1. AUSGABE 2021

EBNER STOLZ

novus

INFORMATIONSTECHNOLOGIE

Post-COVID und die neue (Prüfungs-)Realität

Elektronische Signaturen – Digitalisierung von Zeichnungsprozessen im Geschäftsalltag

Informationssicherheit: Zertifizierung durch die ESecurity-CERT GmbH

POST COVID ist ANTE COVID?

COVID-19 begleitet uns weiterhin – auch wenn für viele Unternehmen so langsam die post-COVID-Zeit beginnt, nachdem man sich mehr als ein Jahr quasi in einer Art „Notfallprozess" befand. Dies bedeutet bspw. für uns als Geschäftsbereich IT-Revision (GBIT), dass wieder häufiger Termine vor Ort durchgeführt werden können, auch wenn sicherlich sowohl Sie als auch wir festgestellt haben, dass eine Remote-Prüfung bis zu einem gewissen Grade möglich und zum Teil sehr effizient ist. Deshalb wird sich auch für uns Prüfer einiges ändern und die post-COVID-Zeit wird höchstwahrscheinlich eine andere als die ante-COVID-Zeit.

Das letzte halbe Jahr hat einige interessante Themen mit sich gebracht, über die wir Sie informieren möchten. Im Rahmen des Aufsichtsrechts wird die Ende des letzten Jahres veröffentlichte Konsultationsfassung der BAIT sicherlich Auswirkungen auf die KAIT und VAIT nach sich ziehen. Wir beleuchten dazu den Notfallmanagement-Prozess aus Sicht der neuen Konsultationsfassung.

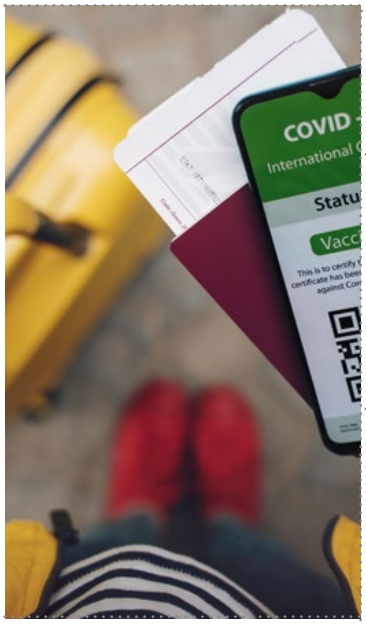
Später als erwartet, ist in diesem Jahr das „lang ersehnte" IT-Sicherheitsgesetz 2.0 in Kraft getreten. Nach dem Beschluss des Bundestages am 23.04.2021, der Zustimmung durch den Bundesrat sowie der Veröffentlichung am 27.05.2021 im Bundesgesetzblatt war dies konkret am 28.05.2021 der Fall. Mit dem IT-Sicherheitsgesetz verbunden sind eine Vielzahl an Änderungen und Anpassungen, die noch folgen werden, wie etwa seitens der Bundesnetzagentur für den IT-Sicherheitskatalog gemäß §11 Energiewirtschaftsgesetz (EnWG). Insb. über die wesentlichen Änderungen, wie die erneute Erhöhung der Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI), möchten wir Sie informieren.

Erfreulicherweise hat die ESecurity-CERT GmbH (ESCERT) als unabhängige Zertifizierungsstelle die Akkreditierung für die DIN EN ISO/IEC 27001:2017-06 erfolgreich abschließen können, sodass diese nun berichtigt ist, entsprechende Zertifizierungsprüfungen durchzuführen. Gerne möchten wir Ihnen die ESCERT kurz vorstellen.

Weitere Themen im Bereich der IT-Sicherheit betreffen Änderungen im IT-Sicherheitskatalog. Bis zum 30.06.2021 hätte die Bundesnetzagentur die Zertifizierungsstelle benennen müssen, mit der das Audit nach IT-Sicherheitskatalog gemäß §11 Abs. 1b EnWG durchgeführt werden soll. Da auch COVID-19-bedingt noch keine Zertifizierungsstelle die Akkreditierung besitzt, um dies durchführen zu können, wurde die Frist verlängert.

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

Ihr GBIT



Informatiker in der Wirtschaftsprüfung: Ebner Stolz

Warum Datenwerkzeuge weiterentwickelt und geschärft werden müssen, um die neuen Geschäftsmodelle bei Mandanten prüfen zu können, erklärt Interviewpartner Holger Klindtworth. Er ist seit 25 Jahren im Beruf, seit 10 Jahren bei Ebner Stolz und bezeichnet sich selbst als „IT-Prüfer aus Leidenschaft".

Holger Klindtworth ist Partner bei Ebner Stolz sowie Mitglied im Fachausschuss IT des IDW. Lange Jahre war er zudem Vorstand im Berufsverband ISACA. Herr Klindtworth besitzt den Expertenstatus beim Bundesverband der mittelständischen Wirtschaft und wird häufig als Gutachter in Fragestellungen der Informationsverarbeitung eingesetzt. Er hat Lehraufträge an mehreren Hochschulen in Deutschland, aktuell an der HAW Hamburg im Fachbereich Informatik, und ist Autor verschiedener Bücher und zahlreicher Publikationen.

Herr Klindtworth, in Ihrem Geschäftsbereich IT-Revision beschäftigen Sie sich mit den Herausforderungen, welche die Digitalisierung für Unternehmen und ihre Geschäftsmodelle mit sich bringt. Mit welchen Fragestellungen werden Sie konfrontiert?

Die Fragestellungen sind sehr vielfältig, lassen sich aber in drei wesentliche Klassen einteilen: Zum einen sind es die Fragestellungen, die sich aus den Veränderungen der Geschäftsmodelle und -prozesse durch die Digitalisierung ergeben, wie z. B. der Einsatz von Kundenportalen mit automatisierter Bestellabwicklung, die Anpassung einer Preisgestaltung auf Basis von „Echtzeitabverkaufsdaten" oder eine KI-gestützte Buchungskontierung.

Die zweite Kategorie ergibt sich aus den Veränderungen der Basis allen digitalen Seins – der technischen (IT-)Infrastruktur, wie z. B. Cloud-Lösungen.

Die dritte, und bei weitem nicht die unwichtigste Kategorie, sind Fragestellungen rund um die neuen Anforderungen an den Menschen, wie etwa „Was sind die notwendigen Qualifikationen der Fachkräfte in der Zukunft und für die Firmen? Wie kommt man an diese Fachkräfte?"

Um uns Ihrer Arbeit einmal über zwei konkrete Aufgabenstellungen zu nähern: Wie gehen Sie vor bei der Prüfung von IT-Sicherheit oder IT-Compliance und was muss man dafür mitbringen?

Technisches Know-how ist eine zwingend notwendige Voraussetzung für gute Prüfungsarbeit. Darüber hinaus ist aber ein schnelles und umfassendes Verständnis der Gesamtsituation dringend erforderlich. Dazu gehören das Wissen über den Mandant, dessen Geschäftsmodelle und das Marktumfeld, aber natürlich auch das Verständnis der rechtlichen und regulatorischen Rahmenbedingungen und ihre Bedeutung im konkreten Fall.

Wie man bei einer Prüfung von IT-Sicherheit bzw. IT-Compliance genau vorgeht, lässt sich dagegen weniger einfach beantworten. Auch wenn sich Problemfälle ähneln, ist jede Prüfung einzigartig. Wesentlich ist in jedem Fall ein gut gefüllter, auch zum Teil digitaler Werkzeugkasten, verbunden mit viel Erfahrung und ständiger Weiterbildung.

Um mit diesem zu arbeiten, suchen Sie Software Developer. Welche Herausforderungen erwarten diese?

Tatsächlich ähnelt die interne Herausforderung in der Entwicklung sehr den Herausforderungen in unseren externen Projekten. Es ist vor allem die Vielfalt, die unsere Aufgaben auszeichnet. Durch die Breite unseres Angebots gegenüber unseren Mandanten wächst natürlich auch der Bedarf an unterschiedlicher Softwareunterstützung. Vom Umsatzsteuercockpit über unser umfangreiches Datawarehouse mit Prüfungsdaten bis hin zur Vertragsanalyse mit KI im Rechtsbereich spannt sich hier der Bogen.

Passiert es, dass Kunden von Ihnen auch konkrete Implementierungen erwarten?

Unsere Softwareentwickler sind unsere Werkzeugmacher. Sie versorgen uns vor allem mit den Werkzeugen, die wir in unseren aktuellen und zukünftigen Projekten benötigen. Aber natürlich gefällt dem ein oder anderen Mandanten auch eines unserer glänzenden Werkzeuge und sie möchten diese für ihre eigenen Zwecke nutzen. Dann wird man sich schon einig. Aber das ist eher die Ausnahme, wir sind – noch – kein Softwarehaus.

Setzen Ihre Kunden auf Präsenz vor Ort?

In Sachen Reisetätigkeit haben sich die Zeiten generell durch die Corona-Pandemie geändert. Wir haben schon vor COVID-19 zum Teil mit Remote-Prüfungen gearbeitet. Das war zu Beginn der Pandemie ein echter Erfahrungsvorsprung und einer der Gründe, warum wir so erfolgreich durch die Corona-Krise gekommen sind. Allerdings haben die Mandanten in der Vergangenheit eher eine Vor-Ort-Prüfung von uns erwartet. Das hat sich mittlerweile komplett gedreht und wird auch nach der Pandemie weitgehend Bestand haben. Hatten wir früher Reiseanteile von ca. 50 %, rechne ich in Zukunft mit maximal 10 bis 20 %.

Ebner Stolz konzentriert sich stark auf die Champions des Mittelstandes. Ist dort der Anpassungsdruck der Digitalisierung nicht noch größer als bei internationalen Industriekonzernen?

Erst einmal ist für uns jeder Mittelständler ein Champion! Was den Mittelstand auszeichnet, ist die Vielfalt, die hohe Dynamik und der unternehmerische Spirit. Dadurch besteht bei vielen Mittelständlern eine richtiggehende Aufbruchstimmung und das macht natürlich einen großen Reiz für uns aus, die Unternehmen auf Augenhöhe zu begleiten und als echte Unterstützung und Teil der Mission wahrgenommen zu werden.

Von Berufseinsteigern erwarten Sie bei manchen Ihrer Stellenausschreibungen ausgeprägte IT-Affinität. Warum ist diese wichtig in der Wirtschaftsprüfung?

Die Informationsverarbeitung bildet die Grundlage digitaler Geschäftsprozesse und damit auch die Grundlage sowohl der Bilanz als auch der Steuererklärung. In unserer Branche ist inzwischen absolutes Teamwork zwischen Wirtschaftsprüfern, Steuerberatern und sogar Rechtsanwälten angesagt. So wie wir von unseren IT-Revisoren betriebswirtschaftliches, steuerliches und zum Teil rechtliches Basiswissen erwarten, erwarten wir von den anderen Bereichen IT-Kenntnisse. Man muss die Probleme insgesamt verstehen, um sie dann im Team zu lösen.

Gerade wenn man als Informatiker noch keine Berührungspunkte mit Prüfung hatte, ist eine fundierte Weiterbildung elementar. Welche Angebote haben Sie für Ihre neuen Mitarbeiter?

In der IT-Revision werden vier wesentliche Kenntnisbereiche erwartet. Das sind zunächst die Themen Informationstechnologie, Betriebswirtschaft und Prüfungswesen. Der vierte Kenntnisbereich betrifft den Umgang mit Mandanten. Absolventen oder andere Bewerber mit eher geringer Berufserfahrung haben je nach Ausbildung in der Regel in einem oder mehreren der Bereiche noch Kenntnislücken. Dies ist eine Situation, die wir sehr gut und seit langem kennen und auch erwarten! Deshalb stecken wir sehr viel Zeit, Geld und Energie in die ergänzende Ausbildung unserer Mitarbeiter. Dies geschieht im Rahmen unserer Ebner Stolz Akademie und einem individuellen Förder- und Ausbildungsprogramm für jeden Mitarbeiter.

Welches Konzept steht dahinter?

Das Konzept der Akademie basiert zum einen auf einer breiten fachlichen Ausbildung in den klassischen Themen rund um Prüfung und Beratung, zum anderen hat die Akademie auch die persönliche Weiterentwicklung, z. B. über Seminare zur Gesprächsführung, zum Zeitmanagement oder zur Rolle der Führungskraft etc., im Blick. Unsere Ausrichtung liegt auf langfristigen Arbeitsbeziehungen zu unseren Mitarbeitern. Unser Ausbildungsprogramm läuft nicht nur wenige Wochen, sondern erstreckt sich konzeptionell über mehrere Jahre hinweg. Die Ausbildungsmodule bauen aufeinander auf und werden durch individuelle Förder- und Ausbildungsmaßnahmen ergänzt. Gerade diese Kombination aus Langfristigkeit, Kontinuität und Individualität kommt bei unseren Mitarbeitern sehr gut an.

