Risikomanagement

zum DSFA-Bericht

Personal verwalten

(Dok-ID: 353535 / Dok-ID des DSFA-Berichts: 222222)

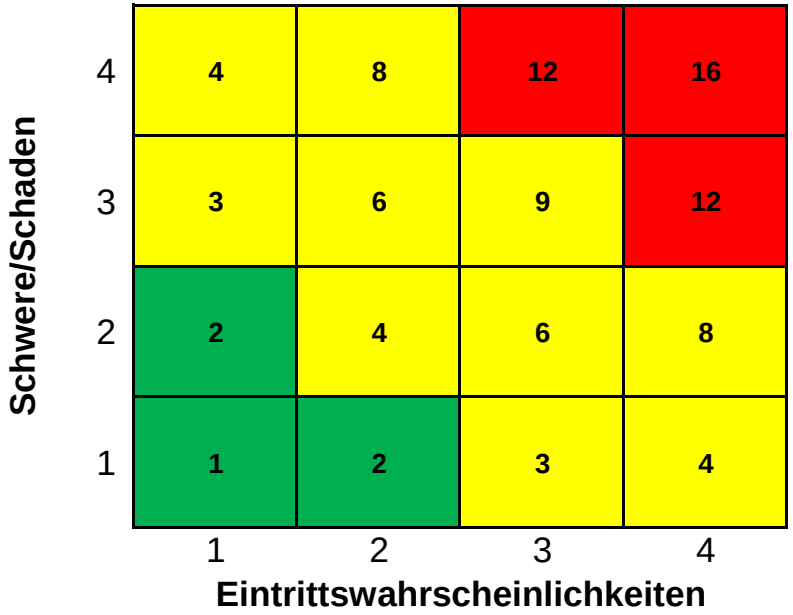
Inhalt:

Änderungshistorie

Wann?	Wer?	Was?
15.03.19	Bauer, Berta	Initialer Entwurf

Legende

1. Risikomatrix für die Indexierung der Risiken



Index	Bezeichnung Risikoindex
	geringes Risiko
	Risiko
	hohes Risiko

2. Eintrittswahrscheinlichkeit

Grad	Bezeichnung des Grads	Eintrittswahrscheinlichkeit	
		Beschreibung	Beispiel
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.
3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und direkt mit dem Internet verbunden ist.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem veralteten Windows-XP Rechner ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

3. Schwere/Schaden

Grad	Bezeichnung des Grads	Schwere der Folgen / möglicher Schaden	
		Beschreibung	Beispiel
1	geringfügig	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.	**immateriell:** leichte Verärgerung **materiell:** Zeitverlust **physisch:** vorübergehende Kopfschmerzen
2	überschaubar	Betroffene erleiden eventuell signifkante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.	**immateriell:** geringe, aber objektiv nachweisbare psychische Beschwerden **materiell:** deutlich spürbarer Verlust an privatem Komfort **physisch:** minderschwere körperliche Schäden (z. B. leichte Krankheit)
3	substanziell	Betroffene erleiden eventuell signifkante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	**immateriell:** schwere psychische Beschwerden **materiell:** finanzielle Schwierigkeiten **physisch:** schwere körperliche Beschwerden
4	groß	Betroffene erleiden eventuell signifkante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.	**immateriell:** dauerhafte, schwere psychische Beschwerden **materiell:** erhebliche Schulden **physisch:** dauerhafte, schwere körperliche Beschwerden

