Bernd Jäger, Reiner Kraft, Annika Selzer, Ulrich Waldmann

Die Kontrolle des Umsetzungsgrades des Zugangs- und Zugriffsschutzes

Teilautomatisierte Datenschutzkontrollen im Cloud-Umfeld zur Stärkung des Vertrauens in Cloud-Dienste

Rechtlich verpflichtende Datenschutzkontrollen im Cloud-Umfeld stellen den Cloud-Nutzer vor eine große Herausforderung. Zusammen mit der Verantwortlichkeit für die in der Cloud verarbeiteten Daten und den immer noch weitverbreiteten Datenschutzbedenken gegen Cloud-Dienste, stellen diese einen Hemmschuh für die Nutzung von Cloud-Diensten dar. Teilautomatisierte Datenschutzkontrollen, die dem Cloud-Nutzer im laufenden Betrieb den Umsetzungsgrad von Datenschutzzielen anzeigen, können dieser Barriere begegnen. Dieser Beitrag schlägt ein Vorgehen für eine teilautomatisierte Messung der Datenschutzziele des Zugangs- und Zugriffsschutzes vor.

Bernd Jäger

ist Sicherheitsarchitekt bei der Colt Technology Services GmbH und zuständig für Plattform-Architekturen und Technologiestrategien.

E-Mail: bernd.jaeger@colt.net

Reiner Kraft

Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie.

E-Mail: reiner.kraft@sit.fraunhofer.de

Annika Selzer

Wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für sichere Informationstechnologie.

E-Mail: annika.selzer@sit.fraunhofer.de

Ulrich Waldmann

Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie.

E-Mail: ulrich.waldmann@sit.fraunhofer.de

1 Datenschutzkontrollen in der Cloud[1]

Unternehmen, die ihre Mitarbeiter/Kundendaten in der Cloud verarbeiten lassen, unterliegen i.d.R. den Vorschriften zur Auftragsdatenverarbeitung. § 11 Abs. 2 Satz 4 BDSG verpflichtet den Auftraggeber einer Auftragsdatenverarbeitung („Cloud-Nutzer“) etwa dazu, den Auftragnehmer einer Auftragsdatenverarbeitung („Cloud-Betreiber“) regelmäßig datenschutzrechtlich zu überprüfen. Eine persönliche Vor-Ort-Kontrolle kann besonders kleinen und mittelständischen Unternehmen jedoch weder inhaltlich noch finanziell zugemutet werden und würde in einen regelrechten „Prüf-Tourismus“ resultieren. Wünschenswert wären daher Ansätze zur automatisierten Datenschutzkontrolle im Cloud-Umfeld.

Ein Lösungsansatz besteht in der Realisierung von automatisiert ermittelbaren Datenschutzmetriken – also Kennzahlen zur Beurteilung datenschutzrelevanter Eigenschaften auf Basis von vertrauenswürdigen Messdaten – für das Cloud-Umfeld. Das Ziel von Datenschutzmetriken sollte es sein, den Umsetzungsgrad der von dem Cloud-Betreiber umgesetzten Datenschutzmaßnahmen kontinuierlich zu überprüfen und dem Cloud-Nutzer diese Ergebnisse branchenspezifisch und verständlich anzuzeigen.

1 Der Beitrag entstand im Projekt VeriMetrix, gefördert vom BMBF im Programm „IKT 2020 – Forschung für Innovationen“, Förderkennzeichen: 16KIS0053K.

In [JäSW15] wurde ein solcher Ansatz beispielhaft für die automatisierte Kontrolle des Verarbeitungsstandortes in der Cloud vorgestellt. In diesem Beitrag möchten die Autoren einen Vorschlag für eine automatisierte Kontrolle des Zugangs- und Zugriffsschutzes in der Cloud unterbreiten.

