Cloud-Arbeitsplatz ohne eigene PKI

Amtsenthebung

Christoph Hannebauer

Viele mittelständische und große Unternehmen leisten sich eine eigene Public-Key-Infrastruktur. Die Cloud macht diese überflüssig und verdrängt sie zunehmend.

Für die Unternehmens-IT bringt die Cloud zum Teil radikale Umbrüche mit sich. Die Praxis zeigt, dass selbst Großunternehmen IT-Kerndienste wie das E-Mail-Backend in die Cloud verlegen können. Ein Cloud-Arbeitsplatz braucht für Provisionierung und Nutzung keine Verbindung ins Unternehmensnetz mehr, eine Internetverbindung reicht völlig aus (siehe Abbildung 1). Was bedeutet dieser Wandel für die Public-Key-Infrastruktur (PKI)? Zum Beispiel ist sie für die ausgelagerten Dienste nicht mehr zwingend erreichbar. Trotzdem muss Vertraulichkeit gewahrt werden, weswegen Anbieter ihre eigenen Mechanismen dafür implementiert haben. Das kann so weit gehen, dass eine PKI nicht mehr nötig ist. Dieser Artikel illustriert an Microsoft Azure, wie sich Sicherheit an einem Cloud-Arbeitsplatz ohne PKI erreichen lässt. Das Sicherheitsniveau übersteigt unter Umständen das, was sich mit On-Premises-Systemen umsetzen lässt, manchmal muss man jedoch mit Abstrichen leben. Es gibt verschiedene Anwendungsfälle für Zertifikate und damit für eine PKI. Die meisten davon lassen sich mit den Mitteln von Azure realisieren.

Die Secure-Varianten der TCP-Protokolle, allen voran HTTPS, basieren auf dem Protokoll TLS und damit auf X.509-Zertifikaten. Betreiber öffentlicher Zertifizierungsstellen (CAs) wie Global Sign und Let's Encrypt verkaufen beziehungsweise vergeben solche Zertifikate für öffentliche DNS-Namen (alle Links unter ix.de/ix1807122). Spätestens für Dienste, die von außerhalb des Firmennetzes erreichbar sein sollen, braucht man ein solches Zertifikat, das für alle Browser vertrauenswürdig ist. Dann kann man ohnehin auf keines einer internen PKI zurückgreifen.

Bei Software-, Platform- und oft sogar bei Infrastructure-as-a-Service-Angeboten ergibt sich daraus kein Problem, da die meisten Provider die Dienste selbst mit einem Zertifikat absichern. Für interne Dienste kann man allerdings keine Zertifikate von einem öffentlichen Anbieter erhalten – für einen internen DNS-Namen wie server.company.local kann schließlich niemand prüfen, ob der Antragsteller die Domain besitzt (tut er ja auch nicht). In einer idealen Cloud-Welt gibt es aber keine Unterscheidung mehr zwischen intern und extern: Alle Dienste liegen in der Cloud und sind von überall erreichbar. In diesem Fall ist die eigene PKI unnötig.

Sichere Windows-Anmeldung

Gibt man ein Passwort an einem öffentlichen Ort ein – zum Beispiel am Flughafen, in der Bahn oder auf dem Mobiltelefon –, geht man das Risiko ein, dass jemand in der Nähe filmt und sich die Zugangsdaten aus dem Video herleitet. Dagegen hilft Multi-Faktor-Authentifizierung: nicht nur etwas, das man weiß (das Passwort), sondern auch etwas, das man hat, wie eine Smartcard mit persönlichem Zertifikat.

Eine Smartcard-basierte Windows-Anmeldung ist außerdem komfortabler, da sie lediglich eine kurze PIN erwartet. Schließlich kann die Smartcard eine begrenzte Zahl der Anmeldeversuche erzwingen, während auf passwortauthentifizierte Dienste oder gar auf einen Passwort-Hash oft eine Brute-Force-Attacke möglich ist.

