Programmakte

OSsecure

UVV-Kassen Sicherheitslösung

Inhaltsverzeichnis

IDENTITÄTSNACHWEIS

EINSATZLISTE DER AKTUELLEN VERSION

Version:	Im Einsatz seit:	Installation durch:	Bemerkungen:
1.16.52 (145)	Q1 / 2014	SAFECOR GmbH	Erste Geräteinstallation/ Auslieferung

TECHNISCHE ZUSTÄNDIGKEIT

Bereich:	Ansprechpartner:	Durchwahl:

FACHLICHE ZUSTÄNDIGKEIT

Bereich:	Ansprechpartner:	Durchwahl:

ALLGEMEINE PROGRAMMBESCHREIBUNG

EINSATZGEBIET UND AUFGABENSTELLUNG

Bei OSsecure-Systemen handelt es sich um „mechanische“ Sicherungssysteme (Geräte), welche in den Geschäftsstellen einer Bank kommen im Rahmen der Kassensicherung zum Einsatz kommen.

Ein OSsecure-System kann ein Tagestresor, eine Personenschleuse, ein Hochsicherheitsschloss auf einem Tresor, Geldautomat, Recycler, o.ä., ein Zutrittssystem für Personaleingänge, Geldbearbeitungsräume oder andere sensible Bereiche sein. OSsecure bringt die Sicherheits-Einrichtungen in den Bank-Filialen auf einen einheitlichen technischen und gesetzlichen Standard und bietet den Benutzern und Verantwortlichen komfortable Möglichkeiten in der Umsetzung interner organisatorischer Prozesse. Die OSsecure-Plattform stellt dabei einen „einheitlichen“ Gerätestandard zur Verfügung und berücksichtigt die gesetzlichen Anforderungen der Unfallkasse (UVV-Kassen, Versicherungsschutz der Beschäftigten).

Die Prozessgestaltungen, sowie die Vorgaben zum Einsatz verschiedener Sicherheitssysteme resultieren aus den gesetzlichen Anforderungen der Unfallkasse oder den Vorgaben der Sachversicherer.

Die Systeme werden von den Filialmitarbeitern genutzt, um den Anforderungen der UVV-Kassen, BGV C9 für den sicheren und UVV-konformen Betrieb gerecht zu werden. Bei den Sicherungsmaßnahmen steht der Mitarbeiter-Schutz im Vordergrund und es soll weiterhin der Anreiz für Überfälle durch das System reduziert werden (Prävention). Mit der OSsecure-Plattform lassen sich alle Filial-Konzepte abbilden (§18, §19 Geschäftsstellen, PLUS- und Kleinstzweigstellen, etc.) und somit flexible Vertriebskonzepte UVV-konform abbilden. Die Bestimmungen der Berufsgenossenschaft sehen u.a. vor, dass in PLUS Filialen Auszahlungen durch einen Mitarbeiter allein nicht möglich sein dürfen. Zur Einleitung einer Auszahlung müssen sich die Mitarbeiter biometrisch identifizieren. Die PLUS-Lösung beinhaltet, dass alle Wertbehältnisse (z.B. Geldautomaten, Tagestresore, Wertschutzschränke) in das biometrische System integriert sind. Eine Öffnung der Wertbehältnisse ist somit nur durch zwei Mitarbeiter zeitverzögert möglich. Mit der PLUS-Lösung können alle anfallenden Bargeldgeschäfte durchgeführt werden. Diese Anforderungen gelten auch bei der Verwendung von White-Cards.

Bei OSsecure handelt es sich NICHT um Systeme, welche Auswirkungen auf das Kernbankensystem haben. Für die sicherheitstechnische Einstufung nach MaRisk ist dieser Sachverhalt entscheidend. Es findet kein Datenaustausch mit Bank-Systemen statt. Das System arbeitet vollkommen autark und ohne jegliche Abhängigkeiten. Ein Ausfall/Abschaltung der Banksysteme (OSPlus, agree BAP oder bank21) hat keinen Einfluss auf den Betrieb des OSsecure Systems. Normale Anforderungen, welche

hinsichtlich der gesetzlichen oder bankaufsichtlichen Vorschriften (MaRisk) für Banksysteme für die Authentifizierung (starke Authentifizierung) und Revision gelten, greifen bei OSsecure-Systemen nicht.