2 Zugangs- & Zugriffsschutz im Überblick

Gem. § 9 Satz 1 Bundesdatenschutzgesetz sind Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, dazu verpflichtet, technische und organisatorische Maßnahmen zu treffen, um die Betroffenen vor unberechtigten Umgängen mit ihren personenbezogenen Daten zu schützen.[2] Dazu gehören auch Maßnahmen zum Zugangs- und Zugriffsschutz auf personenbezogene Daten.

Der Zugangsschutz hat gemäß Satz 2 Nr. 2 der Anlage zu § 9 Satz 1 BDSG das Ziel zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Der Zugriffsschutz hat demgegenüber gemäß Satz 2 Nr. 3 der Anlage zu § 9 Satz 1 BDSG folgende zwei Ziele:

- Die zur Benutzung eines Datenverarbeitungssystems Berechtigten sollen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und
- personenbezogene Daten sollen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Im Gegensatz zur Zugangskontrolle, die verhindern soll, dass Unbefugte ein Datenverarbeitungssystem benutzen können, ist der Nutzer des Datenverarbeitungssystems bei der Zugriffskontrolle grundsätzlich berechtigt, dieses zu nutzen. Die Zugriffskontrolle soll wiederum ausschließen, dass ein berechtigter Nutzer auf alle in dem Datenverarbeitungssystem gespeicherten Daten Zugriff erhält. Der Zugriff auf personenbezogene Daten soll auf bestimmte Daten auf dem System je Nutzer beschränkt werden, welche der jeweiligen Erfüllung der Aufgaben eines Nutzers/Mitarbeiters entsprechen [u. a. TaGa10, Münc10].

Die Zugriffskontrolle – hinsichtlich des ersten der beiden oben genannten Ziele – ist ohne vorherige Zugangskontrolle nicht möglich. Diese wiederum lässt sich unter anderem durch ein Zugangsberechtigungskonzept, die Benutzerkennung sowie durch Firewalls und Verschlüsselung erreichen. Darauf aufbauend erfolgt im zweiten Schritt die Umsetzung von technischen und organisatorischen Maßnahmen zum Zugriffsschutz. Auch hierfür ist zunächst die Erstellung eines umfassenden Berechtigungskonzepts unerlässlich. Zudem sollten unter anderem ein ausreichend sicheres Zugriffsberechtigungssystem eingerichtet werden, eine datenschutzkonforme[3] Protokollierung der Systemnutzung (Zugriff auf ein bestimmtes Objekt; einem Nutzer für einen bestimmten Zeitraum zugewiesenen Rechte) sowie der Missbrauchsversuche erfolgen und ausgewertet werden, dem Stand der Technik entsprechende Verschlüsselungsverfahren zum Einsatz kommen sowie ADV-Verträge mit Wartungs- Putz- und Entsorgungsdienstleistern geschlossen werden, u. a. [GoSc12], [DKWW13], [Münc10], TaGa10].

3 Konzept teilautomatisierter Messungen

Das Projekt VeriMetrix hat es sich zum Ziel gesetzt, den Umsetzungsgrad von Datenschutzmaßnahmen, eines Cloud-Betreibers zum Schutz der personenbezogenen Daten, die ein Cloud-Nutzer in der Cloud verarbeiten lässt, auf Basis von Datenschutzmetriken soweit wie möglich im laufenden Betrieb automatisiert messbar zu machen. Derzeit ist es allerdings auf Grund der Technik sowie der Betriebsgegebenheiten bei Cloud-Betreibern nicht möglich, den Umsetzungsgrad sämtlicher von dem Cloud-Betreiber getroffenen Datenschutzmaßnahmen vollständig automatisiert zu messen. Daher sieht das Projekt VeriMetrix eine Auditorschnittstelle vor, über welche ein Auditor die zur vollständig automatisierten Messung fehlenden Angaben auf Basis von Dokumentenprüfungen und Vor-Ort-Kontrollen in das VeriMetrix-System eingeben kann. Das VeriMetrix-System verarbeitet die Auditor-Eingaben wiederum als weitere Messquelle für die Metrikenberechnung, so dass sich die Gesamtmetrik zu einem Datenschutzziel – wie zum Beispiel dem ordnungsgemäß umgesetzten Zugangs- und Zugriffsschutz – sowohl aus den im laufenden Betrieb automatisiert gemessenen Messdaten sowie aus den händisch erhobenen Auditor-Eingaben berechnet.

