

6. Datenschutz durch Technikgestaltung und –bewertung

6.1 Orientierungshilfe zur Erstellung eines Datenschutzkonzeptes

Häufiges Diskussionsthema bei Schulungen und Workshops für behördliche Datenschutzbeauftragte war in der Vergangenheit die Erstellung der Verfahrensbeschreibungen bei der verantwortlichen Stelle, und hier insbesondere die Darstellung der technischen und organisatorischen Maßnahmen nach § 7 Bremisches Datenschutzgesetz (BremDSG).

Ich habe daher im Berichtsjahr eine Orientierungshilfe erarbeitet, die den behördlichen Datenschutzbeauftragten als Hilfestellung bei dieser Aufgabe dienen soll. Dabei wurde es notwendig, eine klare Linie zu ziehen zwischen den für jedermann öffentlich zugänglichen Verfahrensbeschreibungen und den in einem Konzept festzulegenden Sicherheitsvorkehrungen, die natürlich nicht öffentlich gemacht werden sollen.

Nach § 8 BremDSG ist eine Verfahrensbeschreibung zu erstellen, die öffentlich einsehbar ist. Anders als im Bundesdatenschutzgesetz sind die technischen und organisatorischen Maßnahmen davon nicht ausgenommen. Von Administratoren wurde dieser Sachverhalt kritisiert, denn es bestehe die Gefahr, dass bei der Beschreibung der getroffenen Maßnahmen sicherheitsrelevante Informationen dargestellt werden, die nicht für eine öffentliche Einsichtnahme geeignet seien. Eine detaillierte Beschreibung der Sicherheitsinfrastruktur ist aber in der Regel erforderlich, um eine datenschutztechnische Bewertung durchführen zu können.

Um diesem Dilemma zu entgehen, habe ich folgende Vorgehensweise empfohlen: Die Verfahrensbeschreibung soll bezüglich der technischen und organisatorischen Maßnahmen eine Beschreibung auf abstraktem Niveau enthalten, die bei Einsichtnahme durch den Bürger verstanden werden kann. Ergänzt werden soll diese Verfahrensbeschreibung dann um ein nicht öffentliches Fachdatenschutzkonzept, welches die Maßnahmen zur Erreichung der Schutzziele detailliert beschreibt und eine Bewertung der getroffenen Maßnahmen ermöglicht. Sollen mehrere oder integrierte Verfahren beschrieben werden, können solche Maßnahmen, die für alle Verfahren gelten (z. B. Zutrittskontrolle zu Serverräumen, Zugangskontrolle bezüglich Anmeldeverfahren am PC-Arbeitsplatz, zentrale Datensicherungskonzepte) in einem Rahmendatenschutzkonzept zusammengefasst werden.

Das skizzierte Konzept wird derzeit den behördlichen Datenschutzbeauftragten mitgeteilt und bereits in ersten größeren Behörden, z. B. beim Stadtamt Bremen, umgesetzt.

Datenschutzkonzept

Öffentlicher Teil

Nicht öffentlicher Teil

Verfahrensbeschreibung nach § 8 BremDSG

1. Verantwortliche Stelle...
2. Name und Anschrift...
3. Art. und Rechtsgrundlage...
4. Kreis der Betroffenen...
5. Empfänger...
6. Fristen...
7. Die technischen und organisatorischen Maßnahmen nach § 7 BremDSG
An dieser Stelle erfolgt eine allgemeinverständliche, vollständige, aber abstrakte Beschreibung der nach § 7 BremDSG getroffenen Maßnahmen, ohne dass hierbei sicherheitsrelevante Informationen verwendet werden.
8. eine geplante Datenübermittlung in Staaten außerhalb der Europäischen Union

Alternative A

Rahmendatenschutz- konzept der TOMs *

Detaillierte Beschreibung der Maßnahmen und deren konkrete Implementierung für bestimmte Schutzziele mit allgemeinem und übergreifendem Charakter.

Fachdatenschutz- konzept der TOMs * zum Verfahren

Detaillierte Beschreibung der Maßnahmen und deren konkrete Implementierung für bestimmte Schutzziele speziell für die Fachanwendung.

