitsanforderungen und Handhabung von Codegruppen aus dem Code entfernt werden.
- Es gibt keine Unterstützung für das Attribut *AllowPartiallyTrustedCallers*. Dieses spezielle Attribut, das im Zusammenhang mit vertrauenswürdigen Aufrufen verwendet wird, kann nicht benutzt werden. Für die Programmumsetzung ist ein anderes Design erforderlich.
- Vorsicht, wenn Aktualisierungen für mobile Geräte verteilt werden sollen. Eventuell gibt es Leistungsmerkmale im Update, die die aktuelle Version des Compact Framework auf dem Gerät überfordern.

Regeln im Umgang mit mobilen Geräten

Einige wichtige Regeln sollten bei der täglichen Arbeit mit und um mobile Geräte in jedem Fall beachtet werden:

- **Verschlüsselung der Daten:** Sowohl für Endanwender als auch für Architekten und Entwickler sollte dies oberste Priorität haben. Die Verschlüsselung sollte so erfolgen, dass bei Verlust des

Geräts kein Dritter die Daten auslesen kann.

- **Authentifizierung:** Außer einem Mehraufwand durch zusätzliche Hardware (per SmartCard beispielsweise) kann in manchen Fällen auch eine einfache Authentifizierung per PIN-Eingabe gute Sicherheit bieten.
- **VPN:** Unerwünschte Netzwerkbenutzer können bei Einsatz eines VPN durch Verschlüsselung, Authentifizierungs- und Autorisierungsprozesse ferngehalten werden. Gut durchdachte Lösungen erlauben eine zentrale Konfiguration und Verwaltung der Remote-Zugänge.
- **Mobile Speichermedien:** Kleine und feine Speichermedien sind unheimlich populär. Jedoch können über SD-Karten unerwünschte Eindringlinge wie Viren und Würmer eingeschleust werden und das mobile Gerät wird so zum Trojanischen Pferd für das Unternehmen.
- **Zu guter Letzt:** Schützen Sie Ihr mobiles Gerät durch die PIN und ändern Sie die standardmäßig vergebene Werkseinstellung (zum Beispiel „0000“ oder „1234“). **[am]**

[1] Jörg M. Freiberger, *Tresor auf Reisen; database pro 2/2009, Seite 78 ff.*
 [2] Certgate SmartCards; www.certgate.com/web_de/produkte/index.html
 [3] CheckPoint Sicherheitsprodukte; www.checkpoint.com/products/datasecurity/mobile/index.html
 [4] Charismathics Sicherheitsprodukte; www.charismathics.com/
 [5] E.siqia Whitepaper; www.esiqia.com/fileadmin/pdf/whitepaper/080708_microSD_T30_Linux_Zypad_Rev_1.20.pdf
 [6] TrendMicro mobile Datensicherheit; <http://de.trendmicro.com/de/products/enterprise/mobile-security/index.html>
 [7] Symantec-Tool für mobile Sicherheit; www.symantec.com/de/ch/business/mobile-security-suite-for-windows-mobile
 [8] Utimaco Sicherheits-Tools; www.utimaco.de/
 [9] Sybase OneBridge Mobile Groupware; www.sybase.de/detail?id=1053503
 [10] PDF mit .NET-Framework-3.5-Übersicht; http://download.microsoft.com/download/4/a/3/4a3c7c55-84ab-4588-8a44-f9642a7d82d/NET_35_Namespaces_Poster_JAN08.pdf

Überblick über die Namensräume im Compact Framework 3.5 (Bild 5)