VeriMetrix schlägt vor, für die händischen Anteile einen unabhängigen Auditor einzusetzen, der seine Kontrolle – je nach Schutzbedarf der in der Cloud verarbeiteten personenbezogenen Daten – in einem Prüfturnus von ein bis drei Jahren wiederholt. Um die zusätzlichen Kosten für eine solche Prüfung möglichst niedrig zu halten, schlägt VeriMetrix vor, tatsächlich nur diejenigen Kontrollen händisch durchzuführen, die nicht bereits automatisiert durchgeführt werden können. Da sich im Laufe der Zeit voraussichtlich immer mehr Kontrollbereiche automatisiert erschließen lassen werden, nimmt der Prüfungsaufwand des Auditors in VeriMetrix im Laufe der Zeit idealerweise ab.

Die automatisierten Kontrollen sollen vorwiegend[4] kundenspezifisch durchgeführt werden, das heißt, die automatisierten Kontrollanteile werden auf den virtuellen Maschinen (VMs) eines bestimmten Kunden durchgeführt. Demgegenüber sollen händische Kontrollen durch den Auditor kundenunspezifisch stattfinden, um einerseits das Risiko zu minimieren, dass dem Auditor durch seine Kontrolle personenbezogene Daten der Cloud-Kunden bekannt werden, und um andererseits die Kosten für solche Audits gering zu halten. Eine Ausnahme von der kundenunspezifischen Messung durch den Auditor könnte die auf Wunsch eines Kunden und für ihn spezifische Prüfung des Auftragsdatenverarbeitungsvertrages darstellen.

4 Automatisierte Überprüfung

Die Überprüfung des Zugangs- und Zugriffsschutzes lässt sich in Form von Messfeldern strukturieren, d. h. Prüfkriterien als Grundlage von automatisierten und händischen Messungen heranzuziehen.[5] Die gemessenen Werte entsprechen einer angemessenen oder unangemessenen Umsetzung einer Anforderung

2 Gem. § 9 Satz 2 BDSG sind Maßnahmen nur dann erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

3 Es ist u. a. darauf zu achten, nur notwendige Daten zu protokollieren, den Zugriff auf die Protokolldaten zu beschränken und die Aufbewahrungsfristen für diese Daten so gering wie möglich zu halten.

4 Eine Ausnahme bildet die in 4.3 beschriebene Messung.

5 Die automatisierte Messung von Datenschutzeigenschaften zur Erfüllung des Transparenzgrundsatzes kann im Spannungsfeld zu den Grundsätzen Datensparsamkeit und Datenvermeidbarkeit stehen. Um diesem Spannungsfeld zu begegnen, muss sichergestellt werden, dass die automatisierte Messung wiederum datenschutzkonform erfolgt.

oder legen zumindest den Verdacht einer unzureichenden Umsetzung nahe.
In den folgenden Abschnitten werden als automatisiert überprüfbare Messfelder des Zugangsschutzes die Überprüfung der Firewall-Konfiguration (Abschnitt 4.1) und der netzbasierte Filtermechanismen gegen Spoofing (Abschnitt 4.2) vorgestellt. Als Messfelder des Zugriffschutzes dienen die Konfigurationsprüfung der Web-Portale für den Self-Service (Abschnitt 4.3) und die Überprüfung der Zugriffskonfiguration unter Nutzung der VMM-APIs (Abschnitt 4.4). Beispiele für weitere Messfelder, zur Bewertung des Zugangs- und Zugriffsschutzes, finden sich unter anderem in [Sowa10].