Noch komfortabler und vielleicht sogar eine Spur sicherer ist das mit Windows 10 eingeführte Windows Hello, das ohne Zertifikate auskommt, damit aber

iX-TRACT

- In einer komplexen Firmen-IT-Struktur findet sich oft eine Public-Key-Infrastruktur, die hilft, Nutzer, Geräte und Dienste zu authentifizieren.
- Verwendet man Cloud-Dienste, muss der Anbieter dafür sorgen, dass die Services – Software, Plattform oder Infrastruktur – ein gültiges Zertifikat aufweisen.
- Perspektivisch kann die Cloud eine eigene Public-Key-Infrastruktur obsolet machen.

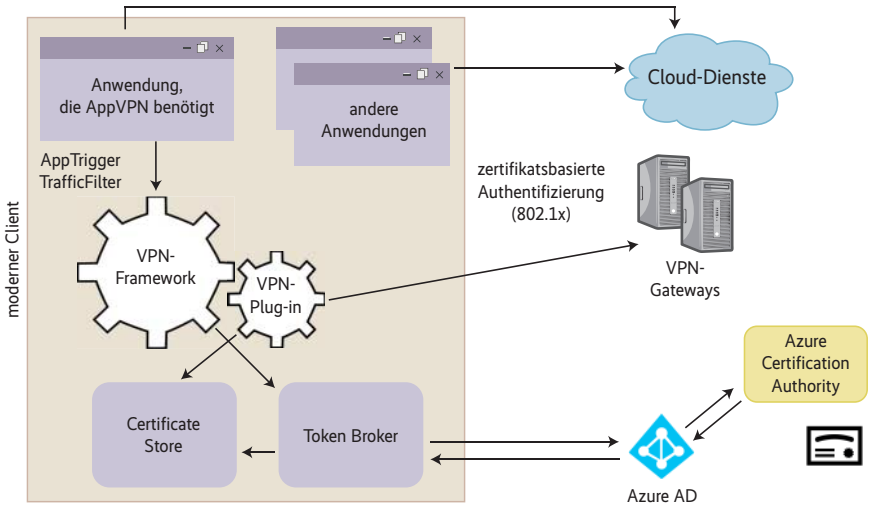
umgehen kann. Die beiden genutzten Faktoren sind das Gerät selbst, genauer sein Trusted Platform Module (TPM), und die PIN des Nutzers. Der TPM-Chip ersetzt quasi die Smartcard. Komfortabler und sicherer ist diese Lösung, weil ein Rechner schwerer zu verlieren oder zu klauen ist als eine Smartcard.

Nach den Erfahrungen des Autors ist der Verlust von 10 Prozent der Smartcards pro Jahr ein realistischer Richtwert. Ob Smartcard und PIN alleine für einen Angriff ausreichen oder ob noch der Zugriff auf einen beliebigen Unternehmensrechner erforderlich ist, hängt von weiteren Rahmenbedingungen ab. Aber der Zugriff auf einen beliebigen Unternehmensrechner ist sicherlich leichter als der auf einen ganz bestimmten. Bei Windows Hello lässt sich statt der PIN eine biometrische Authentifizierung verwenden. Biometrie ist meist ein Komfortgewinn, aber es scheiden sich die Geister, ob es die Sicherheit erhöht oder senkt. Das hängt sicher auch vom Anwendungsfall ab. Einem Grenzbeamten am Flughafen fällt es beispielsweise vermutlich leichter, eine biometrische Authentifizierung zu erzwingen, als ein Passwort zu erfragen.

Wer darf in welches Netz?

Ob eine Organisation ihr kabelgebundenes Netzwerk per 802.1x authentifiziert, ist unter anderem eine Frage der organisationsspezifischen Compliance- und Sicherheitsanforderungen [1]. In einer Cloud-IT, in der die Dienste ohnehin für jeden in der Cloud stehen, sinkt die Notwendigkeit, das eigene Netzwerk abzusichern. Bekannt gewordene Angriffe auf IT-Systeme nutzten zudem immer andere Lücken aus.

