TeleTrusT
Pioneers in IT security.

Informationstag "Ersetzendes Scannen"

Berlin, 19.04.2013

"Schutzbedarfsanalyse, Bedrohungsanalyse, Risikoanalyse - Was versteckt sich dahinter?"

Peter Zech, AuthentiDate

AuthentiDate Member of exceet

AuthentiDate International AG

- Gegründet im Jahr 2000 als Aktiengesellschaft (Sitz Düsseldorf, Deutschland)
- Akkreditierter Zertifizierungsdiensteanbieter seit Nov. 200 durch hochperformante Bereitstellung von qualifizierten Zeitstempeln
- Trust Center gemäß Signaturgesetz
- AuthentiDate Deutschland GmbH: Tochtergesellschaft für Produkte, Services & Beratungsdienstleistungen

exceet Group S.E.

- Muttergesellschaft der AuthentiDate International AG (Sitz St. Gallen, Schweiz)
- Weltweit ca. 1000 Mitarbeiter
- Geschäftsbereiche
  - **ECMS: Electronic Components Modules & Systems**
    Integrierte elektronische Produkte; z.B. miniaturisierte Elektroanwendungen, flexible und starre Leiterplatten
  - **IDMS: ID Management & Systems**
    Entwicklung und Herstellung von Smart Cards & Kartenlesern
  - **ESS: Embedded Security Solutions**
    Software, Services (Cloud Services) und Consulting für sichere Geschäftsprozesse

Geschäftsbereiche

Secure IT

Beratungsdienstleistungen

- Security Solutions
  - Individuelle Softwarelösungen
  - Integration von Hardware Security Modulen
  - Sicherheit in Telematik-Infrastrukturen
- Governance, Risk & Compliance
  - Datenschutz & Informationssicherheit (ISMS)
  - IT-Grundschutz & Risikomanagement
  - Zertifizierungsbegleitung und –vorbereitung
- Penetration-Testing
  - Individuelle Schwachstellenscans
  - Penetrationstests
  - Technische Audits

Secure Data Exchange

für sichere, gesetzeskonforme Geschäftsprozesse

- Cloud Services:
  - Erstellung qualifizierter Signaturen und Zeitstempel
  - Signatur- und Zeitstempelprüfung
  - Daten- und Formatkonvertierung
  - Revisionssichere Archivierung
- Rechtssicherer Eingangsstempel
- Revisionssichere Langzeitarchivierung
- Richtlinienkonforme eInvoicing-Prozesse
- Business Process Management

signamus
Secure Data Exchange

Secure eHealth

Alle Produkte & Leistungen sind auch speziell für die Gesundheitsindustrie verfügbar

Peter Zech – Wer ich bin? Was mache ich?

- Senior IT-Security Consultant
- Mitglied des Competence Center „Governance, Risk & Compliance“
- Tätigkeitsschwerpunkte
  - Informationssicherheits-Managementsysteme (Erstellung und Pflege)
  - Risikomanagement
  - Compliance
  - Business Continuity Management
  - Zertifizierungsbegleitung

Branchenschwerpunkte

- Gesundheitsindustrie (Kostenträger, Leistungserbringer)
- Finanzindustrie (Banken, Versicherungen)
- Dienstleister

AuthentiDate®

Schutzbedarfsanalyse, Bedrohungsanalyse, Risikoanalyse

Was steckt dahinter?

Schutzbedarfsanalyse

- Welche Daten werden verarbeitet?
- Mit welchen Konsequenzen muss bei unautorisierter Veröffentlichung, Beschädigung oder Verlust (d.h. Beeinträchtigung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit) der Daten gerechnet werden?

- **Problem**: Schutzbedarf in der Regel nicht genau quantifizierbar bzw. Bestimmung akkurater Werte zu aufwändig.