4.1 Firewall-Konfiguration

Automatisiert lässt sich überprüfen, ob netzbasierte Zugangskontrollen (z. B. eine Internet-Firewall) vorhanden sind und einen effektiven Zugangsschutz sicherstellen. Ein solcher Schutz ist zwingend erforderlich für Server, welche eine öffentliche Kunden-Administrationsschnittstelle (z. B. Internet-Portal) des Cloud-Services bereitstellen, und liegt in der Verantwortung des Cloud-Betreibers. Eine Überprüfung kann auch dann relevant sein, wenn die VMs eines Kunden durch virtuelle oder physikalische Firewalls, die vom Cloud-Betreiber z. B. als „Managed Service" betrieben werden, geschützt werden.
Ein periodisch ausgeführter Messvorgang entspricht im Prinzip dem eines typischen Tests auf Netzschwachstellen (Port Scan). Der auf dem Kollektor platzierte Portscanner dokumentiert erreichbare Netzdienstzugangspunkte (Ports) und vergleicht diese mit den Sollvorgaben. Beispielsweise sollte das Cloud-Administrationsportal per TCP Port 443 über eine verschlüsselte Verbindung erreichbar sein. Der üblicherweise unverschlüsselte Port 80 oder gar Fernwartungszugänge auf anderen Ports (z. B. SSH auf TCP:22) sollten nicht öffentlich erreichbar sein, selbst wenn diese Zugänge mit Maßnahmen wie etwa einem Zugangspasswort geschützt sind.

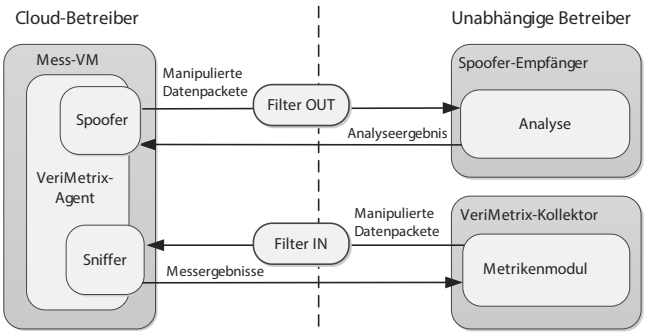
Auf dieselbe Weise kann die zulässige Kommunikation zu und von einer VM automatisiert überprüft werden, falls dies für die Beurteilung des Dienstanbieters relevant ist. Werden mehr offene Ports gemessen als in der Soll-Konfiguration vorgesehen sind, dann muss der Zugangsschutz als verringert gelten.

4.2 Filtermechanismen gegen Spoofing

Ebenfalls kann automatisch überprüft werden, ob netzbasierte Filtermechanismen, z. B. die Anti-Spoofing Konfiguration der Netzknoten auf Seiten des Betreibers, vorhanden sind und wie effektiv diese arbeiten.

Durch das Fälschen („Spoofen") von Absenderadressen kann versucht werden, netzbasierte Zugangskontrollen zu umgehen.[6] Zum Testen des Filters für ausgehende Daten können Tools zum Einsatz kommen, wie sie das MIT Spoofer Project[7] zur Verfügung stellt. Damit wird ein Messaufbau möglich, wie er in Abb. 1 gezeigt ist.

Abb. 1 | Messung auf Quelladressen-Spoofing



Links in der Abbildung ist eine Mess-VM auf Seiten des Cloud-Betreibers zu sehen. Aus der Mess-VM heraus sendet ein Spoofer-Programm Datenpakete mit gefälschten Quell-IP-Adressen zu den öffentlichen Servern des MIT-Projektes. Dort werden alle Pakete analysiert, welche die Filter der Cloud- und Internet-Betreiber durchqueren konnten. Das Ergebnis wird vom VeriMetrix-Agenten automatisiert abgerufen und ausgewertet. Zum Test der Gegenrichtung sendet der VeriMetrix-Kollektor (unten rechts in Abb. 1) ebenfalls Datenpakete mit gefälschten Absenderadressen an die Mess-VM. Ein integriertes Sniffer-Programm wertet diese empfangenen Pakete aus.

