DuD
Datenschutz und Datensicherheit

Sperren von Zertifikaten in der Praxis – eine Fallanalyse

Oder: Theorie – und Praxis...

Holger Mack

Public Key Kryptografie, Zertifikate und Public Key Infrastrukturen bilden einen Lösungsansatz für den Schutz elektronischer Kommunikation und E-Business im Internet. Bei der Konzeption und Realisierung von PKI-Lösungen wird allerdings häufig bei der „Störfallvorsorge" gespart – mit möglicherweise kostspieligen Folgen, wie die folgende Analyse des VeriSign-Microsoft-Falls vom Januar 2001 eindrucksvoll belegt.

MSc. Holger Mack
Secorvo Security

Consulting GmbH
Arbeitsschwerpunkt: Umsetzung und Konzeption von PKIs, Netzwerksicherheit, Sicherheitskonzepte
E-Mail: mack@secorvo.de

Einleitung

Viele Anbieter von Internet-Shops, Online Banking etc. vertrauen beim Schutz ihres Internet-basierten Online-Angebots auf Zertifikate von kommerziellen Zertifizierungsdiensleistern. Diese – überwiegend für SSL oder Code-Signing ausgestellten – Zertifikate werden hauptsächlich dazu eingesetzt, die Kunden von der Sicherheit der Dienstleistung zu überzeugen und dadurch dessen Vertrauen zu gewinnen.

Dass diese eigentlich einfach aussehende Lösung ihre Tücken hat, hat das im folgenden genauer betrachtete Beispiel des Vorfalls bei Microsoft und VeriSign gezeigt. Das beschriebene Problem ist allerdings nicht spezifisch für kommerzielle Zertifizierungsdienstleister; die gleichen Probleme können auch in firmeninternen Public Key Infrastrukturen (PKIs) auftreten. Ebenso sind solche Probleme auf der Anwendungseite nicht spezifisch für einen Hersteller, sondern treten in verschiedener Form bei den Produkten vieler Hersteller auf. Es geht in diesem Beitrag daher darum, an einem praktischen Beispiel zu zeigen, wo heute noch zentrale Probleme in PKI-Lösungen in der Praxis liegen. Ähnliche Fälle sind bereits in der Vergangenheit (siehe [CERT-SUN]) aufgetaucht und werden bei der weiteren Verbreitung von PKIs – das ist zumindest zu befürchten – wahrscheinlich in der Zukunft häufiger auftreten.

Was ist geschehen?

Am 29. und 30. Januar diesen Jahres stellte der amerikanische Zertifizierungsdienstleister VeriSign fest,[1] dass irrtümlich zwei Zertifikate auf den Namen „Microsoft Corporation" ausgestellt wurden. Es handelt sich dabei um Zertifikate der VeriSign Sicherheitsklasse 3 – der Klasse, die u.a. auch von der Deutschen Bank 24 zur Absicherung ihres Online-Angebots genutzt wird. Hierfür gelten nach VeriSign CPS [CPS-VER] hohe Anforderungen an die Prüfung der Identität und Legitimation des Antragstellers.[2] Dennoch gelang es offenbar jemandem (über die Identität des Täters ist nichts bekannt), sich von VeriSign ohne Legitimation ein solches Zertifikat auf den Namen „Microsoft Corporation" ausstellen zu lassen.

Presseberichten zufolge [CW-VERI] führte menschliches Versagen („human error") zu dem Vorfall; Details sind aber nicht bekannt.

Welche Auswirkungen hatte der Vorfall?

Die Konsequenz der fehlerhaften Zertifikatsausstellung ist nun, dass eine unbekannte Person im Besitz eines Zertifikats, das von einer anerkannten, sogar der im Internet meistverwendeten Zertifizierungsstellen ausgestellt worden ist, mit dem sie sich als die Firma Microsoft ausgeben kann. Dabei handelt es sich um ein Zertifikat zum Signieren von (insbesondere mobilem) Programmcode, z.B. ActiveX-Controls oder Java-Applets (Code Signing). Der Besitzer des zugehörigen privaten Schlüssels könnte also z.B. ein ActiveX-Control mit einer Schadensfunktion erstellen und dieses

[1] Laut eigenen Angaben bei einer Routinekontrolle.

