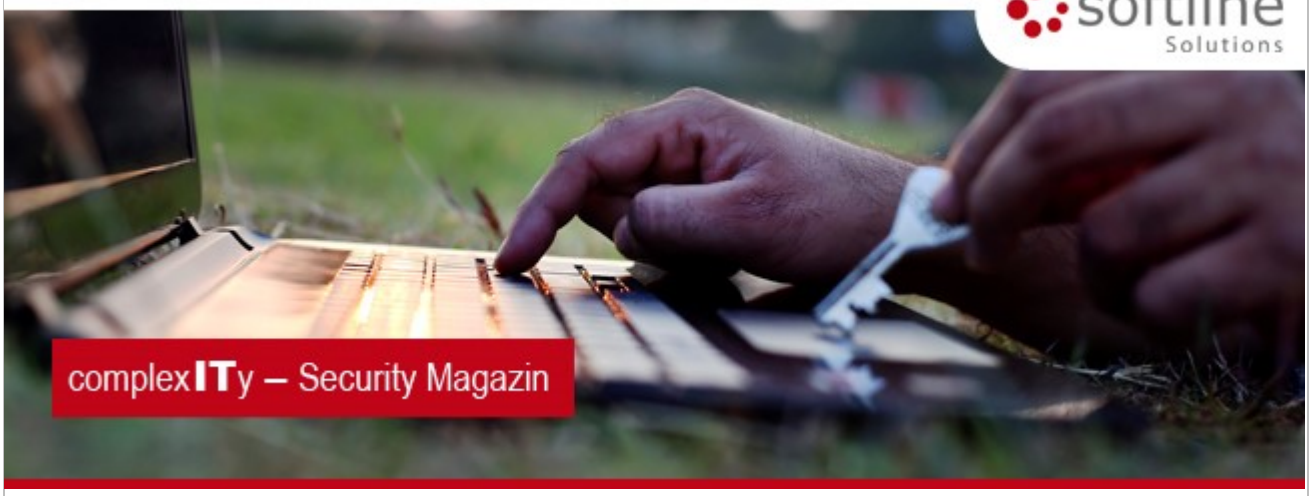


Leipzig, 27.01.2016

Liebe Leserinnen und Leser,

in der ersten Ausgabe unseres **IT-Security eMagazins »complexITy«** in diesem Jahr beschäftigen wir uns mit Entwicklungen aus dem Bereich der **Kryptographie.** Waren vor einigen Jahren vorzugsweise größere Unternehmen und Forschungseinrichtungen Opfer von Wirtschaftsspionage, sind mit steigender Digitalisierung und Vernetzung zunehmend kleine und mittlere Unternehmen betroffen. Vor Angriffen schützen vor allem kryptographische Funktionen, wie die Verschlüsselung der Kommunikation und unternehmenskritischer Daten. Diese stellen Unternehmen jedoch stets vor neue Herausforderungen. Für Sie beleuchten wir in unserem eMagazin die **wichtigsten Fragen:**

- ✓ Wie können digitale Schlüssel sicher erzeugt und aufbewahrt werden?
- ✓ Wie können diese sicher zwischen den Kommunikationspartnern ausgetauscht werden?
- ✓ Wie lässt sich der Lebenszyklus digitaler Schlüssel und verschlüsselter Daten kontrollieren?

Wir wünschen Ihnen viel Spaß beim Lesen!

Gesetze und Normen

BSI TR-02102 Kryptografische Verfahren: In jedem Unternehmen sollte es Sicherheitsrichtlinien geben und speziell eine, die den Rahmen für den Umgang mit Kryptografie innerhalb der Organisation vorgibt. Sie definiert Mindestanforderungen an die zum Einsatz kommenden Algorithmen, Verfahren und Schlüssellängen. Hierbei ist es wichtig festzulegen, auf welche Weise Schlüssel erzeugt, bereitgestellt, getauscht, verarbeitet und gesichert werden dürfen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt mit den **TR-02102-1 bis BSI TR-02102-4 technische Richtlinien** vor, die zur längerfristigen Orientierung bei der Wahl geeigneter Methoden und kryptographischer Verfahren dienen sollen. Weitere Informationen finden Sie hier!

