Thomas Probst

Generische Schutzmaßnahmen für Datenschutz-Schutzziele

Die Datenschutz-Schutzziele Nicht-Verkettbarkeit und Intervenierbarkeit sind in der gesetzlichen Realität angekommen. Für konkrete Maßnahmen zu ihrer Umsetzung gibt es bisher noch keine Vorgaben.

1 Einleitung

Mit dem Inkrafttreten des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG-SH) im Januar 2012 wurden erstmalig die spezifischen Datenschutz-Schutzziele[1] *Nicht-Verkettbarkeit* und *Intervenierbarkeit* gesetzlich verankert. Das dritte Datenschutz-Schutzziel *Transparenz*, das in § 5 LDSG-SH neben die klassischen IT-Sicherheits-Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität tritt, ist hingegen ein alter Bekannter: auch in den Landesdatenschutzgesetzen Berlins, Brandenburgs, Mecklenburg-Vorpommerns, Nordrhein-Westfalens, Sachsen, Sachsen-Anhalts und Thüringens[2] gibt es das Schutzziel Transparenz.[3]

Größtenteils stehen lediglich Daten im Fokus der Schutzziele: Dies ist bei den Schutzzielen Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit der Fall. Der Fokus des Schutzzieles Transparenz liegt jedoch auf ganzen Verfahren und Verfahrensweisen.

In der Formulierung des § 5 LDSG-SH, erstrecken sich die klassischen Schutzziele Vertraulichkeit und Verfügbarkeit nicht nur auf Daten, sondern auch auf Verfahren.[4] Der Fokus der Schutzziele Integrität und Nicht-Verkettbarkeit sind Daten, der Fokus der Schutzziele Transparenz und Intervenierbarkeit sind Verfahren.

1.1 Komponenten

Teilt man Verfahren in die drei Komponenten Daten, IT-Systeme und Prozesse auf[5] und vergleicht dies mit den eben dargestellten normativen Formulierungen, so stellt man Diskrepanzen fest: IT-Systeme sind gar nicht Gegenstand der gesetzlichen Formulierungen; begreift man Verfahrensweisen als Prozesse, so sind sie nicht Gegenstand aller Schutzziele.

Es lohnt sich aber der Versuch, die sechs Schutzziele auf die jeweiligen drei Komponenten anzuwenden und zu untersuchen, ob und inwieweit dies sinnvolle Objekte für Schutzziele sind.

Nachfolgend soll der Versuch unternommen werden, generische und prototypische Schutzmaßnahmen zu benennen, die sich den Schutzzielen und den Verfahrenskomponenten zuordnen lassen.

1.2 Schutzbedarfe

Die Wahl von Schutzmaßnahmen steht unter dem gesetzlichen Primat der Angemessenheit von Aufwand im Verhältnis zum Schutzbedarf der Daten.[6] Auch im Bereich der IT-Sicherheit werden Maßnahmen risikobasiert ausgewählt; es gibt dafür spezifische Standards zur Risikoanalyse.[7] Eine detaillierte quantitative Risikoanalyse von Bedrohungen und Gefährdungen[8] der Schutzziele hat den Vorteil, die erforderlichen und angemessenen Maßnahmen treffsicher auswählen und zuordnen zu können. Sie hat den Nachteil einer hohen Komplexität, da es zahlreiche Gefährdungen gibt, die einzeln zu untersuchen und zu bewerten sind. Eine Alternative ist die Verwendung von Schutzstufen oder Schutzbedarfen, die in (üblicherweise) drei Kategorien (normal, hoch, sehr hoch) beschreiben, welchen Bedarf Daten, IT-Systeme oder Prozesse an der Umsetzung der einzelnen Schutzziele haben. Gradmesser sind dabei möglich Schäden, die aus der Verletzung der Schutzziele resultieren. Diese Vorgehensweise wird im IT-Grundschutz[9] verwendet. Zu beachten ist aber, dass Schutz-

1 Rost, Martin / Bock, Kirsten, 2011 Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen; in: DuD – Datenschutz und Datensicherheit, 35. Jahrgang, Heft 1: 30-34

2 Das Hamburger Datenschutzgesetz benutzt ebenfalls die Formulierung der Schutzziele zur Beschreibung der Technisch-organisatorischen Maßnahmen (§ 8 HamDSG), weist aber das Schutzziel „Transparenz" nicht explizit aus.

3 In einer gängigen Formulierung lautet die gesetzliche Vorgabe, Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass „die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können", z.B. § 5 Abs 2 Nr. 5 BlnDSG

4 Z. B. § 5 Abs. 1 Nr. 1 LDSG-SH: … müssen gewährleisten, dass ... Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit),

5 Siehe ausführlicher bei Rost in diesem Heft.

6 Siehe z.B. § 9 Satz 2 BDSG oder § 5 Abs. 1 Satz 1 LDSG-SH.

7 Z. B. ISO/IEC 27005:2011 Information security risk management oder NIST 800-30: Risk Management Guide for Information Technology Systems

8 Z.B. Höhere Gewalt, technisches und menschliches Versagen, Vorsatz oder Organisationsmängel

9 BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, V 2.0, 2008, Abschnitt 4.2.

Dr. Thomas Probst

Stellvertretender Leiter des Referat „Gütesiegel" beim Unabhängigen sLandeszentrum für Datenschutz Schleswig-Holstein, Kiel

E-Mail: thomas.probst@datenschutzzentrum.de

bedarfe für Datenschutz im Gegensatz zur üblichen Vorgehensweise nicht das Interesse der Organisation, sondern das Interesse der Betroffenen in den Vordergrund stellen.

