2. AUSGABE 2022

EBNER STOLZ

novus

INFORMATIONSTECHNOLOGIE

Ebner Stolz kooperiert mit führendem Software-anbieter für SAP-Berech-tigungsprüfung

Green IT: Der grüne Pfad der Informationstechnologie

ISO/IEC 27001:2022 – alles auf Anfang?

Informationssicherheit nimmt weiter an Fahrt auf

Pünktlich zum Jahresende freuen wir uns, Sie in unserem neuen novus zur Informationstechnologie über aktuelle Themen informieren zu können. Auch das letzte halbe Jahr bringt wieder einige interessante Themen mit sich, die dazu beitragen können, die folgenden Jahre ereignisreich zu gestalten. Dies gilt insbesondere im Bereich der IT-Sicherheit, in dem es in den letzten Monaten einige Änderungen gab und auch für die Zukunft weitere zu erwarten sind. Dies führt dazu, dass die Thematik Informationssicherheit auch künftig eine große Herausforderung darstellt.

Wir freuen uns auch, Ihnen in diesem Zusammenhang zu berichten, dass wir nach bereits jahrelanger erfolgreicher Zusammenarbeit nun eine formelle Kooperation mit der IBS Schreiber GmbH, einem der führenden SAP Security Spezialisten und Marktführer für Software für SAP Berechtigungsprüfungen, geschlossen haben.

Am 10.11.2022 hat das EU-Parlament dem Entwurf der NIS 2.0 Richtlinie zugestimmt, was dazu führt, dass weitere europaweite Anforderungen an die Informationssicherheit gestellt werden und somit mit hoher Wahrscheinlichkeit erneut eine Anpassung des IT-Sicherheitsgesetzes in 2023 folgen wird.

Ende Oktober 2022 wurde nach Veröffentlichung der ISO/IEC 27002:2022 im Februar 2022 die neue ISO/IEC 27001:2022 veröffentlicht. Neben der Neustrukturierung der bereits aus der vorhergehenden Fassung bekannten Anforderungen im Anhang A sowie verschiedener zusätzlicher Anforderungen, über die wir bereits in der ersten Ausgabe des novus IT 2022 berichteten, haben sich auch inhaltliche Änderungen an der Hauptnorm der ISO/IEC 27001:2022 ergeben. Mit Veröffentlichung der neuen ISO/IEC 27001:2022 hat auch der dreijährige Zyklus des Überführens von der alten auf die neue Norm begonnen. Mehr dazu in diesem Heft.

Der Geschäftsbereich IT-Revision (GBIT) wünscht Ihnen viel Freude bei der Lektüre und steht Ihnen bei Rückfragen natürlich gern zur Verfügung.

Wir wünschen Ihnen, Ihren Familien und Angehörigen ein frohes und gesegnetes Weihnachtsfest verbunden mit Glück, Freude und Erfolg. Lassen Sie uns gemeinsam gesund und gestärkt in das Jahr 2023 gehen.

Ihr GBIT

Ebner Stolz kooperiert mit führendem Softwareanbieter für SAP-Berechtigungsprüfung

Bei der Nutzung von ERP-Systemen hat SAP die Nase vorn. Dies ergab unsere im Juli 2022 veröffentlichte Digitalisierungsstudie. So ist der ERP-Systemanbieter SAP bei den befragten mittelständischen Unternehmen mit einem Anteil von 43 Prozent für die Versionen S/4 und deren Vorgänger führend. Die von SAP bis 2007 auslaufende Version R/3 ERP 6.0 verwenden aktuell noch 29 Prozent der befragten Mittelständler; 14 Prozent nutzen bereits die neue Version SAP S/4 HANA.

In jedem Fall werden in den nächsten Monaten und Jahren sehr viele Unternehmen bestehende oder neue SAP S/4 Lösungen an den Start bringen müssen. Das betrifft allein im Bereich der Jahresabschlussprüfungen bei Ebner Stolz annähernd 200 Unternehmen und Unternehmensgruppen. Doch auch die Nutzung der SAP-Systeme birgt Herausforderungen. Eine davon ist das äußerst komplexe SAP-Berechtigungskonzept. Damit dieses sinnvoll vom Mandanten im Griff und vom Prüfer auch beurteilt werden kann, gibt es wiederum spezielle Softwarepakte. Die Komplexität ergibt sich zum einen aus der vieldimensionalen technischen Konzeption der SAP, aber auch aus einer vielschichtigen Implementierung der überwiegend betriebswirtschaftlichen Prozesse.

Ebner Stolz arbeitet seit langen Jahren in diesem Themenfeld mit der IBS Schreiber GmbH, einem SAP-Security-Spezialisten, vertrauensvoll zusammen. Mit einem Kooperationsvertrag heben beide Unternehmen ihre Zusammenarbeit auf eine neue Ebene. Warum eine extra Software außerhalb von SAP für diese Berechtigungskonzepte erforderlich ist und wie die Zusammenarbeit zwischen Ebner Stolz und IBS Schreiber erfolgt, darüber sprechen wir mit Sebastian Schreiber, Geschäftsführer der IBS Schreiber GmbH, und Holger Klindworth, Geschäftsführer und Partner bei Ebner Stolz.

Herr Klindtworth, aus welchem Grund sind Berechtigungskonzepte bei der Nutzung von SAP-Software erforderlich?

Holger Klindtworth: Ein wesentliches Konzept bei der Sicherstellung eines Unternehmenserfolges und bei der Einhaltung von gesetzlichen Rahmenbedingungen ist die Einrichtung interner Kontrollsysteme. Zu internen Kontrollsystemen gehört auch die Einrichtung von Funktionstrennungen. Der Mitarbeiter im Unternehmen, der bestellt, darf nicht Zahlungen auslösen. Der Mitarbeiter, der eine Gutschrift in der Materialwirtschaft bucht, darf keine Wareneingangskontrolle durchführen etc.

Dies ist nicht nur im Sinne des Unternehmens, sondern wird auch von Handelsrecht, Steuerrecht, Datenschutz, Aufsichtsrecht und eigentlich allen anderen Rechtsgebieten – außer vielleicht vom Scheidungsrecht, hier ist es ja irgendwie immanent verpflichtend – gefordert. Habe ich als Unternehmen keine Funktionstrennung eingerichtet und es erfolgt eine Veruntreuung, z. B. durch Zahlung unberechtigter Rechnungen, ist dies z. B. aus Sicht der Finanzverwaltung gemäß BMF-Schreiben aus dem Jahr 2016 ein Indiz für eine billigend in Kauf genommene Steuerhinterziehung im Rahmen von falsch deklarierten Betriebsausgaben.

Jetzt stellen Sie sich das Ganze für Unternehmen mit hunderten Mitarbeitern und Prozessen in einer komplexen dynamischen Unternehmensorganisation vor. Das funktioniert nur mit entsprechenden Lösungen sowohl bei der Einrichtung als auch bei der Pflege der Berechtigungen, aber eben auch bei der Prüfung und Beurteilung der Angemessenheit der Funktionstrennung.

Herr Schreiber, wie kann sich der Laie ein solches SAP-Berechtigungskonzept vorstellen?

Sebastian Schreiber: Zunächst sollte ein Berechtigungskonzept schriftlich vorliegen und allen Verantwortlichen bekannt sein, bevor dies technisch umgesetzt wird. Darin gilt es vor allen Dingen, spezielle Risiken im Berechtigungswesen darzustellen und zu definieren, wie diese Risiken durch Kontrollen minimiert werden. Dazu gehören auch die von Holger beschriebenen Funktionstrennungen. Es gibt die Möglichkeit, diverse technische Kontrollen, wie bspw. Freigabeworkflows, 4-Augen-Prinzipien und die Berechtigungsvergabe über IDM Werkzeuge, in SAP-Systeme zu implementieren. Des Weiteren gibt es auch organisatorische Kontrollen, wenn eine technische Kontrolle nicht ausreichend ist, welche ebenfalls in einem Berechtigungskonzept definiert sein sollen. Eine große Herausforderung stellt in den Unternehmen die Definition der Risiken dar. In vielen Fällen ist nicht bekannt, welche Daten besonders sensibel sind, wie auf diese zugegriffen wird und wie die technische Berechtigung im SAP-System für diesen Zugriff aussieht. Das macht das Thema sehr komplex und es ist oft schwierig, Verantwortliche im Unternehmen zu finden, die sich mit dem Thema befassen, da dies meist neben dem Tagesgeschäft erledigt werden muss. Hier müssen die Verantwortlichen aus den Fachbereichen Verantwortung übernehmen – das ist kein reines IT-Thema! Meist fehlt für solche Kontrollen das technische Prozess-Know-how in den Fachbereichen.

Warum benötige ich als SAP-Nutzer eine spezielle Software, um den Überblick über das Berechtigungskonzept zu wahren?

Sebastian Schreiber: Wie in der letzten Antwort schon angerissen, sehen wir unsere Software auch als Bindeglied zwischen IT und Fachbereich. Wir haben schon sehr viele Risiken vordefiniert, die per Knopfdruck überprüft werden können. Zu jedem dieser Risiken haben wir eine Risikobeschreibung und wir haben ein Reporting, das für jeden Fachbereich sehr verständlich ist. Wichtig ist, dass der Fachbereich die Reports versteht, damit die Bewertung der Ergebnisse ordnungsmäßig durchgeführt werden kann. Unsere Risiken können problemlos durch weitere unternehmensspezifische Risiken ergänzt werden.

Und… wie ist gewährleistet, dass diese Software die erforderlichen Qualitätsstandards erfüllt?

Sebastian Schreiber: Wir setzen hier sehr auf Qualität und investieren eine Menge in den Auf- und Ausbau unserer Regelwerke. Hier haben wir unsere Berater, die zusammen mit Kunden und Partnern ständig daran arbeiten, unsere Regelwerke zu erweitern und zu aktualisieren. Außerdem haben wir die Möglichkeit, automatisch zu kontrollieren, welche Sicherheitseinstellungen der Kunde in seinem SAP-Customizing aktiviert hat, um dann auch nur diese zu prüfen (bspw. Vier-Augen-Prinzip etc.).

Außerdem haben wir unsere Regelwerke und unsere Entwicklungsprozesse von Ebner Stolz nach den relevanten IDW-Standards zertifizieren lassen.

Herr Klindtworth, warum ist die Kooperation zwischen Ebner Stolz und IBS Schreiber sinnvoll und erforderlich, konkret: Aus welchem Grund ist es aus der Sicht der Wirtschaftsprüfer wichtig, dass ein funktionierendes Berechtigungskonzept vorliegt?

Holger Klindtworth: Wie bereits erwähnt, ist die Beurteilung von Prozessen und Systemen eng mit dem Begriff internes Kontrollsystem und damit auch mit dem Begriff der Funktionstrennung verknüpft. Für uns ist eigentlich jede Prüfung immer auch eine Prüfung der Funktionstrennung. Jetzt haben wir mal ein typisches SAP-System mit tausend Benutzern, fünfzigtausend Datentabellen, hunderten von Prozessen – hier ist eine manuelle Prüfung der vergebenen Berechtigungen manuell faktisch nicht möglich, hier brauchen wir eine softwaretechnische Unterstützung. Das haben wir auch in der Vergangenheit genutzt, aber durch die Zusammenarbeit mit IBS können wir jetzt unsere Prüfungen viel besser auf die Gegebenheiten beim Mandanten und die Risikolage zuschneiden. Mit einem Gleichnis aus der Logistik gesprochen, wir haben jetzt einen Lastwagenhersteller, der uns genau den LKW baut, den wir benötigen, um die Güter unseres Mandanten zu transportieren, nicht zu groß, nicht zu klein. Auf der anderen Seite versetzen wir IBS in die Lage, durch unser in Jahrzehnten angewachsenes Prozess-Know how genau die LKWs zu bauen, die auch die Kunden von IBS benötigen und natürlich teilen wir auch unser SAP Know-how.

