3. AUSGABE 2019

EBNER STOLZ

novus

INFORMATIONSTECHNOLOGIE

Was lange währt…
Neufassung der GoBD

Das neue Bußgeld-konzept der deutschen Datenschutzbehörden

Sicherheit im Netz – Netzwerksegmentierung

I'll be back – O Captain! My Captain!

Das Jahr 2019 nähert sich mit großen Schritten dem Ende. Lässt man es Revue passieren, kann man feststellen, dass sich vor dem Hintergrund der vielen Neuerungen und Anforderungen in 2019 viele bekannte Filmzitate hervorragend auf die aktuelle Situation für Unternehmen anwenden lassen:

- „Ein Big Mac ist ein Big Mac, aber die nennen ihn Le Big Macke." > DSGVO goes Europe
- „Keep your friends close, but your enemies closer." > Neuerungen in Sachen Tax Compliance und Kassensicherungsverordnung
- „I'm going to make him an offer he can't refuse." > Neufassung der GoBD

2019 ist damit ein Jahr großer Herausforderungen, insb. durch die Umsetzung regulatorischer Anforderungen (seien es bereits akute oder zukünftige) sowie vor dem Hintergrund des Wettbewerbs.

In unserem diesjährigen „Weihnachts-novus" blicken wir noch einmal auf interessante Themen aus den bekannten Bereichen IT & Wirtschaftsprüfung, IT-Recht, IT-Sicherheit und IT-Beratung.

Dazu gehört die kurz vor Weihnachten überraschend veröffentlichte Neufassung der GoBD, welche an die Stelle der Fassung vom 14.11.2014 tritt und ab dem 1.1.2020 gilt. Zudem kommt ESEF, ein Standard zur Erhöhung der Transparenz in der Berichterstattung von Unternehmen, sowie ein Blick in die Zukunft der Inventuraufnahme mittels Drohnen.

Im IT-Rechtsbereich blicken wir auf Maßnahmen zur Geheimhaltung von Geschäftsgeheimnissen im Rahmen des 2019 veröffentlichten Geschäftsgeheimnisgesetzes sowie das neue Bußgeldkonzept der deutschen Datenschutzbehörden aus Oktober.

Ein Themenschwerpunkt liegt aber insbesondere auf der IT-Sicherheit, u. a. mit einem kurzen Update zur Umsetzung von Tiber-EU (s. dazu bereits novus IT 2. Ausgabe 2019), dem Einsatz von Office 365 und einhergehenden Vorteilen und Herausforderungen, unserem Abschlussartikel zu unserer in der ersten Ausgabe diesen Jahres gestarteten Reihe zum Notfallmanagement sowie einem Thema, was auch 2019 und folgende Jahre noch viele Unternehmen beschäftigen wird, da dies weiterhin nicht vollständig umgesetzt ist: Netzwerksegmentierung.

Der Geschäftsbereich IT-Revision möchte sich bei all seinen Freunden und Geschäftspartnern für ein produktives und gutes Miteinander, für das entgegengebrachte Vertrauen und die Treue sowie die angenehme Zusammenarbeit im zurückliegenden Jahr bedanken.

Wir wünschen Ihnen, Ihren Familien und Angehörigen ein frohes und gesegnetes Weihnachtsfest, Gesundheit verbunden mit Glück, Freude und Erfolg in 2020!

„You don't know the power of the dark side"
Ihr GBIT

ESecurity-CERT GmbH

Der Wettbewerbsmarkt und die Regulatorien, Mitbewerber, Kunden sowie der Gesetzgeber aber auch das eigene Risikobewusstsein führen dazu, dass Sie als Unternehmen sich verstärkt den umfassenden Anforderungen zur Informationssicherheit stellen müssen. Die erfolgreiche Umsetzung lässt sich dabei insbesondere durch Zertifizierungen nachweisen.

Es stellt sich die Frage: Wie belege ich die Qualität der Maßnahmen zur Informationssicherheit nachvollziehbar? Zertifizierungsstellen für einzelne Standards gibt es viele. Zertifizierungsstellen, die sich im Verbund umfänglich mit IT-Compliance beschäftigen und damit die jeweils passende Lösung anbieten können, gibt es wenige.

In diesem Zusammenhang möchten wir unsere ESecurity-CERT GmbH vorstellen. Die ESecurity-CERT ist im Ebner Stolz-Verbund die unabhängige Zertifizierungsstelle. Sie führt gegenwärtig Zertifizierungsprüfungen von Managementsystemen in Form von Konformitätsbewertungen auf dem Gebiet der Informationssicherheit durch.

Zertifizierungsdienstleistungen aus einer Hand

In Verbindung mit unserer Spezialabteilung „Managementsysteme Compliance" des Geschäftsbereichs IT-Revision (GBIT) bei Ebner Stolz mit Erfahrungen aus vielen Implementierungsprojekten zu den unterschiedlichsten Normenanforderungen in den letzten Jahren, können wir Ihnen Zertifizierungsdienstleistungen direkt aus einer Hand anbieten.

Hierbei bildet die ESecurity-CERT die folgenden Bereiche ab, die nur von einer bei der Deutsche Akkreditierungsstelle GmbH (DAkkS) akkreditierten Stelle rechtskräftig zertifiziert werden können:

- Zertifizierung gemäß DIN EN ISO/IEC 27001:2017-06 bzw. gemäß ISO 27001:2013 (nativ)
- KRITIS-Prüfungen gemäß § 8a Abs. 3 BSIG für Betreiber kritischer Infrastrukturen
- Zertifizierung nach IT-Sicherheitskatalog gemäß § 11 ABS. 1A ENWG
- Auditierung nach ISO 27001 auf Basis von IT-Grundschutz

Weitere Zertifizierungsangebote sind nach gesetzlicher Konkretisierung in Vorbereitung (bspw. DSGVO/Datenschutz, Kassensysteme).

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 System zur Absicherung der Informationssicherheit in der Organisation zu sehen. Es wird hierbei nicht nur auf die IT Sicherheit abgestellt.

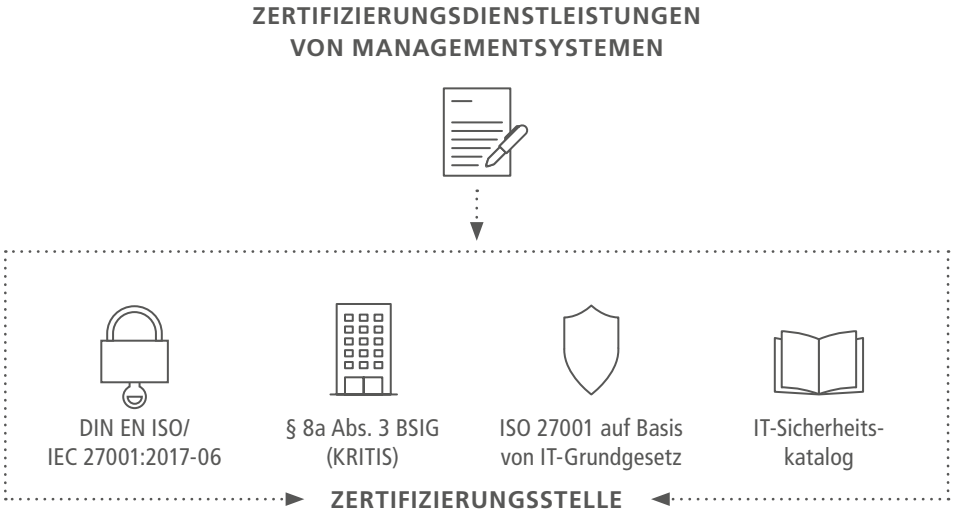
Jedes **Zertifizierungsverfahren** besteht aus **vier Phasen**:

- Erstzertifizierung
- 1. Überwachungsaudit (zehn Monate nach Abschluss der Stage-2 Prüfung bei Erstzertifizierung)
- 2. Überwachungsaudit (zwölf Monate nach dem ersten Überwachungsaudit)
- Rezertifizierung (drei Jahre nach der Erstzertifizierung)

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, welches wir im Folgenden unter Erst-/Rezertifizierung darstellen. Aufbauend darauf erfolgt die Entscheidung über die Zertifizierung.

Durch das jährliche Überwachungsaudit, das im Jahr 2 und 3 erfolgt, wird sichergestellt, dass das ISMS während der gesamten Gültigkeitsdauer des Zertifikates aufrechterhalten wird. Der Prüfungsumfang ist hierbei deutlich geringer als der im Rahmen des Zertifizierungsaudits angesetzten.



AUSSTELLUNG DES ZERTIFIKATS

NEUBEGINN DES ZERTIFIZIERUNGSZYKLUS

ÜBERWACHUNGSAUDIT
Das erste findet zehn Monate nach dem Abschluss der Stufe 2 und danach alle zwölf Monate (bzw. sechs Monate) statt

REZERTIFIZIERUNG
Drei Monate, bevor sich Ihr Zertifikat zum dritten Mal jährt, werden wir Sie für ein erneutes Audit besuchen

ABWEICHUNGEN
Diese werden während der Überwachungsaudits herausgestellt und müssen auf die gleiche Weise beseitigt werden, wie bei einem Audit in Stufe 2

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 nicht so umfassend wie bei der Erstzertifizierung.

Die ESecurity-CERT setzt dabei auf ein mehrstufiges Verfahren. Im ersten Schritt prüft der (Lead) Auditor die Konformität eines ISMS gegen das Regelwerk und fertigt einen Report an. Dieser wird in einer weiteren Stufe durch die ESecurity-CERT geprüft, um eine Vergleichbarkeit zwischen den einzelnen Audits sicherstellen zu können.

- Erst-/Rezertifizierung

- Stage 1-Prüfung (Aufbauprüfung)
  - Grundlegende Beurteilung und Würdigung des Geltungsbereiches
  - Durchsicht und Bewertung des Managementhandbuches sowie der erweiterten Systemdokumentationen
  - Beurteilung der grundsätzlichen Anforderungserfüllung
  - Ermittlung der grundlegenden Prüfungsbereitschaft im Hinblick auf den nächsten Schritt (Funktionsprüfung) und ggf. Aufzeigen von Handlungsbedarf
  - Ableitung des individuellen Auditplans für die Stage 2-Prüfung

- Stage 2-Prüfung (Funktionsprüfung)
  - Prozessorientierte Prüfung und Beurteilung des Managementsystems auf Anforderungserfüllung unter Berücksichtigung der entsprechenden Infrastruktur und Applikationsobjekte
  - Prüfung erfolgt vor Ort an den vorgesehenen Standorten
  - Erstellung eines Auditberichtes

- Zertifikatsverwaltung (Laufzeit von drei Jahren)
  - Zertifikatserstellung
  - Nutzung des Zertifikates für eigene Werbezwecke
  - Veröffentlichung des Zertifikates im Internet
  - ggf. Ausstellung von Zertifikatskopien (optional)

Ansprechpartner

Als Ansprechpartner stehen Ihnen der Geschäftsführer der ESecurity-CERT GmbH, Herr Gerd Niehuis, sowie Herr Marc Alexander Luge zur Verfügung.

Gerd Niehuis
Lead Auditor ISO 27001 (nativ)/EnWg,
Prüfer § 8a (3) BSIG
Auditor
Tel. +49 211 540148-01
Gerd.Niehuis@esecurity-cert.com

Marc Alexander Luge
CISA, CASA
ISO/IEC 27001 Lead Auditor
Tel. +49 211 540148-02
Marc.Luge@esecurity-cert.com

Alles Gute bringt der Januar – ESEF

Bereits Ende 2018 hat die Europäische Kommission die delegierte Verordnung „zur Ergänzung der technischen Regulierungsstandards für die Spezifikation eines einheitlichen elektronischen Berichtsformats" erlassen. Am 29.5.2019 ist die Verordnung im Amtsblatt (S. L143/1 ff.) der Europäischen Union veröffentlicht worden. Mit der Veröffentlichung wirkt sie mittelbar für alle Mitgliedsstaaten und muss nicht in nationales Recht umgesetzt werden. Durch die neue Verordnung soll das European Single Electronic Format (ESEF) eingeführt werden, welches die Transparenz in der Berichterstattung von Unternehmen durch ein einheitliches elektronisches Berichtsformat weiter erhöhen soll. Zudem soll durch ESEF die Zugänglichkeit und Analyse von Jahresfinanzberichten erleichtert werden, da dieser ein einheitliches Design, eine einheitliche Reihenfolge und weitere einheitliche Standards vereint.

ESEF ist erstmals auf Finanzberichte anzuwenden, deren Geschäftsjahr nach dem 31.12.2019 beginnt. Ab diesem Zeitpunkt müssen alle Jahresfinanzberichte – also Jahres- wie auch Konzernabschlüsse deutscher am Kapitalmarkt notierter Unternehmen – diesem neuen Standard entsprechen. Dieses Format sieht eine einzige Datei vor, die den Jahresabschluss, den Lagebericht und die Erklärung der im Unternehmen verantwortlichen Personen enthält.

Betroffen von dieser Verordnung sind rund 7.500 Unternehmen in der EU. In Deutschland sind zunächst die Unternehmen betroffen, die nach § 114 Abs. 1 Satz 1 WpHG einen Jahresfinanzbericht erstellen müssen und dem Enforcement unterliegen. Dies betrifft rund 550 Unternehmen.

Analysten, Banken und Ratingagenturen können mit dem EU-einheitlichen Berichtsformat künftig eine Vielzahl von Konzernabschlüssen unterschiedlicher Emittenten verarbeiten, ohne die Daten vorher aufwendig manuell aufbereiten zu müssen. Auch müssen sie noch nicht einmal die Sprache beherrschen, in der der Finanzbericht erstellt wurde. Ziel der ESEF ist es, die Digitalisierung der Unternehmensberichterstattung weiter voranzutreiben sowie die Vereinfachung der Berichterstattung und Erhöhung der Transparenz und damit eine erleichterte Zugänglichkeit, Analyse und Vergleichbarkeit von Jahresfinanzberichten zu schaffen. Befürchtet wird jedoch, dass der neue Berichtstandard für Unternehmen keinen Mehrwert für ihre Kapitalmarktkommunikation, sondern lediglich Mehraufwand in der Jahresberichtserstellung mit sich bringt.