[2] Nach VeriSign CPS [CPS-VER] muss der Antragsteller entsprechende Beweise für die Berechtigung diesen Namen zu nutzen erbringen (durch unabhängige Dritte) bzw. wird die Berechtigung durch Rückfragen überprüft.

signieren. Wenn der Benutzer das Programm zusammen mit einer Webseite herunterlädt, wird es ihm als von „Microsoft Corporation“ signiert angezeigt. Für den Benutzer sieht es so aus, als ob dieses ActiveX-Control von Microsoft signiert wurde (bestätigt durch das Zertifikat der anerkannten Zertifizierungsstelle VeriSign) und der Benutzer wird es dann möglicherweise – sofern er Microsoft vertraut – ausführen lassen. Der Schadensfunktion steht dann (fast) nichts mehr im Wege.

Was geschah weiter?

Genau genommen ist dieser Fall das „Worst-Case“-Szenario für eine Zertifizierungsstelle, da sie ihre eigentliche Aufgabe, die vertrauenswürdige und zuverlässige Bestätigung, dass ein bestimmter Schlüssel zu einer Person oder Institution gehört, nicht erfüllt hat. Der Fehler ist jedoch passiert, und wahrscheinlich werden in Zukunft ähnliche Probleme wieder auftauchen. In jedem noch so gut konzipierten System kann nun eben auch mal etwas schiefgehen: Gründe hierfür gibt es genug, z.B. menschliches Versagen. Für solche Notfälle müssen dann aber Konzepte vorliegen und natürlich auch befolgt werden, die das Vorgehen in einem solchen Fall festlegen. Dies betrifft übrigens nicht nur den Zertifikatsanbieter, sondern auch die Anwender und Anwendungen solcher Zertifikate, deren Sicherheit zu einem Teil auf der Sicherheit und der Zuverlässigkeit der Zertifizierungsdienstleistung beruhen.

Eigentlich bietet die PKI-Technologie für solche Fälle geeignete Mechanismen wie die Sperrung von Zertifikaten und die Verteilung der Sperrinformation. In diesem Fall unterstützen sowohl Microsoft (z.B. der Internet Explorer) als auch VeriSign diese Technik mit Sperrlisten.[3] Warum die Sperrung trotzdem nicht reibungslos funktioniert hat, zeigt einige Probleme auf, mit denen viele PKI-Lösungen heute noch zu kämpfen haben:

- Als VeriSign das Problem erkannt hatte, hat es die fälschlicherweise ausgestellten Zertifikate sofort gesperrt und in seiner Sperrliste veröffentlicht.[4] Die Zertifikate wurden so nur zwei Tage nach Ausstellung gesperrt, und theoretisch hätte das Problem gelöst sein sollen. Auch Microsoft hat das Problems erkannt und ein entsprechendes Security Bulletin [MS01-017] herausgegeben.

Voraussetzung für eine Wirksamkeit der Sperrung ist jedoch, dass bei der Prüfung der Zertifikate die Sperrliste einbezogen wird. Microsoft unterstützt eine solche Sperrlistenprüfung (zumindest in den aktuellen Versionen), doch obwohl sich sowohl VeriSign als auch Microsoft an die geltenden Standards (X.509, PKIX) halten, war es dem Microsoft Internet Explorer nicht möglich, die VeriSign-Sperrliste zu holen, richtig zu prüfen und somit die Ausführung von Programmen, die mit den fraglichen Schlüsseln signiert waren, zu unterbinden bzw. den Benutzer zu warnen.

Dass dies nicht funktioniert hat, lag daran, dass die von VeriSign ausgestellten Zertifikate das CRL Distribution Point Attribut (CDP) [RFC2459] nicht enthalten. Dieses Attribut enthält Informationen darüber, wo Sperrinformation für das Zertifikate gefunden werden kann. Die Microsoft-Implementierung kann Sperrlisten jedoch nur finden und verarbeiten, wenn dieses Attribut im Zertifikat enthalten ist.[5] Das fragliche Attribut ist zwar im Standard definiert, aber seine Benutzung ist nicht vorgeschrieben.[6] [7] Wie so oft zeigt sich hier wieder einmal deutlich, dass Standardkonformität noch lange nicht Interoperabilität garantiert. Im PKI-Umfeld ist letztere leider nicht nur bei Sperrlisten immer noch ein großes Problem, wie viele PKI-Projekte leidvoll erfahren mussten.