Gibt es spezielle Möglichkeiten für Bachelor-Absolventen der Informatik, die mit einem berufsbegleitenden Masterstudium ihr Profil stärken möchten?

Ein hoher Grad an Individualität ist Bestandteil unserer Unternehmens-DNA. Deshalb unterstützen wir spezielle berufsbegleitenden Konzepte, sei es ein Masterstudium, eine Doktorarbeit oder ein thematisch naheliegendes Zweitstudium. Für all das entwickeln wir gemeinsam mit dem Mitarbeiter eine Lösung, sei es durch abweichende Arbeitszeitmodelle oder andere Formen der Unterstützung. Aber unsere Flexibilität endet nicht beim Thema Ausbildung. Da wir aus einer langfristigen Perspektive kommen, wissen wir, dass Mitarbeiter auch besondere Lebensphasen nach der Ausbildung haben, in denen Bedarf nach flexiblen Regelungen besteht, etwa wenn Kinder kommen und noch klein sind oder aber nahestehende Personen gepflegt werden müssen. Auch hierfür haben wir passende Modelle.

Was denken Sie, an welchen Stellen die Wirtschaftsprüfung in den kommenden Jahren den größten Digitalisierungsschub bekommen wird und welches sind die Treiber dieser Entwicklung?

Wie heißt es so schön: „Daten sind das neue Gold oder auch Öl" – das macht natürlich auch vor der Wirtschaftsprüfung nicht Halt. Es gilt, die eigenen Datenwerkzeuge weiterzuentwickeln und zu schärfen, weil die neuen Geschäftsmodelle beim Mandanten sonst nicht mehr prüfbar sind. Hoher Integrationsgrad über verschiedene Plattformen und Massentransaktionen – das ist die große Herausforderung und der stellt sich die Branche im Allgemeinen und Ebner Stolz im Besonderen.

Für welche Digital Talents mit ausgeprägtem IT-Know-how ist Ebner Stolz der passende erste Arbeitgeber und welches Versprechen können Sie denjenigen machen, die bei Ihnen ihre Karriere starten?

Für diejenigen, die sich auch in Zukunft ständig persönlich und fachlich weiterentwickeln wollen, die kreativ sind, über den Tellerrand hinausschauen wollen und das große Ganze nicht aus dem Blick lassen. Für alle, die Vielfalt in der täglichen Aufgabenstellung lieben, ist Ebner Stolz der richtige Arbeitgeber. Ein Versprechen fällt mir insofern besonders leicht: Es wird niemals langweilig!

Holger Klindtworth
Partner bei Ebner Stolz in Hamburg

Post-COVID und die neue (Prüfungs-)Realität

Frei nach dem Motto „wir können, wenn wir müssen" wurden sämtliche Prüfungen seit dem Frühjahr 2020 erfolgreich im Remote-Ansatz durchgeführt. Unter dem Deckmantel des Notfallprozesses konnten bereits laufende sowie geplante Prüfungen aber auch Neumandate im Remote-Ansatz erfolgen. Die anfängliche Skepsis, sowohl bei uns als auch bei den Mandanten, wurde durch gemeinsame Kraftanstrengungen durch die Erkenntnis „geht doch (!)" ersetzt – zumal Remote-Audits vom Grundsatz her keine wirkliche Innovation darstellten.

Nichtsdestotrotz ist es ein Unterschied, ob man Webmeetings aufgrund ihrer Vorteile durchführt, wie Zeit- und Kostenersparnisse oder einer erhöhten Flexibilität, oder ob man schlicht keine andere Wahl hat. Nachteile können nicht ausbleiben, wenn die Notwendigkeit des Abwägens etwaiger Vor- und Nachteile nicht besteht und eine (zielführende) Durchführung unter geänderten Rahmenbedingungen alternativlos ist.

Wenngleich vereinzelte Aspekte für sich genommen ohne Weiteres als überwindbare Hürden wahrgenommen werden, können sich diese unter der Einwirkung des Faktors Zeit überproportional nachteilig auf das Audit auswirken. Dies gilt sowohl aufseiten des Prüfers ebenso wie auf der des Geprüften. Ohnehin sollten die Nachteile des Umstiegs auf das Remote-Audit, der gewissermaßen nach dem Big-Bang-Ansatz erfolgte, vor dem Hintergrund betrachtet werden, dass Audits auch vor der Pandemie schon unter enormem Zeitdruck und eng getaktet erfolgten. Zieht man etwa den seit Beginn der neuerlichen Home-Office-Kultur merklich spürbaren globalen Engpass an Halbleitern als Beispiel heran, wird die Zeit als Schlüsselfaktor greifbar. Unter der Prämisse, dass sämtliche Mitarbeiter bereits über das notwendige technische Verständnis verfügen, die Geräte ortsunabhängig nutzen zu können, steht und fällt die Unternehmung mit der Bereitstellung der erforderlichen Hardware. Insb. für unsere Mandanten, die ihre Mitarbeitenden kurzfristig ins Home-Office beordern mussten, wirkte sich die Knappheit an Halbleitern sowie das Auftun technischer Grenzen besonders negativ aus. Die Konsequenzen für das Remote-Audit sind unverkennbar.

Mit dem Austausch sensibler Daten unter Einhaltung der rechtlichen Rahmenbedingungen, welche insb. die Wahrung von Sicherheit und Vertraulichkeit umfassen, geht die besonnene Wahl eines geeigneten Kollaborations-Tools einher. Ungeachtet der technischen Infrastruktur stellt die Umstellung eines „physischen" Audits auf das Remote-Audit auch eine nicht zu unterschätzende Gewöhnungsphase für alle beteiligten Parteien dar.

Dennoch wissen wir nun einmal mehr „wir können, wenn wir müssen"; aber vielleicht „wollen" wir ja in Zukunft. Ein Perspektivwechsel zeigt, dass sich vorerst nachteilig geglaubte Charakteristika nun als Vorteile herausstellen und sich insb. auch als solche ausschöpfen lassen. Folglich können die gewonnenen Erkenntnisse und Erfahrungen nicht nur als kurz- bis mittelfristige Notwendigkeit gesehen werden. Vielmehr kann aus ihnen ein langfristig erfolgreiches Konzept für Remote-Audits hervorgehen. Die Methodik soll die herkömmliche Prüfung mit physischer Präsenz nicht gänzlich ersetzen, vielmehr diese für alle beteiligten Parteien effizient ergänzen.

Der unfreiwillige Umstieg auf Remote-Auditing bzw. die daraus gewonnen Erfahrungen sollten in künftige Modellüberlegungen einfließen. Viel deutlicher als noch vor 18 Monaten können nun Vor- und Nachteile, sowohl fachlicher als auch persönlicher Natur, abgewogen werden. Die Durchführung von Prüfungen kann nicht zuletzt aufgrund des niedrigeren organisatorischen Aufwands noch flexibler und individueller an die jeweiligen Bedürfnisse der Kunden und Erfordernisse der Prüfungen angepasst werden. Auf die gemachten Erfahrungen und gewonnen Erkenntnisse sollte wohlüberlegt aufgebaut werden.

Das viel propagierte „gemeinsam durch die Krise"-Credo sollten wir nun umwandeln, in ein gemeinsames Gestalten der post-COVID-Zeit und der damit verbundenen Chancen eines neuen Miteinanders (auch) im Prüfungsalltag.

„Wir können, wenn wir wollen" ist heute „Wir wollen, weil wir können"!

BMF – Einjährige Nutzungsdauer bei Computerhardware und Software

Das Bundesfinanzministerium (BMF) hat am 26.02.2021 ein Schreiben zur Nutzungsdauer von Computerhardware und Software veröffentlicht und räumt darin die Möglichkeit einer einjährigen, statt bisher dreijährigen, Nutzungsdauer ein (Az. IV C 3 – S 2190/21/10002 :013). Das Ziel der Neuregelung besteht in der Anpassung der Abschreibung an die tatsächlichen Wertverhältnisse, da infolge des raschen technischen Fortschritts ein immer schnellerer Wandel entsteht. Auch im Sinne der Digitalisierung soll an dieser Stelle durch die Neuregelung eine zusätzliche steuerliche Förderung gewährt werden.

Steuerbilanzielle Auswirkungen

Der Anwendungsbereich des BMF-Schreibens umfasst sowohl Computerhardware als auch Software. Zu Computerhardware gehören nach Auffassung des BMF neben (Desktop- und Notebook-) Computern z. B. auch Desktop-Thin-Clients, mobile Workstations oder Peripherie-Geräte. Die Anwendung der einjährigen Nutzungsdauer bei bestimmten Computern setzt allerdings voraus, dass der Hersteller einer Kennzeichnungspflicht nach der EU-Verordnung Nr. 617/2013 vom 26.06.2013 zur Umsetzung der Ökodesign-Richtlinie 2009/125/EG vom 21.10.2009 unterliegt.

Unter den Begriff der Software fallen sowohl Betriebs- als auch Anwendersoftware zur Dateneingabe und -verarbeitung, was u. a. auch eine ERP-Software oder sonstige Anwendungssoftware zur Unternehmensverwaltung oder Prozesssteuerung umfasst.

Anders als noch im Entwurfsschreiben vom Januar 2021 wird in dem finalen Schreiben nicht mehr ausgeführt, dass die Anschaffungs- bzw. Herstellungskosten infolge der einjährigen Nutzungsdauer im Jahr der Anschaffung bzw. Herstellung vollständig abzuschreiben wären. Da aber eine Verteilung der Anschaffungs- und Herstellungskosten im Wege der Abschreibung nur für Wirtschaftsgüter mit einer Nutzungsdauer von über einem Jahr vorzunehmen ist, könnte es hier dennoch zu einem Sofortabzug der Anschaffungs- und Herstellungskosten kommen (vgl. H 7.4 „Nutzungsdauer" EStH sowie z. B. Schnitter in Frotscher/Geurts, EStG, § 7, Rz. 263).

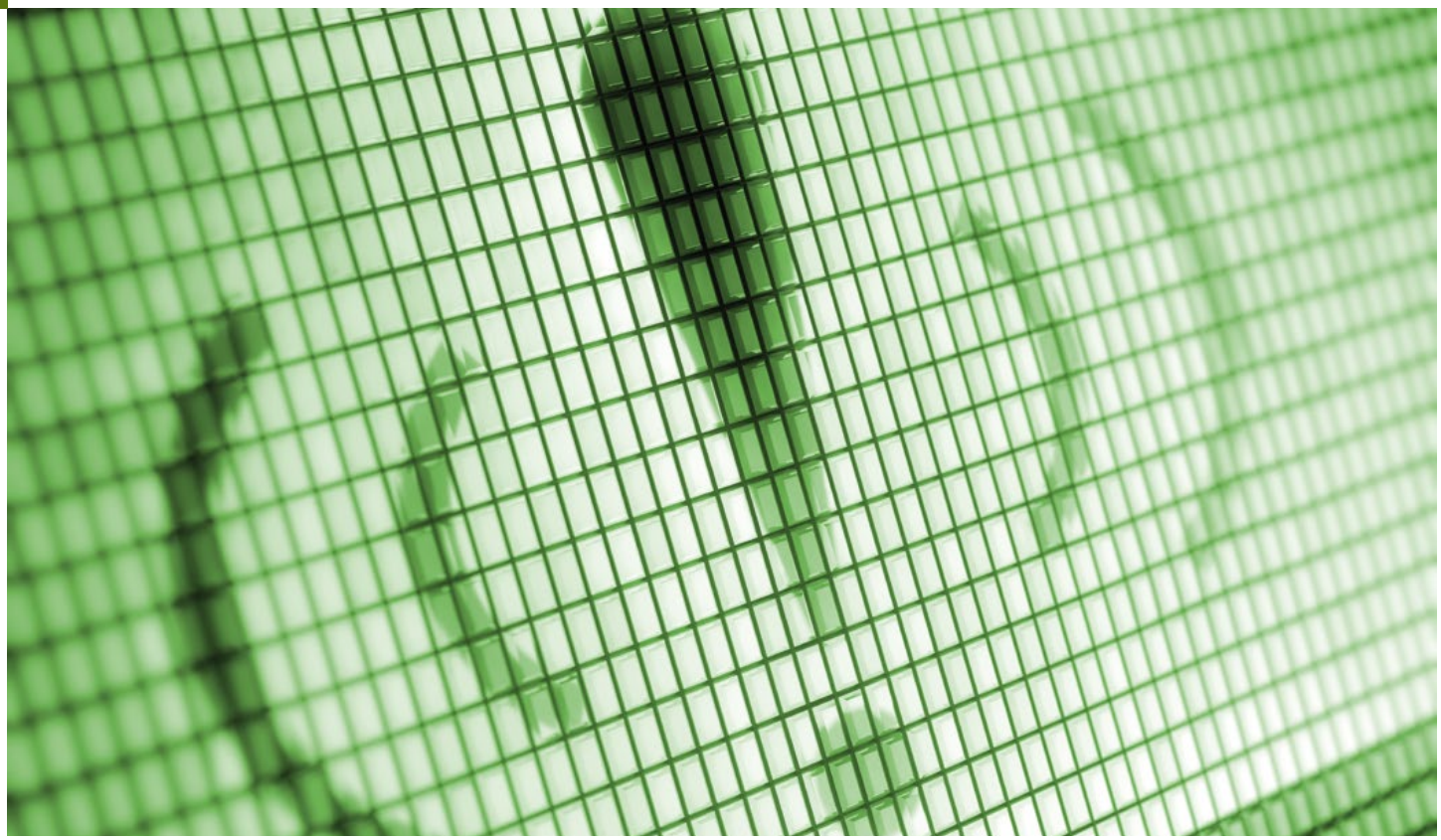
Die Anwendung ist für Geschäftsjahre vorgesehen, die nach dem 31.12.2020 beginnen. Restbuchwerte früher angeschaffter oder hergestellter (digitaler) Wirtschaftsgüter, bei denen bislang eine längere Nutzungsdauer berücksichtigt wurde, können in Gewinnermittlungen nach dem 31.12.2020 vollständig abgeschrieben werden.