- **Lösung**: Anwendung einer nachvollziehbaren Methode.
  1. Bildung von Schutzbedarfsklassen (normal, hoch, sehr hoch [vgl. BSI-Grundschutz])
  2. Höhe des Schutzbedarfs wird durch Abschätzung der Höhe des potenziellen Schadens durch Verlust eines Schutzziels bestimmt
  3. Vereinfachung durch Festlegung vordefinierter Schadenskategorien

Vordefinierte Schadenskategorien

- Verstoß gegen allgemeine Gesetze und Vorschriften (inkl. Personenschäden);
- Verstoß gegen das Bundesdatenschutzgesetz (BDSG);
- Verstoß gegen Verträge;
- Beeinträchtigung der Aufgabenerfüllung;
- Negative Innen- bzw. Außenwirkung;
- Finanzielle/Wirtschaftliche Schäden.

Schadenschwere am Beispiel „Verstoß gegen Verträge“

Schadensschwere	Beschreibung
Kein Schaden	Ein Verstoß würde gegenwärtig nicht mit einem relevanten Schadensereignis verbunden sein. ODER Ein Schaden dieser Kategorie ist auf das Objekt der Betrachtung nicht anwendbar.
Mittel	Ein Verstoß wäre eine Vertragsverletzung, die mit maximal mittleren wirtschaftlichen bzw. finanziellen Schäden verbunden wäre: Wegen fehlender Nacherfüllung oder fruchtlosem Ablauf einer Nachfrist Rücktrittsrecht (§§ 323, 324 BGB) vom Vertrag und Anspruch auf Schadensersatz (§§ 280, 281, 282, 283 BGB = positives Interesse) wegen Pflichtverletzung, Aufwendungsersatzanspruch (§ 284 BGB = negatives Interesse).
Hoch	Ein Verstoß wäre eine Vertragsverletzung, die mit hohen wirtschaftlichen bzw. finanziellen Schäden verbunden wäre. Durch den Verstoß kann es zum Rücktritt vom Vertrag (§§ 323, 324 BGB) kommen, der Schadensersatzansprüche nach § 280 BGB zur Folge hätte.
Sehr hoch	Durch den Verstoß könnten Schadensersatzansprüche nach § 280 BGB geltend gemacht werden: Haftung wegen Verletzung vertraglicher oder gesetzlicher Verpflichtungen. Der Zustand, der bestehen würde, wenn der zum Ersatz verpflichtende Umstand nicht eingetreten wäre, ist nur mit sehr hohem Aufwand herzustellen (vgl. § 249 BGB), der die jeweils vertraglich vereinbarte Haftungsbeschränkung erreicht.

Schutzbedarfsfeststellung am Beispiel „personenbezogene medizinische Daten“

Schadenskategorie	SZ: Vertraulichkeit	SZ: Integrität	SZ: Authentizität
Verstoß gegen allgemeine Gesetze und Vorschriften	sehr hoch	sehr hoch	sehr hoch
Verstoß gegen BDSG	hoch	hoch	hoch
Verstoß gegen Verträge	nicht anwendbar	nicht anwendbar	nicht anwendbar
Beeinträchtigung der Aufgabenerfüllung	nicht anwendbar	mittel	mittel
Negative Innen- bzw. Außenwirkung	sehr hoch	sehr hoch	sehr hoch
Finanzielle Auswirkungen	sehr hoch	sehr hoch	sehr hoch
Gesamtbewertung	**sehr hoch**	**sehr hoch**	**sehr hoch**

Drei Beispiele von Schutzwerten

- Weitere Sicherheitsziele sind: Vollständigkeit, Nachvollziehbarkeit, Verfügbarkeit, Lesbarkeit, Verkehrsfähigkeit, Löschbarkeit

Bedrohungsanalyse

- Welche Schwachstellen existieren in der Organisation?
- Welche Gefährdungen sind realistisch?
- Wie bestimme man, welche Werte durch welche Gefährdungen bedroht sind?

- **Problem**: Vielzahl möglicher Ursachen, Schwachstellen, Gefahren lassen Bedrohungsanalyse komplex werden, wodurch kritische Bedrohungen „vergessen“ werden können.