XHTML als Grundalge des neuen Berichtsformates

Der neue Standard sieht vor, dass Jahresfinanzberichte im eXtensible Hypertext Markup Language (XHTML)-Format veröffentlicht werden. Das bisher von vielen Unternehmen zur Veröffentlichung der Berichte genutzte unstrukturierte und nicht maschinenlesbare PDF-Berichtsformat wird in Zukunft nicht mehr ausreichen.

XHTML ist eine textbasierte Auszeichnungssprache zur Strukturierung und semantischen Auszeichnung („Etikettierung") von Inhalten (Bilder, Texte, Hyperlinks) in Dokumenten. XHTML kombiniert Stärken von HTML (Hypertext Markup Language) und XML (Extensible Markup Language) und ist eine Neuformulierung von HTML 4.01 in XHTML. XHTML-Dokumente genügen also den Syntaxregeln von XML. XHTML-Dateien sind, im Vergleich zu PDF-Dateien, mit einem gängigen Internetbrowser wie Mozilla Firefox aufrufbar. Die Veröffentlichung des Jahresabschlussberichtes in einem XHTML-Format wird verpflichtend. Eine reine Druckversion reicht nicht mehr aus. Da die Publizität weiterhin über den elektronischen Bundesanzeiger erfolgen soll, ist davon auszugehen, dass dieser nur noch das XHTML-Format akzeptieren wird.

Tagging als Erweiterung des neuen Berichtsformates

Börsennotierte Unternehmen, die einen IFRS-Konzernabschluss erstellen, müssen neben dem XHTML-Format zudem noch die Informationen aus Bilanz, GuV, Eigenkapitalspiegel und Kapitalflussrechnung mittels des XBRL (Extensible Business Reporting Language)-Standards etikettieren. Die weiteren Angaben im Anhang müssen erst ab den Geschäftsjahren beginnend ab dem 1.1.2022 gekennzeichnet werden. Bis dahin darf der Anhang im Block getagged werden. D. h. bis zu Beginn des Geschäftsjahres 2022 muss nicht jede erwähnte Zahl einzeln getagged werden. Die zu taggenden Informationen sind gemäß der ESMA-Festlegung auf Basis der IFRS Taxonomie festgelegt.

XBRL ist eine auf XML basierende Sprache, mit der elektronische Dokumente im Bereich der Finanzberichtserstattung erstellt werden. XBRL definiert jedoch keine neuen Rechnungslegungsvorschriften. Sie bildet lediglich die bestehenden Rechnungslegungsvorschriften ab, bspw. die nach HGB oder IFRS. ESMA hat bereits konkrete Details zur Umsetzung dieses XBRL veröffentlicht. Anstatt des XBRL-Formates soll das erweiterte Inline XBRL (iXBRL), ein in HTML eingebettetes XBRL, verwendet werden. Dieses hat gegenüber XBRL den Vorteil, dass der Bericht mit jedem Web-Browser geöffnet werden kann.

ESMA hat eine ESEF-Taxonomie (sog. Basis-Taxonomie) erstellt, welche im Wesentlichen der IFRS-Taxonomie entspricht. Diese ESEF-Basis-Taxonomie stellt hierbei eine Etikettenliste dar, die als Grundlage des Taggings verwendet werden kann. Diese wurde als Anhang der delegierten Verordnung veröffentlicht. Der Grundsatz der Etikettierung ist dabei, dass eine Abschlussinformation mit dem Element der ESEF-Basistaxonomie zu markieren ist, das der rechnungslegungsbezogenen Bedeutung der Information am nächsten kommt. Falls mehrere Taxonomie-Elemente infrage kommen, ist dasjenige auszuwählen, welches den engsten Anwendungsbereich zu dem jeweiligen Element hat. Sollte eine Markierung nicht in den Rahmen der Basistaxonomie fallen, muss der entsprechende Anwender/das jeweilige Unternehmen die Basistaxonomie unternehmensindividuell erweitern Diese Erweiterung ist durch Schaffung von sog. „Extensions" möglich. Diese Extension darf

- jedoch nicht einem Element der Basistaxonomie entsprechen und
- muss den Unternehmensnamen sicherstellen,
- die Bezeichnung muss der rechnungslegungsbezogenen Bedeutung entsprechen und

- die neu geschaffene Erweiterung muss in die hierarchische Struktur eingeordnet werden,

um die Beziehung zu den bestehenden Elementen deutlich zu machen. Diese Basistaxonomie muss jedoch nicht angewendet werden. Die Mitgliedsstaaten können auch eigene Taxonomien herausbringen, die als Grundlage zur Einhaltung des ESEF dienen.

Auswirkungen auf Unternehmen

Betroffene Konzerne, die nach IFRS konsolidieren, müssen eine neue Berichtsstrategie entwickeln. Das neue Berichtsformat und das verpflichtende Tagging nach IFRS bedeutet für viele Unternehmen einen großen Aufwand. Es muss eine iXBRL-kompatible Softwarelösung implementiert werden, die das neue Berichtsformat unterstützt und entsprechende Berichte umsetzen kann.

Neben der Entwicklung der neuen Berichtsstrategie ist ebenfalls die Implementierung neuer Schnittstellen notwendig. Diese Schnittstellen werden sowohl interner als auch externer Form sein. Interne Schnittstellen stellen hier vor allem die Schnittstellen innerhalb des konzernweiten Konsolidierungssystems dar. Eine externe Schnittstelle stellt hierbei die Übermittlung an den Bundesanzeiger dar.

Eine kleine Erleichterung für Unternehmen besteht lediglich darin, dass die umfangreichen Anhang-Angaben erst ab 2022 getagged werden müssen, da zunächst erst einmal die primären Abschlussbestandteile von Konzernabschlüssen nach IFRS vom Tagging nach iXBRL betroffen sind. Wichtig hier, dass neben dem reinen Zahlenwerk auch die „Notes" ab 2020 entsprechend auswertbar im XHTML gemeldet werden.

Auch eine Prüfungspflicht im Hinblick auf die Einhaltung der technischen Vorgaben und der richtigen Adaption der Taxonomie auf den IFRS-Konzernabschluss ist keineswegs auszuschließen. Die Einrichtung des Digitalformats sollte daher unbedingt in enger Abstimmung mit dem Abschlussprüfer in Angriff genommen werden.

Eine Möglichkeit zur Einführung von ESEF bietet der unten abgebildete Ansatz.

Initiale und regelmäßige Anpassungen

Bei der Berichterstattung müssen, neben den nach IFRS verpflichtenden Berichtsteilen, teils auch erweiterte, für das jeweilige Unternehmen verpflichtende Berichtserstattungspunkte erfüllt werden. Es müssen somit, neben der Basistaxonomie nach IFRS, noch Erweiterungstaxonomien erstellt und mit der Basistaxonomie verknüpft werden. Dies muss in der jeweils ausgewählten Software initial und in der genannten Trennung definiert werden. Bei dem Tagging der Berichte werden dann auf Basis der vorher definierten Taxonomie die einzelnen Berichtsbestandteile ausgezeichnet. Aufgrund der regelmäßigen Änderungen der IFRS besteht fortlaufend die Pflicht zur Anpassung der Taxonomie. Zudem müssen neue Schnittstellen eingerichtet werden, damit das neue Berichtsformat innerhalb des Konzerns und an externe Stellen übertragen werden kann.

Unterstützung durch die ESMA

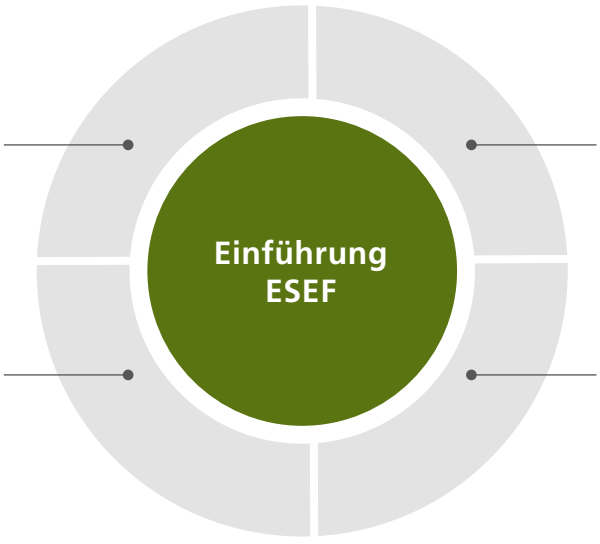
Um die neuen Vorschriften optimal umsetzen zu können, hat die europäische Wertpapier- und Marktaufsichtsbehörde (European Securities and Markets Authority, ESMA) zur Unterstützung ein ESEF-Berichtshandbuch und ESEF-Taxonomie-Dateien erstellt. Diese neuen Bestimmungen werden jährlich überarbeitet, um mögliche Aktualisierungen der Taxonomie der von der EU übernommenen International Financial Reporting Standards zu berücksichtigen. Das Berichtshandbuch und die Taxonomie-Dateien sind über die Homepage der ESMA (https://www.esma.europa.eu) abrufbar.

4. VORBEREITUNG UND HERSTELLUNG

› Überleitungsmethodik auf bestehende Konten anwenden
› Archivierung und Übermittlung der Datei (Übertragungsprotokolle) an Unternehmensregister (OAM Deutschland) bzw. neuen European Access Point (EEAP)
› Veröffentlichung im Internet

3. ANPASSUNGEN IM SYSTEM UND AM PROZESS

› Überleitungsmethodik system- und prozessseitig anpassen (Taxonomie)
› Festlegung Taxonomieupdateprozess
› ggf. Softwareauswahlprozess oder Anpassung bestehender Systeme
› Anpassung von Richtlinien/internen Dokumenten



1. FESTLEGUNG STANDARDS IM REPORTING

› Definition der zukünftigen Berichtsformate (PDF, XHTML/IXBRL etc.) für Monats-, Quartals- und Jahresberichte
› Defintion Verwaltungsprozesse mit Aufgabenverteilung, Prüfung und Freigabe

2. AUSWIRKUNGSANALYSE

› Testweises Mapping auf die IFRS Taxonomie
› Benchmark
› Kontenmapping auf- und vorbereiten
› Definition Überleitungsmethodik und Taxonomiestufen

Die Drohne ist die Zukunft – Zur Ordnungsmäßigkeit der Drohneninventur

Eine ordnungsgemäße Inventur bedeutet trotz fortschreitender Automatisierung und Digitalisierung immer noch eine nicht unerhebliche Belastung für viele Unternehmen. Zwar hat sich der Zeitaufwand von Inventuren durch die Einführung von tragbaren Barcode-Scannern und anderen mobilen Datenerfassungsgeräten (MDE-Geräte) sowie ausgefeilter Software bereits beträchtlich verringert. Jedoch sind Inventuren in Unternehmen gerade mit großen und heterogenen Lagerbeständen jedes Jahr wieder eine planerische und finanzielle Herausforderung – und das unabhängig vom Lagerhaltungsprinzip. Doch es wäre nicht das Zeitalter von „Industrie 4.0", wenn nicht bereits diverse Ansätze zur Optimierung bestünden.

Bereits in anderen Bereichen der Logistik hat sich gezeigt, dass der Einsatz von Drohnen die Branche verändern kann. Was liegt hier – technologisch und zeitlich – näher, als die Idee, mit Hilfe von Drohnen eine Inventur durchzuführen. Abseits der technischen Voraussetzungen, insbesondere in der Sensorik, müssen jedoch, wie bei jeder anderen Inventur, bestimmte Voraussetzungen erfüllt und diverse Regelungen eingehalten werden.

Voraussetzungen für die Drohneninventur

Genau wie Einzelbuchungen in den Hauptbüchern unterliegt auch die Inventur den Grundsätzen der ordnungsmäßigen Buchführung (GoB bzw. steuerlich GoBD) – im Speziellen den Grundsätzen der ordnungsmäßigen Inventur (GoI). Dabei sind folgende Kriterien einzuhalten:

- Vollständigkeit,
- Richtigkeit,
- Zeitgerechtigkeit,
- Ordnung,
- Nachvollziehbarkeit,
- Unveränderlichkeit und Wirtschaftlichkeit.

In den meisten Fällen werden diese Kriterien heutzutage durch Software forciert, welche im Rahmen der Erfassung nur einen geringen Fehlerspielraum zulassen. So werden viele Daten – bspw. das Erfassungsdatum, der Benutzer und die erfasste Ware – automatisch eingetragen und durch das verwendete MDE-Gerät automatisiert an eine zentrale, nicht veränderbare Datenbank oder direkt in das ERP-System übermittelt. Dabei melden Kontrollmechanismen bereits in dieser Phase Abweichungen zum Soll-Zustand direkt an den Erfasser, so dass noch vor der endgültigen Festschreibung überprüft werden kann, ob alle relevanten Bestände erfasst wurden.

The Next Big Thing

Doch was wäre, wenn sich der Scanner allein durch das Lager bewegen würde mit nur einer sehr geringen inventurbedingten Beeinträchtigung des laufenden Betriebs?

Diesen Ansatz verfolgen neben dem Massachusetts Institute of Technology (MIT) auch diverse Start-ups und Universitäten. Eine beindruckende Lösung, die wir auf unserer Mandantenveranstaltung des Geschäftsbereichs IT-Revision (GBIT) vorgestellt haben, kommt z. B. von der doks.Innovation GmbH in Kassel.

Die Idee ist einfach: Eine Drohne bewegt sich in der Regel außerhalb der Betriebszeiten des Lagers durch die Regalreihen und erfasst die Bestände. Dies kann über ein eingebautes

MDE-Gerät oder eine vollständige visuelle Aufzeichnung („Video des Flugweges“) und spätere Verarbeitung der Bilder erfolgen. Das Zählen erfolgt über die Verarbeitung des Barcodes direkt mit dem eingebauten MDE Gerät oder über die spätere Auswertung der Bildinformationen. Gerade bei chaotischer Lagerhaltung oder großen Lagerflächen mit heterogenen Lagergütern (wie z. B. im Baustoffhandel) ist diese Art der Datenerfassung von Vorteil.