OSsecure sichert keine Sachwerte, sondern dient ausschließlich dem Schutz der Mitarbeiter. Sämtliche Schutzziele beziehen sich auf die Anforderungen der UVV-Kassen und dienen der Prävention vor Überfällen. Eine zusätzliche Gefährdungsanalyse ist für die Filialen zwingend erforderlich. Das OSsecure System erhöht durch zusätzliche Maßnahmen (2-Faktor Authentifizierung, wie z.B. Biometrie + PIN-Code) den Schutz der Sachwerte. Die Anforderungen der Sachversicherer unterliegen jedoch separaten Prüfungen und Qualifizierungen und diese werden vom VdS zertifiziert. Tresorschlösser und alle Wertgelasse, welche Sachwerte außerhalb der Öffnungszeiten sichern, müssen somit eine gültige VdS Zertifizierung vorweisen. Mit diesem Zertifikat ist die Produkt-Qualifikation sichergestellt, welche für die Sachversicherer relevant ist. Eine zusätzliche (biometrische) Absicherung ist aus Sicht des Sachversicherers „lobenswert“ (jedoch nicht zwingend erforderlich) und wirkt sich positiv auf die Gefährdungsanalyse aus, führt jedoch selten zur Reduzierung der Police des Sachversicherers, obgleich die Unfallkasse die biometrische Absicherung zum Schutz der Mitarbeiter je nach Filial-Sicherheits-Konzept vorschreibt.

Bitte lesen Sie das zusätzliche Whitepaper, welches alle Fragestellungen zum “Sicheren IT-Betrieb”, den daraus resultierenden “Anforderungen an einen ordnungsgemäßen Programmeinsatz”, sowie der “Ordnungsmäßigkeit und Prüfung der Datenverarbeitung” (OPDV) Nr. 1 / 2006 beschreibt.

Das Whitepaper behandelt auch alle Fragestellungen welche aus den Anforderungen der MaRisk i.Bes. AT 7.2 – Technisch-organisatorische Ausstattung resultieren.

Das OSsecure System berücksichtigt die Anforderungen des Bundesdatenschutzgesetzes (BDSG). Weiterführende Informationen zum Thema Biometrie und der Datensicherheit und Verschlüsselung erhalten Sie in einem zusätzlichen Whitepaper.

KATEGORISIERUNG DER ANWENDUNG

GESETZLICHE ANFORDERUNGEN

Das System unterliegt den Anforderungen der UVV-Kassen (BGV C9) i.V.m. den BGI/GUV-I 819-2 und BGI/GUV-I 819-3 und benötigt eine Zulassungsbescheinigung (Eignungsbescheinigung, Zertifizierung) durch die DGUV – Deutsche Gesetzliche Unfallversicherung.

Das biometrische Erkennungssystem ermöglicht eine direkte Identifizierung einer Person anhand eines körperlichen Merkmals, indem ein biometrischer Datensatz verarbeitet wird. Biometrische Angaben sollten daher stets als personenbezogene Daten angesehen und daher jegliche Verarbeitung und Nutzung dieser Daten als ein rechtlich legitimationsbedürftiger Eingriff in das Recht auf informationelle Selbstbestimmung verstanden werden. Rechtsgrundlage für die Verarbeitung biometrischer Daten können Vereinbarungen mit dem Personalrat oder die Einwilligung des

Betroffenen selbst sein. Durch jede Verwendung personenbezogener Daten wird der Persönlichkeitsschutz des Betroffenen berührt. Das hier betroffene informationelle Selbstbestimmungsrecht beinhaltet das Recht, selbst darüber zu bestimmen, wer auf welche personenbezogenen Daten zugreifen und diese für welche Zwecke verwenden darf. Nach §3 I BDSG sind personenbezogene Daten solche „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmtem oder bestimmbaren natürlichen Person".

