DGI® Deutsche Gesellschaft für Informationssicherheit AG

Management der kryptographischen Verfahren (Kryptographiekonzept)

Kennzeichnung Vertraulichkeitskategorie

Inhaltsverzeichnis

1 Ziel und Zweck

Diese Regelung bestimmt die einzuhaltenden Vorgaben für das Management der kryptographischen Verfahren.

Durch die Einhaltung der Vorgaben dieser Regelung soll insbesondere Folgendes sichergestellt werden

- Das sichere, ordnungsgemäße und konforme Management der Ver- und Entschlüsselung digitaler Daten
- Die Gewährleistung des sicheren Betriebs von Datenverarbeitungen und Anwendungen
- Die Gewährleistung des sicheren Betriebs von Kommunikationswegen und Kommunikationsschnittstellen
- Die Gewährleistung der sicheren Datenübermittlung
- Der Schutz der Identität von Personen
- Die Einhaltung gesetzlicher und vertraglicher Anforderungen zur Risikofrüherkennung sowie der Umsetzung von technischen und organisatorischen Maßnahmen (Compliance)
- Die Einhaltung der Vorgaben der Informationssicherheit sowie des Datenschutzes

2 Geltungsbereich

Die Vorgaben dieser Regelung gelten für

- Geltungsbereich benennen, wie *„die gesamte Organisation, die Abteilung IT oder den Standort Berlin“*

3 Verantwortlichkeiten für das Management dieser Regelung

Verantwortlich für die Planung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.
Verantwortlich für die Umsetzung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.
Verantwortlich für die Überwachung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.
Verantwortlich für die Aufrechterhaltung und Verbesserung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.

5.3 Umsetzung

5.3.1 Allgemeines

Die Prozesssteuerung sowie das Management für die Umsetzung dieser Regelung müssen dokumentiert und sollten in das ISMS integriert werden.

Die Maßnahmen für die Umsetzung müssen kontinuierlich sowie anlassbezogen aktualisiert, angepasst und verbessert werden.

5.3.2 Anforderungen an Aktivitäten für das Management der kryptographischen Verfahren

Die Informationen zu den aktuellen Anforderungen an das Management der kryptographischen Verfahren

- Anforderungen an Medien und IT-Systeme
- Anforderungen an die Übermittlung und den Transport von Informationen
- Anforderungen an die Aufbewahrung und die Archivierung von Informationen
- Anforderungen an Schnittstellen
- Die Verfahren für die Identifikation und Erfassung von zu verschlüsselnden Systemen
- Die Verfahren für die Auswahl und Festlegung der geeigneten Art der Verschlüsselung
- Die Verfahren für die Beschaffung von Produkten für die Verschlüsselung von zu verschlüsselnden Systemen
- Die Verfahren für die Inventarisierung der Komponenten für die Verschlüsselung von zu verschlüsselnden Systemen
- Die Verfahren für die Einrichtung und Konfiguration der kryptographischen Systeme

5.3.3 Einsatz von kryptographischen Verfahren

5.3.3.1 Allgemeines

Die kryptographischen Verfahren müssen für den Einsatz in der Organisation als zulässig freigegeben werden. Der Einsatz von kryptographischen Verfahren muss sodann unter Berücksichtigung der nachfolgenden Regelungen erfolgen.

Der Einsatz von kryptographischen Verfahren muss im Hinblick auf das zu erreichende Sicherheitsniveau für die Durchführung des Geschäftsbetriebs der Organisation geeignet sein, dem Stand der Technik entsprechen und nachweislich erfolgen.

Zudem muss berücksichtigt werden, dass bei unterschiedlichen kryptographischen Systemen

Verfahrensdokumentation sowie den mitgeltenden Dokumentationen beschrieben.

Durch die Einhaltung der Vorgaben der Prozesse, Anweisungen und Regelungen des Managements der Durchführung einer IT-Strukturanalyse wird, in Bezug auf die Identifikation und Erfassung von zu verschlüsselnden Systemen unter Berücksichtigung der Gewährleistung des avisierten Sicherheitsniveaus und der Erfüllung der Anforderungen an eine Verschlüsselung und Entschlüsselung, insbesondere Folgendes sichergestellt

- Erhebung sämtlicher IT-Systeme insbesondere der
    - Endgeräte
    - Server
    - Netzwerkkomponenten
    - virtualisierten IT-Systeme

- Sicherstellung der Anwendung von ausschließlich erprobten und ausreichend getesteten kryptographischen Verfahren

Die festzulegende Art der Verschlüsselung muss für sämtliche kryptographischen Systeme den geforderten und vereinbarten Schutzbedarf sicherstellen.

Die Planung, Steuerung und Durchführung sowie die Überwachung, Aufrechterhaltung und fortlaufende Verbesserung des Managements einer Schutzbedarfsfeststellung sind in der zugehörigen Verfahrensdokumentation sowie den mitgeltenden Dokumentationen beschrieben.