Dabei erfolgt die Navigation der fliegenden Helfer vollautonom – die Software der Drohnen erfasst die dreidimensionale Struktur des Lagerhauses in Eigenregie, so dass kein fester Flugpfad vorgegeben werden muss und auch Veränderungen im Regalaufbau oder bei der Lagerstruktur ohne Weiteres erfolgen können. Die erfassten Daten werden entweder kontinuierlich oder als größere Pakete an eine zentrale Datenbank übertragen und dort mit dem Soll-Zustand verglichen. Bei Abweichungen wird dann z. B. ein Mitarbeiter informiert, der sowohl den Soll- als auch den Ist-Zustand auf Korrektheit überprüft.

Dies bedeutet, dass der Arbeitsaufwand der Mitarbeiter auf die Nachkontrolle sowie das Auffinden von fehlenden Beständen reduziert wird (das Auffinden kann natürlich auch ggf. durch einen „Drohnensucheinsatz“ erfolgen – indem die Drohne im Lager den fehlenden Artikel sucht), während die Drohnen auf Kundenwunsch gleichzeitig noch zusätzliche Daten wie Feuchtigkeit, Temperatur und der Zustand der Verpackungen miterfassen können, ohne dass dabei weiterer Aufwand entstünde.

Bei dieser Möglichkeit zur Automatisierung bietet sich gleichzeitig der Wechsel von der Stichtags- zur kontinuierlichen Inventur an. Dadurch werden Diskrepanzen in den Lagerbeständen nicht erst nach Monaten, sondern innerhalb von wenigen Tagen oder sogar Stunden offensichtlich und können entsprechend untersucht werden.

Technische Umsetzung: Anforderungen an Mensch und Maschine

Auf der technischen Seite gibt es mehrere Ansätze, die alle demselben grundlegenden Prinzip folgen: Ein Fluggerät – meist ein Quadrocopter – mit unterschiedlich vielen Sensoren zur Navigation, Umgebungs- und Datenerfassung wird auf einem entweder vorprogrammierten oder autonom anpassbaren Pfad durch das Lager gesteuert und erfasst dort die vorhandenen Waren und Leerstände in den Regalen. Dabei können entweder klassische Bar- oder QR-Codes erfasst werden.

Bei der Erfassung durch rein optische Systeme muss dementsprechend darauf geachtet werden, dass die maschinenlesbaren Codes sichtbar gelagert werden.

Die Drohne als Zukunft?

Grundsätzlich stellen wir fest, dass der Automatisierung die Zukunft gehört. Das Potenzial zur Kosteneinsparung bei gleichzeitig kürzeren Intervallen zwischen Inventuren – potenziell täglich – ist zu hoch, als profitorientierte Unternehmen es ignorieren könnten. Hinreichend große bzw. umsatzstarke Lager wären jedoch weiterhin mit einer vollautomatischen Lagerhauslösung besser beraten, da sie zwar anfänglich teurer ist, jedoch langfristig Personal und damit Geld einspart und eine Echtzeitüberwachung der Bestände ermöglicht.

Das wird jeder begrüßen der bei Minusgraden eine Inventur in einem Außenlager im Winter durchgeführt oder beobachtet hat.

Pauschal ist kein Grund ersichtlich, der einer ordnungsmäßigen, drohnengestützten Inventur entgegensteht. Jedoch muss im Einzelfall geprüft werden, ob die eingesetzte Hard- und Software den Ansprüchen der GoB gerecht wird. Hier hilft eine Bescheinigung zur GoB-Tauglichkeit der am Markt verfügbaren Lösungen, um sicherzustellen, dass das angebotene System die nötigen Voraussetzungen mit sich bringt.

Was lange währt…Neufassung der GoBD

Bereits mit Schreiben vom 14.11.2014 äußerte sich das BMF umfassend zu den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD). Da die technischen Möglichkeiten seit 2014 enorm zugenommen haben, entsprachen die GoBD an vereinzelten Stellen nicht mehr dem aktuellen Status. Dies hat auch die Finanzverwaltung erkannt und im November 2018 einen Entwurf zur Neufassung der GoBD vorgestellt.

So schnell die Neufassung der GoBD am 11.7.2019 veröffentlicht wurde, so schnell wurde diese im August 2019 auch wieder von der Internetpräsenz des Bundesfinanzministeriums (BMF) entfernt. Am 28.11.2019 erfolgte nun ohne große (Vor-)Ankündigung die Veröffentlichung der Neufassung der GoBD, welche an die Stelle der Fassung vom 14.11.2014 tritt und ab dem 1.1.2020 gilt. In der Entwurfsfassung aus 2018 sowie der Neufassung aus Juli 2019 wurden insbesondere nachfolgend aufgeführte Themen verändert, welche auch in der nun veröffentlichten und gültigen Fassung aus November 2019 so übernommen wurden.

- Speichermedium Cloud (Rz.20)
- Digitalisierung von Dokumenten (Rz.130 / 140)
- Konvertierung und Aufbewahrung (Rz.135)
- Ersetzendes Scannen und Buchführung im Ausland (Rz.136)
- Einzelaufzeichnungspflicht / Vollständigkeit der Aufzeichnungen (Rz.39)
- Periodenweise Verbuchung (Rz.50)
- Erfassungsgerechte Aufbereitung der Buchungsbelege (Rz.76).

Speichermedium Cloud

Im Vergleich zu dem vorgehenden Schreiben aus 2014 wird u. a. die Definition von Datenverarbeitungs- und Ablagesystemen ergänzt. Demnach ist es unerheblich, ob die Systeme als eigene Hard- bzw. Software genutzt oder in einer Cloud bzw. als eine Kombination dieser Systeme betrieben werden (Rz. 20). Das Cloudsystem als Speichermedium sowie als Bearbeitungs- und Ablagetool zählt somit fortan als anerkanntes System für Haupt-, Vor- und Nebensysteme. Entscheidend ist der Standort des Cloud-Servers. Befindet sich dieser im Ausland, ist eine Genehmigung zur Aufbewahrung von Buchführungsunterlagen im Ausland gemäß §146 Abs. 2a AO erforderlich.

Digitalisierung von Dokumenten

Zur elektronischen Aufbewahrung von Buchungsbelegen in Papierform führt das BMF ergänzend aus, dass eine elektronisch bildliche Erfassung, z. B. durch Scannen oder Fotografieren, zulässig ist. Dies kann mit verschiedenen Geräten, z. B. Smartphones, Multifunktionsgeräten oder Scan-Straßen, erfolgen (Rz. 130), sofern die weiteren Anforderungen an die GoBD eingehalten werden. Nach dem bildlichen Erfassen dürfen die Dokumente entsprechend Rz. 140 der GoBD vernichtet werden, sofern sie nicht nach außersteuerlichen oder steuerlichen Vorschriften im Original aufzubewahren sind.

Konvertierung und Aufbewahrung

Unter bestimmten Voraussetzungen ist die Aufbewahrung einer Konvertierung ausreichend und es bedarf nicht weiter der Aufbewahrung der Ursprungsversion (Rz. 135). Dies setzt voraus, dass

- keine bildlichen oder inhaltlichen Veränderungen bei der Konvertierung vorgenommen wurden,
- keine aufbewahrungspflichtigen Informationen bei der Konvertierung verloren gegangen sind,
- die Umwandlung in einer Verfahrensdokumentation festgehalten und somit nachvollziehbar ist und
- die maschinelle Auswertung durch die Konvertierung nicht beeinträchtigt wird.

Ersetzendes Scannen und Buchführung im Ausland

Sind Belege im Ausland entstanden oder wurden sie dort empfangen, z. B. im Rahmen einer Dienstreise im Ausland, können diese aus Vereinfachungsgründen dort direkt durch mobile Geräte bildlich erfasst werden. § 146 Abs. 2 AO, wonach die Aufzeichnungen im Inland zu führen und aufzubewahren sind, steht dem nicht entgegen (Rz. 136). Wichtig ist auch hier analog zu Rz.130, dass die weiteren Anforderungen an die GoBD eingehalten werden.

Einzelaufzeichnungspflicht

Zudem wurde der Grundsatz der Einzelaufzeichnungspflicht ergänzt (Rz. 39). Beim Verkauf von Waren an eine Vielzahl von unbekannten Personen gegen Barzahlung gilt die Befreiung von der Einzelaufzeichnungspflicht lediglich, wenn kein elektronisches Aufzeichnungssystem eingesetzt wird. Sofern ein elektronisches Aufzeichnungssystem verwendet wird, gilt die Einzelaufzeichnungspflicht nach § 146 Abs. 1 AO unabhängig davon, ob das System mit einer zertifizierten technischen Sicherheitseinrichtung zu schützen ist oder nicht. Die Zumutbarkeitsüberlegungen sind grundsätzlich auch auf Dienstleistungen übertragbar. Dies ist insbesondere auch für jene Unternehmen relevant, welche von dem „Kassengesetz" in Verbindung mit der Kassensicherungsverordnung betroffen sind. Nach den GoBD sind Ausnahmefälle möglich, „wenn es technisch, betriebswirtschaftlich und praktisch unmöglich ist, die einzelnen Geschäftsvorfälle aufzuzeichnen."

Periodenweise Verbuchung

Weiter wurden die Voraussetzungen für die periodenweise Verbuchung präzisiert (Rz. 50). Werden Geschäftsvorfälle oder Aufzeichnungen nicht laufend, sondern periodenweise gebucht bzw. erstellt, ist dies unter folgenden Voraussetzungen nicht zu beanstanden:

- Die Geschäftsvorfälle werden vorher zeitnah (bare Geschäftsvorfälle täglich, unbare innerhalb von zehn Tagen) in Grund(buch)-aufzeichnungen oder Grundbüchern fest-

gehalten und es ist sichergestellt, dass die Unterlagen bis zur Erfassung nicht verloren gehen. Dies kann durch eine laufende Nummerierung der eingehenden und ausgehenden Rechnungen, durch Ablage in besonderen Ordnern oder durch elektronische Aufzeichnungen in Kassensystemen, Warenwirtschaftssystemen, Fakturierungssystemen usw. gewährleistet werden.

- die Vollständigkeit der Geschäftsvorfälle wird im Einzelfall gewährleitet und
- es wurde zeitnah eine Zuordnung (Kontierung, mindestens aber die Zuordnung betrieblich/privat, Ordnungskriterium für die Ablage) vorgenommen.

Erfassungsgerechte Aufbereitung der Buchungsbelege

Zur erfassungsgerechten Aufbereitung von Buchungsbelegen führt das BMF aus, dass bei Buchungsbelegen die Aufbewahrung lediglich der tatsächlich weiterverarbeiteten Formate, d. h. buchungsbegründende Belege, ausreichend ist, sofern diese über „die höchste maschinelle Auswertbarkeit" verfügen. Weitere bildhafte Urschriften müssen in diesem Fall nicht aufbewahrt werden. Dies gilt entsprechend, wenn mehrere elektronische Datensätze ohne bildhaften Beleg ausgestellt werden und für elektronische Meldungen (z. B. monatlicher Kontoauszug im CSV-Format oder als XML-File), für die inhaltsgleiche bildhafte Dokumente, z. B. in Papierform, zusätzlich bereitgestellt werden (Rz. 76).

Bei Einsatz eines Fakturierungsprogramms muss unter Berücksichtigung der vorgenannten Voraussetzungen keine bildhafte Kopie der Ausgangsrechnung, beispielsweise als PDF-Datei, gespeichert bzw. aufbewahrt werden, wenn jederzeit ein entsprechendes Doppel der Ausgangsrechnung aus dem System erstellt werden kann. Dazu sind folgende Voraussetzungen zu erfüllen:

- Entsprechende Stammdaten (z. B. Debitoren, Warenwirtschaft etc.) werden laufend historisiert.
- AGB werden ebenfalls historisiert und aus der Verfahrensdokumentation ist ersichtlich, welche AGB bei Erstellung der Originalrechnung verwendet wurden.
- Originallayout des verwendeten Geschäftsbogens wird als Muster (Layer) gespeichert und bei Änderungen historisiert. Zudem ist aus der Verfahrensdokumentation ersichtlich, welches Format bei Erstellung der Originalrechnung verwendet wurde (idealerweise kann bei Ausdruck oder Lesbarmachung des Rechnungsdoppels dieses Originallayout verwendet werden).
- Weiterhin sind die Daten des Fakturierungsprogramms in maschinell auswertbarer Form und unveränderbar aufzubewahren.

Weitere Änderungen – insbesondere auch im Vergleich zu der Entwurfsfassung aus Juli 2019 – betreffen u.a:

- Ausnahme für Kleinstunternehmen (Rz. 15), die ihren Gewinn durch Einnahmen-Überschussrechnung ermitteln (bis 17.500 Euro Jahresumsatz). Im Rahmen dessen ist die Erfüllung der Anforderungen regelmäßig mit Bezug zur Unternehmensgröße zu bewerten.
- Die Ordnungsmäßigkeit der Buchungen (Rz. 55); dies bedeutet, dass eine kurzzeitige gemeinsame Erfassung barer/unbarer Tagesgeschäfte möglich ist, sofern die unbaren Umsätze gesondert kenntlich gemacht sind sowie nachvollziehbar aus dem Kassenbuch auf ein gesondertes Konto übertragen werden.
- Die Erfüllung der Belegfunktion (Rz. 64) dahingehend, dass Korrektur- bzw. Stornobuchungen auf die ursprüngliche Buchung rückbeziehbar sein müssen (was in einer ordnungsgemäßen Buchhaltung selbstredend sein sollte).
- Die Belegsicherung (Rz. 68) kann nicht mehr ausschließlich durch die Vergabe eines Barcodes erfolgen, sondern auch durch die bildliche Erfassung der Papierbelege (vgl. Rz. 130).
- Die Aufbewahrung (Rz.115) für Steuerpflichtige, die nach § 4 Absatz 3 EStG als Gewinn den Überschuss der Betriebseinnahmen über die Betriebsausgaben ansetzen. Diese sind ebenfalls dazu verpflichtet, „Aufzeichnungen und Unterlagen nach § 147 Absatz 1 AO aufzubewahren (BFH-Urteil vom 24.6.2009, BStBl II 2010 S. 452; BFH-Urteil vom 26.2.2004, BStBl II S. 599)."