AUFSICHTLICHE ANFORDERUNGEN

Für den Betrieb und die Benutzung der Geräte, wie z.B. der Tresore für den Tagbetrieb mit zeitverzögerter Freigabe der Geldbeträge, sind keinerlei Softwareinstallationen erforderlich. Auf den Banksystemen (Clients in den Filialen) und auch auf den Backend Systemen (Terminalserver, etc. im Rechenzentrum FI/GAD/FIDUCIA) werden keine bestimmten Softwarepakete, Treiber oder sonstige Einstellungen benötigt. Der Betrieb der Sicherheitseinrichtungen (z.B. Tresore) erfolgt vollkommen „autark" (embedded) und losgelöst von den Banksystemen. Sämtliche Parameter, wie z.B. Berechtigungen oder die Definitionen der Verzögerungszeiten können direkt an den Geräten eingestellt werden. Es sind für jene Parametrisierungen keine zusätzlichen Programme, oder sonstige Softwarekomponenten erforderlich. Zur Administration und Benutzerverwaltung, sowie für die Freigabe der Hintergrundbestände wird ein aktueller Browser benötigt. Der „Administrator" legitimiert sich gegenüber dem System mit ID und Passwort, um relevante Konfigurationsparameter zu setzen, welche dem Schutz der Mitarbeiter nach UVV-Kassen dienen. Sicherheitsmaßnahmen, welche sich auf den Schutz der Sachwerte beziehen unterliegen gesonderten Anforderungen des VdS (VdS Schadenverhütung). Die VdS Zertifizierungen definieren mit Ihren unabhängigen und objektiven Bewertungen und Richtlinien den geforderten Standard der Sachversicherer. Das OSsecure-System setzt beim Schutz der Sachwerte auf den vorhandenen und VdS zertifizierten Sicherungsmaßnahmen auf. Es handelt sich um einen zusätzlichen Schutz, welcher als Mindestschutz die VdS Kriterien aber immer voraussetzt (OSsecure schützt Sachwerte „on top".)

Die Anwendung unterliegt keinen bestimmten aufsichtlichen Anforderungen.

SACHLOGISCHE LÖSUNG

Die OSsecure Geräte dienen dem Schutz der Mitarbeiter im Filialgeschäft und sollen die Anreize für Überfälle reduzieren. Die OSsecure Systeme unterstützen die Anwender und Verantwortlichen bei der Einhaltung der Bestimmungen der UVV-Kassen und der Anforderungen der Berufsgenossenschaft im Umgang mit den „Versicherten" (Mitarbeitern).

Um die Unterstützung zu realisieren, werden biometrische Systeme eingesetzt, die die Anwesenheit von zwei Mitarbeitern zum Zeitpunkt der Auszahlung sicherstellen.

Sobald sich zwei Mitarbeiter am OSsecure Gerät identifiziert haben, erfolgt eine spezifische Freigabe für einen bestimmten Prozess (z.B. die zeitverzögerte Öffnung eines Tresorfaches). Die UVV-Kassen schreiben je nach Betragshöhe verschiedene Verzögerungszeiten vor (je höher der Geldbetrag, desto länger die Verzögerungszeit). Die zeitverzögerte Freigabe der Beträge vermindert den Anreiz eines Überfalls.

Nach Ablauf der Zeitverzögerung kann der Mitarbeiter dann das Tresorfach, den Hintergrundbestand oder andere sensible Sicherungsbereiche öffnen.

Im Protokoll des OSsecure-Systems kann definiert werden, welche Berechtigungen für die jeweilige Freigabe/ Öffnung erforderlich sind und welche Verzögerungszeiten nach UVV-Kassen greifen müssen.

PROGRAMMTECHNISCHE LÖSUNG

Die OSsecure Geräte haben keine spezifischen Hard- und Softwareanforderungen, da keine Softwarekomponenten auf den Banksystemen installiert werden müssen. Die Geräte müssen lediglich in das IP-Netzwerk des Institutes integriert werden.

Es existieren im autark-Betrieb keine Schnittstellen zu anderen Systemen. Die Konfiguration/ Bedienung der OSsecure-Geräte erfolgt per Webbrowser (Port 80).

Die Beschreibung der Ein- und Ausgabemasken ist der jeweils aktuellen Dokumentation zu entnehmen.

BESCHREIBUNG DES VERFAHRENS

BESCHREIBUNG DER STRUKTUREN

AUFBAU

Die OSsecure Geräte erfordern keine zusätzlichen Softwarekomponenten. Die Bedienoberfläche der Systeme (z.B. Tresorschlösser, Tagestresor, Personenschleusen, Zugangssystem) ist vollständig in die Gerätehardware integriert. Die Bedienoberfläche ist getrennt in eine Administrationsebene und eine Anwendungsebene. Alle Geräte lassen sich für einen Großteil der möglichen Anwendungs-Szenarien auch „autark“ direkt über die im Gerät eingebauten Displays und über die Zehner-Tastatur des Gerätes durch den Anwender bedienen.

Die Beschreibung der Administrationsmasken sind der jeweils aktuellen Dokumentation zu entnehmen.

BERECHTIGUNGSKONZEPT

Das System verfügt über ein eigenes Berechtigungskonzept, da keinerlei Schnittstellen zur Domäne (Active Directory, LDAP) oder anderen Systemen existieren. Der Zugriffsschutz kann in der Administrationsebene eingestellt werden.

Es können Berechtigungsgruppen angelegt und definiert werden. Gruppen-Bezeichnungen können so auf die Organisationsstruktur angepasst werden.

