Zentraler Kreditausschuss

ZKA-Datensicherheitsstandard

Version: 1.0

Stand: 18.11.2009

Referenzierung

Die Referenzierung in weiteren Dokumenten des Zentralen Kreditausschusses erfolgt unter:
[ZKA DSS] Zentraler Kreditausschuss: ZKA-Datensicherheitsstandard Version 1.0, 18.11.2009

Dokumentenhistorie

Version	Stand	Abschnitt/ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.2	24.11.2008	alle	Erstellung	SRC
0.5	19.01.2009	alle	Überarbeitung aufgrund der Ergebnisse der Arbeitsgruppensitzung vom 2.12.2008	SRC
0.6	20.02.2009	alle	Überarbeitung aufgrund der Ergebnisse der Arbeitsgruppensitzung vom 29.01.2009	SRC
0.61	06.05.2009	6,8,18 u.a.	Neue Schutzbedarfsklasse "I“ für Integritätsschutz eingefügt.	SRC
0.62	12.05.2009	1, 2, 3.1, 3.2 .3.3	Überarbeitung	ZKA-Arbeitsgruppe
0.63	19.05.2009 20.05.2009	3.4 – 3.6.1.3	Überarbeitung Umformulierung Sicherheitsboxen -> Hardware-Sicherheitsmodule	ZKA-Arbeitsgruppe, SRC
0.64	28.05.2009	3.6.1.5-3.8.2.8	Überarbeitung zur Vorbereitung des Workshops am 17.06.2009	SRC
0.65	17.06.2009	3.6.1.5-3.7.2.4	Überarbeitung.	ZKA-Arbeitsgruppe
0.7	30.06.2009	3.6.5, 3.7.3-3.8.2	Überarbeitung	ZKA-Arbeitsgruppe
0.71	23.07.2009	4	Überarbeitung	SRC
0.9	29.07.2009	1, 1.1, 3.7.1.2, 3.7.3	Überarbeitung	ZKA-Arbeitsgruppe
0.91	07.08.2009	1, 1.1, 2.1, 2.2, 3.3.4	Editorielle Überarbeitung	SRC
0.92	17.09.2009	1, 3.1, 3.2, 3.3, 3.4,. 3.8	Überarbeitung nach Kommentierungsphase	ZKA-Arbeitsstab "Sicherheitsfragen und -strategien", BdB, Postbank
0.93	28.09.2009	1, 3.1, 3.2, 3.3, 3.4,. 3.8	Überarbeitung nach Kommentierungsphase	ZKA-Arbeitsgruppe

Version	Stand	Abschnitt/ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0	18.11.2009	3.2.1.2., 3.2.2.1., 3.3.4, 3.7.3.1 - 3.7.3.3, 3.8.2.3 3.5.4	Überarbeitung nach Kommentierungsphase	BdB, SRC

Inhalt

1 Einleitung und Zielsetzung

Der ZKA Datensicherheitsstandard formuliert die Sicherheitsziele der deutschen Kreditwirtschaft für die für den kartengestützten Zahlungsverkehr relevanten Hintergrundsysteme. Der ZKA Datensicherheitsstandard nimmt Bezug auf die internationalen Ansätze zur Erhöhung der Sicherheit von Transaktionsdaten. Er abstrahiert dabei von bereits in anderen Kriterienwerken vielfältig vorhandenen konkreten Vorgaben und Einzelmaßnahmen und erhält dadurch eine größere Beständigkeit gegenüber kurzfristigen technischen Veränderungen.

Indem die Angemessenheit von Maßnahmen zur Umsetzung des Standards in den Vordergrund gestellt wird, wird ein risikobezogener Ansatz betont, der eine Harmonisierung des Vorgehens zur Erhöhung der IT-Sicherheit und zugleich die angesichts der Vielfalt an technischen Systemen und Prozessen erforderliche Gestaltungsfreiheit in der Umsetzung ermöglicht.

Ein weiterer Beitrag zur Beständigkeit und Praktikabilität des ZKA Datensicherheitsstandards ist die Entkoppelung von Anforderungen und Daten, auf die sich die Anforderungen beziehen. Durch die Festlegung, welche Datenelemente als schützenswert gelten, kann der Standard ausgerichtet werden, ohne dass die Sicherheitsanforderungen selbst angepasst werden müssen. Die Anforderungen werden dabei nicht unmittelbar auf einzelne Datenelemente, sondern auf Schutzbedarfsklassen bezogen. Durch die Möglichkeit der Zuordnung einzelner Datenelemente zu den Schutzbedarfsklassen wird die Anpassung des Standards an die jeweiligen Erfordernisse erleichtert, wenn sich diese im Rahmen der zukünftigen Weiterentwicklung des Standards ändern sollten.

1.1 Geltungsbereich

Die Anforderungen des ZKA-Datensicherheitsstandards beziehen sich auf die Prozesse und IT-Systeme der kreditwirtschaftlichen Hintergrundsysteme, die zur Verarbeitung von kartenbasierenden Transaktionen schützenswerte Datenobjekte übertragen, verarbeiten oder speichern.

Für Endgeräte wie POS-Terminals, Geldautomaten und Online-Terminals, den electronic cash Netzbetrieb sowie für den Interbanken-Zahlungsverkehr gelten eigene Anforderungen. Diese sind u. a. in den folgenden Dokumenten enthalten: "Regelwerk für das Deutsche Geldautomaten-System - Vereinbarungen, Richtlinien und Anlagen zu den Verträgen über das Deutsche Geldautomaten-System“ [GA 2007_REV], "Technischer Anhang zum Vertrag über die Zulassung als Netzbetreiber im electronic cash-System der deutschen Kreditwirtschaft“ [EC_TA7] sowie "Vereinbarung über die Absicherung der PIN für von Instituten der deutschen Kreditwirtschaft herausgegebene Bankkarten und Sparkassenkarten“ [ZKA_PIN] enthaltenen Sicherheitsanforderungen.

1.2 Begriffsbestimmungen

- Der Begriff des "IT-Systems" in der Definition des Geltungsbereichs (Abschnitt 1.1) bezieht sich auf alle Komponenten und Netzwerkstränge, die zur Verarbeitung von zu schützenden Datenelementen (vgl. Abschnitt 2.2) verwendet werden, sowie auf solche, die nicht durch verlässliche Maßnahmen der Netzwerksegmentierung von diesen Komponenten getrennt sind.

- MUSS bedeutet, dass es sich um eine verpflichtende Festlegung bzw. Anforderung handelt.

- DARF NICHT bezeichnet den strikten Ausschluss einer Eigenschaft.

- SOLL beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.

- SOLL NICHT kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.

- KANN bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

- Der Begriff "Mitarbeiter“ bezieht sich auf Vollzeit-, Teilzeit- und befristet beschäftigte Personen sowie auf externe Mitarbeiter eines Unternehmens.

- Der Begriff "zu begleitende Personen“ bezieht sich auf betriebsfremde Personen (z. B. Lieferanten, Gäste von Mitarbeitern, Service-Personal), die aufgrund von bestehenden Regelungen zu begleiten sind.

