Die Pflicht zur Prüfung von Dienstleistern:

WARUM ZERTIFIZIERUNGEN ALLEIN NICHT AUSREICHEN

Die Cyberangriffe der letzten Monate haben gezeigt, dass auch Schwachstellen in Prozessen und Anwendungen von Dienstleistern ein Risiko für die Sicherheit von Organisationen darstellen. Insofern erscheint es nur logisch, dass bereits vor der Auslagerung von (Teil-)Prozessen betreffende Dienstleister überprüft werden müssen. Zur Wahrheit gehört aber auch, dass derartige Prüfungen in der Praxis oft nur unzureichend stattfinden. Organisationen sind jedoch gut beraten, ein gutes Auslagerungsmanagement zu etablieren.

Die zunehmende Komplexität von Prozessen, Systemen und Anwendungen sowie die unter anderem hieraus resultierende Spezialisierung von Unternehmen machen immer öfter eine Einbeziehung Dritter in die eigenen Geschäftsprozesse erforderlich. Gleichzeitig sorgen steigende regulatorische Anforderungen für eine wachsende Verrechtlichung der Informationssicherheit. Probleme ergeben sich daraus, dass der Bereich des IT-Outsourcing – und hier insbesondere die Nutzung von Cloud-Diensten – zunehmend ein Massengeschäft darstellt, wobei die Umsetzung individueller vertraglicher Regelungen nicht oder nur selten möglich ist.

Auftraggeber sind so regelmäßig aufgrund beschränkter Möglichkeiten zur Einflussnahme auf eine ausreichende technische und organisatorische Gewährleistung von Informationssicherheit durch den jeweiligen Dienstleister angewiesen. Die vertragliche Vereinbarung von Kontroll- und Steuerungsrechten ist daher für Auftraggeber zur Überwachung des Auftragnehmers essenziell. Vor diesem Hintergrund wird es in aller Regel nicht ausreichend sein, lediglich vorliegende Testate und Zertifizierungen einzusehen. Zwar können auch durch Prüfungen des Auftragnehmers nicht alle Risiken ausgeschlossen, jedoch auf ein für die Organisation beherrschbares Maß reduziert werden. Nachstehend betrachten wir mögliche Prüfpflichten und Vorgehensweisen für die Umsetzung in der Praxis näher.

MÖGLICHE PRÜFPFLICHTEN IM DETAIL

Ein Blick auf die aktuelle Normenlandschaft macht deutlich, dass umfassende Prüfpflichten bestehen und die Geschäftsleitung die Wirksamkeit der Prüfprozesse gewährleisten muss.

Normen des Gesellschaftsrechts

Bereits aus den gesellschaftsrechtlichen Normen lässt sich eine Überwachungspflicht der Leitungsebene herleiten. Allen voran ist hierbei insbesondere die Regelung des § 93 Aktiengesetz (AktG) zu nennen. Die Norm legt unter Berücksichtigung verschiedener Kriterien, zum Beispiel die Art und Größe des Unternehmens, das wirtschaftliche Umfeld sowie die Art der Geschäftsführungsmaßnahmen, einen Sorgfaltsmaßstab zugrunde. Zwar steht der Geschäftsleitung auch ein erheblicher Ermessensspielraum in Form der sogenannten Business Judgement Rule zu, jedoch sind unternehmerische Entscheidungen stets auf Grundlage angemessener Informationen zu treffen. Insoweit kann man argumentieren, dass die Auslagerung von (Teil-)Prozessen an Dienstleister eine vorherige und fortlaufende Prüfung voraussetzt. Nur so kann die Zuverlässigkeit des Dienstleisters beziehungsweise das Bestehen etwaiger Risiken sowie die Notwendigkeit risikominimierender Maßnahmen unter Berücksichtigung der jeweiligen Risikostrategie (Risikomanagement) wirksam festgestellt werden.

Die Norm bezieht sich zwar zunächst ausschließlich auf Aktiengesellschaften, jedoch lässt sich über § 43 Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) eine solche Verpflichtung ebenfalls für die Geschäftsführungen von Gesellschaften mit beschränkter Haftung sowie nach § 347 Handelsgesetzbuch (HGB) für Leitungspersonen von Handelsgesellschaften herleiten. Flankierend ist weiterhin § 91 Abs. 2 AktG zu nennen, wonach beispielsweise Aufsichtsmaßnahmen ergriffen werden müssen. Insbesondere gilt es existenzgefährdende Risiken rechtzeitig zu erkennen und diese abzuwenden beziehungsweise vorzubeugen. Hierbei sind selbstverständlich auch die wachsenden Risiken durch die stetig steigende Anzahl von (erfolgreichen) Cyberangriffen und der regelmäßig damit verbundene Verlust vertrauenswürdiger Informationen sowie die damit einhergehenden finanziellen Verluste zu berücksichtigen.

