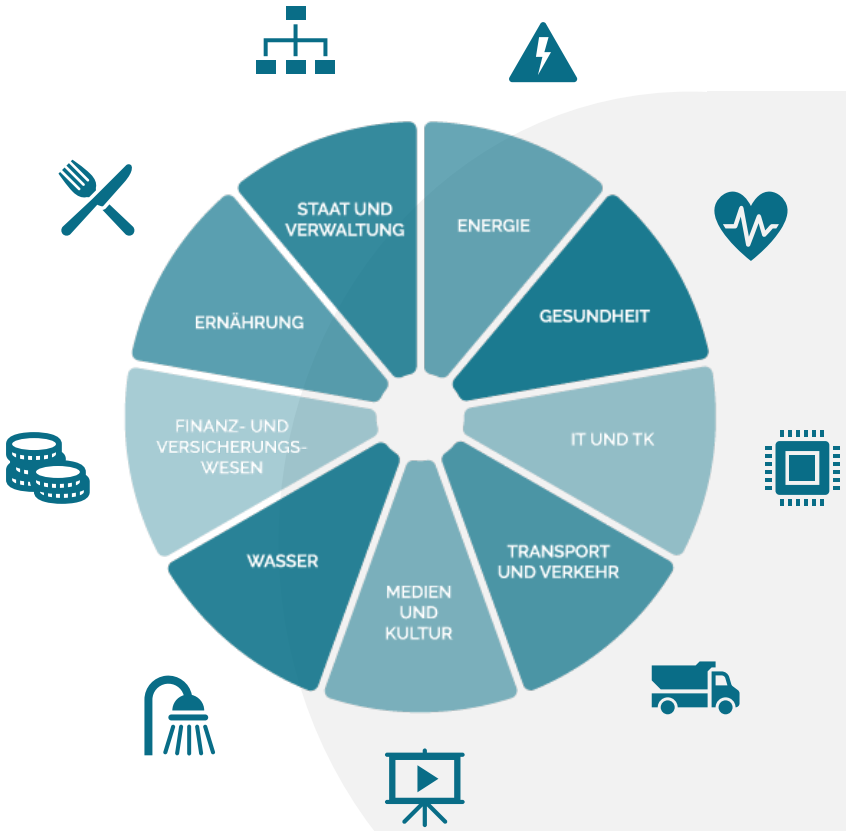
imprivata®
OGITIX

RATGEBER
BSI-KRITIS

Anforderungen der BSI-Kritisverordnung an das
User- & Rechte-Management und
die entsprechenden Lösungsansätze



Inhaltsverzeichnis

1 Einleitung zur BSI-Kritisverordnung ... 3

2 Über diesen Leitfaden ... 6

3 Anforderungen der BSI-Kritisverordnung an das User- & Rechte-Management ... 6

3.1 Bedrohungskategorien ... 6

3.2 Branchenunabhängige Maßnahmen ... 7

4 Wichtige Handlungsfelder und Lösungsansätze ... 7

4.1 Auditierbarkeit der aktuellen Rechtevergabe ... 7

4.1.1 Anforderungen & Ist-Situation ... 7

4.1.2 Lösungsansätze mit OGiTiX unimate ... 9

4.2 Zyklische Re-Zertifizierung der vergebenen Rechte ... 10

4.2.1 Anforderungen & Ist-Situation ... 10

4.2.2 Lösungsansätze mit OGiTiX unimate ... 11

4.3 Sichere Vergabe und zeitliche Begrenzung von Administrationsrechten ... 12

4.3.1 Anforderungen & Ist-Situation ... 12

4.3.2 Lösungsansätze mit OGiTiX unimate ... 12

4.4 Rollentrennung / Vermeidung kritischer Rechtekombinationen ... 13

4.4.1 Anforderungen & Ist-Situation ... 13

4.4.2 Lösungsansätze mit OGiTiX unimate ... 13

4.5 Risikomanagement / Blockabwesenheit ... 14

4.5.1 Anforderungen & Ist-Situation ... 14

4.5.2 Lösungsansätze mit OGiTiX unimate ... 15

5 Zusammenfassung und Empfehlung ... 16

6 Anhang ... 18

6.1 Referenzierte Dokumente ... 18

1 Einleitung zur BSI-Kritisverordnung

Welche Unternehmen aus dem Bereich der Kritischen Infrastrukturen genau von den im IT-Sicherheitsgesetz beschlossenen Regelungen betroffen sind, wird durch die Bestimmung Kritischer Infrastrukturen nach der BSI-Kritisverordnung (BSI-KritisV) festgelegt (§ 10 BSI-Gesetz). Der erste Teil dieser Rechtsverordnung wurde vom zuständigen Bundesministerium des Innern erarbeitet und ist am 3. Mai 2016 in Kraft getreten. Er umfasste die KRITIS-Sektoren Energie, Informationstechnik und Telekommunikation, Ernährung und Wasser und regelt, welche Unternehmen aus diesen Sektoren unter das IT-Sicherheitsgesetz fallen.