- **Lösung**: Anwendung einer nachvollziehbaren Methode
  1. Identifizierung möglicher Bedrohungen
  2. Bestimmung möglicher Schwachstellen
  3. Identifizierung möglicher Angreifer und Motive
  4. Bestimmung der Angriffsszenarien
  5. Ermittlung des Angriffspotentials

Identifizierung möglicher Bedrohungen

- Eine Bedrohung besteht neben einer Ursache immer auch aus einer Aktion auf ein Asset
- Anwendung des Katalogs G0 aus IT-Grundschutz
  - Ursachen: Außeneinwirkung, Elementarereignis, Mensch, Technisches Versagen
  - Assets: Informationen, Datenträger, Hard-/Software, Prozesse, ...
  - Aktionen: Löschen, Kenntnisnahme, Überlastung, Verhinderung, ...

Asset	Bedrohung (Aktionen)
Informationen	Löschen, Kopieren, Modifizieren, Kenntnisnahme Veröffentlichung
Hardware/Software	Modifizieren, Entfernen, Zerstörung, Ausfall, Außerbetriebnahme, Überlastung, Unberechtigte Nutzung
Prozesse	Verändern Unbefugtes Ausführen Verhinderung

Bestimmung möglicher Schwachstellen

- Damit ein Schaden entsteht, muss eine Bedrohung eine Schwachstelle ausnutzen.
- Möglicher Schwachstellentypen: Technisch, organisatorisch, menschliches Fehlverhalten.

Schwachstelle - Typ	Ausprägung
Technisch	Konträre fachliche Anforderung, Konzeptionsfehler, Designfehler, Programmierfehler, Konfigurationsfehler, Mangelnde Resistenz der Hardware, Mangelnde physische Sicherheit der Umgebung
Organisatorisch	Fehlerhafte Verfahrensumsetzung, Fehlerhafte Rollen- oder Rechtezuweisung, Unzureichende Koordination und Kooperation
Menschliches Fehlverhalten	Offenheit für Social Engineering, Mangelnde Kenntnis, Mangelnde Sorgfalt, Fahrlässigkeit, Fehlbarkeit

Identifizierung möglicher Angreifer und Motive

- **Angreifer**
  - Innentäter (Benutzer, Administrator, Entwickler)
  - Außentäter
- **Motive**
  - Schaden anrichten,
  - Bereicherung,
  - Aufsehen erregen,
  - Vertuschung,
  - Bequemlichkeit,
  - mangelnde Kenntnis,
  - Irrtum
- **Physikalischer Prozess**

  (Umwelteinfluss, Defektes Bauteil, Überhitzung, ...)