Können Pakete mit gefälschten Adressen empfangen werden, so bedeutet das, dass die notwendige Filterung unwirksam ist. Beim Empfang gefälschter Pakete wäre der Zugangsschutz unvollständig. Die Ergebnisse der Untersuchungen werden an den Kollektor gesendet und fließen dort in die Berechnung der Kennzahlen des Zugangsschutzes ein.

4.3 Konfiguration der Web-Portale

Der Zugriff auf die vom Cloud-Nutzer genutzte, virtuelle IT-Infrastruktur erfolgt meist über ein Web-Portal, welches im Internet für alle Kunden (Endkunden und Service-Vertriebspartner) des Cloud-Betreibers zur Verfügung steht. Es stellt üblicherweise mächtige, administrative Funktionen wie z. B. die Konfiguration von Firewall-Regeln oder die Verwaltung von Benutzern und deren Zugriffsrechten auf bestimmte Daten innerhalb der Kunden-Domäne zur Verfügung.

Vor unberechtigtem Zugriff auf diese Daten während der Übertragung über einen Transportweg, der sich vom Anwender nicht kontrollieren lässt und auf dessen Verlauf ggf. Einfluss genommen werden kann [Fedl12], schützt nur eine korrekt implementierte und starke Verschlüsselung und eine verlässliche Identifikation der Gegenstelle. Fehler oder bewusste Schwächung in diesem Bereich können Daten aber auch lange nach der eigentlichen Übertragung gefährden.[8] Wird ein Verfahren benutzt, das den privaten Server-Schlüssel zur Absicherung der Übertragung des eigentlichen Sitzungsschlüssel benutzt, besteht das Risiko, dass die gesamte Kommunikation nachträglich entschlüsselt werden kann, falls ein Angreifer zu einem späteren Zeitpunkt (z. B. durch einen Einbruch in den Server) Zugriff auf den Server-Schlüssel erhält. Daher bieten alternative Verfahren wie Diffie-Hellman einen besseren Zugriffsschutz.

6 Oder auch eine Überlastung des Zugangsnetzes bestimmter Dienste (DDoS) herbeizuführen.

7 http://spoofer.cmand.org/index.php.

8 Vgl. „Perfect Forward Secrecy" (PFS) https://www.perfectforwardsecrecy.com/.

Die wesentlichen Parameter der benutzten Verschlüsselung (verwendete Algorithmen, Schlüssellängen, Zertifikatsvalidierung, etc.) und einige Implementierungsdetails können durch das Simulieren eines Verbindungsaufbaus gemessen werden. Da dies aus dem Internet heraus geschehen kann, befindet sich der zugehörige Sensor auf dem Kollektor. Die Durchführung der Messungen in regelmäßigen Intervallen ermöglicht die Ableitung von Trends. Folgende Parameter sollen automatisiert überprüft werden, siehe Tab. 1.

Tab. 1 | Kriterien für den Zugriffschutz durch Verschlüsselung

Beschreibung	Beispiele[1]
Angebotene Verschlüsselungsalgorithmen	Starke Algorithmen: Symmetrisch: AES-128, AES-192, AES-256 mit Betriebsart CBC- oder CTR Asymmetrisch: z. B. RSA Schwache Algorithmen: DES, Blockchiffren im ECB-Modus
Schlüsselaustauschverfahren	Stark: Diffie-Hellman (PFS) Schwach: Verfahren, die direkt einen statischen Serverschlüssel nutzen
Angebotene Schlüssellängen	Stark: AES >= 128 Bit RSA Modulo >= 2048 Bit Elgamal-Untergruppenordnungen >=224 Bit auf einer geeigneten elliptischen Kurve Diffie-Hellman >= 2048 Bit
Transportsicherungsprotokolle	Stark; TLS 1.2 Mittel: TLS 1.0 Schwach: SSL

1 Vgl. u. a. TR-02102-1 des BSI; Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden; www.ecc-brainpool.org.

Beim Zugriff auf das Administrationsportal präsentiert der Server dem Browser ein Zertifikat, welches die Identität des Kommunikationspartners (hier der Portal-Server) beweisen soll. Die folgende Tabelle beschreibt die Zertifikatsparameter, die gemessen werden sollen:

Tab. 2 | Kriterien für die Güte des Serverzertifikats

Beschreibung	Beispiele und Merkmale
Hash-Verfahren	Werden starke Algorithmen (SHA-256, SHA-384, SHA-512) verwendet?
Herausgeber	Deutscher oder europäischer Herausgeber? Sicherheitsvorfälle beim Herausgeber?
Validierungs-kette	Ist die Kette möglichst kurz? Können alle Zwischenzertifizierungsstellen (CAs) verifiziert werden? Ist das Vertrauensniveau der CAs hoch? Ist der OCSP-Server[1] erreichbar? Sind Zertifikate gesperrt oder abgelaufen?
Pinning	Wird Pinning[2] verwendet?
Portal-Server	Liegt der Standort in Deutschland?

1 Server, welcher Informationen über gesperrte Zertifikate bereitstellt.

2 https://tools.ietf.org/html/rfc7469.

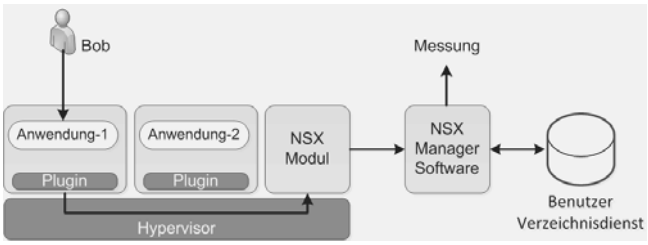
Ein schwaches Server-Zertifikat kann dazu führen, dass sich unberechtigte Teilnehmer in die Kommunikation einschalten und somit der Zugriffsschutz ungenügend ist.

4.4 Zugriffsprüfung mittels VMM-APIs

Auch die internen Managementschnittstellen der Virtualisierungsumgebung eignen sich zur automatisierten Verifikation des Umsetzungsstandes der Zugriffskontrolle. Da der lesende Zugriff auf diese Schnittstellen selbst datenschutzrechtlich höchst sensibel ist, sieht das Messsystem hierfür eine speziell abgesicherte sogenannte Mess-VM anstatt einer normal genutzten Kunden-VM vor.

Einige dieser Schnittstellen erlauben nicht nur das Abfragen von Konfigurationsparametern (z. B. die auf dem System vorhandenen Benutzerrechte) sondern auch die Überwachung der tatsächlichen Zugriffe auf einzelne VMs. Für die prototypische Umsetzung dieser Messung auf einer VMware-basierten Testplattform ist daher der Einsatz des VMware NSX-Moduls geplant, welches auch in Open-Source-Umgebungen genutzt werden kann.[9] Abb. 2 skizziert beispielhaft die Funktion der NSX-Zugriffsüberwachung.

Abb. 2 | Schematische Darstellung der Zugriffsüberwachung



Der Benutzer Bob meldet sich an seinem virtuellen Arbeitsplatz an und greift danach auf eine bestimmte Anwendung innerhalb seiner Cloud-Infrastruktur zu. Dieser Vorgang wird über das NSX-Modul an den NSX-Manager gemeldet und der Benutzer mit Hilfe des AD-Dienstes[10] einer Benutzergruppe zugeordnet. Der Vorgang könnte etwa folgende Rohdaten erzeugen (siehe Tab. 3).

