# Cybersecurity

Kipker

2020
ISBN 978-3-406-73011-5
C.H.BECK

Überdies existieren für einzelne Arten des Outsourcing Prüfungsstandards. Beim Outsourcing von rechnungslegungsrelevanten Prozessen sieht zB der **IDW RS FAIT 5** vor, dass die Grundsätze ordnungsgemäßer Buchführung (→ Rn. 56 ff.) auch beim Outsourcing-Dienstleister zu beachten sind. Darüber hinaus sind Wirtschaftsprüfer nach **IDW PS 331** dazu verpflichtet, die ausgelagerten Prozesse des zu prüfenden Unternehmens und deren Kontrollen im Rahmen ihrer IKS-Prüfung (→ Rn. 59) zu berücksichtigen. 99

## IV. Das Internet der Dinge (IoT)

Das (industrielle) Internet der Dinge beschreibt die weitreichende Vernetzung von Gegenständen, Gebäuden, Maschinen und Objekten, um zB Daten über Personen zu aggregieren und Serviceleistungen besser auf diese zuzuschneiden; ein bekanntes Beispiel ist die sog. Smart Watch. Diese Vernetzung verändert Produktions- und Arbeitsprozesse, Geschäftsmodelle, aber auch das Konsumverhalten nachhaltig. 100

Aus dieser umfassenden Vernetzung können sich **erhebliche Cybersicherheitsrisiken** ergeben. Vernetzte Geräte begleiten Endnutzer oft in besonders schützenswerten privaten und intimen Lebensbereichen, die daraus generierten Daten können in Kombination mit anderen Informationen ein vollständiges Bild bestimmter Eigenschaften einer Person generieren und können somit für Angreifer von besonderem Interesse sein.[128] Systeme mit Netzwerkanbindung sind grundsätzlich aus diesem Netzwerk heraus angreifbar; Maßnahmen zur Datensicherheit sind unerlässlich.[129] So attestierte die länderoffene Arbeitsgruppe „Cybersicherheit" der Innenministerkonferenz dem Internet der Dinge „ohne ausreichende Sicherheitsvorkehrungen eine erhebliche Bedrohung für den Cyberraum".[130] Dem sollen vor allem **Mindestsicherheitsstandards** entgegenwirken, die insbesondere durch ein einheitliches Gütesiegel für IT-Produkte etabliert werden, das die Bundesregierung in ihrer Cybersicherheitsstrategie von 2016 vorgestellt hat.[131] Auch die sich noch im (bald abgeschlossenen) Rechtsetzungsverfahren befindliche europäische **Cybersecurity-Verordnung**[132] wird insoweit eine Rolle spielen (→ Kap. 16) (Cybersecurity-VO-E). Eine IT-Sicherheitszertifizierung könnte zukünftig durch die Europäische Agentur für Netz- und Informationssicherheit (ENISA) erfolgen (vgl. Art. 44 ff. Cybersecurity VO-E). 101



Eine ähnliche Entwicklung wird auch durch die „Charter of Trust" vorgezeichnet. Hierbei handelt es sich um ein im Rahmen der Münchner Sicherheitskonferenz 2018 von Technologiefirmen formuliertes Regelwerk zur Cybersicherheit. Die unterzeichnenden Unternehmen attestieren damit ihre Bestrebung, ein **Identitäts-Management** für IoT-Geräte, eine konsequente sichere **Verschlüsselung** der Daten und Kommunikation sowie die kontinuierliche Versorgung mit **Updates** zu gewährleisten.[133] Ferner wird angeregt, eine **Sicherheitszertifizierung** (nur) von Kritischen Infrastrukturen und Produkten im IoT zu etablieren.[134] Die Unternehmen verbinden somit ihre Anstrengungen zur ord- 102

[128] *Šehić/Rengers/Hense,* DSRI-TB 2015, 393 (401).
[129] *Schöttle,* DSRI-TB 2015, 365 (374).
[130] Sachstandsbericht der AG Cybersicherheit der IMK vom 20.11.2017, https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2017-12-07_08/anlage-zu-top-8.pdf (3.7.2018).
[131] Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016, S. 9, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (3.7.2018).
[132] Momentan: „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit")".
[133] „Charter of Trust", Nr. 2, https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/shi-13378-cot-dok-narrative-washington-online-2018-05-04-sbi-en.pdf (3.7.2018).
[134] „Charter of Trust", Nr. 7, https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/shi-13378-cot-dok-narrative-washington-online-2018-05-04-sbi-en.pdf (3.7.2018).

