Verschlüsselt an alle und überall

Eine effiziente Verschlüsselungstechnik kann heute die gesamte IT-Infrastruktur im Unternehmen absichern

Fast jedes dritte Unternehmen in Deutschland war laut einer aktuellen Studie in den vergangenen zwei Jahren von konkreten IT-Sicherheitsvorfällen betroffen. Cyberattacken auf das geistige Eigentum sind mittlerweile zu einer existenziellen Bedrohung geworden, die auch vor dem Firmenhandy nicht haltmacht.

Angriffe auf die IT-Kommunikation von Unternehmen werden zunehmend von professionellen Organisationen bis hin zu staatlichen Geheimdiensten durchgeführt. Bedrohungen gehen nicht allein von der viel gescholtenen US-amerikanischen NSA aus, sondern insbesondere auch von Diensten aus Ländern wie China, Russland, Iran u.v.a.m. Und das Ausspähen von Daten findet nicht nur an den Überseekabeln statt – die Angriffe erfolgen mehr und mehr direkt im Unternehmensnetzwerk und betreffen alle vernetzten Systeme und Endgeräte. Wichtige Daten müssen also bereits innerhalb des Unternehmens effektiv vor unautorisiertem Zugriff geschützt werden.

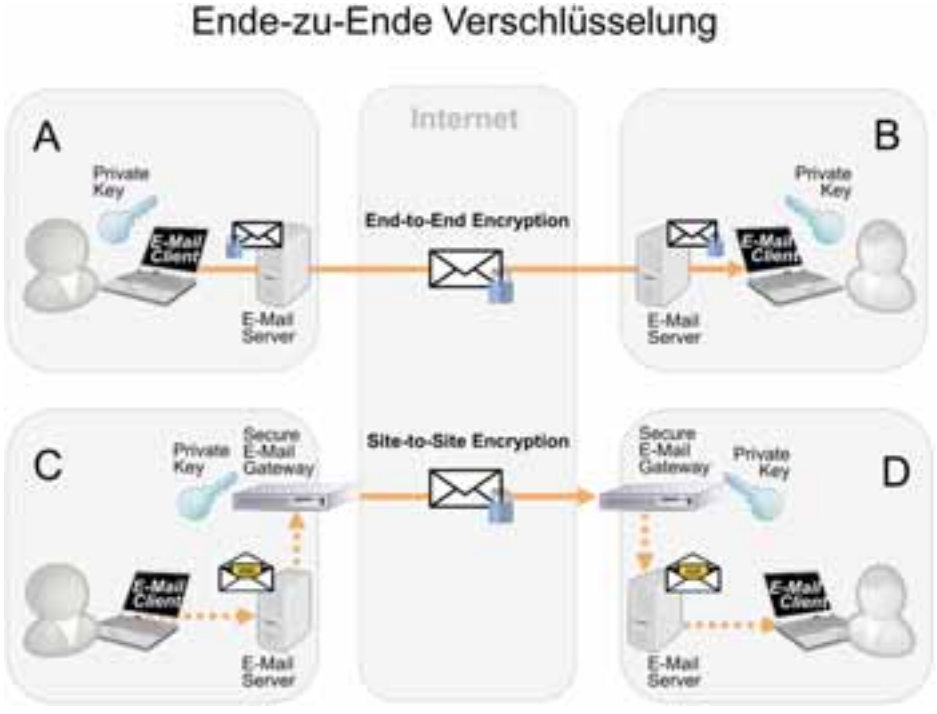
Sicherheit vom Sender bis zum Empfänger

Eine starke Ende-zu-Ende-Verschlüsselung (End-to-End Encryption, kurz: E2EE), die alle Daten bei der Speicherung und der Übertragung wirksam zu schützen vermag, stellt somit schlicht eine wirtschaftliche Notwendigkeit dar. Im Übrigen entspricht eine wirksame Absicherung der Unternehmenskommunikation nicht nur den Anforderungen zur Abwehr von Cyberspionage, sie wird darüber hinaus auch in vielen Bereichen gefordert, um Compliance-Vorgaben oder Datenschutzgesetze zu erfüllen.

Ende-zu-Ende-Verschlüsselung bedeutet, dass eine Nachricht an der Quelle verschlüsselt wird und nicht entschlüsselt werden kann, bis sie am endgültigen Ziel eintrifft. Bereits im E-Mail-Client des Absenders werden die Daten verschlüsselt und erst von der Software des Empfängers wieder entschlüsselt. Eine TLS-Verschlüsselung (Transport Layer Security) zwischen Client und E-Mail-Server bietet übrigens keine echte E2EE, ebenso wenig wie ein Secure E-Mail Gateway. Denn damit sind nur bestimmte Transportstrecken abgesichert. Der Zugriff auf unverschlüsselte E-Mails durch Serverbetreiber oder Administratoren bleibt weiterhin möglich (Abbildung 1).