2 Schutzbedarfsklassen und zu schützende Datenelemente

2.1 Schutzbedarfsklassen

Als Voraussetzung für den effizienten Einsatz von Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit von Datenelementen ist deren Differenzierung hinsichtlich des Schutzbedarfs unverzichtbar. Diese Differenzierung erfolgt auf der Basis von Schutzbedarfsklassen, denen die zu schützenden Datenelemente zugeordnet werden. Im Kontext dieses Dokuments werden die Schutzbedarfsklassen "V-Hoch" und "V-Mittel" hinsichtlich der Vertraulichkeit und "I-Mittel“ hinsichtlich der Integrität von Datenobjekten unterschieden. Datenobjekte, die keiner Schutzbedarfsklasse zugeordnet sind, werden im Kontext dieses Dokuments als nicht schutzwürdig betrachtet.

Schutzbedarfsklasse "V-Hoch“: Datenelemente, für die der Schutz der Vertraulichkeit von besonders hoher Bedeutung ist.

Schutzbedarfsklasse "V-Mittel“: Datenelemente, für die der Schutz der Vertraulichkeit von mittlerer Bedeutung ist.

Schutzbedarfsklasse "I-Mittel“: Datenelemente, für die der Schutz der Integrität von Bedeutung ist.

2.2 Zu schützende Datenelemente

Die folgende Tabelle listet die zu schützenden Datenelemente Transaktionsdaten auf. Die Tabelle ist folgendermaßen aufgebaut:

- In der ersten Spalte ist der Name der Transaktionsdaten angegeben.
- In der zweiten Spalte ist die Feldnummer der ISO-8583-Autorisierungsnachricht angegeben, sofern die Daten in der Autorisierung übertragen werden.
- Die dritte Spalte gibt an, ob die Transaktionsdaten in der Autorisierung übertragen werden.
- Die vierte Spalte gibt an, ob die Transaktionsdaten im Clearing übertragen werden.
- Die fünfte Spalte gibt an, ob es Vorgaben zur Protokollierung der Daten gibt.
- Die sechste Spalte enthält Bemerkungen zu diesen Daten.
- Die siebte Spalte enthält die Einordnung der Datenelemente in die Schutzbedarfsklassen "V-Mittel“, "V-Hoch“ oder "I-Mittel“.

Datenelement einer Transaktion	Feld-nummer	Übertragung bei der Autorisierung	Übertragung beim Clearing	Speicherung zur Protokollierung	Bemerkung	Schutzbe-darfsklasse
Kundenkontoverbindung (Kombination aus Kundenkontonummer und BLZ/Kurz-BLZ)					Bei einer Kombination aus 1. Kundenkontonummer und 2. BLZ oder Kurz-BLZ unterliegen diese beiden Datenelemente in ihrer Gesamtheit der Einstufung in die Schutzbedarfsklasse V-Mittel.	V-Mittel
Kundenkontonummer						V-Mittel
PAN	BMP 2	electronic cash, GA-Aktiv, Passiv, GK	electronic cash, GA-Aktiv, Passiv	electronic cash, GA-Aktiv	Primary Account Number (Spur 2-PAN)	V-Mittel
PVV	BMP 35	electronic cash, GA-Aktiv, Passiv			Ein PIN Verification Value (PVV) kann in den Spur 2-Daten enthalten sein.	V-Mittel
CVC bzw. CVV	BMP 35	electronic cash, GA-Aktiv			Ein CVC bzw. CVV kann in den Spur 2-Daten enthalten sein.	V-Mittel
Spur 2-Daten	BMP 35	electronic cash, GA-Aktiv, Passiv				V-Mittel
PIN						V-Hoch
Verschlüsselter PIN-	BMP 52	electronic cash,			Der verschlüsselte PIN-Block ist	V-Mittel

Datenelement einer Transaktion	Feld-nummer	Übertragung bei der Autorisierung	Übertragung beim Clearing	Speicherung zur Protokollierung	Bemerkung	Schutzbe-darfsklasse
Block (PAC)		GA-Aktiv, Passiv			vorhanden bei Online-PIN-Prüfung. Der PAC ist die Triple-DES-Verschlüsselung der im 8 Byte langen ISO 1 PIN-Block Format dargestellten PIN.	
PAC-Schlüssel					Der Schutzbedarf gilt sowohl für einen Masterkey als auch für davon abgeleitete Sessionkeys.	V-Hoch
Schlüssel zur Absicherung von OPT						V-Hoch
Schlüssel zur MAC-Berechnung						V-Hoch

3 Sicherheitskriterien

Alle nachfolgenden Sicherheitsanforderungen stehen unter dem Vorbehalt eventueller rechtlicher Rahmenbedingungen. Einzelne Anforderungen, die bestimmte Formen der Umsetzung beinhalten, können auch durch alternative Implementierungen erfüllt werden, wenn hierdurch die intendierten Schutzziele ohne Abstriche erreicht werden. Sollten einzelne Sicherheitsanforderungen im Widerspruch zu rechtlichen oder behördlichen Bestimmungen stehen, so sind diese Anforderungen auf eine Weise umzusetzen, dass ihre Umsetzung der ursprünglichen Intention so gut wie im rechtlichen Rahmen möglich entspricht.

Falls eine Anforderung nicht erfüllt werden kann, besteht generell die Möglichkeit, diese durch eine sogenannte kompensierende Maßnahme zu ersetzen. Dafür sind die folgenden Voraussetzungen zu berücksichtigen:

1. Es MUSS ein nachvollziehbarer Grund vorliegen, der die Umsetzung einer Sicherheitsanforderung maßgeblich beeinträchtigt.
2. Die kompensierende Maßnahme MUSS dem Ziel der ursprünglichen Anforderung entsprechen.
3. Es MUSS eine Risikoanalyse für das betreffende Risiko erstellt werden. Eine kompensierende Maßnahme MUSS geeignet sein, das zugrundeliegende Risiko angemessen zu mindern.
4. Die kompensierende Maßnahme MUSS erneut überprüft werden, wenn sich der ZKA-Datensicherheitsstandard ändert.

3.1 Sicherheitsgrundsätze

3.1.1 Es MUSS ein Dokument mit Sicherheitsgrundsätzen erstellt, veröffentlicht und gepflegt werden, mit folgendem Inhalt:

- Abdeckung aller in diesem Dokument enthaltenen Anforderungen,
- Festlegung der Verantwortlichkeiten von Mitarbeitern und Verpflichtungen von Vertragspartnern für die in den Sicherheitsgrundsätzen genannten Sicherheitsaspekte,
- Beschreibung eines Prozesses zur Identifizierung von Bedrohungen und Schwachstellen sowie zur Durchführung formaler Risikoanalysen auf periodischer Basis,
- Eine Regelung zur periodischen Überprüfung der Sicherheitsgrundsätze, der hieraus abgeleiteten Dokumente sowie deren Anpassungen an geänderte Rahmenbedingungen.
- Eine Regelung zur Kommunizierung aller Anforderungen an die beteiligten Personen.