Handelsrechtliche Auswirkungen

Das veröffentlichte BMF-Schreiben betrifft die Steuerbilanz und ist demnach nicht auf die Handelsbilanz anzuwenden. Der Fachausschuss Unternehmensberichterstattung (FAB) des IDW stellte in einer außerordentlichen Sitzung im März dieses Jahres zudem klar, dass er die Zugrundelegung einer Nutzungsdauer von nur einem Jahr für die begünstigten digitalen Investitionen für handelsbilanzielle Zwecke regelmäßig als nicht zulässig erachtet.

Eine Verkürzung der Nutzungsdauer von Hard- und Software durch den zunehmenden technologischen Wandel lässt sich nicht bestreiten, allerdings würde eine Sofortabschreibung regelmäßig nicht dem tatsächlichen Nutzungsverlauf dieser Vermögensgegenstände entsprechen.

Die Zugrundelegung einer tatsächlichen betriebsgewöhnlichen Nutzungsdauer von mehr als einem Jahr für Zwecke der Handelsbilanz führt nicht dazu, dass nach dem Grundsatz der Maßgeblichkeit die steuerliche Möglichkeit der Zugrundelegung einer fiktiven betriebsgewöhnlichen Nutzungsdauer von einem Jahr ins Leere läuft. Wird in der Steuerbilanz von der einjährigen Nutzungsdauer Gebrauch gemacht, kommt es folglich zu einer Durchbrechung der Maßgeblichkeit der Handelsbilanz für die Steuerbilanz. Als Resultat aus den unterschiedlichen Wertansätzen ergibt sich (bei isolierter Betrachtung des Sachverhalts) in der Handelsbilanz das Erfordernis des Ausweises passiver latenter Steuern.



Prüfung des IT-Notfallmanagement – (nicht nur) aus Sicht der BAIT

Business Continuity Management bzw. Notfallmanagement stellt viele Unternehmen vor ernsthafte Herausforderungen, da dies grundlegende prozessuale Einschnitte bedeutet sowie konkrete Maßnahmen bedarf, die im gesamten Unternehmen umzusetzen sind. Dafür stellt das Notfallmanagement aber auch die Aufrechterhaltung des Geschäftsbetriebes in Krisensituationen sicher. Eine wesentliche Voraussetzung dafür ist die jederzeitige Verfügbarkeit der IT-Systeme. Aus diesem Grund fordern sowohl u. a. das Institut der Wirtschaftsprüfer e. V. (IDW), das Bundesamt für Sicherheit in der Informationstechnik (BSI), die ISO/IEC 2700x als auch die Mindestanforderungen an das Risikomanagement (MaRisk), Vorkehrungen für einen Notbetrieb zu treffen. Ein Ausfall wesentlicher IT-Anwendungen ohne kompensierende Notfallstrategien und kurzfristige Ausweichmöglichkeit (Anforderung der Bankaufsichtliche Anforderungen an die IT (BAIT)) kann materielle und immaterielle Vermögensschäden nach sich ziehen und stellt einen wesentlichen Mangel der Buchführung dar.

Im Rahmen der Reihe „Notfallkonzept" verweisen wir auf die dreiteilige Reihe in unserem novus IT 2019, Ausgaben 1 bis 3:

- Ausgabe 1/2019: Hintergrund bzw. der Weg hin zu einem Notfallkonzept
- Ausgabe 2/2019: Beschreibung von Maßnahmen zur Aufrechterhaltung des Notfallkonzeptes
- Ausgabe 3/2019: Aufbau eines (IT-) Notfallhandbuches (praxisbezogene Umsetzung).

Die Ausführungen, die sich im Folgenden insb. aus Anforderungen der MaRisk und den BAIT ergeben, können ebenfalls auf Unternehmen übertragen werden, die nicht den bankaufsichtlichen Anforderungen unterworfen sind. Berücksichtigt wird dabei die Konsultationsfassung der BAIT aus 2020. Es ist davon auszugehen, dass diese nach Verabschiedung ebenfalls auf die Konsultationsfassungen der Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT) und Versicherungsaufsichtliche Anforderungen an die IT (VAIT) übertragen werden.

Aufgrund der Bedeutung und der weitreichenden Konsequenzen der zu treffenden Entscheidungen muss der Prozess „Notfallmanagement" von der obersten Leitungsebene der Unternehmen initiiert, gesteuert und kontrolliert werden.

Die Verfahren für den Notbetrieb umfassen organisatorische Regelungen zur Wiederherstellung der Betriebsbereitschaft und reichen von Maßnahmen bei Systemstörungen (Wiederanlaufkonzepte) bis hin zu Konzepten bei einem vollständigen Ausfall des IT-Systems (Katastrophenfall-Konzept).

Weiter sind Notfallhandbücher vorzuhalten und die betroffenen Mitarbeiter in den Maßnahmen zu schulen. Die definierten Maßnahmen haben den Bedürfnissen des Unternehmens zu entsprechen. Ferner sind die Notfalllösungen regelmäßig zu testen und der geordnete Wiederanlauf der einzelnen Systeme in der von der Unternehmensleitung vorgegebenen Zeit sicherzustellen (Testsequenz).

Ergänzend erwähnen die MaRisk das Erfordernis, dass die Notfallkonzepte des Instituts und des Auslagerungsunternehmens aufeinander abzustimmen sind.

Bisher war in den BAIT der Themenkomplex des Notfallbetriebs keinem eigenen Abschnitt zugeordnet. Vielmehr fand der Begriff des Notfallmanagements in den Abschnitten „IT-Strategie" und „Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen" Anwendung. Die Konsultationsfassung aus Oktober 2020 der BAIT enthält nun einen gesonderten Abschnitt zum IT-Notfallmanagement.

Gemäß der BAIT und MaRisk müssen Ziele zum Notfallmanagement definiert und darauf aufbauend ein Notfallmanagementprozess implementiert werden. Für Aktivitäten und Prozesse, bei deren Beeinträchtigung für definierte Zeiträume ein nicht mehr akzeptabler Schaden zu erwarten ist, ist ein Notfallkonzept zu erstellen.

Des Weiteren sind auf Basis des Notfallkonzeptes für diejenigen Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, IT-Notfallpläne auszuarbeiten. Die Wirksamkeit der Pläne ist mindestens jährlich zu überprüfen und das Notfallkonzept gemäß MaRisk anlassbezogen zu aktualisieren. Die Geschäftsleitung ist dazu aufgefordert, sich mindestens quartalsweise- oder anlassbezogen über den Zustand des Notfallmanagements schriftlich berichten zu lassen.

Nach den BAIT besteht darüber hinaus die Anforderung nachzuweisen, dass bei einem Ausfall des Rechenzentrums die zeitkritischen Aktivitäten und Prozesse aus einem ausreichend entfernten Rechenzentrum für eine angemessene Zeit sowie für die Wiederherstellung des IT-Normalbetriebs erbracht werden können.

Der Begriff des Notfallmanagements fordert gemäß dem BSI-Standard „100-4 Notfallmanagement" definierte Leitlinien zum Notfallmanagement, Rollenbeschreibungen mit Aufgaben, Rechten und Pflichten, eine Übersicht über Ressourcen-Anforderungen und deren Bereitstellung sowie Notfallkonzepte nebst Notfallhandbuch (Anleitung zur Bewältigung des Notfalls).

Darüber hinaus stellt der Standard klar, dass das Notfallmanagement einen kontinuierlichen Verbesserungsprozess darstellt, der die Maßnahmen und Konzepte hinterfragt sowie auch die Sensibilisierung und Schulung der Mitarbeiter vorsieht.

Die folgende Aufstellung gibt Ihnen einen Überblick, welche Prüfungsfragen im Rahmen der IT-Revision durch den Jahresabschlussprüfer oder die Interne Revision hinsichtlich des IT-Notfallmanagements relevant sein könnten. Weiterhin bieten sie ergänzend zu den oben genannten Standards, z. B. vom BSI oder aus der Informationssicherheit, eine gute Grundlage für eine Selbsteinschätzung, z. B. zur Prüfungs- oder Zertifizierungsvorbereitung, oder als Unterstützung für eine Reifegradbestimmung.

Ausgewählte Prüfungsfragen zum Notfallmanagement:

- Nimmt die oberste Leitungsebene des Unternehmens eine angemessene Rolle (Initiieren, Steuern und Kontrollieren) im Notfallmanagement ein?
- Ist ein Notfallmanagementprozess, der die Notfallvorsorge, die Notfallbewältigung und die Notfallnachsorge umfasst, definiert?
- Wurde eine Klassifizierung/Kategorisierung der Systeme nach ihrer Wichtigkeit für den Geschäftsbetrieb durchgeführt?
- Ist ein IT-Notfallkonzept sachgerecht umgesetzt und wird dieses kontinuierlich angepasst?
- Sind hier u. a. auch wesentliche IT-Kontakte und Ansprechpartner von IT-Dienstleistern und Lieferanten festgehalten? Sind Verhaltensweisen und Prozesse für (IT-)Notfälle definiert?
- Ist das verantwortliche (IT-)Personal entsprechend geschult und sensibilisiert?
- Wie werden durchgeführte Wiederanlaufprozeduren dokumentiert und ausgewertet?
- Welche IT-Sicherheitsmaßnahmen sind festgelegt?
- Wie werden Sicherheitsvorfälle festgehalten und Maßnahmen aus diesen abgeleitet?

Abgeleitete Fragen aus BAIT und MaRisk

- Welche Ziele des Notfallmanagements wurden definiert? Wurden Schnittstellen zu anderen Bereichen (z. B. Risikomanagement, Informationssicherheitsmanagement) berücksichtigt?
- Wurden zeitkritische Aktivitäten und Prozesse definiert und finden diese Berücksichtigung im Notfallmanagement?
- Welche Regelungen sind für den Notbetrieb und zur Wiederherstellung der Betriebsbereitschaft getroffen? Liegen Wiederanlaufkonzepte für Systemstörungen und den vollständigen Ausfall des IT-Systems (Katastrophenfall-Konzept) vor?
- Werden Notfallhandbücher mit definierten Maßnahmen, die den Bedürfnissen des Instituts entsprechen, vorgehalten?
- Werden die definierten Notfalllösungen regelmäßig getestet, um den anforderungsgerechten Wiederanlauf der einzelnen Systeme sicherzustellen?
- Sind die Notfallkonzepte des Instituts und die der Auslagerungsunternehmen für Auslagerungen und auch sonstigen Fremdbezug aufeinander abgestimmt?
- Können zeitkritische Aktivitäten und Prozesse bei Ausfall eines Rechenzentrums in einem Ausweichrechenzentrum erbracht werden?
- Sind die Leitlinie zum Notfallmanagement, die Notfallkonzepte und -handbücher (Anleitung zur Bewältigung des Notfalls) kommuniziert und zugänglich?
- Unterliegt das Notfallmanagement einem kontinuierlichem Review- und Verbesserungsprozess?

Neue EU-Standardvertragsklauseln für internationale Datentransfers

Die Europäische Kommission hat am 04.07.2021 die finale Version der neuen „EU-Standardvertragsklauseln" für die Übermittlung personenbezogener Daten ins EU-Ausland veröffentlicht. Mit den neuen EU-Standardvertragsklauseln sollen internationale Datentransfers vereinfacht und die Anforderungen der Schrems-II-Entscheidung berücksichtigt werden. Unternehmen sind zur Umsetzung der neuen Vertragsbedingungen verpflichtet und sollten sich rechtzeitig mit den neuen Regelungen vertraut machen. Absolute Rechtssicherheit für internationale Datenübermittlungen können die neuen Standardvertragsklauseln aber nicht bieten.