2 Maßnahmen für Schutzziele

2.1 Verfügbarkeit

Die normativen Anforderungen bezüglich der Verfügbarkeit beziehen sich überwiegend auf Daten; im LDSG-SH wird auch die Verfügbarkeit von Verfahren betrachtet.

Maßnahmen zur Sicherung der Verfügbarkeit sind Standardmaßnahmen im Bereich der IT-Sicherheit und reichen von klassischen Backups und Spiegeldateien (Daten) über Kopien der System- und Konfigurationsdateien, Ersatzhardware und Clustersysteme (IT-Systeme) bis hin zu Ausweichrechenzentren, Ersatzlokationen oder ganz generell der Verlagerung von Verfahrensteilen (z.B. Amtshilfe oder durch die Übertragung von Aufgaben an Dritte, für die ein Verfahrenszugriff möglich ist, wenn er der ausführenden Stellen aus technischen Gründen verwehrt ist).

Ganz allgemein hat man dafür Sorge zu tragen, dass *alle* Komponenten eines Verfahrens (u.a. Daten, IT-Systeme, Software, Gebäude, Personal) verfügbar sind bzw. dass Ersatz bereitsteht. Der zu treffende Aufwand bemisst sich üblicherweise an den Anforderungen der Verfügbarkeit, nämlich welche Ausfallzeiten zu tolerieren sind.

Etwas komplexer wird die Betrachtung, wenn man Wechselwirkungen der Schutzziele betrachtet und Vertraulichkeit als „gesicherte Nicht-Verfügbarkeit“[10] begreift: Eine allzu perfekte Umsetzung des Schutzziels Verfügbarkeit, im Extremfall etwa durch eine Veröffentlichung der Daten im Internet, stünde sehr deutlich im Konflikt zum Schutzziel Vertraulichkeit. Das Gesetz löst dieses Problem durch das Wort „befugt“, das die Verfügbarkeit einschränkt und das Problem aufwirft, Befugte von Unbefugten zu unterscheiden. Aber trotz der (formalen) Einschränkung auf befugte Zugriffe ist ein Ausbalancieren bzw. Abwägen der Schutzziele Vertraulichkeit und Verfügbarkeit gegeneinander erforderlich – nämlich im Hinblick darauf, dass eine Umsetzung der Schutzziele nicht zu 100 % erfolgt bzw. erfolgen kann (Restrisiko): So sind aufgrund technischen oder menschlichen Fehlverhaltens unbefugte Zugriffe denkbar (=Verlust der Vertraulichkeit), die man durch Einschränkungen der Verfügbarkeit abwenden könnte.[11]

Die Unterscheidung von Befugten und Unbefugten ist eine (Teil-)maßnahme, die sehr häufig verwendet wird, etwa um befugte von unbefugter Kenntnisnahme (Vertraulichkeit) und befugte von unbefugter Datenänderung (Integrität) und Löschung (Verfügbarkeit[12]) zu unterscheiden. In der Formulierung des BDSG und vieler Landesdatenschutzgesetze findet sich dies unter den Begriffen Zutritts-, Zugangskontrolle und Zugriffskontrolle.[13] Typische Mechanismen sind Authentisierung (z. B. durch Benutzername und Passworte) und Autorisierung (Durchsetzung von Zugriffsrechten), siehe dazu später auch Abschnitt 4.2.

Zu beachten ist, dass es bei der Umsetzung von Maßnahmen des Schutzziels Verfügbarkeit nicht zu Verletzungen der Vertraulichkeit kommen darf. Dies gilt jedoch für alle Umsetzungen aller Maßnahmen und wird im Abschnitt 4 betrachtet, der sich mit der Anwendung der Schutzziele auf Maßnahmen befasst.

Die Feststellung, dass die Unterscheidung befugt/unbefugt bei der Umsetzung mehrerer Schutzziele hilft, führt zur

Erste Beobachtung
Es gibt Schutzmaßnahmen, die sich nicht eins-zu-eins einzelnen Schutzzielen zuordnen lassen, sondern der Umsetzung mehrerer Schutzziele dienen können.

Weiterhin wird bei genauerer Betrachtung klar, dass Maßnahmen, die ein Schutzziel unterstützen, auch gegen das Versagen von Maßnahmen helfen, die primäre anderen Schutzziele dienen. Man könnte dies als „second line of defence“ bezeichnen: Das Backup von Daten hilft nicht nur bei einem unmittelbaren Datenverlust, sondern kann auch bei einer Beeinträchtigung der Integrität durch unerkannte Schadsoftware („Virenbefall“), durch nicht abwendbare Manipulationen[14] oder durch technischbedingte Integritätsverluste[15] zumindest einen früheren Datenbestand wieder herstellen.

Zweite Beobachtung
Maßnahmen für ein Schutzziel können teilweise den Ausfall bzw. Unzulänglichkeiten der Mechanismen für andere Schutzziele kompensieren.

Zwischenfazit

Im Ergebnis stellt man bezüglich des Schutzziels Verfügbarkeit fest, dass die Standardmaßnahmen für dieses Schutzziel häufig auch weitere Schutzziele umsetzen bzw. ihre Umsetzung unterstützen. Umgekehrt darf die Umsetzung eines Schutzziels andere nicht gefährden (beispielsweise sind Backup-Dateien besonders gegen Vertraulichkeitsverluste zu sichern).