nungsgemäßen Erfüllung der Legalitätspflicht als Ausprägung der Leitungs- und Sorgfaltspflicht ihrer Geschäftsführungen (→ Rn. 43). Dies wird dazu beitragen, einen einheitlichen Rahmen für die inhaltliche Ausgestaltung dieser Pflichten zumindest in Hinblick auf große Unternehmen zu bilden.

103 Jenseits einer Zertifizierung von IoT-Produkten stellt sich bereits im Hinblick auf die kontinuierliche Gewährleistung der Sicherheit eingespielter Software die Frage nach einer Realisierbarkeit am Markt. So muss in IoT-Produkten verwendete Software regelmäßig geupdated werden, um ihre kontinuierliche Sicherheit auch angesichts festgestellter Sicherheitslücken und stets neuer Bedrohungen im Internet durch Malware, Viren oä zu gewährleisten[135]; insoweit besteht die Verpflichtung zur Etablierung eines umfassenden und aktuellen **Patch-Management-Systems.**[136] Grundsätzlich bestünde diese Pflicht nur bis zum Ablauf der Produktgewährleistung – sollte aber zB bei einem vernetzten Kühlschrank nach einigen Jahren der Softwaresupport eingestellt werden, könnte dieser hiernach trotz eigentlicher technischer Funktionsfähigkeit aufgrund einer Sicherheitslücke unbrauchbar werden. Dies wird für die meisten Verbraucher ein nicht tragbares Risiko sein; demgegenüber würde ein jahrzehntelanges Patch Management für die meisten Unternehmen zu aufwändig und wenig lohnenswert sein. Lösungsansätze für diese Problematik sind bislang, auch aufgrund der noch nicht eingesetzten generellen Marktreife vernetzter Produkte, zumeist spärlich. Die Artikel 29-Datenschutzgruppe (heute: Europäischer Datenschutzausschuss) bedenkt die Thematik in ihrem Working Paper 223 mit dem Hinweis, dass Kunden mitzuteilen ist, wann Software-Updates für Geräte eingestellt werden.[137]

104 Über diese Bestrebungen hinaus gelten für das IoT, soweit hierdurch personenbezogene Daten erfasst oder verwertet werden, die datenschutzrechtlichen Pflichten zur Ergreifung angemessener technischer und organisatorischer Maßnahmen (Art. 24, 25 DS-GVO), und außerdem, soweit es sich um einen Telekommunikationsdienst handelt, die Vorgaben der §§ 109 f. TKG (→ Rn. 32 f.).[138]



## V. Bring Your Own Device

105 Spezielle IT-Sicherheitsrisiken bestehen auch bei der zusehends populärer werdenden Praktik der **Einbindung privater Endgeräte** (Smartphones, Laptops, Tablet-PCs) **in die IT-Struktur des Unternehmens,** auch als „Bring Your Own Device" (BYOD) bezeichnet. Die von den Mitarbeitern eingebrachten Geräte werden sowohl privat, als auch dienstlich genutzt. Vorteile bestehen hierbei zum einen für den Arbeitgeber, der sich unter anderem eine höhere Mitarbeiterzufriedenheit und eine Kostenersparnis erhofft, zum anderen auch für den Arbeitnehmer, der idR kein zweites Gerät zu Arbeitszwecken mit sich führen wollen wird.[139] Zu differenzieren ist beim BYOD zwischen der bloßen **Vornahme betrieblicher Handlungen auf privaten Geräten** (zB Führen von Telefonaten mit Kunden) und einer darüber hinausgehenden **Anbindung an das unternehmensinterne Netzwerk** (zB Zugriff auf die unternehmensinterne Kundendatenbank via VPN-Verbindung).[140] Eine weitere Erscheinungsform ist auch das sog. „**unechte BYOD**". Dies bezeichnet die Zurverfügungstellung von Endgeräten durch den Arbeitgeber und die Erlaubnis ihrer (auch) privaten Nutzung.[141]