Implementierung & Betrieb

Unternehmensweiter Einsatz von Kryptographie

Die erste Hürde beim Einsatz von digitalen Verschlüsselungen ist die Frage nach ihrer **Vertrauenswürdigkeit:** Wie lässt sich sicherstellen, dass der Schlüssel des Gegenübers ein

unverfälschter ist? Dieses Problem lösen öffentliche Zertifizierungsstellen, welche die Schlüssel digital signieren. Sie übernehmen die Beantragung, Erneuerung sowie Abmeldung der Zertifikate. Diese technischen und organisatorischen Prozesse werden unter dem Begriff **Public-Key-Infrastructure (PKI)** zusammengefasst.

Jeder Client der verschlüsselt kommunizieren oder Nachrichten signieren will, benötigt mindestens ein eigenes Zertifikat. Daher empfiehlt sich der Aufbau einer unternehmenseigenen PKI. Dabei ist zu beachten, dass die oberste Zertifizierungsstelle der PKI (Root CA) wiederum von einer öffentlichen beglaubigt wird, damit Nachrichten an externe Kommunikationspartner keine Sicherheitswarnungen beim Adressaten auslösen. Die Registrierung der eigenen PKI in einem Verbund, z. B. dem TeleTrusT European Bridge CA (EBCA), ermöglicht die sichere Kommunikation mit anderen Verbund-Teilnehmern, wie z. B. Lieferanten, Herstellern, öffentlichen Einrichtungen oder Kunden. Aufgrund der Wichtigkeit der Root CA für das Unternehmen sollte der digitale Schlüssel in einem Hardware-Sicherheitsmodul (HSM) aufbewahrt sein – nur so kann er hardwaregestützt vor Bedrohungen geschützt werden.

Beim Einsatz von Kryptographie stellt, neben der Verwaltung des digitalen Schlüsselmaterials, auch die sichere Verwendung durch Applikationen, eine Herausforderung dar. Bei der Verschlüsselung oder Signierung kann hierbei ebenfalls auf die Funktionalitäten von HSM, Trusted Platform Modules (TPM) oder Smartcards zurückgegriffen werden. Dabei erfolgt die Verwendung des Schlüssels nicht mehr direkt durch die Applikationen selbst, sondern wird an das HSM, TPM oder die Smartcard delegiert, wodurch der Schlüssel einbruchssicher in der Hardware gespeichert werden kann.

Verschlüsselung in der Cloud: Durch die zunehmende Etablierung von Cloud-Services profitieren Unternehmen von der dadurch entstehenden Flexibilität. Im schlimmsten Fall bergen diese jedoch das Risiko, dass Daten unbeabsichtigt für Dritte sichtbar werden und dadurch Strafen für das Verletzen von Gesetzen sowie Verträgen auferlegt werden. Abhilfe schafft hierbei die transparente Verschlüsselung der Daten, bevor diese in die Cloud übertragen werden. Die dabei verwendeten Schlüssel sollten wiederum in der HSM gespeichert und nicht beim Cloud-Anbieter erzeugt werden.

Key Life Cycle: Jeder digitale Schlüssel durchläuft innerhalb seines Lebenszyklus **sechs Phasen:** Die Konfigurierung, Erstellung, Verteilung, das Backup und nach Ablauf der Verwendungsdauer den Austausch durch einen neuen Schlüssel sowie die finale Vernichtung des alten. In jeder Phase kann der Schlüssel seine Vertraulichkeit verlieren, z. B. bei Design-Fehlern oder bei der Implementierung. Dies kann zur Entschlüsselung sowie Manipulation von Daten oder der Unternehmenskommunikation führen.