Wenn es sich bei der im Berechtigungskonzept angelegten Gruppe um „Bediener“ handelt, welche keine zusätzlichen Verwaltungs-Funktionen in der Software freigeschaltet bekommen sollen, sondern ausschließlich Nutzer/Bediener der Tagestresore, Schlösser und Personenschleusen sind, dann müssen lediglich die jeweiligen Sicherungssysteme der Gruppe zugeordnet werden, welche von der Gruppe bedient werden sollen.

Wenn es sich bei der im Berechtigungskonzept angelegten Gruppe um „Administratoren“ handelt, welche Verwaltungs-Funktionen im System freigeschaltet bekommen sollen (z.B. um Verzögerungszeiten gemäß UVV-Kassen definieren zu können), so können diesen Administrativen Personen verschiedene Verwaltungsfunktionen zugeordnet werden.

Administratoren können das System verwalten, neue Bediener anlegen und Berechtigungen vergeben. Bediener können die Geräte (z.B. Kassenschleuse, Türzugänge, Tresorschlösser, Tagestresore) „lediglich“ bedienen. Sie verfügen aber über keine zusätzlichen administrativen Rechte im System.

Beispiel für eine im System hinterlegte Standard-Berechtigung:

- **OE3310 hat die Berechtigung Administrator** *(Rechte siehe Tabelle unten)*
- **OE51 (Filialen) hat die Berechtigung Kassenmitarbeiter.**

Die folgende Beschreibung erläutert die Programmfunktionen im System, welche optional (auch) anderen Berechtigungsgruppen zugeordnet werden können. Standardmäßig sind jene Berechtigungen der Gruppe „Administrator“ zugeordnet.

Programmfunktion	Beschreibung
Bearbeiten der Stamm und Authentifizierungsdaten	Berechtigung für das Anlegen von Stammdaten und das Erfassen von biometrischen Daten, sowie PIN-Berechtigungen, RFID Karten und weiteren Authentifizierungsdaten.
Geräte verwalten	Berechtigung für das Zuordnen von Geräten (z.B. Kassenschleuse), welche von im Berechtigungskonzept hinterlegten Gruppen/ Rollen (z.B. Kassenmitarbeiter) benutzt werden dürfen.
Bearbeiten des Berechtigungskonzeptes	Berechtigung für das Anlegen oder Löschen von Berechtigungsgruppen
Systembackup erstellen	Berechtigung für das Erstellen einer separaten (zusätzlichen) Datensicherung
Einsicht von Synchronisationsfehlern	Berechtigung für das Einsehen des Synchonisationsstatus
Einspielen von Systemupdates	Berechtigung für das Einspielen von Systemupdates (diese Funktion steht in neueren Systemen nicht mehr zur Verfügung)
System herunterfahren	Berechtigung für das softwareseitige Neustarten eines Systems (Kassenschleuse)
Programmfunktionen bearbeiten	Berechtigung für das Zuweisen von Programmfunktionen zu einer Berechtigungsgruppe
Logdateien einsehen	Berechtigung für das Einsehen von Logdaten
Alarm deaktivieren	Berechtigung für das Rücksetzen eines Alarms (betrifft nur bestimmte Geräte und Steuerplatinen). Eine Kassenschleuse muss nach einer Alarmabsetzung nicht zurückgesetzt werden.
Reset der Controllerkarte	Berechtigung für einen Reset einer Controllerkarte (betrifft nur bestimmte Geräte und Steuerplatinen, wie z.B. Tagestresore älterer Bauart).