---

[135] *Beukelmann,* NJW-Spezial 2017, 376 (376).
[136] *Schöttle,* DSRI-TB 2015, 365 (374).
[137] Artikel 29-Datenschutzgruppe, WP 223, S. 22.
[138] *Grünwald/Nüßing,* MMR 2015, 378 (383).
[139] *Zöll/Kielkowski,* BB 2012, 2625 (2625); *Wisskirchen/Schiller,* DB 2015, 1163 (1163).
[140] Forgó/Helfrich/Schneider/*Helfrich,* Betrieblicher Datenschutz, Teil IV. Kap. 2 Rn. 4 f.
[141] Forgó/Helfrich/Schneider/*Helfrich,* Betrieblicher Datenschutz, Teil IV. Kap. 2 Rn. 9.

BYOD wirft als Bestandteil der unternehmerischen IT-Compliance Probleme in diversen Rechtsbereichen auf. Hierzu gehören neben arbeits- und urheberrechtlichen Bestimmungen insbesondere die IT-Sicherheit und der Datenschutz. 106

## 1. IT-Sicherheit

Insbesondere für den vielleicht häufigsten Fall von BYOD, der **Datenverarbeitung via Smartphone,** besteht eine **besondere Gefährdungslage** der IT-Sicherheit. So sind Smartphones nicht nur handlich und werden idR stets am Körper geführt, wodurch sie schnell zum Ziel eines Diebstahls werden können. Ihre stetig steigenden Speicherkapazitäten erlauben es auch, ein hohes Volumen an potenziell sensiblen Informationen abzuspeichern. Dazu sind Log-In-Daten, zB für E-Mail-Programme, meist auf den Smartphones hinterlegt, wodurch im Falle einer Entwendung durch Nichtberechtigte auf diese zugegriffen werden kann. Auch durch die hohe Anzahl an Netz-Schnittstellen (USB, WLAN, Bluetooth) ergeben sich zusätzliche Angriffspunkte, wenn diese nicht korrekt abgesichert werden. Zusätzlich existiert immer mehr auf Smartphones und Mobile Devices spezialisierte Schadsoftware, die Hacker zB in Apps tarnen, die durch Downloads im App Store auf den Geräten installiert werden. 107

Aufgrund dieser Gefährdungslage ist es notwendig, im Falle des Einsatzes von BYOD in besonderem Maße auf die Sicherheit der genutzten Geräte zu achten. Dies folgt für die **Unternehmensleitung** auch aus der Pflicht zur sorgfältigen Unternehmensführung des § 76 Abs. 1 AktG bzw. der Sorgfalt des ordentlichen Geschäftsmanns aus § 43 Abs. 1 GmbHG (→ Rn. 42 ff.).[142] Ebenfalls sind dem Steuerrecht entstammende Pflichten zur **revisionssicheren Aufbewahrung** erstellter betrieblicher Dokumente zu berücksichtigen (§ 147 AO).[143] Zur ordnungsgemäßen Erfüllung dieser Pflichten ist es notwendig, im Rahmen der **unternehmensinternen IT-Sicherheitsstrategie** auch den Einsatz von BYOD im Unternehmen zu berücksichtigen und ggf gesondert zu regeln, wobei dies zB in den **Betriebsrichtlinien** verankert werden kann.[144] Beim „unechten" BYOD bietet es sich an, das Aktualisierungs- und Patch-Management zentral durch ein Programm zu administrieren (**Mobile Device Management,** MDM), um die Aktualität und Einheitlichkeit des Sicherheitsniveaus der genutzten Geräte zu gewährleisten.[145] Ein solch umfassender Zugriff wird aber bei der betrieblichen Nutzung privater Endgeräte („echtes" BYOD) in aller Regel einen zu intensiven Eingriff in die Privatsphäre des Mitarbeiters darstellen. Zur Identifikation bestehender Risikofelder beim Einsatz von Smartphones für BYOD und Bestimmung der dahingehend zu ergreifenden Maßnahmen hat das BSI einen Fragenkatalog angefertigt, der unter anderem folgende Fragen enthält[146]: 108