Hier haben IBS und auch wir viel Erfahrung, aber eins ist jedem Marktteilnehmer klar, der sich professionell und im Sinne seiner Kunden / Mandanten mit dem Thema beschäftigt: Der wahre Widersacher für den IT-Prüfer ist nicht der Wettbewerber im Markt, die wahren Widersacher haben die Namen Komplexität und Nachvollziehbarkeit und natürlich auch Wirtschaftlichkeit. Ein offener Informationsaustausch der Fachleute auf Augenhöhe im Sinne von „Quid quo pro" ist in der Welt der IT-Prüfung dringender erforderlicher denn je.

Wie erfolgt die Zusammenarbeit zwischen IBS Schreiber und Ebner Stolz? Welcher Mehrwert ergibt sich dadurch für mittelständische Unternehmen?

Sebastian Schreiber: Der Mehrwert ergibt sich daraus, dass wir die Prüfungsanforderungen, die sich aus diversen Regularien ergeben, durch unser vereintes Know-how sehr effizient für die Kunden umsetzen können. Das spart Kosten, gerade auch für Unternehmen ohne eigene Compliance-Abteilung.

Gibt es Themengebiete der Kooperation, die über die Prüfung von SAP-Berechtigungen hinaus gehen?

Holger Klindtworth: Ja. Wir planen auch eine Unterstützung bei der Weiterentwicklung der IBS Produkte, gerade auch bei der Qualitätssicherung und es wird sicherlich auch gemeinsame Veranstaltungen für unsere Mandanten und die Kunden von IBS geben. Wir haben bei Ebner Stolz auch eigene Softwareentwicklung für unsere Prüfungswerkzeuge. Unsere „Werkzeugmacher" und die Entwickler von IBS nutzen hier sehr ähnliche Entwicklungsumgebungen und Programmiersprachen. So ist auch hier eine engere Zusammenarbeit in Zukunft vorgesehen.

Agile Verträge für agile Projekte

Ursprünglich aus der Softwareentwicklung stammend, werden agile Arbeitsmethoden in Unternehmen zunehmend in verschiedenen Dienstleistungsbereichen eingesetzt. Wird dabei mit Dienstleistern oder Kunden zusammengearbeitet, bedarf es vertraglicher Vereinbarungen, die dieser Arbeitsweise gerecht werden.

So kann z. B. gemeinsam mit Dienstleistern an Smart-Tool-Lösungen für das bestehende Produktportfolio gearbeitet werden, wozu je nach noch zu eruierendem Nutzerverhalten der Kunden digitale Zusatzfunktionen entwickelt werden sollen. Dazu kommen regelmäßig Software-Tools wie z. B. Kanban oder SCRUM zum Einsatz, um Teilziele zu dem gemeinsamen Projekt zu definieren. Diese können flexibel auf sich verändernde Rahmenbedingungen angepasst werden und gewähren einer innovativen Herangehensweise möglichst viel Raum. Zeigt z. B. das Nutzerverhalten der Kunden, dass eine Interaktion zwischen den angebotenen Produkten als besonders wichtig erachtet wird, wird der Lösungsansatz ein völlig anderer sein, als wenn den Kunden ausschließlich am Remote-Zugriff auf einzelne Produkte gelegen ist. Entscheidend für den beidseitig erfolgreichen Abschluss agiler Projekte ist ein gemeinsames Verständnis der Vertragspartner u. a. darüber, welche Leistungen wie erbracht werden, wann diese als erfüllt gelten und abgenommen werden können sowie wie die Vergütung ausgestaltet wird. Dies muss auch seinen Niederschlag in der Vertragsgestaltung finden.

Standardverträge sind nicht geeignet

Standardklauseln, die dem Werk- und / oder dem Dienstrecht entstammen, eignen sich regelmäßig nicht zur Gestaltung von agilen Verträgen, denn es gilt der agilen Methodik und dem agilem Mindset Rechnung zu tragen. Dazu ist letztlich ein Loslösen von den bekannten Vertragstypologien erforderlich. Entscheidend muss sein, wie die agile Zusammenarbeit konkret ausgestaltet ist, um diese in rechtsverbindliche Regelungen umzusetzen.

Ausgestaltung am Beispiel von SCRUM

Die erste Zutat für einen umsetzbaren und damit guten agilen Vertrag ist die Beschreibung und Regelung der tatsächlichen Ausgestaltung der agilen Zusammenarbeit. Hierzu ist es unerlässlich, sich mit den Grundzügen der Methodik des eingesetzten Software-Tools und dem agilen Mindset auseinanderzusetzen. Von besonderer Bedeutung für die Zusammenarbeit sind die Rollen, die das eingesetzte Software-Tool vorsieht. Bei SCRUM sind dies konkret der Product Owner, das Entwicklungsteam und der SCRUM-Master. So wird der Product Owner zwar oftmals mit dem Auftraggeber identisch sein bzw. von diesem gestellt werden. Als Product Owner kann aber auch eine andere Person definiert werden, die letztlich die Interessen des Auftraggebers vertritt und aufgrund ihrer guten Marktkenntnisse am besten die zu realisierenden Produkteigenschaften und Produktfunktionalitäten bestimmen kann. Das Entwicklungsteam wird jeweils nach den Zielen individuell und ggf. multidisziplinär zusammengestellt. Unterstützt wird die Arbeit des Entwicklungsteams durch den SCRUM-Master, der als Moderator und Vermittler unterstützt.

Ein klares gemeinsames Rollenverständnis der Vertragsparteien ist für die Vertragsgestaltung essentiell. Oftmals wird es Aufgabe des bei der Vertragsgestaltung hinzugezogenen Beraters sein, hier dieses Verständnis zu schärfen.

Definition von Abnahmen

Mit eine der größten Herausforderungen bei der agilen Vertragsgestaltung ist regelmäßig die Regelung der Abnahme. Bei der Gestaltung einer agilen Abnahmeklausel gilt es zunächst, den Gegenstand der Abnahme zu identifizieren und zu beschreiben. Weit verbreitet ist der Irrglaube, dass sich bei agilen

Projekten nicht definieren lässt, wie das Ergebnis aussehen soll. Trotz der Möglichkeit, die Ergebnisse immer wieder anzupassen, bestehen zumeist diverse Grundannahmen beim Auftraggeber im Hinblick auf das Ergebnis, die in einem Product Backlog festgehalten werden. Wichtig ist, dass der Inhalt dieses Product Backlogs nicht zum Gegenstand der Abnahme gemacht wird, weil damit das Product Backlog dem klassischen Pflichtenheft gleichsetzt wird, was jedoch nicht dem Ansatz des agilen Arbeitens entspricht. Im Eingangsbeispiel wäre etwa die Entwicklung digitaler Zusatzfunktionen zu den bestehenden Produkten im Produkt Backlog festzuhalten.

Der Inhalt des Sprint Backlogs, mit dem die Aufgaben innerhalb einer vorgegebenen Zeitspanne zur Erzielung eines Zwischenergebnisses definiert werden, kann hingegen Gegenstand der Abnahme sein. Das zu Beginn des agilen Projekts grob definierte Werk wird damit im Wege der agilen Entwicklung mit jedem Inkrement, dem Ergebnis aus einem erledigten Sprint, immer weiter konkretisiert. Die Sprintreviews können hierbei als Teilabnahme genutzt werden, wenn diese ähnlich einem Abnahmeprotokoll schriftlich dokumentiert sind. Wurde im Beispielsfall definiert, dass die Interaktion der Produkte im Vordergrund steht, und dazu in einem Sprint Backlog vereinbart, dass mittels einer zu erstellenden digitalen Schnittstelle ein Produkt sich autonom betriebsbereit schalten soll, sobald sich ein anderes Produkt innerhalb eines Radius von 20 m befindet, könnte dies Gegenstand einer Abnahme sein.

Für die Gesamtabnahme gibt es zwei unterschiedliche Herangehensweisen: Entweder muss zur Erzielung der Abnahmefähigkeit eines Werks eine sog. Frozen Zone des Product Backlogs eingerichtet werden, innerhalb derer das Product Backlog nicht mehr geändert werden darf. Zwar kann dieses Vorgehen den agilen Prozess verlangsamen, bringt aber einen sinnvollen Abschluss für das Projekt. Oder aber das sog. Automated Testing kommt zum Einsatz. Dies ersetzt eine Abnahme zu jedem von den Parteien gewünschten Zeitpunkt. So kann das als Inkrement oder sog. Shippable Product erzielte Teilergebnis, das nach jedem Sprint grundsätzlich vorhanden sein sollte, sogleich in der Praxis eingesetzt werden, da immer eine Abnahme erfolgt. Vorteile bringt dieses Vorgehen insb. bei Projekten mit einer kurzen Time-to-Market-Zeitspanne oder bei denen eine frühzeitige Kundenreaktion maßgeblich für die weitere Entwicklung ist. Allerdings sind hohe Anforderungen an die Technik und die Betriebsumgebung, inklusive entsprechender Verantwortlichkeiten sowie die herausfordernde Kalibrierung für das Testing zu meistern. Sofern das Automated Testing genutzt wird, ist in den Abnahmeregelungen festzuhalten, wie und durch wen die Ergebnisse des Testings abgerufen und dokumentiert werden und welche Rechtswirkung dies haben soll. Im Beispielsfall könnte vereinbart werden, dass 14 Tage nach einem Software-Update der Produkte mit der Zusatzfunktion der autonomen Inbetriebnahme ermittelt wird, wie oft Kunden autonom eingeschaltete Produkte sofort wieder abschalten und sich damit diese Zusatzfunktion als nicht erwünscht erweist.

Kernpunkt der Vertragsgestaltung: die Vergütung

Im Rahmen von agilen Verträgen wird letztlich zwischen drei Vergütungsmodellen unterschieden:

Beim agilen Festpreis werden sog. User Stories, also Beschreibungen der Anwendung eines Produkts, dem Aufwand nach geschätzt und es werden sog. Story Points, mit der die Größe der User Story beschrieben werden, vergeben. Daraus ergibt sich ein Pauschalpreis, der durch die Anpassung der User Stories und damit der Story Points modifiziert werden kann. Erschwert wird dadurch allerdings die Beendigung des Projekts. Eine Abwandlung dessen sieht vor, dass auch im Rahmen von Vereinbarungen zum agilen Festpreis das Projekt nach jedem Sprint beendet werden kann und dann nur die bis dahin vom Auftraggeber genutzte oder nutzungsfähige Software bzw. das erzielte Produkt zu bezahlen ist. Klärungsbedürftig ist hier allerdings, wie das Vergütungsrisiko auf die Parteien interessengerecht verteilt wird.

Beim Pay-per-Sprint-Modell wird nach jedem oder für jeden Sprint gezahlt. Dies kann allerdings bei Vereinbarung einer konkludenten Abnahme zu Komplikationen führen. Zudem wird die Bedeutung von Sprintreviews gesteigert, die ggf. unbeabsichtigt gegen Ende des Projekts komplexer und länger werden können, so dass die Effizienzgewinne der agilen Methode gefährdet sind.

Schließlich gibt es Bonus- / Malus-Modelle, die auf eine gewisse Erfolgsbelohnung abzielen und z. B. 20 % mehr Vergütung versprechen, wenn das Produkt nach acht anstelle von zehn Sprints fertiggestellt wird. Dieses Modell birgt die Gefahr, dass die Qualität des Produktes leidet, weil es vorrangig um ein vorgegebenes zeitliches Ziel geht.

Weiterer Regelungsbedarf

Alle weiteren für einen agilen Vertrag typischen Klauseln sind mit Blick auf dessen Besonderheiten zu gestalten. Grundsätzlich gilt, dass stets anhand der Parteiinteressen abgewogen werden muss, welche Standards in welchem Umfang benötigt werden und wie sich diese auf die Agilität des Projekts auswirken können. So bedarf es keiner umfangreichen Garantie eines MVP (Minimal Viable Product), also einer Entwicklungsstufe des Produkts, in der es erstmals real getestet werden kann, wenn sich bereits abzeichnet, dass diese sich in naher Zukunft noch verändern könnte. Zudem sind Nutzungsrechte und die Art und Weise der Dokumentation in Form von Handbüchern und Entwicklungsdokumentationen zu regeln.