Fingerscanner Verwalten	Berechtigung für die Konfiguration bestimmter Fingerprintscanner (z.B. Auftischvariante, welche Bei Whitecard-Dispensern eingesetzt wird).
Systemzeit einstellen	Berechtigung für das Einstellen der Uhrzeit
Netzwerk einstellen	Berechtigung für das Einstellen der Netzwerkdaten
BioEntry Verwalten	Berechtigung für das Einstellen von biometrischen Türzugängen
Kurzfreischaltung	Berechtigung für das Sonderrecht „Kurzfreischaltung“, was bei bestimmten Prozessen für die gesonderte Berechtigung externer Personen verwendet werden kann (spezielle Service- oder Cashhandling-Prozesse).
System einstellen	Berechtigung für die Konfiguration diverser Systemparameter
Depotfachverwaltung	Berechtigung für das Verwalten von Depotfächern (z.B. Vorbestelltes Geld bei Tagestresoren).
Berechtigung für Benutzer von Depotfächern	Berechtigung für die Benutzer von Depotfächern
Pin - User Berechtigung	Systemberechtigung für das automatische Anlegen von PIN Code berechtigungen über das Display eine PIN bedienten Tagestresors (Admin kann über Fach 0 User ohne Webinterface anlegen). Der neue User bekommt dann autom. alle Berechtigungsgruppen zugewiesen, welche jene Programmfunktion enthalten.
TwinLock BioPIN Verwalten	Berechtigung für das Verwalten von BioPINs für die zusätzliche biometrische Absicherung von Hochsicherheitsschlössern der Baureihe TwinLock WTU.
TwinLock BioPIN Master	Berechtigung für das Verwalten von Einmalmaster-TANs für Hochsicherheitsschlössern der Baureihe TwinLock WTU.
TwinLock BioPIN freie PIN-	Berechtigung für das Wählen eines beliebigen Zeitraums für das Erstellen von BioPINs für Hochsicherheitsschlössern der Baureihe

Generierung	TwinLock WTU.
Exports - User Berechtigung	Berechtigung für das Exportieren (CVS-Export) der im System hinterlegten Berechtigungen in einem Zentralsystem (Windows).

KOMPETENZEN

Für die UVV-Kassensicherheit sind zwei verschiedene Berechtigungsgruppen vorgesehen.

1. **Kassenmitarbeiter**

   Der Mitarbeiter in der Filiale hat Öffnungsberechtigungen für die Kassensicherungssysteme (Schlösser, Tagestresore, etc.)

2. **Administrator/Systemadministrator**

   Der Administrator übernimmt die fachliche Administration und Konfiguration (Zeitverzögerung, Berechtigungen für Kassenmitarbeiter).

Es lassen sich darüber hinaus eigene Berechtigungsgruppen im rollenbasierten Berechtigungskonzept festlegen.

PROZESSE UND ABLÄUFE

ALLGEMEINE BESCHREIBUNG

Beispielhafte Beschreibung Ablauf Tagestresor

Für die zeitgesteuerte Öffnung eines Faches bei einem Tagestresor wählen die Mitarbeiter das jeweilige Fach an, identifizieren/ legitimieren sich und warten die Verzögerungszeit ab. Nach Ablauf der Zeit wird das Fach mechanisch freigegeben und kann geöffnet werden.

Beispielhafte Beschreibung Ablauf Personenschleuse

Bei einer Personenschleuse wird die erste Tür über Taster, eine Codetastatur oder ein biometrische Zugangssystem, Transponder, o.ä. freigegeben. Innerhalb der Schleuse erfolgt dann eine Prüfung auf Vereinzelung (je nach Hardwaretyp über Sensorik, Gewicht oder in Kombination auch visuelle Überprüfung durch Kameratechnik). Weiterhin muss sich die Person biometrisch identifizieren, um für den Schleusen-Durchgang berechtigt zu sein.

Beispielhafte Beschreibung Ablauf Wertschutzschrank

Bei einem Wertschutzschrank (z.B. GAA, Hintergrundbestand) wird der normale Öffnungsprozess des Wertgelasses (Achtung: Sachwerte) nach den Richtlinien des VdS zusätzlich freigegeben. Es müssen sich z.B. erst zwei Mitarbeiter biometrisch identifizieren, damit der normale VdS-Ablauf freigegeben wird. Die Mitarbeiter haben erst nach biometrischer Überprüfung die Möglichkeit Ihre Kombination am Wertgelass einzugeben. Der VdS relevante Schutz ist und bleibt die Kombination (z.B. PIN-Code oder Chipkarte). Der biometrische Schutz kommt hier nur „on top“. Alle tatsächlich „öffnungsrelevanten“ Informationen (z.B. PIN-Code) werden nicht im OSsecure System verwaltet.

ARBEITSANWEISUNGEN

Arbeitsanweisungen sind gesondert zu definieren.

HANDBÜCHER

Die jeweils aktuelle Dokumentation kann unter http://update.ossecure.de abgerufen werden.

FACHLICHE ADMINISTRATION

ALLGEMEIN

Wer ist für die fachliche Administration zuständig?

OE3310.11

Eine Administratoren Schulung wird zum Thema OSsecure von der Firma SAFECOR angeboten. Es ist zusätzlich ein fundiertes Hintergrundwissen zum Thema UVV-Kassen und den BGI‘en 819 1-3 erforderlich.

PARAMETRISIERUNG

Es sind die Verzögerungszeiten der einzelnen Verschlussbereiche gemäß UVV-Kassen zu definieren.