- Lassen sich die Geräte zentral administrieren und updaten?
- Können zuverlässige und regelmäßige Datensicherungen durchgeführt werden?
- Gibt es Mechanismen zur Identifikation und Authentisierung der Benutzer?
- Können die auf den Geräten gespeicherten Daten verschlüsselt werden oder Daten sogar verschlüsselt übertragen werden? Sind die bestehenden Verschlüsselungsmechanismen auf dem aktuellen Stand der Technik?
- Sind zusätzliche Sicherungsmechanismen vorgesehen (zB Virenschutz, Spam-Filter) bzw. können solche nachträglich auf den Geräten installiert werden?



[142] *Zöll/Kielkowski,* BB 2012, 2625 (2625).
[143] *Koch,* ITRB 2012, 35 (36).
[144] BSI, Überblickspapier Smartphones, S. 6, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf (22. 8. 2018).
[145] Kramer/*Hoppe,* IT-ArbR, Rn. 636; BSI, Überblickspapier Consumerisation und BYOD, S. 4, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf (22. 8. 2018).
[146] BSI, Überblickspapier Smartphones, S. 6. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf (22. 8. 2018).

109 Regelmäßig wird es beim echten BYOD so sein, dass eine **Vielzahl unterschiedlicher Gerätetypen, -modelle und -hersteller** eingesetzt werden. Dies stellt eine zusätzliche Schwierigkeit für die wirksame Gewährleistung der IT-Sicherheit dieser Geräte dar, da sich deren Sicherheitsarchitekturen und -programme je nach Gerätetyp und auch Betriebssystem-Version unterscheiden. Werden verschiedene Geräte zum BYOD genutzt, bietet es sich daher an, eine **Übersicht** über die durch die Mitarbeiter verwendeten Geräte und deren Sicherheitsmechanismen anzufertigen, um potenziell unsichere Geräte zu identifizieren und diese nachzurüsten oder, im schlimmsten Fall, deren Benutzung für betriebliche Zwecke zu untersagen.[147] Um eine solche Übersicht aktuell und komplett zu halten, ist nicht nur eine **regelmäßige Aktualisierungsstrategie,** sondern auch eine **klare Kommunikation** zwischen Mitarbeitern und Geschäftsleitung bzw. dem hierfür Verantwortlichen (zB dem IT-Sicherheitsbeauftragten) zu gewährleisten.

110 Zum Schutz der unternehmensinternen Informationen bei Verlust des Geräts sollte der Einsatz einer **Löschung oder Deaktivierung per Fernzugriff** überlegt werden.[148] Da diese jedoch datenschutzrechtlich nicht unproblematisch ist, sollte diese Funktionalität in Individual- oder Betriebsvereinbarungen ausdrücklich legitimiert werden. Auch sollten Verbindungen mit der IT-Infrastruktur des Unternehmens, zB der Zugriff auf Datenbanken oder den betrieblichen E-Mail-Account, stets **verschlüsselt** erfolgen. Unverschlüsselte Verbindungen zum Austausch geschäftsrelevanter Daten sollten explizit für unzulässig erklärt werden. Zusätzlich sind nicht nur die von den Geräten ausgehenden Risiken, sondern auch der **menschliche Risikofaktor** zu minimieren. Hierfür sollten **regelmäßige Mitarbeiterschulungen** stattfinden, um Mitarbeiter, die BYOD nutzen oder nutzen möchten, für die Gefahren und den sicheren Umgang mit ihren mobilen Geräten zu sensibilisieren.[149]



### 2. Datensicherheit und Datenschutz

111 Eine Verpflichtung zur Datensicherheit enthält insbesondere auch der Art. 24 Abs. 1 DS-GVO, wonach geeignete **technische und organisatorische Maßnahmen** zur Einhaltung des Datenschutzrechts ergriffen werden müssen. Die **Integrität und Vertraulichkeit verarbeiteter personenbezogener Daten** als Teilbereich der IT-Sicherheit ist nach Art. 5 Abs. 1 lit. f DS-GVO diesbezüglicher Bestandteil der zu ergreifenden Maßnahmen. Somit muss ein Arbeitgeber beim Einsatz von BYOD in der durch seine Mitarbeiter erfolgenden Datenverarbeitung (zB beim Führen von betrieblichem E-Mail-Verkehr oder der Abwicklung von Kundenanfragen) entsprechende technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der hierbei verarbeiteten personenbezogenen Daten vornehmen.[150]