Für WLAN-Netze ist eine zertifikatsbasierte Authentifizierung aber nicht nur eine Frage der Sicherheit, sondern auch des Komforts. Ein Angriff über ein drahtloses Netz ist wesentlich leichter, weil ein Angreifer kein Gerät in ein Unternehmensgebäude einschleusen muss. Eine Absicherung über Nutzernamen und Passwort und ohne Zertifikate ist zwar beispielsweise mit EAP-MS-CHAP v2 grundsätzlich möglich, aber auf Client- und Access-Point-Seite teilweise schwieriger einzurichten, gilt als weniger sicher und verhindert auch moderne Anmeldeverfahren wie Azure Multi-Factor Authentification (MFA). Leider bieten Azure und Office 365 bisher keine befriedigende Lösung für dieses Problem. Bei einigen Unternehmen ist WLAN-Authentifizierung der letzte verbliebene Anwendungsfall der PKI.

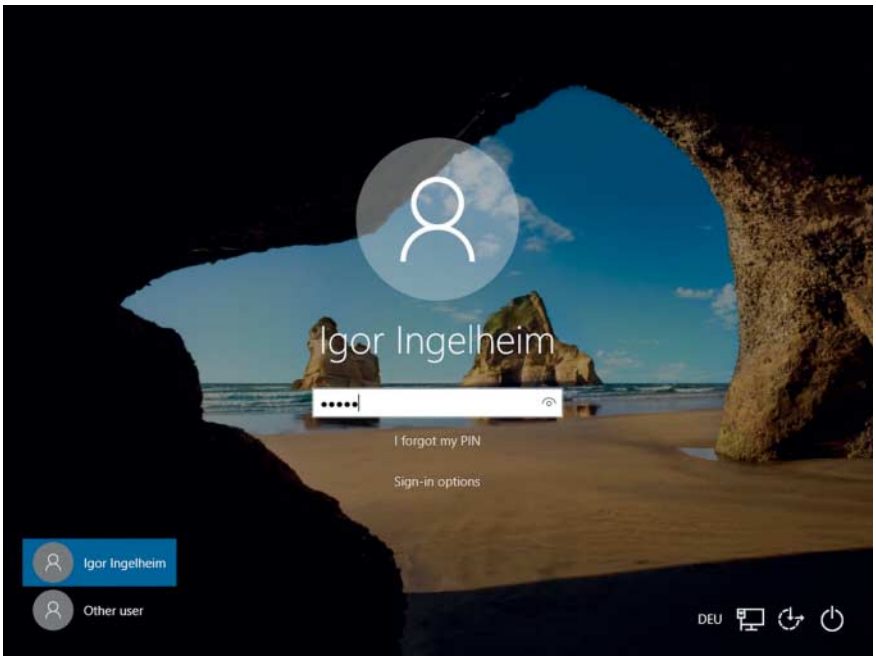


Legt man sich auf einen Cloud-Betreiber fest, übernehmen dessen interne Mechanismen einen Großteil der Aufgaben, für die bisher eine zentrale Schlüsselverwaltung nötig war (Abb. 1).

Das Mobile Device Management (MDM) Intune verteilt an alle registrierten Geräte ein eigenes Maschinenzertifikat, mit dem sich die Maschinen gegenüber Intune authentifizieren. Das Zertifikat weist zudem alle erforderlichen Eigenschaften auf, um als WLAN-Authentifizierungszertifikat verwendet werden zu können. Da jedoch ein und dieselbe CA alle diese Zertifikate mandantenübergreifend ausgestellt hat, muss der Access Point noch prüfen, ob ein gegebenes Zertifikat zum eigenen Mandanten gehört. Die zugehörige ID steht in der Extension 1.2.840.113556.5.14 dieses Zertifikats, kann aber von den meisten Radius-Servern, etwa CISCO ISE und Microsoft NPS, nicht ausgewertet werden.