Anforderungen aus dem Informationssicherheitsrecht

Ergänzend ergeben sich weitere zahlreiche Verpflichtungen aus den Vorgaben des Rechtes der Informationssicherheit. So lassen sich speziell aus dem Datenschutzrecht unter Heranziehung von Art. 5 Abs. 2 und Art. 24 Datenschutz-Grundverordnung (DS-GVO) entsprechende Nachweispflichten zur ordnungsgemäßen Datenverarbeitung herleiten. Im Rahmen der Auftragsverarbeitung kann sich eine Prüfpflicht bereits aus Art. 28 Abs. 1 DS-GVO (Geeignetheit des Auftragsverarbeiters) und einem bestehenden Haftungsrisiko des für die Datenverarbeitung Verantwortlichen für die Handlungen des Auftragsverarbeiters ergeben. Ebenso kann Art. 32 DS-GVO mit seiner Verpflichtung des Verantwortlichen und des Auftragsverarbeiters für eine angemessene Sicherheit der Verarbeitung zu sorgen, angeführt werden.

Für den Bereich der kritischen Infrastrukturen gilt zudem das BSI-Gesetz (BSIG) und insbesondere § 8a BSIG mit der Verpflichtung angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Vergleichbare Anforderungen gelten nach § 8c BSIG für die Anbieter digitaler Dienste.

Indes kann in Anbetracht der zahlreichen Normen zum Recht der Informationssicherheit die Auflistung auch an dieser Stelle beliebig fortgeschrieben werden. Auch wenn aus den meisten der vorbenannten Normen keine Prüfpflicht aus dem direkten Wortlaut hervorgeht, ist eine Prüfung von Dienstleistern zur vollumfänglichen Erfüllung der rechtlichen Anforderungen wohl unumgänglich.

Ableitung aus dem Informationssicherheits-managementsystem

Ergänzend ist anzuführen, dass sich bereits aus der regelmäßigen Funktionsweise eines Managementsystems zwangsläufig das Bestehen regelmäßiger Prüfpflichten ergibt. Dies lässt sich insbesondere bereits aus dem PDCA-Zyklus ableiten, welcher einem jedem Informationssicherheits-Managementsystem (ISMS) zugrunde liegt. Die Organisation hat demnach nicht nur ein bestimmtes Vorgehen zu planen und vorgabenkonform danach zu handeln, sondern die hieraus resultierenden Ergebnisse stets zu prüfen und die betreffenden Abläufe gegebenenfalls anzupassen. Grundsätzlich sind dabei die spezifischen Anforderungen und die zur Verfügung stehenden Ressourcen einer Organisation angemessen zu berücksichtigen.

MAßNAHMEN NACH BSI IT-GRUNDSCHUTZ

Mit Blick auf die Praxis stellt sich anschließend die Frage der Umsetzung. Die Betrachtung von Sicherheitsaspekten in einem Outsourcing-Vorhaben ist, wie im BSI-Grundschutz-Kompendium im Baustein *OPS.2.3 Nutzung von Outsourcing* explizit vorgeschlagen, typischerweise direkt im Outsourcing-Vertrag zu regeln. Teil-

weise bestehen sogar gesetzliche Verpflichtungen zur vertraglichen Fixierung diverser Aspekte, wie mit Blick auf Art. 28 DS-GVO deutlich wird. Es empfiehlt sich zudem die Aspekte der Informationssicherheit bereits ab der Entscheidung für das jeweilige Outsourcing-Projekt einzubeziehen. Ziel sollte der Aufbau einer möglichst umfassenden Schutzsphäre sein.

Festlegung von Anforderungen an Dienstleister und Verträge

Zunächst bietet sich eine vertragliche Spiegelung der verschiedenen regulatorischen Anforderungen zur Informationssicherheit an. Hierbei erlegt der Auftraggeber den jeweiligen Vertragspartnern die jeweils einschlägigen Vorgaben zur Informationssicherheit auf. Zu beachten ist in diesem Zusammenhang jedoch, dass selbst im Fall derartiger Auslagerung von Aufgaben und Pflichten an Dritte dies nicht gleichbedeutend mit einer Entbindung der Informationssicherheitspflicht, mithin von der generellen Verantwortlichkeit, seitens der auslagernden Stelle ist. Zwar erfolgt die Umsetzung der jeweiligen Vorgaben durch den Vertragspartner, die Verantwortung gegenüber Dritten verbleibt jedoch beim Auftraggeber. Aus diesem Grund erfolgt vielfach die vertragliche Vereinbarung zur ordnungsgemäßen Leistungserbringung sowie zur Überwachung derselben.