3.1.2 Im Falle einer vorliegenden ISO-27001-Zertifizierung gelten die Anforderungen aus 3.1.1 als erfüllt.

3.2 Sicherheitsorganisation

3.2.1 Interne Organisation

3.2.1.1 Es MÜSSEN Verfahren zur Umsetzung aller in diesem Dokument enthaltenen Sicherheitsanforderungen im täglichen Betrieb entwickelt und dokumentiert werden.

3.2.1.2 Für alle Mitarbeiter sind Vorgaben für die korrekte Nutzung der zur Verfügung gestellten Technik zu definieren. Es MUSS sichergestellt werden, dass Vorgaben zu folgenden Themen enthalten sind:

1. Es MUSS dokumentiert werden, welche wesentlichen Komponenten zur Verarbeitung schutzwürdiger Daten eingesetzt werden. . (Beispiele: Kryptohardware, Autorisierungssysteme, Kartenmanagementsysteme etc.. Nicht gemeint sind Netzwerkkomponenten zur Übertragung verschlüsselter Daten.)

2. Die Nutzung solcher Komponenten DARF NICHT ohne Genehmigung erfolgen.

3. Es MUSS dokumentiert werden, wer auf die unter 1. genannten Komponenten Zugriff hat.

4. Eine Liste der für den Betrieb der wesentlichen Komponenten verantwortlichen Personen MUSS gepflegt werden.

5. Erlaubte Nutzungsarten der wesentlichen Komponenten MÜSSEN dokumentiert werden.

6. Remote-Zugriffe auf wesentliche Komponenten (z. B. im Rahmen der Fernwartung) müssen entsprechend dem Stand der Technik abgesichert sein.

7. Wenn über Remote Access-Verbindungen auf zu schützende Datenelemente zugegriffen werden kann, MUSS das Kopieren oder Verschieben der Daten auf lokale oder mobile Datenträger verboten werden. (Beispiel: Maßnahmen zu Data Leakage Protection)

8. Für alle Festlegungen und Genehmigungen MUSS die Zustimmung des Informationseigentümers vorliegen.

3.2.1.3 Für alle Mitarbeiter und Vertragspartner mit Zugriff auf wesentliche Komponenten MÜSSEN verbindliche Regelungen für die korrekte Nutzung zur Verfügung gestellter Dienste, z. B. Internet und E-Mail, formuliert werden. Es MUSS sichergestellt werden, dass Vorgaben zu folgenden Themen enthalten sind:

1. Die erlaubten Nutzungsarten der Dienste sowie die Rechte und Pflichten im Umgang mit den Diensten.

2. Alle Genehmigungen zur Nutzung von Diensten erfordern die Zustimmung einer fachlich verantwortlichen Person.

3.2.1.4 Folgende Verantwortlichkeiten MÜSSEN an einzelne Personen oder an Gruppen von Personen delegiert werden:

1. Erarbeitung, Dokumentation und Bekanntmachung von Sicherheitspolitik und Sicherheitsprozeduren.

2. Überwachung und Analyse von Sicherheitswarnungen und -informationen sowie deren Weiterleitung an die verantwortlichen Personen.

3. Erarbeitung, Dokumentation und Bekanntmachung von Prozeduren zur Reaktion auf Sicherheitsvorfälle und von Eskalationsprozessen zur Sicherstellung einer kurzfristigen und effektiven Handhabung von sicherheitskritischen Situationen.

4. Verwaltung von Benutzerkennungen und Berechtigungen, einschließlich Anlage, Änderung und Löschung.

5. Kontrolle der unter 1. – 4. genannten Verantwortlichkeiten.

3.2.1.5 Auf Sicherheitsvorfälle MUSS unverzüglich in geeigneter Weise reagiert werden können. Mit dieser Zielsetzung MUSS ein Prozess zur Reaktion auf Sicherheitsvorfälle eingerichtet sein, der folgendes berücksichtigt:

1. Es MUSS sichergestellt werden, dass der Prozess spezifische Schritte für einzelne Vorfälle, für die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit, Backup-Regelungen für Daten, Aufgaben, Rollen und Verantwortlichkeiten sowie Regelungen zur Kommunikation und Eskalation beinhaltet.

2. Der Prozess zur Reaktion auf Sicherheitsvorfälle MUSS mindestens jährlich getestet werden.

3. Es MÜSSEN Personen benannt werden, die täglich rund um die Uhr (24/7) für die Reaktion auf Sicherheitsvorfälle und –alarme erreichbar sind.

4. Für die mit diesen Aufgaben betrauten Mitarbeiter MUSS eine geeignete Aus- und Weiterbildung sichergestellt sein.

5. Der Prozess zur Reaktion auf Sicherheitsvorfälle MUSS regelmäßig überprüft und aktualisiert werden. Dabei MÜSSEN Erfahrungen aus der Vergangenheit ("Lessons Learned“) und neue Entwicklungen in der Industrie einbezogen werden. Das Verfahren zur Aktualisierung des Prozesses MUSS dokumentiert werden.

6. Ergebnisse der installierten Warnsysteme MÜSSEN in diese Betrachtung einbezogen werden.

3.2.2 Externe Parteien

3.2.2.1 Es MUSS dokumentiert werden,- wer Zugang zu Bereichen hat, in denen wesentliche Komponenten betrieben werden, oder die mit der Verarbeitung schützenswerter Daten beauftragt sind, geführt und aktuell gehalten werden.

3.2.2.2 Der Umgang mit zu schützenden Datenelementen durch externe Dienstleister MUSS in folgenden Punkten bei Neuverträgen oder Vertragsanpassungen geregelt werden:

1. Die Erfüllung des ZKA Datensicherheitsstandards

2. Treuhänderische Wahrnehmung der Verantwortung für die Sicherheit der zu schützenden Datenelemente aller Mandanten, die durch den Dienstleister verarbeitet oder gespeichert werden. Dies schließt angemessene Maßnahmen zur Mandantentrennung mit ein.

3.2.2.3 Für die Auswahl externer Dienstleister SOLL ein Prozess eingerichtet werden, der die Vertrauenswürdigkeit des Vertragspartners bewertet.

3.2.2.4 Die Verlässlichkeit externer Vertragspartner MUSS überprüft werden, beispielsweise anhand der Vorlage von Erklärungen zum Datenschutz und zur Einhaltung des Bankgeheimnisses sowie durch eine Prüfung des Dienstleistungs- oder Werkvertrages.

3.3 Umgang mit zu schützenden Datenelementen

3.3.1 Für Datenelemente der Schutzbedarfskategorie "V-Hoch“ gelten, soweit anwendbar, die Sicherheitsanforderungen der Regelwerke [EC_TA7] und [GA 2007_REV] sowie der ZKA-PIN-Vereinbarung [ZKA_PIN].

3.3.2 Die Berechtigungen für den Zugriff auf die wesentlichen Komponenten und die zu schützenden Datenelemente MÜSSEN auf die Personen beschränkt sein, welche diese zum Erledigen ihrer Arbeit benötigen.

