Die Welt der PKI, der Bereitstellungen und der Anwendungen hat sich beträchtlich weiterentwickelt, seit Microsoft in Windows XP und Windows Server 2003 die Benutzerzertifikatregistrierung eingeführt hat. Uns war zwar klar, dass wir die Art und Weise ändern würden, wie Public Key-Infrastrukturen aufgebaut und bereitgestellt werden, aber wir waren überrascht, wie schnell sich der Markt ändern und die Bereitstellungen erfolgen sollten. Als wir die Veröffentlichung der Microsoft PKI für Microsoft Windows 2000 vorbereiteten, wollten wir sie so einfach wie möglich gestalten, damit sie sich durchsetzen kann und wie TCP/IP, Kerberos oder die Arbeit im Web praktisch überall zum Alltag gehört. Um dieses Ziel zu erreichen, mussten zwei wichtige Kriterien erfüllt werden:

- Die Konfiguration und Verwaltung von Zertifizierungsstellen sollte möglichst einfach sein.
- Endbenutzer sollten sich nicht mit der PKI beschäftigen und sie auch nicht verstehen müssen.

Natürlich unterscheiden sich die Bereitstellungen und jede Anwendung stellt andere Ansprüche, aber anscheinend hat die Welt eine einfache, kosteneffiziente und sichere Infrastruktur gebraucht, um den wachsenden Bedarf an Verschlüsselung, Datenschutz und Authentifizierungsmöglichkeiten in einer Umwelt zu decken, die sich zunehmend als feindlich darstellt. Wenn wir nun, 5 Jahre später, den Erfolg an unseren Zielen messen, bin ich angesichts der großen Zahl an Bereitstellungen und angesichts der Ausgereiftheit der Public Key-Infrastrukturen mehr als angenehm überrascht. Es vergeht praktisch keine Woche, in der ich nicht höre, dass ein weiterer Kunde mit einem einzigen Windows Server 2003-Zertifikatserver Millionen Zertifikate für IPsec ausgestellt hat oder dass ein Unternehmen eine Smartcard-Lösung für die Anmeldung bei Remotezugriffen und VPN-Benutzung installiert hat. Dauerte es vor nicht allzu langer Zeit noch Monate, die erforderlichen Installationen durchzuführen, und Jahre, um große Bereitstellungen abzuschließen, ist es nun eher eine Sache von Tagen. Auch große Bereitstellungen lassen sich in wenigen Monaten erledigen.

Trotz der Ausgereiftheit der PKI und der Massenbereitstellungen entwickelt sich die Technik natürlich weiter und passt sich an die geänderten Sicherheitsrisiken, Angriffe und Anforderungen an. Kunden, Konsumenten und Unternehmen werden sich zunehmend der Risiken bewusst und verlangen nach Verschlüsselung und anderen Sicherheitsmaßnahmen, die erforderlich sind, wenn sensible Informationen gespeichert oder übertragen werden. Das führt zu steigenden Anforderungen an die Leistung, Zuverlässigkeit und Eignung der Plattformen und der Anwendungen. Windows Server 2008 bietet die neusten Verbesserungen in den Bereichen Verschlüsselung, Leistung und Optimierung.

Windows Server 2008 bietet die neuste Technologie und Aktualisierungen, um für die sich ständig weiterentwickelnden Ansprüche und Sicherheitsanforderungen gerüstet zu sein. Es bietet nicht nur die neusten Hashalgorithmen und asymmetrische Verschlüsselungstechnologien mit öffentlichen Schlüsseln sowie eine moderne Zertifikatsperrungsinfrastruktur, sondern es bietet diese Fähigkeiten auf einer modernen, flexiblen Kryptografieplattform. Das Besondere an Windows Server 2008 ist die Einführung von Cryptography Next Generation (CNG), das es Hardwareherstellern, Softwareentwicklern und Kunden ermöglicht, ihre eigenen Algorithmen einzufügen und zu verwenden, ohne auf eine vollständige Überarbeitung oder Aktualisierung der Windows-Plattform warten zu müssen. Das ist ein wesentlicher Schritt, der es der Infrastruktur ermöglicht, sich dynamisch weiterzuentwickeln, falls sich die Sicherheitslage unvorhergesehen ändert.