Fazit

Bei agilen Verträgen sind die Vertragsparteien und deren Berater gefordert, wie auch beim agilen Arbeiten an sich, gewohnte Pfade zu verlassen. Vielmehr sind individuelle Regelungen notwendig, die den agilen Werten gerecht werden. Standardlösungen verbieten sich damit zumeist. Sofern sich aber die Vertragsparteien über das Ziel und die Rahmenbedingungen einig sind, können durchaus pragmatische Lösungen gefunden werden. Beratern mit einem vertieften Verständnis zum agilen Arbeiten kommt dabei eine zentrale Rolle zu.

Microsoft Office 365 als technische Überwachungseinrichtung

Die unternehmenseinheitliche Nutzung von Microsoft Office 365 mit der Möglichkeit einer zentralen Kontrolle von Verhalten und Leistung der Arbeitnehmer erfordert aus zwingenden technischen Gründen eine betriebsübergreifende Regelung, für die der Gesamtbetriebsrat zuständig ist. Dies stellte das BAG mit Urteil vom 08.03.2022 (Az. 1 ABR 20/21, DB 2022, S. 2101) klar.

Der Betriebsrat hat nach § 87 Abs. 1 Nr. 6 BetrVG bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, mitzubestimmen. Zur Überwachung „bestimmt" sind dabei solche technischen Einrichtungen, die objektiv geeignet sind, Verhaltens- oder Leistungsinformationen über den Arbeitnehmer zu erheben und aufzuzeichnen. Dabei kommt es auf die subjektive Überwachungsabsicht des Arbeitgebers nicht an. Unstreitig handele es sich bei dem Softwarepaket Office 365 um eine technische Einrichtung in diesem Sinn. Die im Zusammenhang mit einer Verwendung der Desktop-Anwendungen Office 365 ProPlus und den einzelnen Diensten erstellten, anfallenden oder erhobenen Daten können laut BAG für eine Leistungs- oder Verhaltenskontrolle der Arbeitnehmer genutzt werden.

Hinweis: Bei der Einführung und Anwendung der neuen Software handele es sich um eine Angelegenheit, die mehrere Betriebe betrifft und nicht durch die einzelnen Betriebsräte geregelt werden kann. Aus diesem Grund sei für die Ausübung des Mitbestimmungsrechts der Gesamtbetriebsrat zuständig.

Vergabeverfahren: Kein Ausschluss wegen potenzieller Einbindung eines US-Hosting-Dienstes

Mit seinem Beschluss kippte das Oberlandesgericht Karlsruhe (OLG) am 07.09.2022 (Az. 15 Verg 8/22) die Entscheidung der Vergabekammer (VK) Baden-Württemberg vom 13.07.2022, nach der die potenzielle Einbindung eines US-Hosting-Dienstes datenschutzrechtlich ein Ausschlusskriterium in einem Vergabeverfahren darstellen sollte (Az. 1 VK 23/22).

Hintergrund der Entscheidung war die europaweite Ausschreibung zweier kommunaler Krankenhausgesellschaften zur Beschaffung einer Software für ein digitales Entlassmanagement für Patienten. insb. aufgrund der Sensibilität der für die Software erforderlichen personenbezogenen Daten war beim Verfahren vorausgesetzt, dass die Anforderungen der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) erfüllt sein müssen. Es bewarben sich mehrere Unternehmen auf die Ausschreibung. Ein Unternehmen, welches als Hosting-Dienstleister eine luxemburgische Tochtergesellschaft eines US-amerikanischen Unternehmens einbinden wollte, erhielt den Zuschlag in diesem Vergabeverfahren. Dabei versicherte es in seinem Angebot, dass die personenbezogenen Daten ausschließlich auf einem in Frankfurt am Main befindlichen Server einer deutschen GmbH verarbeitet würden. In einem nachfolgenden Nachprüfungsantrag rügte eine Konkurrentin bei der VK, dass das ausgewählte Unternehmen vom Verfahren hätte ausgeschlossen werden müssen, weil es personenbezogene Daten auf Servern verarbeite, auf die die USA als Drittstaat Zugriff hätten. Die VK entschied daraufhin, das Unternehmen aus dem Vergabeverfahren auszuschließen, da es für einen Verstoß gegen §§ 44 ff. DSGVO ausreiche, wenn das latente Risiko eines Zugriffs von staatlichen und privaten Stellen außerhalb der Europäischen Union bestehe.

Gegen diese Entscheidung legte das zuvor beigeladene Unternehmen, welches den Zuschlag erhalten hatte, Beschwerde beim OLG ein und begehrte die Aufhebung der Entscheidung. Das OLG gab der Beschwerde statt und hob die Entscheidung der VK unter Zurückweisung des Nachprüfungsantrags auf. Es seien keine Anhaltspunkte gegeben, nach denen anzunehmen wäre, dass ein Drittstaat Zugriff auf die sensiblen Daten erlangen könnte. Grundsätzlich könne ein öffentlicher Auftraggeber davon ausgehen, dass die Angaben eines Bieters im Vergabeverfahren korrekt seien und er seine vertraglichen Zusagen erfüllen wird. Erst wenn sich aufgrund konkreter Anhaltspunkte Zweifel daran ergäben, müsse der öffentliche Auftraggeber ergänzende Informationen einholen und die Erfüllbarkeit des Leistungsversprechens prüfen. Im vorliegenden Fall hat das Unternehmen jedoch unzweifelhaft Zusicherungen zu dem Vertragsinhalt zwischen ihm und dem luxemburgischen Tochterunternehmen gemacht. So wurde vereinbart, dass die personenbezogenen Gesundheitsdaten ausschließlich nach Luxemburg übermittelt und auch zu ihrer Verarbeitung die EU nicht verlassen, sondern nur in Deutschland verarbeitet würden. Auf dieser Grundlage konnten die zwei kommunalen Krankenhausgesellschaften darauf vertrauen, dass das Unternehmen diese Vorgaben auch in ihrem Verhältnis zur luxemburgischen Tochtergesellschaft vertragsgemäß umsetzen werde. Sie mussten auch im Hinblick auf eine mögliche Konzernbindung nicht davon ausgehen, dass personenbezogene Daten in die USA übermittelt werden. Damit erfüllte das Angebot des ausgewählten Unternehmens alle Anforderungen an die DSGVO und BDSG und war nicht vom Verfahren auszuschließen.

Hinweis: Für öffentliche Auftraggeber bedeutet dieser Beschluss, dass sie bei Projekten, bei denen personenbezogene Daten verarbeitet werden und Drittstaaten auf Bieterseite involviert sein könnten, bezüglich der Einhaltung der DSGVO und des BDSG zwar besonders gründlich die vertraglichen Vereinbarungen überprüfen müssen, sie aber grundsätzlich auf die Angaben des Bieters vertrauen können und nur bei konkreten Anhaltspunkten einen Ausschluss vom Verfahren in Betracht ziehen müssen.

Green IT: Der grüne Pfad der Informationstechnologie

War die Beurteilung von ökologischen Aspekten eines Unternehmens in der Vergangenheit sowohl für Unternehmenslenker als auch für Prüfer eher ein „esoterisches" Thema von geringer Relevanz, hat sich dies nicht nur durch die Anforderungen der Nachhaltigkeitsberichterstattung massiv gewandelt. Ein wesentlicher Faktor in der ökologischen Betrachtung eines Unternehmens ist in der digitalisierten Welt die Umweltverträglichkeit der Informationstechnologie.

Die Bedeutung von „Green IT"

Der Begriff „Green IT" beschreibt umweltverträgliche Produkte und Dienstleistungen der Informationstechnologie (IT) sowie eine möglichst ressourcenschonende Nutzung von Informations- und Kommunikationstechnik. Dabei wird neben der Nutzung auch der gesamte Lebenszyklus von der Herstellung bis zur Entsorgung und dessen Auswirkungen auf das Klima und andere Umwelteinwirkungen wie z.B. der Einsatz von kritischen Rohstoffen berücksichtigt.

Längst ist in vielen Firmen die Auslagerung von Informationstechnologie ein wichtiger Bestandteil von Unternehmen. Daher trifft Green IT nicht nur die hauseigenen Abteilungen, sondern ist gerade bei Rechenzentren ein wichtiges Thema. Bspw. basiert jede Cloud-Technologie, jedes E-Mail-Programm und jeder Streamingdienst auf Servern, welche in einem Rechenzentrum betrieben werden.

Der Bau eines Rechenzentrums

Der Lebenszyklus eines Rechenzentrums beginnt mit dem Bau. Neben der Auswahl eines geeigneten Bauplatzes bietet die Auswahl der Materialien eine viel größere Möglichkeit. Carbonbeton ist ein Verbundwerkstoff aus Hochleistungsbeton und einer Bewehrung aus Carbon. Im Vergleich zum herkömmlichen Stahlbeton reduziert die Verwendung von Carbonbeton den Energiebedarf und den CO_2-Ausstoß bei der Herstellung und Instandsetzung von Gebäuden um die Hälfte. Ein weiterer Vorteil ist die Haltbarkeit des speziellen Betongemisches. Carbonbeton hat eine doppelt so lange Lebensdauer wie Stahlbeton. Dies senkt auch die Kosten für Instandhaltungen.

Strom zum Betrieb

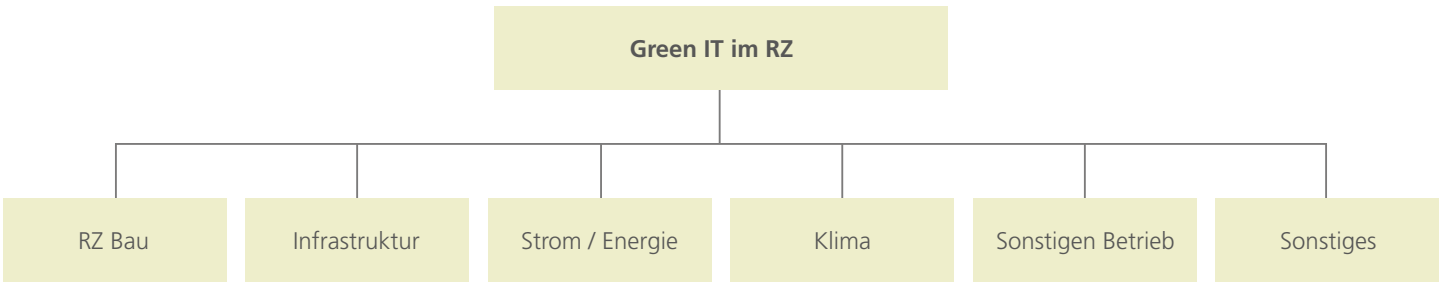
Ein bedeutender Ansatz hin zu einer grünen IT liegt in der Nutzung eines Rechenzentrums. Dabei ist am Stromverbrauch sowie dessen Gewinnung nicht vorbeizukommen. Es gibt kein Rechenzentrum und keine Informations- und Kommunikationstechnik, welche ohne Strom funktioniert. Laut einer Studie des Fraunhofer-Instituts für Zuverlässigkeit und Mikrointegration (IZM), Berlin (Abschlussbericht der Studie: Entwicklung des IKT-bedingten Strombedarfs in Deutschland: https://www.bmwk.de/Redaktion/DE/Downloads/E/entwicklung-des-ikt-bedingten-strombedarfs-in-deutschland-abschlussbericht.pdf?__blob=publicationFile&v=3), betrug der Stromverbrauch für Informationstechnologie im Jahr 2017 rund 58,4 Terrawattstunden (TWh), was zwei Prozent des gesamten Stromverbrauchs in Deutschland entspricht. Aufgrund stetiger Entwicklungen in der Digitalisierung, welche immer höhere Rechenleistungen benötigen, wie z. B. Künstliche Intelligenz oder die Blockchain-Technologie, ist laut Expertenschätzungen von einem weiterhin steigenden Energiebedarf von mehr als 60 Prozent im Zeitraum von 2015 bis 2025 auszugehen.