1. Die Vergabe von Zugriffsrechten erfolgt auf Basis der jeweiligen Stellenbeschreibung und Funktion eines Mitarbeiters.

2. Für die Vergabe von Zugriffsrechten MUSS ein Prozess eingerichtet sein, der die Zustimmung des Informationseigentümers für die Vergabe beinhaltet.

3.3.3 Es MUSS ein Zugriffskontrollsystem eingerichtet werden, welches die Zugriffmöglichkeiten der Anwender auf die wesentlichen Komponenten reduziert, die zum Ausführen ihrer Aufgaben benötigt werden.

3.3.4 Für zu schützende Datenelemente gelten die folgenden Regeln:

Schutzbedarfsklasse	**Autorisierung**	**Clearing/ Settlement/ Reklamations verarbeitung**	**Protokollierung**
V-Hoch	Daten DÜRFEN außerhalb von sicheren Umgebungen (vgl. 3.5) NICHT im Klartext gespeichert, verarbeitet oder übertragen werden.	Daten DÜRFEN NICHT im Klartext gespeichert, angezeigt oder übertragen werden. Kryptographische Schlüssel DÜRFEN NICHT im Klartext außerhalb von sicheren Umgebungen (vgl. 3.5) verarbeitet, gespeichert oder übertragen werden. Es gelten die Anforderungen aus [ZKA_PIN], 2.3	
V-Mittel	Die Speicherung und Verarbeitung von Daten einschließlich ihrer Anzeige auf Bildschirmen und Hardcopies MUSS hinsichtlich ihrer Dauer, ihres Umfangs und der vergebenen Zugriffsrechte auf das für die geschäftlichen Abläufe und zur Erfüllung gesetzlicher oder regulatorischer Anforderungen erforderliche Maß beschränkt werden. Dies MUSS in spezifischen Regelungen zur Datenhaltung und zu Aufbewahrungsfristen dokumentiert werden. Daten DÜRFEN in offenen Netzen NICHT unverschlüsselt übertragen werden.		

Schutzbedarfsklasse	Autorisierung	Clearing/ Settlement/ Reklamationsverarbeitung	Protokollierung
I-Mittel	Daten aus Kartentransaktionen MÜSSEN bei Ihrer Übertragung zwischen Karte, Terminal oder Geldautomat und Autorisierungszentrale durch Mechanismen zur Erkennung von Integritätsverletzungen abgesichert werden, z. B. durch Berechnung und Prüfung eines Message Authentication Codes (MAC).		
	Das Einbringen von Software bzw. Firmware in Geräte, die Datenelemente der Sicherheitsklasse "V-Hoch" verarbeiten und selbst nicht innerhalb einer gesicherten Umgebung betrieben werden, MUSS durch Mechanismen zur Erkennung von Integritätsverletzungen abgesichert werden.		

3.4 Personelle Sicherheit

3.4.1 Mitarbeiter, die im Rahmen von Verarbeitungsprozessen in großem Umfang Zugriff auf zu schützende Datenelemente erhalten sollen, SOLLEN ein polizeiliches Führungszeugnis oder einen gleichwertigen Nachweis vorlegen.

3.4.2 Durch geeignete Maßnahmen MÜSSEN alle Mitarbeiter periodisch über die Bedeutung der Sicherheit im Allgemeinen und von zu schützenden Datenelementen unterrichtet werden.

3.4.3 Mitarbeiter MÜSSEN schriftlich die Kenntnis und das Verständnis der Sicherheitspolitik und der Sicherheitsprozesse des Unternehmens bestätigen.

3.5 Sichere Umgebungen

In einer sicheren Umgebung KÖNNEN zu schützende Datenelemente und kryptographische Schlüssel im Klartext bearbeitet werden. Die wichtigste Eigenschaft einer sicheren Umgebung ist, dass geeignete Maßnahmen existieren, um den unbefugten Zugriff auf schützenswerte Daten zu verhindern.

3.5.1 Zutrittskontrolle

3.5.1.1 Der Zutritt zu sicheren Umgebungen wie Rechenzentren, in denen zu schützende Datenelemente verarbeitet, gespeichert oder übertragen werden oder die den Zugriff auf zu schützende Datenelemente ermöglichen, MUSS kontrolliert werden:

1. Die Zutrittskontrolle MUSS mittels geeigneter technischer Einrichtungen erfolgen.

2. Der Zugang zu sicheren Umgebungen MUSS mit Kameras oder gleichwertigen Mechanismen überwacht werden. Die Daten MÜSSEN für einen Zeitraum von mindestens drei Monaten gespeichert werden.

3. Der Zugang zu Netzwerkanschlüssen in sicheren Umgebungen MUSS kontrolliert werden.

3.5.1.2 Es SOLLEN Verfahrensweisen eingerichtet werden, die eine leichte Unterscheidbarkeit zwischen Mitarbeitern und zu begleitenden Personen ermöglichen.

3.5.1.3 Alle zu begleitenden Personen MÜSSEN wie folgt behandelt werden:

1. Sichere Umgebungen DÜRFEN ohne Genehmigung NICHT betreten werden.

2. Zu begleitende Personen MÜSSEN ein sichtbares Merkmal (Anhänger mit Ausweis oder Zugangsgerät) mit zeitlich begrenzter Gültigkeit tragen.

3. Zu begleitende Personen MÜSSEN ihren Ausweis oder ihr Zugangsgerät mit Ablauf der Gültigkeit oder bei Verlassen des Geländes bzw. des Gebäudes abgeben.

3.5.1.4 Es MUSS ein Besuchertagebuch geführt werden, mit dem alle Besuche nachvollziehbar gemacht werden. Die Aufzeichnungen MÜSSEN für einen Zeitraum von mindestens drei Monaten gespeichert werden.

3.5.2 Kryptographische Funktionen und Komponenten

3.5.2.1 Die Daten aus jedem administrativen Zugriff, der nicht von einer Operating-Konsole aus erfolgt, MÜSSEN verschlüsselt übertragen werden, insbesondere wenn die Administration web-basiert durchgeführt wird.

3.5.2.2 Für die Verschlüsselung zu schützender Datenelemente bei der Übertragung über öffentliche Netze MÜSSEN angemessen starke Kryptoalgorithmen und Sicherheitsprotokolle verwendet werden.

Als öffentliche Netze in diesem Zusammenhang gelten z. B. das Internet, WiFi-Netze nach IEEE 802.11x sowie Mobilfunknetze (GSM und UMTS).

3.5.2.3 In Funknetzen MÜSSEN zu schützende Datenelemente mittels starker Verschlüsselung gesichert werden.

3.5.2.4 Falls Mechanismen für die Verschlüsselung von zu schützenden Datenelementen der Schutzbedarfsklasse "V-Hoch" eingesetzt werden, MUSS die für den Zugriff auf die Daten erforderliche Entschlüsslung unabhängig von der Zugriffskontrolle auf Betriebsystemebene verwaltet werden. Die Sicherheit und Verwendung kryptographischer Schlüssel DARF NICHT von der Sicherheit der Benutzerverwaltung auf Betriebssystemebene abhängen.