Neben den neuen Algorithmen, Verschlüsselungsmethoden und Protokollen bietet Windows Server 2008 auch noch andere Erweiterungen für die Verwaltung und Bereitstellung, wie die Integration von SCEP (Simple Certificate Enrollment Protocol), das MOM-Überwachungspaket (Microsoft Operations Manager) und Inlinesperrdienste, die OCSP-Clients (Online Certificate Status Protocol) unterstützen. Wenn Sie sich die Verbesserungen und den Funktionsumfang von Windows Server 2008 ansehen, werden Sie wohl der Einschätzung zustimmen, dass sich der Technologiebereich weiterentwickelt und reift.

Wie sieht die weitere Zukunft von PKI aus? Wäre ich ein Orakel und könnte die Zukunft vorhersagen, würde ich wohl sagen, dass die Integration der Kartenverwaltungssysteme weitergehen wird, dass auch Identitätsverwaltungssysteme integriert und die nächste Generation der Bereitstellungsmethoden in die neusten Webdienste und Drahtlos- oder Funknetzwerkprotokolle integriert sein werden. Ich denke, dass man Windows Server 2008 als Vorschau auf viele dieser Integrationen betrachten kann, wobei natürlich noch andere Microsoft Produkte wie der Identity Lifecycle Manager, das System Center und Forefront eine Rolle spielen.

Warum ein zweites Buch über Microsoft PKI? Weil der Markt für PKU und die Active Directory-Zertifikatdienste es erfordert. Insgesamt sind nicht viele Bücher über PKI erschienen, aber ich denke, dass Microsoft Press mit diesem Buch einen tatsächlich bestehenden Bedarf deckt. Das Buch konzentriert sich auf die praktische Bereitstellung und auf die Bedürfnisse von IT-Profis. Zudem behandelt es das PKI-System mit der weltweit größten Verbreitung, nämlich die Active Directory-Zertifikatdienste.

Brian Komar hat sich zu einer Leitfigur und zum weltweit ungeschlagenen Meister der Microsoft PKI-Vision und deren praktischer Umsetzung entwickelt. Auf seine besondere Weise bietet er IT-Profis und Unternehmen eine pragmatische Sicht der Dinge, wobei er gleichzeitig auf die Fallstricke, die kleinen Tricks und Empfehlungen hinweist, die man vor Beginn einer Bereitstellung kennen sollte. Brian hat sich das Wissen, das er in diesem Buch präsentiert, im Verlauf seiner langjährigen Zusammenarbeit mit dem PKI-Produktentwicklungsteam in Redmond und im Rahmen zahlloser Kundenaufträge erworben, in denen es um die Bereitstellung der Microsoft PKI-Lösung ging.

Für den Microsoft PKI-Administrator ist dieses Buch unverzichtbar. Es fasst das Wissen des Produktentwicklungsteams, die Empfehlungen unserer weltweit tätigen Berater (Microsoft Consulting Services) und die Erfahrungen aus unseren bisherigen Bereitstellungen zu einer einzigartigen Quelle des Praxiswissens zusammen. Das Ziel dieses Buchs ist es, die Umsetzung des Vorhabens zu unterstützen, mit dem wir vor vielen Jahren begonnen haben, nämlich Kunden in die Lage zu versetzen, in ähnlich einfacher Weise, wie andere wichtige Netzwerkinfrastrukturen aufgebaut werden, ein PKI-System bereitzustellen, das ihren Ansprüchen an die Sicherheit und an den Schutz der Anwendungen genügt. Ich warte eigentlich schon auf den Tag, an dem PKI im Internet ein ebenso gebräuchlicher Ausdruck wie „IP-Adresse“ ist. Ich denke, dass wir mit Leuten wie Brian, die ihr Wissen so gekonnt weitergeben können, auf dem richtigen Weg sind.

Dezember 2007

David B. Cross
Director of Program Management Windows Security
Microsoft Corporation

Einführung

Willkommen bei Windows Server 2008 PKI- und Zertifikat-Sicherheit. Dieses Buch bietet Ihnen detaillierte Informationen über den Entwurf und die Implementierung von PKI-Lösungen (Public Key-Infrastruktur) mit Windows Server 2008-Zertifizierungsstellen. Das Buch beruht auf den Whitepapers und den Richtlinien des PKI-Produktteams von Microsoft und auf der Erfahrung, die ich in den letzten 5 Jahren bei der Arbeit mit den Microsoft Consulting Services und bei Kunden sammeln konnte.