Was muss verschlüsselt werden?

Wenn man vertrauliche Daten via Internet austauscht, dann kann dies mittels unterschiedlicher Dienste, Protokolle und Datenformate erfolgen. Der klassische Fall ist nach wie vor die E-Mail-Kommunikation. Für den Austausch größerer Dateien eignen sich hingegen Cloud-ba-



Quelle: Gunnar Jacobson

Echte Ende-zu-Ende-Verschlüsselung gewährt Sicherheit auf dem gesamten Übertragungsweg (Abb. 1).

Quelle: Gunnar Jacobson

Öffentlich zugängliche Server übernehmen das Schlüssel- und Zertifikatsmanagement (Abb. 2).

sierte Speichersysteme. Auch hier sollte man sich nicht auf die Transportverschlüsselung und eine serverseitige Chiffrierung verlassen, denn der Cloud-Betreiber hat dann immer eine Möglichkeit zum lesenden Zugriff. Beispiele für ein effizientes End-to-End in der Cloud sind Boxcryptor auf der Basis von Passwörtern sowie certDrive auf der Basis von digitalen Zertifikaten.

Eine weitere populäre Anwendung ist Instant Messaging (IM), also die spontane Übermittlung von Textnachrichten im Push-Verfahren (Chat). Verbreitet sind im privaten Umfeld WhatsApp und im geschäftlichen Bereich Microsoft Lync. Während Lync keine Ende-zu-Ende-Verschlüsselung bietet, gibt es hierzu zahlreiche IM-Anwendungen wie Threema oder TextSecure. Der große Nachteil solcher IM-Dienste ist, dass sie kaum interoperabel sind. Ob das Off-the-Record Messaging Protocol (OTR) dies ändert, bleibt abzuwarten.

Beim E-Mail-Verkehr kann man hingegen Interoperabilität als Selbstverständlichkeit voraussetzen – auch was die Verschlüsselung mit S/MIME (Secure/Multipurpose Internet Mail Extensions) angeht. Andere Verfahren wie Identity Based Encryption (IBE) oder auch XML Encryption konnten sich hier nicht durchsetzen.

Geheimbotschaften waren schon immer gefragt

Die Verschlüsselung von Nachrichten war schon zu Zeiten Julius Cäsars eine wichtige militärische Aufgabe, und das Brechen der deutschen Enigma-Codes durch Alan Turing hat den Zweiten Weltkrieg vermutlich um einige Jahre verkürzt. Ein Hauptproblem solcher symmetrischer Verschlüsselungsverfahren ist der sichere Austausch der Schlüssel. Dieses Problem schien in den 1970er Jahren gelöst, nachdem Diffie und Hellman das Prinzip der asymmetrischen (Public Key) Kryptografie und Rivest, Shamir und Adleman das nach ihren Initialen benannte, vor allem in der E-Mail-Kommunikation praktisch nutzbare RSA-Verfahren vorstellten. Man konnte nun also seinen Public Key veröffentlichen, mit dem jedermann in der Lage war, Nachrichten an einen zu verschlüsseln, während man selbst diese nur mit dem Private Key dechiffrieren konnte. Nebenbei lässt sich mit dem privaten Schlüssel eine digitale Signatur erzeugen. Der Empfänger kann dann anhand des Public Keys die Authentizität der Nachricht feststellen.

Da asymmetrische Kryptoverfahren rechenintensiv sind, verwendet man meist eine Kombination, die hybride Verschlüsselung. Symmetrische Verfahren wie 3DES oder AES werden dabei mit einem Data Encryption Key (DEK) zur Datenverschlüsselung eingesetzt. Der DEK wird mit den Public Keys der Empfänger verschlüsselt und zusammen mit der Nachricht übertragen. Public-Key-Verfahren haben somit zwei Hauptanwendungsgebiete: Schlüsselverteilung und digitales Signieren.

Aufgaben der Public-Key-Infrastruktur

Aus kryptologischer Sicht waren Public-Key-Verfahren ein Durchbruch, dennoch hat sich E2EE bis heute nicht in der Breite durchgesetzt. Was sind die Voraussetzungen für eine stärkere Verbreitung? Zunächst muss die Verschlüsselung rechtlich zulässig sein und darf nicht durch Gesetzeslücken ausgehebelt werden. Darüber hinaus sollte sie für den Benutzer völlig transparent erfolgen. Und schließlich muss der Aufwand für ein Public-Key-System so gering wie möglich gehalten werden.