112 **Technisch** sind die Geräte vor allem gegen den Zugriff unbefugter Dritter auf die auf ihnen gespeicherten Daten zu schützen. Hier kommen **Zugangssperren** wie ein Passwortschutz oder eine Verschlüsselung der Daten in Betracht, sowie Schutzmaßnahmen im Falle eines Diebstahls oder Verlusts.[151] Außerdem empfiehlt sich insbesondere die Einführung einer **Virtualisierungstechnologie** zur Minimierung der auf den Endgeräten gespeicherten Daten. So können relevante Daten auf dem Unternehmensserver statt auf dem Endgerät abgelegt werden, damit ein Verlust des Endgeräts nicht automatisch auch zu einem Datenverlust führt.

---

[147] BSI, Überblickspapier Smartphones, S. 7, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf (22. 8. 2018).
[148] BSI, Überblickspapier Smartphones, S. 7, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf (22. 8. 2018).
[149] BSI, Überblickspapier Consumerisation und BYOD, S. 5, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf (22. 8. 2018).
[150] Auer-Reinsdorff/Conrad/*Conrad,* IT- und Datenschutzrecht, § 37 Rn. 294 ff.
[151] Forgó/Helfrich/Schneider/*Helfrich,* Betrieblicher Datenschutz, Teil IV. Kap. 2 Rn. 40.

**Organisatorisch** ist die Wahrung der Grundsätze der Datenverarbeitung (wie Zweckbindung und Datenminimierung) sicherzustellen, außerdem ggf eine **Trennung** der verschiedenen Sphären entstammenden Daten. So sind die der betrieblichen Sphäre zuzuordnenden Daten von denen der privaten Sphäre des Mitarbeiters entstammenden Daten zu trennen.[152] Hierfür bietet es sich zB an, für die betriebliche Nutzung eigens dafür bestimmte und zur Verfügung gestellte sichere Software zu benutzen, die sich von der regulär privat genutzten Software unterscheidet. Ferner bietet sich zur Trennung privater und betrieblicher Daten und Anwendungen eine sog. **Zwei-Container-Lösung** an, bei der durch technische Mittel betriebliche Daten und Anwendungen in einem passwortgeschützten, separaten Bereich (Container) abgelegt werden.[153] Beliebt ist diese Lösungsmöglichkeit insbesondere, um innerhalb eines Containers ein komplettes Betriebssystem zur unternehmerischen Nutzung zu verorten (zB das Citrix-System). Wird der Container geöffnet, fährt der Computer in einem Fenster „neu hoch", zwischen den beiden Systemen lässt sich per Mausklick wechseln. Zusätzlich könnten auch die durch die private Nutzung des Arbeitnehmers produzierten Daten in einem vor dem Zugriff des Arbeitgebers gesicherten Container platziert werden, um sicherzustellen, dass der Arbeitgeber bei Software-Wartungen oä auf nicht-betriebliche Informationen keinen Zugriff hat. 113