Über das Buch

Sie können das Buch natürlich auf herkömmliche Art von vorne nach hinten durchlesen, sich aber auch auf die Bereiche konzentrieren, die Sie noch nicht kennen. Das Buch wurde in drei eigenständige Teile gegliedert, die jeweils mehrere Kapitel umfassen. Jedes Kapitel endet mit einer Fallstudie, in der die beschriebenen Konzepte aufgegriffen und umgesetzt werden. Auf diese Weise können Sie überprüfen, wie weit Sie die Konzepte beherrschen.

HINWEIS:
Die Antworten auf die Fragen zu den Fallstudien stehen im Anhang „Antworten zu den Fallbeispielen“. Diesen Anhang gibt es nicht nur in der herkömmlichen gedruckten Form des Buchs, sondern auch im englischsprachigen eBook, das Sie auf der Begleit-CD des Buchs finden.

Das Buch besteht aus folgenden drei Teilen:

- **Teil 1, „PKI-Grundlagen“** Teil 1 bietet einen Überblick über Kryptografie- und PKI-Konzepte und enthält eines der wichtigsten Kapitel dieses Buchs, „Richtlinien und PKI“. Teil 1 hilft Ihnen dabei, die Zusammenhänge zwischen PKI und den Sicherheitsrichtlinien Ihrer Organisation zu verstehen. Ohne strenge Richtlinien und präzise Vorschriften ist eine PKI nichts weiter als eine Ansammlung von Anwendungsservern und kein Mechanismus zur Sicherung Ihres Netzwerks mit seinen Anwendungen.

- **Teil 2, „Einrichtung einer PKI“** Teil 2 erläutert die Grundkonzepte für den Entwurf und die Implementierung einer PKI in einer Organisation und beschreibt unter anderem die Vorbereitung der Active Directory-Domänendienste (AD DS) sowie den Entwurf und die Implementierung einer Zertifizierungsstellenhierarchie. Teil 2 enthält den Entwurf von Zertifikatvorlagen, die Vorbereitungen für die Verteilung der Zertifikate an die entsprechenden Benutzer und Computer sowie Empfehlungen zum Schutz gegen Systemausfälle und zur Wiederherstellung des Systems danach. Am Ende von Teil 2 steht Ihre Zertifizierungsstellenhierarchie so weit, dass sie an alle PKI-fähigen Anwendungen, die von Ihrer Organisation benutzt werden, Zertifikate ausgeben kann. Außerdem beschreibt dieser Abschnitt die Sicherung der Verfügbarkeit einer Zertifizierungsstelle durch die Erstellung eines Clusters und die Implementierung von OCSPs (Online Certificate Status Protocol).

- **Teil 3, „Bereitstellen anwendungsspezifischer Lösungen“** Teil 3 bietet ausführliche Informationen über die Verteilung und Installation von Zertifikaten für bestimmte PKI-

fähige Anwendungen. In jedem Kapitel dieses Teils wird beschrieben, welche Zertifikate für die betreffenden Anwendungen erforderlich sind und wie man die Zertifikate am besten an die Benutzer und Computer übermittelt und installiert. Außerdem werden Empfehlungen für den Einsatz der PKI-fähigen Anwendungen gegeben. In dieser zweiten Ausgabe des PKI-Buchs wurden neue Anwendungen hinzugefügt. Dazu gehören der Microsoft Identity Lifecycle Manager 2007 (ILM 2007), die digitale Signatur von Dokumenten, die Bereitstellung von Zertifikaten für Domänencontroller und die Registrierungsdienste für Netzwerkgeräte (NDES). Außerdem wurden die Kapitel über Smartcards und über die Implementierung von SSL (Secure Sockets Layer) für Webserver stark überarbeitet.

HINWEIS:
Wenn man ein Buch schreibt, muss man leider den vorgesehenen Umfang einhalten. Um den nicht zu überschreiten, konnte ich leider keine Kapitel über die Bereitstellung von Zertifikaten für NAP (Network Access Protection) und RDP (Remote Desktop Protocol) ins Buch aufnehmen. Daher habe ich Informationen über diese beiden Technologien auf die Begleit-CD dieses Buchs genommen, damit Sie zumindest Basisinformationen über diese Technologien erhalten.

Die Begleit-CD

Auf der Begleit-CD zu diesem Buch finden Sie verschiedene Programme und Skripts, die Ihnen bei der Einrichtung einer Windows Server 2008-PKI und bei der Ausgabe von Zertifikaten an Computer helfen sollen, auf denen Windows 2000, Windows XP, Windows Server 2003, Windows Vista oder Windows Server 2008 läuft.