Die noch ausstehenden Festlegungen für die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr wurden mit einer Änderungsverordnung getroffen. Diese ist am 30. Juni 2017 in Kraft getreten. Somit findet die BSI-KritisV nun Anwendung auf die folgenden Bereiche.

Überschneidungen sind durchaus relevant, auch Unternehmen, die die Schwellwerte nicht erreichen, können im Sinne von BSI-KritisV zu betrachten, wenn Sie als Dienstleister für ein Kritis-Unternehmen tätig sind. Beispielhaft im Bereich Transport und Verkehr tätig für den Sektor Energie oder Gesundheit.

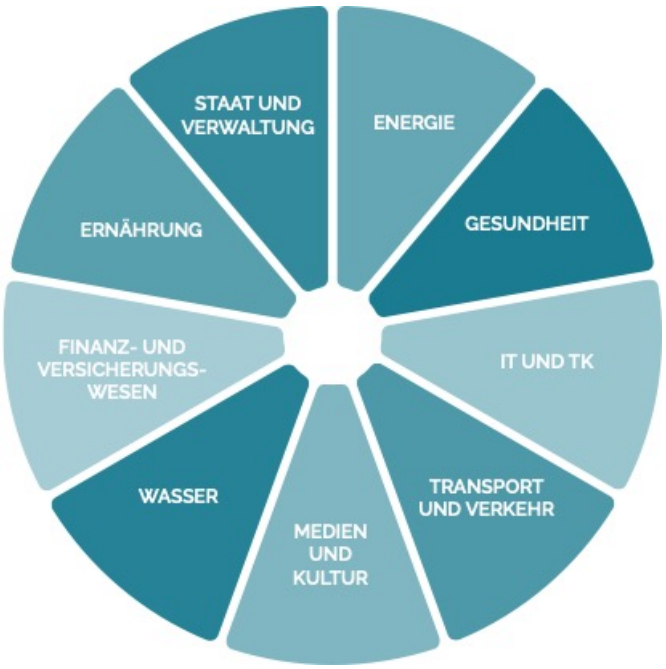


Abbildung 1: Kritis Sektoren
Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Sektor Gesundheit

- Stationäre medizinische Versorgung
- Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten
- Versorgung mit Arzneimitteln und Blut- und Plasmakonzentraten
- Laboratoriumsdiagnostik

Sektor Finanz- und Versicherungswesen

- Bargeldversorgung
- Kartengestützter Zahlungsverkehr
- Konventioneller Zahlungsverkehr
- Verrechnung und Abwicklung von Wertpapier und Derivatgeschäften
- Versicherungsdienstleistungen

Sektor Transport und Verkehr

- Personen- und Güterverkehr
    - Luftverkehr
    - Schienenverkehr
    - See und Binnenschifffahrt
    - Straßenverkehr

Sektor Energie

- Stromversorgung/-erzeugung
- Gasversorgung
- Fernwärmeversorgung
- Kraftstoff- und Heizölversorgung

Sektor Wasser

- Gewinnungsanlagen
- Aufbereitungsanlagen
- Verteilungssysteme
- Kanalisation
- Kläranlagen

Sektor Ernährung/Lebensmittelversorgung

- Lebensmittelherstellung/-versorgung
- Lebensmittelhandel

Sektor Informationstechnik und Telekommunikation

- Sprach- und Datenübertragung
- Datenspeicherung und -verarbeitung

Sektor Sonstige

- Anlagen zur Wettervorhersage, zur Gezeitenvorhersage oder zu Wasserstandsmeldungen
- Satellitennavigation

Die Rechtsverordnung legt qualitative und quantitative Kriterien, wie beispielsweise die Anzahl der versorgten Personen mit einer bestimmten Dienstleistung fest. Wer diese Kriterien erfüllt, betreibt eine Kritische Infrastruktur im Sinne des Gesetzes.
Betreiber Kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes sind nach Verabschiedung der BSI-Kritisverordnung verpflichtet,

- eine Kontaktstelle zu benennen,
- IT-Störungen zu melden,
- den "Stand der Technik" umzusetzen
- und dies alle zwei Jahre gegenüber dem BSI nachzuweisen.

2 Über diesen Leitfaden

Im Fokus der zum Schutz Kritischer Infrastrukturen geforderten Sicherheitsvorkehrungen steht die Sicherung der Versorgung der Bevölkerung mit der kritischen Dienstleistung zur Vermeidung von Versorgungsengpässen sowie der Gewährleistung der öffentlichen Sicherheit. Dies kann sich mit unternehmerischen Zielsetzungen weitgehend decken, ist zunächst aber eine andere, auf die Auswirkungen für die Bevölkerung gerichtete Betrachtung.

