DuD
Datenschutz und Datensicherheit

Virtuelle Poststelle

Dirk Fox

Insbesondere für den Schutz der elektronischen Kommunikation, namentlich E-Mail, wurden in den vergangenen Jahren in Unternehmen und Behörden zahlreiche Public Key Infrastrukturen (PKI) aufgebaut. Regelmäßig genutzt werden die neuen Schutzmöglichkeiten in vielen der – oft mit hohen Investitionen installierten – Infrastrukturen allerdings bis heute häufig nur von wenigen Anwendern. Trotz der zumeist sehr benutzerfreundlich realisierten Anwendungsschnittstelle übersteigt das Erfordernis, bei jeder Nachricht sensiblen Inhalts die Sicherheitsmechanismen Verschlüsselung oder Signatur explizit zu aktivieren, die Mitwirkungsbereitschaft vieler Anwender.

Diese Beobachtung motivierte vor einigen Jahren das Interesse an zentralisierten Lösungen: E-Mail-Gateways, die dem Nutzer die Ver- und Entschlüsselung von Nachrichten, ggf. sogar die Signaturerzeugung vollständig abnehmen [BeSt_01]. Diskutiert wird dieser Ansatz auch unter der Bezeichnung „Virtuelle Poststelle“ [MaMi2_04]: Analog zur Poststelle in Behörden und Unternehmen werden dabei alle Nachrichten an einer zentralen Stelle kryptographisch behandelt.

Vorteile

Ein solcher zentralistischer Ansatz hat zahlreiche Vorteile:

- Die Verschlüsselung einer Nachricht erfolgt bei entsprechender Konfiguration automatisch und unabhängig davon, ob der Nutzer diese Funktion auswählt.
- Auf den Client-Systemen sind weder die Installation zusätzliche Software (Plugins) noch die Konfiguration von Schlüsseln und Zertifikaten erforderlich.
- Vertretungsregelungen lassen sich leicht abbilden, da die interne Weiterleitung ankommender E-Mails unverschlüsselt erfolgt – der als Vertreter ausgewählte Empfänger muss den privaten Entschlüsselungsschlüssel des eigentlichen Adressaten nicht kennen.
- Eine Schlüsselhinterlegung (Key Recovery)[1], die es ermöglicht, verschlüsselt gespeicherte Nachrichten auch nach einem Schlüsselverlust noch zu entschlüsseln, ist nicht erforderlich: Der E-Mail-Client des Empfängers erhält alle eingehenden Nachrichten in entschlüsselter Form.
- Auch verschlüsselte Nachrichten können nach der Entschlüsselung im Gateway an zentraler Stelle auf Viren untersucht und unerwünschte Nachrichten (SPAM) ausgefiltert werden.

Die heute verfügbaren E-Mail-Sicherheits-Gateways unterstützen zudem meist die Schlüssel- und Austauschformate von S/MIME und OpenPGP – eine in der Praxis oft wichtige Anforderung, die sich bei einer Ende-zu-Ende-Sicherung oft nur mit (ggf. mehreren) Plugins lösen lässt. Auch die Nutzung von Rückruflisten gesperrter Schlüssel (CRLs)[2] vereinfacht sich, weil der dafür erforderliche Directory-Zugriff nur noch an einer zentralen Stelle konfiguriert werden muss.

Ein besonders wichtiger Vorteil ist die Vereinfachung des Schlüsselmanagements: Die privaten und öffentlichen Schlüssel werden an einer zentralen Stelle vorgehalten und müssen nicht mehr auf vertrauenswürdige Weise an die Nutzer direkt verteilt werden. Auch die Einweisung der Nutzer in den Umgang mit den Schlüsseln kann entfallen – in vielen größeren Unternehmen ebenfalls ein signifikanter Kostenfaktor.

Nachteile

Für diesen vielfältigen Komfortgewinn zahlt man allerdings auch einen Preis: Der Schutz der übermittelten Nachrichten erfolgt nicht mehr Ende-zu-Ende, sondern nur noch ab dem Gateway. Eine signierte E-Mail garantiert daher nicht mehr, dass die Nachricht auch vom angegebenen Sender stammt – nur noch, dass das Gateway sie signiert und versendet hat. Die interne Kommunikation erfolgt sogar vollständig ungesichert. Hinzu kommen einige grundsätzliche Nachteile des zentralen Lösungsansatzes:

- Die Verschlüsselung einer Nachricht entzieht sich vollständig der Kontrolle durch den Sender. Einige Produkte erlauben daher die Einfügung standardisierter Kommandos in der Betreff-Zeile, mit denen z. B. eine Verschlüsselung erzwungen werden kann – keine sehr benutzerfreundliche, aber alternativlose Lösung.
- Soll die Nachrichtenübertragung auch im internen Netz (d. h. zwischen Gateway und PC) vor unberechtigter Kenntnisnahme und Veränderung geschützt sein, sind zusätzliche Mechanismen erforderlich.
- Zwar erlauben die verfügbaren Gateway-Lösungen die Konfiguration auch sehr komplexer Regelungen (welche Nachrichten werden signiert, welche verschlüsselt?). Die Administration kann dadurch allerdings sehr aufwändig werden.
- Das zentrale Schlüsselmanagement umfasst nicht nur die Erzeugung und Vorhaltung der Schlüssel aller (internen) Nutzer, sondern auch die Verwaltung und Prüfung der Zertifikate aller externen Kommunikationspartner, mit denen geschützt kommuniziert werden soll. Hinzu kommen CRLs, die für die Gültigkeitsprüfung aktuell aus unterschiedlichen Verzeichnissen heruntergeladen werden müssen.

In der Praxis darf auch die zusätzliche Last am Gateway nicht unterschätzt werden. Denn insbesondere die korrekte Überprüfung von signierten Nachrichten ist rechenaufwändig: Je Signatur ist die gesamte Zertifikatskette inklusive zugehöriger CRLs zu prüfen. Sollten verschlüsselte und signierte E-Mails überwiegen, dürfte dies die Leistungsfähigkeit heutiger Gateway-Lösungen schnell überfordern.

Literaturhinweise

[BeSt_01] Bertsch, Andreas; Stark, Claus: *Verschlüsselung und Inhaltssicherung*. DuD 12/2001, S. 711-716.

[MaMI_04] Maseberg, Sönke; Mrugalla, Christian; Intemann, Matthias: *Datensicherheit in BundOnline 2005*. DuD 11/2004, in diesem Heft.

[MaMi1_04] Mack, Holger; Michels, Markus: *Praktischer Einsatz von E-Mail-Gateways zur Sicherung der E-Mail-Kommunikation*. Secorvo White Paper, WP11, Version 1.0 vom 20.07.2004. http://www.secorvo.de/whitepapers

[MaMi2_04] Mack, Holger; Michels, Markus: Praktischer Einsatz von E-Mail-Gateways zur Sicherung der E-Mail-Kommunikation. DuD 8/2004, S. 480-485.

[1] Siehe *Key Recovery*, Dirk Fox, Gateway, DuD 4/1997, S. 227.

[2] Siehe *Certificate Revocation List – CRL*, Dirk Fox, Gateway, DuD 8/2001, S. 483.