HINWEIS:
Die Skripts werden ohne jegliche Garantie zur Verfügung gestellt und dienen lediglich als Beispiele dafür, wie Sie Skripts zur Konfiguration Ihrer Windows Server 2008-PKI-Bereitstellung verwenden können.

Wenn Sie die Microsoft Knowledge Base befragen möchten, gehen Sie auf: http :// www .microsoft .com/learning/support/search.asp. Sollten Sie Fragen zum Betriebssystem Windows haben, finden Sie im Lieferumfang Ihres Produkts weitere Informationen zum Support.

Systemvoraussetzungen

Um die Skripts von der Begleit-CD verwenden zu können, müssen folgende Voraussetzungen erfüllt sein:

1. Sie können die Skripts von der Begleit-CD auf einem Computer verwenden, auf dem Windows 2000, Windows XP, Windows Vista, Windows Server 2003 oder Windows Server 2008 ausgeführt wird. Die speziellen Anforderungen an das Betriebssystem werden in den Kapiteln genannt, in denen die Skripts beschrieben werden.

2. Die Zertifikatdienste können Sie nur auf einem Computer bereitstellen, auf dem Windows Server 2003 oder Windows Server 2008 Standard, Enterprise oder DataCenter ausgeführt wird.

3. Eine eigenständige Zertifizierungsstelle in einer Zertifizierungsstellenhierarchie sollte auf einem Computer eingerichtet werden, auf dem Windows Server 2003 oder Windows Server 2008 Standard ausgeführt wird.

4. Eine ausstellende Zertifizierungsstelle sollte auf einem Computer eingerichtet werden, auf dem Windows Server 2003 oder Windows Server 2008 Enterprise oder DataCenter ausgeführt wird.

WEITERES MATERIAL FINDEN SIE ONLINE:
Wenn neues oder aktualisiertes Material verfügbar wird, das dieses Buch ergänzt, wird es auf der Microsoft Press Online Windows Server and Client-Website bereitgestellt. Zu dem Material können aktualisierte Passagen des Buchs, Artikel, Verknüpfungen zu Begleitmaterialien, Fehlerkorrekturen, Beispielkapitel und ähnliche Dinge gehören. Diese Website ist unter www .microsoft .com/leaming/books/online/serverclient verfügbar und wird regelmäßig aktualisiert.

Der Autor

Brian Komar ist der Vorsitzende und Mitbegründer von IdentIT, einer Consulting-Firma, die sich auf Identitätsintegration und Netzwerksicherheit spezialisiert hat. Zusammen mit Brians Geschäftspartner Paul Adare berät IdentIT Microsoft-Kunden bei der Einrichtung von PKIs und in Fragen der Identitätsverwaltung und Netzwerksicherheit.

Brian hat in den letzten Jahren mehrere Bücher zum Thema Computersicherheit verfasst, darunter Microsoft Windows - Die technische Referenz, MCSE-Training Kit: Designing Microsoft Windows 2000 Network Security und Firewalls for Dummies. Neben diesen Büchern hat Brian auch drei Whitepapers über PKI-Themen für Microsoft geschrieben: „Implementing and Administering Certificate Templates in Windows Server 2003“, „Troubleshooting Certificate Status and Revocation“ und „Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003“. Und er hat den Microsoft Official Curriculum-Kurs 2821 über PKI mit dem Titel „Designing and Managing a Windows Public Key Infrastructure“ entwickelt. Brian hält zudem häufig Vorträge auf Konferenzen der IT-Branche, zum Beispiel auf der Microsoft Tech Ed, der Windows Connections und dem Microsoft IT Forum. Brian bietet tiefergehende Beschreibungen, die auch schon einmal einen Blick hinter die Bühne werfen, und beschreibt praxisorientierte Implementierungen der Sicherheitssysteme, in die seine Praxiserfahrungen einfließen.

In seiner (spärlichen) Freizeit spielt Brian Volleyball oder Golf und unternimmt Wanderungen mit seiner Frau Krista.

Wenn Sie Kontakt mit Brian aufnehmen möchten, erreichen Sie ihn unter brian.komar @ identit .ca.