Im Zusammenhang mit den aktuell steigenden Energiepreisen können hier hohe Kosten auf Unternehmen zukommen. Daher ist eine Reduzierung des Stromverbrauchs nicht nur unter Betrachtung der Umweltaspekte nützlich, sondern sorgt für eine Reduzierung der Betriebskosten. Natürlich spielt auch die Art der Stromgewinnung eine große Rolle für eine grüne IT. Hier kann auf Ökostrom durch nachhaltige Technologien zurückgegriffen werden.

Klimatisierung der Server

Die Klimatisierung der Server ist ein weiteres Thema, mit dem ein Rechenzentrum zu kämpfen hat. Server erzeugen in Form von Wärme große Mengen an Energie. Diese bleibt jedoch zum Großteil ungenutzt, da sie nicht effizient weiterverwendet werden kann. Durch die Nutzung von sog. Warm- und Kaltgängen kann eine effizientere Kühlung gewährleistet sowie eine Nutzung der Abwärme ermöglicht werden. Dadurch kann beispielweise die Gebäudeheizung oder die Warmwasseraufbereitung mit der Abwärme aus dem Rechenzentrum versorgt werden.

Häufig werden zur besseren Kühlung auch Kältemittel eingesetzt. Die sog. HFKW- oder FKW-Kältemittel (FKW steht für Fluorkohlenwasserstoffe und bezeichnet fluorierte Derivate der Kohlenwasserstoffe. Es wird zwischen teilweise (HFKW) und vollständig halogenierten (FKW) Fluorkohlenwasserstoffen unterschieden.) verzichten auf Chlor und schädigen damit nicht mehr die Ozonschicht. Allerdings tragen sie weiterhin zur Erderwärmung bei. In grünen IT-Landschaften werden Kälteanlagen mit nicht-halogenierten Kältemitteln eingesetzt, welche auch ressourcenschonend sind.



Umgang mit Hardware

Weltweit sind rund zwei bis drei Prozent der Kohlenstoffdioxid-Emission auf die Informationstechnologie zurückzuführen. Eine Studie des französischen „The Shift Project" prognostiziert, dass die Emissionen der Informationstechnologie bis 2025 sogar acht Prozent am gesamten CO_2-Ausstoß ausmachen könnten. Damit würde die IT-Branche die Umwelt stärker belasten als Autos und Motorräder. Zieht man nur die Hardware in Betracht, so entsteht der überwiegende Teil der klimaschädlichen Emissionen im Rahmen der Herstellung. Eine lange Nutzungsdauer der Hardware verringert entsprechend diese Bilanz.

Die Außenwirkung von Green IT

Unternehmen, welche sich mit dem Thema Green IT befassen und entsprechende Maßnahmen ergreifen, sollten dies auch außenwirksam bekannt machen. Durch Green Marketing erfahren auch Kunden und Geschäftspartner von der nachhaltigen Ausrichtung. Dies verbessert das Ansehen sowie die öffentliche Wahrnehmung des Unternehmens. Auch innerhalb von Lieferketten und zwischen Geschäftspartnern spielt die nachhaltige Aufstellung eines Unternehmens eine zunehmend wichtigere Rolle. Eine sehr populäre Bewegung der letzten Jahre stellt hier „Fridays for Future" dar. In der Politik und vor allem in der Gesellschaft wächst das Bewusstsein für ein ressourcenschonendes und umweltverträgliches Unternehmen. Da vor allem die Informationstechnologie ressourcenintensiv ist, rückt auch sie ins Zentrum solcher Überlegungen.

Lagert ein Unternehmen seine IT an ein grünes Rechenzentrum aus oder bezieht von dort betriebene Systeme, kann es seine Umweltbilanz einfacher optimieren, als selbst in eine grüne IT zu investieren, da in Rechenzentren gebündelte Maßnahmen einfacher ergriffen werden können.

Prüfung und Beurteilung der Umweltverträglichkeit der IT

Die genannten Aspekte der Green IT stellen Ausschnitte einer ganzheitlichen Umweltbetrachtung dar. In jedem Fall müssen alle wesentlichen Umweltaspekte berücksichtigt werden, um zu validen Prüfungsergebnissen zu gelangen. Neben Energie und Umweltverträglichkeit der Infrastruktur stellen sich hier auch Fragen zum Betrieb, z. B. welche Kältemittel verwendet werden oder wie viele Mitarbeiter mit welchen Verkehrsmitteln wie oft zum Rechenzentrum reisen etc. Die Beurteilung der Umweltverträglichkeit der Informationstechnologie ist ein komplexes Themenfeld, das viele Herausforderungen beinhaltet.

ISO/IEC 27001:2022 – alles auf Anfang?

Nach Veröffentlichung der FDIS (Final Draft International Standard) im Juli 2022, erfolgte am 25.10.2022 die Veröffentlichung der finalen Version der ISO/IEC 27001:2022. Nach redaktionellen Anpassungen der deutschen Übersetzung, zuletzt 2017, ist dies nach beinahe zehn Jahren die erste inhaltliche Aktualisierung der zentralen Norm für Informationssicherheit. Die ISO/IEC 27001 definiert die Rahmenbedingungen für ein Informationssicherheitsmanagementsystem (ISMS) nach best practice Ansatz und stellt gleichzeitig die Norm dar, gegen die die jeweilige ISMS-Implementierung geprüft und damit zertifiziert werden kann.

Die Liste möglicher Informationssicherheitsmaßnahmen im normativen Anhang A der neuen ISO/IEC 27001:2022 ist identisch aus dem überarbeiteten Leitfaden ISO/IEC 27002:2022 abgeleitet (siehe dazu unseren Artikel in der ersten Ausgabe 2022). Dies stellt auch für die Unternehmen die zentrale Anforderung bei der Umsetzung dar.

Neben der Neustrukturierung der bereits aus der vorhergehenden Fassung bekannten Anforderungen im Anhang A sowie der zusätzlichen Anforderungen im Anhang A, über die wir bereits im ersten novus IT 2022 berichteten, haben sich auch inhaltliche Änderungen der Hauptnorm der ISO/IEC 27001:2022 ergeben. Hierbei sind insb. drei Anpassungen erwähnenswert.

Harmonized Structure

Eine Änderung betrifft die sog. „Harmonized Structure". Die Harmonized Structure (HS), ehemals High Level Structure (HLS), wurde 2012 von der International Organization for Standardization (ISO) entwickelt und eingeführt. Hintergrund war die Schaffung einer einheitlichen Struktur, wonach Managementsysteme geplant und umgesetzt werden können. Durch die Umstellung auf die HS erfolgt nun, wie bereits bei anderen Normen, die Umstellung dahingehend, dass die Geschäftsprozesse in den Fokus eines ISMS rücken. Neu ist Kapitel 6.3 und damit die Anforderung, dass Änderungen am ISMS geplant umzusetzen sind. Es handelt sich hierbei um eine bereits aus anderen Managementsystemen bekannte Anforderung. Bereits der Übergang von der ISO/IEC 27001:2013 auf die ISO/IEC 27001:2022 ist als ein Beispiel einer solchen Änderung zu sehen. Die Überführung in die HS führt an weiteren Stellen in der Norm dazu, dass formale Anpassungen vorgenommen wurden (bspw. zusätzliche Unterpunkte in Kapitel 9.2 (Internes Audit) mit 9.2.1 und 9.2.2 sowie Kapitel 9.3 (Managementbewertung) mit 9.3.1, 9.3.2, 9.3.3).

MC 4.4 – Informationssicherheitsmanagementsystem

Eine weitere Änderung betrifft Kapitel 4.4 (Informationssicherheitsmanagementsystem). Die bisherige Anforderung war: „Die Organisation muss entsprechend den Anforderungen dieser Internationalen Norm ein Informationssicherheitsmanagementsystem aufbauen, verwirklichen, aufrechterhalten

und fortlaufend verbessern." Dies wird dahingehend erweitert, dass die für eine Aufrechterhaltung und Umsetzung erforderlichen Prozesse und ihre Wechselwirkungen im Rahmen des ISMS zu definieren sind.

MC 8.1 – Betriebliche Planung und Steuerung

Die letzte Änderung betrifft Kapitel 8.1 (Betriebliche Planung und Steuerung). Ergänzend muss die Organisation nun auch Prozesskriterien festlegen, um die Maßnahmen zur Bewältigung der Informationssicherheitsrisiken umzusetzen. Die Steuerung der Prozesse muss entsprechend in Übereinstimmung mit diesen Kriterien umgesetzt werden.

Die weiteren zentralen Änderungen liegen in der ISO/IEC 27002:2022 und haben damit auch Auswirkungen auf die ISO/IEC 27001:2022 – bspw. hinsichtlich der Maßnahmen zur Informationssicherheitsrisikobehandlung aus Kapitel 6.1.3. Der Anhang A der ISO/IEC 27002:2022 ist zentraler Bestandteil der Anforderung aus 6.1.3 c)

Umstellung der Zertifikate

Die Umstellung der Zertifikate erfolgt in einem zweistufigen Verfahren. Im ersten Schritt müssen die bei der Deutsche Akkreditierungsstelle GmbH (DAkkS) akkreditierten Zertifizierungsstellen (so auch die ESecurity-CERT GmbH als unabhängige Zertifizierungsstelle im Ebner Stolz Verbund) einen Antrag auf Änderung der Akkreditierung bei der DAkkS stellen und sich einem Audit durch die DAkkS unterziehen, um eine Neu-Akkreditierung für die ISO/IEC 27001:2022 zu erhalten. Dieser Prozess muss gemäß Vorgabe des IAF durch die DAkkS bis Oktober 2023 abgeschlossen sein. In einem zweiten Schritt können dann die von der jeweiligen Zertifizierungsstelle ausgegebenen Zertifikate nach DIN EN ISO/IEC 27001:2017-06 im Rahmen des Prüfungszykluses auf die ISO/IEC 27001:2022 umgestellt werden.

Für den Prozess der Transition auf die ISO/IEC 27001:2022, wurde durch das IAF (International Accreditation Forum) entsprechende Vorgaben definiert – sowohl für die Akkreditierungsstelle als auch für die Zertifizierungsstellen. Hieraus ergibt sich auch der zeitliche Rahmen für die bereits zertifizierten sowie die neu zu zertifizierenden Unternehmen. In Kürze zusammengefasst wurde folgendes festgelegt:

- **Die Transitionsphase beträgt drei Jahre ab Veröffentlichung der ISO/IEC 27001:2022 (und endet somit am 24.10.2025)**
- **Vorgaben für die DAkkS/Akkreditierungsstellen:**
  - Spätestens sechs Monate nach Veröffentlichung (25.10.2022) der ISO/IEC 27001:2022 (somit am 25.04.2023) müssen die nationalen Akkreditierungsstellen die Möglichkeit bieten, sich für die neue Norm akkreditieren lassen zu können.
  - Erstakkreditierungen nach ISO/IEC 27001:2022 müssen spätestens ab dem 25.4.2023 möglich sein.
  - Die Umstellung der Akkreditierung für Zertifizierungsstellen (wie die ESecurity-CERT GmbH) muss innerhalb von zwölf Monaten (somit bis zum 24.10.2023) abgeschlossen sein.
- **Vorgaben für die ESecurity-CERT GmbH/Zertifizierungsstellen:**
  - Zertifizierte Mandate müssen bis Oktober 2025 umgestellt sein.
  - Die Umstellung kann in Verbindung mit einem Überwachungsaudit, Rezertifizierungsaudit oder in einem separaten Audit erfolgen (nachfolgend wird nur das Wort „Audit" verwendet).
  - Das Audit darf sich nicht nur auf eine Dokumentenprüfung stützen, insb. für die Überprüfung der technischen Kontrollen.
  - Das Audit umfasst u.a.:
    - die Lückenanalyse der ISO/IEC 27001:2022 sowie die Notwendigkeit von Änderungen am ISMS.
    - die Aktualisierung der Anwendbarkeitserklärung (SoA).
    - gegebenenfalls die Aktualisierung des Risikobehandlungsplans.
    - die Umsetzung und Wirksamkeit der neuen oder geänderten Kontrollen, die von den Mandanten gewählt wurden.
  - Das Audit kann remote durchgeführt werden, sofern sichergestellt werden kann, dass die Ziele des Audits erreicht werden.
  - Unabhängig von der Auditform (Überwachungsaudit, Rezertifizierungsaudit, separates Audit) ergeben sich zusätzliche Mindestaufwände, die bei der ESecurity-CERT GmbH anfallen und die berechnet werden müssen.
  - Mit Abschluss des Audits erfolgt eine Aktualisierung der Zertifizierungsdokumente. Sofern das Audit im Rahmen eines separaten Audits erfolgt und damit nur die Transition geprüft wurde, wird der Ablauf des aktuellen Zertifizierungszyklus nicht geändert.