Fernzugang ins Intranet

In einer IT aus Cloud-Diensten gibt es kein Intranet und damit keine Notwendigkeit für ein VPN. Doch in dieser Radikalität werden in den nächsten Jahren sicherlich nur wenige große Unternehmen den 100%-Cloud-Ansatz umsetzen



Windows Hello ist eine Form der Authentifizierung am Betriebssystem, die mit oder ohne Zertifikate arbeitet. Sie entspricht der Anmeldung mit einer Smartcard, wobei das im PC verbaute TPM-Modul deren Rolle übernimmt (Abb. 2).

(können). VPN wird mindestens die nächsten paar Jahre noch eine Notwendigkeit bleiben. Glücklicherweise bietet Azure im Gegensatz zur WLAN-Authentifizierung eine vorgefertigte Lösung für die VPN-Authentifizierung.

Microsoft stellt eine mandantenspezifische CA für VPN bereit, um Conditional Access (in diesem Zusammenhang verwirrenderweise ebenfalls oft CA abgekürzt) umzusetzen. Diese Azure CA stellt automatisch kurzlebige Zertifikate aus, wenn ein Benutzer eine VPN-Verbindung aufbaut, die über ein Intune-Profil angelegt wurde. Diese Lösung erfordert fast keinen Einrichtungsaufwand, wenn die Geräte über Intune verwaltet werden, und ist gleichzeitig durch Conditional Access sicher. Demgegenüber bietet eine eigene PKI keinen Vorteil.

Statt Dateisystemverschlüsselung (Encrypting File System, EFS) ist Azure Information Protection (AIP) das Mittel der Wahl in der Microsoft-Cloud. So vermeidet man wieder die Verwaltung der privaten Schlüssel, zudem kann man Dateien nicht nur auf einem bestimmten Rechner schützen, sondern sogar dann, wenn die Dateien von USB-Sticks, aus der Cloud oder von mehreren Nutzern geöffnet werden sollen (siehe Abbildung 4).

Auf einer niedrigeren Ebene setzt bei Windows BitLocker als Festplattenverschlüsselung an. Es verschlüsselt auch USB-Sticks. Man kann es ohne PKI einsetzen, bestimmte Funktionen gibt es jedoch nur mit zentraler Schlüsselinfrastruktur. Konkret kann eine interne PKI für BitLocker zwei Arten von X.509-Zertifikaten ausstellen, die auf den Vorlagen Network Unlock und Data Recovery Agent einer Microsoft CA basieren. Für einen Windows-10-basierten Cloud-Arbeitsplatz sind diese Zertifikate jedoch weder aus Usability- noch aus Sicherheitsgründen nötig. Bei Azure-AD-registrierten Maschinen ist der BitLocker-Recovery-Key beispielsweise komfortabel über das Azure-Portal abrufbar und ersetzt den Data Recovery Agent.