Alternative B

Gesamtdatenschutz- konzept der TOMs *

Detaillierte Beschreibung der Maßnahmen und deren konkrete Implementierung für bestimmte Schutzziele speziell für die Fachanwendung sowie eine detaillierte Beschreibung der Maßnahmen und deren konkrete Implementierung für Schutzziele mit allgemeinem und übergreifendem Charakter.

* TOMs = Technisch-organisatorische Maßnahmen gem. § 7 BremDSG

6.2 Protokollierung und Revision

Im Berichtsjahr habe ich bei meinen Prüfungen und Beratungen festgestellt, dass eine sachgerechte Protokollierung und Revision in komplexen DV-Systemen mit Anforderungen verbunden ist, die umfangreiche konzeptionelle Überlegungen erfordert. Die Protokollierung und darauf aufsetzend die Revision sind zu eigenen Verfahren geworden. Sie fallen insbesondere bei vielschichtigen Verarbeitungsprozessen nicht mehr „nebenbei“ in Form einer speziellen, bestenfalls noch überschaubaren Logdatei an, sondern sind viel umfangreicher und erfordern eine gezielte Planung. Angesichts des rasanten Aufbaus neuer Systeme wird für eine datenschutzgerechte Konzeption der Protokollierung oft nicht die nötige Zeit eingeplant.

Unter Protokollierung beim Betrieb von IT-Systemen im datenschutzrechtlichen Sinn wird die Erstellung von manuellen, in der Regel automatisierten Aufzeichnungen verstanden, aus denen insbesondere nachvollziehbar sein muss, welche Person zu einem bestimmten Zeitpunkt mit welchen Funktionen auf personenbezogene Daten zugegriffen hat. Hinzu kommt, dass Systemzustände, wie beispielsweise die Dokumentation der Zugriffssystematik über einen definierten Zeitraum, ableitbar sein müssen.

Die rechtlichen Verpflichtungen ergeben sich dabei direkt aus den Datenschutzgesetzen. Das Bundesdatenschutzgesetz (BDSG) schreibt in der Anlage zu § 9 Nr. 4 und 5 und das Bremische Datenschutzgesetz (BremDSG) in § 7 Abs. 4 Satz 2 Nr. 4 und 5 entsprechende Dokumentationen in Rahmen der Eingabe- und Weitergabekontrolle vor. Auch im Zusammenhang mit automatisierten Abrufverfahren sind solche Protokolle zu erstellen (§ 14 Abs. 3 BremDSG). Im Security Management muss durch Zugangskontrolle und Rechteverwaltung dafür gesorgt werden, dass nur Berechtigte in der Lage sind, auf Protokolle zuzugreifen. Hierzu gehört beispielsweise als technische Maßnahme die Speicherung der Daten außerhalb der produktiven Systeme, auch um die Anforderung der Revisionsfähigkeit umzusetzen.

Diese Protokolldaten unterliegen selbst wieder eigenen Datenschutzregelungen. So dürfen die in diesem Rahmen erhobenen personenbezogenen Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden (besondere Zweckbindung). Es ist also das Verfahren der Protokollierung selbst und damit verbunden der Schutz der in diesem Rahmen erhobenen personenbezogenen Daten technisch und organisatorisch zu klären. Da im Rahmen der Protokollierung Daten von Arbeitnehmern und Arbeitnehmerinnen verarbeitet werden, ist das Verbot der Leistungs- und Verhaltenskontrolle (vgl. § 20 BremDSG) zu garantieren. Eine weitere datenschutzrechtliche Anforderung gilt natürlich grundsätzlich auch hier: Das Prinzip der Datensparsamkeit und Datenvermeidung (§ 7 BremDSG, § 3 a BDSG).

Vor diesem Hintergrund muss die Protokollierung hinsichtlich ihrer Art, ihrer Ziele, ihrer Inhalte und Auswertbarkeit beschrieben werden. Es gibt Protokolle auf verschiedenen Systemebenen, die sich auf benutzer-, prozess- oder/und sicherheitstechnische Ereignisse beziehen. Diese Protokolle dienen

grundsätzlich zwei Zielen: Es soll möglich sein, Sicherheitsverletzungen durch Aufzeichnung sicherheitsrelevanter Ereignisse zu erkennen. Außerdem müssen für Zwecke der Beweissicherung Handlungen von Benutzern im System nachvollziehbar sein. Mit einer revisionssicheren Protokollierung der Systemadministration kann beispielsweise die Frage beantwortet werden, welcher Administrator zu welchem Zeitpunkt welche das Security Management betreffenden Aktionen (wie etwa Änderung einer Sicherheitsregel, Ändern von Benutzerrechten, Löschen von Logdateien) durchgeführt hat. Auch die Durchführung von Servicearbeiten muss entsprechend nachvollziehbar sein. Die Protokollierung von Administratortätigkeiten dient der Kontrolle der gesamten Systemsicherheit. Sie kann auch Schutz vor eventuellen Verdächtigungen bieten.