Ein interessanter Aspekt verbirgt sich in der Änderung von Rz.164 hinsichtlich Umfangs und Ausübung des Rechts auf Datenzugriff nach § 147 Absatz 6 AO durch die Behörde. Erfolgte im Rahmen eines Systemwechsels eine Migration von aufzeichnungs- und aufbewahrungspflichtigen Daten, so war dies bisher zwingend damit verbunden, dass für diese Daten den kompletten Zeitraum von zehn Jahren folgend auf dem Jahr, in dem der Systemwechsel erfolgte, ein unmittelbarer (Z1, Rz.165) bzw. mittelbarer (Z2, Rz.166) Datenzugriff gewährleistet wird. Mit Neufassung der GoBD ist es ausreichend, sofern noch nicht mit einer Außenprüfung begonnen wurde, bei einem Systemwechsel oder einer Auslagerung, nach Ablauf des fünften Kalenderjahres, das auf die Umstellung folgt, einen Z3-Zugriff (Rz.167, Datenträgerüberlassung) zur Verfügung zu stellen.

Fazit

Was bedeutet die Neufassung der GoBD nun? Die Welt wird jedenfalls nicht auf den Kopf gestellt. In der finalen Fassung, die sehr nah an der Fassung aus Juli 2019 liegt, erfolgte vielmehr ein Update an geänderte informationstechnische Möglichkeiten. Daher ist es auch weniger als eine GoBD 2.0 zu sehen, als vielmehr als eine Version 1.1 mit überwiegend realistischen Maßnahmen bzw. auch Erleichterungen.

Man könnte daher das Gefühl bekommen, dass die Finanzverwaltung etwas mehr in der Moderne angekommen ist. Deshalb ist davon auszugehen, dass solche Anpassungen auch zukünftig veröffentlicht werden. Interessant wird hierbei sein, ob man sich abermals ca. fünf Jahre Zeit lässt – in der Informationstechnologie sind fünf Jahre ein langer Zeitraum.

IT-Sicherheit, Datenschutz, Know-how-Schutz – Drei auf einen Streich?

Know-how soll durch das neue Geschäftsgeheimnisgesetz besser geschützt werden. Doch müssen dafür Schutzmaßnahmen umgesetzt werden – sonst entfällt der Schutz. Unternehmen, die im Bereich IT-Sicherheit und Datenschutz gut aufgestellt sind, können diese Schutzmaßnahmen leicht umsetzen.

Wer nicht handelt, bleibt schutzlos

Betriebsgeheimnisse, aber auch technische Erfindungen, können Geschäftsgeheimnisse sein. Damit Know-how rechtlich geschützt wird, müssen seit April 2019 bauliche, technische, organisatorische und vertragliche Maßnahmen zur Geheimhaltung umgesetzt werden (vgl. dazu novus Mandanteninformation Mai 2019, S. 20).

Organisatorische und technische Maßnahmen – alte Bekannte?

Auch die Datenschutz-Grundverordnung (DSGVO) verlangt die Umsetzung „technischer und organisatorischer Maßnahmen" (kurz: TOM). Können sich also Unternehmen, die bereits ausreichende TOM umgesetzt haben, entspannt zurücklehnen? Sind TOM immer auch gleichzeitig Geheimhaltungsmaßnahmen zum Schutz von Know-how? Oder verlangt das Geschäftsgeheimnisgesetz Maßnahmen, die über die TOM zum Datenschutz hinausgehen?

Datenschutzvorkehrung = Geheimhaltungsmaßnahme?

Viele TOM zum Datenschutz und aus dem Bereich der IT-Sicherheit eignen sich auch zum Schutz von Geschäftsgeheimnissen. Dies gilt vor allem für bauliche und technische Maßnahmen, z. B.:

- Kontrolle des Zugangs zu Gebäuden
- Kontrolle des Zutritts zu IT-Systemen (z. B. Passwörter, Firewall)
- Verschlüsselungstechniken
- privacy by design.

Wurden genügend wirksame technische Maßnahmen zum Datenschutz umgesetzt, dürften dadurch auch die Anforderungen des Geschäftsgeheimnisgesetzes an den technischen Geheimnisschutz erfüllt sein.

Andere TOM aus dem Datenschutz sind dagegen nicht erforderlich, um einen Schutz von Geschäftsgeheimnissen sicherzustellen. Dies gilt insbesondere für TOM zur Sicherstellung der Integrität („Richtigkeit") von Daten, Speicherbegrenzung (z. B. Löschkonzepte), Verfügbarkeit und Belastbarkeit von Systemen.

Need-to-know: Höhere Anforderungen als im Datenschutzrecht

Für einen Schutz von Know-how sind wegen des Need-to-know-Prinzips jedoch zusätzliche Maßnahmen erforderlich, die über vergleichbare TOM zum Datenschutz hinausgehen. Need-to-know bedeutet, dass geheime Informationen nur einer möglichst geringen Anzahl an Personen mitgeteilt werden, die diese unbedingt benötigen. In der Regel ist es daher zur Umsetzung dieses Prinzips nicht mit den TOM zum Datenschutz getan. Es bedarf zusätzlicher Maßnahmen zum Schutz von Geschäftsgeheimnissen in folgenden Bereichen:

- Maßnahmen zur Beschränkung des Zugriffs z. B. durch Rollenkonzepte
- Maßnahmen zur Beschränkung der Weitergabe von Informationen an Dritte.

Organisatorische Maßnahmen: oft nur kleine Anpassungen nötig

Organisatorische Maßnahmen zum Datenschutz können gleichzeitig Geheimhaltungsmaßnahmen sein. Voraussetzung ist allerdings, dass Arbeitsanweisungen und Schulungen von Mitarbeitern um konkrete Hinweise zu Geschäftsgeheimnissen erweitert werden.

Hinweis: *Viele technische und organisatorische Maßnahmen aus dem Datenschutz und der IT-Sicherheit eignen sich auch zum Schutz Ihrer Geschäftsgeheimnisse. Hier ergeben sich kostensenkende Synergieeffekte.*

Das neue Bußgeldkonzept der deutschen Datenschutzbehörden

Bußgelder in Millionenhöhe im Datenschutzrecht haben nun auch Deutschland erreicht: In Berlin wurde am 30.10.2019 ein Bußgeld in Höhe von 14,5 Mio. Euro verhängt. Wegen des neuen Bußgeld-Konzepts der deutschen Datenschutzbehörden müssen alle Unternehmen in Zukunft mit höheren Bußgeldern rechnen.

Verstöße gegen das Datenschutzrecht können mit einer Geldbuße geahndet werden. Bei wesentlichen Verstößen sieht die Datenschutz-Grundverordnung (DSGVO) Bußgelder in Höhe von bis zu 4 % des weltweiten Vorjahresumsatzes eines Unternehmens oder bis zu 20 Mio. Euro vor. Der jeweils höhere Betrag ist die Obergrenze. Solche Verstöße umfassen z. B. auch fehlende oder unvollständige Datenschutzerklärungen. Bei nur formalen Verstößen liegt die Obergrenze bei 2 % des Vorjahresumsatzes bzw. 10 Mio. Euro. Beispiele für derartige Verstöße sind fehlende Verarbeitungsverzeichnisse oder Auftragsverarbeitungs-Vereinbarungen.

Neues Bußgeld-Konzept der Datenschutzkonferenz

Die DSGVO enthält für Geldbußen nur relativ vage Kriterien, die die Datenschutzbehörde bei der Festlegung der konkreten Höhe der Geldbuße berücksichtigen soll. Die Datenschutzkonferenz (DSK) als Dachverband der deutschen Datenschutzbehörden hat daher am 14.10.2019 ein Konzept zur Berechnung von Geldbußen für Datenschutzverstöße veröffentlicht. Das Bußgeldmodell gilt für alle Unternehmen, Selbstständige und Gewerbetreibende mit Sitz in Deutschland, nicht aber für nicht wirtschaftlich tätige Vereine. Durch das neue Konzept soll die Bußgeldzumessung nachvollziehbarer und gerechter werden.

Erster Schritt: Berücksichtigung des Umsatzes des Unternehmens

Grundlage der Bußgeldberechnung ist der Vorjahresumsatz des jeweiligen Unternehmens. Dadurch soll sichergestellt werden, dass Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU) für einen vergleichbaren Verstoß geringere Bußgelder zahlen müssen als umsatzstarke Großunternehmen. Bei Unternehmensgruppen soll nach Auffassung der DSK auf den gesamten Konzernumsatz abgestellt werden.

Das Bußgeldkonzept unterscheidet beim Umsatz hinsichtlich der Größenklassen zwischen Kleinstunternehmen, kleinen und mittleren Unternehmen sowie Großunternehmen. Für jede Größenklasse wird der jeweilige Umsatz durch 360 geteilt. Dadurch erhält man den durchschnittlichen Tagesumsatz des Unternehmens einer Größenklasse. Dieser Tagesumsatz ist der (wirtschaftliche) Grundwert für die Bußgeldberechnung.

Zweiter Schritt: Berücksichtigung der Schwere des Verstoßes

Verstöße gegen das Datenschutzrecht werden unterschiedlich schwer gewichtet. Dies wird im neuen Bußgeldkonzept dadurch berücksichtigt, dass der Grundwert mit einem Faktor multipliziert wird. Je schwerer der Verstoß, desto höher der Faktor. Hier wird nach formalen und inhaltlichen Verstößen differenziert:

Größenklassen Kleinstunternehmen			Größenklassen kleine Unternehmen		
Umsatz (Mio. Euro)	bis 0,7	0,7 - 1,4	1,4 - 2	2 - 5	5 - 7,5	7,5 - 10
Grundwert (Euro)	972	2.917	4.722	9.722	17.361	24.306

Größenklassen mittlere Unternehmen							Größenklassen Großunternehmen						
Umsatz (Mio. Euro)	10 - 12,5	12,5 - 15	15 - 20	20 - 25	25 - 30	30 - 40	40 - 50	50 - 75	75 - 100	100 - 200	200 - 300	300 - 400	400 - 500	über 500
Grundwert (Euro)	31.250	38.194	48.511	62.500	76.389	97.222	125.000	173.611	243.056	416.667	694.444	972.222	Mio. 1,25	Umsatz / 360

Beispiel: Der Grundwert für ein mittleres Unternehmen mit einem Vorjahresumsatz von Mio. 45 Euro beträgt 125.000 Euro.

Schwere des Verstoßes	Faktor für formale Verstöße (Art. 83 Abs. 4 DSGVO)	Faktor für wesentliche Verstöße (Art. 83 Abs. 5, 6 DSGVO)
leicht	1 bis 2	1 bis 4
mittel	2 bis 4	4 bis 8
schwer	4 bis 6	8 bis 12
sehr schwer	min. 6 bis max. 2 % des Umsatzes	min. 12 bis max. 4 % des Umsatzes

Das Bußgeldkonzept enthält keine Aussagen dazu, welche DSGVO-Verstöße besonders schwer wiegen. Schon deshalb führt das neue Konzept – kurzfristig betrachtet – nicht zu mehr Rechtssicherheit.

Grundsätzlich dürfte ein Verstoß umso schwerer sein, je

- mehr personenbezogene Daten betroffen sind,
- sensibler die personenbezogenen Daten sind,
- höher der Schaden bei den betroffenen Personen sein kann und
- länger der Verstoß andauert.

Beispiel: Ein Unternehmen mit einem Vorjahresumsatz von 45 Mio. Euro begeht einen mittelschweren, wesentlichen Datenschutzverstoß. Das Bußgeld beträgt mindestens 500.000 Euro (Grundwert 125.000 Euro multipliziert mit Faktor 4).

Dritter Schritt: Berücksichtigung sonstiger Umstände

In einem dritten Schritt kann die Datenschutzbehörde bei der Berechnung der konkreten Geldbuße den Geldbetrag mindern oder bis zu den jeweiligen Obergrenzen erhöhen. Hierbei wird jedoch nicht der Datenschutzverstoß als solcher berücksichtigt, weil diese tatbezogenen Umstände bereits im zweiten Schritt berücksichtigt wurden. Vielmehr berücksichtigt die Datenschutzbehörde hier belastende und sonstige entlastende Umstände. Es handelt sich vor allem um solche Umstände, die in dem Unternehmen selbst begründet sind (täterbezogene Umstände).