Kryptografie im E-Mail-Verkehr

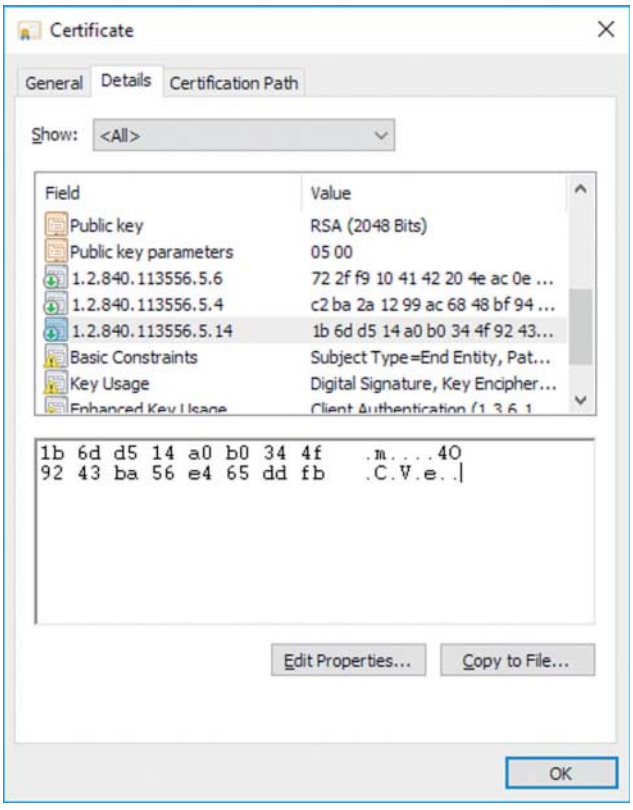
Bei E-Mails hat Kryptografie zwei Einsatzgebiete: Verschlüsseln und Signieren. Verschlüsselung soll sicherstellen, dass Unberechtigte den Inhalt nicht lesen können. Signaturen sollen belegen, dass eine E-Mail von dem Absender kommt, von dem sie vorgibt zu sein. S/MIME erfüllt diese Anforderungen grundsätzlich und alle gängigen E-Mail-Programme unterstützen das Protokoll seit Jahren nativ außer interessanterweise den Outlook-Versionen für Android und iOS.

Allerdings hatte S/MIME schon immer mit Schwierigkeiten zu kämpfen. Ein Problem ist, dass der Absender das Zertifikat des Empfängers besitzen und dieses für den Absender vertrauenswürdig sein muss. Während das innerhalb einer Organisation meist unproblematisch ist, hat sich für den Zertifikatstausch zwischen Organisationen bezeichnenderweise sehr häufig ein unschöner Workaround eingebürgert: das Signatur-Pingpong. Die Kommunikationsteilnehmer schicken sich signierte Mails, denen das gleichzeitig für Signaturen und Verschlüsselung eingesetzte Zertifikat anhängt. Eigentlich als Nebeneffekt gedacht, tauschen die Teilnehmer so ihre Zertifikate aus und können danach Botschaften verschlüsseln – bis der E-Mail-Client die Zertifikate aus dem Cache löscht und das Pingpong von vorne anfängt.

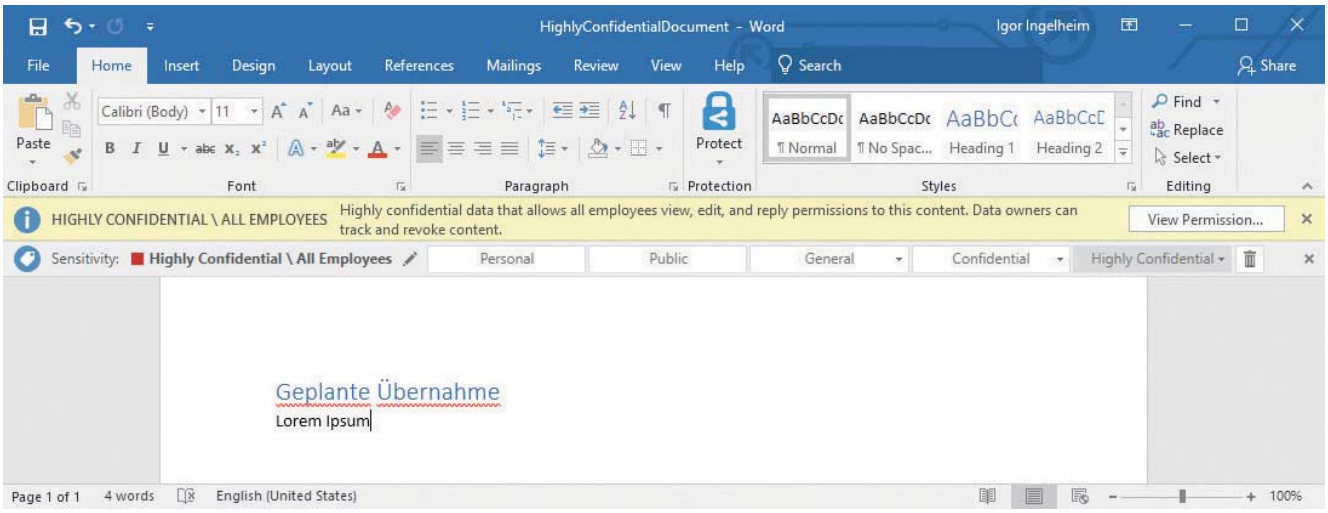
Bei Verschlüsselungszertifikaten ist es in der Praxis darüber hinaus essenziell, die privaten Schlüssel zentral zu speichern. Was für Sicherheitsgurus eigentlich ein No-Go ist, ist für Unternehmen oft gesetzliche Anforderung. E-Mails als Vertragsdokumente unterliegen oft Aufbewahrungspflichten und der Zugriff muss auch bei Urlaub, Ausscheiden oder Unwillen des Mitarbeiters zeitnah möglich sein, etwa bei Strafverfahren oder Betriebsprüfungen. Zudem will sich verständlicherweise kein Mitarbeiter mit den Details von E-Mail-Kryptografie auseinandersetzen oder sich um Backups und Transfer von privaten Schlüsseln von einem Rechner zum Nachfolger kümmern. Ebenso muss ein und derselbe private Schlüssel auf allen Geräten (PC, Tablet, Mobiltelefon) zur Verfügung stehen, da sonst verschlüsselte Mails nur an einem der Geräte gelesen werden können. Solch eine zentrale und zugleich sichere Aufbewahrung privater Schlüssel ist verständlicherweise mit einigen praktischen Problemen verbunden.