Mapping ISO/IEC 27002:2013 vs. ISO/IEC 27002:2022

Als Unterstützung zur Umsetzung der Anforderungen, finden Sie auf der Homepage der ESecurity-CERT GmbH eine frei verfügbare Excel-Liste mit dem Mapping der Kontrollen aus dem Anhang A zwischen der ISO/IEC 27002:2022 und der bisherigen ISO/IEC 27002:2013. Ebenso eine beispielhafte Darstellung einer angepassten Statement of Applicability (SoA), welche naturgemäß um weitere Spalten individualisiert werden kann (bspw. KPI-Reporting und Risikomanagement).

NIS 2.0 Direktive – Update des IT-SiG 2.0

Durch die europäische Kommission wurde Ende 2015 vor dem Hintergrund einer einheitlichen europäischen Cyber-Sicherheitsstrategie die sog. Netzwerk- und Informationssicherheit (NIS) Richtlinie finalisiert. Sie ist am 08.08.2016 mit der Vorgabe der länderspezifischen Umsetzung in Kraft getreten (EU-Richtlinie 2016/1148). In Deutschland ist am 25.7.2015 das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz, kurz IT-SiG) verabschiedet worden sowie am 30.6.2017 das „Gesetz zur Umsetzung der NIS-Richtlinie" in Kraft getreten. Zum 28.5.2021 erfolgte bereits das Inkrafttreten des IT-Sicherheitsgesetzes 2.0, das u. a. die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erhöhte, eine Erweiterung der betroffenen Unternehmen als KRITIS-Betreiber vornahm und gleichzeitig auch zusätzliche Pflichten für KRITIS-Betreiber definiert.

Die Umsetzung in den Mitgliedsstaaten erwies sich insgesamt als schwierig, was dazu führte, dass die EU-Kommission sich veranlasst sah, Ende 2020 eine Überarbeitung der NIS-Richtlinie im Entwurf vorzunehmen, um durch die fortschreitende Digitalisierung und die damit in Zusammenhang stehende wachsende Bedrohungslage für kritische Infrastrukturen sowie die Zunahme von Cyberangriffen zu reagieren. Die vorgeschlagene Ausweitung des Geltungsbereichs der NIS 2.0, die mehr Einrichtungen und Sektoren dazu verpflichtet, Maßnahmen zur Absicherung zu ergreifen, würde dazu beitragen, das Niveau der Cybersicherheit in Europa langfristig zu erhöhen. Am 10.11.2022 hat das EU-Parlament dem Entwurf der NIS 2.0 Richtlinie zugestimmt (T9-0383/2022).

Änderungen in NIS 2.0

Änderungen bzw. Neuerungen der NIS 2.0 sind u. a.:

- Erweiterung der KRITIS-Sektoren und der betroffenen Unternehmen (Art.2 und 3)
  - Sehr starke Erhöhung der Anzahl der betroffenen Unternehmen – Schwellenwerte durften in der Vergangenheit durch die Mitgliedstaaten festgelegt werden, was in Deutschland durch die hohen Schwellenwerte (abgeleitet aus der Anzahl versorgter Personen) je nach Sektor und Anlagenart realisiert wurde. Künftig werden die Schwellenwerte unternehmensgrößenbezogen durch die NIS Direktive vorgegeben, was künftig mittlere und große Unternehmen betreffen wird. Inwieweit bei nationaler Umsetzung der Richtlinie bei der Definition der Unternehmen, die schlussendlich in den Anwendungsbereich der NIS 2 Richtlinie national fallen, Erleichterung durch die Berücksichtigung der Verhältnismäßigkeit, des höherwertigen Risikomanagements und eindeutiger Kritikalitätskriterien Einfluss finden, bleibt abzuwarten. Die Größenordnung der NIS stellt sich derzeit wie folgt dar:
    - Mittlere Unternehmen: 50 bis 250 Beschäftigte, 10 bis 50 Mio. Euro Umsatz, ‹ 43 Mio. Euro Bilanzsumme.
    - Große Unternehmen: mehr als 250 Beschäftigte, mehr als 50 Mio. Euro Umsatz, mehr als 43 Mio. Euro Bilanzsumme.
- Erhöhung der Anzahl an Sektoren von Betreibern (sog. Entities) auf insgesamt 18. Hierbei ist zu differenzieren zwischen elf „essentiell" (wesentlichen) sowie sieben „important" (wichtigen) Sektoren.
- Die NIS 2.0 erweitert die KRITIS-Betreiber ebenfalls um den Sektor „Öffentliche Verwaltung" (Regionale Regierung, Zentralregierung, Regionale Regierung (kritisch)) sowie weitere Industriezweige. Darüber hinaus sind Teilsektoren in der NIS-Richtlinie neu mit aufgenommen worden, bspw. im Bereich Energie Wasserstoff sowie Fernwärme und -kälte.
- Ausgewählte Sektoren (u. a. „Digitale Infrastruktur") sollen unabhängig ihrer Größe reguliert werden.
- Maßnahmen zur Optimierung der Cyber-Security:
  - Die Richtlinie gibt erstmals Mindestanforderungen an Cyber-Security vor (Art.20).
  - Definition von 14 Cyber Security Maßnahmen, welche Betreiber in der EU umsetzen müssen, u. a. Supply Chain/ Lieferkettenmanagement, Business Continuity, Authentification Management, Kryptographie (Art.21).
  - Kritische Betreiber von digitalen Diensten und Infrastrukturen müssen sich bei der ENISA registrieren (Art.25).
- Jeder Mitgliedsstaat muss Anbieter von essentiell und important Entities an die EU-Kommission melden (Art, 3).
- Erhöhung der Sanktionen (Maximalstrafen in Höhe von 10 Mlo. Euro oder 2 Promille des weltweiten Umsatzes bei Essential Sektoren und 7 Mio. Euro oder 1,4 Promille des weltweiten Umsatzes bei important Sektoren.

Ausblick

Das IT-SiG 2.0 nahm einige Anpassungen wie bspw. die Meldung von Cybersicherheitsvorfällen innerhalb eines definierten Zeitraums, die Aufnahme weiterer Sektoren sowie erhöhte Cyber-Security Anforderungen aus der NIS 2.0 bereits auf. Allerdings sind die Anforderungen noch nicht vollständig umgesetzt – bspw. spezifische festgelegte Maßnahmen im Bereich Lieferkettenmanagement oder die Definition der Betroffenheit von großen und mittleren Unternehmen. Bei der Umsetzung in nationales Recht sind einige Vorgaben zu berücksichtigen – wie bspw. die Differenzierung zwischen den essential und important Entities, was es so in dem IT-SiG. 2.0 bisher nicht gab.

Nach Zustimmung zur NIS 2.0 Richtlinie ist das Inkrafttreten der Richtlinie, was bereits kurzfristig erfolgen wird, noch ausstehend. Ab diesem Zeitpunkt besteht dann eine verpflichtende Überführung in nationales Recht innerhalb von 21 Monaten.

Cyber Resilience Act – Cyber-Security im Produktlebenszyklus

Vor dem Hintergrund der steigenden Anzahl von Schwachstellen in Produkten mit digitalen Elementen (insb. Hard- und Software sowie die damit verbundenen Fernzugriffsmöglichkeiten) und der unzureichenden Bereitstellung von Sicherheitsupdates sowie dem Wunsch zur Steigerung der ganzheitlichen digitalen Resilienz in der gesamten IT-Wertschöpfungskette, verabschiedete die EU-Kommission am 15.10.2022 den sog. „Cyber Resilience Act" (CRA). Es handelt sich hierbei um die erste EU-weite rechtliche Verordnung zur Cyberresilienz von Produkten mit digitalen Elementen. Unter das Gesetz fallen alle Produkte, die im europäischen Binnenmarkt veräußert werden. Explizit ausgenommen ist Software, die als Dienstleistung bereitgestellt wird (u. a. Software-as-Service sowie Open Source Software Lösungen). Ebenso bspw. Cloud-Anbieter, da diese unter die NIS-2.0 Richtlinie fallen (siehe separater Artikel).

Auswirkungen des CRA

Der CRA hat Auswirkungen auf alle im Prozess der Veräußerung von IT-Produkten involvierten Parteien – Händler, Importeuer, Vertreiber und Hersteller. Im Detail bedeutet dies im Wesentlichen:

- Die Sicherheitsverantwortung über den gesamten Produktlebenszyklus liegt zukünftig für mindestens fünf Jahre beim Hersteller, so dass diese dazu veranlasst werden, durchgängig Sicherheitsupdates zur Verfügung zu stellen.
- Durchgehende Überwachung und verpflichtende Beseitigung von Schwachstellen während des Produktlebenszyklus von maximal fünf Jahren.
- Dokumentationspflicht für Cybersicherheitsrisiken.
- Durchführung eines Risk Assessments mit Bezug zur Cybersicherheit und Berücksichtigung der Cybersicherheit in der Planungs-, Entwurfs-, Entwicklungs-, Produktions-, Liefer- und Wartungsphase.
- Meldepflicht von aktiv ausgenutzten Schwachstellen und Vorfällen.
- Pflicht für verständliche Gebrauchsanweisungen.

Der CRA sieht vor, dass Produkte in drei Sicherheitsklassen u. a. auf Basis der Funktionalität und der beabsichtigten Art der Verwendung unterteilt werden:

- Standardprodukte: u.a. Fotobearbeitung, Intelligente Lautsprecher, Festplatten
- kritische Produkte Klasse I: u. a. Passwort-Manager, Firewalls
- kritische Produkte Klasse II: u. a. Betriebssysteme, Industrielle Firewalls, CPUs

Hinweis: Die Einteilung in die Klasse erfolgt auf Basis von Hersteller-Selbsterklärungen. Es wird davon ausgegangen, dass ca. 90 % der Produkte Standardprodukte sein werden.

Zum Nachweis der Erfüllung der definierten Anforderungen, muss sich der Hersteller einem Konformitätsbewertungsverfahren unterziehen. Das jeweilige Verfahren ist abhängig von der Zugehörigkeit des Produktes zur Sicherheitsklasse. Als kritisch eingestufte Produkte müssen sich der Bewertung eines sachkundigen, unabhängigen Dritten unterziehen oder nach einem Standard (der noch nicht eindeutig benannt ist) erfolgen. Die Mitgliedstaaten werden verpflichtet eine oder mehrere Marktüberwachungsstellen einzurichten.

Die Sanktionen bei Nichteinhaltung der Pflichten durch die Hersteller/Importeure/Händler orientieren sich, wie bereits bei der NIS 2.0 Richtlinie, an denen der EU-DSGVO. Schwerwiegende Verstöße können mit einem Bußgeld von max. 15 Mio. Euro oder 2,5 % des gesamten weltweiten Jahresumsatzes geahndet werden.