Hinweis: *Das neue Bußgeldkonzept ist kein Bußgeldkatalog. Das konkret drohende Bußgeld für einen bestimmten Verstoß kann auch mit dem neuen Konzept nicht auf den Euro genau ausgerechnet werden. Es wird jedoch zu deutlich höheren Bußgeldern als bisher führen, insbesondere für umsatzstarke Unternehmen. Geldbußen wegen Datenschutzverstößen können gerichtlich überprüft werden, wobei die Gerichte nicht an das Konzept der DSK gebunden sind. Derzeit ist noch nicht absehbar, ob und inwieweit Bußgelder nach dem neuen Konzept vor Gericht Bestand haben werden.*

Beispiele:

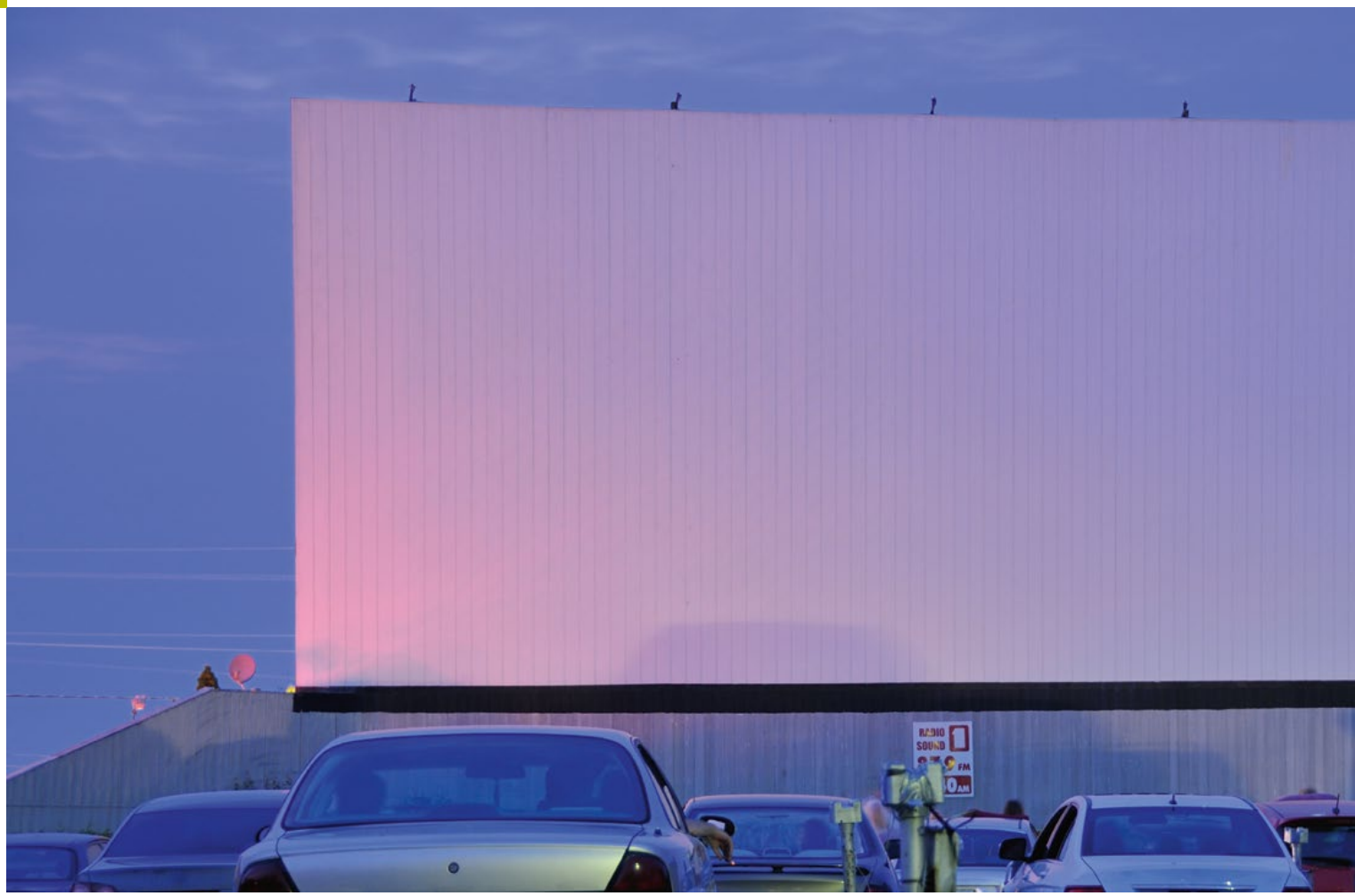
bußgelderhöhende Umstände	bußgeldmindernde Umstände
bewusster Verstoß	Vorgaben wurden aus Versehen nicht eingehalten
erneuter Verstoß (Wiederholungsfall)	freiwillige Kooperation mit der Aufsichtsbehörde
durch Verstoß erlangter finanzieller Vorteil	drohende Insolvenz des Unternehmens

TIBER-DE – Umsetzung des europäischen Rahmenwerks zur Erhöhung der Cybersicherheit

In unserer 2. Ausgabe 2019 des novus IT haben wir ausführlich über das TIBER-EU Rahmenwerk – das erste zentrale gemeinsame europäische Rahmenwerk zur Prüfung der Widerstandsfähigkeit von Unternehmen und Behörden aus dem Finanzsektor gegenüber Cyberattacken („Threat Intelligence-based Ethical Red Teaming") – berichtet.

Mittlerweile erfolgte im September 2019 die bis dahin noch offene Umsetzung in nationales Recht durch die Verabschiedung von „TIBER-DE". Der Rahmen für TIBER-DE wurde durch das Bundesministerium der Finanzen (BMF) gemeinsam mit der Bundesagentur für Finanzdienstleistungsaufsicht (BaFin) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgearbeitet. Die Koordination des „Ethical Red Teaming" erfolgt in Deutschland durch die Deutsche Bundesbank. Das Kompetenzzentrum bei der Bundesbank wird durch einen Lenkungsausschuss gesteuert, dem auch die BaFin angehört.

In Deutschland wird für die betroffenen Unternehmen (erst einmal) keine Verpflichtung bestehen, an den entsprechenden TIBER-Tests teilnehmen zu müssen. Allerdings sollte durch die entsprechenden Institute, Banken, Finanzdienstleister, Versicherungen etc. frühzeitig und zur Erhöhung der IT-Sicherheit geprüft werden, inwiefern eine Teilnahme sinnvoll ist.



Neue Sicherheitsvorgaben für den 5G-Rollout

Ab 2020 soll auch in Deutschland das 5G-Netz zur Verfügung stehen. 5G ist der neueste Standard für mobiles Internet und Mobiltelefonie. Zum sicheren Betrieb und zur Sicherheit der Mobilfunknetze wurde seitens der Bundesnetzagentur bereits im Frühjahr ein Eckpunktepapier veröffentlicht.

Was ist 5G?

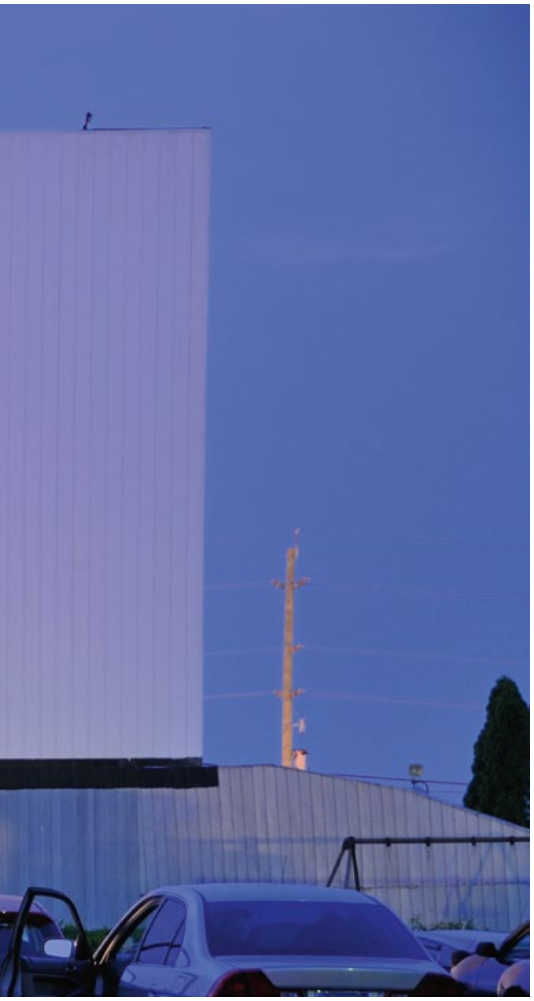
Das 5G-Netz soll die Digitalisierung vieler Lebensbereiche, die Vernetzung von Maschinen in der Industrie und intelligenten Geräten unterstützen. Der grundsätzliche Unterschied zwischen dem derzeit aktuellen Mobilfunkstandard 4G (LTE) und 5G sind die höheren Bandbreiten, die erreicht werden können. Darüber hinaus gehören eine verbesserte Kryptografie, ein sichereres Roaming sowie weitere Maßnahmen zur Absicherung der Signalisierung zwischen unterschiedlichen Mobilfunknetzen zu den Innovationen. Insbesondere verspricht man sich von 5G aber auch, dass bestehende Sicherheitslücken vorheriger Technologien geschlossen werden.

Die Einführung des 5G-Netzes soll aber nicht das Ende der LTE-Frequenzbänder bedeuten, sondern im Idealfall eine Ergänzung, um zukünftig eine noch größere Kapazität und höhere Netzgeschwindigkeiten bedienen zu können. Zudem müssen die beiden Mobilfunkstandards noch eine Zeit lang nebeneinander arbeiten, bevor in Deutschland eine flächendeckende Verfügbarkeit des 5G-Netzes vorhanden ist.

5G ist dabei weniger ein „Netz" – wie bspw. noch bei den Vorgängertechnologien – sondern vielmehr ein Baukasten, aus dem man Dienste und Strukturen mit unterschiedlichsten Eigenschaften gleichzeitig realisieren kann. Dazu gehört die Realisierung separater virtueller Netze innerhalb öffentlicher Infrastrukturen, aber auch die Möglichkeit, geographisch begrenzte 5G-Nutzungslizenzen zu erwerben.

Sicherheitskatalog für Telekommunikationsnetze und IT-Systeme

Durch die Bundesnetzagentur, das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist im Oktober 2019 aufbauend auf dem Eckpunktepapier aus dem Frühjahr eine Neufassung des Sicherheitskatalogs für Telekommunikationsnetze und IT-Systeme vorgelegt worden. Diese Neufassung sieht spezifische Sicherheitsanforderungen vor, welche durch Telekommunikationsbetreiber und entsprechende Zulieferer einzuhalten sind. Die Sicherheitsanforderungen betreffen dabei im Wesentlichen den Betrieb von Telekommunikationsnetzen.



Zusätzlich zu den Standardsicherheitsanforderungen, wurden für öffentlich zugängliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotential spezifische Sicherheitsanforderungen definiert.

Neue Sicherheitsanforderungen

Die „spezifischen Sicherheitsanforderungen" treffen auch das 5G-Netz. Dies zeigt, dass dem Aufbau des 5G-Netzes in Deutschland deutlich höhere Sicherheitsanforderungen zugrunde gelegt werden, als noch bei 3G oder 4G. Ein zentraler Aspekt im Rahmen der Sicherheitsanforderungen sieht dabei vor, dass technische Komponenten und Software in kritischen Bereichen zertifiziert werden müssen. Dies soll durch das BSI erfolgen. Zertifizierungsvoraussetzung ist, dass Lieferanten oder Hersteller ihre Vertrauenswürdigkeit zusichern. Im Detail ist dies im Sicherheitskatalog definiert. In diesem Zusammenhang sollen Systeme ausschließlich von Lieferanten bezogen werden, welche die Bestimmungen zum Fernmeldegeheimnis und zum Datenschutz einhalten. Sofern kritische Prozesse durch einen Netzbetreiber ausgelagert werden, stehen diese in der Verantwortung nachzuweisen, dass bei den Dienstleistern entsprechende Sicherheitsstandards und -anforderungen eingehalten wurden und werden.

Darüber hinaus sind seitens der Netz- und Systembetreiber folgende Anforderungen zu erfüllen:

- Sicherstellung der Produktintegrität
- Einführung eines Sicherheitsmonitorings
- besondere Anforderungen an das Personal in sicherheitsrelevanten Bereichen
- Gewährleistung ausreichender Redundanzen
- Vermeidung von Monokulturen.

Ausblick

Betroffene Verbände und Unternehmen hatten bis 13.11.2019 die Möglichkeit, Stellung zu dem vorgestellten Sicherheitskatalog zu nehmen. Aktuell werden diese Stellungnahmen geprüft und der Katalog finalisiert.

Office 365 in Unternehmen

Teil 1: Rahmenbedingungen, Chancen und Herausforderungen

Wie die Modernisierung auf die Urbanisierung, folgt die Cloud-Infrastruktur auf die Digitalisierung. Mit zunehmender Verbreitung von digital gesteuerten Diensten wird proaktiv in deren Migration investiert, um weiterhin flexibel auf viele neue Anforderungen, die an Unternehmen gestellt werden, reagieren zu können. Ob webspezifische Apps oder mobile Anwendungen, die Cloud-Integration hat sich von einer Option zu einem Bedürfnis gewandelt.

Das Fehlen einer Cloud-Infrastruktur in Organisationen kann sich in Bezug auf den Betrieb und die Kosten gegenüber Ökosystemen mit Cloud-Unterstützung als Nachteil erweisen.

Wir informieren Sie mit einer zweiteiligen Artikelreihe in unserem novus IT über aktuelle Entwicklungen zum Einsatz von Microsoft Office 365.

In diesem ersten Artikel stellen wir das Produkt Office 365 vor und gehen auf grundlegende Herausforderungen und Chancen ein. Im zweiten Teil, der in der nächsten Ausgabe des novus IT veröffentlicht wird, betrachten wir das Thema dann aus Compliance- bzw. datenschutzrechtlicher Sicht.

Office 365 – Die Rahmenbedingungen:

Office 365 ist nicht ausschließlich die Online-Version der herkömmlichen Office-Software, vielmehr enthält sie die bereits bekannten, installierbaren Anwendungen, wie Outlook, Word, Excel, PowerPoint, Access und den Dienst OneDrive, die um überall verfügbare Werkzeuge, wie Exchange, SharePoint und Teams erweitert werden können. Sie unterscheidet sich vor allem im Zugang. Dabei bleibt sie nicht auf die Hardware beschränkt, sondern ist global über die Cloud verfügbar. Für Unternehmen gibt es Lizenzmodelle mit acht verschiedenen Tarifen, von ProPlus über Business bis zur Enterprise Edition, die sich im angebotenen Umfang an Nutzern, Speicherkapazitäten und Applikationen unterscheiden.

Vorteile:

- Größerer Funktionsumfang
  Gegenüber der Desktop-Version sind bei der 365-Version bereits Funktionsupdates, Web- und Mobilversionen der Anwendung, Dateifreigabe, Sicherheit, Compliance Features und ein Support für die Bereitstellung enthalten. OneNote, OneDrive for Business, Publisher und Access sind ebenfalls nur in der Online-Version erhältlich, ebenso weitere Business-Premium-Dienste, wie SharePoint oder Microsoft Teams.

- Geschäftliche Agilität
  Ein wichtiger Vorteil ist die Kommunikation und Zusammenarbeit in Echtzeit, ermöglicht durch die sofortige Bereitstellung der benötigten Daten und der Möglichkeit, sie sich über eine sichere Freigabe selbst einzuholen. Es kann von überall aus gemeinsam über verschiedenste Geräte hinweg gearbeitet werden. Kommenden Features, wie Machine Learning und Sprachassistent werden den Funktionsumfang von Office 365 noch erweitern und für jede Unternehmensgröße das Arbeiten 4.0 im Team mit unternehmensweiter Kommunikation ermöglichen.