Um diese Kriterien zu erfüllen, bedarf es einiger technischer Anforderungen: Der Public Key des Empfängers muss überall verfügbar sein und eindeutig seinem Besitzer zugeordnet werden können. Seine Gültigkeit muss sich zweifelsfrei bestimmen lassen. Der Besitzer sollte vollständige Kontrolle über seinen Private Key haben, der auch immer dort verfügbar sein muss, wo man ihn benötigt, und bei Verlust wiederhergestellt werden kann. Zudem sollten die Prozesse zur Schlüsselverwaltung weitgehend automatisierbar sein. Und nicht zuletzt muss das ganze Verfahren interoperabel sein, das heißt: Absender und Empfänger können unterschiedliche Produkte und Dienstanbieter verwenden. Diese Anforderungen an die Schlüsselverwaltung werden durch eine Public-Key-Infrastruktur (PKI) erfüllt.

Kann man einem Public Key vertrauen?

Neben den kryptografischen Eigenschaften ist das wichtigste Merkmal eines Public Keys die eindeutige Zuordnung zu seinem Besitzer, beispielsweise in Form einer E-Mail-Adresse. Wenn es jemandem gelingt, einen Public Key mit der Adresse einer anderen Person zu verteilen, wird er die für diese Person verschlüsselten E-Mails lesen können, der vorgesehene Empfänger aber nicht mehr. Solche Vorfälle sind im Fall von PGP-Verschlüsselung (Pretty Good Privacy) bekannt.

Um das Vertrauen in Public Keys zu stärken, werden verschiedene Verfahren angewandt. Das einfachste beruht auf bilateralem Vertrauen:

Die Kommunikationspartner A und B tauschen gegenseitig ihre Public Keys, beispielsweise auf einer Krypto-Party. Erweitern lässt sich diese Konstellation durch ein Vertrauensgeflecht (Web of Trust): Der Partner B, dessen Public Key Partner A bereits vertraut, bestätigt das Vertrauen in den Public Key einer weiteren Person C durch eine digitale Signatur. Somit kann A auch dem Public Key von C vertrauen. Schließlich ergibt sich eine weiter gefasste Vertrauenshierarchie: Die Glaubwürdigkeit von Public Keys wird durch eine Certification Authority (CA) hergestellt, der alle Teilnehmer vertrauen. Die CA signiert ein digitales Zertifikat gemäß ITU X.509, das neben dem Public Key auch den Namen sowie weitere Attribute enthält (X.509-Zertifikate bieten daneben auch die Option der Sperrung eines Public Keys durch die CA). Alle Teilnehmer haben die Möglichkeit, das Zertifikat anhand des Public Keys der CA zu prüfen. Eine CA kann auch selbst ein Zertifikat durch eine übergeordnete CA erhalten. Die Vertrauenshierarchie endet schließlich an einer sogenannten Root CA.

Bei all diesen Verfahren wird das Vertrauen in Public Keys, vor der eigentlichen Anwendungskommunikation, offline hergestellt. Während des Anwendungsprotokolls führt der Client eine Validierung des Public Keys durch. Bei vielen proprietären E2EE-Anwendungen im Bereich von Instant Messaging oder Cloud Encryption wird das Vertrauen in Public Keys durch den Dienstanbieter online hergestellt. Der Service liefert im Protokollablauf dem Client den benötigten Public Key des Partners zurück (ein Beispiel hierfür wäre Apple iMessage). Hierbei muss man allerdings dem Dienstanbieter vollständig vertrauen. Denn dieser kann sich durch Verteilung vorgetäuschter Keys Zugriff auf alle über seinen Server ausgetauschten Daten verschaffen.

Eine deutliche Anhebung des Sicherheitsniveaus wird erst durch eine strikte Trennung von Anwendungs- und Schlüsseldienst geschaffen: Ein vertrauenswürdiger Schlüsseldienst stellt dem Client die benötigten Public Keys bereit, die er zuvor zentral validiert hat. Er entlastet damit den Client von dieser komplexen Aufgabe. Der Schlüsseldienst hat selbst keinen Zugriff auf die ausgetauschten Nachrichten und ebenso, mangels Schlüssel, auch der Anwendungsdienst nicht.