Hinweis: Nach Verabschiedung am 18.10.2022 besteht nun bis zum 17.10.2024 eine Übergangsfrist, welche den Herstellern/Importeuren/Händlern von entsprechenden IT-Produkten und den Mitgliedstaaten (Aufbau Marktüberwachungsstellen) gegeben wird, um sich auf die neuen Anforderungen einzustellen. Die Meldepflicht für aktiv ausgenutzte Schwachstellen und Vorfälle soll allerdings bereits ein Jahr nach Verabschiedung anwendbar sein.

Systeme zur Angriffserkennung – Orientierungshilfe des Bundesamtes für Sicherheit in der Informationstechnik zur Umsetzung

Am 28.5.2021 trat das IT-Sicherheitsgesetz 2.0 (IT-SiG) in Kraft. Wie bereits das IT-SiG 1.0, bedingte auch die Version 2.0 als Artikelgesetz weitreichende Änderungen in einer ganzen Reihe von Einzelgesetzen (neben dem BSI-Gesetz – BSIG – u. a. das Energiewirtschaftsgesetz (EnWG) und das Telekommunikationsgesetz). Das IT-SiG 2.0 geht insb. mit zusätzlichen Pflichten, u. a. für Betreiber kritischer Infrastrukturen (KRITIS-Betreiber), einher. Diese sind z. B. verpflichtet, ab dem 01.05.2023 ganzheitliche Systeme zur Angriffserkennung (SzA) nach dem geltenden Stand der Technik einzusetzen und dies gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachzuweisen (§ 8a Abs. 1a BSIG). KRITIS-Betreiber müssen den Einsatz der SzA ab dem 01.05.2023 mit dem nächsten fälligen Nachweis gemäß § 8a Abs. 3 BSIG darlegen. Für Betreiber von Energieversorgungsnetzen und Energieanlagen, die nach § 8d BSIG von der KRITIS-Regulierung gemäß BSIG ausgenommen sind, gelten die Neuerungen für SzA parallel gemäß § 11 Absatz 1e und 1f EnWG. Betreiber von Energieversorgungsnetzen und solchen Energieanlagen, die nach der Rechtsverordnung gemäß § 10 Absatz 1 BSIG als Kritische Infrastruktur gelten, haben unabhängig vom nächsten fälligen Nachweis gemäß § 11 Absatz 1f EnWG dem BSI bereits am 1. Mai 2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nach § 11 Absatz 1e EnWG nachzuweisen.

Gesetzliche Anforderungen

Ausgehend von der Definition aus § 2 Abs. 9b Satz 1 BSIG handelt es sich bei SzA um Prozesse u. a. zur Erkennung von Angriffen auf die Infrastruktur des KRITIS Betreibers, die „durch technische Werkzeuge und organisatorische Einbindung" (BSI, Orientierungshilfe, 2022, S. 6) unterstützt werden. SzA als ganzheitliche Systeme sind so definiert, dass sie „geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten" (BSI, Orientierungshilfe, 2022, S. 6) müssen und „dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen" (§ 8a Abs. 1a BSIG – BSI, Orientierungshilfe, 2022, S. 6). Weiter heißt es in BSIG §2 Abs. 9b: „Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten" (BSI, Orientierungshilfe, 2022, S. 6) Zusammengefasst bedeutet dies, dass neben technischen Maßnahmen insb. auch organisatorische Maßnahmen erforderlich sind.

Zur Unterstützung der Umsetzung dieser neuen Anforderungen hat das BSI zum 26.09.2022 die finale Version der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung" (BSI-OH-SzA) veröffentlicht. Nachfolgend stellen wir dar, wie diese Hilfestellung Unternehmen im Hinblick auf die SzA unterstützen kann.

Exkurs: Cyberangriffe versus KRITIS?

Die Motive für Cyberangriffe können unterschiedlich sein – beginnend mit finanziellen Interessen über persönliche motivierte bis hin zu gesellschaftspolitischen Interessen. Die Motive haben die Gemeinsamkeit, dass es sich dabei um Versuche handelt, durch unbefugten Zugriff auf die Informationssysteme Informationen / Daten zu erhalten, die – je nach Zielsetzung – gestohlen, geändert, gelöscht oder offengelegt werden sollen. Der Erfolg eines jeden Angriffs besteht darin, dass das Eindringen oder der Schadcode für eine möglichst lange Zeit unentdeckt bleibt, damit der Angreifer sich möglichst weit im Netzwerk ausbreiten kann. Die Vorgehensweise kann dabei auch variieren – dies zeigte bspw. der Angriff auf die Stadt Witten im Südosten des Ruhrgebietes, der zwar entdeckt wurde, aber dem Angriff aufgrund dessen Schnelligkeit nicht mehr entgegengesteuert werden konnte. Dies führte dazu, dass die gesamte Daten-Organisation verschlüsselt sowie Sicherungsfestplatten gelöscht wurden und die Stadt Witten nach dem Angriff lediglich noch eine Handvoll Magnetbänder hatte und seitdem die komplette IT neu aufbauen musste. Die bestmögliche Maßnahme bei einem solchen Vorfall ist schnelles Gegensteuern und die Isolation der kompromittierten Netzbereiche.

Eine zentrale Voraussetzung für das frühzeitige Gegensteuern ist die rechtzeitige Erkennung von Abweichungen aus bekannten Mustern, somit die Erkennung von Anomalien. Ein Beispiel kann ein ungewöhnlicher Login-Zeitpunkt eines Nutzers, unter Umständen verbunden mit erhöhten Netzaktivitäten sein. Das solche Anomalien nicht zwangsweise Cyberangriffe darstellen, ist die eine Sache – allerdings geht es darum, dass diese Anomalien von SzA überhaupt erkannt und analysiert werden können, um ggf. Maßnahmen einleiten zu können.

Orientierungshilfe des BSI

Mit der Orientierungshilfe gibt das BSI mögliche Ausgestaltungsvorgaben zur individuellen Umsetzung und Prüfung einer SzA. Dazu differenziert das BSI neben allgemeingültigen, grundlegend geltenden Anforderungen, auch Anforderungen für folgende drei Funktionsbereiche von SzA:

- **Protokollierung:** Fortlaufende Auswertung der gesammelten Information
- **Detektion:** Erkennung der sicherheitsrelevanten Ereignisse anhand der gesammelten Informationen
- **Reaktion:** Implementierung von Maßnahmen, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren

Die Anforderungen für diese Funktionsbereiche haben – differenziert nach der **Planung** und **Umsetzung** adäquater Maßnahmen – wiederum drei verschiedene Anforderungsausprägungen, die sich in der geforderten Verbindlichkeit der Umsetzung unterscheiden (Muss, Sollte, Kann). Gemäß IT-Grundschutzkompendium ist die Abgrenzung zwischen „Muss" und „Sollte":

- „Muss": Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderung).
- „Sollte": Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden." (BSI, IT-Grundschutzkompendium, Stand Februar 2022, S. 5/6).
- „Kann": Dieser Ausdruck bedeutet, dass die Anforderungen nicht zwingend erforderlich sind, aber eine sinnvolle Ergänzung darstellen, wenn ein Umsetzungsgrad der Stufe 5 erreicht werden soll (vgl. „Reifegradmodell zur Bewertung des Grades der Umsetzung" in diesem Artikel).

Die grundsätzlichen Anforderungen für alle Bereiche sind, dass

- „die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen geschaffen werden müssen,
- Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden müssen,
- durchgängig alle zur effektiven Angriffserkennung erforderliche Hard- und Software auf einem aktuellen Stand gehalten werden muss,
- die Signaturen von Detektionssystemen immer aktuell sein müssen,
- alle relevanten Systeme so konfiguriert sein müssen, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt, sofern keine schwerwiegenden Gründe dagegensprechen." (BSI, Orientierungshilfe, 2022, S.8)

Zusätzlich verweist das BSI auf Bausteine aus dem IT-Grundschutz des BSI, wobei die kursiv markierten Punkte von wesentlicher Bedeutung in der Planung und Umsetzung sind.

- *OPS.1.1.4 Schutz vor Schadprogrammen*
- *OPS.1.1.5 Protokollierung*
- *NET.1.2 Netzmanagement*
- *NET.3.2 Firewall*
- *DER.1 Detektion von sicherheitsrelevanten Ereignissen*
- *DER.2.1: Behandlung von Sicherheitsvorfällen*

Jeder dieser Bausteine umfasst – analog der Orientierungshilfe – Anforderungen, die für den jeweiligen Baustein erfüllt werden müssen. Außerdem wird der Mindeststand zur Protokollierung und Detektion von Cyberangriffen des BSI sowie die ISO/IEC 2700x-Reihe und die Norm IEC 62443 referenziert.

Nachfolgend stellen wir im Detail dar, welche Mindestanforderungen das BSI zur Umsetzung für die drei Bereiche Protokollierung, Detektion und Reaktion sieht.

Protokollierung

Im Rahmen der Planungsphase werden durch das BSI folgende Muss-Anforderungen gestellt:

- **Milestone-Planung:** Die Schritte der Implementierung sind so zu wählen, dass eine angemessene Sichtbarkeit* während einer adäquaten Zeit erzielt wird. Im Rahmen der Planung müssen alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Infrastruktur maßgeblich sind. (*Unter Sichtbarkeit versteht das BSI die Anzahl der Datenquellen, deren zu protokollierende Ereignisse durch die Einrichtung erhoben werden. Es wird differenziert zwischen der Quantität der Sichtbarkeit (Anzahl der IT-Systeme und Datenquellen auf Endpunkten und im Netz, deren Daten durch die Einrichtung gesammelt werden) und der Qualität der Sichtbarkeit (Positionierung der Punkte der Erhebung (wie z. B. Sensoren)
- **Dokumentation:** Der gesamte Prozess der Planungsphase ist in geeigneter, nachvollziehbarer Form zu dokumentieren und muss alle „Netzbereiche, die Protokollierungsquellen, deren Beziehungen untereinander und den Datenfluss der Protokollierungsereignisse im Anwendungsbereich umfassen" (BSI, Orientierungshilfe, 2022, S. 9). Gleichzeitig muss für die Systeme/Systemgruppen dokumentiert werden, welche Ereignisse protokolliert werden.
- **Vollständige Analyse:** Es müssen alle zur wirksamen Angriffserkennung notwendigen Protokoll- und Protokollierungsdaten auf System- und Netzebene erhoben, gespeichert und für die Auswertung bereitgestellt werden, um sicherheitsrelevante Ereignisse (SRE) zu erkennen und beurteilen zu können. Darüber hinaus sind alle Systeme zu identifizieren und zu analysieren, die zum Betrieb der kritischen Infrastruktur notwendig sind sowie diejenigen Systeme, die zur Speicherung notwendigen Systemen und deren IT-Sicherheitsvorkehrungen.

- Datenschutz: Aufgrund von ggf. personenbezogenen Datensätzen, muss der Datenschutz mit einbezogen werden.

- Change-Management: Bei Änderungen im Anwendungsbereich muss sichergestellt werden, dass entsprechend ein Change-Prozess implementiert ist.

Im Rahmen der Umsetzungsphase sieht das BSI als Mindestanforderung den **Aufbau einer zentralen Protokollierungsinfrastruktur** sowie die **Bereitstellung von Protokollierungsdaten für die Auswertung** vor. Um alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten an den für den jeweiligen Netzbereich zentralen Stelle (im Sinne der Netzarchitektur) speichern zu können, muss die Infrastruktur ausreichend dimensioniert sein (Verfügbarkeit von technischen, finanziellen und personellen Ressourcen). Im Rahmen der Bereitstellung muss sichergestellt werden, dass die Protokoll- und Protokollierungsdaten gefiltert, normalisiert, aggregiert und korreliert sowie geeignet verfügbar gemacht werden, um diese auswerten zu können. Nach erfolgreicher Umsetzung der Protokollierung muss geprüft werden, ob alle geplanten Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden.