In der Praxis habe ich häufig die Erfahrung gemacht, dass die Administratoren die Revisionsmöglichkeit ihrer Tätigkeit ablehnen. Sie argumentieren, dass eine Vertrauensposition, die uneingeschränkte Aktivitäten in den Systemen ermöglicht, nicht umfassend kontrolliert werden kann und dies auch nicht erforderlich sei. Es gibt jedoch in komplexen DV-Systemen eine Vielzahl administrativer Tätigkeiten, die von verschiedenen Personen und auch externen Firmen wahrgenommen werden. In diesem Umfeld existiert die klassische, an eine Person gebundene Vertrauensposition nicht mehr. Hinzu kommt, dass der Verarbeitungsumfang bezogen auf Datenmengen und Möglichkeiten (insbesondere Verknüpfungen von Informationen und Datenabgleiche) stark zugenommen hat. Es ist daher wichtig, die Aufzeichnungen nach bestimmten Fragestellungen auswertbar zu machen. Hierfür sind entsprechende Tools einzusetzen, um ein „Ereignismanagement“ zu ermöglichen.

Aufgrund der im Rahmen einer sinnvollen Protokollierung und Revision zu behandelnden Fragestellungen wird deutlich, dass eine Grundlage für die konzeptionelle Gestaltung dieses Verfahrens bereits im Rahmen einer Sicherheitspolicy, die u. a. Basisdefinitionen für die Sicherheit allgemein vornimmt, geschaffen werden muss. In diesem Rahmen müssen grundlegende Überprüfungsmodalitäten festgelegt werden.

Ich halte zur Erfüllung der datenschutzrechtlichen Normen eine sachgerechte, nicht ausufernde Protokollierung für unbedingt notwendig. Der Aufwand für die Gestaltung der Verfahren zur Protokollierung und zur Revision, verbunden mit der Konzeption des Sicherheitsmanagements bei der Einführung und Administration von Verfahren, darf im Hinblick auf die hierfür erforderlichen Ressourcen weder aus den Augen verloren noch unterschätzt werden.

6.3 Funktionstrennung: Berechtigungen entsprechend der Aufgaben vergeben

Die Zahl der Informationssysteme wächst stetig und schnell. Und mit ihnen die Zahl der darin gespeicherten und verarbeiteten Daten. Mit der Anzahl der Informationssysteme wächst aber auch die Aufgabenflut für die Administratoren, die (oft) mehrere davon gleichzeitig betreuen müssen. Auch in der öffentlichen Verwaltung in Bremen ist diese Entwicklung deutlich bemerkbar.

Die große Zahl der verschiedenen Systeme bedingen aber auch eine genaue Planung und Umsetzung von differenzierten Berechtigungskonzepten für die jeweils im Einsatz befindlichen Systeme. Berechtigungen regeln, wer in IT-Systemen welche Funktionen nutzen darf. Grundsätzlich ist bei diesen Berechtigungen von zwei verschiedenen Ebenen auszugehen: Den Berechtigungen, die unbedingt dazu notwendig sind, das System zu betreiben (administrative Berechtigungen) und die Berechtigungen, die zur Aufgabenerfüllung notwendig sind (operative Berechtigungen).

Aus Sicht des Datenschutzes ist eine klare Trennung zwischen diesen Bereichen anzustreben. Darüber hinaus gibt es Funktionen, die in einer Person liegend unvereinbar sind, hier muss es zwingend zu einer klaren personellen Trennung kommen (z. B. Administrator und Revisor).