Das erste Verfahren ist zuverlässig, aber aufwendig und kommt daher zwar im privaten, nicht aber für den betrieblichen Einsatz infrage. Das zweite Verfahren kommt bei PGP zum Einsatz. Die CA-kontrollierte Vertrauenshierarchie ist das heute für Organisationen bevorzugte Modell. Diese können hiermit das Vertrauen in alle internen Public Keys regeln – nicht nur für Personen, sondern auch für Geräte und Dienste. Oft kommt hier eine Windows-PKI zum Einsatz. Das Vertrauen in die PKI anderer Organisationen kann dann entweder durch eine Kreuz-Zertifizierung der CAs oder durch die Teilnahme in einer Bridge CA hergestellt werden, die beispielsweise eine Certificate Trust List bereitstellt. Ein sehr erfolgreiches Beispiel hierfür ist die TeleTrusT European Bridge CA (EBCA).

CA-Dienste stellen auch kommerzielle Anbieter (Trust Service Provider) wie Symantec, QuoVadis oder SwissSign bereit. Mithilfe der Managed-PKI-Dienstleistungen dieser Anbieter werden Unternehmen mit Zertifikaten versorgt. Der Vorteil dabei ist, dass die zugehörigen Root-

Quelle: Gunnar Jacobson

Eine Integration sämtlicher Endgeräte schließt die letzten Lücken in der Verschlüsselungskette (Abb. 3).

Zertifikate in vielen Systemen bereits vorkonfiguriert sind und der Public Key des Anwenders damit global als vertrauenswürdig gilt.

Wie kommt man an die Public Keys?

Verschlüsselung muss spontan und ohne Aufwand für jeden Empfänger möglich sein. Einem Anwender kann nicht zugemutet werden, dass er sich die Public Keys seiner Partner manuell besorgt, in seinem lokalen Adressbuch speichert und als vertrauenswürdig markiert. Digitale Zertifikate kann man in einem extern erreichbaren Zertifikatsserver veröffentlichen, der über eine LDAP-Anwendung (Lightweight Directory Access Protocol) abgefragt wird. Er stellt die internen Zertifikate abgesichert im Internet bereit und dient ferner als Zertifikatssuchmaschine. Gängige Clients wie Microsoft Outlook, die LDAP unterstützen, aber auch mobile Endgeräte wie das iPhone können über das ActiveSync-Protokoll hierüber automatisiert suchen.

Die Validierung der gefundenen Zertifikate kann der Zertifikatsserver zentral übernehmen, er liefert dem Client dann nur gültige Zertifikate zurück. Alternativ lässt sich über ein HTML-Formular auch manuell nach Zertifikaten für eine E-Mail-Adresse suchen. Nach X.509-Zertifikaten und PGP-Keys kann man beispielsweise auf certbox.org oder auf pgp.mit.edu (MIT-Keyserver) recherchieren. Ein für den Datenschutz äußerst wichtiges Merkmal ist dabei die Eigenschaft, nur auf gültige Adressanfragen zu antworten und ein unberechtigtes Abgreifen von E-Mail-Adressen (Address Harvesting Attacks) sowie weiterer organisationsinterner Daten zu verhindern. Leider haben nur wenige öffentliche Key- und Zertifikatsserver diese Eigenschaft. Auch andere Verfahren wie Public Key Pinning oder DNSSEC muss man in dieser Hinsicht sorgfältig überprüfen (Abbildung 2).

Bevor ein Public Key veröffentlicht werden kann, muss zunächst ein Schlüsselpaar generiert werden. In einer Windows PKI übernehmen das die Clients. Die Zertifikatsausstellung kann in mehrstufigen manuellen Genehmigungsprozessen bis hin zum völlig benutzertransparenten Auto-Enrollment erfolgen. Die Option, private Schlüssel durch autorisierte Instanzen zu rekonstruieren, ist dabei für Unternehmen unerlässlich, um Daten bei Schlüsselverlust oder nach dem Ausscheiden eines Mitarbeiters wieder lesbar zu machen.

Sicher Verschlüsseln – auch mit dem Smartphone

Wie schafft man nun aber den Private Key bequem und sicher auf alle eigenen Endgeräte, damit man überall seine E-Mails entschlüsseln kann? Aus Sicht des Benutzers und der IT-Sicherheit wäre eine Smartcard ideal, kombiniert mit einem multifunktionalen Mitarbeiterausweis, den man immer bei sich trägt. Die Unterstützung von Smartcards unter Windows ist gewährleistet, auf Mobilgeräten aber begrenzt und teuer.

Softwareschlüssel werden von Windows und gängigen Mobilgeräten unterstützt und zugriffsgeschützt gespeichert. Die Herausforderung ist hier, den einmal erzeugten Private Key eines Benutzers samt Zertifikat auf all seine Geräte zu verteilen. Das kann beispielsweise durch einen Push-Dienst realisiert werden, der die Keys verschlüsselt auf die Geräte sendet. Am Ende ist dann der Benutzer in der Lage, auf jedem seiner Geräte Nachrichten zu ver- und entschlüsseln.