In Bezug auf unterschiedliche Schutzbedarfe hinsichtlich der Verfügbarkeit lassen sich die erforderlichen Maßnahmen (relativ) einfach skalieren, wenn man als Kenngröße eine maximal tolerierbare Ausfallzeit vorgibt. Zu bestimmen bleibt aber vor eine Festlegung der Maßnahmen, welche Risikoszenarien zu betrachten sind: Die Maßnahmen zur Wiederherstellung der Verfügbarkeit innerhalb von sechs Stunden nach Schadensfall unterscheiden sich je nach dem, ob als Schadensfall ein Festplattenausfall oder ein Rechenzentrumsbrand betrachtet wird. Daher scheint eine rein schematische Vorgehensweise, die sich ausschließlich auf den Wert des Schutzbedarfs stützt, nicht sinnvoll. Im IT-

10 Abschnitt 2.2 in Rost, Martin/Pfitzmann, Andreas: Datenschutz-Schutzziele – revisited. DuD – Datenschutz und Datensicherheit, 33. Jahrgang 2009, Heft 6, S. 353-358.

11 Sollte beispielsweise ein öffentlicher Anbieter von E-Mail-Diensten Nachrichten auch nach der Löschung durch den Anwender auf Backups bereithalten (und wenn ja: wie lange?) oder sie sofort und endgültig löschen (um den Preis, dass auch bei versehentlicher Löschung oder Löschung durch Schadsoftware keine Wiederherstellung erfolgen kann, folglich die Verfügbarkeit „leidet“)?

12 Art. 17 Abs. 1 Satz 1 der Richtlinie 95/46/EG.

13 Siehe Anlage zu § 9 Abs. 1 BDSG, wobei sich der Mechanismus (Unterscheidung Befugter – Unbefugte) hinsichtlich des Ziels, nämlich Zutritt zu IT-Systemen und Datenträgern, Zugang zu IT-Systemen bzw. Zugang zu Daten zu erlangen, unterscheidet.

14 Beispielsweise lassen sich Manipulationen (etwa im Einzelfall unrichtige Datenveränderungen) durch befugte Innentäter nicht mit Hilfe des üblichen Zugriffsschutzes unterbinden, da ja der Täter gerade befugt ist. Hiergegen helfen spezifische Zugriffsschutzmechanismen (z. B. Vier-Augen-Mechanismen) oder (eingeschränkt) eine Protokollierung und Protokollkontrollen mit dem Ziel, solche Manipulationen im Nachhinein entdecken zu können.

15 Solche können, ähnlich wie bei elektronischen Signaturen, zwar erkannt, aber nicht ohne weitere Hilfsmittel rückgängig gemacht werden. Ein Daten-Backup wäre ein solches Hilfsmittel.

Grundschutz wird daher für den Schutzbedarf „normal“ eine Vielzahl von Schutzmaßnahmen festgelegt, die einzelnen Gefährdungen der Verfügbarkeit entgegenwirken. Für höhere Schutzbedarfe sind eine individuelle Risikoanalyse und die Festlegung spezifischer Maßnahmen erforderlich.[16]

2.2 Integrität

Das Schutzziel Integrität bezieht sich nach dem Gesetzeswortlaut nur auf Daten; aber auch die Integrität der übrigen Verfahrenskomponenten wie Hardware, Software, Konfigurationen und Personal, also die Integrität der (IT-) Systeme muss gesichert sein. Hierbei wird Integrität als „korrekte Funktionsweise“ interpretiert[17]. Mit Standardmechanismen lassen sich alle Facetten der rechtlichen Integritätsanforderungen („unversehrt, vollständig, zurechenbar und aktuell“)[18] abdecken: Dazu gehört in erster Linie, befugte von unbefugten Zugriffen zu unterscheiden, Maßnahmen gegen technische Fehler (z. B. Checksummen, fehlerkorrigierende Codes) zu ergreifen, Metadaten (etwa verarbeitende Person oder Institution) hinzuzufügen und schließlich auch inhaltliche Änderungen von Daten nachzuvollziehen, etwa durch Update-Verfahren und Berücksichtigung von Änderungsmitteilungen (Nachberichtigungspflicht).

Nicht immer ist gewährleistet, dass Daten sich unter alleiniger Verfügungsgewalt der Daten verarbeitenden Stelle befinden (etwa während einer Datenübertragung) oder ein IT-System sie verlässlich schützt (z.B. bei der Umgehung von Zugriffsschutzmechnismen, etwa durch Schadsoftware oder Administratoren). Wie bei der Maßnahme „Verschlüsselung“ für das Schutzziel Vertraulichkeit gibt es auch in Bezug auf die Integrität Mechanismen, die direkt auf Ebene der Daten ansetzen, nämlich Prüfsummen (z. B. Hashwerte) und Signaturen. Diese können (anders als eine Verschlüsselung) eine Schutzzielverletzung nicht verhindern, aber zumindest erkennen lassen. Um den gewünschten Zustand wieder herstellen zu können, müssen weitere Maßnahmen implementiert werden, etwa Archivierungen und Backups, Rückgriffe auf Änderungsprotokollierungen oder erneute Anforderungen von Datenübertragungen.

Hier wird auch die Skalierung der Maßnahmen im Hinblick auf Schutzbedarfe deutlich: Misst man den Schutzbedarf bezüglich der Integrität anhand der Folgen einer Integritätsverletzung für den Betroffenen, so lassen sich notwendige Maßnahmen daraus ableiten. Hat beispielsweise eine nicht nachvollziehbare Adressänderung eines Betroffenen bei der Zusendung von Werbematerial nur geringe Folgen, so dürfte eine Einschränkung der Schreibrechte hinreichend sein. Geht es hingegen um den Schutz gegen unbefugte Änderungen von Kontodaten, so wird neben einer sorgfältigen Authentisierung und Autorisierung auch eine Änderungsprotokollierung erforderlich sein. Ist man im Bereich ausschließlich elektronisch gespeicherter Personal- oder Krankenakten, so dürfte (neben diesen Maßnahmen) eine elektronische Signatur angemessen sein.