- Transparenz und planbare Kosten
  Lizenzen für Mitarbeiter können monatlich hinzugebucht oder reduziert werden bzw. von ausscheidenden Mitarbeitern auf neue übertragen werden. Je nach Paket kann ausschließlich das gebucht und bezahlt werden, was benötigt wird.

- Verbesserung der IT-Infrastruktur
  Office 365 eliminiert dabei IT-bezogene Aufgaben, wie Patching und reduziert die Kosten für die laufende Infrastruktur, da zur Nutzung ‚nur' eine Internetverbindung benötigt wird. Eine derartige Bereitstellung ist schneller und einfacher als einen Benutzer-Account anzulegen. Der Service wird ab dem ersten Quartal 2020 über neue Rechenzentren in Deutschland bereitgestellt. Microsoft hat angekündigt, sicherzustellen, dass die in den deutschen Rechenzentren gehosteten Daten entsprechend den Anforderungen aus der europäischen Datenschutz-Grundverordnung (DSGVO) geschützt werden.

Herausforderungen:

- Stockende Migration
  Für die Migration von bspw. Exchange 2010 nach Office 365 von einem lokalen auf einen in der Cloud gehosteten Server sind mehrere Herausforderungen zu meistern. Ohne ausreichende Kenntnisse in der Cloud-Bereitstellung und von On-Premise-Lösungen kann es bei einer hybriden Migration zu Problemen kommen, vor allem bei der Synchronisierung, der Authentifizierung und bei den Leistungsrückständen in beiden Umgebungen. Häufig gerät eine Migration ins Stocken, wenn keine vorläufige Zustandsbewertung der bestehenden Systeme vorgenommen, die Komplexität des Migrationsprozesses unterschätzt, oder die Fähigkeiten der internen IT-Spezialisten falsch beurteilt wurde.

  Hierfür ist eine gute Vorbereitung mit detaillierter Planung erfolgsentscheidend. Microsoft oder sein Partner, die Telekom, stellen Assistenten und Prüflisten für die Migration zur Verfügung, die auf deren Webseite in einem Artikel genauer beschrieben sind.

- Compliance- und Sicherheitsbedenken
  Ein wesentlicher Faktor im Bereich der Nutzung von Office 365 sind die Compliance- und Sicherheitsbedenken, die mitunter durch die EU-Datenschutz-Grundverordnung zugenommen haben Microsoft wird seit längerem dafür kritisiert, Nutzerdaten auch ohne Einwilligung zu sammeln. Schon bei Windows 10 wurde Microsoft vorgeworfen, heimlich verschlüsselte Daten abzugreifen und an eigene Server in den USA zu übermitteln. Datenschützer monieren, dass bei den Office-Anwendungen die Sammelwut noch weitaus höher einzustufen ist, als bei Windows 10.

  Mit der Wahl des richtigen Partners, betreffend die Standortfrage der Server und die Auswahl der Cloud-Modelle, können diese Sicherheitsbedenken abgemildert werden. In Bezug auf Compliance helfen Drittanbieterlösungen, um z. B. die Anforderungen an die Archivierung zu erfüllen.

- Kompatibilitätsprobleme
  Eine wichtige Herausforderung, insbesondere aus dem Produktionsumfeld, ist die immer aktuellste Office-Version zu haben. Schnittstellen, Prozesse und durchgeführte Changes in den anderen Systemen, wie z. B. dem ERP, müssen dazu kompatibel sein, um Probleme zu vermeiden. Hersteller wie Datev bieten diese Unterstützung nur in den aktuellen Versionen ihrer Produkte an, in diesem Fall wäre es aktuell ab der Version 12.1.

Fazit

Bei Microsoft scheint der Trendwechsel von der Stand-Alone-Kaufsoftware hin zum Softwarevertrieb als Abo-Modell und zur Nutzung in der Cloud vollzogen zu sein. Ob im Abonnement oder als Dauerlizenz, lokal installiert als auch online genutzt, Office 365 ermöglicht gleichermaßen eine Offline- und Online-Nutzung. Spätestens mit der Einstellung des Supports für die Stand-Alone-Software müssen sich die Kunden für ein Modell entschieden haben. Der Weg führt eindeutig in die Cloud. Die meisten Implementierungen fangen mit einer hybriden Cloud an, bei der einzelne Aufgabenbereiche verlagert werden.

Aber wie sieht es mit der Sicherheit oder dem Datenschutz aus? Welche Mittel gibt es und wie lassen sich diese einsetzen? Microsoft hat in diesem Bereich nachgebessert und bietet mehrere Tools und Neuerungen an. Das Unternehmen spricht von vier Säulen der IT-Sicherheit, nämlich Identitäts- und Zugriffsverwaltung, Bedrohungsschutz, Informationsschutz und Sicherheitsverwaltung. Im weiteren Verlauf dieser Serie werden die Säulen und die darunter gruppierten Tools näher betrachtet.

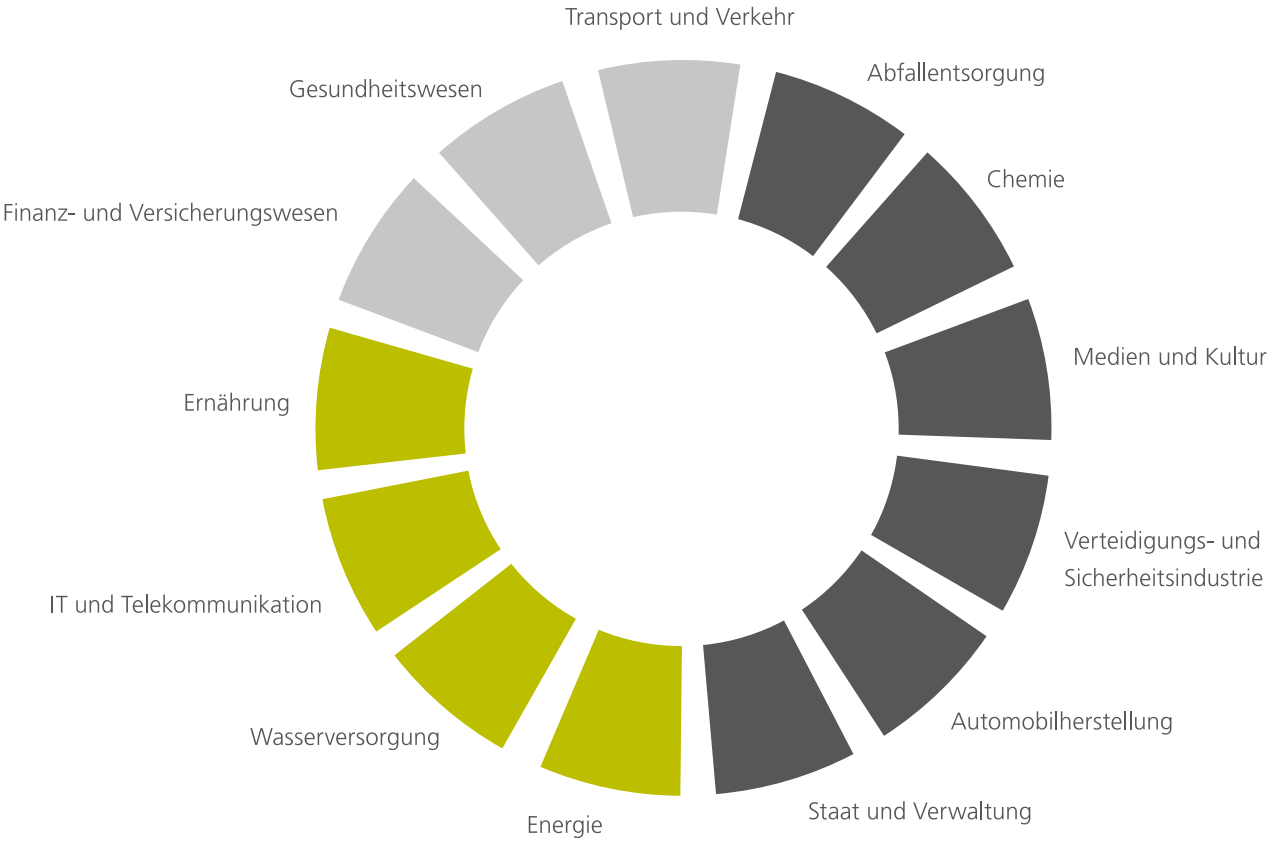
IT-Sicherheitsgesetz 2.0 – Auswirkungen auf nicht-kritische Infrastrukturen

Durch Inkraftsetzung des IT-Sicherheitsgesetzes (IT-SiG) 1.0 im Juli 2015 hat der deutsche Gesetzgeber vorbildlich auf die legislativen Bewegungen zur angedachten EU-Richtlinie NIS (August 2016) reagiert. Die Richtlinie fordert alle EU-Staaten auf sicherzustellen, dass eine "Sicherheitskultur" in Industriesektoren, welche für das Funktionieren von Wirtschaft und Gesellschaft wesentlich ist, Einzug hält. Zudem haben in diesen Sektoren identifizierte Unternehmen als Betreiber von kritischen Dienstleistungen angemessene technische und organisatorische Schutzmaßnahmen umzusetzen.

IT-SiG 2.0

Im Rahmen der ersten Ausgabe des novus IT 2019 haben wir ausführlich den am 27.3.2019 veröffentlichten Entwurf des IT-Sicherheitsgesetzes dargestellt. Zentrale Änderungen sind:

- mehr Geld und Personal für das BSI
- vehementer Ausbau des Aufgabenbereichs und der Kompetenzen des BSI – bspw. statt reiner „Verteidigung" in der Vergangenheit, nun aktives Hacking, Hack-back, Verschweigung von Schwachstellen, Lahmlegung von gefährlichen Botnetzen sowie Annahme virtueller Identitäten zur verbesserten Ermittlung möglich
- Ausweitung der KRITIS-Definition und neue Meldepflichten u. a. für Zulieferer/Dienstleister
- Ausbau und Verschärfung des Strafrechts
- Änderung weiterer zehn Gesetze, u. a. des Strafgesetzbuchs (StGB), Telekommunikationsgesetzes (TKG), Telemediengesetzes (TMG) und Bundeskriminalamtsgesetzes.



- 1. Korb: in Kraft getreten am 03.05.2016; Umsetzung nach § 8a BSIG bis 03.05.2018
- 2. Korb: in Kraft getreten am 30.06.2017; Umsetzung nach § 8a BSIG bis 30.06.2019
- Mit Entwurf des IT-SiG 2.0 hinzugekommen

Auswirkungen IT-SiG 2.0 auf nicht-kritische Infrastrukturen

Die Anforderungen des IT-SiG 2.0 richten sich nicht ausschließlich an Betreiber kritischer Infrastrukturen, sondern insbesondere auch an nicht-kritische Infrastrukturen. Durch die steigenden Anforderungen an KRITIS erhöhen sich automatisch die steigenden Anforderungen auch auf die gesamte Lieferkette, Zulieferer und Dienstleister von KRITIS, da auch diese erhöhten Sicherheitsvorkehrungen einzuhalten haben, welche durch das KRITIS-Unternehmen sicherzustellen sind. Die Hersteller von Komponenten, die im KRITIS-Bereich eingesetzt werden sollen, müssen zukünftig die Vertrauenswürdigkeit ihrer gesamten Lieferkette sicherstellen und eine Vertrauenswürdigkeitserklärung abgeben. Die Art und der Umfang dieser Erklärung werden noch definiert. Sie unterliegen, ebenso wie allgemein alle Hersteller von IT-Produkten, einer Meldepflicht gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bei Sicherheitsvorfällen. Das zentrale Problem ist: Viele Details des IT-Sicherheitsgesetzes sind noch unklar – z. B. fehlt noch eine Rechtsverordnung, die die Meldepflicht der KRITIS spezifiziert.

Es sind somit wesentlich mehr Unternehmen und Branchen betroffen als ausschließlich KRITIS-Unternehmen.

Ansätze zur Umsetzung durch nicht KRITIS-Unternehmen

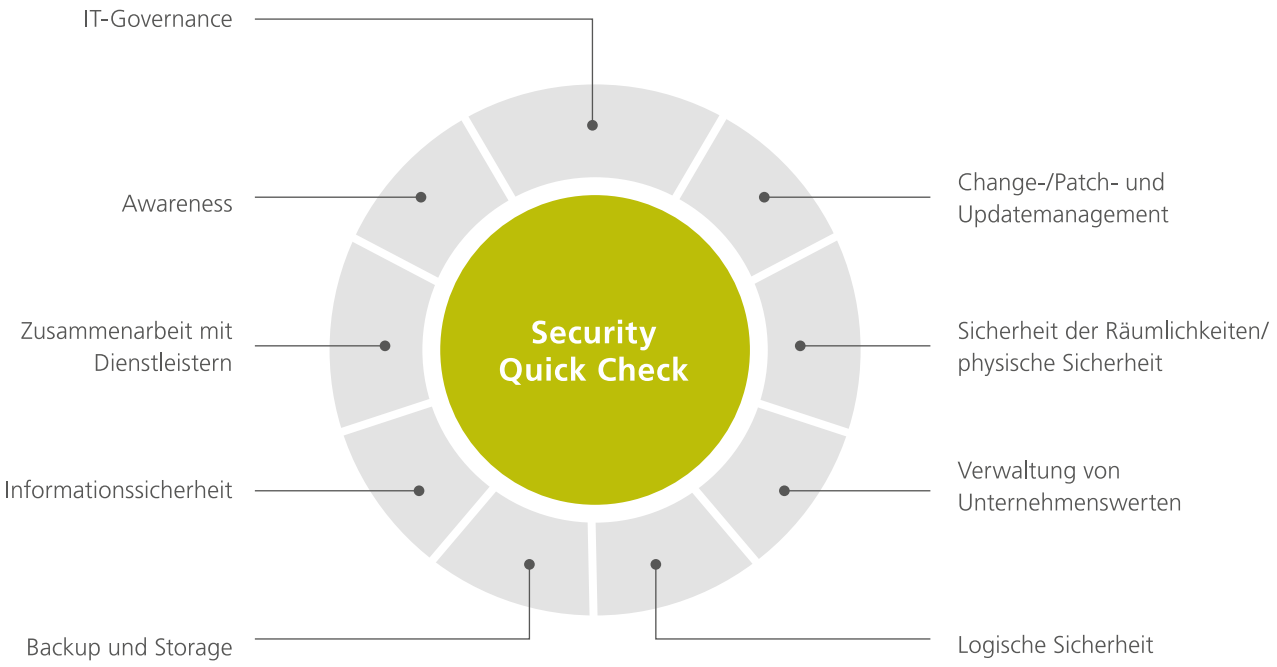
Betroffene Unternehmen sollten

- die Informationssicherheit gewährleisten,
- ein Information Security Management Systeme (ISMS) einsetzen
- sowie ggf. entsprechende Zertifikate einholen.