Risikoanalyse

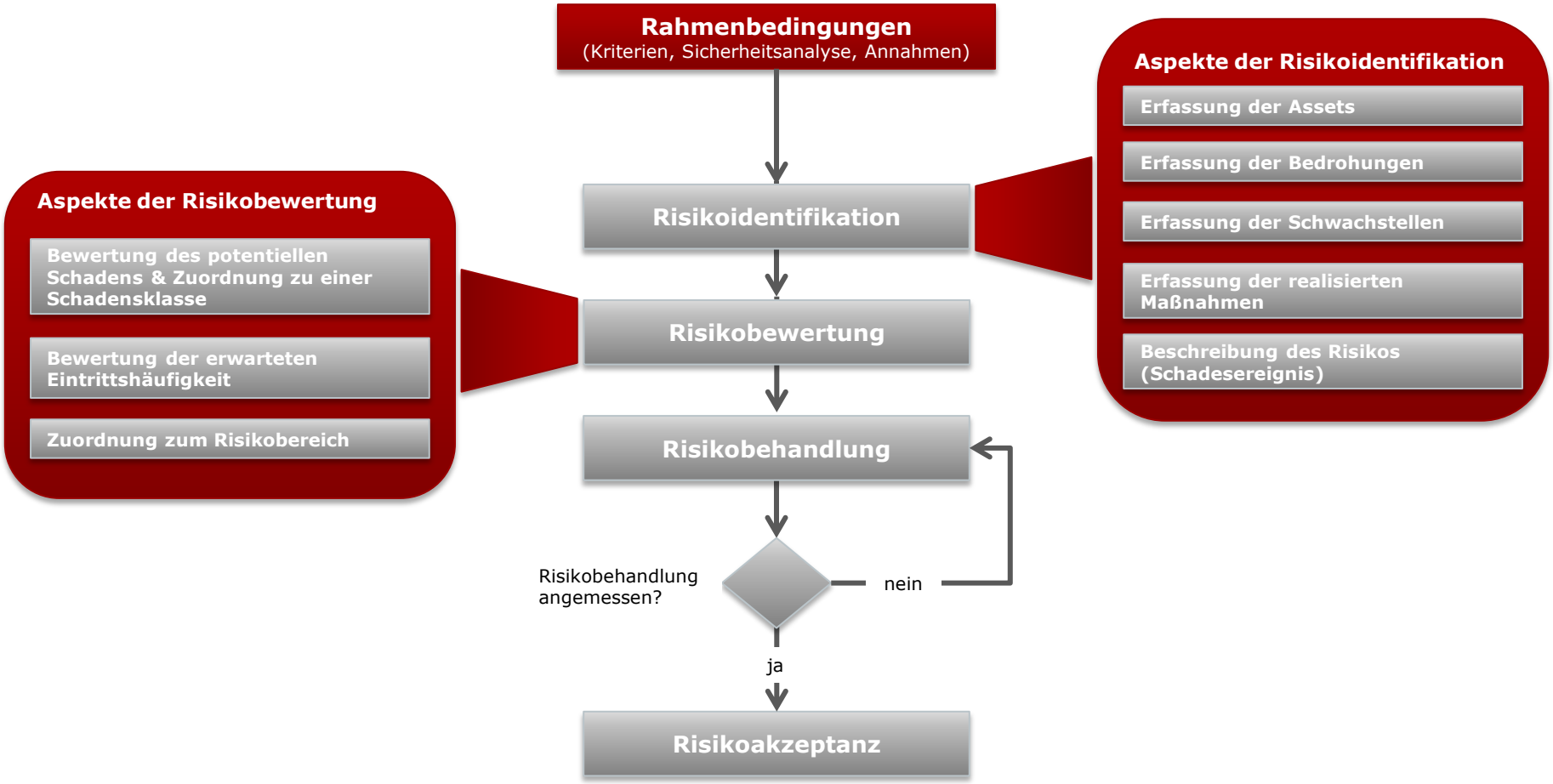
- Welche Schadensereignisse können eintreten und wie oft?
- Wie hoch wäre der Schaden?
- Wie kann man dem Schadensereignis am besten entgegentreten?

- **Definition**: Ein Risiko besteht immer dann, wenn ein Asset eine Schwachstelle aufweist, die durch eine Bedrohung ausgenutzt werden kann.

- **Problem**: Ermittlung geeigneter Maßnahmen im Rahmen des Risikomanagements.

- **Lösung**: Anwendung einer nachvollziehbaren Methode
  1. Risikoidentifikation
  2. Risikobewertung
  3. Risikobehandlung
  4. Restrisikoakzeptanz

Ablauf Risikoanalyse



Risikoidentifikation

- Feststellung und Dokumentation potentieller Risiken in folgender Art und Weise:

  Weil
  < die folgende Situation besteht: Asset, Schwachstelle, und/oder Bedrohung > besteht das Risiko, dass
  <der folgende Schaden eintreten kann>

  ➡ Die Risiken werden aus den in der Bedrohungsanalyse ermittelten Angriffsszenarien abgeleitet

Beispiel:
Weil…

die **Rechtevergabe für Benutzer nicht zentral verwaltet wird** und durch **Fahrlässigkeit der Administratoren** falsche Rechte vergeben werden, besteht das Risiko, dass Benutzer privilegierte Zugriffsrechte erhalten und damit die **Funktionstüchtigkeit von IT-Systemen beeinträchtigen** können.