Ein weiteres Problem, das dieser Fall aufzeigt, ist, dass das Behandeln von Zertifikats-Sperrungen sehr häufig bei der Umsetzung von PKIs unzureichend gelöst wird. In diesem Fall arbeiteten Microsoft und VeriSign schon seit einiger Zeit zusammen, und einige der Microsoft-Server nutzen Zertifikate, die von VeriSign für sie ausgestellt wurden. In dieser gesamten Zeit wurde das Problem, dass ein Zertifikat auch einmal gesperrt werden könnte, entweder nicht gesehen oder systematisch ignoriert – jedenfalls offensichtlich nie getestet, sonst hätte der Vorfall die Verantwortlichen nicht völlig überrascht.

Aufgrund der technischen Probleme war Microsoft gezwungen, zuerst nur eine Warnung [MS01-017] an Benutzer herauszugeben mit Hinweisen, wie die falschen Zertifikate erkannt werden können. Es wurde empfohlen, mit diesen Zertifikaten signierten Code nicht auszuführen. In einem zweiten Schritt erstellte Microsoft dann einen Patch für alle Microsoft-Betriebsysteme, der allerdings erst sieben Wochen nach Sperrung der Zertifikate verfügbar war.

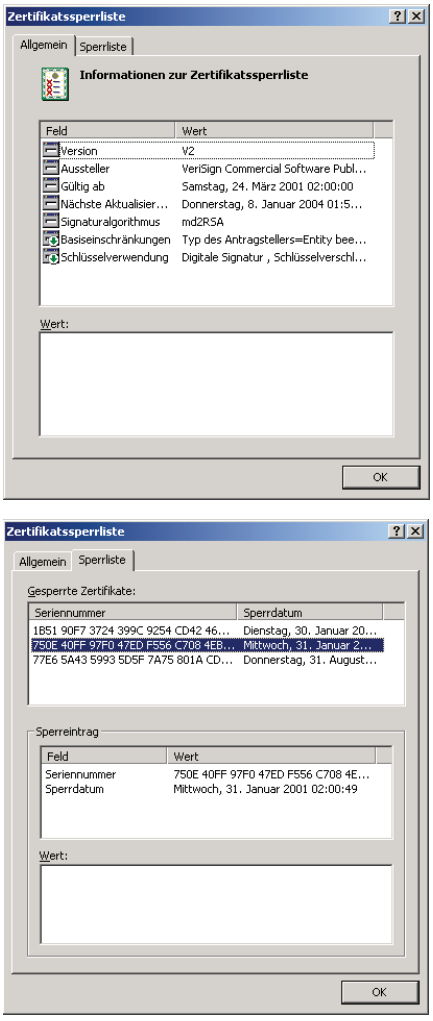

Bild 1: CRL, die mit dem Patch von Microsoft ausgeliefert wird

Dieses Update enthält zum einen eine Sperrliste mit den gesperrten Zertifikaten und zusätzlich einen „revocation handler“, d.h. eine Logik, die diese Sperrliste prüfen kann. Für diesen Patch wurde eine spezielle Sperrliste erstellt, die nur die beiden ge-

[3] VeriSign unterstützt zusätzlich OCSP zur Veröffentlichung von Sperrinformationen; dies wurde aber hier nicht getestet.

[4] Die Sperrliste kann unter http://crl.verisign.com abgerufen werden.

[5] Eine Alternative ist, das Zertifikat anhand des Namens der CA aus einem Directory zu beziehen, bzw. gegen eine manuell lokal importierte CRL zu prüfen.

[6] Das Attribut ist bei den meisten ausgestellten Zertifikaten nicht vorhanden.