Microsofts Antwort aus der Cloud ist erneut Azure Information Protection (AIP), das auf den Azure Rights Management Services (Azure RMS) aufbaut und es zunehmend ersetzt. AIP bietet viele Vorzüge gegenüber S/MIME:

- Es schützt nicht nur E-Mails, sondern auch andere Dateien, insbesondere Office-Dokumente.
- Der verschlüsselte Austausch mit Externen ist ebenfalls einfacher, da er auf der Identitätsdatenbank Azure AD aufbaut.
- Klassifizierungen erlauben den Nutzern einen intuitiven Zugang zur Verschlüsselung.
- Auch Mobilplattformen unterstützen AIP. Outlook gibt es für Windows, macOS, Android und iOS.
- Eine Schlüsselhistorie zu speichern und zu verteilen, ist nicht notwendig.



Verwaltet man mobile Geräte zentral über Intune, versorgt dieses sie mit den passenden (kurzlebigen) Zertifikaten, mit denen sich Nutzer etwa am Drahtlosnetzwerk der Firma anmelden (Abb. 3).



Nutzt man auch Bürosoftware aus der Cloud, greift die bei Azure auf die dort hinterlegten Zugriffsbestimmungen zu. Über AIP lässt sich steuern, welche Kollegen, Abteilungen oder sogar externe Nutzer ein Dokument öffnen und bearbeiten dürfen (Abb. 4).

– RMS verschlüsselt nicht nur, sondern setzt auch weiter gehende Rechte wie die Druckerlaubnis durch.

Zu den Kritikpunkten an AIP gehört, dass durch den Master-Schlüssel keine echte Ende-zu-Ende-Verschlüsselung erreicht wird und ein Vendor-Lock-in entsteht. Deutlicher wird es beim Thema Signaturen: AIP ist schlicht nicht für diesen Anwendungsfall gedacht und bietet hierfür keine Lösung. Zum Validieren von E-Mail-Absendern empfiehlt Microsoft für Exchange Online aber das Sender Policy Framework (SPF). SPF hat gegenüber Signaturen durchaus Vorteile: Nutzer können zum Beispiel in Echtzeit beim Absenden einer E-Mail geprüft werden statt nur einmal pro Zertifikatsausstellung.