SCHNITTSTELLEN / ABHÄNGIGKEITEN ZU ANDEREN SYSTEMEN

Es sind keine Schnittstellen zu anderen Systemen vorhanden.

TECHNISCHER BETRIEB

ADMINISTRATION

Die technische Administration erfolgt „remote“ per Webbrowser auf dem jeweiligen System (z.B. Tagestresor). Der Zugriff ist kennwortgeschützt.

REGELBETRIEB UND WARTUNGSARBEITEN

Es sind keine Wartungsarbeiten an der Software durchzuführen. Updates werden je nach Wartungsvertrag und Vereinbarung zur Verfügung gestellt. Wartungsarbeiten an der Hardware sind je nach Typ abzustimmen. Die Unfallkasse schreibt regelmäßige Wartung bei bestimmten Sicherungssystemen (z.B. Personenschleusen) zwingend vor.

IT-SICHERHEIT

Im Abschnitt 4.2 ist einer weitergehende Bearbeitung nicht erforderlich.

Lesen Sie für zusätzliche Informationen das Whitepaper "Sicherer IT-Betrieb – Anforderungen an einen ordnungsgemäßen Programmeinsatz".

IT-SICHERHEITSMANAGEMENT

➔ Regelungen dazu bei dem IT-Sicherheitsbeauftragten der Bank

RAUMPLAN

➔ sofern vorhanden, abgelegt bei Abteilung…

VERKABELUNG

➔ sofern vorhanden, abgelegt bei Abteilung…

Alle Geräte benötigen einen Netzwerkanschluss (RJ45 Buchse, min. CAT5), sowie 220V Spannungsversorgung. Bei Umtresoren ist darauf zu achten, dass die Lesegeräte aufgrund der Kabelwege/länge unmittelbar darüber auf dem Möbel stehen müssen. Personenschleusen benötigen je nach Typ auch zwei Netzwerkanschlüsse. Verkabelungen für Zutrittssysteme sind individuell mit dem Elektriker abzustimmen (Fluchtwege- und Brandkonzepte sind von den Türschlössern abhängig).

Alle Kabelpläne zu den einzelnen Sicherungsprodukten, finden Sie auch im Support-Portal unter www.safecor.net

RAUMABSICHERUNG

➔ *sofern vorhanden, abgelegt bei Abteilung…*

Die OSsecure Zugangssicherung ermöglicht eine Türfreigabe mittels biometrischer Identifikation, RFID (Transponder) oder via Codetastatur. Die Raumabsicherung wird in zwei Sicherheitsstufen definiert. In der hohen Sicherheitsstufe (z.B. Außentüren) ist eine Manipulation der eigentlichen Leseeinheit ausgeschlossen, da die eigentliche Türöffnung aus dem gesicherten Bereich heraus erfolgt. Leseeinheit und Steuereinheit kommunizieren hierbei verschlüsselt (vergl. VdS Klasse B). Bei der normalen Sicherheitsstufe (vergl. VdS Klasse A) erfolgt die Türansteuerung aus der Leseeinheit heraus. Eine Manipulation der Leseeinheit ist über Abrissmelder gesichert.

DATENSICHERUNG & ARCHIVIERUNG

Eine Datensicherung ist nicht erforderlich, die Geräte synchronisieren/spiegeln sich gegenseitig. Die Daten sind somit redundant gesichert.

REGELUNGEN DATENSCHUTZ

Siehe gesondertes Dokument zur Datensicherheit, Datenschutz.