[7] Dieses Attribut kann zusätzlich auch noch in verschiedener Form vorkommen.

sperrten Zertifikate (sowie ein Testzertifikat) enthält und die drei Jahre gültig ist. Üblicherweise sind VeriSign-Sperrlisten nur eine Woche gültig . Microsoft empfiehlt sogar, diese Sperrliste nicht durch die eigentliche VeriSign Sperrliste zu ersetzen, da man diese sonst regelmäßig erneuern müsste – ein ausgesprochen zweifelhafter Rat, durch den der nächste Vorfall vorprogrammiert sein könnte.

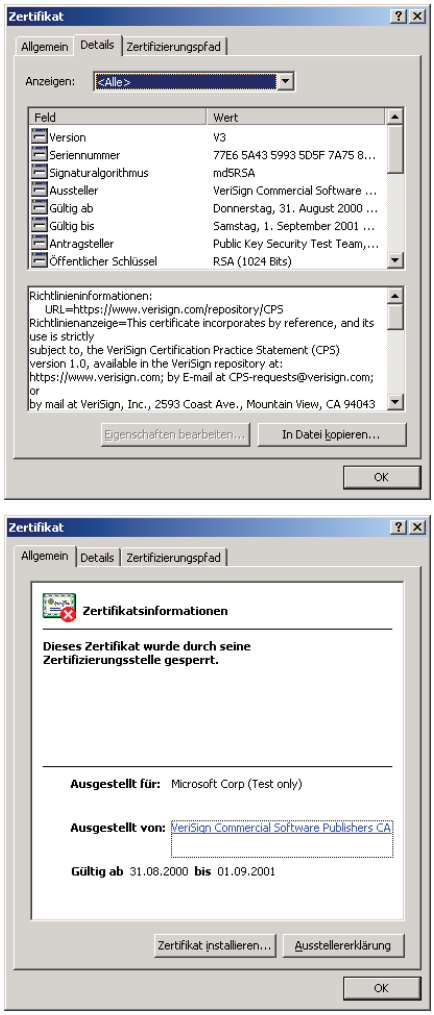

Bild 2: Ansicht des Testzertifikats nach Installation des Patches

Fazit

An dem Beispiel von Microsoft und VeriSign zeigt sich sehr deutlich, dass es noch einiges zu tun gibt, bis Public Key Infrastrukturen die Lösung für die Sicherheitsprobleme von Online-Angeboten sind. Bezüglich des Sperrens von Zertifikaten und insbesondere des Einbeziehens von Sperrungen in die Zertifikatsprüfung herrscht leider weiterhin oft die „Das-passiert-(uns)-schon-nicht“-Einstellung vor. Wie sonst ließen sich solche Fälle erklären? Eine PKI ist eben nur dann die sichere, elegante und akzeptierte Lösung, wenn man auch mit Störfällen richtig umgehen kann. In dem beschriebenen Fall muss man wohl davon ausgehen, dass auch nach der Sperrung der Zertifikate, den Warnungen durch VeriSign und Microsoft und der Verfügbarkeit des Patches ein Großteil der Benutzer weiterhin ungeschützt sind.

Fälle wie der hier beschriebene tragen sicherlich nicht dazu bei, das mangelnde Vertrauen in die Sicherheit von E-Commerce und PKI-basierte Sicherheitslösungen zu erhöhen. Um sicherere Online-Angebote zur Verfügung zu stellen sind alle Beteiligten (Zertifizierungsdienstleiter, Anbieter, Hersteller) gefragt. Nur wenn alle zusammenarbeiten und eine Lösung für den Endanwender anbieten, die sicher, aus Sicht des Anwenders verständlich und bedienbar ist, kann deren Vertrauen gewonnen werden.

Literatur

[CERT-SUN] CERT Advisory CA-2000-19 Revocation of Sun Microsystems Browser Certificates

[CPS-VER] VeriSign Certificate Practice Statement, Version 1.2, May 15,1997, VeriSign, Inc.

[CW-VERI] J. Vijayan, „VeriSign certificate snafu highlights threat of human errors“, Computerworld, Mar. 30 2001.

[MS01-017] Microsoft Security Bulletin MS01-017, Microsoft Corporation

[RFC2459] Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459), IETF

[VERISIGN] „Verisign Security Alert Fraud Detected in AuthentiCode Signing Certificates“, March 22, 2001, VeriSign