Durch die Einhaltung der Vorgaben der Prozesse, Anweisungen und Regelungen der Durchführung der Schutzbedarfsfeststellung wird, in Bezug auf die Auswahl und Festlegung einer geeigneten Art der Verschlüsselung unter Berücksichtigung der Gewährleistung des avisierten Sicherheitsniveaus und der

Umsetzung und fortlaufende Gewährleistung des avisierten Sicherheitsniveaus

Die Ergebnisse der Auswahl und Festlegung der geeigneten Art der Verschlüsselung und der Schutzbedarfsfeststellung müssen anforderungsgerecht dokumentiert, kommuniziert, bereitgestellt und aufbewahrt werden.

5.3.4 Beschaffung von Produkten und Verfahren für die Verschlüsselung von Systemen

Durch die Einhaltung der Vorgaben der Prozesse, Anweisungen und Regelungen des Managements der IT-Beschaffung von kryptographischen Produkten und Verfahren sowie des IT-Outsourcing von kryptographischen Verfahren und Systemen sollte insbesondere Folgendes sichergestellt werden

- Gewährleistung der Erfüllung der Anforderungen an das Management der IT-Beschaffung sowie des IT-Outsourcing für die Verschlüsselung von Systemen
- Entwicklung und Steuerung des Servicekatalogs für den Bezug von Services für die Verschlüsselung von Systemen
- Steuerung des Lieferantenmanagements (Supplier Management) für den Bezug von Leistungen für die Verschlüsselung von Systemen
    - Festlegung des Vorgehens der Beschaffung von kryptographischen Produkten und Verfahren sowie von kryptographischen Systemen

Zeitraum technischen Support, Updates und Wartungsgarantien für die verwendeten Produkte und Verfahren gewährleisten.

Die Erstbeschaffung, die Ersatzbeschaffung oder die Wiederbeschaffung von Produkten und Verfahren für die Verschlüsselung von Systemen muss in die Prozesse des Service Asset and Configuration Management integriert sein.

Die Ergebnisse der Auswahl für die IT- Beschaffung und für das IT-Outsourcing von kryptographischen Produkten und Verfahren sowie der kryptographischen Systeme müssen anforderungsgerecht dokumentiert, kommuniziert, bereitgestellt und aufbewahrt werden.

5.3.6 Steuerung des Einsatzes von kryptographischen Systemen

5.3.6.1 Einrichtung und Konfiguration eines kryptographischen Systems

Die Verantwortlichen für die Einrichtung und Konfiguration der kryptographischen Systeme müssen sicherstellen, dass die ordnungsgemäße, sichere und konforme Verschlüsselung und Entschlüsselung gemäß dem avisierten Schutzniveau umgesetzt wird und nachgewiesen werden kann.

Bei der Einrichtung und Konfiguration von kryptographischen Systemen muss insbesondere Folgendes berücksichtigt werden

- Die Verwendung eines geeigneten und sicheren Schlüsselmanagements
- Die Verwendung geeigneter und sicherer kryptographischer Verfahren
- Die Verwendung geeigneter und sicherer kryptographischer Produkte

- Die sichere Löschung und Vernichtung von kryptographischen Schlüsseln und Zertifikaten
- Die sichere Außerbetriebnahme von kryptographischen Systemen

Die zu erfüllenden Anforderungen und umzusetzenden Maßnahmen, um den ordnungsgemäßen, sicheren und konformen Betrieb eines kryptographischen Systems zu gewährleisten, müssen anforderungsgerecht dokumentiert, kommuniziert, bereitgestellt und aufbewahrt werden.

5.3.6.2 Vorgaben für die Umsetzung und Einhaltung des avisierten Sicherheitsniveaus

Um das avisierte Sicherheitsniveau durch den Einsatz der kryptographischen Systeme gewährleisten zu können muss insbesondere Folgendes berücksichtigt und umgesetzt werden

- Die sichere Installation und Konfiguration sämtlicher Produkte und Verfahren für den Betrieb der kryptographischen Systeme
- Die unverzügliche Änderung voreingestellter Schlüssel
- Die angemessene Validierung und Durchführung von Tests der kryptographischen Systeme vor der Inbetriebnahme sowie fortlaufend während des Betriebs
- Die angemessene Validierung und Durchführung von Tests nach Änderungen der Einsatzumgebung sowie nach Änderung der relevanten IT-Systeme
- Das angemessene Monitoring der Betriebsfähigkeit und Resilienz der eingesetzten kryptographischen Systeme

5.3.6.3 Sichere Verwendung von Schlüsseln und Zertifikaten

Für den sicheren Einsatz und die sichere Steuerung von kryptographischen Schlüsseln und Zertifikaten muss insbesondere Folgendes berücksichtigt werden

- Jeder öffentliche Schlüssel ist vor Verlust und Beschädigung zu schützen
- Jeder nicht-öffentliche Schlüssel ist vor Verlust, Beschädigung und unberechtigtem Zugriff zu schützen
- Sämtliche Schlüssel sind in regelmäßigen Zeitabständen und spätestens bei Auslaufen eines Schlüssels zu ändern
- Für jeden Schlüssel ist ein Verfahren für dessen Wiederherstellung festzulegen
- Für unterschiedliche Einsatzgebiete sind unterschiedliche Schlüssel zu verwenden