Möglichkeit zur Umsetzung sind bspw.:

- Security Quick Checks
- GAP-Analysen
- Risikomanagement- bzw. Business-Impact-Analysen
- Einführung und Zertifizierung eines ISMS nach ISO 27001
- Business Continuity Management

Im Rahmen eines Security Quick Checks lassen sich bei einer Überprüfung zentrale Parameter auf ihren Grad der Umsetzung nach Best Practices sowie definierter Standards testen.



Sicherheit im Netz – Netzwerksegmentierung

Viele Unternehmen nutzen in Bereichen der Lagerhaltung oder der Produktion häufig noch eine ältere IT-Ausstattung, bspw. einen oder mehrere Windows-XP-Rechner in der Produktionshalle. Durch die Verwendung von alten Servern bzw. Clients entsteht das Risiko, von außen angreifbar zu werden. Das zentrale Problem sind fehlende Sicherheitsupdates für Server und Clients.

Im Produktionsumfeld sind die Anlagen und Produktionsmaschinen vor dem Hintergrund angeschafft worden, dem Unternehmenszweck gegebenenfalls 15 bis 20 Jahre (oder noch länger) zu dienen. Die hierfür verwendeten Systeme können meist nur auf dem ursprünglichen Betriebssystem betrieben werden. Möchte man bei diesen Clients bzw. Servern auf ein neues Betriebssystem migrieren, entstehen oft hohe Kosten und Mühen, vorausgesetzt, das System bzw. die Produktionsanlage lässt dies überhaupt zu. Dies kann daran liegen, dass die Produktionssysteme sehr individuell und speziell auf bspw. den unternehmenseigenen Produktions- oder Lagerprozess angepasst oder nur für diesen entwickelt wurden.

Um allerdings trotzdem die IT-Sicherheit und die Gefahr eines Eingriffs von außen nicht komplett zu vernachlässigen, besteht die Möglichkeit einer netzwerktechnischen Segmentierung solcher Systeme.

Die Netzwerksegmentierung stellt in der Informationstechnologie eine Variante dar, ein bestimmtes Netzwerk in unabhängige (sichere) Segmente zu unterteilen.

Trotz einer Firewall, einem Antivirusprogramm und ständigen Updates in der IT-Infrastruktur haben die meisten Unternehmen dennoch Sicherheitsrisiken.

Netzwerksegmentierung – Eine Möglichkeit

Ein möglicher Lösungsansatz, trotz alter Server bzw. Clients eine gewisse Sicherheit zu gewährleisten, ist die erwähnte Netzwerksegmentierung. Das grundlegende Vorgehen bei der Netzwerksegmentierung sieht vor, dass die gefahrbringende Umgebung vom produktiven System getrennt wird. Das bedeutet, dass das firmeninterne IT-System in Netzwerksegmente unterteilt wird, um eine höhere IT-Sicherheit gewährleisten zu können. Der typische in die Jahre gekommene Windows-XP-Rechner stellt so kein großes Risiko mehr dar, da der Bereich, in welchem er ans Netz angeschlossen ist, vom produktiven System getrennt ist. Mit einer Netzwerksegmentierung kann also im Vorfeld verhindert werden, dass sich ein Angriff im gesamten Netzwerk ausbreitet.

Das einfachste Beispiel für den Einsatz von Netzwerksegmentierung sind deutsche Schulen. In allen Bundesländern ist es Vorschrift, das schulische Verwaltungsnetz vom sog. pädagogischen Netz zu trennen. Aber auch in allen Bereichen der freien Wirtschaft und Industrie wird Netzwerksegmentierung häufig angewendet.

Erste Schritte zur Implementierung

Entscheidet man sich als Unternehmen, eine Netzwerksegmentierung durchzuführen, um seine unternehmensinterne IT-Infrastruktur zu schützen, sollten sich die Verantwortlichen zunächst um die folgenden Themen kümmern:

- Im ersten Schritt sollten die Bereiche, die kritische Daten, Prozesse und Systeme enthalten, identifiziert und analysiert werden. Diese Bereiche bilden dann die sogenannten Segmente.
- Auf Basis dieser Aufnahme sollten die entsprechenden Sicherheitszonen definiert werden. Diese Segmentierung sollte anhand der Kritikalität der Daten sowie der Zugriffsanforderungen erstellt werden.
- Um gewährleisten zu können, dass im Verlauf von Netzwerkänderungen oder -erweiterungen alle Sicherheitskontrollen erhalten bleiben, sollte die Netzwerksegmentierung regelmäßig überprüft und im Zweifelsfall angepasst werden. Im Rahmen dieser Überprüfung sollte auch immer die Funktionsfähigkeit der IT-Infrastruktur geprüft werden.

Wie wird Netzwerksegmentierung in aller Regel umgesetzt?

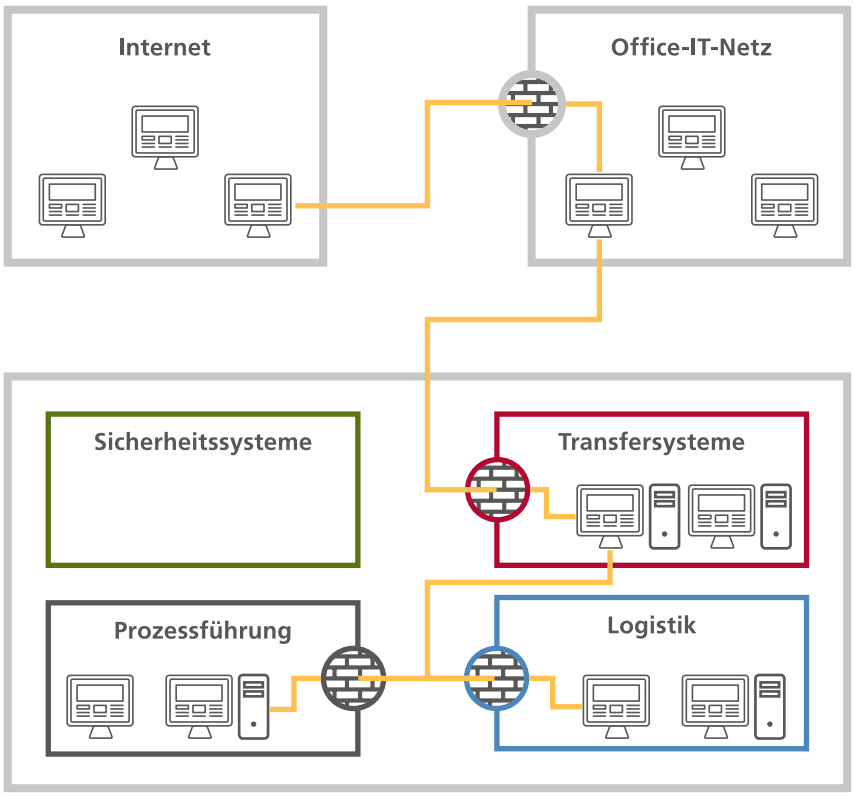
Grundsätzlich wird die Netzwerksegmentierung anhand von sowohl virtuellen LANs (VLANs) als auch physisch voneinander getrennten LANs umgesetzt. Das Firmennetz wird dabei in verschiedene Bereiche unterteilt. In den meisten Fällen erfolgt die typische Unterteilung des Unternehmensnetzwerks in ein Office-IT-Netz, in dem alle Arbeitsplatzrechner miteinander verbunden sind, und ein Produktionsnetz. In diesem Produktionsnetz sind dann alle Produktionssysteme miteinander vernetzt, u. a. auch die unsicher gewordenen Windows-XP-Rechner, sofern diese noch im Einsatz sind. Das in aller Regel stärker gefährdete Produktionsnetz wird dann oftmals zusätzlich noch in weitere Sicherheitsbereiche unterteilt.

Die zwei am häufigsten verwendeten Architekturen, um eine Netzwerksegmentierung technisch umzusetzen, sind die Segmentierung mittels VLAN und die sogenannte Jumping Host Methode.

VLAN versus Jumping Host

Bei der Segmentierung mittels VLANs wird das Netzwerk im Grunde auf logischer Ebene (OSI-Layer 2) über die entsprechenden VLANs durchgeführt. Entweder wird bei dieser Methode ein Switch an sich unterteilt oder es werden den einzelnen Datenframes eine eigene VLAN-Kennung zugewiesen. Letzteres wird auch „tagged VLAN" genannt und bietet die Alternative, auch mehrere VLANs über nur eine Kabelstrecke zu betreiben.

In der Regel verwendet man zusätzlich zur Netzwerksegmentierung auch, entsprechend der jeweiligen Segmente zugeordnet, eine oder mehrere Firewalls. Ein segmentiertes Netzwerk bietet ein hohe IT-Sicherheit für Unternehmensserver, auf denen Daten von hoher Kritikalität gespeichert sind. Die Erkennungs- und Abwehrmechanismen eines Unternehmens in Bezug auf Cyberangriffe werden besser, je mehr ein Netzwerk segmentiert wird. Im Falle einer hohen Netzwerksegmentierung können die angesprochenen Cyberangriffe verlangsamt werden, da die Angriffe frühzeitiger erkannt werden können. Schutzmaßnahmen für höhere IT-Sicherheit lassen sich einfacher, effizienter und qualitativer umsetzen, wenn Netzwerke, Daten und Prozesse klar getrennt sind. Auch in Bezug auf den Datenschutz bietet Netzwerksegmentierung eine gute Möglichkeit, die vom Gesetzgeber veröffentlichten Richtlinien zu unterstützen.



Ist die Netzwerksegmentierung abschließend umgesetzt worden, empfiehlt es sich, einen Belastungs- bzw. einen Penetrationstest durchzuführen. Mit Hilfe dieser Tests kann man im Anschluss an eine durchgeführte Segmentierung des unternehmensinternen Netzwerkes testen, ob diese auch erfolgreich umgesetzt wurde bzw. belastbar ist. Ein Penetrationstest soll hier die noch offenen Schwachstellen aufdecken. Er prüft im besten Falle, wie verwundbar das System wirklich ist und kann ggf. Aufschluss darüber geben, ob die Netzwerksegmentierung sinnvoll gestaltet wurde oder ob es weiteren Verbesserungsbedarf gibt.

Fazit

U. a. führen alte Geräte mit alten Anwendungen zu erhöhten Sicherheitsrisiken. Durch Netzwerksegmentierung können Risiken und potentielle Schadenhöhen verringert werden. Notwendig sind hierfür eine kluge Architekturwahl, Implementierung und Überwachung.

Aufbau eines (IT-)Notfallhandbuchs

In der letzten Ausgabe des novus IT haben wir die theoretischen Hintergründe sowie die einzelnen Bestandteile eines (IT-)Notfallkonzepts vorgestellt. Zusammenfassend wird, ausgehend von der Business Impact Analyse (BIA), bei der die Identifikation sämtlicher Prozesse eines Unternehmens und deren Aufgliederung nach ihrer Kritikalität erfolgt, ein Handlungsbedarf festgelegt. Nach einer entsprechenden Kosten-Nutzen-Analyse werden darauf Kontinuitätsstrategien abgeleitet, die letztendlich im Notfallhandbuch festgehalten und veröffentlicht werden. Diese Vorgehensweise orientiert sich an den Empfehlungen des BSI.

Nicht vollständig deutlich wird in den Angaben des BSI der inhaltliche und strukturelle Aufbau sowie die Abfolge der Bestandteile des Konzepts. Wie sieht also ein (optimales) Notfallhandbuch, welches das Produkt dieser Prozesse innerhalb des Notfallmanagements darstellt, tatsächlich aus?

Form und Gliederung

Das Notfallhandbuch sollte grundsätzlich übersichtlich sein, so dass im Notfall die entsprechenden Stellen schnell gefunden und die darin enthaltenen Informationen genutzt werden können. Daher sollte eine Einteilung in zweckmäßige Kapitel vorgenommen werden.

Ein allgemeiner Teil, der Informationen über das Dokument, Definitionen, übergeordnete Ansprechpartner und die Meldung von Notfällen enthält, sowie ein spezieller Teil, welcher Handlungsanweisungen für einzelne Notfälle beinhaltet, wird dabei empfohlen.

Eine Beispielgliederung könnte folgendermaßen aussehen:

- 1. Einleitung: Über dieses Handbuch
- 2. Notfalldefinition
- 3. Verantwortlichkeiten & Personen
- 4. Meldung von Notfällen
- 5. Handlungsanweisungen je Notfall
- 6. Notfallvorsorge & -übungen
- 7. Anlagen

Allgemeiner Teil

Einer Einführung mitsamt kurzer Anleitung zur Nutzung des Dokuments sollte eine im Unternehmen anerkannte Definition des Begriffs „Notfall" folgen. Dies schafft ein einheitliches Verständnis und dient später dazu, zwischen normalen Incidents aus dem Tagesgeschäft und echten Notfällen unterscheiden zu können. Eine allgemeine Vorgehensweise zum Ablauf eines Notfalls in Form eines Flussdiagramms kann außerdem erste Anhaltspunkte für die notwendigen Handlungen geben.