Aufgrund zahlreicher gesetzlicher Anforderungen, technische und organisatorische Maßnahmen (TOM) umzusetzen, besteht regelmäßig ein Interesse seitens der gesetzlichen Adressaten auch die Vertragspartner zu konkreten TOM zu verpflichten. An dieser Stelle prallen häufig die Interessen der Auftragnehmer an einer größten möglichen Flexibilität in Bezug auf die Umsetzung der TOM und die Interessen der Auftraggeber an der Vereinbarung weiterreichender Kontroll- und Nachweisrechten aufeinander. In der Vertragsgestaltung werden derartige Konflikte häufig durch die Vereinbarung von flexiblen Änderungsrechten seitens der Auftragnehmer unter Einhaltung bestimmter Mindeststandards, entsprechender Dokumentationspflichten und der Einräumung von Sonderkündigungsrechten seitens der Auftraggeber bei wesentlichen Änderungen gelöst.

Im Rahmen der konkreten Umsetzung erfolgt nicht selten zunächst eine abstrakte Verpflichtung im Hauptvertragswerk der Auftragnehmer zur Umsetzung bestimmter TOM in Übereinstimmung mit dem aktuellen Stand der Technik und hieran anknüpfend eine konkrete Festlegung von Einzelmaßnahmen, meist in Form einer gesonderten Anlage zum Hauptvertrag.

Weiterhin werden die übertragenen Anforderungen durch entsprechende vertragliche Nachweisregelungen abgesichert. Sinn und Zweck liegt darin, dass der Auftraggeber zunächst einmal in die Lage versetzt wird, seinen gesetzlichen Nachweispflichten – wie zum Beispiel aus Art. 5 Abs. 2 DS-GVO – nachkommen zu können. Der Auftraggeber muss bestrebt sein, die einzuhaltenden Informationssicherheitsanforderungen detailliert darzulegen und für den Nachweis Konzepte sowie unabhängige Zertifikate und Prüfberichte seitens des Auftragnehmers einzufordern. Schwierigkeiten bei der Überprüfung ergeben sich allerdings regelmäßig dann, wenn die Wirksamkeit sowie die Aussagekraft hinter derartigen Nachweisen zu hinterfragen ist. Abzugrenzen sind an dieser Stelle zunächst Normen und Standards, die ein ISMS innerhalb einer Organisation beschreiben, wie zum Beispiel die ISO 27000-Reihe oder der BSI-Grundschutz, von Zertifizierungen zur IT-Sicherheit, bei denen beispielsweise ein Produkt oder ein IT-Dienst durch eine zuständige Stelle geprüft und zertifiziert wird. Nur bei der zweiten Gruppe an Zertifizierungen, Normen und Standards, werden tatsächlich technische Anforderungen und mithin der Stand der Technik beschrieben. Dies soll keinesfalls die Bedeutung oder Wertigkeit der Zertifizierungen eines ISMS schmälern. Es ist jedoch hervorzuheben, dass die Unterscheidung in der Praxis nicht immer trennscharf durchgeführt wird und somit beispielsweise eine fehlerhafte Bewertungsgrundlage für die Zuverlässigkeit eines Auftragnehmers geschaffen werden kann.

Bestandteil vertraglicher Regelungen können ferner die Festlegung von Zugangsrechten sowie die Durchführung von Audits und anderen Kontrollmaßnahmen sein. Hinsichtlich des konkreten Umfangs der vertraglich zu vereinbarenden Pflichten können insbesondere Orientierungshilfen und Positionspapiere der deutschen und europäischen Aufsichtsbehörden, Best Practices von Interessenverbänden sowie einschlägige technische Normen, Standards und Regelwerke als Maßstab herangezogen werden. Ferner kann die Implementierung von Berichts- und Informationspflichten vereinbart werden.

Gleichwohl können sich Überprüfungspflichten im Bereich der Haftungsfrage ergeben. Ausgangsfrage ist zunächst, welche Leistung und mithin welche Informationssicherheitspflichten geschuldet sind. Möglicherweise fällt so in diesem Bereich der Nachweis einer Pflichtverletzung leichter, wenn die vertraglich in Bezug genommenen Vorgaben nicht oder nicht vollständig umgesetzt wurden. Jedoch kann sich im Rahmen des Mitverschuldens nach § 254 Bürgerliches Gesetzbuch (BGB) das Vernachlässigen beziehungsweise die Nichteinhaltung der Überprüfungspflichten niederschlagen.