Die Integration eines **Key Lifecycle Managements** in die Geschäftsprozesse eines Unternehmens lässt sich nicht ohne Anpassung der technischen und organisatorischen Unternehmensprozesse realisieren. Lösungen hierfür sind am Markt rar.

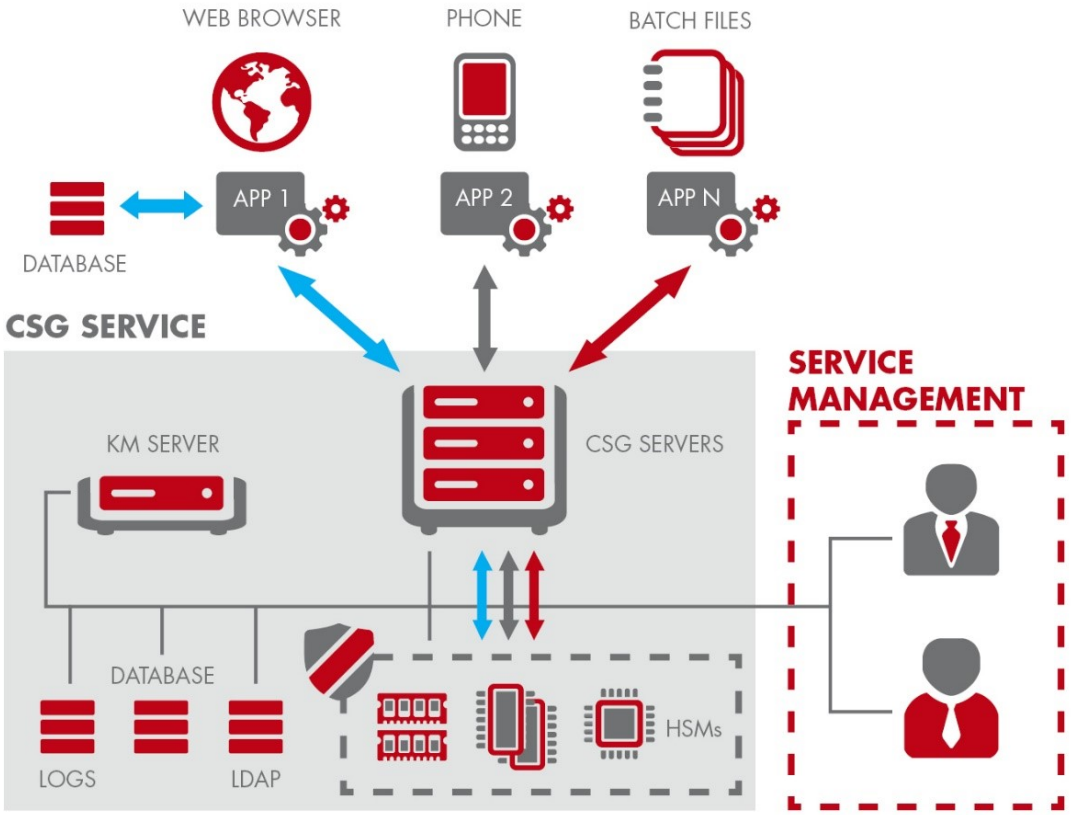
Benötigen Sie Unterstützung bei der Analyse Ihres Schutzbedarfs oder haben Sie Fragen zur kryptographischen Verschlüsselung? Unsere Experten stehen Ihnen gern mit Rat und Tat zur Seite. Senden Sie einfach eine E-Mail an it-sicherheit@softline-group.com und vereinbaren Sie einen Gesprächstermin!

Best Practice

Das Thema Compliance ist in aller Munde. Ganz aktuell durch das am 25. Juli 2015 in Kraft getretene **IT-Sicherheitsgesetz**. Die Sicherheitsrichtlinien des eigenen Unternehmens auf dem

Papier festzuhalten ist nur eine kleine Hürde. Diese jedoch praktisch umzusetzen, eine große Herausforderung. Die Idee hinter **»Crypto as a Service«** besteht darin, Unternehmen in die Situation zu versetzen (Inhouse oder aus der Cloud), Kryptographie leicht nutzen zu können, um somit die Erreichung der Sicherheitsziele (Verfügbarkeit, Integrität, Vertraulichkeit) zu unterstützen. »Crypto as a Service« hat zum Ziel, die Nutzung für Anwender/ Anwendungen und die Administration von Crypto-Systemen zu vereinfachen.