3.5.2.5 Zugriffe DÜRFEN NICHT alleine auf der Basis der Identifizierung von MAC-Adressen gewährt werden. Als ergänzende Sicherheitsmaßnahme KANN dies jedoch in Betracht gezogen werden.

3.5.2.6 Passwörter für den Zugriff auf Systeme in der sicheren Umgebung MÜSSEN während ihrer Übertragung und während ihrer Speicherung in Systemkomponenten verschlüsselt werden.

3.5.3 Schlüsselverwaltung

3.5.3.1 Kryptographische Schlüssel, die zur Verschlüsselung von zu schützenden Datenelementen verwendet werden, MÜSSEN gegen Offenlegung und jede missbräuchliche Nutzung geschützt werden:

1. Es SOLLEN nur so viele Schlüsseladministratoren Zugriff auf einzelne Schlüssel erhalten, wie unbedingt zu deren Verwaltung benötigt werden.

2. Schlüssel MÜSSEN an so wenigen verschiedenen Stellen und in so wenigen unterschiedlichen Formaten wie möglich sicher hinterlegt werden.

3.5.3.2 Die Prozesse zur Schlüsselverwaltung und die Verfahren zur Verwendung von Schlüsseln für die Verschlüsselung von zu schützenden Datenelementen MÜSSEN vollständig und ausführlich dokumentiert werden. Dies schließt folgende Aspekte ein:

1. Die Erzeugung kryptographisch starker Schlüssel,
2. Sichere Verteilung von Schlüsseln,
3. Sichere Speicherung von Schlüsseln,
4. Periodische Schlüsselwechsel, vorzugsweise automatisiert, in je nach Anwendung angemessenen zeitlichen Abständen,Löschung alter oder ungültiger Schlüssel, so dass diese nicht durch einen Angreifer rekonstruierbar sind,
5. Aufteilung der Kenntnis von Schlüsselteilen auf mindestens zwei Personen (Vier-Augen-Prinzip), die zur Bildung eines Schlüssels zusammenwirken müssen,
6. Verhinderung der unautorisierten Ersetzung von Schlüsseln,
7. Ersetzung von kompromittierten sowie als kompromittiert verdächtigten Schlüsseln,
8. Die Protokollierung der Vorgänge zur Schlüsselverwaltung.

3.5.4 Der Betrieb von Hardware-Sicherheitsmodulen

Als Hardware-Sicherheitsmodul (HSM) wird ein internes oder externes Peripheriegerät für die sichere Ausführung kryptographischer Operationen bezeichnet. Ein HSM ist mit Sicherheitsmechanismen ausgestattet, die vor unberechtigtem Zugriff auf Daten und insbesondere auf kryptographische Schlüssel schützen, die in dem HSM verarbeitet oder gespeichert sind. Die nachfolgenden Anforderungen beziehen sich auf HSMs, die in Rechenzentralen betrieben werden. PIN-Entry-Devices (PEDs) oder Encrypting PIN Pads (EPPs), die in POS-Terminals oder Geldautomaten betrieben werden, sind nicht Gegenstand der nachfolgenden Anforderungen. Sicherheitsanforderungen an solche Geräte sind in [EC_TA7], [GA 2007_REV] und [ZKA_PIN] festgelegt.

3.5.4.1 HSMs MÜSSEN in einer sicheren Umgebung betrieben werden.

3.5.4.2 HSMs SOLLEN am Aufstellungsort befestigt werden.

3.5.4.3 Alle Geräte zur Einbringung von Schlüsselkomponenten MÜSSEN sicher vor unberechtigter Nutzung aufbewahrt werden.

3.5.4.4 Am initialen Einbringen von Schlüsseln MÜSSEN mindestens zwei Personen beteiligt sein. Ggf. vorhandene Transportschlüsselhälften MÜSSEN in getrennten Tresoren gelagert werden.

3.5.4.5 Eine dedizierte über das Netzwerk angeschlossene angeschlossenes HSM MUSS in einem eigenen Netzsegment betrieben werden.

3.5.4.6 In einem HSM gespeicherte Schlüssel MÜSSEN gelöscht werden, wenn das HSM die sichere Umgebung verlässt (z. B. zur Wartung).

3.5.4.7 Eventuell vorhandene Sensoren des HSM SOLLEN aktiviert sein.

3.5.4.8 Der Zugriff auf Keymanagement-Funktionen MUSS auf die Sicherheitsbeauftragten des HSM beschränkt sein.

3.5.4.9 Erlaubt das HSM eine Administration über externe Netze, dann DARF die Nutzung dieser Schnittstelle zur Administration NICHT möglich sein, wenn sie nicht von Sicherheitsexperten geprüft wurde.

3.5.4.10 Die Software eines HSM SOLL aktuell sein.

3.5.4.11 Das nicht autorisierte Einspielen von Software in ein HSM MUSS verhindert werden.

3.5.4.12 Alle im Handbuch eines HSMs aufgeführten Sicherheitsmaßnahmen SOLLEN beachtet werden.

3.5.4.13 Nicht benötigte deaktivierbare Funktionsvarianten eines HSM MÜSSEN deaktiviert sein. Dies MUSS dokumentiert sein.

3.5.4.14 Kryptographische Schlüssel SOLLEN NICHT für API-Aufrufe verwendet werden, die für diese kryptographischen Schlüssel nicht explizit erlaubt sind. Dies wird beispielsweise dadurch erreicht, dass die Schlüssel kryptographisch mit den erlaubten API-Aufrufen verbunden werden.

3.5.4.15 Wird die API zur Übertragung von einem PIN-Block-Format in ein anderes PIN-Block-Format verwendet, dann SOLLEN Sitzungsschlüssel für die Entschlüsselung des Eingang-PIN-Blocks und Sitzungsschlüssel zur Verschlüsselung des Ausgang-PIN-Blocks verwendet werden.

3.5.4.16 Falls für die Verschlüsselung bzw. Umschlüsselung von PIN-Blöcken die Verwendung von Sitzungsschlüsseln nicht mit systemtechnischen Mitteln erzwungen wird, gelten folgende Regeln:

1. Die Übertragung von standardisierten PIN-Block-Formaten in nicht standardisierte PIN-Block-Formate DARF NICHT möglich sein.

2. PIN-Block-Formate, die die PAN (Kontonummer) beinhalten, SOLLEN NICHT in Formate übertragen werden, die die PAN nicht bein-

halten. Insbesondere SOLLEN ISO Format 0 und ISO Format 3 NICHT in ISO Format 1 übertragen werden.

3. Wenn ein PIN-Block-Format mit PAN in ein anders PIN-Block-Format mit PAN übertragen werden soll, dann DARF es NICHT möglich sein, hierbei die PAN zu modifizieren.

