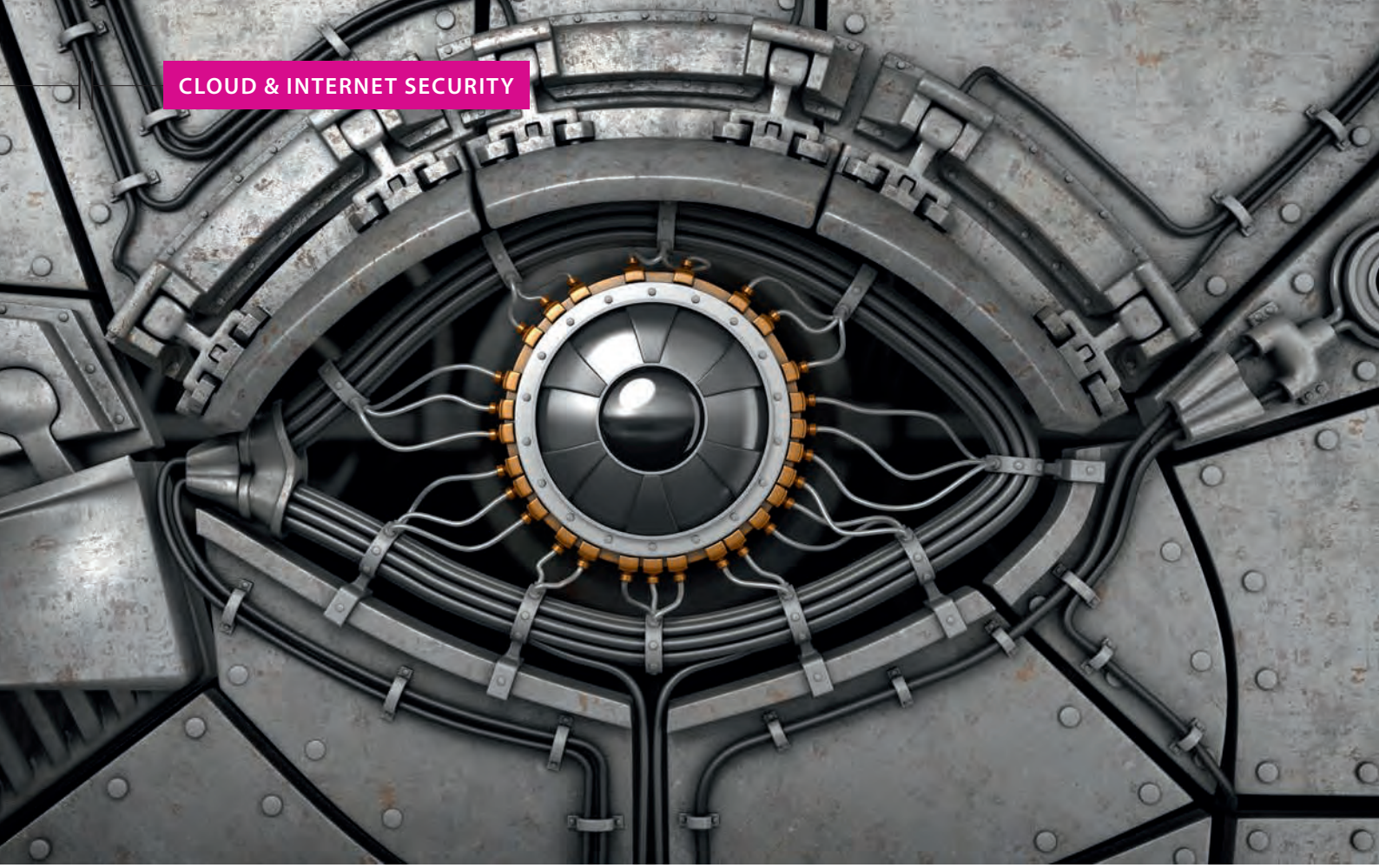

Digitale Zertifikate

Schutz vor **Cyberwar** & **Datenspionage**

Die nicht endenden Enthüllungen über die Abhörmöglichkeiten von Geheimdiensten und die schockierenden Meldungen über die Kaperung kompletter Unternehmensnetzwerke wie bei SONY Pictures setzen IT Verantwortliche zunehmend unter Handlungsdruck.