Etablierung eines Auslagerungsmanagements

Der im BSI IT-Grundschutz enthaltene Baustein *OPS.2.3 Nutzung von Outsourcing* enthält unter dem Begriff des Auslagerungsmanagements bereits eine Reihe von Maßnahmen, mit denen die zuvor genannten Problematiken adressiert sowie bestehende Prüfpflichten strukturiert und dokumentiert umgesetzt werden können. Insbesondere werden auf verschiedensten Ebenen zahlreiche Möglichkeiten zur Prüfung in Form eines Soll-Ist-Abgleichs aufgezeigt:

- Die Auslagerung von (Teil-)Prozessen und Geschäftsbereichen bedarf zunächst stets einer kontextbasierten Betrachtung potenzieller Risiken. Zu berücksichtigen sind hierbei insbesondere die Kritikalität und die Abhängigkeit der betroffenen Prozesse sowie die Art und Kategorien, der in diesem Zusammenhang betroffenen Informationen. So muss zunächst geklärt werden, ob überhaupt eine Auslagerung an einen Dienstleister erfolgen kann oder ob die Gefährdungslage eine ausschließlich interne Umsetzung gebietet. Dies stellt grundsätzlich zwar keine Prüfung eines konkreten Auftragnehmers in jedem Fall jedoch eine essenzielle Vorprüfung dar.

- Ist der Einsatz eines Auftragnehmers grundsätzlich möglich, sind weiterhin konkrete Anforderungen an diesen zu definieren. Hierzu muss bereits im Vorfeld festgelegt werden, welche Kompetenzen für die Erbringung der Leistung aus Sicht der Informationssicherheit als erforderlich angesehen werden und welchen Grad an Vertrauenswürdigkeit sowie Zuverlässigkeit der Auftragnehmer leisten muss. Möglicherweise sind derartige Aspekte im öffentlichen Sektor bereits in einem Vergabeverfahren zu berücksichtigen. Ein Dienstleister sollte möglichst schon vor Aufnahme von Vertragsgesprächen anhand der

definierten Kriterien überprüft werden. In diesem Zusammenhang sollten gegebenenfalls bestehende Interessenkonflikte ausgeschlossen werden.

- Im nächsten Schritt sind konkrete Anforderungen an die vertraglichen Regelungen mit dem jeweiligen Dienstleister unter Berücksichtigung der oben aufgeführten Aspekte festzulegen und zu prüfen. So müssen Verträge zumindest ein Recht auf Überprüfung, einen Zustimmungsvorbehalt zur weiteren Verlagerung der Tätigkeit auf Unterauftragnehmer sowie weitere wesentliche Aspekte der Informationssicherheit, wie beispielsweise eine Verpflichtung auf Vertraulichkeit und die Gewährleistung angemessener Sicherheitsmaßnahmen nach IT-Grundschutz oder vergleichbarer Maßnahmen, umfassen. Auch die Bereitstellung eines auf den jeweiligen Prozess angepassten Sicherheitskonzeptes durch den Dienstleister ist zu vereinbaren. Sinnvoll ist in diesem Zusammenhang auch die Etablierung eines Mustervertrags, der die von der Organisation als essenziell angesehenen Anforderungen dienstleisterunabhängig auch für zukünftige beziehungsweise weitere Vertragsverhältnisse einheitlich darstellt.

Ausgehend von diesen Mindestanforderungen können sich auch weitergehende Maßnahmen als sinnvoll erweisen. Dazu können beispielsweise die Erstellung einer organisationsweiten Strategie sowie die Verabschiedung von Richtlinien zu den Voraussetzungen für die Auslagerungen von Tätigkeiten gehören. Je umfangreicher die Anforderungen einer Organisation zur Inanspruchnahme derartiger Dienstleister gestaltet werden, umso eher empfiehlt sich die Etablierung eines umfassenden Auslagerungsmanagements, einschließlich der Benennung einer zuständigen Person, die beispielsweise auch die zuvor genannten Prüfungen im Rahmen vorvertraglicher Maßnahmen durchführen kann.