4. Die vorherigen drei Spiegelpunkte werden durch die folgende Tabelle nach [ISO 9564-1] verdeutlicht:

Umschlüsselung nach / von	**ISO Format 0**	**ISO Format 1**	**ISO Format 3**
ISO Format 0	Änderung der PAN nicht erlaubt	Nicht erlaubt	Änderung der PAN nicht erlaubt
ISO Format 1	PAN Eingabe vorgesehen	Erlaubt	PAN Eingabe vorgesehen
ISO Format 3	Änderung der PAN nicht erlaubt	Nicht erlaubt	Änderung der PAN nicht erlaubt

5. Andere Formate als ISO Format 0 und ISO Format 3 DÜRFEN NICHT für die Berechnung von Werten, die aus einer PIN und einer PAN abgeleitet werden, wie z. B. PIN Offsets und PIN Verifikationswerte (PVV), unterstützt werden.

6. Werden Werte aus einer PIN und einer PAN abgeleitet, und der Teil der Kontonummer, der im verschlüsselten PIN-Block enthalten ist, stimmt nicht mit dem Teil der eingegeben PAN überein, so DARF der berechnete Werte NICHT zurückgegeben werden.

3.5.4.17 ISO Format 2 SOLL durch HSMs nicht unterstützt werden.

3.5.4.18 Wird die API zur Übertragung von einem PIN-Block-Format in ein anderes PIN-Block-Format verwendet und wird zur Ableitung von Sitzungsschlüsseln für die Verschlüsselung des Ausgang-PIN-Blocks eine Zufallszahl benötigt, dann DARF es NICHT möglich sein, diese Zufallszahl von außen vorzugeben. Die Zufallszahl MUSS von dem HSM intern erzeugt werden.

3.5.4.19 Die Administration von HSMs MUSS folgende Regeln beachten:

1. Der für ein HSMs Verantwortliche MUSS dokumentieren, welche Funktionen aktiviert sind.

2. Der für ein HSM Verantwortliche MUSS dokumentieren, welche API-Aufrufe tatsächlich benötigt werden. Dazu liegen Netz- oder Betriebskonzepte vor. Auch die Spezifikationen der Anwendung, die das HSM anspricht, also die API nutzt, ist hierzu heran zu ziehen.Die verbliebenen API-Aufrufe MÜSSEN anhand der vorgenannten Sicherheitsregeln geprüft werden.

3.5.4.20 Für ein HSM MUSS ein Sicherheitsgutachten nach einem anerkannten Standard vorliegen.

3.6 Kommunikations- und Betriebsverwaltung

3.6.1 Systemplanung und -abnahme

3.6.1.1 Systeme und Geräte MÜSSEN so konfiguriert werden, dass Missbrauch verhindert wird. Für alle Systemkomponenten MÜSSEN Konfigurationsstandards vorliegen. Die Konfigurationsstandards SOLLEN alle bekannten Sicherheitsschwachstellen berücksichtigen und am Stand der Technik im Hinblick auf die Härtung von IT-Systemen und –Komponenten ausgerichtet sein.

3.6.1.2 Die Aufgabenbereiche von Entwicklung und Betrieb MÜSSEN organisatorisch und physikalisch oder logisch voneinander getrennt sein. Tests MÜSSEN unabhängig vom Betrieb erfolgen.

3.6.1.3 Produktionsdaten DÜRFEN NICHT für Tests verwendet werden. Anonymisierte Produktionsdaten gelten nicht als Produktionsdaten.

3.6.1.4 Zur Inbetriebnahme eines Systems, einer Systemkomponente oder eines Programms MÜSSEN alle nicht für die Produktion benötigten Daten, z. B. Testdaten, gelöscht werden.

3.6.1.5 Wichtige Serverfunktionen wie Web-Server, Datenbank-Server oder DNS-Server SOLLTEN auf jeweils eigenen Maschinen (physikalisch/virtuell) laufen.

3.6.1.6 Die Nutzung überflüssiger Funktionen, Dienste oder Protokolle wie Skripte, Treiber, Subsysteme, Dateisysteme, Web-Dienste oder sonstiger nicht benötigter Eigenschaften SOLL verhindert werden. Die Nutzung nicht benötigter sicherheitskritischer Funktionen MUSS wirksam verhindert werden.

3.6.1.7 Bei der Installation von Systemkomponenten im Netzwerk MÜSSEN durch den Hersteller vorgewählte Parameter wie Passwörter oder sicher-

heitsrelevante Voreinstellungen verändert bzw. geprüft und auf sichere Werte gesetzt werden. Nicht benötigte Benutzerkennungen MÜSSEN gelöscht werden.

3.6.2 Schutz gegen Schadsoftware

3.6.2.1 Auf allen Systemen, die üblicherweise durch Computerviren oder durch die bekannten Arten von Schadsoftware bedroht sind, MÜSSEN geeignete Schutzmaßnahmen umgesetzt sein.

3.6.2.2 Es MUSS sichergestellt werden, dass die Schutzmaßnahmen den aktuellen Bedrohungen entsprechen.

3.6.2.3 Der Schutz vor Schadsoftware MUSS in die Incident Response-Prozesse integriert sein.

3.6.3 Sicherheitsmanagement für Netzwerke

3.6.3.1 Es MÜSSEN Sicherheitsanforderungen an Firewalls für jede Verbindung zum Internet sowie zwischen demilitarisierten Zonen (DMZ) und dem internen Netzwerk formuliert und umgesetzt werden.

3.6.3.2 Für die Administration von Netzwerken und Netzwerkkomponenten MÜSSEN Rollen und Verantwortlichkeiten definiert werden.

3.6.3.3 Es MUSS ein formaler Prozess für Ersteinsatz und Änderungen aller externen Netzwerkverbindungen sowie für alle Änderungen an Konfigurationen von Firewalls eingerichtet und aufrecht erhalten werden.

3.6.3.4 Es MUSS eine Dokumentation der relevanten Netzwerkbereiche mit allen Verbindungen zu Systemkomponenten, die zu schützende Datenelemente verarbeiten, gepflegt und auf dem jeweils aktuellen Stand gehalten werden.

3.6.3.5 Werden verwendete Protokolle als riskant eingeschätzt, MÜSSEN Sicherheitsmaßnahmen zu ihrer Absicherung ergriffen werden.

3.6.3.6 Die Standardkonfigurationen für aktive Netzwerkkomponenten MÜSSEN dokumentiert werden.

3.6.3.7 Alle Firewall- und Router-Regelungen und -Konfigurationen MÜSSEN periodisch überprüft werden.

3.6.4 Datenträgerverwaltung

3.6.4.1 Alle beleghaften und elektronischen Datenträger, die zu schützende Datenelemente beinhalten, MÜSSEN angemessen vor unerlaubten Zugriffen gesichert werden.

3.6.4.2 Die Versendung von Datenträgern MUSS über einen nachverfolgbaren Sendungsweg erfolgen.

3.6.4.3 Alle Backups von Datenträgern MÜSSEN in sicheren Umgebungen vorgehalten werden.

3.6.4.4 Datenträger und Daten, die nicht länger aus geschäftlichen oder gesetzlichen Gründen benötigt werden, MÜSSEN auf geeignete Weise der Nutzung entzogen bzw. entsorgt werden.