Interessant ist die Betrachtung des Schutzzieles Integrität in Bezug auf Prozesse und Verfahren: Ziel ist hier, dass ein Verfahren so abläuft, wie es konzipiert und festgelegt wurde. Dies hat mittelbare Auswirkungen auf die Integrität der Daten. Standardmechanismen sind geordnete Änderungsprozesse[19], die ein unkoordiniertes und ggf. manipulatives Eingreifen in Prozesse und Verarbeitungsweisen abwehren.

2.3 Intervenierbarkeit

Die Intervenierbarkeit soll Voraussetzungen für die Durchsetzbarkeit von Betroffenenrechten (z.B. Auskunft, Gegendarstellung, Löschung, Sperrung) schaffen. Auf Ebene der Daten sind entsprechende Datenkategorien (etwa Sperr- und Widerspruchshinweise), und (Text-) Felder für Gegendarstellungen zu schaffen, die auf der Systemebene (insbesondere softwareseitig) auch genutzt werden.[20] Bei IT-Systemen bedeutet Intervenierbarkeit, dass auch einzelne Funktionalitäten und Systemkomponenten gesperrt werden können, ohne dass das Gesamtsystem in Mitleidenschaft gezogen wird. Bei Prozessen ist ggf. eine bewusste Durchbrechung der „üblichen“ Verfahrensweise erforderlich, um die Betroffenenrechte durchsetzen zu können, etwa die komplette Löschung bei unrechtmäßiger Speicherung. Aber auch Eingriffsmöglichkeiten bei nicht korrekt ablaufenden automatisierten Einzelentscheidungen[21] sind zunächst auf der Prozessebene vorzusehen, und technisch auf Ebene der Systeme und Daten bereitzustellen.

2.4 Vertraulichkeit

Anforderungen an die Vertraulichkeit beziehen sich zunächst auf Daten, dem Wortlaut des LDSG-SH nach auch auf Verfahren: Es ist zu gewährleisten, dass „nur befugt auf Verfahren und Daten zugegriffen werden kann“[22]. Bei der Formulierung wurde die Tatsache, dass Daten nicht alleine existieren, sondern durch IT-Systeme und in Prozessen verarbeitet werden, nicht ganz präzise formuliert: Der Begriff „Zugriff“ ist nicht legaldefiniert. Gemeint ist auf Ebene der Daten sicherlich die Möglichkeit der Kenntnisnahme und weiteren Verarbeitung von Daten; ein „Zugriff“ auf Verfahren könnte man als „Verwendung“ oder „Benutzung“ von Verfahren verstehen.

Wie bei Maßnahmen zur Umsetzung des Schutzziels Integrität ist zu unterscheiden, ob die Daten selbst geschützt werden müssen (etwa bei der Übertragung in Netzen, auf Datenträgern wie USB-Sticks oder Laptop-Festplatten) oder ob IT-Systeme zur Verfügung stehen, um zwischen befugten und unbefugten Zugriffen unterscheiden zu können (etwa bei der Durchsetzung von Zugriffsrechten durch Betriebs- oder Datenbankmanagementsyste-

16 BSI-Standard 100-2, Kap. 4.6.

17 Siehe auch die Definition in Abschnitt 2.25 der Norm ISO 27000:2009 : integrity = property of protecting the accuracy and completeness of assets, wobei man unter „assets“ alles das versteht, was Wert für eine Organisation hat (2.23: asset: anything that has value to the organization). Als Beispiele werden u.a. Informationen, Software, Hardware, Personen und ihre Fähigkeiten sowie immaterielle Güter wie Reputation genannt.

18 § 5 Abs. 1 Nr. 2 LDSG-SH

19 Z. B. Test- und Freigabeverfahren, aber auch geordnete Verfahren zur Berücksichtigung von Wechselwirkungen bei Veränderungen, etwa im Rahmen eines Change-Managements. Change-Managements siehe auch Prietz, Christian: Musterprozesse zum Datenschutzmanagement.DuD, 36. Jahrgang 2012, Heft 1, S. 14-19.

20 Ein Beispiel für detaillierte Anforderungen finden sich in der „Orientierungshilfe Krankenhausinformationssysteme“ der Datenschutzbeauftragten des Bundes und der Länder [http://www.datenschutz.rlp.de/downloads/oh/dsb_info_kis.pdf] , wo neben der Existenz von Kennzeichen (etwa „Mitarbeiter“, „VIP“) (Kapitel 1) auch die entsprechenden Konsequenzen für die Zugriffsrechte (Kapitel 4.1) gefordert werden.

21 § 6a Abs. 1 BDSG

22 § 5 Abs. 1 Nr. 3 LDSG-SH, ähnlich, aber präziser ISO27000 Nr. 2.29: confidentiality: „property that information is not made available or disclosed to unauthorized individuals, entities, or processes“

me oder Applikationen). Im ersten Fall ist eine Verschlüsselung das Mittel der Wahl. Je nach dem Schutzbedarf der Daten sind die Stärke der Verschlüsselung (Algorithmen, Schlüssellänge), das Algorithmenmanagement (Umschlüsseln) und das Schlüsselmanagement zu wählen.