Während sich die Anforderungen der personellen Trennung von Aufgaben in größeren Organisationseinheiten relativ problemlos umsetzen lassen, bestehen hierfür in kleinen Einheiten weitaus mehr Schwierigkeiten. Solange keine miteinander unvereinbaren Aufgaben betroffen sind, sind bei einer Doppelfunktion der Aufgabenwahrnehmung auf verschiedenen Ebenen besondere Regeln zu beachten. In IT-Systemen soll jeder nur mit so viel Rechten ausgestattet sein wie es zur Wahrnehmung der spezifischen Aufgaben notwendig ist. In der Literatur wird oft vom „Need-to-know-Prinzip“ gesprochen. So soll ein Administrator sich an den IT-Systemen nur dann mit administrativen Berechtigungen anmelden, wenn er auch administrative Tätigkeiten durchzuführen hat („Wartung ohne inhaltlichen Zugriff“). Bei operativer Tätigkeit muss er über den hierfür vorgesehenen Berechtigungspfad gehen. Eine Funktionstrennung wird dabei durch die Nutzung unterschiedlicher Benutzerkennungen und Passwörter erreicht.

Auch innerhalb von DV-Fachverfahren soll eine strikte Funktionstrennung umgesetzt werden. Es ist nicht auszuschließen, dass Anwender des Systems auch Aufgaben mit administrativem Hintergrund zu erledigen haben. Diese Berechtigungen sind im System getrennt voneinander abzubilden und die Funktionstrennung dadurch zu realisieren, dass wiederum je nach Aufgabe eine spezifische Anmeldung an das Fachverfahren erfolgen muss.

Strikte Funktionstrennung ist ein wichtiges Werkzeug, um ein hohes Sicherheitsniveau zu erreichen. Auch Vertretungsregelungen sollten unter Wahrung strikter Funktionstrennungen realisiert werden, womit auch Risiken minimiert und das Wissen bzw. bestimmte Fähigkeiten auf mehrere Personen verteilt werden. Letztendlich lässt sich nur durch saubere Funktionstrennung, eine Trennung zwischen Entscheidung, Ausführung, Kontrolle (und Berichterstattung), eine richtige und aussagekräftige Revision der IT-Systeme realisieren.

Zum Aufbau einer Funktionstrennung gehört, dass ein umfassendes Berechtigungskonzept erarbeitet wird, das alle notwendigen Rollen vollständig mit den zugehörigen Rechten beschreibt. Dies gilt sowohl für die in den Organisationseinheiten im Einsatz befindliche IT-Basisinfrastruktur als auch für die angewendeten Fachverfahren. Das Berechtigungskonzept ist auf aktuellem Stand zu halten, veränderten Rahmenbedingungen anzupassen und die richtigen Abbildungen sind in den Systemen turnusmäßig zu überprüfen.

6.4 Active Directory für das Bremische Verwaltungsnetz

Im Berichtsjahr habe ich vom Senator für Finanzen verschiedene Unterlagen zum geplanten Echtbetrieb des bremischen Verzeichnisdienstes „Active Directory“ (AD) mit der Bitte um Stellungnahme erhalten. Ein AD ist bereits im Pilotbetrieb und wird für diverse (Test-)Anwendungen genutzt. Dieser Pilot soll in den Echtbetrieb überführt werden. Ich habe zunächst zur gesamten Infrastruktur Stellung genommen und Basisanforderungen an den datenschutzkonformen Betrieb eines AD formuliert. Auf Grund der Vielzahl der sicherheitsrelevanten Einstellungsmöglichkeiten eines AD konnte ich mich nicht zu allen Einstellungen äußern.

Für das Bremer Verwaltungsnetz (BVN) bedeutet die Einführung des zentralen Active Directory einen tiefgreifenden Wandel; die bisherige Struktur des BVN wird komplett umgebrochen. Die herkömmliche Version des BVN ist so aufgebaut, dass die bremische Verwaltung einer geschlossenen Benutzergruppe mit gleichwertigen Partnern entspricht. Jede Dienststelle hat die alleinige tatsächliche Verfügungsgewalt über ihre DV-Systeme und die darin gespeicherten und verarbeiteten Daten. Sie verfügt allein über die Administrationsrechte für DV-Systeme und -Verfahren. Die Dienststelle kann entscheiden, wer notwendigerweise Zugriff von außen auf Systeme oder Verfahren haben muss bzw. darf, z. B. im Rahmen von Fernwartung oder Auftragsdatenverarbeitung. Diese sind vertraglich oder über eine Verwaltungsvereinbarung rechtlich geregelt. Die Dienststelle als verantwortliche Stelle nach § 2 Abs. 3 Nr. 1 des Bremischen Datenschutzgesetzes (BremDSG) hat somit die volle Kontrolle über ihre Daten und Systeme; die Anforderungen nach § 7 Abs. 3 und Abs. 4 BremDSG können unproblematisch erfüllt werden.