3.6.5 Betriebsüberwachung

3.6.5.1 Es MUSS ein Prozess implementiert werden, durch den alle Zugriffe auf Systemkomponenten, insbesondere Zugriffe mit Administrator-Rechten, den jeweiligen Benutzern zugeschrieben werden können.

3.6.5.2 Es MÜSSEN Verfahren etabliert sein, die geeignet sind, Indikatoren für missbräuchliche Zugriffe auf zu schützende Datenelemente zu liefern. Zur Missbrauchserkennung SOLLEN diese Verfahren regelmäßig angewendet werden.

3.6.5.3 Anhand der Auswertung von Protokolldaten SOLLEN Art und Umfang eines möglichen Schadens nachvollziehbar sein.

3.6.5.4 Alle Uhren kritischer Systeme MÜSSEN synchronisiert werden.

3.6.5.5 Protokolldaten MÜSSEN durch geeignete Mechanismen vor Manipulationen geschützt werden.

3.6.5.6 Protokolldaten MÜSSEN für einen Zeitraum vorgehalten werden, der für die in 3.6.5.2 genannten Verfahren gut geeignet ist.

3.7 Zugriffskontrolle

3.7.1 Zugriffskontrolle für Netzwerke

3.7.1.1 Jeder Netzwerkzugriff aus externen Netzwerken[1] auf Systeme, die zu schützende Datenelemente verarbeiten oder speichern, MUSS durch geeignete technische Maßnahmen kontrolliert werden.

3.7.1.2 Es MUSS eine Regelung für das Anschließen von Hardware-Komponenten an das Unternehmensnetzwerk existieren.

3.7.1.3 Für den Fernzugriff (Remote Access) auf das Netzwerk durch Anwender und Administratoren MUSS ein zweistufiges Authentikationsverfahren (Nachweis von Besitz und Wissen) verwendet werden.

3.7.1.4 Firewall-Konfigurationen MÜSSEN so beschaffen sein, dass jeder nicht ausdrücklich erlaubte Datenverkehr verhindert wird.

3.7.1.5 Eine Datenhaltung DARF NICHT in Netzsegmenten erfolgen, die aus öffentlichen Netzen erreichbar sind. Dies schließt insbesondere auch die Datenhaltung innerhalb einer DMZ aus.

3.7.2 Zugriffskontrolle für Betriebssysteme und Anwendungen

3.7.2.1 Alle Benutzer MÜSSEN vor der Gewährung von Zugriffsberechtigungen mittels einer individuellen Benutzerkennung identifiziert werden.

3.7.2.2 Zusätzlich zu der individuellen Benutzerkennung MUSS eine angemessene Methode zur Benutzerauthentikation angewendet werden.

3.7.2.3 Für alle Anwender und Administratoren MUSS ein geeignetes Management von Benutzer- und Rechteverwaltung erfolgen, mit folgenden Merkmalen:

1. Das Anlegen, Löschen oder Ändern von Benutzer-IDs und damit zusammenhängenden Datenobjekten zum Nachweis von Benutzeridentität und -rechten ("Credentials“) MUSS anhand eines etablierten Prozesses erfolgen.

2. Nicht mehr benötigte Benutzerkennungen MÜSSEN nach einem angemessenen Zeitraum deaktiviert oder gelöscht werden.

[1] Als externe Netzwerke werden solche Netzwerke bezeichnet, die nicht durch eine kreditwirtschaftliche Rechenzentrale und Anwender dieses Standards betrieben werden und die auch nicht mittelbar deren Kontrolle unterliegen, z.B. über Verträge mit den Betreibern der Netzwerke.

3. Für jede verwendete Methode der Benutzerauthentikation MUSS eine Regelung existieren, die alle sicherheitsrelevanten Aspekte beinhaltet.

4. Die Zahl von Wiederholungen nicht erfolgreicher Zugriffsversuche MUSS begrenzt werden. Auf die Überschreitung der zulässigen Fehlversuche ist in angemessener Weise zu reagieren.

5. Es MUSS eine Regelung existieren, die sicherstellt, dass eine aktive Benutzersitzung nach einer angemessenen Zeit ohne Benutzeraktion gesperrt wird.

3.7.3 Mobile Endgeräte und Fernzugriffe

3.7.3.1 Es MUSS eine Regelung für den Einsatz mobiler Endgeräte existieren. Insbesondere MUSS auf allen mobilen Endgeräten, von denen aus Anwender auf zu schützende Datenelemente der Schutzbedarfsklasse "V-Hoch" im Unternehmensnetzwerk zugreifen können und die selbst mit dem Internet verbunden sind, eine geeignete Schutzsoftware installiert sein.

3.7.3.2 Die Datenübertragung von zu schützenden Datenelementen der Schutzbedarfsklasse "V-Mittel" zwischen mobilen Endgeräten und dem Unternehmensnetzwerk über öffentlich Netzwerke MUSS mit geeigneten Sicherheitsmaßnahmen geschützt werden.

3.7.3.3 Für die Datenspeicherung von zu schützenden Datenelementen der Schutzbedarfsklasse "V-Hoch" auf mobilen Endgeräten MÜSSEN Sicherheitsmaßnahmen existieren, die lokale Kopien der Datenelemente dauerhaft schützen.

3.8 Beschaffung, Entwicklung und Wartung von IT-Systemen

3.8.1 Sicherheit in Entwicklungs- und Unterstützungsprozessen

3.8.1.1 Selbstentwickelte oder im Auftrag entwickelte Software MUSS über ihren gesamten Lebenszyklus hinweg auf der Basis von Richtlinien zur Entwicklung sicherer Software entwickelt und gepflegt werden.

3.8.1.2 Selbstentwickelte oder im Auftrag entwickelte Individualsoftware SOLL einer Qualitätssicherung unterzogen werden mit dem Ziel, eventuelle Schwachstellen bezüglich der Sicherheit zu identifizieren, bevor die Software in Betrieb genommen wird.

3.8.1.3 Alle Änderungen von Software- oder Systemkomponenten MÜSSEN nach festgelegten Regeln und Prozessen erfolgen. Insbesondere MUSS beachtet werden, dass

1. jede Änderung hinsichtlich ihrer Auswirkungen dokumentiert wird,

2. jede Änderung durch die fachlich verantwortliche Person genehmigt wird,

3. jede Änderung ausführlich in ihrer Funktionalität getestet wird,

4. zu jeder Änderung eine Rückfall- oder Ausweichmöglichkeit definiert wird.

3.8.1.4 Alle Web-Anwendungen MÜSSEN anhand von Richtlinien für die Erstellung von sicherer Software erstellt werden. Die Vermeidung von geläufigen Schwachstellen ist in die Entwicklungsrichtlinien aufzunehmen, insbesondere SOLLEN die OWASP Top Ten [OWASP] in der jeweils gültigen Fassung berücksichtigt werden.