Können IT-Systeme zum Schutz der Vertraulichkeit beitragen, so kommen Zugriffskontrollverfahren zum Einsatz. Nicht in allen Fällen können diese einen wirksamen Schutz garantieren, da sie meistens durch eine hierarchische Rechtestruktur geprägt sind, in der eine einzelne Person oder Rolle („Chefadministrator") sich Zugriffsrechte verschaffen kann, die ihm nicht zusteht. Hier müssen ergänzende Maßnahmen zum Einsatz kommen, vgl. Zweite Beobachtung. Je nach Schutzbedarf kann eine Protokollierung und Protokollkontrolle administrativer Tätigkeiten, ggf. kombiniert mit automatisiertem Monitoring und Alarmierung ausreichend sein; denkbar ist bei höheren Schutzbedarfen auch der Einsatz von Verschlüsselungen auf Datenebene (z.B. in Datenbankmanagementsystemen, Festplattenverschlüsselung). Dadurch kann eine zufällige (ungewollte) Kenntnisnahme durch Administratoren verhindert werden; bei geeigneter Verteilung der Schlüsselgewalt an eine zweite Instanz (z. B. Administratoren eines Auftraggebers) kann eine technische Gewaltenteilung erreicht werden kann.

2.5 Transparenz

Das Schutzziel Transparenz erfordert, dass „die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann". Dies betrifft wohl die Verarbeitung auf Ebene einzelner Daten(sätze) als auch die dazu verwendeten IT-Systeme und die Verfahrensweise einschließlich einzelner Prozessschritte und schließt den Begriff der Revisionsfähigkeit mit ein.[23]

Standardmaßnahmen auf Ebene der Daten ist die Protokollierung der Datenverarbeitung, deren Detaillierungsgrad bei normalem Schutzbedarf mit der Protokollierung der Eingabe beginnt und bei sehr hohem Schutzbedarf auch die Protokollierung einzelner Lesezugriffe auf dedizierten Protokollservern umfassen kann.

Auf Ebene der Systeme erfordert das Schutzziel Transparenz zum einen die Dokumentation der eingesetzten Systeme und ihrer Konfiguration, zum anderen auch die Dokumentation von Veränderungen und administrativen Eingriffen. Ob man dies durch eine Protokollierung der Eingriffe (z. B. Aufzeichnung aller administrativer Tätigkeiten mittels Kommandozeilen-Protokoll oder Screenshots) oder durch Versionierung der Systemdokumentation umsetzt, dürfte eine Frage der Dynamik und des Umfangs der Veränderungen sein. Aber auch der Schutzbedarf ist relevant, nämlich im Hinblick auf die Frage der Folgen, wenn die Dokumentation nicht ordnungsgemäß erfolgt: Hier macht es eine Unterschied, ob beispielsweise der Aufstellungsort von IT-Systemen nicht korrekt nachgepflegt wurden oder ob (manipulative) Änderungen von Zugriffsrechten durch Administratoren nicht protokolliert werden.

Auf Ebene der Prozesse sind zum einen die Verfahren selbst im Sinne einer klassischen Verfahrensdokumentation zu dokumentieren[24], zum anderen auch die Prozesse, mit denen Änderungen bewirkt werden (Änderungsprozesse)[25].

2.6 Nicht-Verkettbarkeit

Durch das Schutzziel Nicht-Verkettbarkeit soll verhindert werden, dass „personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können"[26]. Vordergründig sind allein Daten Gegenstand des Schutzzieles; die Schutzmaßnahmen können aber auch auf Ebene der IT-Systeme und Prozesse angreifen, etwa durch das Unterbinden unbefugter Zugriffe auf Systemebene oder durch eine Prozessgestaltung, die nicht erforderliche Daten gar nicht erst erhebt, die Daten unmittelbar nach Zweckerreichung löscht[27] und eine Sperrung effektiv durchsetzt, d.h. eine weiteren Nutzung unterbindet.

Ähnlich wie bei den Schutzzielen Vertraulichkeit und Integrität kann man unterscheiden, ob ein Schutz

- auf Ebene der Daten selbst (z. B. durch Anonymisierung, Pseudonymisierung oder Nicht-Erhebung identifizierender Daten),
- auf Ebene der Systeme, etwa durch Einrichtung entsprechender Zugriffsrechte oder der Verarbeitung auf unterschiedlichen Systemen oder
- auf Ebene der Prozessgestaltung (z. B. durch spezifisch Vorgaben für Auftragsdatenverarbeiter, die diesem Zusammenführung und damit zweckwidrige Verarbeitung erschweren)

erfolgt. Der umzusetzende Schutzbedarf kann dazu herangezogen werden, Schutzmaßnahmen zu skalieren: Eine solche Skalierung könnte von organisatorischen Regelungen (etwa Verwendungsverbote[28], Vier-Augen-Prinzipien (z. B. bei Protokollauswertungen[29]), institutionalisierter Gewaltenteilung (Datenverarbeitung durch unterschiedliche Verantwortliche Stellen), technische Gewaltenteilung (z. B. logische Trennung durch Zugriffsrechte unter Berücksichtigung derjenigen Rollen, die eine Änderung der Zugriffsrechte und damit Aufhebung der Trennung bewirken könnten, Mandantentrennung, unterschiedliche physische Systeme) bis hin zu einem Schutz auf Ebene der Daten selbst (Anonymisierung, Pseudonymisierung, explizite Verwendung verschiedener Identifizierungsdaten[30] oder regelmäßige Neuvergabe von Identifizierungsdaten) reichen.[31]

3 Maßnahmenkataloge

Tabelle 1 gibt einige der aufgeführten Maßnahmen wieder. Sie beantwortet die Frage: Welche Maßnahmen sind für die Umset-

23 Die meisten Landesdatenschutzgesetze beziehen das Schutzziel Transparenz auf „Verfahrensweisen" und somit auf eine Verfahrensbegriff; die Verarbeitung einzelner Daten betrachten sie beim Schutzziel Revisionsfähigkeit.