Verfügbarkeit

Gewährleistungsziel	Summarische Risikobetrachtung	Index
Verfügbarkeit	**Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.**	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
VB.1	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	IT-Fehlfunktion	Hard- und/oder Software-Fehlfunktion führen dazu, dass erforderliche digitale Daten unwiederbringlich verloren gehen.	Aufgrund der Komplexität des HCM-Systems (zahlreiche, zusammenwirkende Komponenten, häufige Updates usw.) ist ein Datenverlust durch IT-Fehlfunktionen sehr wahrscheinlich.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	8	M.1 Basis Backup-Struktur nutzen M.2 Dienstleistungsangebot HCM-Hersteller nutzen	Datenverluste bei von der Stadt betriebenen Systemen, die mit dem HCM-System vergleichbar sind, gehen gegen Null.	gr
VB.2	= VB.1 =	Interner User	User-Interaktionen mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Aufgrund der angespannten Personalsituation werden teilweise auch noch sehr unerfahrene HCM-Sachbearbeiter eingesetzt.	2	Fehlbedienungen von internen Usern, die zu einem Datenverlust führen (z.B. Daten versehentlich überschreiben), sind punktuell und werden i.d.R. rasch erkannt und wieder berichtigt.	2	4	M.1 Basis Backup-Struktur nutzen M.3 Löschberechtigung restriktiv vergeben M.4 HCM-Benutzer schulen	Die Maßnahmen zusammen führen zu einer deutlich reduzierten Eintrittswahrscheinlichkeit.	gr
VB.3	= VB.1 =	Externer User	Interaktionen externer User (z.B. Finanzprüfer, Auditoren) mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Zugriffe externer User auf das produktive HCM-System finden nur selten statt.	2	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	4	M.5 Lesenden Zugriff für berechtigte Dritte konfigurieren	Fehlbedienungen von externen Benutzern, die zu einem Datenverlust führen, sind nicht vorstellbar, da solche Benutzer stets nur mit Leserechten ausgestattet sind (bewährtes Standardbenutzerprofil).	gr
VB.4	= VB.1 =	Interner Administrator	Interaktionen eines User mit weitreichenden Administratorenrechten mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Da es das Alltagsgeschäft von Administratoren ist, mit produktiven IT-Systemen richtig umzugehen, ist der Eintritt unwahrscheinlich.	2	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	4	M.1 Basis Backup-Struktur nutzen M.3 4-Augen-Prinzip für tragende Personaldatenänderungen umsetzen M.6 HCM-Administratoren zertifizieren	Blickt man auf die schon lange aktive Administrationstätigkeit mit Umsetzung der Maßnahmen zurück, so erscheint der Eintritt als sehr unwahrscheinlich.	gr
VB.5	= VB.1 =	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware gehen erforderliche Daten unwiederbringlich verloren.	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	8	M.7 Basis Schadsoftware-/ Hackerabwehrsystem nutzen M.1 Basis Backup-Struktur nutzen	Datenverluste bei ebenfalls betriebenen IT-Systemen, die mit dem HCM-System vergleichbar sind, sind entsprechend eingestuft. Bzgl. HCM-System sind keine Besonderheiten erkennbar.	ge
VB.6	Monatlichen Gehaltsabrechnung kann nicht rechtzeitig durchgeführt werden	Interner User	Fehlendes, nicht mittelfristig ersetzbares Personal bringt monatliche Personalabrechnung zum Stehen.	Altersstruktur des betroffenen Personals und relativ hohe Fluktation von Experten im HCM-Umfeld verschärfen die Situation.	4	Falls die Entgeltabrechnung nicht ordnungsgemäß läuft, kann dies zu ernsthaften finanziellen Schwierigkeiten der Beschäftigten führen.	3	12	M.8 Kopfmonopole mittels Teambildung reduzieren M.9 Dienstleistung Dritter nutzen M.10 Manuelle Abschlagzahlung	Trotz der ergriffenen Maßnahmen für die aktive und passive Risikobewältigung kann das Risiko nicht in den grünen Bereich gebracht werden.	ge
VB.7	= VB.6 =	IT-Fehlfunktion	*noch weiter zu ergänzen*	usw.	1	usw.	3	3	usw.	usw.	ge