Mit der Einführung eines verwaltungsweiten AD geht dieser Zustand der administrativen Hoheit der jeweiligen verantwortlichen Stelle jedoch verloren. Die einzelnen Dienststellen werden als Organisationseinheiten (OU) unterhalb von Domänen oder sogar als Sub-OU unterhalb anderer OU im AD abgebildet, z. B. Dienststelle unterhalb der senatorischen Behörde. Das hat zur Folge, dass sich z. B. Administratoren hierarchisch höher liegender Ebenen grundsätzlich jederzeit Rechte verschaffen können, um auf die Systeme und die darin gespeicherten Daten der darunter liegenden Ebene zuzugreifen. Dies kann technisch nicht verhindert werden. Besonders problematisch ist dieser Umstand in sensiblen Bereichen, in denen z. B. auch Daten von Berufsheimnisträgern oder sonstigen Personen, die einer besonderen Schweigepflicht unterliegen, verarbeitet werden (Gesundheitsämter, Beratungsstellen etc.).

Die Architektur des AD ist mit einem grundsätzlichen Fehler behaftet: Die verantwortlichen Stellen können nicht mehr, wie in § 7 Abs. 3 und 4 BremDSG gefordert, selbst die vollständige Kontrolle über ihre Daten und Systeme ausüben. Zwar kann die lokale Administration der verantwortlichen Stelle Maßnahmen zur Abschottung gegenüber zentralen Zugriffs- und Steuerungsmöglichkeiten für eigene Ressourcen ergreifen, diese sind jedoch jederzeit durch die zentrale Administration aufhebbar. Da sich kein zentraler Durchgriff auf die Ressourcen einzelner Organisationseinheiten verhindern lässt, muss daher insbesondere auf der Ebene der lokalen und zentralen Administration eine sichere Protokollierung und Revision gegenüberstehen.

Eine leistungsfähige Revision, wie unter Ziffer 6.2 dieses Berichts beschrieben, ist in den mir vorliegenden Dokumenten des Finanzressorts zum Einsatz des AD noch nicht dokumentiert worden. Sie ist aber parallel zur Einführung des AD zur Verfügung zu stellen und alle durch die Administration ausgelösten sicherheitsrelevanten Ereignisse sind revisionssicher zu protokollieren.

Die Protokollauswertung und Revision muss durch eine vom verantwortlichen Betreiber unabhängige Instanz durchgeführt werden. Die erforderlichen Details dafür, wie etwa der physikalische Ort der Speicherung, der Inhalt der Prüfrichtlinien, Revisionshäufigkeit, Zieldefinitionen, Rechtekontrollen, Erkennen von Manipulationsversuchen, Revisionsrollen, Kontrolle der Richtlinien für die Protokollauswertung selbst etc., müssen in einem gesonderten Revisionskonzept beschrieben werden. Darüber hinaus sollte den Administratoren der Dienststellen, die zukünftig ihre Organisationseinheit innerhalb des AD zu verwalten haben, eine Guideline zur datenschutzgerechten Konfiguration ihrer Infrastruktur und Systeme innerhalb des AD zur Verfügung gestellt werden.

Für den Einsatz eines zentralen AD muss die Summe aus Revision und Protokollierung in allen Bereich des BVN und der teilnehmenden Dienststellen einen für alle transparenten und nachvollziehbaren dokumentierten Betrieb ermöglichen. Zentrale Eingriffe können dadurch zwar nicht ausgeschlossen, aber nachträglich erkannt werden. Nur so kann von der „verantwortlichen Stelle“, wie es von den Datenschutzgesetzen verlangt wird, auch tatsächlich noch Verantwortung übernommen werden.

Über die Ausgestaltung der einzelnen Anforderungen befinde ich mich mit der für die Einführung einer AD im BVN betreuenden Einheit beim Senator für Finanzen noch im Dialog.