BDSG Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

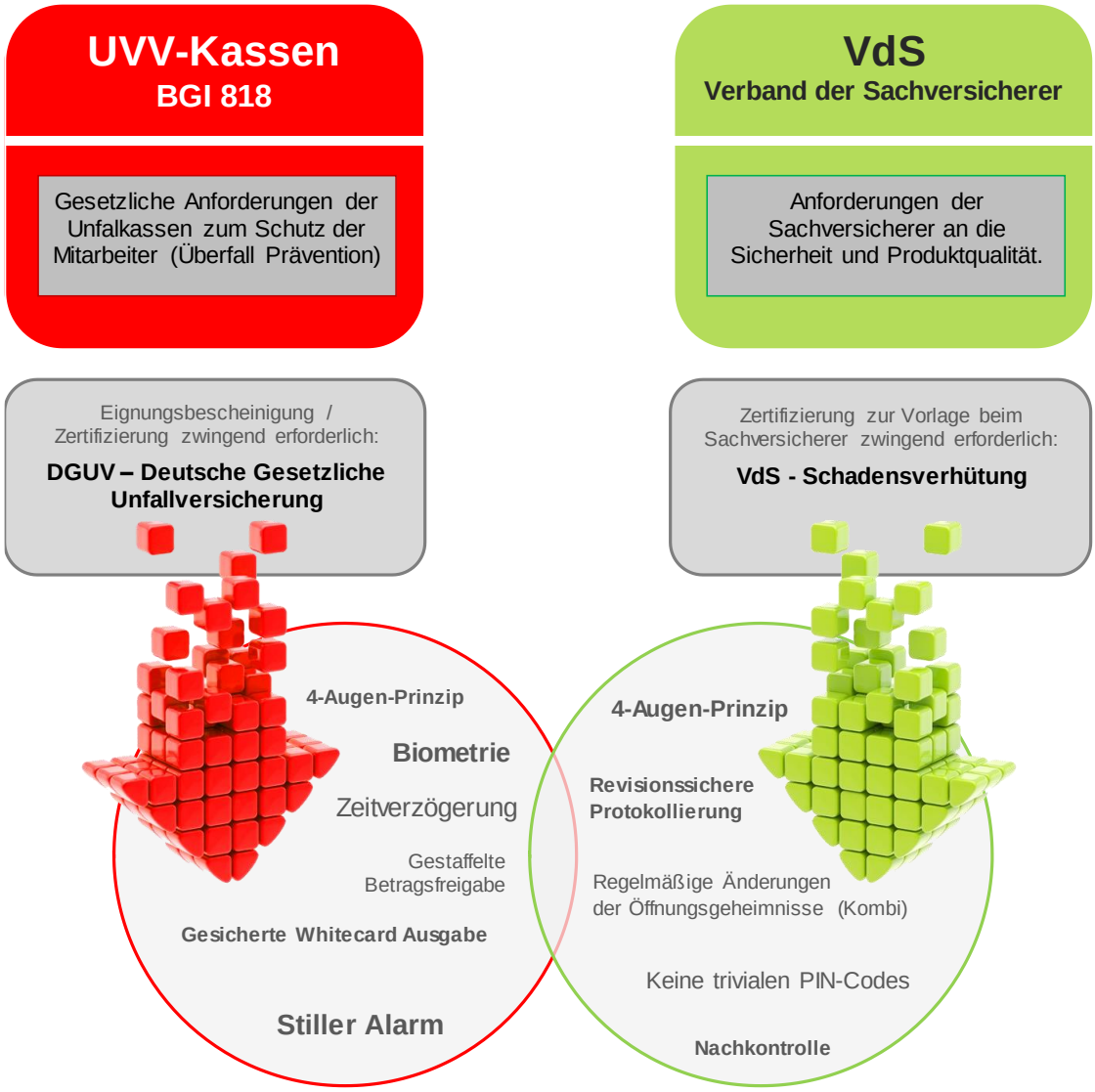
EINBINDUNG IN DAS INTERNE KONTROLLSYSTEM

Eine Einbindung in das interne Kontrollsystem ist insofern nicht erforderlich, da die Schutzziele sich auf den Personenschutz und nicht auf den Sachwerteschutz beziehen. Sachwerte (Wertgelasse), welche durch zusätzliche Absicherungen (z.B. Biometrie) aufgrund Anforderungen der UVV-Kassen mit in das OSsecure-System integriert wurden, unterliegen weiterhin den internen Kontrollsystemen.

Tresore (Sachwerte), welche im 4-Augen-Prinzip geöffnet werden, unterliegen weiterhin den Anforderungen der Innenrevision.

Zwischen den Anforderungen der UVV-Kassen und denen der Sachversicherer muss unterschieden werden. Die folgende Grafik soll die Unterscheidung vereinfachen. Aufgrund der Überschneidungen der unterschiedlichen und teilweise gleichen Anforderungen ergeben sich häufig Missverständnisse. Das 4-Augen-Prinzip wird beispielsweise von der Unfallkasse, der Innenrevision und dem Sachversicherer gefordert. Die revisionssichere Protokollierung der Öffnungsvorgänge wird hingegen nur von der Innenrevision und dem Sachversicherer gefordert. Eine Protokollierung, welche diesen Anforderungen gerecht wird, ist daher in die Tresor-Schlosssysteme integriert und mit der VdS Zertifizierung qualifiziert bestätigt. Das OSsecure-System bietet auch Protokollfunktionen – diese sind jedoch nicht „revisionssicher“, da die UVV-Kassen eine solche Art der Protokollierung nicht fordert und dieses Protokollverfahren sich negativ auf die Wirtschaftlichkeit des OSsecure-Systems auswirken würde.