Tab. 3 | Rohdaten einer NSX-Zugriffsüberwachung

User	AD-Gruppe	Anwendungsname	Quell VM
Bob	Ärzte	Anwendung-1.exe	PC_Arzt_5
Ziel VM		**Quell IP**	**Ziel IP**
Server-Buchhaltung		172.16.120.102	172.16.20.6

Mittels der NSX-Schnittstelle können auf diese Weise Untersuchungsbereiche erschlossen werden, die für den Zugriffsschutz relevant sind. Mit den NSX-Rohdaten lassen sich beispielsweise Fragen zu Nutzergruppen, Zugriffsrechten und Zugriffsverletzungen beantworten: Existieren unterschiedliche Rollen und Gruppen von Benutzern? Es sollte mehrere solcher Gruppen geben und die relevanten Gruppen sollten nicht leer sein. Es sollte eine Trennung zwischen Kunden und Betreibergruppen geben. Gibt es somit überhaupt eine Differenzierung von Zugriffsrechten? Existieren Zugriffsbeschränkungsprofile und werden diese erfolgreich angewandt? Der Betreiber sollte nur auf so genannten Infrastruktur-VMs, d. h. virtuelle Maschinen mit Manage-

9 Die Funktionalität kann hier aber z.Zt. noch eingeschränkt sein.

10 Active Directory Service.

mentaufgaben, Zugriff haben. Welcher Benutzer hat auf welche VM zugegriffen? Gibt es Zugriffsverletzungen?

5 Händische Überprüfung

Für die ergänzende händische Überprüfung durch einen Auditor sind insbesondere die in den folgenden Abschnitten genannten Messfelder zu überprüfen, u. a. [DKWW13], [GoSc12], [Münc10], [TaGa10].

Das erste Messfeld der händischen Überprüfung befasst sich mit dem Vorhandensein eines ADV-Vertrages mit Regelungen zum Zugangs- und Zugriffsschutz. Das Messfeld ist als angemessen zu bewerten, wenn u. a. der Vertrag schriftlich vorliegt, dieser Details zur Umsetzung von Zugangs- und Zugriffsschutz enthält und dem Auftraggeber umfangreiche Weisungs- und Kontrollbefugnisse zugesteht.

Ein weiteres Messfeld thematisiert das Vorhandensein eines schriftlichen Zugangs- und Zugriffsberechtigungskonzepts. Das Messfeld ist als angemessen zu bewerten, wenn u. a. geregelt ist, wer zum Zugang auf Daten berechtigt ist, wer wie (Lese-, Schreib-, Lösch-, Kopier- und Übermittlungsrechte) auf welche Daten zugreifen darf, wie die Zugangs- und Zugriffsrechte vergeben und (z. B. im Falle eines Funktions- oder Arbeitsplatzwechsels) entzogen werden und wer für das Berechtigungskonzept und dessen regelmäßige Pflege verantwortlich ist.

Auch der Nachweis der Benutzerkennung wird durch ein Messfeld thematisiert. Das Messfeld ist als angemessen zu bewerten, wenn u. a. geregelt ist, dass jeder Benutzer eines Datenverarbeitungssystems ein eigenes Passwort bzw. eine gleichwertige eigene Benutzerkennung erhält, das Passwort – je nach branchenspezifischen Anforderungen bzw. je nach Schutzbedarf –mindestens 12 / 16 Zeichen lang ist und diese Anforderung erzwungen wird, das Passwort in regelmäßigen Abständen geändert werden muss und jederzeit geändert werden kann.

Ein weiteres Messfeld thematisiert die Durchführung regelmäßiger Penetrationstests. Das Messfeld ist als angemessen zu bewerten, wenn u. a. aus der Dokumentation der Prüfungen ersichtlich wird, dass die Tests regelmäßig durchgeführt und gefundene Schwachstellen nachweisbar und zeitnah geschlossen werden.

Darüber hinaus stellt das Vorhandensein einer datenschutzkonformen Protokollierungsstrategie ein Messfeld der händischen Überprüfung dar. Das Messfeld ist als angemessen zu bewerten, wenn u. a. unberechtigte Zugriffsversuche datenschutzkonform protokolliert werden und die Protokolle zeitnah und datenschutzkonform ausgewertet sowie nach einem festgelegten Zeitraum, der dem Prinzip der Datensparsamkeit genügt, gelöscht werden.