Ableitung des KRITIS-IT-Schutzbedarfs aus den KRITIS-Schutzzielen
Für einen störungsfreien Betrieb der kritischen Dienstleistung sind IT-Systeme, Komponenten und Prozesse erforderlichen, für diese soll unter Berücksichtigung der KRITIS-Schutzziele der KRITIS-IT-Schutzbedarf hergeleitet werden. Dabei sollten Störungen oder Störungsklassen der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität (VIVA, IT-Schutzziele) behandelt werden.

> **Hinweis:**
> Der KRITIS-IT-Schutzbedarf kann vom herkömmlichen IT-Schutzbedarf abweichen, da die in den KRITIS- Schutzzielen ermittelten Anforderungen hier im Vordergrund stehen. Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit müssen bei der Ermittlung des Schutzbedarfs betrachtet werden, um die gesetzlichen Anforderungen zu erfüllen. Es ist aber zulässig, dies über eine andere Einteilung der IT-Schutzziele zu erreichen.

3 Anforderungen der BSI-Kritisverordnung an das User- & Rechte-Management

Im Folgenden sind die für das User- & Rechte-Management relevanten Artikel der BSI-Kritisverordnung (BSI-KritisV) aufgeführt. Quellen sind die Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG sowie die daraus abgeleiteten Anforderungen und Pflichten.

3.1 Bedrohungskategorien

In den Bedrohungskategorien wir als Maßnahme unter Kapitel A 3.4 explizit ein Identitäts- und Rechtemanagement gefordert.

- **Missbrauch Innentäter (A 1.5)**
- **Menschliche Fehlhandlungen, menschliches Versagen (A 2.4)**

- **Sicherer Authentisierung (A 3.4)**
- **Identitäts- und Rechtemanagement (A 3.4.1)**
- **Rollentrennung / Funktionstrennung (A 3.4.4)**

Die Umsetzungsempfehlungen zu diesen Anforderungen variieren branchenspezifisch teilweise. Je nach „gemeinsamem Nenner" einer Branche kann die Ausgestaltung in einem B3S auf sehr unterschiedlichem Abstraktionsgrad erfolgen. Teilweise können konkrete Maßnahmen definiert werden, teilweise können nur Sicherheitsanforderungen oder Vorgehensweisen benannt werden. Gemein ist die Nachweisbarkeit der getroffenen Maßnahmen. Die Umsetzung der angemessenen und wirksamen Maßnahmen kann gemäß § 8a (3) BSIG durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.

3.2 Branchenunabhängige Maßnahnamen

Die allgemeingültige branchenunabhängige Maßnahnamen sind:

- **Audittierbarkeit der aktuellen Rechtevergabe**
- **Zyklische Re-Zertifizierung der vergebenen Rechte**
- **Sichere Vergabe und zeitliche Begrenzung von Administrationsrechten**
- **Rollentrennung**
- **Risikomanagement**

4 Wichtige Handlungsfelder und Lösungsansätze

4.1 Auditierbarkeit der aktuellen Rechtevergabe

4.1.1 Anforderungen & Ist-Situation

Die Auditierbarkeit der aktuell zugewiesenen Benutzerkonten und vergebenen Zugriffsrechte stelle in der Praxis eine große Herausforderung dar. Um eine Auditierbarkeit zu gewährleisten, ist eine lückenlose und systemübergreifende Dokumentation der Berechtigungen erforderlich.

Über den reinen Status-quo der Berechtigungen hinaus müssen für ein aussagekräftige Reporting die folgende drei Aspekte der Zugriffsberechtigungen in Balance gebracht werden:

- Art: Wer hat welche Zugriffsrechte auf welche Ressourcen?
- Herkunft: Wer hat diesen Zugriff beantragt, genehmigt und / oder freigeschalten? Welcher Grund wurde angegeben?
- Historie: Seit wann besteht bzw. in welchem Zeitraum bestand die Berechtigung?

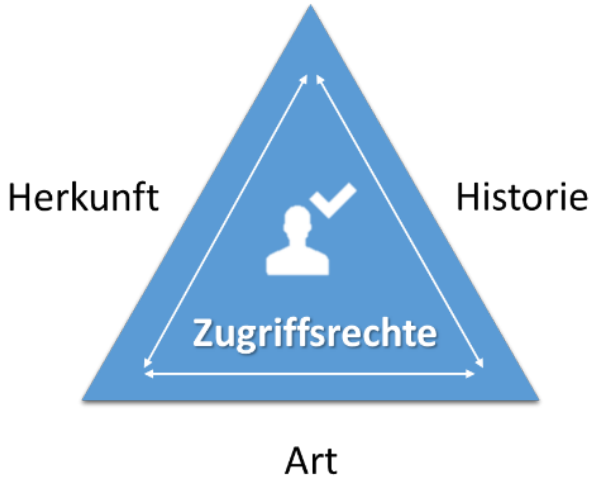


Abbildung 2: Das Zugriffsrechte-Dreieck

Die größten Herausforderungen für die meisten Unternehmen bestehen heute darin, dass Datenhaushalte, Prozesse und Verwaltungstools sehr fragmentiert sind:

- **Inkonsistente und verteilte Datenhaushalte**
- **Medienbrüche und schlechte Nachvollziehbarkeit**
- **Eingeschränkte Belastbarkeit der Auswertungen**

Heute werden schlichtweg zu viele Tools und Verwaltungsprogramme genutzt, um die Prozesse zu bewerkstelligen und Benutzerkonten und Rechte zu administrieren: Checklisten, Ticketsysteme, E-Mails, Telefonate, Formulare und diverse Management-Konsolen. Durchgeführte Arbeiten, die umgesetzten Zugriffsrechte und die vorangegangenen Entscheidungen sind aufgrund dieser mannigfaltigen Medienbrüche und der Vielzahl manueller Prozessschritte nur schlecht dokumentiert und sind kaum auswertbar.

Ein lückenloser Nachweis ist damit kaum umsetzbar. Die fragmentierten Tools und Prozesse machen eine lückenlose Protokollierung über die Entstehung, den Status-quo oder den Verlauf von Benutzerrechten nahezu unmöglich.

Hinzukommt, dass Auswertungen belastbar und teilweise tagesaktuell sein sollten. Im Zuge von Stichproben oder bei sicherheits- oder datenschutzrelevanten Vorkommnissen müssen auch historische Daten über den Verlauf oder den Berechtigungsstand in der Vergangenheit auswertbar sein.

Das fragmentierte User- & Rechte-Management macht die Erstellung von Reports allerdings nur mit hohem manuellem Aufwand möglich. Hieraus resultieren einerseits veraltete Berichte, weil die Erstellung teilweise Wochen dauert. Andererseits sind die manuell erstellten Berichte fehleranfällig, was wiederum die Belastbarkeit in Frage stellt.

4.1.2 Lösungsansätze mit OGiTiX unimate

Um eine lückenlose Protokollierung der Berechtigungen inkl. Herkunft und Historie zu gewährleisten sind verschiedene Lösungskomponenten zur berücksichtigen:

- **Durchgängige Prozesse im Berechtigungsmanagement**
- **Systemübergreifende Datenbank für Benutzerkonten und Zugriffsrechte**
- **Austomatisiert erstellte, tagesaktuelle Auswertungen**

Diese Anforderungen lassen sich mit Business Prozess Management- oder mit Identity Management-Lösungen besonders gut umsetzen, da diese Softwarelösungen Prozessmanagement, Datenmanagement und technische Orchestrierung in einer Plattform vereinen.

Automatisierte Prozesse im Berechtigungsmanagement

- Softwaregesteuerte Prozesse für das User- & Rechte-Management
  - Mitarbeiter-Eintritt (Identity Life-Cycle)
  - Mitarbeiter-Austritt (Identity Life-Cycle)
  - Mitarbeiter-Änderung (Identity Life-Cycle)
  - Nachversorgung mit Rechten (Self-Service & Approvals)
- Systembedingt, lückenlose Nachvollziehbarkeit
  - Vom Antrag über Entscheidungen bis zur technischen Umsetzung
- Jeder Prozessschritt wird den der IAM/BPM Software automatisch protokolliert
- Systemübergreifendes Datenmanagement im Prozesskontext

Systemübergreifende Rechte- und Identitätsdatenbank

- Automatisches Datenmanagement (HR, Org. Management, AD, Apps)
  - über Schnittstellen, CSV-Dateien oder Aufgaben
- Synchronisierung von Berechtigungs- & Organisationsstrukturdaten
- Verknüpfung der unterschiedlichen Benutzerkonten zu Identitäten
  - über sog. Identifier wie Personalnummer, Name, Geburtsdatum usw.
- Automatischer Aufbau und Pflege einer übergreifenden Identitätsdatenbank

Austomatisiert erstellte, tagesaktuelle Auswertungen

- Anwendungsübergreifende Rechte- bzw. Identitätsdatenbank
- Auswertungen auf Knopfdruck | Self-Service
  - Wer hatte wann welche Rechte?
  - Wer hat diese beantragt und genehmigt?
- Benutzerreports über den Status-quo
- Reports pro Abteilung, Standort, Org.-Einheit
- Mitgliederreports für Gruppen, Rollen und Profile
- Zyklisch-automatische Reports für Vorgesetzte oder Data Owner

4.2 Zyklische Re-Zertifizierung der vergebenen Rechte

4.2.1 Anforderungen & Ist-Situation

Die Praxis zeigt, dass der Status-quo an Zugriffsrechten fast immer von dem Sollzustand abweicht. Problematisch ist häufig, dass der Entzug von Zugriffsrechten bei einem Wechsel oder Austritt nicht oder nur verzögert umgesetzt wird. Das Risiko unerlaubter Zugriffe auf sensible Datenbereiche und deren Missbrauch ist hoch.