Darüber hinaus verweist das BSI darauf, dass alle Basisanforderungen von **OPS.1.1.5 Protokollierung** aus dem Grundschutz erfüllt werden müssen. Dies bedeutet:

- **Sicherheitsrichtlinie für die Protokollierung (OPS.1.1.5.A1):** Es muss eine eigenständige, spezifische Richtlinie existieren, in der Anforderungen und Vorgaben nachvollziehbar beschrieben sind, wie die Protokollierung sicher geplant, aufgebaut sowie betrieben und wie, wo und was protokolliert werden soll. Die Richtlinie, die vom Informationssicherheitsbeauftragten und den Fachverantwortlichen erstellt und allen involvierten Mitarbeitenden bekannt gemacht werden muss, ist regelmäßig auf Aktualität zu prüfen, Änderungen sind mit dem ISB abzustimmen und zu dokumentieren. Ebenso müssen die Ergebnisse dokumentiert werden.

- **Konfiguration der Protokollierung auf System- und Netzebene (OPS.1.1.5.A3):** Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen müssen protokolliert werden. Dabei sind verpflichtend die Protokollierungsfunktionalitäten der in der Richtlinie benannten IT-Systeme und Anwendungen zu nutzen (sofern dies systemseitig vorhanden ist). Bei der Einrichtung sind jeweils die Herstellervorgaben zu beachten. Darüber hinaus müssen Abstände für die Überprüfung der Funktionalität der Protokollierung in der Richtlinie definiert sowie stichprobenartig überprüft werden.

- **Zeitsynchronisation der IT-Systeme (OPS.1.1.A4):** Die Systemzeit aller protokollierenden IT-Systeme und Anwendungen muss immer synchron und das Datum- und Zeitformat der Protokolldateien einheitlich sein.

- **Einhaltung rechtlicher Rahmenbedingungen (OPS.1.1.5.A5):** Die jeweils geltenden Bundes- und Landesdatenschutzbestimmungen sowie weitere, relevante gesetzliche Bestimmungen müssen eingehalten sowie Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden. Protokollierungsdaten sind nach einem definierten Verfahren zu löschen, wobei das unkontrollierte Ändern oder Löschen von Protokollierungsdaten technisch verhindert werden muss.

Neben diesen teils umfangreichen Muss-Anforderungen, gibt es weitere Sollte-Anforderungen sowie Kann-Anforderung. Bereits hier zeigt sich, dass ein bereits implementiertes Informationssicherheitsmanagementsystem (ISMS) bei der Umsetzung der SzA Anforderungen hilfreich ist.

Detektion

Wenn man ein SzA gemäß Anforderung umsetzen will, muss man bei der Planung zur Sicherstellung der Detektion berücksichtigten, dass die Abdeckung der Bedrohungslandschaft vor dem Hintergrund der durchgeführten Risikoanalyse und der Größe sowie Struktur des Unternehmens bei der Auswahl und dem Einsatz von Detektionsmaßnahmen sicherzustellen ist und damit in der Planung zu berücksichtigen sind.

Im Rahmen der Umsetzungsphase der SzA werden folgende Mindestanforderungen definiert:

- **Kontinuierliche Überwachung und Auswertung von Protokolldaten:** Die Protokolldaten müssen möglichst kontinuierlich überwacht und ausgewertet werden. Die Prüfung des Ereignisses und ggf. die Reaktion muss innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen. Dafür müssen ausreichend personelle Ressourcen zur Verfügung gestellt werden. Die verantwortlichen Mitarbeitenden des Unternehmens (bzw. bei Auslagerung der Funktion an einen Dienstleister die jeweiligen Mitarbeitenden) sind namentlich zu benennen und müssen aktiv nach SRE suchen. Es müssen somit ausreichend personelle Ressourcen zur Verfügung stehen.

- **Einsatz zusätzlicher Detektionssysteme:** Schadcodedetektionssysteme müssen eingesetzt und zentral verwaltet werden, wobei anhand des Netzplans festgelegt werden muss, welche Segmente durch weitere Detektionssysteme geschützt werden müssen. insb. Übergänge zwischen internen und externen Netzen müssen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

- **Protokollierungsinfrastruktur:** Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse. Die Auswertung auf Auffälligkeiten sämtlicher Ereignismeldungen muss regelmäßig erfolgen. Zusätzlich sind die Signaturen der jeweiligen Systeme stets auf dem aktuellen Stand zu halten.

- **Auswertung von Informationen aus externen Quellen:** Externe, zuverlässige Quellen müssen genutzt und ausgewertet werden. Es ist sicherzustellen, dass den relevanten Mitarbeitern die Meldungen aus den externen Quellen auch vorliegen, so dass alle eingehenden Informationen dahingehend bewertet werden können, ob sie relevant für das Unternehmen sind und ob sich daraus ggf. ein Sicherheitsvorfall ergibt, der gemeldet/weiterverfolgt werden muss.

- **Auswertung der Protokolldaten durch spezialisiertes Personal:** Einerseits muss eine spezielle Beauftragung zur Auswertung der Protokolldaten vorliegen, andererseits muss der mit der Auswertung von Protokolldaten verantwortliche Personen-

kreis benannt werden. Dieser Personenkreis muss für die Thematik-Auswertung von Protokoll- und Protokollierungsdaten verantwortlich sein.

- **Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen:** Es müssen sowohl zentrale Komponenten eingesetzt werden als auch zentrale automatisierte Analysen, „um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen (BSI, Orientierungshilfe, 2022, S. 11)." Die Protokollierungsdaten müssen lückenlos, einsehbar und auswertbar sein, kontinuierlich ausgewertet werden und bei Überschreitung definierter Schwellwerte, automatisch alarmieren. Das zuständige Personal muss sicherstellen, dass bei einem Alarm nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. Die definierten Parameter in der Analyse sind laufend auf Aktualität zu prüfen und anzupassen. Zusätzlich sind „bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch (BSI, Orientierungshilfe, 2022, S. 11)" zu untersuchen.

Zudem ist sicherzustellen, dass laufend Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten und u. a. Meldungen von Hard- und Softwareherstellern eingeholt werden, um die Vollständigkeit möglicher Schwachstellen identifizieren zu können. Dementsprechend sind die Detektionssysteme regelmäßig zu überprüfen und anzupassen. Die SRE müssen überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Darüber hinaus müssen auf Basis der gewonnenen Erkenntnisse Detektionsmechanismen nachjustiert werden.

Zusätzlich sind die Muss-Basisanforderungen des Bausteins „DER.1 Detektion von sicherheitsrelevanten Ereignissen" zu berücksichtigen. Dies bedeutet:

- **Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen (DER.1.A1):** Analog der Sicherheitsrichtlinie für die Protokollierung, ist eine spezifische Richtlinie für die Detektion zu erstellen, in der beschrieben ist, wie die Detektion geplant, aufgebaut und betrieben werden kann. Die Richtlinie, die allen verantwortlichen Mitarbeitenden bekannt gemacht werden muss, ist regelmäßig auf Aktualität zu prüfen, Änderungen mit dem ISB abzustimmen und zu dokumentieren. Ebenso müssen die Ergebnisse dokumentiert werden.

- **Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokolldaten (DER.1.A2):** Die jeweils geltenden Bundes- und Landesdatenschutzbestimmungen, weitere, relevante gesetzliche Bestimmungen (wie das Telemediengesetz (TMG) müssen eingehalten sowie Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden.

- **Festlegung von Meldewegen für sicherheitsrelevante Ereignisse (DER.1.A3):** Es muss ein Melde- und Alarmierungsplan definiert und dokumentiert werden, aus dem hervorgeht, welche Stellen wann zu informieren sind und wie die Personen der Stellen erreicht werden können. Dieser muss den Mitarbeitenden ausgedruckt vorliegen. Je nach Kritikalität der Sicherheitsereignisses, sind unterschiedliche Kommunikationswege zu wählen. Die involvierten Personen müssen über ihre Aufgaben informiert sowie alle Schritte des Prozesses dokumentiert sein.

- **Sensibilisierung der Mitarbeiter (DER.1.A.44):** Zur Sensibilisierung sind regelmäßig Schulungen durchzuführen, insb. dahingehend, dass Ereignismeldungen direkt an das Incident Management verpflichtend zu melden sind.

- **Einsatz von mitgelieferten Systemfunktionen zur Detektion (DER.1.A.5)** in Verbindung damit, dass geprüft werden muss, ob zusätzliche Schadcodescanner auf zentralen IT-Systemen installiert werden sollen.

Reaktion

Folgende zentrale Anforderung gemäß SzA muss erfüllt sein:

„Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren. In Netzen, wo die kritische Dienstleistung durch die Umsetzung nicht gefährdet wird, MUSS es möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden. Sollte eine automatische Reaktion nicht möglich sein, MUSS über manuelle Prozesse sichergestellt werden, dass der mögliche Sicherheitsvorfall unterbunden wird. Der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion, bzw. dem Eingriff in den Datenstrom MUSS schlüssig begründet sein.

Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen MÜSSEN behandelt werden. Bei Störungen und Sicherheitsvorfällen insb. im vermeintlichen Zusammenhang mit Angriffen MUSS überprüft werden, ob diese den Kriterien der Meldepflicht nach § 8b Absatz 3 BSIG bzw. §11 Absatz 1c EnWG entsprechen und eine Meldung an das BSI notwendig ist" (BSI, Orientierungshilfe, 2022, S.14).

Zentraler Baustein als Mindestanforderung nach BSI ist DER.2.1: Behandlung von Sicherheitsvorfällen. Die spezifischen Anforderungen sind somit über das Vorfallsmanagement sicherzustellen – dazu gehört neben der Meldung von Vorfällen, die die kritische Infrastruktur betreffen, an die Behörden, auch die Meldung von entsprechenden Sicherheitsvorfällen, die im Zusammenhang mit Angriffen stehen. Festgestellte Vorfälle aus Sicherheitsangriffen müssen behandelt werden. Dabei muss auch sichergestellt werden, dass Maßnahmen, die allein automatisiert ergriffen werden, nicht die kritische Infrastruktur beeinträchtigen dürfen.

Gemäß DER.2.1 gilt zudem:

- **Eindeutige Definition eines Sicherheitsvorfalls (DER.2.1.A.1),** der allen an der Behandlung von Sicherheitsvorfällen beteiligten Mitarbeitenden bekannt sein muss sowie Abgrenzung zu einer Störung im Tagesbetrieb.

- **Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen (DER.2.1.A2):** Dazu gehört, dass Zweck und Ziel sowie Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen definiert werden, es zielgruppenorientierte Handlungsanweisungen gibt,

die Richtlinie von der Geschäftsführung verabschiedet und allen Mitarbeitenden bekannt gemacht sowie in regelmäßigen Abständen auf Aktualität überprüft wird.

- **Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen (DER.2.1.A3):** Dies besagt insb., dass eindeutige Verant-wortlichkeiten definiert, Aufgaben und Kompetenzen für alle Mitarbeitenden festgelegt und die zentralen Ansprechpartner allen Mitarbeitenden bekannt gemacht wurden. Es muss auch geregelt sein, wer die mögliche Entscheidung für eine forensische Untersuchung trifft, nach welchen Kriterien diese vorgenommen wird und wann sie erfolgen soll.

- **Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen (DER.2.1.A4):** Dies inkludiert auch die Prüfung dahingehend, ob alle internen und externen Stellen unmittelbar informiert werden, der Datenschutz sowie ggf. Betriebs- und Personalrat sowie Mitarbeitende aus dem Rechtsbereich hinzugezogen werden müssen und die übergeordneten Meldepflichten für Behörden und regulierte Branchen berücksichtigt sind. Die Kontaktinformationen müssen immer aktuell und leicht zugänglich sein.