Folgende Darstellung illustriert die Funktionsweise der »Crypto as a Service«-Architektur:



KLICKEN SIE HIER FÜR WEITERE INFORMATIONEN ZU »CRYPTO AS A SERVICE«

FAQ – Was bedeutet eigentlich…?

Wo liegt der Unterschied zwischen HSM, TPM und einer Smartcard?

Obwohl sich Hardware Security Modules (HSM), Trusted Platform Modules (TPM) und Smartcards in ihrer Funktionalität, der Form und ihrem Einsatzzweck unterscheiden, sind sie technisch gesehen jeweils ein System aus Prozessor, Arbeitsspeicher und nicht-flüchtigem Speicher. Sie verfolgen alle ein Ziel: Die Verwaltung von digitalem Schlüsselmaterial.

Während die Spezifikationen von TPM und Smartcards standardisiert sind – ISO/ IEC 11889 bzw. ISO/ IEC 7816 – sind Funktionalität und Ausprägung von HSM nicht standardisiert, weshalb auch TPM und Smartcards formal gesehen als Ausprägung eines HSM angesehen werden können.

In der Praxis unterscheidet man zwischen Hochleistungs-HSMs, die als externe Geräte über TCP/ IP im Netzwerk angeschlossen sind und Steckkarten die als Erweiterung für Server und Computer erhältlich sind. Beide dienen dem Schutz des darauf befindlichen Schlüsselmaterials und werden

nach dem **FIPS 140 Standard** zertifiziert. Während Smartcards benutzerspezifisch verwendet werden, ist das TPM an ein einziges physisches System gebunden, das sich als Hardwarechip auf der Hauptplatine des Computers befindet.

Was bedeutet PKCS#11?

PKCS steht für Public Key Cryptography Standards und bezeichnet aktuell 13 Standards der asymmetrischen Kryptographie. Der elfte Standard (#11) heißt Cryptographic Token Interface (Cryptoki) und beschreibt eine plattformunabhängige Programmierschnittstelle (API), die einen Schlüsselwert z. B. auf einer HSM, einem Token oder einer Smartcard festlegt.

Was bedeutet KMIP?

KMIP steht für Key Management Interoperability Protocol. Dieses Protokoll ermöglicht die Kommunikation zwischen der zentralen Schlüsselverwaltung (Key Lifecycle Management System) und dessen Clients. U. a. definiert es wie eine Nachricht aufgebaut ist und was sie beinhaltet. Dies kann z. B. der Algorithmus sein, mit dem der Schlüssel erstellt wurde, die Länge, der Besitzer, das Ablaufdatum oder die eindeutige Bezeichnung des Schlüssels. Um die Integrität der Daten und die Authentifizierung zu sichern, stützt sich die Kommunikation auf ein Sicherungsprotokoll in der Transportschicht (TLS).

Wo liegt der Unterschied zwischen symmetrischer und asymmetrischer Kryptographie?

Die **symmetrische Verschlüsselung** wird zum sicheren Austausch von geheimen Daten über das Netzwerk genutzt. Sie ermöglicht die Verschlüsslung von großen Datenmengen und deren Integritätssicherung (Message Authentication Code). Hierbei wird der gleiche Schlüssel vom Sender und Empfänger verwendet. Dieses Verfahren stellt eine schnelle und effiziente Methode zur Datenverschlüsselung dar.