Diese Problematik ist den meisten IT-Verantwortlichen bewusst, jedoch fehlen praktikable Lösungen und eine konsolidierte, belastbare Datenbasis. Die Folge: Regelmäßige Rechteüberprüfungen erfordern sehr hohen Aufwand und werden nicht ordnungsgemäß umgesetzt, obwohl gesetzliche Regularien wie MaRisk oder KRITIS dies vorschreiben.

4.2.2 Lösungsansätze mit OGiTiX unimate

OGiTiX unimate bietet hierfür eine einfache und schnell betriebsfertige Lösung: Automatisierte Prozesse fordern regelmäßig eine Rechtekontrolle von Vorgesetzten und Rollenverantwortlichen ein. In einem Webportal werden die Rechte pro Identität, also pro natürlicher Person, in einer Übersicht eingesehen, bestätigt und ggfs. entzogen.

Bidirektionale Schnittstellen zu bspw. Active Directory, SAP und weiteren Applikationen liefern dafür eine stets aktuelle und systemübergreifende Rechtedatenbank. Veränderte Berechtigungen werden zudem unmittelbar und automatisiert in den jeweiligen Zielsystemen umgesetzt. Anwendungen ohne technische Anbindung werden über Importfunktionen in die Rezertifizierung eingebunden.

Grafisch anpassbare Workflows steuern die Prozesse der Rezertifizierung. Neben den Aufgaben zur Rechtekontrolle werden Erinnerungen, Eskalationen, Genehmigungen, Ausnahmen und Benachrichtigungen flexibel geregelt.

Über das rollenbasierte Service-Portal können die Rezertifizierungen überwacht, ausgewertet und konfiguriert werden. Einzelne Rezertifizierungen pro Abteilung, Applikation, Rolle oder Identität können ebenfalls über die unimate Weboberfläche ohne IT-Know-how initiiert werden.

Die lückenlose und revisionssichere Protokollierung ermöglicht nicht nur Rechteberichte, sondern auch Kampagnenreports für Auditoren, Vorgesetzte oder Rollenverantwortliche auf Knopfdruck.

OGiTiX unimate - Rezertifizierung

- Automatische, zeitgesteuerte Re-Zertifizierungsprozesse
  - Aufbereitung der Benutzerkonten und Zugriffsrechte pro Person auf Basis der anwendungsübergreifende unimate Identitätsdatenbank
  - Zusendung einer Übersicht der zu re-zertifizierenden Zugriffsrechte an Vorgesetzte und/oder Rollen- bzw. Rechteverantwortliche
- Einforderung einer elektronischen Bestätigung der Rechtestrukturen
- Veränderungen werden dokumentiert und anschließend automatisiert umgesetzt
- Durchführungsnachweis über lückenlose Re-Zertfizierungsberichte

4.3 Sichere Vergabe und zeitliche Begrenzung von Administrationsrechten

4.3.1 Anforderungen & Ist-Situation

Die größten IT-Sicherheits-Bedrohungen für Unternehmen sind nicht etwa Angriffe von außen, sondern Aktivitäten, die sich im Inneren eines Netzwerkes abspielen. Die Gefahr geht speziell von Superusern oder Anwendern mit privilegierten Benutzerkonten aus, die administrative Rechte auf das Netzwerk, Datenbanken oder Applikationen haben.
Diese Anwender haben Zugriffe auf teils hochsensible Datenbereiche. Durch Missbrauch, Diebstahl oder menschliche Fehler können Unternehmen deshalb schweren Schaden nehmen. Folglich erfordern Sicherheitsvorgaben und gesetzliche Regularien wie MaRisk oder KRITIS die Absicherung und Auditierung privilegierter Zugriffsrechte:

- Administratoren & Superuser
- Remote Access Anwender
- Zugänge externer Dienstleister

4.3.2 Lösungsansätze mit OGiTiX unimate

OGiTiX unimate bietet hierfür eine einfache und sichere Lösung: Ein einfach zu bedienender Self-Service ermöglicht die Anforderung und automatisierte Freischaltung privilegierter Zugriffe in Echtzeit. In der produktiven Umgebung herrscht so mehr Sicherheit, da dauerhaft aktive administrative Zugriffe verzichtbar werden.
Flexibel anpassbare Workflows regeln den Prozess und ermöglichen die Integration von Genehmigungen oder Ausnahmen. So können Zugriffe für definierte Zeitfenster oder Anwendungen vollautomatisch freigeschaltet werden, die Anforderung längerer Nutzungszeiten oder spezieller Zugriffsrechte bedarf hingegen einer Genehmigung.
Über Schnittstellen zum Active Directory, SAP und weiteren Systemen schaltet OGiTiX unimate die angeforderten Zugriffe unmittelbar frei und deaktiviert diese nach Ablauf des Zeitfensters wieder – vollautomatisch und in Echtzeit!
Die lückenlose und revisionssichere Protokollierung ermöglicht Berichte auf Knopfdruck. So kann jederzeit der Verwendungsnachweis geführt werden, welche Person wann welche privilegierten Rechte mit welcher Begründung genutzt hat – Auditierbarkeit by Design.