Risikobewertung (Schadensklassen)

- Schätzung der Schadensschwere und der Eintrittshäufigkeit.
  Schadensschwere x Eintrittshäufigkeit = Risikobereich (blau, grün, gelb, rot) des Risikos.
- Bewertung des potentiellen Schadens, Zuordnung zu einer Schadensklasse und Bewertung der erwarteten Eintrittshäufigkeit.
- Festlegung von Schadensklassen:

Schadens-klasse	Beschreibung
SK1	Es ist ein niedriger Schaden zu erwarten, der sich höchstens auf einzelne Assets auswirken würde.
SK2	Es ist ein niedriger Schaden zu erwarten, der sich jedoch auf sehr viele oder möglicherweise alle Assets auswirken würde. ODER Es ist ein mittlerer Schaden zu erwarten, der sich jedoch höchstens auf einzelne Assets auswirken würde.
SK3	Es ist ein mittlerer Schaden zu erwarten, der sich auf sehr viele oder möglicherweise alle Assets auswirken würde. ODER Es ist ein hoher Schaden zu erwarten, der sich aber höchstens auf einzelne Assets auswirken würde.
SK4	Es ist ein hoher Schaden zu erwarten, der sich auf sehr viele oder möglicherweise alle Assets auswirken würde. ODER Aus dem Eintritt des Risikos ist ein sehr hoher Schaden zu erwarten.

Risikobewertung (Schadenspotential & EHK)

- Zuordnung der Schadenspunkte zu den Schadensklassen zur Berechnung der Risikolevel.

Schadensschwere pro Asset/Akteur	Schadensklassen (Schadenspunkte)	
Niedrig	1 (10)	2 (100)
Mittel	2 (100)	3 (1000)
Hoch	3 (1000)	4 (10000)
Sehr hoch	4 (10000)	4 (10000)
	Einzelnes Asset/Akteur	Sehr viele/alle Assets/Akteure

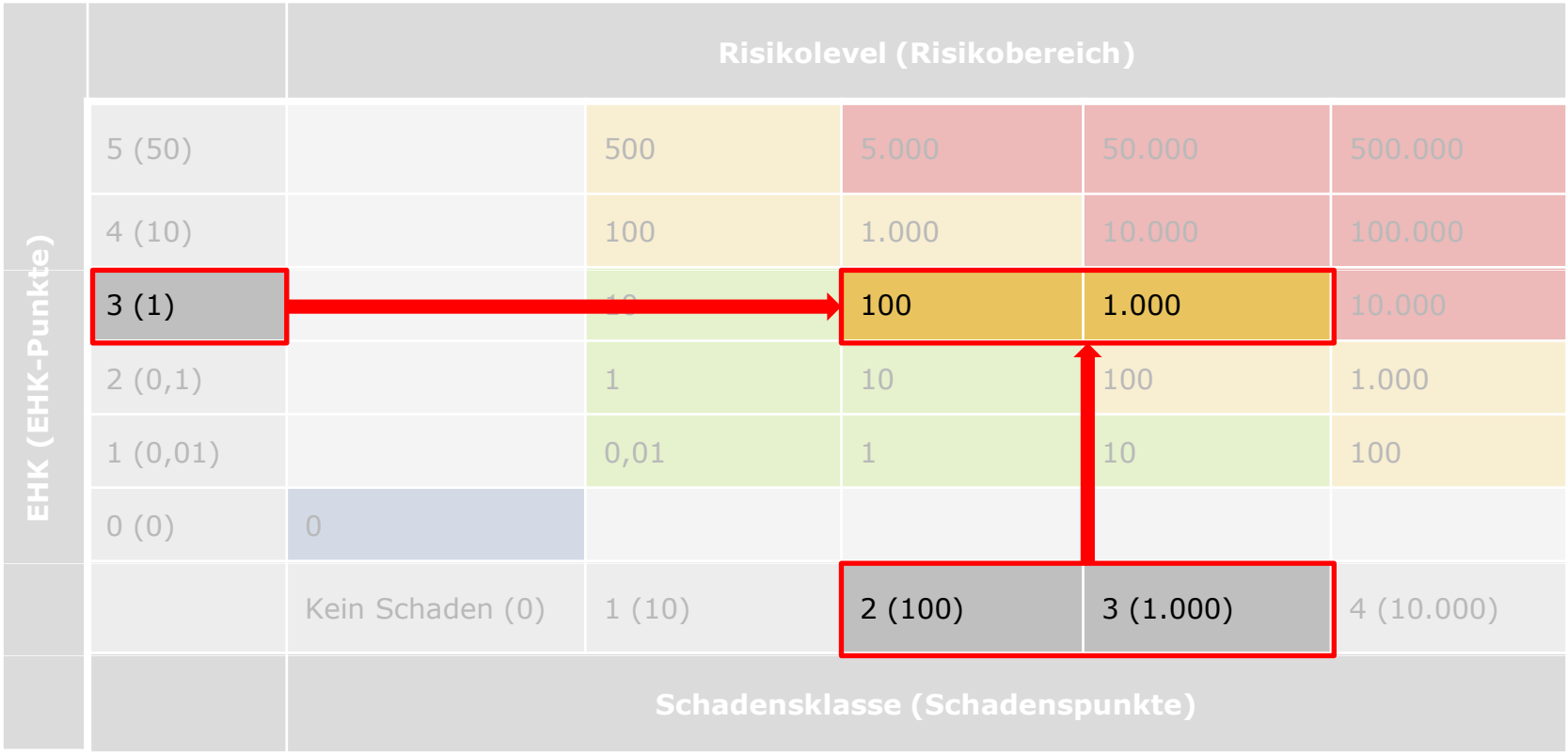
- Festlegung der Eintrittshäufigkeitsklassen (EHK-Klassen) zur Bewertung der Eintrittswahrscheinlichkeit und Kennzeichnung mit Eintrittshäufigkeitspunkten zur späteren Berechnung der Risikolevel.