Aus der Verpflichtung des Arbeitgebers, bei BYOD technische und organisatorische Maßnahmen zur Gewährleistung ua der Datensicherheit zu ergreifen, folgt ebenfalls das Recht, die Einhaltung und Funktionsfähigkeit dieser Maßnahmen überprüfen zu können.[154] Hierzu müssen dem Arbeitgeber gewisse **Kontrollmöglichkeiten** eingeräumt werden.[155] Problematisch ist hierbei, dass sich bei entsprechenden Kontrollen kaum verhindern lassen wird, dass ebenfalls auf privat verarbeitete Daten des Arbeitnehmers zugegriffen wird (oder eine solche Zugriffsmöglichkeit zumindest besteht). Hier könnte der Mitarbeiter dem Arbeitgeber ein **eigentumsrechtliches Abwehrrecht** aus § 903 S. 1 BGB entgegenhalten, sollte dieser versuchen, von seiner Kontrollbefugnis Gebrauch zu machen.[156] Auch arbeitsrechtlich wird dem Arbeitgeber ein Zugriffs- und Kontrollrecht abgesprochen, sofern er dabei auf private Daten des Arbeitnehmers zugreifen kann.[157] Somit besteht zwar theoretisch ein Kontrollrecht des Arbeitgebers, dieses stößt aber in der praktischen Ausübung auf erhebliche Widerstände. Eine Lösungsmöglichkeit liegt im Abschluss von **Individual- bzw. Betriebsvereinbarungen** zur Einräumung entsprechender Kontrollrechte.[158] Hierbei ist jedoch strikt das Verhältnismäßigkeitsgebot zu beachten.[159] Selbst bei Individualvereinbarungen zur Einräumung von Kontrollrechten wäre eine allumfassende, jegliche private Daten einschließende Vereinbarung ungültig. Vielmehr sind durch das Ausmaß des möglichen Zugriffs die Rechte und Interessen des Arbeitgebers und der Mitarbeiter in Ausgleich zu bringen. 114



[152] Forgó/Helfrich/Schneider/*Helfrich,* Betrieblicher Datenschutz, Teil IV. Kap. 2 Rn. 41; Auer-Reinsdorff/Conrad/*Conrad,* IT- und Datenschutzrecht, § 37 Rn. 282 ff., 294, 299.
[153] *Zöll/Kielkowski,* BB 2012, 2625 (2625); *Voigt,* IT-Sicherheitsrecht, Rn. 180.
[154] Forgó/Helfrich/Schneider/*Helfrich,* Betrieblicher Datenschutz, Teil IV. Kap. 2 Rn. 42.
[155] Auer-Reinsdorff/Conrad/*Conrad,* IT- und Datenschutzrecht, § 37 Rn. 288.
[156] Forgó/Helfrich/Schneider/*Helfrich,* Betrieblicher Datenschutz, Teil IV. Kap. 2 Rn. 45.
[157] *Conrad/Schneider,* ZD 2011, 153 (155).
[158] Forgó/Helfrich/Schneider/*Helfrich,* Betrieblicher Datenschutz, Teil IV. Kap. 2 Rn. 47; Auer-Reinsdorff/Conrad/*Conrad,* IT- und Datenschutzrecht, § 37 Rn. 289; Betriebsvereinbarungen zum Einsatz von BYOD ablehnend indes *Zöll/Kielkowski,* BB 2012, 2625 (2626).
[159] Forgó/Helfrich/Schneider/*Helfrich,* Betrieblicher Datenschutz, Teil IV. Kap. 2 Rn. 48 f.

## VIII. IT-Forensik (rechtssichere Ermittlungen nach IT-Sicherheitsvorfällen)

115 IT-forensische Analysen gewinnen bei Ermittlungsbehörden, aber auch durch das Angebot privater Dienstleister, zusehends an Bedeutung, da sie die Nachvollziehbarkeit sowie ggf. Ahndung von IT-Sicherheitsvorfällen und anschließende Verbesserung der Systemsicherheit ermöglichen bzw. vereinfachen.