Self-Service für zeitbeschränkte, privilegierte Benutzerkonten

- Privilegierte Konten werden nur bedarfsorientiert und zeitbegrenzt bereitgestellt
- Ein Self-Service ermöglicht die Anforderung und automatisierte Bereitstellung
- Die vorher erforderliche Authentifizierung und die Protokollierung ermöglichen den lückenlosen Nachweis, wer wann Zugriff auf welches privilegierte Konto hatte
- Optional mit elektronischer Genehmigung
- Die Automation sorgt für den Zugriff innerhalb weniger Minuten

4.4 Rollentrennung / Vermeidung kritischer Rechtekombinationen

4.4.1 Anforderungen & Ist-Situation

Das Risikomanagement nach bspw. MaRisk oder KRITIS fordert die Sicherstellung, dass Berechtigungskombinationen für miteinander unvereinbare Tätigkeiten vermieden werden. Ein praxistauglicher Ansatz zur Vermeidung solcher Kombinationen ist die Festlegung sogenannter SoD-Trennkriterien.
Man kann SoD-Trennkriterien als maximale Tätigkeitsbereiche auffassen, die vereinbar oder unvereinbar sein können. Die SoD-Trennkriterien werden in der sogenannten SoD-Matrix gegeneinander aufgetragen. Bilden zwei Trennkriterien eine kritische Kombination, wird der Schnittpunkt der entsprechenden Zeile und Spalte markiert und in einer sogenannten SoD-Regel beschrieben.

4.4.2 Lösungsansätze mit OGiTiX unimate

Die Herausforderung in der Praxis ist sicherzustellen, dass die SoD-Regeln auch im Zuge der Vergabe von Rollen und Berechtigungen befolgt werden. Erfolgen die Rechtevergabe und SoD-Prüfung manuell, so kann die Einhaltung der Rollentrennung nicht sichergestellt werden. Menschliche Fehler oder absichtlicher Missbrauch lassen sich nicht gesichert unterbinden.
Eine saubere Lösung besteht demnach aus verschiedenen Komponenten:

- **Durchgängige Prozesse im Berechtigungsmanagement**
- **Softwareseitige Abbildung und Prüfung der SoD-Matrix**
- **Automation der Benutzerkonten- & Rechte-Administration**

Automatisierte Prozesse im Berechtigungsmanagement

- Softwaregesteuerte Prozesse für das User- & Rechte-Management
  - Mitarbeiter-Eintritt (Identity Life-Cycle)
  - Mitarbeiter-Austritt (Identity Life-Cycle)
  - Mitarbeiter-Änderung (Identity Life-Cycle)
  - Nachversorgung mit Rechten (Self-Service & Approvals)
- Systembedingt, lückenlose Nachvollziehbarkeit
  - Vom Antrag über Entscheidungen bis zur technischen Umsetzung
- Jeder Prozessschritt wird den der IAM/BPM Software automatisch protokolliert
- Systemübergreifendes Datenmanagement im Prozesskontext

Softwareseitige Abbildung und Prüfung der SoD-Matrix

- Automatische Prozesse zur Überprüfung der SoD-Regeln
- Integriertes Eskalations- & Ausnahmen-Management
- Eliminierung von Fehler- & Missbrauchsquellen in der SoD-Pürfung
- Alarmierung bei der nachträglichen Erkennung kritischer Kombinationen

Automation der Benutzerkonten- & Rechte-Administration

- Bedarfsgerechte, automatisierte Umsetzung in den Zielsystemen
- Reduktion des Aufwandes und der Wartezeiten
- Eliminierung von Fehlerquellen in der Rechtevergabe

4.5 Risikomanagement/Blockabwesenheit

4.5.1 Anforderungen & Ist-Situation

Das Risikomanagement nach bspw. MaRisk oder KRITIS fordert bei vielen Unternehmen die Einhaltung einer sog. Blockabwesenheit. Für privilegierte Benutzerkreise wie Händler oder Administratoren müssen Organisationen sicherstellen, dass für einen definierten Zeitraum keinerlei Zugriffe auf IT-Systeme und Anwendungen bestanden.