Vertraulichkeit

Gewährleistungsziel	Summarische Risikobetrachtung	Index
Vertraulichkeit	**Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.**	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
VT.1	Personen können unmittelbar unbefugt auf digitale HCM-Daten zugreifen	IT-Fehlfunktion	Aufgrund eines Hard- und/oder Softwarefehlers (z.B. Fehler in Berechtigungsmanagementfunktion) können städtische Beschäftigte unbefugt durch das IT-Personalwirtschaftssystem HCM-Fiktivia auf HCM-Daten zugreifen.	Nach den bisher gemachten Erfahrungen ist HCM-Fiktivia so ausgereift, dass eine derartige unbefugte Datenoffenlegung sehr unwahrscheinlich ist.	2	Städtische Beschäftige sind zur Verschwiegenheit und zur Meldung solcher Fehlfunktionen verpflichtet.	1	2	---	---	gr
VT.2	= VT.1 =	Internes Personal	Das Rollen- und Berechtigungskonzept weist Fehler auf oder die aktuelle Konfiguration ist veraltet.	Bei der Berechtigungskonfiguration können leicht Fehler passieren. Bei einem Beschäftigtenwechsel werden nicht immer zeitnah die Berechtigungen angepasst.	4	Städtische Beschäftige sind zur Verschwiegenheit und zur Meldung solcher Fehlfunktionen verpflichtet.	1	4	M.29 Rollen- und Berechtigungskonzept umsetzen M.11 Berechtigungskonfiguration testen M.12 Identity Management (IdM) umsetzen	Bei der Komplexität der Berechtigungs-verwaltung im HCM-System muss dieses Einzelrisiko stets im Fokus bleiben.	ge
VT.3	= VT.1 =	Interner User	Beim Verlassen des Arbeitsplatzes wird dieser nicht gesperrt, so dass andere Personen unbefugt Einblick in HCM-Daten erhalten können.	Das Sperren des IT-Arbeitsplatzes beim Verlassen ist noch nicht zur Selbstverständlichkeit geworden	2	Neben anderen städtischen Beschäftigten ist auch eine Kenntnisnahme Dritter möglich, die zu weiterführenden Unanehmlichkeiten der betroffenen Person(en) führen kann.	3	6	M.13 Städtischen Beschäftigten durch Dienstanweisung sensibilisieren M.14 IT-Arbeitsplatz wird automatisiert gesperrt	Durch das technsich organisatorische Maßnahmenbündel kann von einer deutlichen Reduzierung des Einzerisikos ausgegangen werden.	gr
VT.4	= VT.1 =	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware wird unbefugt auf die Daten zugegriffen.	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4	Die Kenntnisnahme krimineller Dritter kann zu weiterführenden Unanehmlichkeiten der betroffenen Person(en) führen.	3	12	M.7 Basis Schadsoftware-/ Hackerabwehrsystem nutzen	Angriffsrisiko bei anderen betriebenen IT-Systemen, die mit dem HCM-System vergleichbar sind, ist entsprechend eingestuft.	ge
VT.5	Personen können unmittelbar unbefugt auf papiergebundene Personalakten zugreifen	Internes Personal	Eine unbefugte Person erhält Aktenzugriff über das Aktenarchiv, den Aktentransport oder den Arbeitsplatz eines Beschäftigten, der befugt Zugriff auf die betroffene Akte hat.	Das Aktenverwaltungs- und Aktenverteilungssystem hat sich schon lange bei der Stadt bewährt und ist hinsichtlich seiner Sichheit ausgereift.	1	Neben anderen städtischen Beschäftigten ist auch eine Kenntnisnahme Dritter möglich, die zu weiterführenden Unanehmlichkeiten der betroffenen Person(en) führen kann.	3	3	---	---	ge
VT.6	Personen können mittelbar unbefugt auf digitale HCM-Daten zugreifen	~ Internes Personal ~ IT-Fehlfunktion	Aufgrund eines menschlichen Versehens oder eines Hard- und/oder Softwarefehlers (z.B. Fehler in Schnittstelle) werden Daten an einen falschen Empfänger übermittelt.	Insbesondere bei der allgemeinen Bürokommunikation (z.B. Brief, Fax) kam es in der Vergangenheit zu Fehladressierungen.	3	Neben anderen städtischen Beschäftigten ist auch eine Kenntnisnahme Dritter möglich, die zu weiterführenden Unanehmlichkeiten der betroffenen Person(en) führen kann.	3	9	M.15 Dienstanweisung für die Übermittlung personenbezogener Daten umsetzen M.16 Internen Meldeprozess für Datenschutz-Verstöße implementieren	Nach Wirksamkeit der Maßnahmen kann dieses Einzelrisiko zwar deutlich reduziert, nicht aber aus der ständigen Sensibilisierung genommen werden.	ge
VT.7	= VT.6 =	Internes Personal	Datenträger mit Personaldaten geht verloren	Zahlreiche Beschäftige verfügen über ein dienstliches Laptop, das mit einem Verlustrisiko verbunden ist	3	Neben anderen städtischen Beschäftigten ist auch eine Kenntnisnahme Dritter möglich, die zu weiterführenden Unanehmlichkeiten der betroffenen Person(en) führen kann.	3	9	M.17 Nur verschlüsselte Datenträger verwenden M.18 Datenexport auf das Notwendige beschränken	Durch die technische Maßnahmen gelangt das Einzelrisiko in den grünen Bereich	gr
VT.8	Personen können mittelbar unbefugt auf papiergebundene HCM-Daten zugreifen	Internes Personal	Person kann auf Auszüge aus einer Personalakte unbefugt zugreifen	Posteingang- und Postauslauf geht oft über verschiedene Arbeitsplätze. Zudem werden Kopien relevanter Dokumente und Nebenakten angefertigt.	3	Neben anderen städtischen Beschäftigten ist auch eine Kenntnisnahme Dritter möglich, die zu weiterführenden Unanehmlichkeiten der betroffenen Person(en) führen kann.	3	9	M.19 Beteiligungen am Posteinlauf und Postauslauf auf das Notwendige beschränken M.20 Beschäftige bzgl. der Anfertigung von Kopien sensibilisieren M.21 Thema "Führung von Nebenakten" in die Fortbildung für Führungskräfte mit aufnehmen	Nach Wirksamkeit der Maßnahmen kann dieses Einzelrisiko zwar deutlich reduziert, nicht aber aus der ständigen Überwachung genommen werden.	ge
VT.9	= VB.6 =	IT-Fehlfunktion	*noch weiter zu ergänzen*	usw.	1	usw.	3	3	usw.	usw.	ge

