Richtlinie zum Umgang mit Verschlüsselung und Kryptographie

Untertitel

Klassifikation:	Bitte klassifizieren!
Datum:	21.02.2019
Version:	**0.1**
Autor:	Reiner Schröppel
Dok.-Name:	RL_Kryptographie_V0.10.docx
Seiten:	8

Dokumentenhistorie

Version	Datum	Bearbeiter	Status	Bemerkung/Änderung
0.10	29.01.2019	R. Schröppel	In Bearbeitung	Ersterstellung

Inhaltsverzeichnis

1 Einleitung, Zweck und Ziele

Der Zweck dieses Dokuments ist die Festlegung von Regeln für die Anwendung kryptografischer Maßnahmen sowie der Regeln für die Nutzung kryptografischer Schlüssel, um die Vertraulichkeit, Integrität, Authentizität (Nichtabstreitbarkeit) von Informationen zu schützen.

Das Unternehmen ist stark von ihrer informationstechnischen Infrastruktur abhängig und muss die gespeicherten und zu verarbeitenden Informationen, sowohl bei der Verarbeitung, wie auch bei der Kommunikation, angemessen schützen. Aus diesem Grund sind entsprechende Maßnahmen zu treffen, damit dies realisiert werden kann. Zu solchen Maßnahmen zählen auch kryptographische Verfahren/Lösungen, die über eine einfache Verschlüsselung hinausgehen.

...

2 Anwender

Anwender dieses Dokuments sind alle Abteilungen und Bereiche des Unternehmens, die kryptografisches Material nutzen, bereitstellen, speichern oder verwalten.

Grundsätzlich ist es Aufgabe der Informationseigentümer, festzulegen, ob Informationen vertraulich, korrekt und/oder nachvollziehbar gespeichert, verarbeitet und/oder übertragen werden müssen.

Die technische Umsetzung, mit dem Ziel den Anforderungen des Informationseigentümers nachkommen zu können, liegt in der Verantwortung des Bereich IT. Für Anwendungen/Verfahren, die nicht durch den Bereich IT betrieben werden, obliegt es dem Fachbereich, die Vorgaben dieser Richtlinie einzuhalten.

3 Geltungsbereich

Jeder Bereich innerhalb des Unternehmens, der wesentlich mit kryptografischem Material arbeitet, mit Systemen, die kryptografisches material speichern, erzeugen oder nutzen, ist angehalten, die in dieser Richtlinie vorgegebenen Anforderungen zu prüfen und umzusetzen. Für den Fall, dass einzelne Maßnahmen in dieser Richtlinie nicht umgesetzt werden können, ist eine entsprechende Risikobewertung durchzuführen und dem Informationssicherheitsbeauftragten zu kommunizieren.

4 Definitionen und Begriffe (falls vorhanden)

Begriff	Erläuterung
Kryptografie	...
Kryptografisches Schlüsselmaterial	...
...	...
...	...
...	...
...	...
...	...
...	...

Begriff	Erläuterung
Informationseigentümer	Die einzelnen Bereiche/Abteilungen des Unternehmens sind Eigentümer ihrer erzeugten Daten.

Begriff	Erläuterung
Richtlinienverantwortlicher	Der Bereich/Die Rolle, welche die Richtlinie Kryptografie in regelmäßigen Abständen überprüft und pflegt. Im Unternehmen ist der Richtlinienverantwortliche der ISB.

5 Mitgeltende Unterlagen und Referenzdokumente

Die nachfolgend aufgeführten Referenzdokumente verweisen auf Dokumente, bzw. Richtlinien des Unternehmens, die beim Umgang mit kryptografischem Material zu berücksichtigen sind bzw. in denen Konkretisierungen zur Umsetzung des dieser Richtlinie beschrieben sind.

- Informationssicherheitsleitlinie des Unternehmens
- ...
- ...
- Richtlinie zur Klassifizierung von Informationen
- Methodik zur Risikoeinschätzung und -behandlung

6 Zuständigkeit

Die Richtlinie Kryptografie richtet sich an alle Verantwortlichen der Informationssicherheit, sowie an alle Mitarbeiterinnen und Mitarbeiter des Unternehmens, die in Ihrer täglichen Arbeit mit kryptografischem Material arbeiten, dieses nutzen oder Kryptosysteme administrieren.

...

7 Umsetzung

7.1 Abgrenzung

Die in dieser Richtlinie gemachten Vorgaben befassen sich in der Hauptsache mit der Nutzung von Schlüsselmaterial beim Einsatz auf IT-Systemen, d.h. vornehmlich zum Schutz von Daten/Informationen während der Übertragung oder bei der Speicherung.