Danksagungen

An der Entstehung eines Buchs sind auf die eine oder andere Weise viele Menschen beteiligt. Ich möchte mich nun, so gut es geht, bei allen bedanken, die mir beim

Schreiben dieses Buchs geholfen haben. Sollte ich versehentlich jemanden nicht erwähnen, so liegt das nur daran, dass erstaunlich viele Menschen an der Entstehung beteiligt waren.

Zuerst möchte ich den derzeitigen und ehemaligen Mitgliedern des PKI-Produkt- und Testteams von Microsoft danken: David Cross, Vic Heller, Phil Hallin, Avi Ben-Menahem, Oded Ye Shekel, Jen Field, Kelvin Yiu und Yogesh Mehta. Sie haben mir dabei geholfen, einige der schwierigeren Punkte der Microsoft PKI und der neuen Funktionen von Windows Server 2008 zu verstehen.

Insbesondere möchte ich mich bei Avi, Oded, Jen und Carsten Kinder bedanken, die viele der Whitepapers schrieben, mit denen ich mich in die neuen Themen der zweiten Ausgabe eingearbeitet habe. Eure Whitepapers halfen mir, die Technologie zu verstehen und so manche der entscheidenden Feinheiten zu erkennen.

Die zweite Gruppe, der ich danken möchte, sind die Kunden, mit denen die Firma IdentIT in den letzten 5 Jahren die Ehre und das Vergnügen hatte, zusammenarbeiten zu dürfen. Paul Adare und ich haben während der Arbeit mit Ihnen und Ihren Netzwerken mehr gelernt, als Sie sich vorstellen können.

Ein Buch ist nur so gut wie das Projektteam, das den Autor bei der Umsetzung seiner Gedanken in einen lesbaren Text unterstützt. Bei den folgenden Personen möchte ich mich ganz besonders bedanken:

- Martin DelRe, dem Produktplaner, dafür, dass er das Buch bei Microsoft Press empfahl.
- Seth Scruggs, Chris Gregory und Shawn Rabourn dafür, dass sie mich zum Schreiben einer zweiten Ausgabe bewegten.
- Denise Bankaitis dafür, dass sie das Projekt am Laufen gehalten hat (insbesondere vor dem Hintergrund, dass Teile des Buchs anscheinend über alle Kontinente verstreut entstanden sind - wieder einmal …).
- Paul Adare für das hervorragende fachliche Lektorat des Inhalts. Es hat mich zwar Stunden gekostet,
die Korrekturen einzuarbeiten, aber das Buch hat von Deiner Arbeit und Deinem Wissen profitiert.
- Dem Trustworthy Computing Security Content Review Board (TwC SCRB), einem Microsoft-Team, das jedes einzelne Kapitel überprüft hat, um für eine möglichst hohe technische Genauigkeit zu sorgen und die Beschreibungen mit den Produktbeschreibungen und Erklärungsmodellen von Microsoft abzugleichen. Zum SCRB-Team dieses Buchs gehörten David Kennedy, Shawn Rabourn, Jonathan Stephens, Michiko Short, Elton Tucker, Ken Carr, Sanjay Pandit, Jose Luis Auricchio, Matthijs ten Seldam, Akshat Kesarwani, Edward Gomes, Lupe Brieno, Anders Brabxk, Mark Eden und Monica Ene-Pietrosanu. Ein besonderes Dankeschön geht an Ken, Shawn und Jonathon dafür, dass sie die Zeit fanden, jedes einzelne Kapitel dieses Buchs zu überprüfen.
- Sue McClung für die Leitung des Vendor Editorial Teams und die Begleitung dieses Buchs durch den Entstehungsprozess.
- Kenneth Jackson für die Aktualisierung des Zertifikatregistrierungsskripts und die Erstellung einer neuen Version für Windows Vista-Clients auf der Basis der CertEnroll.dll.
- Ryan Hurst für die Informationen über das OCSP (Online Certificate Status Protocol) und für sein Einverständnis, im OCSP-Kapitel zitiert zu werden.

Schließlich möchte ich auch noch Ihnen danken, verehrter Leser. Falls Sie bereits die erste Ausgabe dieses Buchs erworben haben, haben Sie dazu beigetragen, Microsoft

davon zu überzeugen, dass es sich um eine Technologie handelt, die dokumentiert und beschrieben werden muss, um eine erfolgreiche Bereitstellung zu erleichtern. Ich habe in vielen öffentlichen Foren mit Lesern diskutiert und freue mich darauf, das auch weiterhin zu tun, soweit meine Zeit es zulässt.