3.8.1.5 Es MUSS sichergestellt werden, dass alle Web-Applikationen gegen bekannte Angriffe durch eine der folgenden Methoden geschützt sind:

1. Web-Applikationen werden anhand von periodischen Code Reviews durch eine auf Anwendungssicherheit spezialisierte Unternehmenseinheit oder externe Institution auf mögliche Schwachstellen und bekannte Angriffsmöglichkeiten untersucht.

2. Web-Applikationen werden durch jeweils eine Application-Layer-Firewall (ALF) geschützt.

3.8.2 Umgang mit technischen Schwachstellen

3.8.2.1 Es MUSS ein Prozess eingerichtet und gepflegt werden, der regelt, wie Informationen über neu entdeckte bzw. bekanntgewordene Schwachstellen bezogen werden und wie hierauf zu reagieren ist. (Beispielsweise KANN einer der im Internet angebotenen CERT-Dienste genutzt werden, die auch unentgeltlich angeboten werden).

3.8.2.2 Für alle System- und Software-Komponenten MUSS ein risikoorientierter Prozess für die Bewertung und das Einspielen von Patches vorhanden sein, durch den sichergestellt ist, dass die Installation von relevanten Sicherheits-Patches unverzüglich nach Veröffentlichung durch den Hersteller erfolgt.

3.8.2.3 Alle Sicherheits-Patches sowie alle Änderungen an der Software- oder Systemkonfiguration SOLLEN vor der produktiven Inbetriebnahme getestet werden.

3.8.2.4 Alle Sicherheitsregelungen und -einschränkungen sowie alle Netzwerkverbindungen MÜSSEN auf der Grundlage eines risikobasierten Ansatzes dahingehend überprüft werden, ob alle unautorisierten Zugriffsversuche abgewehrt werden können. Risikobewertungen MÜSSEN in periodischem Abstand sowie nach jeder signifikanten Veränderung der relevanten Infrastruktur oder Anwendungen erfolgen.

Um sicherzustellen, dass keine unautorisierten WLAN-Zugänge existieren, MUSS ein geeignetes Kontrollinstrument eingesetzt werden.

3.8.2.5 Interne und externe Schwachstellen-Scans MÜSSEN auf der Grundlage eines risikobasierten Ansatzes durchgeführt werden. Risikobewertungen MÜSSEN in periodischem Abstand sowie nach jeder signifikanten Veränderung der relevanten Infrastruktur oder Anwendungen (z. B. Neuinstallation oder Änderung von Systemkomponenten, Änderungen der Netzwerktopologie) erfolgen.

Schwachstellen-Scans MÜSSEN durch eine für diese Aufgabe bestimmte Unternehmenseinheit oder durch ein qualifiziertes Unternehmen durchgeführt werden.

3.8.2.6 Penetrationstests MÜSSEN auf der Grundlage eines risikobasierten Ansatzes durchgeführt werden. Risikobewertungen MÜSSEN in periodischem Abstand sowie nach jeder signifikanten Veränderung der relevanten Infrastruktur oder Anwendungen erfolgen..

3.8.2.7 Maßnahmen für das Bedrohungsmanagement MÜSSEN etabliert sein, um vermutete Gefährdungen zu erkennen und angemessen hierauf zu reagieren.

3.8.2.8 Es SOLLEN Systeme zur Dateiüberwachung eingesetzt werden, um die zuständigen Personen über unautorisierte Veränderungen an kritischen Systemkomponenten bzw. Dateiinhalten zu informieren. Kritische Dateiinhalte SOLLEN in periodischen Abstand mit dem Sollzustand verglichen werden.

4 Referenzen

[AIS 20] Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretation zum Schema (AIS), Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren AIS 20, Version 1, Bonn, 1999

[AIS 31] Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretation zum Schema (AIS), Funktionalitätsklassen und Evaluations-methodologiefür physikalische Zufallszahlengeneratoren, AIS 31, Version 1, Bonn, 2001

[BeOst] Omer Berkman, Odelia Moshe Ostrovsky, The unbearable lightness of PIN cracking, The Academic College of Tel Aviv Yaffo, School of Computer Science, Algorithmic Research Ltd., Tel Aviv University, School of Computer Science

[BON04] Understanding Security APIs, Doktorarbeit, University of Cambridge, Cambridge, Großbritannien, Januar 2004

[CC23] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[CC31] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007

[CLU03] The Design and Analysis of Cryptographic Application Programming Interfaces for Security Devices, Master Thesis, University of Natal, Durban, Südafrika, Januar 2003

[EC_TA7] Technischer Anhang zum Vertrag über die Zulassung als Netzbetreiber im electronic cash-System der deutschen Kreditwirtschaft

[EC_PIN] Sicherheitskriterien für PIN Berechnung und PIN-Prüfung bei Debit- und Kreditkarten, Version: 2.0, Anhang der ec-PIN-Vereinbarung der deutschen Kreditwirtschaft [ZKA-PIN], 2008

[FBZ_F] Schnittstellenspezifikation für die ZKA-Chipkarte

[GA 2007_REV] Regelwerk für das Deutsche Geldautomaten-System

[GK LZ] Schnittstellenspezifikation für die ZKA-Chipkarte

[ISO 13491-2] ISO 13491-2:2005, Banking -- Secure cryptographic devices (retail) -- Part 2: Security compliance checklists for devices used in financial transactions

[ISO 9564-1] Banking – Personal Identification Number (PIN) management and security, Part 1, Basic principles and requirements for online PIN handling in ATM and POS systems, Entwurf zur ISO 9564-1, 2007

[OPT] Schnittstellenspezifikation für die ec-Karte mit Chip

[OPTDAT] Schnittstellenspezifikation für die ec-Karte mit Chip

[OPTREG] Schnittstellenspezifikation für die ZKA-Chipkarte

[OPTVOR]	Schnittstellenspezifikation für die ZKA-Chipkarte
[OWASP]	The Open Web Application Security Project (OWASP), http://www.owasp.org
[PASAUT]	Passiv-Schnittstelle und chipspezifische Schritte bei der Autorisierung
[PCI DSS]	Payment Card Industry (PCI), Data Security Standard, Requirements and Security Assessment Procedures, Version 1.2, October 2008
[PIN]	Payment Card Industry PIN Security Requirements, MasterCard, VISA, 2004
[POA]	Aufladung von Prepaid-Mobilfunkkonten im deutschen Geldautomatensystem
[SU]	Ergebnisse aus Sicherheitsuntersuchungen von Sicherheitsboxen (HPCompaq Atalla, IBM, Atos Utimaco) für das Zahlungssystem electronic cash, streng vertraulich, Offenlegung nur für ZKA-Arbeitsstab "Sicherheitsfragen und -strategien" und Sicherheitsgutachter
[ZKA_PIN]	Vereinbarung über die Absicherung der PIN für von Instituten der deutschen Kreditwirtschaft herausgegebene Bankkarten und Sparkassenkarten, 2008