Auch das Vorhandensein von Zugriffsschutzmaßnahmen für Datenträger ist Teil der händischen Überprüfung. Das Messfeld ist als angemessen zu bewerten, wenn u. a. ein Datenträger-Inventurbuch vorhanden ist und regelmäßig gepflegt wird sowie bei einem (sehr) hohen Schutzbedarf Sperrzonen für Datenträger eingerichtet sind.

Die Ergebnisse der händischen Kontrolle gibt der Auditor über eine Auditor-Schnittstelle in das Metriken-System ein. Im Anschluss können die automatisierten und händischen Eingaben zu einer Metrik berechnet werden.

6 Zusammenfassung der Prüfergebnisse

Ergebnisse händischer und automatisierter Messungen lassen sich zu einer Metrik aggregieren, die einen kompakten Überblick über die Stärke der Mechanismen gibt, die ein Cloud-Betreiber zum Zugangs- und Zugriffsschutzes umgesetzt hat. Tab. 4 zeigt eine Berechnungsvorschrift und weitere Merkmale einer solchen Kenngröße. Es wird in diesem Modell davon ausgegangen, dass ein einzelnes Messfeld entweder die angemessene oder unangemessene Umsetzung einer Anforderung eindeutig begründen kann oder aber als dazwischenliegende Möglichkeit den Verdacht einer unzureichenden Umsetzung zumindest nahelegt.

Tab. 4 | Steckbrief einer Metrik zum Zugangs- und Zugriffsschutz

Bezeichnung	Erläuterung
Metrikname	Stärke des Zugangs- und Zugriffsschutzes
Beschreibung	Die Metrik klassifiziert die Qualität der zum Zugangs- und Zugriffschutz auf personenbezogene Daten getroffenen Maßnahmen durch Zusammenfassung der Einzelergebnisse aus automatisierten & händischen Messungen.
Zielgruppen	Datenschutzbeauftragte, Management, Compliance-Manager, Rechts-, IT-, Revisionsabteilung
Formel	Stärke des Zugangs- & Zugriffsschutzes = $\frac{\sum Messfeld_i \alpha_i}{\sum Messfeld_i}$
	Angemessen: $\alpha_i = 1$
	Nicht angemessen: $\alpha_i = 0$
	Verdacht: $\alpha_i = 0{,}5$
	Relevantes Messfeld: $Messfeld_i = 1$
	Nicht relevantes Messfeld[4]: $Messfeld_i = 0$
Zielwert	1 (= Angemessen)

4 Der Wert „Nicht relevant" kann vergeben werden, wenn eine Anforderung zwar nicht umgesetzt wird, dies aber auf Grund alternativer Maßnahmen keinen negativen Einfluss auf die Erfüllung des Datenschutzziels hat.

Die Metrik zum Zugangs- und Zugriffsschutz kann sowohl die vor dem Beginn einer Auftragsdatenverarbeitung in der Cloud verpflichtende Erstkontrolle als auch die anschließend erforderlichen regelmäßigen Datenschutzkontrollen erleichtern. Sie ist darüber hinaus auch nach Beendigung der Nutzung hilfreich, wenn beurteilt werden muss, ob verbliebene Backups oder Daten, die aufgrund von Sperrpflichten nicht gelöscht werden können, durch den Cloud-Betreiber angemessen geschützt werden.

Literatur

[DKWW13] Däubler/Klebe/Wedde/Weichert (Hrsg.): Kompaktkommentar zum BDSG, 2013.

[Fedl12] Fedler: Prefix Hijacking-Angriffe und Gegenmaßnahmen, 2012, S. 1-8.

[GoSc12] Gola / Schomerus: BDSG Kommentar, 2012.

[JäSW15] Jäger/Selzer/Waldmann: Die automatisierte Messung von Cloud-Verarbeitungsstandorten, DuD 2015, S. 26-30.

[Münc10] Münch: Technisch-organisatorischer Datenschutz, 2010.

[Sowa10] Sowa: Access Control Controls, In: <kes> 1/2010, S. 7-12.

[TaGa10] Taeger/Gabel (Hrsg.): Kommentar zum BDSG, 2010.