Konnte man sich vor ein paar Jahren noch mit Firewall, Virenscanner und Passwort-basierten Verfahren zurück lehnen, so sind diese Zeiten endgültig vorbei. Der zunehmende Einsatz von Sicherheitsinformations- und Ereignis-Management-Lösungen (SIEM) ist sicher richtig, wenn es darum geht, Vorfälle zu erkennen um dann entsprechend zu reagieren. Noch sinnvoller ist es aber, es gar nicht so weit kommen zu lassen. Sind starke Authentisierung, Ende-zu-Ende-Verschlüsselung und digitale Signaturen womöglich die Zaubermittel der Zeit? Fest steht, dass man mit solchen Mechanismen die Hürde für Angriffe und Abhörversuche extrem hoch legt oder diese sogar praktisch unmöglich machen kann. So führen mehr und mehr Unternehmen E-Mailverschlüsselung, VPNs, Geräteauthentisierung nach IEEE 802.1x oder Dateiverschlüsselung für Cloud-Speichersysteme ein. Hierbei ist zu beachten, dass eine Ende-zu-Ende-Verschlüsselung am Client erfolgen muss und nicht durch Secure E-Mailgateways oder Cloud Encryption Gateways erbracht werden kann. Dies wird in Zeiten, in denen sich der professionelle Angreifer im internen Netz platziert zunehmend wichtiger.

WEB-TIPP:
www.secardeo.de
www.ebca.de

Public-Key-Infrastruktur

Die Basis für diese „stählernen" Mechanismen stellt eine Public-Key-Infrastruktur (PKI) in Form von digitalen Zertifikaten gemäß ITU-T X.509 und zugehörigen privaten Schlüsseln bereit. Eine PKI kann entweder intern im Unternehmen aufgebaut und betrieben werden – in vielen Fällen kommt dabei eine Windows PKI zum Einsatz – oder es wird eine Managed PKI genutzt, die von einem externen Trustcenter-Betreiber bereitgestellt wird. Zertifikate, die von einer solchen öffentlichen Certification Authority (CA) ausgestellt wer-

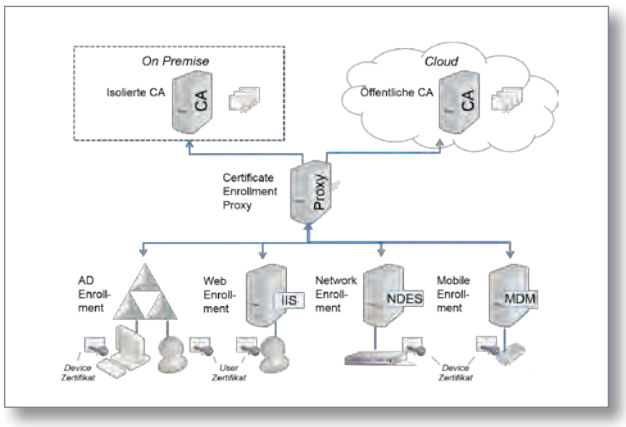

Bild 1: Certificate Enrollment Proxy.

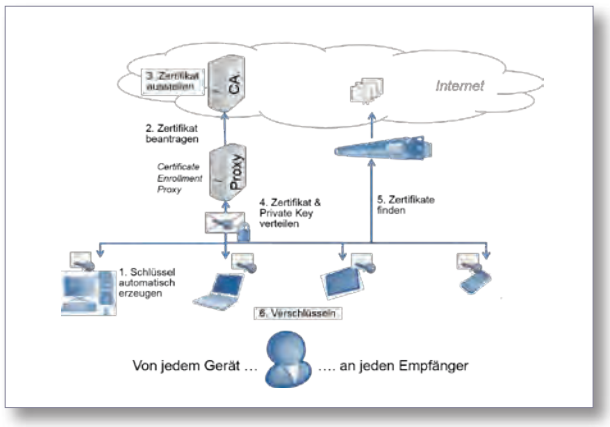

Bild 2: Any-to-Any Encryption.