Hintergrund

Die EU-Standardvertragsklauseln sind das in der Praxis mit Abstand am häufigsten verwendete Instrument für die Übermittlung personenbezogener Daten in Länder außerhalb der EU bzw. des EWR (sog. Drittländer). Nahezu jedes Unternehmen hat in der Vergangenheit bei internationalen Datentransfers bereits auf die EU-Standardvertragsklauseln zurückgegriffen, sei es ganz bewusst durch gesonderte Vereinbarung oder aber durch die Akzeptanz Allgemeiner Geschäftsbedingungen, in denen die Standardvertragsklauseln bereits integriert sind. Gerade bekannte US-Provider wie Amazon, Google und Facebook beziehen Standardvertragsklauseln regelmäßig in ihre AGB mit ein, sodass diese bei Vertragsschluss automatisch mit vereinbart werden.

Die bisherigen Standardvertragsklauseln, zuletzt aktualisiert im Jahr 2010, waren jedoch noch ein Relikt aus der Zeit vor Inkrafttreten der Datenschutzgrundverordnung (DSGVO) und bedurften dringend einer Modernisierung, nicht zuletzt im Nachgang zu dem EuGH-Urteil „Schrems-II" zum internationalen Datentransfer. Dem ist die EU-Kommission durch Verabschiedung neuer Standardvertragsklauseln nun nachgekommen. Die neuen Standardvertragsklauseln sollen vor allem bestehende Anwendungslücken schließen und die seit geraumer Zeit geforderte Vereinheitlichung mit den Regelungen der DSGVO schaffen.

Modularer Aufbau und Ersatz von Auftragsverarbeitungsvereinbarungen

Eine wesentliche Neuerung ist der modulare Aufbau des Vertragswerks. Insgesamt wird es nunmehr vier verschiedene Module der Standardvertragsklauseln geben:

- Modul 1: Datenübermittlungen zwischen zwei Verantwortlichen
- Modul 2: Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter
- Modul 3: Datenübermittlungen von Auftragsverarbeitern an (Unter-)Auftragsverarbeiter
- Modul 4: Datenübermittlungen von Auftragsverarbeitern an Verantwortliche.

Die letzten beiden Konstellationen waren bislang nicht von den Standardvertragsklauseln umfasst und mussten in der Praxis durch umständliche Alternativen gelöst werden. Die Erweiterung ist daher sehr begrüßenswert.

Eine weitere Vereinfachung ergibt sich durch die Aufnahme der notwendigen Regelungen einer Vereinbarung zur Auftragsverarbeitung (Art. 28 DSGVO). Während unter Geltung der alten Standardvertragsklauseln zwischen Datenexporteur und Datenimporteur jeweils noch gesonderte Auftragsverarbeitungsverträge geschlossen werden mussten, sind die hierfür erforderlichen Vorschriften in den neuen Standardvertragsklauseln bereits enthalten. Darüber hinaus haben Dritte nunmehr die Möglichkeit, einer zwischen Importeur und Exporteur bereits existierenden Vereinbarung, die auf Grundlage der neuen Standardvertragsklauseln geschlossen wurde, beizutreten. Dies dürfte gerade bei komplexen Mehrparteienverträgen zu einer Vereinfachung führen.

Berücksichtigung der Schrems-II-Entscheidung

Neben einem erweiterten Anwendungsbereich sollen durch die neuen EU-Standardvertragsklauseln auch die Anforderungen der im letzten Jahr ergangenen sog. „Schrems-II-Entscheidung" berücksichtigt werden, die für viele Unternehmen nach wie vor eine gewaltige Herausforderung darstellt. Der EuGH hatte in seinem „Schrems-I-Urteil" vom 16.07.2020 (Rs. C-311/18) festgestellt, dass Datenübermittlungen in die USA nicht länger auf Grundlage des Privacy Shields erfolgen können und der Einsatz von EU-Standardvertragsklauseln bei Datenübermittlungen in Drittländer nur noch unter Verwendung wirksamer zusätzlicher Maßnahmen erfolgen darf, die ein dem Schutz personenbezogener Daten innerhalb der EU gleich-

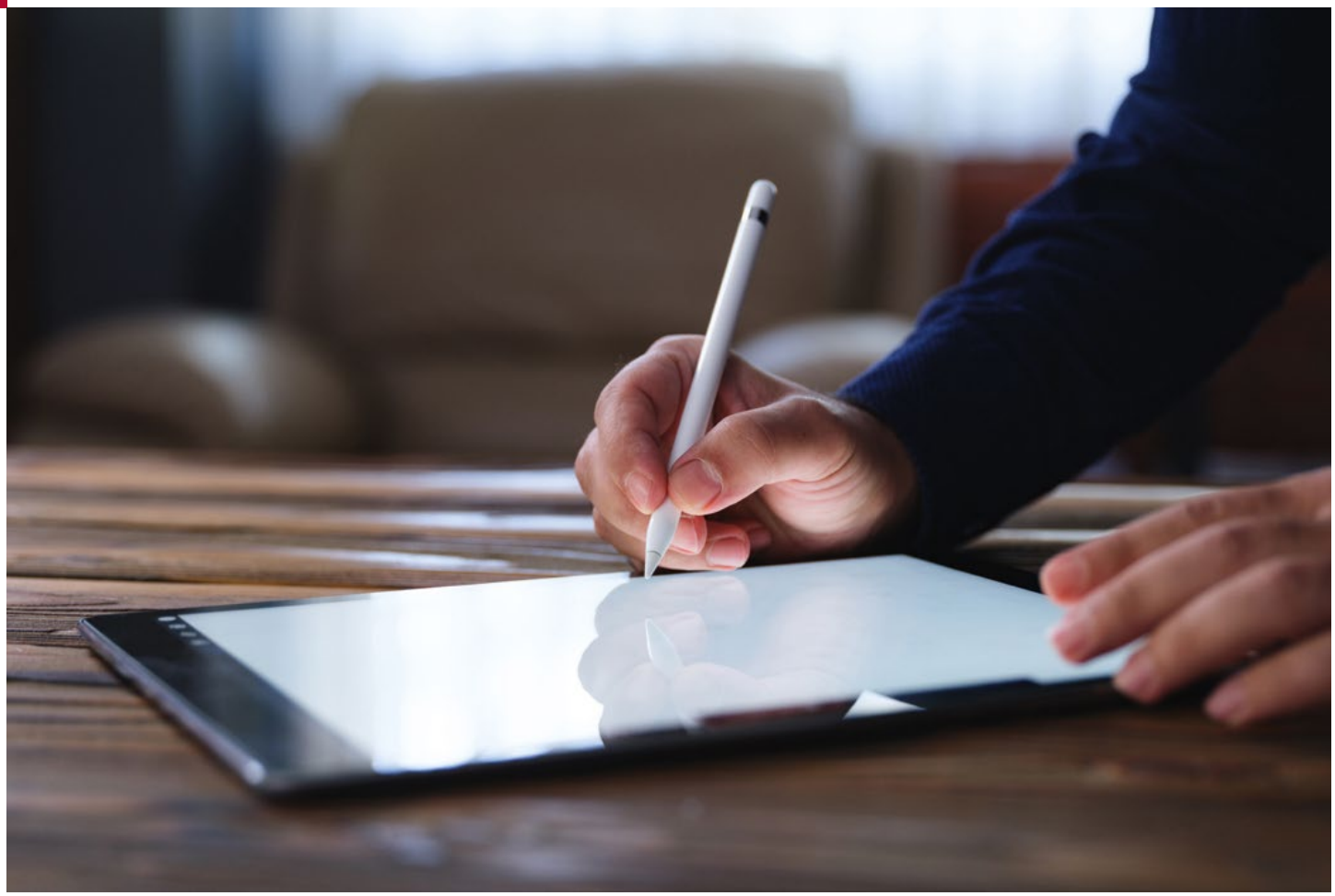
wertiges Niveau sicherstellen (mehr dazu lesen Sie unter www.ebner.stolz.de, Stichwort „Privacy Shield".

Die neuen EU-Standardvertragsklauseln sehen vor diesem Hintergrund vertragliche Regelungen vor, die sowohl das datenexportierende als auch das importierende Unternehmen verstärkt in die Pflicht nehmen. So reicht es für Datenübermittlungen in Drittländer künftig ausdrücklich nicht mehr aus, sich alleine auf die Standardvertragsklauseln zu berufen, ohne zuvor geprüft zu haben, ob der vertraglich vorgesehene Schutz personenbezogener Daten im jeweiligen Drittland auch tatsächlich gewährleistet werden kann. Insoweit bleibt es den exportierenden Unternehmen auch unter Geltung der neuen Standardvertragsklauseln nach wie vor nicht erspart, das Datenschutzniveau im jeweiligen Drittland zu überprüfen und bei Bedarf zusätzliche Maßnahmen zu ergreifen („Datentransfer-Folgenabschätzung").Umgekehrt ist der Datenimporteur dazu verpflichtet, sich gegen unverhältnismäßige Behördenanfragen, die den Anforderungen der DSGVO widersprechen, zu verteidigen und den Datenexporteur hierüber zu informieren. Anschließend muss der Datenexporteur selbst entscheiden, ob eine Datenübermittlung weiterhin stattfinden kann und die zuständige Aufsichtsbehörde über die Entscheidung in Kenntnis setzen. Die Pflicht zur Abwehr von Regierungsanfragen geht sogar so weit, dass Datenimporteure gegen entsprechende Behördenzugriffe gerichtlich vorgehen und die eigenen Abwehrmaßnahmen umfassend dokumentieren müssen. Unklar ist bisweilen jedoch, wer die dadurch entstehenden Kosten zu tragen hat.

Fazit und Handlungsempfehlung

Die neuen Standardvertragsklauseln enthalten längst überfällige Anpassungen an die DSGVO und schaffen durch den modularen Aufbau in Verbindung mit der Beitrittsmöglichkeit zu bestehenden Verträgen einen deutlich flexibleren Rechtsrahmen für die Übermittlung personenbezogener Daten in Drittländer. Gleichwohl können auch die neuen Standardvertragsklauseln die bestehende Rechtsunsicherheit infolge der Schrems-II-Entscheidung nicht vollständig beseitigen. Die erweiterten vertraglichen Schutzmaßnahmen können insoweit für sich genommen keine Übermittlung personenbezogener Daten in Drittländer rechtfertigen, in denen das Datenschutzniveau nicht dem der EU entspricht. In diesen Fällen sollten Unternehmen nach wie vor eine gründliche Risikoanalyse durchführen, zusätzliche Maßnahmen in Betracht ziehen und die Ergebnisse der Datentransfer-Folgenabschätzung dokumentieren. Andernfalls drohen aufsichtsrechtliche Sanktionen, zumal einige deutsche Aufsichtsbehörden erst vor Kurzem in diesem Zusammenhang gemeinsam abgestimmte Kontrollen angekündigt haben.

Aber auch unabhängig von der Schrems-II-Problematik ergibt sich aufgrund der neuen Standardvertragsklauseln Handlungsbedarf: Bei allen neu geschlossenen Verträgen müssen nach Veröffentlichung des Annahmebeschlusses im Amtsblatt der EU die neuen Standardvertragsklauseln berücksichtigt werden. Für alle bestehenden Verträge gilt eine Frist von 18 Monaten, innerhalb der alle bestehenden Standardvertragsklauseln durch die neuen Standardvertragsklauseln ersetzt werden müssen. Betroffene Unternehmen sollten sich daher schnellstmöglich mit den neuen Vertragsbedingungen vertraut machen, die entsprechenden Altverträge identifizieren und für eine fristgerechte Umstellung sorgen.



Elektronische Signaturen – Digitalisierung von Zeichnungsprozessen im Geschäftsalltag

Viele Unternehmen und Institutionen stehen vor der Herausforderung, bestehende Workflows unter Einsatz elektronischer Signaturen zu digitalisieren. Die daraus resultierenden Fragen greifen wir auf und geben Handlungsempfehlungen für die Praxis.

Hintergrund

Zunächst stellt sich die Frage, was unter einer „digitalen Unterschrift" zu verstehen ist. Eine digitale Unterschrift stellt rechtlich betrachtet eine elektronische Signatur dar. Früher waren die entscheidenden Regelungen national im Signaturgesetz umgesetzt. Mittlerweile greift mit der Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-VO) eine europaweite Regelung.

Das europäische Signaturrecht

Seit dem 01.07.2016 findet die eIDAS-VO unmittelbare Anwendung und gilt somit unmittelbar in allen Mitgliedstaaten der Europäischen Union. Zur Feststellung des erforderlichen Signaturlevels muss aber auch das nationale Recht beachtet werden. Aus diesem können sich Formerfordernisse ergeben, die bei der Wahl der Signatur ausschlaggebend sind. Qualifizierte elektronische Signaturen stehen der klassischen handschriftlichen Unterschrift gleich.