- **Behebung von Sicherheitsvorfällen (DER.2.1.A5):** Es muss eine dokumentierte Ursachenanalyse durchgeführt werden auf Basis derer die korrekte Maßnahme zur Behebung ausgewählt werden kann, die nach Freigabe durch den Leiter IT-Betrieb umgesetzt wird. Dazu muss sowohl ein interner/externer Kommunikationsplan sowie eine Liste interner und externer Sicherheitsexperten vorhanden sein. Es müssen sichere Kommunikationsverfahren mit diesen internen und externen Stellen etabliert werden.

- **Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen (DER.2.1.A6):** Im ersten Schritt müssen die betroffenen Komponenten isoliert und somit vom Netz getrennt werden. Darauf aufbauend müssen Daten zur Ursachenanalyse gesichert und auf allen betroffenen Komponenten die Systeme und Applikationen geprüft werden. Die Originaldaten müssen von schreibgeschützten Datenträgern wieder eingespielt werden. Es müssen alle sicherheitsrelevanten Konfigurationen und Patches mit aufgespielt werden, wobei sicherzustellen ist, dass die eingespielten Datensätze nicht vom Sicherheitsvorfall betroffen waren. Nach einem Angriff müssen alle Zugangsdaten auf den betroffenen Komponenten geändert werden, bevor sie wieder in Betrieb genommen werden.

Ausschließlich automatisiert ergriffene Maßnahmen dürfen nicht zu einer relevanten Beeinträchtigung der kritischen Infrastruktur führen.

„Exkurs": Auswirkungen sowie Anpassungen im § 8a für die Energieversorgungsunternehmen

Neben KRITIS-Betreibern sind durch die Anpassung des Energiewirtschaftsgesetzes (EnWG) auch Betreiber von Energieversorgungsnetzen dazu verpflichtet „…in ihren informationstechnischen Systemen, Komponenten oder Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind, in angemessener Weise Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dabei soll der Stand der Technik eingehalten werden. Der Einsatz von Systemen zur Angriffserkennung ist angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung des betroffenen Energieversorgungsnetzes oder der betroffenen Energieanlage steht" (IT-Sicherheitsgesetz 2.0, BGBl. I 2021 vom 27.5.2021, S. 1137).

Ein Großteil der Energieversorgungsunternehmen ist bereits nach der ISO/IEC 27001:2017 zertifiziert, um den Anforderungen des IT-Sicherheitskatalogs gemäß § 11 Abs. 1a EnWG nachzukommen. Wie eingangs erwähnt, sind durch die Anpassungen im IT-SiG 2.0 nicht nur Betreiber kritischer Infrastrukturen betroffen. Dies hatte auch Auswirkungen auf weitere Gesetze, wie das EnWG. Im Rahmen dessen wurde definiert, dass SzA einzusetzen sind. Dies hat Auswirkungen dahingehend, da die SzA die Kommunikationstechnik möglichst umfassend schützen sollte, dass insb. die Netzleittechnik (zumeist zentraler Bestandteil des Geltungsbereichs beim IT-Sicherheitskatalog) und Fernwirktechnik betroffen sein werden.

Betreiber von Energieversorgungsnetzen und Energieanlagen, die gemäß § 10 Abs. 1 BSIG als KRITIS eingestuft werden, haben nach § 11 Abs. 1f EnWG dem BSI erstmalig spätestens am 01.05.2023 sowie im Anschluss im Turnus von zwei Jahren die Erfüllung der Anforderungen nach § 11 Abs. 1e EnWG nachzuweisen.

Reifegradmodell zur Bewertung des Grades der Umsetzung

Beim BSI müssen alle zwei Jahre Nachweise zur Umsetzung gemäß § 8a Absatz 3 BSIG eingereicht werden. Dabei ist zwingend zu beachten, dass Nachweise, die dem BSI ab dem 01.05.2023 vorgelegt werden, auch Aussagen zur Umsetzung des § 8a Absatz 1a BSIG, also zum Einsatz von Angriffserkennungssystemen, enthalten müssen. Für die Bewertung setzt das BSI analog der bereits bekannten Einschätzung zum ISMS und BCMS aus dem Nachweisdokument P, auf ein Reifegradmodell. Folgende Reifegrade sind vorgesehen:

- „0: Es sind bisher keine Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Anforderungen.

- 1: Es bestehen Planungen zur Umsetzung von Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.

- 2: In allen Bereichen wurde mit der Umsetzung von Anforderungen begonnen. Es sind noch nicht alle Muss-Anforderungen umgesetzt worden.

- 3: Alle Muss-Anforderungen wurden für alle Bereiche umgesetzt. Idealerweise wurden Sollte-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

- 4: Alle Muss-Anforderungen wurden für alle Bereiche umgesetzt. Alle Sollte-Anforderungen wurden umgesetzt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

- 5: Alle Muss-Anforderungen wurden für alle Bereiche umgesetzt. Alle Sollte-Anforderungen und Kann-Anforderungen wurden für alle Bereiche umgesetzt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse / Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert (BSI, Orientierungshilfe, 2022, S.13)."

Das BSI legt allerdings auch dar, dass – vor dem Hintergrund der Einführung von SzA – im ersten Nachweiszyklus ein Reifegrad der Stufe 3 ausreichend ist, langfristig allerdings mindestens die Stufe 4 erreicht werden müsste. Abweichungen nach unten müssten begründet werden.

Nachweiserfüllung

Die Erfüllung von § 8a Abs. 1a BSIG (SzA) ist – ab dem 01.05.2023 – gemeinsam mit dem Nachweis nach § 8a Abs. 1 BSIG (grds. Anforderung zur Erfüllung für KRITIS-Betreiber) zu erbringen. Ab 01.05.2023 muss ein Nachweis nach § 8a Abs. 3 BSIG auch die Ergebnisse der Prüfung SzA enthalten, inklusive der aufgedeckten Sicherheitsmängel. Entsprechende Nachweisformulare werden durch das BSI angepasst bzw. für Betreiber von Energieversorgungsnetzen und Energieanlagen neue Formulare erstellt. Betreiber von Energieversorgungsnetzen und solchen Energieanlagen, die nach der Rechtsverordnung gemäß § 10 Abs. 1 BSIG als Kritische Infrastruktur gelten, haben unabhängig vom nächsten fälligen Nachweis gemäß § 11 Abs. 1f EnWG dem BSI bereits am 01.05.2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nach § 11 Abs. 1e EnWG nachzuweisen.

Sinnvolle nächste Schritte

Unternehmen, die noch keine Maßnahmen zur SzA-Anforderungserfüllung eingeleitet haben, sollten im ersten Schritt eine Risikobetrachtung durchführen. Es gibt spezifische Rahmenbedingungen sowie insb. auch branchenspezifische Anforderungen, die in der Orientierungshilfe selbst nicht spezifiziert werden. Achten Sie im ersten Schritt auf den zu **betrachtenden Scope**. KRITIS-Unternehmen kennen die relevanten Systeme ihrer kritischen Infrastruktur. Bei der Einführung von SzA macht es aber ggf. durchaus Sinn, den bereits bekannten Scope zu erweitern und eine ganzheitliche Betrachtung mehrerer oder aller Systeme umzusetzen. Ergänzend müssen auch **personelle sowie organisatorische Voraussetzungen** geschaffen und implementiert werden, da insb. auch die Auswertung der Sicherheitsvorfälle sowie der rein operative Betrieb sichergestellt werden muss. Ebenso hängt es davon ab, für **welche Art von SzA** sich entschieden wird. Handelt es sich bspw. um ein System, welches eine Überwachung / Analyse in Echtzeit vornimmt oder um eines, welches dieses zeitversetzt durchführt und daher im ersten Schritt Daten sammelt. Systemseitig gibt es die verschiedensten Möglichkeiten zur Implementierung, wobei nicht alle vollumfänglich die Anforderung erfüllen, so beispielsweise:

- IDS (Intrusion Detection System): System zur Erkennung von Angriffen ohne Abwehr. Zumeist konzentriert sich dies auf den ein- und ausgehenden Internetverkehr.

- IPS (Intrusion Prevention System): System zur Erkennung von Angriffen mit automatischen Abwehrmaßnahmen.

- SIEM (Security Information and Event Management): Ein SIEM sammelt, analysiert, bewertet und klassifiziert Daten aus den verschiedensten Quellen, um Anomalien festzustellen. Im Gegensatz z. B. zu einem IDS, können in einem SIEM durch den Benutzer auch vorbeugende Maßnahmen ergriffen werden.

- SOC (Security Operations Center): Ein SOC geht über das SIEM hinaus und ist eine Zusammenstellung aus Menschen, Prozessen und Systemen, um sich mit den Vorfällen/Sicherheitsereignissen, die aus dem SIEM gemeldet werden, zu befassen.

- SOAR (Security Orchestration, Automation and Response): Ein SOAR hat grundsätzlich die identische Funktionalität wie ein SIEM, geht allerdings dahingehend noch darüber hinaus, dass ein SOAR bspw. zusätzliche Informationen aus externen Feeds bzw. allgemeinen Quellen von Drittanbietern heranzieht, um ein ganzheitliches Bild der Sicherheitslandschaft des Netzwerks, innen wie außen, zu erhalten. In einem SOAR ist es bspw. möglich, spezifische Untersuchungsphasen zu erstellen, die auf Basis eines Alarms verfolgt werden.

Bereits nach Veröffentlichung des IT-SiG 2.0 wurde auf die Frage zur Erfüllung eines SzAs zumeist geantwortet, dass idealerweise mindestens ein SIEM zu implementieren ist. Mit der Orientierungshilfe wurden nun durch das BSI konkret Anforderungen definiert, welche zu erfüllen sind.

Implementierung ISMS

Darüber hinaus empfiehlt es sich, kurz-, mittel- und langfristig die SzA in das bestehende ISMS des Unternehmens zu implementieren. Grundlage kann die internationale Norm ISO/IEC 27001 sein, welche durch die neue ISO/IEC 27001:2022 bzw. insb. ISO/IEC 27002:2022 auch einen Fokus auf die technischen Kontrollen / Maßnahmen hat. Einige der in der Orientierungshilfe aufgeführten Aspekte können über bestehende Prozesse in einem ISMS abgedeckt werden – beginnend bei der Risikoanalyse, über das Schwachstellenmanagement sowie Netzwerksicherheit bis hin zum Vorfallmanagement/Information Security Incident Management Prozess.

Ausblick

Wir empfehlen die unterschiedlichen Interessensgruppen – bspw. Betriebsrat und Datenschutz – frühzeitig bei der Implementierung und Umsetzung mit einzubeziehen. Der zentrale Faktor wird allerdings der Faktor „Zeit" sein – bis zur notwendigen Umsetzung ist es nur noch etwas mehr als ein halbes Jahr. Sofern noch nicht begonnen wurde, sollte daher umso schneller in die Planungsphase eingestiegen werden.

Eine aktuelle, vollständige Übersicht aller Anforderungen komprimiert zusammengefasst finden Sie hier:

IMPRESSUM

Herausgeber:
Ebner Stolz GmbH & Co. KG
www.ebnerstolz.de

Ludwig-Erhard-Straße 1, 20459 Hamburg
Tel. +49 40 37097-0

Holzmarkt 1, 50676 Köln
Tel. +49 221 20643-0

Kronenstraße 30, 70174 Stuttgart
Tel. +49 711 2049-0

Redaktion:
Marc Alexander Luge, Tel. +49 211 91332-663
Hanna Pentzek, Tel. +49 211 91332-664
Dr. Ulrike Höreth, Tel. +49 711 2049-1371
novus.it@ebnerstolz.de

Wir legen großen Wert auf Gleichbehandlung. Aus Gründen der besseren Lesbarkeit verzichten wir jedoch auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers. Im Sinne der Gleichbehandlung gelten entsprechende Begriffe grundsätzlich für alle Geschlechter. Die verkürzte Sprachform beinhaltet also keine Wertung, sondern hat lediglich redaktionelle Gründe.

Fotonachweis:
©www.gettyimages.com