den haben den großen Vorteil, dass sie weltweit von gängigen IT-Plattformen und Anwendungen anerkannt werden. Dies ist bei intern, mit einer Windows CA erzeugten Zertifikaten, ein Problem. Ihnen wird außerhalb des Unternehmens zunächst nicht vertraut und der Partner bekommt eine Warnmeldung. Hier kann die Anbindung an eine sogenannte Bridge-CA wie die TeleTrusT European Bridge CA (EBCA) helfen: Durch die Aufnahme in deren Certificate Trust List kann das Vertrauen in die jeweilige Unternehmens-CA hergestellt und an andere Organisationen übertragen werden. Der große Vorteil einer internen Windows PKI ist die Möglichkeit, automatisiert Zertifikate für Benutzer und Geräte auszustellen. Mit einem solchen Autoenrollment werden die Betriebskosten massiv reduziert. Eine externe Managed PKI Lösung hingegen schafft dies auf der herkömmlichen Grundlage von Web-basierten Registrierungswerkzeugen nicht. Hierzu kann eine spezielle Komponente, Certificate Enrollment Proxy genannt, dienen. Dieser verbindet das interne Active Directory (AD) mit einer öffentlichen CA wie z. B. SwissSign und kann somit das Autoenrollment anerkannter Zertifikate durchführen (siehe Bild 1). Ein solcher Proxy kann auch genutzt werden, um eine interne Non-Microsoft CA mit Autoenrollment über das AD zu nutzen. Beispielsweise kann damit eine Open Source CA wie OpenXPKI eingesetzt werden. Die CA kann dann in einem isolierten Netzwerk betrieben werden, wo sie praktisch nicht mehr angreifbar ist. Angriffe auf Online CA Server häufen sich und auch ein Hardware Security Modul (HSM) hilft hier nur begrenzt, wie der Vorfall bei DigiNotar gezeigt hat, bei dem sich der Angreifer trotz HSM beliebige Zertifikate ausstellen lassen konnte. Eine Windows Enterprise CA wird somit immer im Focus professioneller Angreifer stehen.

Neben dem Enrollment von Zertifikaten in einer Windows Domäne spielt zunehmend auch die Versorgung von Netzwerkkomponenten wie Routern aber auch von Mobilgeräten wie iPhones eine wichtige Rolle. Zum einen, um diese Geräte zweifelfrei für einen Netzwerkzugang mittels IEEE 802.1x authentisieren zu können und zum anderen, um VPN-Verbindungen mit diesen Geräten zu ermöglichen. Die Geräte können über den Windows Network Device Enrollment Service (NDES) oder ein Mobile Device Management System (MDM) mit Device-Zertifikaten bestückt werden. Da viele MDM-Systeme die Microsoft-Schnittstellen und Protokolle unterstützen, können über den Certificate Enrollment Proxy problemlos auch andere interne oder auch externe CAs genutzt werden.

> „Zertifikaten einer internen Windows PKI wird zunächst außerhalb des Unternehmens nicht vertraut. Hier kann die Anbindung an eine sogenannte Bridge-CA wie der TeleTrusT European Bridge CA (EBCA) helfen."
>
> Dr. Gunnar Jacobson, Geschäftsführer Secardeo GmbH, Mitglied im TeleTrusT – Bundesverband IT-Sicherheit e.V.

Any-to-Any Encryption

Parallel hierzu wächst auch die Anforderung, die Schlüssel eines Benutzers nicht nur auf dem Windows-Client sondern auf all seinen (mobilen) Geräten verfügbar zu haben. Denn der Anwender will Zugriff auf seine verschlüsselten E-Mails haben, egal an welchem Gerät er gerade arbeitet. Hierzu verteilt der Certificate Enrollment Proxy den benötigten Private Key eines Benutzers verschlüsselt auf all seine Geräte. Ebenso möchte der Benutzer an beliebige Partner verschlüsseln können, ohne sich vorher umständlich deren Zertifikate beschaffen zu müssen. Dafür dient ein Zertifikatsserver, der dem E-Mailclient automatisch die benötigten Zertifikate im Internet beschafft, ohne dass der Benutzer davon etwas bemerkt. Damit kann er von jedem Gerät mit jedem Partner Ende-zu-Ende verschlüsselt kommunizieren – wir sprechen von Any-to-Any Encryption.

Die Mechanismen zur starken Authentisierung von Geräten und Benutzern sowie zur sicheren, unternehmensübergreifenden aber auch komfortablen Verschlüsselung sind also da. Auf den Geräten muss keine Spezial-Software installiert werden. Heutige Betriebssysteme unterstützen digitale Zertifikate und moderne E-Mailclients, sei es Outlook, Thunderbird oder iOS Mail-App und können damit verschlüsseln – es muss nur genutzt werden, dann beißen sich selbst mächtige Geheimdienste die Zähne aus.

Dr. Gunnar Jacobson

Weiterführende Informationen: www.it-daily.net

Datenblatt

Die Buttons führen Sie in der ePaper-Version direkt zum Ziel. In der Printversion nutzen Sie bitte den QR Code.