KONTRÄRE ANFORDERUNGEN BEI MITTEILUNGEN

Business E-Mail	Privater Chat
Nicht-Abstreitbarkeit: Der Empfänger möchte den Urheber gegenüber Dritten nachweisen.	*Abstreitbarkeit:* Im Chat will keiner, dass eine Aussage gegen ihn verwendet werden kann.
Key Recovery: Ein Unternehmen muss E-Mails jederzeit kontrolliert lesbar machen können.	*Forward Secrecy:* Chats sind flüchtig. Ein geknackter Schlüssel soll nicht für alte oder künftige Chats genutzt werden können.
Organisiertes Vertrauen: Schlüsseln muss innerhalb der Organisation vertraut werden.	*Bilaterales Vertrauen:* Schlüssel werden direkt mit dem Partner ausgetauscht.
Interoperabilität: Herstellerunabhängigkeit und Investitionssicherheit stehen im Vordergrund.	*Proprietäre Lösung:* Man einigt sich auf die beste App.

Windows CA oder Managed PKI?

Windows Server bringt eine komplette PKI mit sich, die sich mit wenigen Mausklicks installieren lässt. In puncto Sicherheit wird man aber bei einer Online Enterprise CA an Grenzen stoßen. Angreifer mit Insiderwissen oder mit fortgeschrittenen Fähigkeiten und Tools können eine ernsthafte Bedrohung darstellen. Berichte über solche Angriffe häufen sich. Der Angriff auf die CA von DigiNotar im Jahr 2011, der letztlich zur Liquidation der Firma führte, lief übrigens trotz verwendetem Hardware Security Module (HSM) erfolgreich ab.

Um direkte Angriffe auf die interne CA und deren private Schlüssel zu verhindern, gibt es nur einen effektiven Weg: Die CA muss von dem produktiven Netzwerk und vom Active Directory (AD) isoliert werden. Damit trotzdem weiterhin aus dem Produktiv-AD manuell oder automatisiert Zertifikate beantragt und ausgestellt werden können, sollte ein Certificate Enrollment Proxy in das AD integriert werden, der eine abgesicherte Verbindung zur eigentlichen CA unterhält. Wenn man der Microsoft Software nicht vertraut und Backdoors in der Windows CA befürchtet, kann man so beispielsweise andere CA-Produkte aber auch Open Source CAs wie OpenSSL, OpenXPKI oder Dogtag anbinden.

Über einen solchen Proxy lässt sich auch die CA eines öffentlichen Trustcenters anbinden. Damit stehen einem die Dienste einer Managed PKI zur Verfügung. Das hat den enormen Vorteil, dass die Zertifikatsausstellung nicht umständlich manuell über ein Web-Portal stattfinden muss, sondern dass ein Auto-Enrollment von weltweit anerkannten Zertifikaten für interne Benutzer sowie Windows- und Mobilgeräte erfolgen kann. Benutzer sind somit in der Lage, mit einem öffentlichen, anerkannten Zertifikat auf all ihren Geräten (Any-to-Any) beispielsweise verschlüsselte E-Mails (Ende-zu-Ende) auszutauschen (Abbildung 3).

Fazit

Nach heutigem Stand der Technik sind alle Technologien und Dienste verfügbar, die eine interoperable Any-to-Any-Verschlüsselung ermöglichen. Sie müssen zum Schutz vor Cyberspionage und Hackerangriffen einfach nur intensiver genutzt werden – und das nicht nur in Großkonzernen, sondern insbesondere auch in der IT-Infrastruktur mittelständischer Unternehmen.

Dr. Gunnar Jacobson
Geschäftsführer Secardeo GmbH

Referenzen

[1] Corporate Trust: Studie: Industriespionage 2014, Cybergeddon der deutschen Wirtschaft durch NSA & Co.?
[2] Shirey: RFC 4949, Internet Security Glossary, Version 2, IETF 2007.
[3] Borisow, Goldberg, Brewer: Off-the-record communication, or, why not to use PGP, Proceedings of the 2004 ACM workshop on Privacy in the electronic society, ACM 2004.
[4] Ramsdell, Turner: RFC 5751, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, IETF 2010.
[5] Schmidt: Die Schlüssel-Falle – Gefälschte PGP-Keys im Umlauf, c't 6, Heise Verlag 2015.
[6] ITU: Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, ITU 2012.
[7] Jacobson, Neppach: Zertifikatsverzeichnisse für „öffentliche" Public Keys, DuD 7/2009, Gabler 2009.