Zu beachten ist, dass im internationalen Kontext das Recht desjenigen Staates gilt, in welchem die Signatur zur Anwendung kommen soll. Welche Signaturform im jeweiligen Staat erforderlich ist, sollte im Einzelfall geprüft werden.

Die drei Stufen der digitalen Signatur

Es bestehen drei Stufen der digitalen Signaturen. Dies sind die „einfache Signatur", die „fortgeschrittene Signatur" und die „qualifizierte Signatur". Je höher die Signaturstufe ist, desto höher sind die an sie gestellten technischen Anforderungen.

Die erste Stufe stellt die einfache Signatur als schwächste Form der Signatur dar. Dementsprechend sollte sie nur genutzt werden, wenn bei der Verwendung nur ein geringes rechtliches Risiko besteht. Die einfache Signatur stellt keinerlei Anforderungen an die Identifizierung des Unterzeichners und ist daher nicht fälschungssicher. Über ein Zertifikat lässt sich jedoch die Integrität des Dokuments sicherstellen, sodass es nach dem „Signieren" nicht mehr abgeändert werden kann. Dies ist auch an den Attributen im PDF-Dokument erkennbar.

Die nächste Stufe stellt die fortgeschrittene Signatur dar. Auch hier erfolgt keine Identifikation durch ein Identifikationsdokument. Für die Authentifizierung genügt eine Anmeldung via Username und Passwort, was ebenfalls nicht fälschungssicher ist. Dennoch vereinfacht sie die Prüfung der Gültigkeit der Unterschrift im Streitfall. Der Einsatz dieser Signatur ist bei einem mittleren rechtlichen Risiko angemessen. Einige Vertrauensdienstleister ziehen zusätzliche Sicherheitsfaktoren für die Authentifizierung heran, wie z. B. die Personalausweisnummer. Das Vorliegen dieses Signaturlevels ist auch an den Attributen im PDF-Dokument erkennbar. Dort findet sich bspw. die Formulierung „Unterschrieben von [Name]" und „Vertrauensquelle wurde vom [Adobe Approved Trust List (AATL)]" verifiziert.

Die dritte und höchste Stufe stellt die qualifizierte Signatur dar. Nur diese erfüllt die Schriftform gemäß § 126 in Verbindung mit § 126a Bürgerliches Gesetzbuch (BGB). Damit kommt ihr dieselbe Rechtswirkung zu wie einer handschriftlichen Unterschrift. Bei der qualifizierten Signatur lässt sich der Inhaber der Signatur eindeutig zuordnen, da die Authentifizierung z. B. über PostIdent, VideoIdent oder eine Online-Ausweisfunktion stattfindet. Zudem wird ein qualifiziertes Zertifikat verwendet, welches von einem Vertrauensdienstanbieter ausgestellt wird. Auch dies ist an den Attributen im PDF-Dokument erkennbar. Dort findet sich bspw. die Formulierung „Unterschrieben von [Name]" und „Vertrauensquelle wurde vom [European Union Trusted Lists (EUTL)]" verifiziert sowie „Das ist eine qualifizierte elektronische Signatur gemäß EU-Verordnung 910/2014".

Was gilt es zu beachten? – Legal Best Practices

Wenn ein gesetzliches oder vertraglich vereinbartes Schriftformerfordernis vorliegt, sollte die qualifizierte elektronische Signatur verwendet werden. In allen anderen Fällen kann prinzipiell auf die einfache oder die fortgeschrittene elektronische Signatur zurückgegriffen werden. Beweiskraft als Urkunde im gerichtlichen Sinne hat in erster Linie nur die qualifizierte elektronische Signatur. Die Haftungsrisiken und das Interesse an einer Beweiswürdigung vor Gericht sind stets abzuwägen. Bestehen bspw. hohe Risiken, so sollten diese durch eine entsprechend höhere Signaturstufe abgesichert werden.

Es können jedoch auch Besonderheiten bestehen, denn einige Dokumente können nicht rechtlich wirksam elektronisch signiert werden. Hierzu gehören Dokumente, die notariell beglaubigt werden müssen, Kündigungen und Auflösungsverträge zur Beendigung des Arbeitsverhältnisses, Arbeitszeugnisse sowie Bürgschaftserklärungen und abstrakte Schuldanerkenntnisse, soweit es sich nicht um Handelsgeschäfte handelt.

Fazit und Handlungsempfehlungen

Rechtsgrundlage für elektronische Signaturen ist die eIDAS-VO, die unmittelbar in allen EU-Staaten gilt. Unterschieden werden drei Arten der elektronischen Signatur. Beweiskraft einer Urkunde hat nur die qualifizierte elektronische Signatur. Die Wahl der Form der Signatur ist abhängig von Schriftformerfordernissen. Daher müssen die im Unternehmen einschlägigen Prozesse dahingehend bestimmt werden, welche Formerfordernisse nach nationalem Recht gelten. Danach kann entschieden werden, welche Signatur rechtlich notwendig bzw. risikoabhängig angemessen ist. Bei der Wahl des Diensteanbieters sollte eine verbindliche Erklärung zur Erfüllung der gesetzlichen Norm der technischen Anforderungen eingeholt werden.

Informationssicherheit: Zertifizierung durch die ESecurity-CERT GmbH

Regulatorien, u. a. des Gesetzgebers, der Wettbewerb, Kunden und nicht zuletzt das eigene Risikobewusstsein führen dazu, dass sich Unternehmen verstärkt den umfassenden Anforderungen zur Informationssicherheit stellen. Im Vorteil ist, wer die Umsetzung mit einer Zertifizierung auch nachweisen kann.

Doch: Wie kann die Qualität der im Unternehmen implementierten Maßnahmen zur Informationssicherheit nachvollziehbar belegt werden? Zertifizierungsstellen für einzelne Standards gibt es viele. Zertifizierungsstellen, die sich im Verbund umfänglich mit IT-Compliance beschäftigen und damit die jeweils passende Lösung anbieten, sind jedoch eher selten anzutreffen.

Ebner Stolz bietet durch den Geschäftsbereich IT-Revision einerseits und die ESecurity-CERT andererseits genau diese umfängliche und übergreifende Sicht auf IT-Compliance. Im Folgenden stellen wir die Bedeutung von Zertifizierungen durch eine Zertifizierungsstelle wie die ESecurity-CERT dar.

ISO/IEC-Normen sind weltweit anerkannte Standards. Sie bieten einen systematischen sowie strukturieren Ansatz und haben so den Vorteil, dass bspw. eine Zertifizierung in der Informationssicherheit nach DIN EN ISO/IEC 27001:2017-06 weltweit Anerkennung findet.

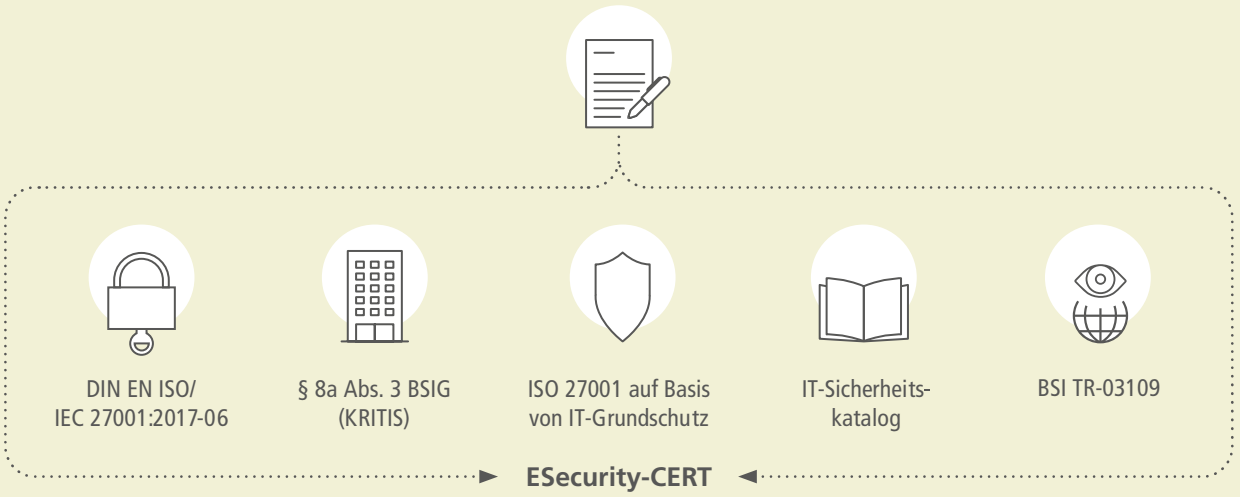
Zertifizierungsdienstleistungen

„In Deutschland hat im Bereich der Informationssicherheit insb. das IT-Sicherheitsgesetz mit dazu beigetragen, dass Prüfungen nach DIN EN ISO/IEC 27001:2017 sowie § 8a KRITIS durchgeführt werden müssen", sagt Gerd Niehuis, Geschäftsführer der ESecurity-CERT. „Es werden sich bspw. durch das IT-Sicherheitsgesetz 2.0, das am 28.05.2021 in Kraft trat, noch einmal deutliche Änderungen ergeben. Die ESecurity-CERT GmbH versteht sich im Rahmen dessen als unbürokratisches Bindeglied zur Erreichung der Anforderungen. Zertifizierungsaudits mit dem Nachweis der Wirksamkeit von Managementsystemen sollen Nutzen für unsere Mandanten schaffen. Unser Ziel ist, unsere Kompetenz in einem ganzheitlichen Ansatz zur Verfügung zu stellen."

Die ESecurity-CERT ist eine bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) akkreditierte Konformitätsbewertungsstelle, die rechtskräftig Zertifizierungen nach DIN EN ISO/IEC 27001:2017-06 vornehmen kann. Eine Akkreditierung bei der DAkkS ist Grundvoraussetzung, um rechtskräftig zertifizieren zu dürfen. Weitere Akkreditierungen befinden sich bei der ESecurity-CERT bereits in Umsetzung.

Insgesamt bildet die ESecurity-CERT folgende Bereiche ab:

- Zertifizierung gemäß DIN EN ISO/IEC 27001:2017-06
- KRITIS-Prüfungen gemäß § 8a Abs. 3 BSIG für Betreiber kritischer Infrastrukturen
- Zertifizierung nach IT-Sicherheitskatalog gemäß § 11 Abs. 1a und 1b EnWG
- Auditierung nach ISO 27001 auf Basis von IT-Grundschutz
- Smart Meter Gateway nach TR-03109



„Auch zukünftig wird erwartet, bspw. im Datenschutz, dass entsprechende Zertifizierungen nur durch akkreditierte Stellen erfolgen dürfen“, erläutert Marc Alexander Luge, Prokurist der ESecurity-CERT GmbH. „Daher sind weitere Zertifizierungsangebote in Vorbereitung, sobald diese gesetzlich konkretisiert sind.“

Leistungen am Beispiel einer Zertifizierung des ISMS nach DIN EN ISO/IEC 27001:2017-06

Das Informationssicherheitsmanagementsystem (ISMS) wird durch die ESecurity-CERT GmbH im Hinblick auf die Identifikation, Analyse und Ableitung von Maßnahmen zur Steuerung der Informationssicherheitsrisiken geprüft.

Die Norm ISO/IEC 27001 hat sich international als Standard für Informationssicherheit in Unternehmen und Behörden etabliert. Das ISMS ist als ein ganzheitliches und auf Kontinuität ausgelegtes System zur Absicherung der Informationssicherheit in der Organisation zu sehen. Es darf nicht der Fehler gemacht werden, Informationssicherheit mit dem Teilgebiet IT-Sicherheit gleichzustellen. Informationssicherheit geht über die rein technische Absicherung hinaus und bildet einen Prozess zur kontinuierlichen Verbesserung im Unternehmen, in Geschäftsprozessen und der IT ab.

Der Zertifizierungszyklus ist aufgrund der Gültigkeit der Zertifikate auf drei Jahre ausgelegt. Zu Beginn ist ein formaler Antrag zur Zertifizierung durch die zu prüfende Organisation zu stellen.

Im Anschluss erfolgt das Zertifizierungsaudit, das wir im Folgenden unter Erst-/Rezertifizierung darstellen. Darauf baut die Entscheidung über die Zertifizierung auf.

Durch das jährliche Überwachungsaudit, welches im zweiten und dritten Jahr erfolgt, wird sichergestellt, dass das ISMS während der gesamten Gültigkeitsdauer des Zertifikats aufrechterhalten wird. Der Prüfungsumfang ist hierbei deutlich geringer als der im Rahmen des Zertifizierungsaudits angesetzte.

Der Unterschied zwischen der Erst- und Rezertifizierung ist methodisch gering. Aufgrund der bestehenden Zertifizierung ist der Zeitbedarf für das Audit in der Rezertifizierung i. d. R. jedoch etwas geringer als bei der Erstzertifizierung.