24 Vgl. § 3 Datenschutzverordnung Schleswig-Holstein (DSVO-SH)

25 z.B. Change-Management gemäß ITIL.

26 § 5 Abs. 1 Nr. 5 LDSG-SH

27 Entsprechenden Regelung sind zwar an anderer Stelle schon gesetzlich normiert (z.B. § 3a BDSG Datensparsamkeit und Datenvermeidung; § 20 Abs. 2 Nr. 2 und § 35 Abs .2 Nr. 3, 4 BDSG zur Löschung nach Wegfall der Erforderlichkeit), doch steht die Beschreibung der Umsetzung durch technisch-organisatorische Maßnahmen aus.

28 Z. B. § 31 BDSG, §§ 13 Abs. 6, 23 Abs. 2 LDSG-SH

29 Z. B. Beteiligung der Personalvertretung, siehe § 21 Abs. 2 Nr. DSG M-V

30 Beispielsweise der Verzicht auf ein allgemeines Personenkennzeichen und stattdessen die Nutzung verschiedener Nummern wie Sozialversicherungsnummer, Krankenversicherungsnummer, Steuer-Identifikationsnummer etc.

31 Etwa durch die Begrenzung der Lebensdauer von identifizierenden Cookies in Web-Anwendungen, siehe z. B. Position paper on certifiability of online behavioural advertising systems according to Euro-PriSe – Follow-up, 2011, https://www.european-privacy-seal.eu/results/Position-Papers/EuroPriSe Follow.pdf, S. 11.

Tabelle 1 |

	Daten	Systeme	Prozesse
Verfügbarkeit Findbarkeit Ermittelbarkeit Verbindlichkeit	D 1.1 Einschränkung von Lösch-/Veränderungsrechten D 1.2 Schutz vor Schadsoftware D 1.3 Backup der Daten	S 1.1: Schutz vor Schadsoftware S 1.2: Backup von Konfigurationen und Software S 1.3: Hardwareredundanz S 1.4: Ausweichräume, und -Netze	P 1.1: Vertretungspersonal P 1.2: Fähigkeit zur Aufgabenerledigung durch Dritte (Vorbereitung Outsourcing) P 1.3: Ausweichprozesse, Planung von Notfallszenarien, Amtshilfe
Vertraulichkeit Verdecktheit Anonymität Unbeobachtbarkeit	D 2.1: Einschränkung von Leserechten (für Datenverarbeiter, ggf. durch den Nutzer selbst) D 2.2: Protokollierung lesender Zugriffe D 2.3: Verschlüsselung der Daten D 2.4: Ende-zu-Ende-Verschlüsselung	S 2.1: Einschränkung von lesenden Zugriffsrechten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 2.2: Verschlüsselung auf Systemebene (Festplatten, Datenbank)	P 2.1: Verpflichtung auf das Datengeheimnis (BDSG) P 2.2: Verschwiegenheitsvereinbarungen P 2.3: Geeignete Organisation bei der Vergabe von Zugriffsrechten („need-to-know“)
Integrität Zurechenbarkeit	D 3.1: Einschränkung von Schreib- und Änderungsrechten D 3.2: Protokollierung von schreibenden/ändernden Zugriffen D 3.3: Protokollierung geänderter Daten D 3.4: Nachberichtigung D 3.5: technische Integritätskontrollen (Signaturen/Hashes)	S 3.1: Einschränkung von schreibenden Zugriffen/Konfigurationmöglichkeiten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 3.2 Schutz vor Schadsoftware S 3.3: Regelmäßige Integritätsprüfungen/Audits	P 3.1: Detaillierte Planung von Verfahren und Verfahrensschritten P 3.2: Geordnete Zuweisung von Rechten und Rollen P 3.3: Geordnete Änderung von Verfahren und Verfahrensschritten P 3.4: Regelmäßige Überprüfung (z.B. Verfahrensqualität) und Nachsteuern
Nicht-Verkettbarkeit	D 4.1: Löschen, nach Wegfall der Erforderlichkeit; ggf. „Wipen“ D 4.2 Einschränkung von Verarbeitungs- / Nutzungs- / Übermittlungsrechten für einzelne Daten D 4.3: Kennzeichnung der Zwecke auf Ebene der Daten D 4.4: Einschränkung von identifizierenden Daten; Pseudonymisierung D 4.5: Anonymisierung von Daten	S 4.1: Kennzeichnung der Zwecke auf Ebene des Systeme S 4.2: Trennung von Datenbeständen S 4.3: Einschränkungen von Verarbeitungs-, Nutzungs- und Übermittlungsmöglichkeiten (Funktionalitätseinschränkung) S 4.4: Trennung auf Systemebene (Software, Hardware; Mandantenfähigkeit) S 4.5: Physikalische Trennung und unabhängige RZ-Betreiber	P 4.1: Trennung auf Verfahrensebene P 4.2: Rechte + Rollenvergabe, ggf. an eine andere rechtliche Entität (z. B. Personalvertretung) P 4.3: Gewaltenteilung (z.B. Durchführung einzelner Verfahrensschritte durch andere rechtliche Entitäten)
Transparenz	D 5.1: Dokumentation der Datenfelder einschließlich Erforderlichkeit D 5.2: Protokollierung von Datenverarbeitungen mit Schutzbedarf zunehmender Detaillierungsgrad und Speicherdauer D 5.3: Integritätsschutz der Protokolle (separater Protokollierungsserver)	S 5.1: Dokumentation der Systeme (Hardware, Software, Algorithmen) S 5.2: Protokollierung von Konfigurationsänderungen S 5.3: zunehmende Kontrolldichte bei höherem Schutzbedarfen; automatisiertes Monitoring	P 5.1: Dokumentation des Verfahren und einzelner Prozesse (einschließlich beteiligter Organisationseinheiten, Rollen und Übermittlungen an Dritte) P 5.2: Dokumentation der Änderungsprozesse
Intervenierbarkeit Kontingenz / Abstreitbarkeit	D 6.1: Schaffung notwendiger Datenfelder (z. B. für Gegendarstellungen) und Kennzeichnungen	S 6.1: Funktionalitäten in den Systemen für die Bearbeitung von Sperrungen, Widersprüchen, Beauskunftungen S 6.2: Funktionalitäten in den Systemen für die Umsetzung von weiteren Rechten Betroffener (z. B. Rufnummerunterdrückung, Pseudonyme Nutzungsmöglichkeit, etc.) S 6.3: Funktionalitäten für Betroffene, einzelne Betroffenenrechte direkt wahrzunehmen (z.B. Auskunftsportal, „Datenbrief“, Zusendung von Protokollen, eigene Änderungsmöglichkeiten) S 6.4: Steuerungsmöglichkeiten für einzelne Funktionen („Overrride“) bei automatisierten Einzelentscheidungen S 6.5: Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem	P 6.1: Organisation der Umsetzung der Betroffenenrechte (Rechte + Rollen für Auskunft, Sperrungen) P 6.2: Single Point of Contact für Datenschutzfragen P 6.3: Organisation der Umsetzung der Betroffenenrechte (Rechte und Rollen bei der Bearbeitung von Gegendarstellungen und Einwänden; Übersteuern einzelner Prozesse, insb. automatisierter Einzelfallentscheidungen) P 6.4: Durchgriff des Nutzers auf seine Daten („Selbstverwaltung“) P 6.5: (zertifiziertes) Changemanagement auf Seiten der Organisation