Eintrittshäufigkeit	Beschreibung	EHK-Klasse	EHK-Punkte
sehr selten	Eintritt wird einmal alle 100 Jahre erwartet.	1	0,01
selten	Eintritt wird einmal alle 10 Jahre erwartet.	2	0,1
gelegentlich	Eintritt wird einmal pro Jahr erwartet.	3	1
häufig	Eintritt wird einmal pro Monat erwartet.	4	10
sehr häufig	Eintritt wird einmal pro Woche erwartet.	5	50

Risikobewertung (Zuordnung)

EHK (EHK-Punkte)		Risikolevel (Risikobereich)				
	5 (50)		500	5.000	50.000	500.000
	4 (10)		100	1.000	10.000	100.000
	3 (1)		10	100	1.000	10.000
	2 (0,1)		1	10	100	1.000
	1 (0,01)		0,01	1	10	100
	0 (0)	0				
		Kein Schaden (0)	1 (10)	2 (100)	3 (1.000)	4 (10.000)
		Schadensklasse (Schadenspunkte)				

Risikobewertung (Zuordnung)



Weil die **Rechtevergabe für Benutzer nicht zentral verwaltet wird** und durch **Fahrlässigkeit der Administratoren (Häufigkeit = EHK 3)** falsche Rechte vergeben werden, besteht das Risiko, dass Benutzer privilegierte Zugriffsrechte erhalten und damit die **Funktionstüchtigkeit von IT-Systemen beeinträchtigen (Schadensklasse 2/3)** können.

Risikobehandlung

- Festlegung des Umgangs mit dem bestehenden Risiko:
  - Akzeptieren,
  - Vermeiden,
  - Reduzieren oder
  - Transferieren.

- Wird das Risiko als nicht akzeptabel eingeschätzt, so müssen Maßnahmen vorgeschlagen werden, wie mit dem Risiko verfahren werden soll.

Beispiele:

- Vermeidung: Deaktivierung des IT-Systems bzw. Isolation des IT-Systems (Trennen vom Netzwerk) / Einstellen des Prozesses
- Reduktion: Identifikation und Umsetzung wirksamer Schutzmaßnahmen, Outsourcing
- Transfer: Versicherung abschließen

Restrisikoakzeptanz

- Das verbleibende Restrisiko wird formal dokumentiert. Sollte das Restrisiko von den Entscheidungsträgern als nicht tragbar eingeschätzt werden, so muss der Prozessschritt der Risikobehandlung erneut durchlaufen werden.

Kontakt

AuthentiDate International AG
Rethelstraße 47
40237 Düsseldorf

Peter Zech
Fon: +49 211 436989-0
E-Mail: peter.zech@authentidate.de

www.authentidate.de | www.signamus.de | www.signature-check.de