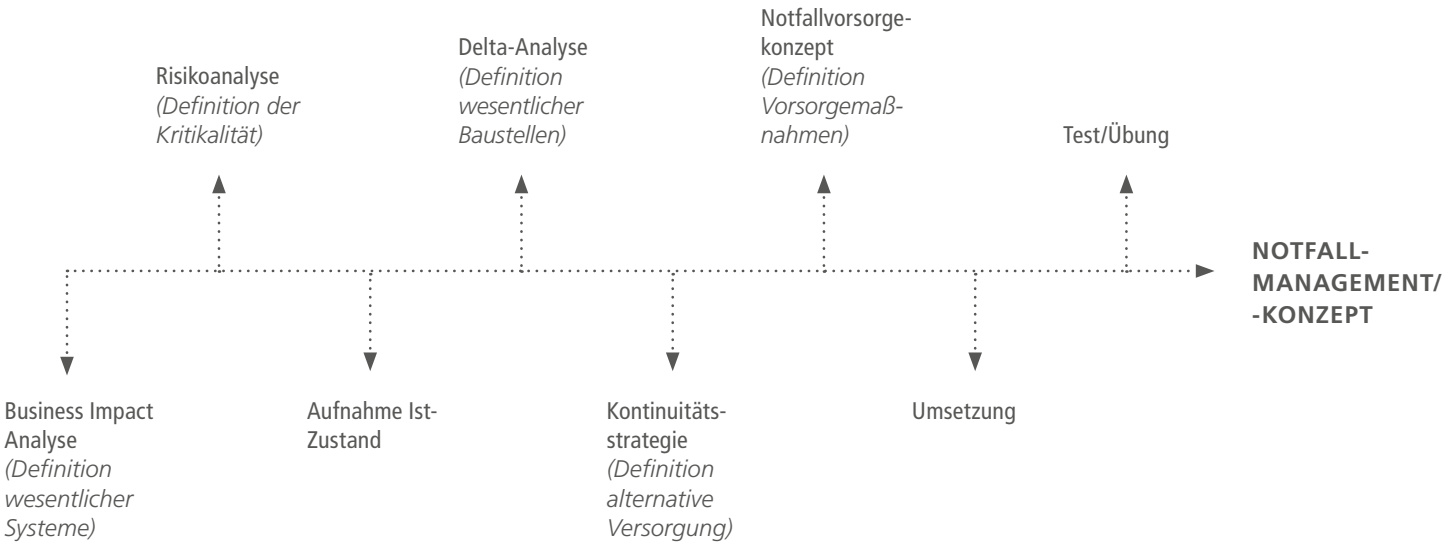
Beispiele: Tritt ein Störfall ein, muss zuerst überprüft werden, ob dieser auch einen Notfall nach der allgemeinen Definition begründet. Liegt ein Notfall mit akuter Lebensgefahr vor, sollte das Unternehmen grundsätzlich sofort evakuiert und zuständige Behörden, wie die Polizei und Feuerwehr, informiert werden – unabhängig von den Details des speziellen Falls.

Darüber hinaus sollten im allgemeinen Teil Personen genannt werden, die Ansprechpartner im Zusammenhang mit Notfällen sind. So können z. B. je nach Fall ein spezieller Krisenstab gebildet oder einzelne Notfallteams und „Recovery-Teams" für den Wiederanlauf – je nach Bereich – definiert werden. Des Weiteren ist es von Vorteil, eine globale Meldestelle einzurichten, bei der jeder potentielle Notfall sofort gemeldet wird. Diese kann die Meldung dann ggf. inhaltlich einschätzen und möglicherweise weiterleiten. Dort sollte auch die Form der Meldung definiert werden. Diese sollte stets möglichst sachlich, vollständig und inhaltlich korrekt durchgeführt werden.

Spezieller Teil

Hier werden separate Handlungsanweisungen für jeden kritischen Notfall definiert und dokumentiert. Es sollte insbesondere darauf geachtet werden, angemessen zur Größe und Komplexität des Unternehmens nur die wirklich kritischen und potentiell auch eintreffenden Notfälle (vgl. BIA) auszuwählen und aufzulisten. Eine endlose Aufzählung von möglichen Notfällen führt in diesem Zusammenhang nicht unbedingt zu steigender Sicherheit, sondern zu einer fehlenden Übersichtlichkeit.

Alternativ kann die Einteilung von Notfällen nach Themengebieten hilfreich sein. Bspw. „Ausfall von Netzwerkkomponenten" sowie „Auftreten eines Brandes". Je Gebiet sind Mitarbeiter zu benennen, die für die Überwachung sowie die Wiederherstellung zuständig sind. Auch mögliche externe Ansprechpartner, wie Dienstleister oder Behörden, sind hier aufzuführen.



Für den einzelnen Notfall sind Maßnahmen aufzulisten, die in gegebener Reihenfolge durchzuführen sind. Hier sollten stets mögliche Abwandlungen der Notfälle bedacht werden. Die Maßnahmen sind dann ggf. vom zuständigen Mitarbeiter nach eigenem Ermessen anhand von gegebenen Kriterien zu priorisieren. Die Prozesse sollten jedoch so definiert werden, dass im Notfall ein sachverständiger Dritter die Maßnahmen in einer angemessenen Zeit durchführen kann.

Ein Verweis auf die Dokumentation der zugehörigen Notfallvorsorge und -übungen sollte außerdem angefügt werden, um einen Überblick über alle Aktivitäten im Zusammenhang zu erhalten. Sämtliche Dokumente sind stets auf Aktualität zu überprüfen. Die zugehörigen Übungen sollten außerdem regelmäßig durchgeführt und protokolliert werden.

Fazit

Der tatsächliche Aufbau und Inhalt von Notfallhandbüchern weichen in der Praxis häufig von den zuvor genannten Vorgaben ab. Anstatt ausführlicher Prozessdefinitionen, Handlungsanweisungen und Verantwortlichkeiten, werden entweder Schlagworte zur Lösung eines Notfalls ohne ausreichende Details genannt oder sich zu tief im Detail verloren. Die entsprechenden Dokumente sollen dazu dienen, dass sowohl eingeweihte Mitarbeiter als auch nicht geschulte Dritte mit Hilfe der vorliegenden Informationen im Notfall optimal agieren und den Geschäftsbetrieb möglichst schnell wiederherstellen können. Notfälle können damit effektiv eingedämmt und größere Schäden verhindert werden. Auch die Auseinandersetzung mit dem breiter gefassten Notfallkonzept trägt bereits dazu bei, Risiken im Geschäftsablauf zu identifizieren und geeignete Maßnahmen zur Risikominimierung herauszuarbeiten. Regelmäßige Notfallübungen stärken außerdem die Effektivität der definierten Handlungen.

Letztendlich ist die Anfertigung eines Notfallhandbuchs keine Pflicht, sondern jedem Unternehmer selbst überlassen. Die intensive Befassung mit dem Themenkomplex des Notfallkonzepts ist allerdings uneingeschränkt zu empfehlen und als Chance sowie Instrument des Risikomanagements und nicht als lästiges Beiwerk zu sehen.

Die dunkle Seite der Technologie: Deepfakes – CEO-Fraud 2.0

Social Engineering („CEO-Fraud 1.0" oder der digitale Enkeltrick) ist weiterhin eine gängige Methode, um an sensible Geschäftsgeheimnisse oder Geld zu kommen. Dies stellt gleichzeitig eine hohe Gefahr für die IT-Sicherheit dar, weil sie technische Abwehrmaßnahmen umgehen. Was aber, wenn sich auch diese Branche auf Basis neuerer Technologien weiterentwickelt? Künstliche Intelligenz (KI) und Machine Learning (ML)-basierte Deepfakes sind eine derartige Weiterentwicklung.

Deepfakes – abgeleitet von den Begriffen Deep Learning und Fake – sind simple aber bösartige Mittel der Manipulation von Bild-, Video oder Audiodateien, bei der biometrische Merkmale wie bspw. Aussehen oder Stimme von CEOs täuschend echt imitiert werden, sozusagen CEO-Fraud 2.0. Die Folgen eines erfolgreich durchgeführten Deepfake können für Unternehmen sowohl aus Datenschutzgründen als auch aus finanzieller Sicht verheerend sein.

Was sind Deepfakes?

Grundsätzlich versteht man unter Deepfakes ein mit Hilfe künstlicher Intelligenz hergestelltes Bild, Video oder eine Sprachsimulation. Dies wirkt augenscheinlich authentisch, ist es aber nicht. Der Unterschied zwischen einem originalen Video und der manipulierten Sequenz ist kaum zu erkennen.

Auch die unsachgerechte Verwendung einer aufgenommenen Sprachsequenz kann schon zu Manipulationen mittels Deepfake führen:

Der erste, öffentlich gewordene Betrugsfall ereignete sich bei einer britischen Gesellschaft, bei der der Geschäftsführer durch einen solchen Deepfake manipuliert wurde. Der angebliche Anruf des CEOs der deutschen Muttergesellschaft, welcher eine Transaktion über 220.000 Euro auf ein durch ihn angegebenes Konto beauftragte, stellte sich schlussendlich als Fälschung mit erheblichem Schaden dar. Betrüger haben mit einer Deepfake-Software die Stimme des CEO nachgeahmt. Man spricht in diesem Zusammenhang von einem „C-Level-Fraud", einer Weiterentwicklung des klassisches E-Mail-Phishings.

Solche Deepfake-Software arbeitet im Hintergrund mit künstlicher Intelligenz und erstellen mit Hilfe von Machine Learning, genauer gesagt mit Deep-Learning-Algorithmen, die oben beschriebenen Fälschungen. Werden Videos manipuliert, wird die gefälschte Sequenz in Einzelbilder aufgesplittet und das zu fälschende Objekt analysiert. Bei dieser Analyse werden die gesplitteten Einzelbilder der Quelle und die des Ziels per Gesichtserkennung abgeglichen. Dieser Prozess ist das sog. Training. Am Ende wird dann das neue Zielobjekt über das ursprüngliche Original geblendet und im Film ersetzt.

Welche Bedrohungen können sich für Unternehmen ergeben?

Die Computersoftware zum Nachahmen von Gesichtszügen und Sprechweisen hat sich so schnell weiterentwickelt, dass die Produktion von Deepfakes keine anspruchsvolle Aufgabe mehr ist, aber eine zunehmend ernstzunehmende Gefahr darstellt – und zwar sowohl für Politik als auch für die Wirtschaft. Besonders hohe Gefahren verbergen sich für Unternehmen in den Bereichen Datenschutz, Finanzen und Personal. Die Zielsetzung eines Deepfakes kann die finanzielle Vorteilsnahme, Verletzung von Persönlichkeitsrechten, Anschuldigungen oder gefälschte Auseinandersetzungen sein. Selbst im privaten Umfeld könnte Deepfakes in spezieller Form des Enkeltricks Anwendung finden.

Neben den Gefahren des Geldabflusses durch Betrug oder Erpressung (z. B. Androhung von Pleitemeldungen), droht den Unternehmen durch Deepfakes bspw. die Manipulation von Vorstellungsgesprächen, die mittlerweile häufig über Videotelefonie oder Telefoninterviews stattfinden, sowie Datenpannen und Imageverlust. Weiterhin wird die Thematik „Fake News" durch Manipulationen per Deepfakes immer kritischer und kann Einfluss auf Unternehmensentscheidungen nehmen.

Die Unterscheidung zwischen Original und Fälschung wird immer mühevoller. In vielen Fällen wird dies nur noch Experten gelingen. Zu beachten ist, dass die Schwachstelle hierbei der Mensch selbst bleibt. Es muss ein Maß an Sicherheitsbewusstsein bestehen, um eine Bedrohung durch Deepfakes zu enttarnen.

Die innovative Informationstechnik hinter Deepfakes bietet eine Menge Potential für viele Wirtschaftszweige, aber leider auch für viele Kriminelle. Die Technik muss durchaus kritisch betrachtet werden und stellt die Sicherheitsexperten vor große Herausforderungen. Noch bis vor ein paar Jahren war diese Art von Manipulation nur Softwareentwicklern und Video-Experten möglich. Heute können Bilder, Videos oder Tonsequenzen ganz einfach mit Hilfe von Desktop-Apps wie bspw. „Fake App" erstellt werden.

Möglichkeiten zur Prävention

Im Sommer 2018 hat ein US-Forscher eine bis dato revolutionäre Methode veröffentlicht, Deepfakes im Vorhinein zu erkennen. Es handelt sich um eine Anti-Deepfake-KI, welche anhand der Lidschläge erkennen kann, ob es sich um eine Videofälschung oder ein Original handelt.

Allerdings müssen sich die Methoden zur Erkennung von Deepfakes mit der Weiterentwicklung der Deepfake-Techniken ständig verbessern. Es ist davon auszugehen, dass die Forensik-Werkzeuge heutzutage nur noch wenige Monate aktuell sind, wohingegen sie früher über Jahre aktuell waren. Durch die gezielte Weiterentwicklung von künstlicher Intelligenz werden Deepfakes zu immer natürlicheren und authentischeren Ergebnissen führen, woraus für Unternehmen, natürliche Personen und Politik immer größere Gefahren drohen.

Daher ist insbesondere das Sicherheitsbewusstsein (Security-Awareness) auch in diesem Zusammenhang ein sehr wichtiges Mittel, um dieser Gefahr zu begegnen. Es gilt im Unternehmen ein Bewusstsein zu schaffen und darzulegen, welche Präventionsmöglichkeiten es gibt. Dies gilt insbesondere auch für Deepfakes, da diese noch nicht die mediale Präsenz haben wie andere Methoden.

ANSPRECHPARTNER

DÜSSELDORF

Christian Wieder
CISA, CRISC
Tel.: +49 211 91332-650
Christian.Wieder@ebnerstolz.de

HAMBURG

Holger Klindtworth
CISA, CIA, CISM
Tel. +49 40 37097-220
Holger.Klindtworth@ebnerstolz.de

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

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

KÖLN

Thomas Heithausen
Wirtschaftsprüfer, Steuerberater, CISA,
ISO/IEC 27001 Lead Auditor
Tel. +49 221 20643-24
Thomas.Heithausen@ebnerstolz.de

MÜNCHEN

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

Michael Burkhardt
CISA, CRISC,
ISO/IEC 27001 Lead Auditor
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

ANSPRECHPARTNER
ESECURITY-CERT GMBH

Gerd Niehuis
Lead Auditor ISO 27001 (nativ) / EnWg,
Prüfer § 8a (3) BSIG
Tel. +49 211 540148-01
Gerd.Niehuis@esecurity-cert.com

Marc Alexander Luge
CISA, CASA, ISO/IEC 27001 Lead Auditor
Tel. +49 211 540148-02
Marc.Luge@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

Fotonachweis:
Alle Bilder: © www.gettyimages.com