Die ESecurity-CERT setzt dabei auf ein mehrstufiges Verfahren: Im ersten Schritt prüft der (Lead-)Auditor beim Unternehmen die Konformität eines ISMS unter Verwendung des ISO-Regelwerks und fertigt einen Report an. Dieser wird im nächsten Schritt durch andere Mitarbeiter der ESecurity-CERT qualitätsgesichert und es wird durch die ESecurity-CERT abschließend die Entscheidung über die Zertifikatserteilung getroffen.

Über die Website der ESecurity-CERT (www.esecurity-cert.com) haben Sie die Möglichkeit, sich einen Überblick der Leistungen zu verschaffen.

1 **Ausstellung des Zertifikats**

2 **Überwachungsaudit**
Das erste darf nicht mehr als zwölf Monate nach dem Datum der Zertifizierungsentscheidung liegen. Das zweite erfolgt spätestens zwölf Monate nach dem ersten.

3 **Abweichungen**
Diese werden während des Überwachungsaudits herausgestellt und müssen auf die gleiche Weise beseitigt werden wie in einem Audit in Stufe 2.

4 **Rezertifizierung**
Drei Monate bevor sich Ihr Zertifikat zum dritten Mal jährt, werden wir Sie für ein erneutes Audit besuchen.

5 **Neubeginn des Zertifizierungszyklus**

IT-Sicherheitsgesetz 2.0 – Durchbruch für Deutschlands Cybersicherheit?

Bereits im Frühjahr 2019 wurde der erste Referentenentwurf zum IT-Sicherheitsgesetz (IT-SiG) 2.0 veröffentlicht, um das aus dem Jahr 2015 stammende IT-SiG umfangreich anzupassen. Zwei Jahre später wurde es zum 27.05.2021 im Bundesgesetzblatt veröffentlicht und trat zum 28.05.2021 in Kraft.

Was bedeutet diese Anpassung nun? Wie das IT-SiG 1.0 bedingt auch die neue Version 2.0 als Artikelgesetz weitreichende Änderungen in einer ganzen Reihe von Einzelgesetzen (neben dem BSI-Gesetz – BSIG – u. a. das Energiewirtschaftsgesetz und das Telekommunikationsgesetz).

Die einzelnen wesentlichen Änderungen bzw. Neuerungen sind:

1. Erhöhung der Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
2. Erweiterung der betroffenen Unternehmen als KRITIS-Betreiber
3. Zusätzliche Pflichten für KRITIS-Betreiber
4. Schutz der Bürger
5. Neufassung der Bußgeldvorschrift.

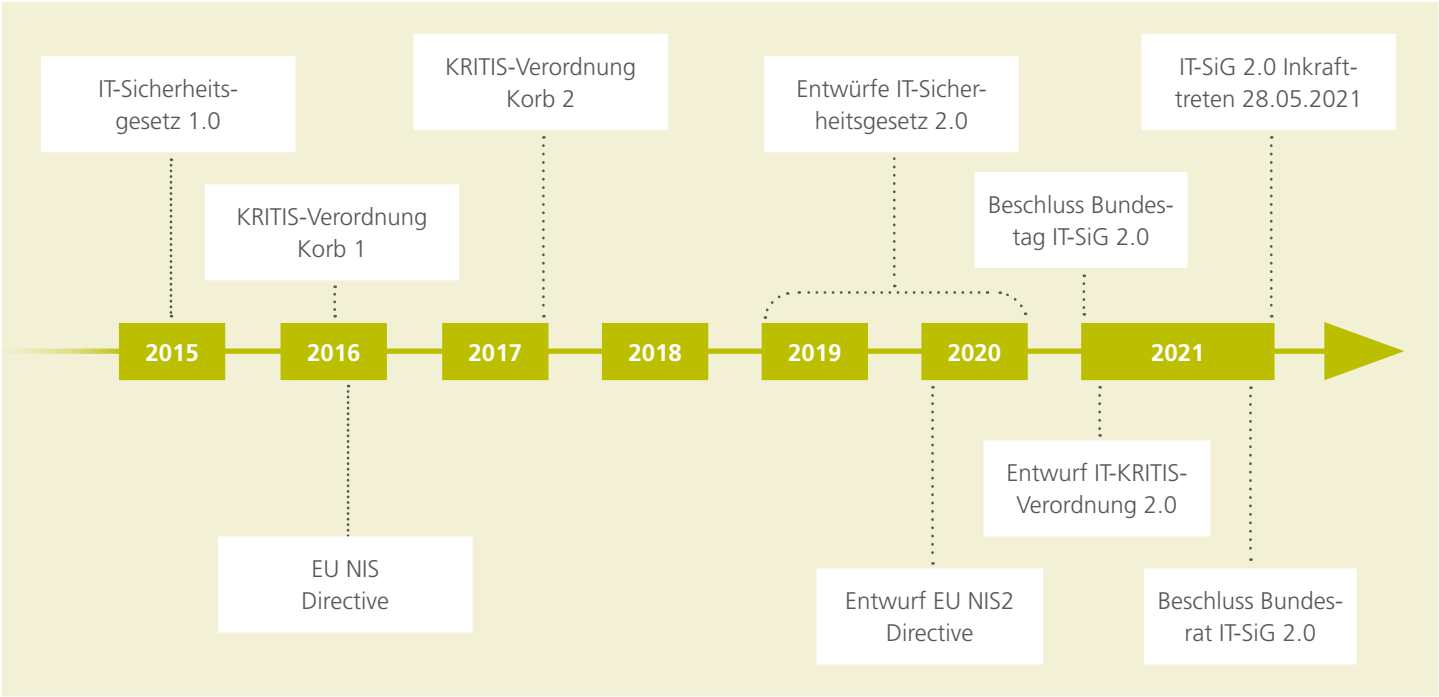
Erhöhung der Befugnisse des BSI

Ein Kernaspekt betrifft die Kompetenzen des BSI, die erheblich ausgeweitet werden. Das BSI ist zum einen dazu berechtigt, sog. Portscans gemäß § 7b Abs. 1 BSIG durchzuführen. Durch Portscans können Sicherheitslücken, z. B. veraltete Software oder offene Ports, in den IT-Systemen identifiziert werden. Durch die neue Gesetzgebung soll das BSI die Möglichkeit erhalten, solche Schwachstellen zu identifizieren, das betroffene Unternehmen zu informieren und zu überwachen, sodass die Sicherheitslücken zeitnah geschlossen werden. Zum anderen wird das BSI zum Einsatz von Honeypots i. S. d. § 7b Abs. 4 BSIG berechtigt, d. h. zum Einsatz von Systemen und Verfahren zur Analyse von Schadprogrammen sowie Angriffsmethoden.

Gemäß § 5 Abs. 2 BSIG war das BSI bereits in der Vergangenheit zur Erhebung und Auswertung von Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen (Protokolldaten i. S. d. § 5 Abs. 1 Nr. 1 BSIG), berechtigt. Der Zeitraum für die Datenspeicherung wurde von drei auf zwölf Monate erhöht.

Zudem erfolgte die Aufnahme von Protokollierungsdaten in das BSIG. Gemäß § 2 Abs. 8a BSIG versteht man unter Protokollierungsdaten Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme. Laut § 5a BSIG ist das BSI bei Protokollierungsdaten, analog zu den Protokolldaten, zur Verarbeitung berechtigt, sofern dies zur Erkennung, Eingrenzung oder Beseitigung von Störungen, Fehlern oder Sicherheitsvorfällen notwendig ist.

Durch den neu eingeführten § 7a BSIG, in dem die Untersuchung der Sicherheit in der Informationstechnik geregelt ist, darf das BSI nun jegliche, bereits auf dem Markt bereitgestellte wie auch dafür vorgesehene informationstechnische Produkte und Systeme untersuchen. Hersteller dieser Produkte und Systeme sind zur Auskunft gegenüber dem BSI verpflichtet, dazu gehört insb. die Auskunft über technische Details. Kommt ein Hersteller dieser Pflicht nicht nach, begeht er eine Ordnungswidrigkeit i. S. d. § 14 Abs. 2 BSIG, welche ein Bußgeld nach sich ziehen kann.



Zusätzlich werden die Kontroll- und Prüfbefugnisse zum Schutz der Regierungsnetze ausgebaut.

Was als These aufgeworfen wurde, scheint sich nun zu bestätigen: Augenscheinlich entwickelt sich der BSI, analog zu der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Bereich des Finanzwesens, zu einer Aufsichtsbehörde, jedoch nur spezialisiert auf die IT-Sicherheit.

Erweiterung der betroffenen Unternehmen als KRITIS-Betreiber – Ausweitung auf weitere Teile der Wirtschaft

Im Zuge des IT-SiG 2.0 wird der Anwendungsbereich des BSIG um sog. Unternehmen „im öffentlichen Interesse" erweitert. Dies sind Unternehmen, die von „erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind" (vgl. § 2 Abs. 14 Satz 1 Nr. 2 BSIG).

Dazu gehören gemäß § 2 Abs. 14 BSIG drei Fallgruppen:

- Unternehmen, die Güter nach § 60 Abs. 1 Nr. 1 und 3 der Außenwirtschaftsverordnung herstellen oder entwickeln. Das sind insb. Unternehmen aus der Rüstungs-, Raumfahrt- und IT-Sicherheitsindustrie.

- Unternehmen, die gemessen an ihrer inländischen Wertschöpfung zu den größten Unternehmen des Landes gehören und daher von erheblicher Bedeutung für Deutschland sind. In einer künftigen Rechtsverordnung soll festgelegt werden, welche Kennzahlen maßgeblich für die Festlegung sind, ob ein Unternehmen von erheblicher Bedeutung für das Land ist.

- Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung oder eines diesen gemäß § 1 Abs. 2 der Störfall-Verordnung gleichgestellten Bereichs, hierunter fallen insb. Unternehmen aus der chemischen Industrie.

Unternehmen mit besonderen öffentlichen Interesse werden KRITIS-Betreibern zwar nicht gleichgestellt, allerdings haben sie nun erhöhte Anforderungen gemäß § 8f BSIG zu erfüllen. Darunter fällt insb. die Selbsterklärung zur IT-Sicherheit gemäß § 8f Abs. 1 BSIG. Diese muss von den oben genannten ersten beiden Unternehmensgruppen mindestens alle zwei Jahre vorgelegt werden. Aus dem IT-Sicherheitskonzept muss hervorgehen, welche Zertifizierungen, sonstigen Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt wurden. Ergänzend dazu muss erklärt werden, wie der Schutz besonders schützenswerter IT-Systeme, Komponenten und Prozesse sichergestellt wird.

Zudem haben Unternehmen der ersten beiden Fallgruppen bei Störungen eine unverzügliche Meldung gemäß § 8 Abs. 7 BSIG an das BSI vorzunehmen. Eine entsprechende Meldepflicht gilt ebenfalls für Unternehmen der chemischen Industrie, allerdings gilt hier eine Besonderheit, denn Störungen können hier in Gefahren für die öffentliche Sicherheit und Ordnung resultieren. Ein entsprechender Meldeweg ist zu definieren.

Durch die Ausweitung des Anwendungsbereichs, trifft die Regulierung nun alle Unternehmen ab einer bestimmten Bedeutung für das Allgemeinwohl. Dazu zählen ebenfalls Unternehmen, die keinem der in § 2 Abs. 10 BSIG aufgezählten Sektoren angehören. Insb. jene sollten prüfen, ob sich aus der Inkraftsetzung nun Erfüllungspflichten ergeben.

Darüber hinaus werden die KRITIS um den Sektor „Siedlungsabfallentsorgung" (§ 2 Abs. 10 BSIG) erweitert, wodurch nun u. a. Entsorger KRITIS sind (Dienstleistung Entsorgung von Siedlungsabfällen mit Sammlung, Beseitigung und Verwertung).

Die gegenwärtig definierten Schwellenwerte werden gesenkt, sodass mehr Unternehmen als kritische Infrastruktur eingestuft werden. Es wird davon ausgegangen, dass die Anzahl der KRITIS-Unternehmen um 15 bis 20 % steigen wird.

Analog des IT-SiG 1.0 wird die Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) novelliert, in welcher die exakten Schwellenwerte definiert werden. Noch in 2020 wurde ein Entwurf der BSI-KritisV veröffentlicht.

Zusätzliche Pflichten für KRITIS-Betreiber

Betreiber kritischer Infrastrukturen sind verpflichtet, sich unmittelbar beim BSI zu registrieren (vgl. § 8b Abs. 3 Satz 1 BSIG) und sie müssen ab dem 01.05.2023 ganzheitliche „Systeme zur Angriffserkennung" nutzen (§ 8a Abs. 1a BSIG). Solche ganzheitlichen Systeme sind dabei so definiert, dass sie „geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten" müssen.