Diese Methode wird als Algorithmus AES (Advanced Encryption Standard) u. a. bei kabellosen Netzwerken (WPA2) und bei der Komprimierung von Dateien (RAR, ZIP), verwendet. Einen Nachteil stellt der Austausch des Schlüssels dar, denn dieser sollte so übertragen werden, dass nur Berechtigte den Schlüssel erhalten. Die Übertragung über eine Out-of-band Methode ist aber gefahrenlos möglich.

Das Problem des sicheren Schlüsselaustauschs wird durch die **asymmetrische Verschlüsselung** gelöst: Hierbei werden jeweils ein öffentlicher (Public Key) und ein privater Schlüssel (Private Key) erstellt. Diese werden als Schlüsselpaar bezeichnet. Der öffentliche Schlüssel kann beliebig verbreitet werden, der private Schlüssel ist jedoch geheim und muss gut geschützt werden.

Ein Beispiel hierfür ist die RSA-Verschlüsselung. Sie wird bei E-Mail Verschlüsselungen (OpenPGP, S/MIME) oder als RFID Chip auf dem deutschen Reisepass verwendet. Der Nachteil dieses Verfahrens ist die zeitaufwändige Verschlüsselungsprozedur.

Um die Vorteile beider Systeme zu vereinen, gibt es hybride Verschlüsselungen. Dabei wird der symmetrische Schlüssel durch den öffentlichen Schlüssel des Empfängers verschlüsselt, so dass der symmetrische später beim Empfänger mithilfe des privaten Schlüssels entschlüsselt werden kann.

Wofür steht Salz in der Kryptologie?

Wenn ein Benutzer ein Passwort anlegt und speichert, wird aus dieser Klartext-Passwort-Eingabe ein Hashwert erzeugt. Wird dieser Hashwert vom Speicherort oder bei der Übertragung

abgegriffen oder abgehört, so könnte das Passwort bspw. über Rainbow-Tables (Tabelle die auf das Passwort referenziert) oder einen Wörterbuchangriff entziffert werden. Um die Entschlüsselung zu erschweren, wird an das Passwort eine zufällig gewählte Zeichenfolge angefügt. Dadurch erhöht sich die Entropie des Passworts und damit auch der Hashwert. Das Hinzufügen der zusätzlichen Zeichenfolge wird als Salt (engl. für Salz) bezeichnet.

Softline Services

Damit Sie sich in Zukunft keine Sorgen mehr über die Verschlüsselung und das Zugriffsmanagement in Ihrem Unternehmen machen müssen, bietet Ihnen die Softline folgende Services an:

- Health-Check Sicherheitsrichtlinien/ Einsatz von Kryptografie (Aktualität, Angemessenheit der Maßnahmen)
- Evaluierung, Konzeption und Implementierung einer Public-Key-Infrastructure
- Beratung und Implementierung eines Hardware-Sicherheitsmoduls (HSM)
- Konzeptionelle Beratung zum Thema „Key Life Cycle Management“

Haben wir Ihr Interesse geweckt? Dann kontaktieren Sie uns unter it-sicherheit@softline-group.com oder rufen Sie uns an: +49 341 24051-0. Wir helfen Ihnen gern weiter.

Veranstaltungshinweise

- **19.02. bis 21.02.2016**
  2nd International Conference on Information Systems Security and Privacy
- **29.02. bis 04.03.2016**
  RSA Conference 2016
  Weitere Informationen
- **08.03. bis 09.03.2016**
  The Cyber Security Show 2016
  Weitere Informationen

Falls Sie Fragen oder Hinweise zu gewünschten Magazininhalten haben oder unsere Unterstützung in IT-Sicherheitsprojekten benötigen, dann kontaktieren Sie uns unter it-sicherheit@softline-group.com oder telefonisch unter +49 341 24051-0.

Mit freundlichen Grüßen

Ihr Softline Team.

Softline Solutions GmbH // Geschäftsführer: Martin Schaletzky // Sitz der Gesellschaft: Leipzig // Handelsregister Leipzig: HRB 26058 // Steuer Nr.: 232/118/06001 // USt ID: DE270894910