In der Praxis ist dies ein manueller Prozess, der einerseits aufwendig und andererseits fehleranfällig ist. Die IT muss auf Anforderung den Rechteentzug umsetzen und den Nachweis über die Anmeldungen der User dokumentieren. Eine Auditierbarkeit kann nur mit viel Aufwand sichergestellt werden und menschliche Fehler führen zu Sicherheitslücken.

4.5.2 Lösungsansätze mit OGiTiX unimate

OGiTiX unimate bietet hierfür eine schnelle und betriebsfertige Lösung: Automatisierte Prozesse gewährleisten die Einhaltung der inaktiven Zeiten in der Blockabwesenheit durch eine systemseitige Sicherstellung von Technik und Prozess. Zudem sind lückenlose Protokolle jederzeit als Bericht abrufbar.

Über Schnittstellen zu bspw. Active Directory, SAP und weiteren Anwendungen aktiviert und deaktiviert unimate die relevanten Benutzerkonten und Zugriffsrechte automatisch. Auch die Überprüfung und der Nachweis der Anmeldungen der betreffenden Benutzer erfolgt automatisiert.

Die Prozesse der Blockabwesenheit lassen sich über grafisch konfigurierbare Workflows einfach anpassen. Erinnerungen, Eskalationen, Genehmigungen oder Benachrichtigungen werden so im Handumdrehen ergänzt oder angepasst.

Im unimate Service-Portal kann die Blockabwesenheit ohne jegliches IT-Know-how initiiert, verändert oder vorzeitig abgebrochen werden. Darüber hinaus kann der Prozess der Blockabwesenheit auch automatisch über die Anbindung an ein HR-System oder eine eingehende E-Mail initiiert werden.

Alle Prozesse werden lückenlos und revisionssicher protokolliert – natürlich auch inklusive aller technisch automatisierten Schritte. Im Service-Portal stehen auf dieser Grundlage sowohl Berichte auf Knopfdruck als auch interaktive Auswertungen zur Verfügung.

Blockabwesenheit inkl. Reporting

- E-Mail- oder Formularbasierter Start des Prozesses Blockabwesenheit
- Automatische und zeitgesteuerter Deaktivierung der Benutzerkonten des Mitarbeiters
- Bedarfsweise sind Änderungen und ein vorzeitiger Abbruch im lfd. Prozess möglich
- Sicherstellung und Nachweis der Einhaltung durch technische Prüfung
- Lückenlose Protokollierung über den gesamten Abwesenheitszeitraum
- Beendigung der Abwesenheit mit automatisierter Re-Aktivierung der Konten

5 Zusammenfassung und Empfehlung

Für Unternehmen die, auf Grund der erreichten Schwellwerte, als Kritis Unternehmen eingestuft sind, wird künftig die strategische Planung der Informationssicherheit als Teil einer IT-Strategie immer wichtiger werden, um auch künftig auf die Herausforderungen einer stetig zunehmenden Digitalisierung vorbereitet zu sein.

In diesem Zusammenhang ist eine Erhebung des Status quo der eingesetzten Systeme, Prozesse und Verfahren empfehlenswert, da mit Überschreitung des Schwellenwertes und der daraus folgenden Erklärung gegenüber dem BSI sofort die Anforderungen nach den §§ 8a und 8b BSIG hinsichtlich der Meldepflichten, Erreichbarkeiten und Maßnahmen zum Schutz der informationstechnischen Systeme greifen.

Identifiziert die Geschäftsleitung das Unternehmen als kritische Infrastruktur, ist dies dem BSI gemäß BSI-KritisV zu melden. Hierfür hält das BSI einen Registrierungsprozess vor, der jedoch zuvor notwendige Anpassungen der internen Organisationsstruktur sowie den Aufbau einer entsprechenden IT-Sicherheitsmanagementstruktur bedingt. U. a. sollten die notwendigen Zuständigkeiten und Verantwortlichkeiten geklärt sein, damit im Ernstfall alle notwendigen Schritte definiert und bekannt sind.

Überschreitet eine Kritische Infrastruktur den Schwellenwert in zwei aufeinander- folgenden Jahren, hat der Betreiber nachzuweisen, dass er die notwendigen „...angemessenen organisatorischen und technischen Vorkehrungen...“ zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse getroffen hat, „...die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind...“.

Der Nachweis ist gegenüber dem BSI zu führen. Dabei kommen Audits, Zertifizierungen usw. infrage. Der Gesetzgeber hat hierzu, wie oben schon genannt, die Möglichkeit branchenspezifischer Sicherheitsstandards vorgesehen. Diese können von der Branche erarbeitet und dem BSI auf Antrag zur Eignungsprüfung vorgelegt werden. Bestätigt das BSI die Eignung und weist der Betreiber im Rahmen eines Audits die Umsetzung dieses B3S nach, wird die Erfüllung der gesetzlichen Anforderungen angenommen.