zung auf Ebene der Komponenten Daten, Systemen und Prozessen geeignet, um im Zusammenwirken das Schutzziel X zu befördern bzw. umzusetzen? Sie trifft eine Tendenzaussage in Bezug auf die Mechanismenstärke und damit auf den Schutzbedarf: tendenziell steigt innerhalb einer Tabellenzelle die Stärke von Maßnahmen und damit die Geeignetheit für höhere Schutzbedarfe. Diese Tabelle kann, insbesondere im Hinblick auf die umfangreichen Maßnahmenkataloge zur IT-Sicherheit[32], allenfalls als erster Diskussionsbeitrag verstanden werden; zu untersuchen bleibt beispielsweise, ob es *innerhalb* der Umsetzung einer Maßnahme (z. B „Zugriffskontrolle“) verschiedene Mechanismenstärken gibt, die mit den Schutzbedarfen korrelieren (beispielsweise im Hinblick auf die Güte der Authentisierung oder die Qualität der Rechtezuweisung).

4 Anwendung der Schutzziele bei der Maßnahmenumsetzung

Bereits im Abschnitt Verfügbarkeit war darauf hingewiesen worden, dass bei der Umsetzung von Maßnahmen zur Implementierung eines Schutzzieles die übrigen Schutzziele ebenfalls betrachtet werden müssen. Es geht nicht um die Abwägung von Schutz-

32 Z. B. die Maßnahmenbündel der IT-Grundschutzkataloge oder die „Controls“ der Norm ISO 27002.

zielen (bzw. der Umsetzungsintensität der zugehörigen Maßnahmen) gegeneinander, sondern um die Beachtung der Schutzziele *bei* der Maßnahmenumsetzung. Dabei sollte man sich nicht nur am (gesetzlichen) Wortlaut der Schutzziele orientieren, der personenbezogene Daten im Blick hat, sondern am Fokus der Schutzziele: Maßnahmen sind so umzusetzen, dass die durch sie geschützten Verfahrenskomponenten (Daten, Systeme und Prozesse) die Betroffenenrechte wahren. Zusätzlich müssen sie auch die Rechte anderer Betroffener wahren (z. B. des Personals der Daten verarbeitenden Stelle). Folgende Beispiele mögen dies erläutern:

4.1 Beispiel Backup

Beim „Durchdeklinieren" der Schutzziele für Backup-Verfahren findet man einige bedenkenswerte Aspekte: Auch Backup-Dateien sind vertraulich zu behandeln und ggf. zu verschlüsseln, sind ihrerseits schutzbedürftig im Hinblick auf Verfügbarkeit (Haltbarkeit und Aufbewahrung von Datenträgern) und vor Manipulation zu schützen (Integrität). Aber auch die Betrachtung der Schutzziele Transparenz (z. B. Dokumentation des Ablaufs der Datensicherung, der Verantwortlichkeiten und der entstehenden Datenbestände; Protokollierung von Datensicherungen und Rückeinspielungen), Nicht-Verkettbarkeit (z.B. keine zweckwidrige Nutzung von Backup-Daten in anderen Zusammenhängen, klare Trennung von Backup und Archivierung) und Intervenierbarkeit (Löschungsmöglichkeiten in Backup-Dateien, Schutz vor versehentlicher Rückeinspielung bereits gelöschter Datenbestände aus Backups) kann dabei helfen, Backup-Verfahren datenschutzgerecht zu implementieren.