Darüber hinaus gab es bisher nur den Begriff der Kritischen Infrastrukturen (KRITIS) im BSIG, nun gibt es auch den der Kritischen Komponenten. Hinter sog. Kritischen Komponenten verbergen sich gemäß § 2 Abs. 13 BSIG IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, da auftretende Störungen erheblichen Einfluss auf die Kritische Infrastruktur selbst oder auch auf die öffentliche Sicherheit haben können. Ebenso fallen darunter IT-Produkte, die kraft Gesetzes als Kritische Komponente definiert werden.

Im ersten Schritt besteht eine Meldepflicht, wenn sich Kritische Komponenten im Einsatz befinden. Benannte Komponenten dürfen nur noch zum Einsatz kommen, sofern eine entsprechende Garantieerklärung des Herstellers abgegeben wurde, in der er seine Vertrauenswürdigkeit unter Beweis stellt. Darin anzugeben ist, ob und wie sichergestellt wird, dass die Kritische Komponente frei von Eigenschaften ist, die missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit und Funktionsfähigkeit der Kritischen Infrastruktur einwirken könnten. Dabei wird vor allem auf Sabotage, Spionage oder Terrorismus abgestellt. Im nächsten Schritt hat das

BSI die Möglichkeit, den Einsatz eingesetzter kritischer Komponenten zu untersagen. Hierfür müssen allerdings öffentliche Interessen gegen besagten Einsatz sprechen. Diese Klausel wird auch als „Lex Huawei" bezeichnet.

Schutz der Bürger

Verbraucherschutz wurde neu im BSIG als Aufgabe des BSI verankert. Den Kernpunkt bildet dabei das freiwillige IT-Sicherheitskennzeichen gemäß § 9c BSIG. Ziel dabei ist es, eine verständliche, transparente und einheitliche Darstellung von Verbraucherprodukten und IT-Dienstleistungen zu gewährleisten. Das IT-Sicherheitskennzeichen besteht aus der Herstellererklärung und der Sicherheitserklärung des BSI. In der Herstellererklärung garantiert der Hersteller dafür, dass das Produkt bestimmte IT-Sicherheitsanforderungen erfüllt.

Bußgeldvorschriften

Die Regelung zu den Bußgeldvorschriften befindet sich weiterhin in § 14 BSIG. Es erfolgte allerdings eine komplette Überarbeitung des aufgeführten Katalogs, wobei Tatbestände ergänzt und die Bußgelder deutlich erhöht wurden. Bislang waren nicht alle Pflichten, die laut BSIG erfüllt werden müssen, durch die Bußgeldvorschrift erfasst, was durch das nun verabschiedete Gesetz geändert wurde. Die Notwendigkeit, auf die Einhaltung der Vorschriften des IT-Sicherheitsgesetzes 2.0 ein Auge zu haben, wird spätestens bei der Betrachtung der Bußgeldhöhe deutlich. In der Vergangenheit lag die maximale Bußgeldhöhe bei nur 100.000 Euro, in der Zukunft kann das BSI Unternehmen bis zu einem Betrag von zwei Mio. Euro zur Kasse bitten. Durch den Verweis auf § 30 Abs. 2 Satz 3 OWiG kann sich die Bußgeldhöhe sogar noch auf bis zu 20 Mio. Euro verzehnfachen. Das ist bspw. der Fall bei Zuwiderhandlung von Anordnungen, aber auch bei der Unterlassung der Nachweiserbringung in Form des § 8a-Audit sind bis zu 10 Mio. Euro möglich. Die Höhe liegt im Ermessen des Bundesamtes.

ISO/IEC DIS 27002:2021-01 – Überarbeitung oder Erweiterung der Version aus 2013?

Die internationale Norm ISO/IEC 27002 ist ein Leitfaden für Informationssicherheitsmaßnahmen, welcher momentan noch in der englischen Fassung aus dem Jahr 2013 bzw. in der deutschen Fassung aus dem Jahr 2017 anzuwenden ist. Die Vorgaben der Norm sind nicht verpflichtend anzuwenden, es handelt sich vielmehr um Empfehlungen, die umgesetzt werden können. Allerdings ergeben sich durchaus Auswirkungen auf andere Standards aus der 27000-Normenreihe, da die Norm die Informationssicherheitsmaßnahmen (Controls) des Anhangs A der Norm ISO/IEC 27001, welche die zentrale Norm für Informationssicherheitsmanagementsysteme darstellt, konkretisiert und erläutert.

Für die Norm ist jeweils fünf Jahre nach dem Inkrafttreten eine Überarbeitung vorgesehen, welche planmäßig im März 2018 begann. Nach einer knapp dreijährigen Überarbeitungsphase haben die International Organization for Standardization (ISO) und die International Electrotechnical Commission (IEC) im Januar dieses Jahres den Entwurf für die Norm ISO/IEC DIS 27002:2021-01 veröffentlicht. Der Erlass der finalen Version wird spätestens Ende des laufenden Jahres erwartet.

Allgemein

Bereits die Tatsache, dass die Bezeichnung der Norm geändert wurde, lässt darauf schließen, dass weitreichende Änderungen vorgenommen wurden. Während ISO/IEC 27002:2013 den Titel „Information technology – Security techniques – Code of practice for information security controls" trägt, wurde die neue Norm mit dem Titel „Information security, cybersecurity and privacy protection – information security controls" bezeichnet. Demnach beschäftigt sich die neue Norm neben der Informationssicherheit auch explizit mit den Themengebieten Cyber-Sicherheit und Datenschutz. Ebenso wird bei dem Vergleich des Umfangs deutlich, dass die geplante Norm ISO/IEC DIS 27002:2021-01 mit 50 Seiten mehr deutlich umfassender ist.

Anwendungsbereich

Der Anwendungsbereich der Norm hat sich nicht verändert. Sie richtet sich weiterhin sowohl an Organisationen, die ein Informationssicherheitsmanagementsystem gemäß ISO/IEC 27001 eingerichtet haben und hierfür Maßnahmen auswählen, als auch an Organisationen, die allgemein akzeptierte bzw. selbst entwickelte Maßnahmen für Informationssicherheit umsetzen bzw. entwickeln möchten. Bislang wurde hinsichtlich Definitionen und Abkürzungen auf die übergeordnete Norm ISO/IEC 27000 verwiesen. Da sich jedoch Änderungen ergeben haben, bzw. ergänzende Begriffsdefinitionen notwendig waren, wurde ein separater Abschnitt hierfür in die neue Norm aufgenommen.

Aufbau

Der Aufbau der Norm ISO/IEC 27002 wurde vollständig überarbeitet. Während in der bisherigen Norm 14 Control Clauses (Sicherheitsmaßnahmen) mit 35 Security Categories (Hauptsicherheitskategorien) und 114 Controls (Maßnahmen) enthalten waren, unterteilt die neue Norm nur noch in die vier Themes (Themen): organizational controls, people controls, physical controls und technological controls. Das Thema organizational controls ist dabei als eine Art Residualkategorie anzusehen, der alle Controls (Maßnahmen) zugeordnet wurden, die thematisch nicht den anderen Themenbereichen zugeordnet werden konnten. Den Themen sind wiederum insgesamt 93 Controls (Maßnahmen) zugeordnet. Auch wenn die Struktur der Norm komplett geändert wurde, dürften die jeweiligen Maßnahmen vergleichsweise leicht zu finden sein, da die Zuordnung zu den Themen selbsterklärend ist. Zudem ist im Anhang der Entwurfsfassung ein Mapping enthalten, welches beschreibt, an welcher Stelle sich die jeweiligen Controls (Maßnahmen) aus der alten 27002-Norm in der neuen Norm wiederfinden lassen.

Jede dieser Controls setzt sich nun aus den folgenden Bestandteilen zusammen:

- **Control Title**
  Bezeichnung der Maßnahme
- **Attribute Table**
  Werte der jeweiligen Attribute
- **Control**
  Beschreibung der Maßnahme
- **Purpose**
  Zweck der Maßnahme
- **Guidance**
  Implementierungsanleitung
- **Other Information**
  Erläuternder Text, Verweise

Attributes

Zu den in der Norm aufgeführten Controls (Maßnahmen) wurden sog. Attributes aus fünf verschiedenen Kategorien hinzugefügt:

- **Control Title**
  Kontrolltyp
- **Information security properties**
  Informationssicherheitseigenschaften
- **Cybersecurity concepts**
  Cybersicherheitskonzepte
- **Operational capabilities**
  Operative Fähigkeiten
- **Security domains**
  Sicherheitsdomänen

Jeder Control (Maßnahme) wird zu jedem Attribut mindestens ein Wert zugeordnet. Bspw. werden für das Attribut Control Type (Kontrolltyp) die Controls (Maßnahmen) mit den Werten #Preventive (#Präventiv), #Detective (#Erkennend) oder #Corrective (#Korrigierend) verbunden. Im Anhang der Norm ISO/IEC DIS 27002:2021 findet sich eine Tabelle zur Verwendung dieser Attribute. Durch die Zuordnung der Attribute zu den Controls (Maßnahmen) wird den Organisationen zum einen eine zielgerichtete und fokussierte Anwendung der Norm ermöglicht, zum anderen besteht dadurch ein geringerer Interpretationsspielraum bei der Anwendung. Bspw. kann so direkt nach allen Maßnahmen gefiltert werden, die sich auf eine bestimmte Informationssicherheitseigenschaft wie die Vertraulichkeit beziehen.

Kontroll-Ebene

Bei der Betrachtung der neuen Norm auf Kontrollebene lässt sich feststellen, dass keine einzige Control (Maßnahme) unverändert aus der bisher gültigen Norm übernommen wurde. Stattdessen gibt es 11 komplett neue Controls, eine Control wurde nicht übernommen, eine Control wurde aufgeteilt, 56 Controls wurden auf 24 Controls komprimiert und die verbleibenden Controls wurden neu formuliert.

Die neuen Controls (Maßnahmen) stammen überwiegend aus dem Themenbereich technological controls. Bei der entfernten Control (Maßnahme) handelt es sich um die Control 11.2.5 Removal of assets (Entfernen von Werten), welche sich mit der Entfernung von Geräten, Betriebsmitteln, Informationen und Software vom Betriebsgelände ohne vorherige Genehmigung befasst. Diese Control (Maßnahme) wurde als redundant angesehen, da dieselbe Thematik bereits in der Control (Maßnahme) zur Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten (11.2.6. ISO/IEC 27002-2017) behandelt wird. Durch die Zusammenfassung und Integration mehrerer Kontrollmaßnahmen dürfte es in der Zukunft schwieriger werden, bestimmte Maßnahmen nicht umzusetzen, sofern sie im eigenen Unternehmen nicht vorhanden sind.

Guidance and other Information (Maßnahmen zur Umsetzung und andere Informationen)

Im Rahmen der Überarbeitung der Norm wurde zu jeder Control (Maßnahme) ein Abschnitt zu Guidance and Other Information (Maßnahmen zur Umsetzung und andere Informationen) formuliert. Bislang gab es auch vereinzelt Maßnahmen, bei denen diese Angaben nicht vorhanden waren. Zudem sind diese Bereiche nun deutlich umfassender gestaltet und konkretisieren die jeweiligen Umsetzungsmöglichkeiten. Der höhere Detaillierungsgrad ist zwar mitverantwortlich für den größeren Umfang der Norm, allerdings bietet er durchaus eine nützliche Hilfestellung, insb. auch bei der Erstellung von unternehmensinternen Richtlinien.

Fazit

Mit der ISO/IEC DIS 27002:2021-01 ist eine umfassende Überarbeitung der bisherigen Vorgaben vorgesehen. In der Praxis wird nur die Umsetzung der 11 neu implementierten Maßnahmen nicht ausreichend sein, denn auch die übernommenen Maßnahmen haben weitreichende Änderungen erfahren. Es handelt sich bei der Norm um einen Code of Practice, was bedeutet, eine Zertifizierung nach dieser Norm ist nicht möglich. Demnach bleibt eine Aktualisierung der ISO 27001 abzuwarten, um anschließend zertifiziert werden zu können.

Hinsichtlich der inhaltlichen Änderungen der Norm lässt sich allerdings festhalten, dass sich keine tiefgreifenden neuen Aspekte in der Norm vorfinden. Bei den aufgeführten Maßnahmen handelt es sich um allgemein akzeptierte Maßnahmen, die teilweise bereits in der Praxis umgesetzt werden.

Auch wenn es sich bislang nur um einen Entwurf handelt, ist damit zu rechnen, dass dessen Inhalt größtenteils in die finale Fassung übernommen wird. Organisationen, die ein Informationssicherheitsmanagementsystem implementiert haben, sollten sich daher bereits jetzt mit den Änderungen auseinandersetzen.