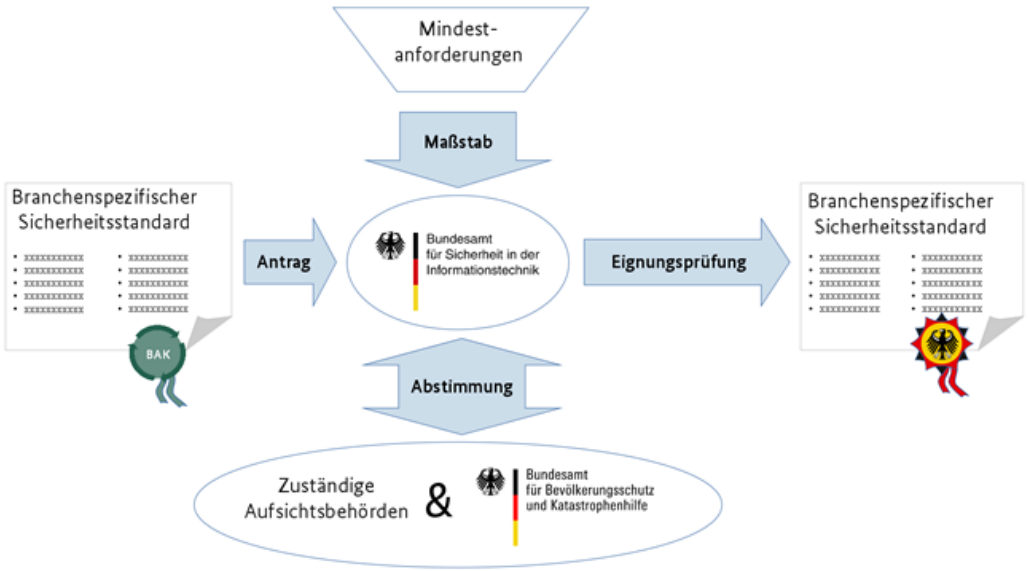


Abbildung 3: Eignungsprüfung für Branchenspezifische Sicherheitsstandard (B3S)

Der einzelne Betreiber wird mit dieser Verordnung relative allein gelassen, wenn keine branchenspezifischen Sicherheitsstandards von einem Dachverband erarbeitet und von der zuständigen Aufsichtsbehörde des Bundes anerkannt wurde. Es wird dann, wie so oft, auf den „Stand der Technik" verwiesen, dies ist im üblichen Sinne ein Abwägen zwischen Nutzen (Schutz) und Aufwand.

Allerdings wird diese Vorgabe um folgende Aussage ergänzt: „Bei der Beurteilung der Angemessenheit von Maßnahmen müssen stets die Folgen eines potentiellen Ausfalls für das Gemeinwohl (Wirtschaft, Staat und Gesellschaft) betrachtet werden. Aufgrund der besonderen Bedeutung der Kritischen Infrastrukturen für das Gemeinwohl ist eine rein betriebswirtschaftliche Kosten-Nutzen-Betrachtung der Maßnahmen nicht angemessen."

Hieraus resultieren die oben genannten Maßnahmen, welche branchenübergreifend zur Anwendung kommen und zusätzlich die Grundforderung zur Einführung eines Identitäten- und Rechtemanagements erfüllt. Diese Grundforderung ist durch aus logisch, da die oben genannten Lösungsansätze alles Merkmale einer modernen Indentity & Access Manangement-Lösung sind.

6 Anhang

6.1 Referenzierte Dokumente

ID	Dokument	Version	Datum	Autor
1	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT- SiG)	1.0	2015-07-17	Bundesregierung
2	KRITIS-Sektor Studie Informationstechnik und Telekommunikation (IKT)	1.0	2015-02-05	BSI
3	BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)	1.5	2017	BSI
4	BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise	2.0	2017	BSI
5	BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz	2.0	2017	BSI

WIR SIND IAM

SEIT ÜBER 15 JAHREN LEBEN UND ENTWICKELN WIR IAM-LÖSUNGEN FÜR SIE!

WIR ÜBERZEUGEN SIE GERNE:

MAIL TO

WEB-SEMINARE

UNSERE KUNDEN BERICHTEN:

KUNDENBERICHTE

Imprivata OGiTiX GmbH
(vormals OGiTiX Software AG)
Hans-Böckler-Str. 12
40764 Langenfeld
Deutschland

Fon +49 2173 99385-0
Fax +49 2173 99385-900
Mail info@ogitix.de
Web www.ogitix.de

Vertretungsberechtigt:
Geschäftsführer Ingo Buck,
Jeffrey Kowalski

Amtsgericht Düsseldorf
Nummer: HRB 100306
Sitz der Gesellschaft:
Langenfeld