### 1. Grundlagen der IT-Forensik

116 Der Begriff der IT-Forensik meint die Untersuchung und Rekonstruktion des Tathergangs bei Angriffen auf oder Schäden an IT-Systemen. Sie gliedert sich in die Bereiche der **Computerforensik** (Analyse von Geräten) und der **forensischen Datenanalyse** (Analyse von Daten und Datenbanken). Zusätzlich können die sog. „Post Mortem"-Analyse und die Live-Forensik unterschieden werden. Bei der **„Post Mortem"-Analyse** werden Sicherheitsvorfälle im Nachgang untersucht und aufgeklärt, indem Spuren, insbesondere gelöschte oder verschlüsselte Dateien, gefunden und ausgewertet werden; die **Live-Forensik** bezeichnet hingegen die Untersuchung von Sicherheitsvorfällen, während diese noch im Gange sind.[160] Hier sollen va sog. **„flüchtige Daten",** also Daten zB aus dem Arbeitsspeicher eines Systems, die nach Beendigung einer Nutzungsaktivität bzw. Herunterfahren des PCs gelöscht werden, aufgefunden und ausgewertet werden. Mit diesen Analysearten wird die IT-Forensik insbesondere bei der Krisenreaktion im Ernstfall relevant und bildet somit einen Teil des **Notfallmanagements.** Das Notfallmanagement ist seinerseits Teil des **allgemeinen Risikomanagementsystems,** das bei der Ausübung ordentlicher Sorgfalt der Geschäftsleitung einzurichten ist (→ Rn. 46 ff.). Häufig ist der Einsatz von IT-Forensikern im Ernstfall bereits in sog. **Cyberpolicen,** dh Versicherungen gegen virtuelle Angriffe auf oder Schäden an Unternehmen, mitversichert (→ Rn. 121 ff.).

117 Eine forensische Analyse zielt stets auf die Beantwortung bestimmter Fragen ab, um IT-Sicherheitsvorfälle zu aufzuklären[161]:

- **Was** ist passiert?
- **Wo** ist es passiert?
- **Wann** ist es passiert?
- **Wie** ist es passiert?

Zusätzlich können je nach Lage des konkreten Einzelfalls die folgenden Fragen relevant werden:

- **Wer** hat es getan?
- Was kann getan werden, um eine Wiederholung zu vermeiden?

Diese Fragen bestimmen das **Ziel** und den **Inhalt** der IT-Forensik.



### 2. Durchführung einer IT-forensischen Analyse

118 Die Durchführung einer IT-forensischen Analyse wird zumeist in verschiedene logisch abgrenzbare **Handlungsabschnitte** geteilt. Hierbei unterscheiden sich Modelle zB danach, ob sie von Strafverfolgungsbehörden oder von privaten Akteuren angewandt werden.

[160] BSI, Leitfaden IT-Forensik, S. 13, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf (23. 8. 2018).
[161] BSI, Leitfaden IT-Forensik, S. 22, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf (23. 8. 2018).

Für Private lassen sich IT-forensische Analysen anhand der folgenden 5 Handlungsschritte systematisieren[162]:

- **Vorbereitung**

Die Vorbereitung erfolgt sowohl strategisch als auch operational. Hierbei werden geeignete forensische Werkzeuge identifiziert und bereitgestellt. Die Kriterien, nach denen Werkzeuge als „geeignet" beurteilt werden, sollten dokumentiert werden.

- **Datensammlung**

Dieser Schritt meint die Aggregation von Daten bezüglich des Sicherheitsvorfalls von (potenziell) betroffenen Komponenten. Die Daten sind vollständig zu erfassen und zu speichern, wobei vor allem zu gewährleisten ist, dass keine Verfälschung erfolgt.

- **Untersuchung**

Bei der Untersuchung werden die für den Sicherheitsvorfall relevanten Daten extrahiert.

- **Datenanalyse**

Die extrahierten Daten werden in der Analyse logisch miteinander verknüpft und systematisiert.

- **Dokumentation**

In diesem Schritt werden die vorherigen Handlungen kontextualisiert und zu Berichten zusammengefasst. Hier lassen sich auch Handlungsempfehlungen zur zukünftigen Verbesserung der IT-Sicherheit verorten.

Jeder dieser Schritte ist sorgfältig zu dokumentieren. Denn wenn die IT-forensischen Ermittlungen der Aufdeckung und Ahndung von Straftaten dienen sollen, müssen diese **gerichtsfest,** dh vor Gericht verwertbar sein. Hierfür muss die Dokumentation von Handlungsschritten und Beweismitteln lückenlos und umfassend sein **(Chain of Custody).** Eine solche Lückenlosigkeit lässt sich ua mit der Anfertigung eines Datenträgerabbilds erreichen (sog. **forensische Duplikation**). Hierbei wird eine Kopie des jeweiligen Datenträgers erstellt, an dem Untersuchungsschritte mehrmals ausgeführt werden können, ohne dass der Originalzustand der Daten verändert wird.[163] Dies gewährleistet nicht nur die Unveränderbarkeit und somit **Integrität der Daten,** sondern auch die **Nachprüfbarkeit der Analyse** zB vor Gericht. 119