Datenintegrität

Gewährleistungsziel	Summarische Risikobetrachtung	Index
Datenintegrität	**Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.**	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
DI.1	Digitale Daten werden fehlerhaft oder unzulässig verändert	Interner User	Interne Systembenutzer verändern versehentlich fehlerhaft Daten.	Aufgrund der angespannten Personalsituation werden teilweise auch noch sehr unerfahrene HCM-Sachbearbeiter eingesetzt.	4	Fehlbedienungen von Systemusern, die zu einer unerwünschten Datenveränderung führen, sind punktuell und werden i.d.R. über die vorgegebenen Plausibilitätskontrollen rasch erkannt und wieder berichtigt.	2	8	M.22 4-Augen-Prinzip für tragende Personaldatenänderungen umsetzen M.4 HCM-Benutzer schulen M.23 Wiederholte Falscheingaben sammeln und auswerten	Die Erfahrung zeigt, dass bei der hohen Bedienungskomplexität und der hohen Änderungsdynamik trotz der ergriffenen Maßnahmen ein gelbes Restrisiko verbleibt.	ge
DI.2	= DI.1 =	Externer User	Externe Systembenutzer (z.B. Finanzprüfer, Auditoren) verändern versehentlich fehlerhaft Daten.	Zugriffe externer User auf das produktive HCM-System finden nur selten statt.	2	Fehlbedienungen von Systemusern, die zu einer unerwünschten Datenveränderung führen, sind punktuell und werden i.d.R. über die vorgegebenen Plausibilitätskontrollen rasch erkannt und wieder berichtigt.	2	4	M.5 Lesenden Zugriff für berechtigte Dritte konfigurieren	Fehlbedienungen von externen Benutzern, die zu einer unerwünschten Datenänderung führen, sind nicht vorstellbar, da solche Benutzer stets nur mit Leserechten ausgestattet sind (bewährtes Standardbenutzerprofil).	gr
DI.3	= DI.1 =	Böswilliger interner User	Interne Systembenutzer verändern vorsätzlich fehlerhaft oder unzulässig Daten, etwa um sich oder einem anderen einen Vorteil zu verschaffen.	In der Vergangenheit konnte vereinzelt solch ein vorsätzliches Verhalten aufgedeckt werden.	3	Fehlbedienungen von Systemusern, die zu einer unerwünschten Datenveränderung führen, sind punktuell und werden i.d.R. über die vorgegebenen Plausibilitätskontrollen rasch erkannt und wieder berichtigt.	2	6	M.22 4-Augen-Prinzip für tragende Personaldateneingaben umsetzen M.24 Keine Selbstbearbeitung zulassen	Nach konsequenter technischer Umsetzung des Selbstbearbeitungsverbots gab es keine Hinweise auf Manipulationsfälle durch böswillige interne Beschäftigte.	gr
DI.4	= DI.1 =	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware werden Daten fehlerhaft oder unzulässig verändert (z.B. externe Datenverschlüsselung durch Ransomware).	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4	Das Änderungspotenzial von cyberkriminellen Angriffen umfasst auch unerwünschte Massendatenänderungen mit den daraus folgenden Auswirkungen.	3	12	M.7 Basis Schadsoftware-/ Hackerabwehrsystem nutzen M.1 Basis Backup-Struktur nutzen	Trotz der ergriffenen Maßnahmen für die aktive und passive Risikobewältigung kann das Risiko nicht in den grünen Bereich gebracht werden.	ge
DI.5	Daten in Papierform werden fehlerhaft oder unzulässig verändert	Internes Personal	*noch weiter zu ergänzen*	usw.	3	usw.	3	9	usw.	usw.	gr

Glossar

Begriff/Abkürzung	Erläuterung
Beschäftigte/r	Natürliche Person, die sich bei der Stadt um ein Arbeits-/Dienstverhältnis bewirbt, die in einem wirksamen Arbeits-/Dienstverhältnis bei der Stadt steht oder die ein wirksamen Arbeits-/Dienstverhältnis mit der Stadt hatte (z.B. Ruhestand, neuer Arbeitgeber).
Daten	Personenbezogene Daten von Beschäftigten
Dokument-ID	Eindeutige Identitätsangabe (ID) für ein bestimmtes Dokument.
DSFA	Datenschutz-Folgenabschätzung
HCM	Personalwesen der Stadt ("Human Capital Management")
Persoaldaten	Personenbezogene Daten, die typischer Weise in der Personalwirtschaft verarbeitet werden.
SDM	Standard-Datenschutzmodell beschreibt eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Näheres im Internet unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell.
SDM-Datensicherheitsziele	Davon umfasst sind die beiden SDM-Gewährleistungsziele Verfügbarkeit und Vertraulichkeit sowie der Teilzielaspekt Dateninteg-rität des SDM-Gewährleistungsziels Integrität.