Durchführung fortlaufender Prüfungen

Jedoch erschöpft sich die Pflicht zur Prüfung von Dienstleistern nicht in einer einmaligen Vorabprüfung. Schließlich kann eine solche ausschließlich eine Momentaufnahme darstellen, wobei nicht sichergestellt werden kann, dass der Dienstleister fortlaufend ein ISMS oder entsprechende Maßnahmen aufrechterhält und weiterentwickelt. Insofern ist auch die ausschließliche Vorlage einer Zertifizierung regelmäßig als unzureichend zu erachten.

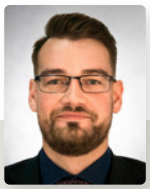
Dementsprechend obliegt der Organisation die Pflicht, die Einhaltung der auferlegten Kriterien fortlaufend zu prüfen. Eine solche Prüfung ist einerseits anlassbezogen, also beispielsweise bei Vorliegen von rechtlichen Änderungen oder bei Eintritt von Sicherheitsvorfällen beziehungsweise -ereignissen, andererseits regelmäßig – anlassunabhängig – durchzuführen. Hinsichtlich des Begriffs der Regelmäßigkeit wird keine allgemeingültige Definition möglich sein. Auch hierbei ist Bezug auf die Kritikalität der jeweiligen Prozesse und der hieraus resultierenden Gefährdungslage zu nehmen. Demnach kann es sinnvoll sein, innerhalb einer Organisation unterschiedliche Prüfungsintervalle zu etablieren. Je nach Komplexität der Anforderungen kann die Erstellung einer entsprechenden Richtlinie oder zumindest die Festlegung entsprechender Kennzahlen Erleichterungen in der praktischen Umsetzung ermöglichen. Gegenstand der fortlaufenden Prüfungen sollten stets die vertraglich festgelegten Sicherheitsanforderungen, ergänzt um zwischenzeitlich gegebenenfalls hinzugetretene gesetzliche Anforderungen sowie Inhalte des vorliegenden prozessspezifischen Sicherheitskonzeptes sein.

Sämtliche der aufgeführten Prüfungen sollten in einer dokumentierten und nachvollziehbaren Form erfolgen. Derartige Prüfberichte ermöglichen unter anderem auch der Leitungsebene die Nachweisbarkeit eingerichteter Prüf- und Überwachungsprozesse zur Abwendung existenzgefährdender Risiken. Auch der zugrunde liegende PDCA-Zyklus kann durch die Prüfergebnisse genährt und die Gewährleistung der Informationssicherheit somit insgesamt (besser) sichergestellt werden.

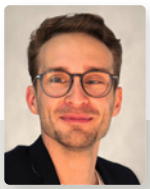
FAZIT

Für den Aufbau einer ganzheitlichen Informationssicherheit ist es für Organisationen unumgänglich, sich mit der (Über-)Prüfung der eingesetzten Dienstleister auseinanderzusetzen. Der Pflichtenkanon reicht von nationalen Vorschriften des Gesellschaftsrechts über das Datenschutzrecht bis hin zu einer eindeutigen Erforderlichkeit aus dem Funktionieren des Informationssicherheitsmanagementsystems selbst. Die Vernachlässigung dieser Anforderungen kann weitreichende Folgen haben. Organisationen ist deshalb zu raten, ihren Prüfpflichten auch tatsächlich nachzukommen.

Mit Blick auf den Baustein *OPS.2.3 Nutzung von Outsourcing* des BSI IT-Grundschutz sind Organisationen gut beraten, ein entsprechendes Auslagerungsmanagement zu betreiben. Vielfach bildet die vertragliche Gestaltung die Basis für den Start einer Outsourcing-Beziehung. Organisationen sehen sich hierbei nicht selten vorgegebenen Vertragsdokumenten der Auftragnehmer ausgesetzt. Ein schlechter Ratgeber ist das einfache Durchsehen und das „Abnicken" vorgelegter TOM-Auflistungen und/oder bestimmter Zertifizierungen, ohne deren konkrete Bedeutung und Auswirkung für den zu betrachtenden Einzelfall zu würdigen. Das Outsourcing-Management endet jedoch nicht mit der Auftragsvergabe, sondern erfordert eine kontinuierliche Überprüfung der eingesetzten Auftragnehmer. ■



ALEXANDER WEIDENHAMMER, LL.M.
ist Rechtsanwalt, Datenschutzbeauftragter (GDD) und BSI IT-Grundschutz-Praktiker (DGI) beim Dresdner Institut für Datenschutz (DID).



MAX JUST, LL.M.
ist Wirtschaftsjurist, Datenschutzbeauftragter (GDD) und BSI IT-Grundschutz-Praktiker (DGI) beim Dresdner Institut für Datenschutz (DID)