Für einen Einsatz einer PKI-Lösung zur sicheren E-Mailkommunikation mittels PGP-Schlüssel oder S/MIME-Zertifikaten ist eine entsprechende, aus dieser Richtlinie ab-geleitete, Detailrichtlinie zu erstellen und umzusetzen.

7.2 Grundsätzliches

Sowohl die Informationseigentümer, wie auch der Bereich IT sind angehalten, technische und organisatorischen Anforderungen und Notwendigkeiten angemessen gegeneinander abzuwägen.

...

7.3 Organisatorische Sicherheit

7.3.1 *Einsatzumgebungen und -bedingungen der kryptographischen Produkte*

...

7.3.2 *Sicherheitsregeln*

...

7.3.3 *Qualifikation und Schulung der Mitarbeiter*

Mitarbeiter sind im richtigen Umgang und der Vertraulichkeit des kryptografischen Materials zu schulen.

Mitarbeiter, die Geräte administrieren, auf denen kryptografisches Material zum Einsatz kommt (z. B. VPN-Gateways, Router, Web-Server, etc.), oder die kryptografisches Material erstellen, verteilen, speichern, etc., sind im Umgang mit dem kryptografischen Material zu schulen.

7.3.4 *Verlust, Kompromittierung*

Liegt der Verdacht nahe, dass kryptografisches Material verloren oder kompromittiert wurde, ist umgehend der ISB des Unternehmens zu informieren.

...

7.4 Kryptografische Verfahren

7.4.1 *Allgemeines*

Es sind Vorgaben für die zu nutzenden Verschlüsselungsverfahren, wie z. B. die im Unternehmen zugelassenen und einzusetzenden Verschlüsselungsverfahren, Schlüssellängen, Hashes, etc. festzulegen.

...

7.4.2 *Softwareentwicklung*

...

7.5 Schlüsselmanagement

Ziel eines Schlüsselmanagements muss es sein, dass Schlüssel, egal ob symmetrisch (PINs, Passwörter, etc.) oder asymmetrisch (getrennte öffentliche und private Schlüssel), sicher

- erzeugt,
- verteilt,
- genutzt,
- gespeichert,
- deaktiviert und
- gelöscht

werden.

7.5.1 *Schlüsselerzeugung*

Grundsätzlich muss die asymmetrische Schlüsselerzeugung zentral und gesteuert erfolgen. Für den Fall von extern (offiziell) beglaubigtem Schlüsselmaterial ist ein CSR (Certificate Signing Request) zu erstellen und mittels dieses CSR der öffentliche Schlüssel zu beglaubigen.

...

7.5.2 *Schlüsselverteilung und -installation*

...

7.5.3 ...

...

7.5.4 ...

...

7.5.5 ...

...

7.5.6 ...

...

7.5.7 *Schüsselerneuerung*

Es sind Vorkehrungen zur Schlüsselerneuerung/-verlängerung zu treffen.

Besonders für den Fall, dass Schlüsselmaterial auf Systemebene zum Einsatz kommt, d.h. vornehmlich zum Schutz von Daten/Informationen während der Übertragung oder bei der Speicherung, sind die mit dem Schlüsselmaterial verbundenen Ablaufzeiten zu überwachen, so dass rechtzeitig vor Ablauf des Schlüsselmaterials entsprechende Maßnahmen zum Austausch/Verlängerung des Schlüsselmaterials getroffen werden können.

7.6 Umgang mit kryptografischem Material

...

7.6.1 *Ausmusterung von Systemen*

Bei der Ausmusterung von Systemen ist relevantes Schlüsselmaterial zu entfernen und, soweit möglich, der Werkszustand des Systems herzustellen.

Ist eine Löschung von auf dem System gespeicherten relevantem Schlüsselmaterial nicht möglich, so ist das System oder die Komponente, auf der das relevante Schlüsselmaterial gespeichert ist, sicher zu entsorgen bzw. zu vernichten.

7.6.2 *Entsorgung von Speichermedien*

...

7.6.3 *Umgang bei Reparatur, Garantie*

...

7.6.4 ...

...

7.7 Notwendige Aufzeichnungen

Um den Anforderungen dieser Richtlinie zu entsprechen, sind mindestens die nachfolgende Vorgänge, Nachweise, etc. zu dokumentieren und aufzubewahren:

...

8 Freigabe

Ort, Datum	Name in Druckbuchstaben	Unterschrift