Umstellung ISO/IEC 27019:2017

Am 01.11.2017 wurde die überarbeitete ISO/IEC 27019:2017 „Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmaßnahmen für die Energieversorgung“ veröffentlicht. Alle Betreiber von Energieversorgungsnetzen in Deutschland müssen sich seit 2017 einer Zertifizierung nach dem IT-Sicherheitskatalog (nachfolgend IT-SiKat) nach § 11 Abs. 1a EnWG der Bundesnetzagentur (BNetzA) unterziehen.

Die Anforderungen, die dabei zu erfüllen sind, sind detailliert im IT-SiKat aufgeführt. Dazu gehört auch die Umsetzung der Normen DIN EN ISO/IEC 27001:2017-06 (nachfolgend ISO/IEC 27001) und DIN EN ISO/IEC 27019:2020-08 (nachfolgend ISO/IEC 27019) in der jeweils gültigen Fassung. Wie bei jeder Norm gibt es auch hier Übergangsfristen, die einzuhalten sind.

Bis zum 31.12.2020 konnte alternativ für Erst-, Überwachungs- und Rezertifizierungsaudits noch die DIN ISO/IEC TR 27019:2015-3 berücksichtigt werden. Ab dem 01.01.2021 ist jedoch die Anwendung der neuen DIN EN ISO/IEC 27019:2020-08 bzw. der entsprechenden DIN-Norm verpflichtend.

Weiterhin wird durch die BNetzA spezifiziert, dass der Fachexperte, sofern notwendig, mit dem Auditteam vor Ort anwesend sein muss. Als ESecurity-CERT GmbH stellen wir sicher, dass der Fachexperte über die Kompetenzen entlang dem Konformitätsbewertungsprogramm verfügt.

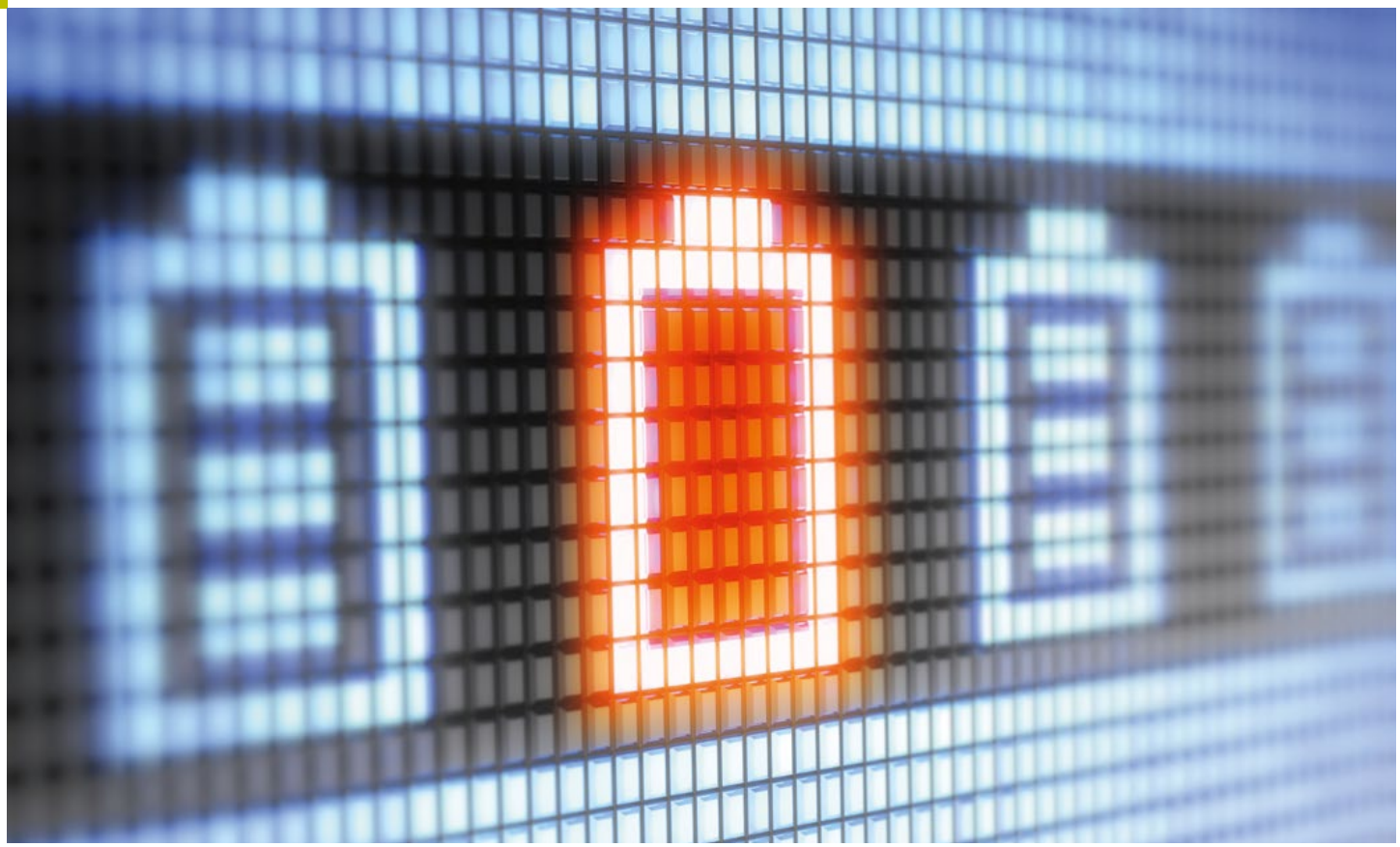
Was ändert sich mit der ISO/IEC 27019:2017?

Durch die neue ISO/IEC 27019 wird eine Herausforderung beseitigt, welche die Umsetzung der ergänzenden Anforderungen in der Vergangenheit etwas erschwert hatte. Die DIN ISO/IEC TR 27019:2015 war gemäß der alten DIN EN ISO/IEC 27002:2005 aufgebaut. Da sich die Struktur der Maßnahmen in der aktuellen Version jedoch geändert hat, musste man mit Hilfe einer Mapping-Tabelle die energiespezifischen Ergänzungen der ISO/IEC 27019 zuordnen. Ein einheitliches Vorgehen konnte nicht sichergestellt werden und verursachte häufig Diskussionen mit den Auditoren.

Bei der aktuellen ISO/IEC 27019 ist eine Mapping-Tabelle nicht mehr relevant. Die Nummerierung der Controls (A.5-A.18) sind nun kompatibel zu den Controls aus dem Annex A der ISO/IEC 27001 und der DIN EN ISO/IEC 27002:2017-06 (nachfolgend ISO/IEC 27002). Dies erleichtert zusätzlich die Darstellung des Statement of Applicability (SoA).

Neu hinzu kommen die sog. ENR-Kontrollen. ENR steht in diesem Fall für „Energy“. Dies betrifft insgesamt 39 Kontrollen, wobei nur bei 13 Änderungen vorgenommen wurden, zu welchen die sogenannten Umsetzungsanleitungen erweitert wurden und im ISMS berücksichtigt werden müssen. Diese verweisen zusätzlich auf den aktuellen „Stand der Technik“. Die tatsächlichen Anpassungen an den Inhalten sind somit sehr gering. Insgesamt sind zwei Maßnahmen zusätzlich zu betrachten, mit Bezug zur ISO/IEC 27002 sowie die 13 Ergänzungen.

Die neue Norm fordert auch, dass von wesentlichen Dienstleistern ein gleichwertiges Sicherheitsniveau nachgewiesen wird. Die Betreiber sind in der Pflicht, dies einzufordern und zu dokumentieren.



Fristverlängerung – Update BNetzA Umsetzung IT-Sikat § 11 Abs. 1b EnWG

Betreiber von Energieanlagen, die nach der BSI-KritisV als Kritische Infrastruktur bestimmt wurden, sind gemäß § 11 Abs. 1b EnWG dazu verpflichtet, den von der Bundesnetzagentur (BNetzA) am 18.12.2018 veröffentlichten IT-Sicherheitskatalog für Energieanlagen umzusetzen. Zum Nachweis der Umsetzung haben Betreiber von Energieanlagen bis zum 31.03.2021 den Abschluss des vorgeschriebenen Zertifizierungsverfahrens anzuzeigen.

Bereits im Dezember 2020 hat die BNetzA darüber informiert, dass es aufgrund der Corona-Pandemie den Energieanlagenbetreibern derzeit nicht möglich ist, das vorgeschriebene Zertifizierungsverfahren durchzuführen. Zusätzlich wurde die BNetzA darüber in Kenntnis gesetzt, dass es aufgrund der aktuellen Lage seitens der Deutschen Akkreditierungsstelle GmbH (DAkkS) noch nicht möglich ist, die für die bevorstehenden Zertifizierungen benötigten Zertifizierungsstellen zu akkreditieren. Auch die geforderten Aufbauschulungen für die Auditoren aus dem Konformitätsbewertungsprogramm konnten zu diesem Zeitpunkt noch nicht angeboten werden. Derzeit gibt es nur wenige von der BNetzA anerkannte Schulungsanbieter, die diese Aufbauschulung anbieten.

Um auf die vorgetragenen Schwierigkeiten angemessen zu reagieren, wird die BNetzA zum Ablauf der Frist am 31.03.2021 lediglich das Erreichen der Zertifizierungsreife, nicht jedoch den Abschluss des geforderten Zertifizierungsverfahrens, verlangen. Es ist daher ausreichend, wenn Betreiber von Energieanlagen gegenüber der BNetzA zum genannten Stichtag eine schriftliche Erklärung abgeben, aus der hervorgeht, dass sie die Anforderungen des IT-Sicherheitskatalogs gemäß § 11 Abs. 1b EnWG in ihrem Haus vollständig umgesetzt haben. Dieser Erklärung ist ein Nachweis über die Beauftragung einer Zertifizierungsstelle und die geplante Terminierung der notwendigen Audits spätestens bis zum 31.10.2021 anstatt dem 30.06.2021 beizufügen. Das Zertifizierungsverfahren selbst muss schnellstmöglich nach Rücksprache mit der beauftragten Zertifizierungsstelle abgeschlossen werden. Die eingereichten Dokumente müssen vom Vertretungsberechtigten des jeweiligen Unternehmens mit Unterschrift bestätigt werden.

Die ESecurity-CERT befindet sich im Akkreditierungsverfahren der DAkkS gemäß IT-Sicherheitskatalogs nach § 11 Abs. 1b EnWG. Unsere Auditoren besitzen bereits die notwendigen Qualifikationen, um entsprechende Audits durchzuführen.

Wir gehen davon aus, dass durch die Lockerungen der aktuellen Corona-Regeln, eine Akkreditierung bis Ende Q4/2021 durch die DAkkS möglich ist.

ANSPRECHPARTNER

HAMBURG

Holger Klindtworth
Tel. +49 40 37097-220
Holger.Klindtworth@ebnerstolz.de

Claudia Stange-Gathmann
CISA, CIA, CISM, QA (DIIR),
ISO/IEC 27001 LA
Tel. +49 40 37097-313
Claudia.Stange@ebnerstolz.de

Ingo Köhne
CISA, CISM, PMP, QAR-IT (DIIR)
Tel. +49 40 37097-315
Ingo.Koehne@ebnerstolz.de

DÜSSELDORF / KÖLN

Christian Wieder
CISA, CRISC
Tel.: +49 211 30143213
Christian.Wieder@ebnerstolz.de

FRANKFURT

Sebastian Adam
CISA, ISO/IEC 27001 LI
Tel. +49 69 1539249-21
Sebastian.Adam@ebnerstolz.de

MÜNCHEN

Mark Alexander Butzke
Wirtschaftsprüfer, Steuerberater, CISA, CRISC,
ISO/IEC 27001 Senior LA
Tel. +49 89 549018-292
Mark.Butzke@ebnerstolz.de

Michael Burkhardt
CISA, CRISC, ISO/IEC 27001 LA
Tel. +49 89 549018-293
Michael.Burkhardt@ebnerstolz.de

STUTTGART

Ralf Körber
Wirtschaftsprüfer, Steuerberater, CISA, CRISC
Tel. +49 711 2049-1378
Ralf.Koerber@ebnerstolz.de

ESECURITY-CERT GMBH

Marc Alexander Luge
CISA, CASA, ISO ISO/IEC 27001 LA,
zus. Prüfverfahrenskompetenz für § 8a Abs. 3
BISG, IT-Sicherheitskatalog §11 Abs. 1a und
1b EnWG
Tel. +49 211 540148-02
Marc.Luge@esecurity-cert.com

Ricky Stewart
ISO/IEC 27001 LA, zus. Prüfverfahrenskom-
petenz für §8a Abs. 3 BISG, IT-Sicherheits-
katalog §11 Abs. 1a und 1b EnWG
Tel. +49 211 540148-05
Ricky.Stewart@esecurity-cert.com

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
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