4.2 Beispiel Zugriffskontrolle

Schutzziele und ihre Umsetzung durch Schutzmaßnahmen erfordern, befugte Handlungen zuzulassen und unbefugte Handlungen abwehren zu können. Befugt bzw. unbefugt können nicht nur Personen, sondern auch Rollen, andere verantwortliche Stellen, IT-Systeme und Prozesse sein. Der Begriff „Handlung" ist hier ganz allgemein zu verstehen und umfasst nicht nur die in § 9 Abs. 1 BDSG (vgl. Fußnote 13) genannten Zutritte, Zugänge und Zugriffe[33], sondern auch einzelne Verarbeitungsschritte (z. B. Nutzen oder Übermitteln), die Konfiguration von IT-Systemen oder die Festlegung von Prozessschritten.[34] Eine technisch-organisatorische Umsetzung erfolgt mit Hilfe eines Berechtigungskonzeptes (Sollvorgabe) und seiner (größtenteils technischen) Durchsetzung.[35] Neben der Festlegung von Berechtigungen und ihrer Durchsetzung (Autorisierung) ist die Überprüfung der Identität der handelnden Personen, IT-Systeme und Prozesspartner entscheidend (Identifizierung und Authentisierung, z.B. durch Passwörter, Chipkarten, biometrischen Verfahren und Zertifikate). Auch eine Authentisierung ohne Identifikation ist möglich (z.B. durch mechanische Schlüssel), die aber eine Protokollierung und eindeutige Zuordnung der Handlungen erschwert[36].

Da eine Zugriffskontrolle gleichzeitig mehreren Schutzzielen zumindest teilweise dienen kann (vgl. Erste Beobachtung), sollte sie als Querschnittsfunktion als eigenständiges Verfahren betrachtet werden. Eine Betrachtung unter dem Aspekt „Lebenszyklus" ermöglicht es, vergessene Prozessschritte (wie den Entzug von Zugriffsrechten) aufzuspüren.

Schutzziele für Zugriffskontrollen

Betrachtet man die Implementierung einer Zugriffskontrolle unter dem Blickwinkel der Schutzziele, so werden typische Aufgaben offenbar: Authentisierungsdaten und ggf. Nutzernamen sind vertraulich zu behandeln; Passwörter nur als Hashwerte zu speichern. Auch die Integritätsanforderungen an diese Daten sind evident. Ebenso muss zusammen mit den Daten auch das gesamte Verfahren verfügbar sein und im Fehlerfall in einen sicheren Zustand fallen. Ob durch ein Authentisierungsverfahren eine Verkettung mit anderen Aktivitäten erfolgen kann und soll, ist hingegen eine Designfrage: Wird beispielsweise als Benutzername einer Authentisierung (Name/Passwort) in einer Webanwendung eine E-Mail-Adressse verwendet, so wurde eine Verkettungs- und Adressierungsmöglichkeit geschaffen. Im Hinblick auf die Intervenierbarkeit findet man die Notwendigkeit von Passwortrücksetzungsmechanismen, aber auch von Sperr- und Konto-Deaktivierungsmöglichkeiten. Es kann auch bedeuten, dass Nutzer selbst (temporäre) Sperrmöglichkeiten haben müssen. Auf Ebene der Transparenz stellt man fest, dass nicht nur der technische Vorgang selbst sowie das Verfahren zur Vergabe und Entzug von Authentisierungsmitteln beschrieben werden muss (Dokumentation), sondern dass auch einzelne Authentisierungsvorgänge durch den Nutzer selbst nachvollzogen werden können sollten.[37]

5 Fazit

Die gegenwärtig bekannten und gebräuchlichen Maßnahmen lassen sich nicht eins-zu-eins einzelnen Schutzzielen zuordnen, sondern tragen (häufig) zur Umsetzung mehrerer Schutzziele bei, indem sie sie direkt unterstützen oder unzulängliche Umsetzungen anderer Maßnahmen flankieren.

Betrachtet man einzelne Schutzmaßnahmen als (Unter-)Verfahren, so bestehen auch sie aus dem Komponenten Daten, Systeme und Prozesse, die sich wiederum an den Schutzzielen messen lassen müssen. Bei dieser Betrachtung sollte man sich nicht an den (gesetzlichen) Wortlaut der Schutzziele klammern.

33 Im englischen Sprachgebrauch „access control", siehe z.B. Anderson, Ross: Security Engineering. A Guide to Building Dependable Distributed Systems. 2. Auflage. Wiley, 2008, Kap. 4 und 11.

34 Mangels eines besseren Begriffes wird hier der Begriff „Zugriffkontrolle" verwendet.

35 Nicht-technische Umsetzungen sind manuelle Berechtigungsprüfungen, etwa Prüfungen von Zutrittsberechtigungen durch Wachpersonal, oder Weisungsberechtigungen im Rahmen der Auftragsdatenverarbeitung. Die Qualität der Prüfung hängt dabei von der Sorgfalt und Durchsetzungsfähigkeit der Prüfenden ab

36 Zu Credentials, die einerseits eine eindeutige Zuordnung erlauben, die Auswertung aber stark einschränken, siehe Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin and Harald Zwingelberg: D2.1 Architecture for Attribute-based Credential Technologies, 2011, https://abc4trust.eu/index.php/pub/107-d21architecturev1, Kap. 2.

37 Dies ist in Online-Banking-Anwendungen zu beobachten, in den Zeitpunkt der letzten Anmeldung und teilweise auch des letzten erfolglosen Zugriffsversuches angezeigt werden.