Code-Signing und Continuous Integration

Bei öffentlich vertriebenen Anwendungen ist ein öffentliches, vertrauenswürdiges Code-Signing-Zertifikat fast zwingend erforderlich. Für interne Anwendungen wie PowerShell-Skripte, die die IT zur Konfiguration verwendet, lassen sich aber problemlos Zertifikate der internen PKI einsetzen. Je nach Szenario muss ohnehin jedes Code-Signing-Zertifikat einzeln als vertrauenswürdig markiert werden.

Organisationen benötigen aber typischerweise höchstens eine Handvoll Code-Signing-Zertifikate. Tatsächlich ist es gute Praxis, nicht jedem einzelnen Entwickler eines auszustellen, sondern Quelltext über einen definierten Prozess innerhalb eines Continuous-Integration-Systems automatisiert zu signieren. Die Organisation benötigt dann oft nur ein einziges Code-Signing-Zertifikat. Ein öffentlich eingekauftes Zertifikat fällt gegenüber den Kosten einer eigenen PKI kaum ins Gewicht.

Für rechtsverbindliche Dokumentensignaturen braucht man Zertifikate einer öffentlichen PKI. Allerdings kann man auch interne Prozesse mit elektronischen Signaturen vereinfachen, und die müssen nicht unbedingt rechtsverbindlich sein. Beispielsweise lassen sich interne IT-Bestellprozesse papierlos gestalten. Ein erster Schritt dorthin besteht darin, bisherige Formulare aus Papier in digital signierbare PDFs umzuwandeln. Mitarbeiter können diese mit einer elektronischen Signatur unterzeichnen und sie per E-Mail verschicken, statt Papier hin- und herzufaxen. Solche Prozesse lassen sich allerdings auch ohne digitale Signaturen sicher abbilden, etwa mit Microsoft PowerApps. Ein solcher Zugang über Apps und Webanwendungen ist für die Nutzer zudem intuitiver und schneller, als digital zu signieren. Eine weiter gehende Automatisierung ist ebenfalls einfacher.

Verschiedene Anwendungsfälle für Zertifikate werden für den Betrieb der PKI selbst genutzt, allen voran die Zertifikate der CAs selbst, aber auch solche für das Online Certificate Status Protocol (OCSP) und für die Certificate Revocation Lists (CRL) gehören dazu. Ohne eigene PKI braucht man diese Typen nicht mehr. In einem 100%-Cloud-Konzept fällt auch das Active Directory weg – das technisch grundverschiedene Azure Active Directory (AAD) übernimmt diese Rolle. Ohne Domain-Controller und ohne Key Distribution Center (KDC) sind auch keine Zertifikate mehr nötig, die die Replikation zwischen den Domain-Controllern absichern oder beim Ausstellen von Kerberos-Tickets helfen. Tatsächlich sind diese Zertifikate ohnehin selten zwingend erforderlich für den Betrieb des Active Directory.

Fazit

Die Cloud bietet tatsächlich für fast jede Zertifikatsanforderung eine Lösung, wie die Beispiele auf Basis von Microsoft Azure und Office 365 zeigen. Die Cloud-Lösungen sind fast immer günstiger und einfacher umzusetzen, mindestens so sicher wie das klassische Pendant und versprechen erhöhten Komfort für die Nutzer. Für einige Lösungen muss die IT aber insgesamt schon sehr weit auf einen Cloud-Ansatz umgestellt sein. In der Übergangszeit kann es zumindest das ein oder andere Jahr durchaus noch einen Bedarf für Zertifikate einer eigenen PKI geben – danach lässt sich komplett darauf verzichten. (jab@ix.de)

Dr. Christoph Hannebauer

ist Senior Consultant bei Glück & Kanja und beschäftigt sich mit Sicherheitsthemen in der Microsoft-Cloud.

Literatur

[1] Benjamin Pfister; Authentifizierung; Absperraufwand; Auswahl einer Zugangskontrolle fürs LAN; *iX* 2/2018, S. 84

Alle Links: ix.de/ix1807122