- *Unterlagen, Berichte der Innenrevision, Verbandsrevision*
- *Erfordernis eines Vier-Augen-Prinzips, einer Nachkontrolle, etc.*



NOTFALLBETRACHTUNGEN

IT-RECOVERY

Die aktuelle Übersicht der Wiederanlaufklassen und deren zugeordneten Anwendungen ist im UHB (1.60.01.10.50 Wiederanlauf IT (IT Recovery)) veröffentlicht.

Alle Tresore (nicht Tagbetrieb) können auch unabhängig von OSsecure über Notfall-PIN-Codes geöffnet werden.

BUSINESS RECOVERY

Es sind keine „klassischen“ Recovery Prozesse zu definieren, da keine Abhängigkeiten zu den Banksystemen bestehen. Es ist empfehlenswert, SLAs in Wartungsverträgen zu definieren, welche Zeiträume für eine Wiederherstellung der Sicherheitsgeräte definieren.

Für Tresorschloss-Systeme (risikorelevant i.S. der MaRisk) müssen Notfall-Prozesse für z.B. Stromausfall, definiert werden.

Die aktuelle Übersicht der Wiederanlaufklassen und deren zugeordneten Anwendungen ist im UHB (1.60.01.10.40 Wiederanlauf der Geschäftsfunktionen (Business Recovery)) veröffentlicht.

Zusätzliche Informationen:

- *Welche Anforderungen sind an den Wiederanlauf zu stellen?*
  - *Ressourcen für den Wiederanlauf*
  - *Ausweichlokation für den Notfall*
- Gibt es Übergangsregelungen bzw. „Not-„Lösungen, die greifen, wenn die Anwendung nicht zur Verfügung steht.
- Ggf. einen Verweis auf die Notfall-Handbücher einfügen!

QUALITÄTSSICHERUNGSMAßNAHMEN

ERFORDERLICHE MITARBEITERQUALIFIKATION

ANFORDERUNGSPROFIL

Platzhalter bis Stellenbeschreibung/Anforderungsprofil/Aufgabenbeschreibung fertig gestellt

a) für fachl. Admins

b) für Mitarbeiter (Berater, Analysten)

STELLENBESCHREIBUNG

Platzhalter bis Stellenbeschreibung/Anforderungsprofil/Aufgabenbeschreibung fertig gestellt

c) für fachl. Admins

d) für Mitarbeiter (Berater, Analysten)

AUFGABENBESCHREIBUNG

Platzhalter bis Stellenbeschreibung/Anforderungsprofil/Aufgabenbeschreibung fertig gestellt

e) für fachl. Admins

f) für Mitarbeiter (Berater, Analysten)

FREIGABEVERFAHREN

PROGRAMM- UND EINSATZFREIGABEFREIGABE

Die Dokumentation des Programmeinsatz- und Freigabeverfahrens inkl. der programmeinsatz- und Freigabeerklärung ist hier abzulegen.

Zusätzlich können hier folgende Unterlagen abgelegt werden:

- Stellungnahmen des Datenschutzbeauftragten der Sparkasse Holstein
- Stellungnahmen des IT-Sicherheitsbeauftragten

DOKUMENTATION DER TESTERGEBNISSE

Wenn im Rahmen der Programmeinsatz- und Freigabeverfahrens sparkasseninterne Tests durchgeführt wurden, werden die hier abgelegt.

- ggf. reicht hier auch ein Verweis auf einen separaten „Test"-Ordner, wenn solche Tests sehr umfangreich waren
- Ist eine Einsatzfreigabe durch die Bank erforderlich, so sind die Integrationstests (Test für die Einsatzfreigabe gem. OPDV 1/2006 (ehem. OPDV 1/1994) ebenfalls hier abzulegen.
- Kurze Beschreibung der Tests, der Testdaten, etc.

RELEASEINFORMATIONEN

Aktuelle Releaseinformationen (Versionshistorie) finden Sie unter (Login erforderlich)

http://safecor.net/update/ossecure-update/versionshistorie-ossecure/

ANLAGEN

VERTRÄGE / ANGEBOTE

Nachfolgende Unterlagen einheften bzw. Lagerstelle angeben:

- Angebote
- Kaufverträge
- Wartungs- / Serviceverträge

WEITERE UNTERLAGEN

- Vorstandsbeschlüsse
- Informationen an Personalrat, wenn die Anwendung beteiligungspflichtig ist