Aufgrund der hohen Sensibilität der IT-forensischen Tätigkeit ist hierbei in besonderem Maße auf die **Einhaltung von Recht und Gesetz** zu achten. So bestehen gerade bei der Verfolgung externer Angreifer oder auch bei der Auslesung privater Daten von Mitarbeitern (zB Angriff auf ein BYOD-Gerät) **Datenschutzrisiken,** die Schadensersatzforderungen oder die Verhängung von Bußgeldern zur Folge haben können. Auch kommt unter Umständen eine **strafrechtliche Relevanz,** zB nach § 202a StGB, in Betracht. Hierfür müsste sich der IT-Forensiker unbefugt Zugang zu nicht für ihn bestimmten oder gegen unberechtigten Zugriff besonders gesicherten Daten verschaffen, indem er eine Zugangssicherung überwindet. Zwar wird dies bei gesicherten Unternehmensdaten nicht der Fall sein, da hier eine Berechtigung zur Einräumung des Zugangs besteht. Anders liegt es aber zB, wenn auf einem Mitarbeiterlaptop, den dieser auch privat nutzt, auf einen passwortgeschützten privaten Ordner zugegriffen wird. 120

[162] BSI, Leitfaden IT-Forensik, S. 10, 24 f., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf (23. 8. 2018).

[163] BSI, Leitfaden IT-Forensik, S. 26, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf;jsessionid=F5352B2E403B9A838D1352EC192F4A82.1_cid369?__blob=publicationFile&v=2 (23. 8. 2018).

## VIII. Versicherungsschutz und Cyberpolicen

121 Obwohl am deutschen Markt immer noch kein Standardprodukt, schließen immer mehr Unternehmen **D&O *(Directors & Officers)*-Versicherungen** mit Cyberpolicen ab, um die aus Eigen- und Drittschäden durch Verstöße gegen das Cybersicherheitsrecht resultierenden (Haftungs-)Risiken auszulagern. Versicherungen wie ACE, Allianz, AXA, Chubb, HDI, Hiscox oder Zurich bieten entsprechende Versicherungspolicen an.

**Directors & Officers-Versicherungen:**

Unternehmen können sich durch sog. D&O-Versicherungen vor Vermögensschäden durch fahrlässige Pflichtverletzungen ihrer Gesellschaftsorgane (Vorstand, Geschäftsführung, Aufsichtsrat) absichern. Besonders hierbei ist, dass sowohl **Außenhaftungsfälle** (also ua Ansprüche von Kunden wegen Vermögensschäden, die zB durch ein Auslesen von Zahlungsdaten bei einem Hacking-Angriff auf die Server des Unternehmens entstanden sind), als auch **Innenhaftungsfälle** (Ansprüche des Unternehmens selbst gegen die für eine Pflichtverletzung verantwortlichen Organe) vom Versicherungsschutz gedeckt sind.

Allerdings besteht für versicherte Vorstandsmitglieder einer AG, SE, KGaA oder eines VVaG nach § 93 Abs. 2 S. 3 AktG ein gesetzlich festgelegter **Selbstbehalt** von mindestens 10 Prozent des entstandenen Schadens bis mindestens zur Höhe des Eineinhalbfachen der festen jährlichen Vergütung.[164] Diese Verpflichtung besteht nicht für andere Gesellschaftsformen, insbesondere nicht für GmbHs.[165]



### 1. Versicherungsschutz für Eigenschäden

122 Bei der Versicherung von Risiken ist zwischen denjenigen Gefahren, die **Eigenschäden** verursachen, und solchen, die Haftungsrisiken auslösen, also **Drittschäden** verursachen, zu unterscheiden.

Relevante Gefahren bestehen hierbei bezüglich des **Verlusts, der Zerstörung oder der Beschädigung** von Daten, Programmen und Hardware. Ferner können sich Daten und/oder Programme durch mut- oder böswillige Handlungen von Arbeitnehmern oder Dritten, Schadsoftware (Viren, Trojaner, etc.), oder auch menschliches Versagen **nachteilig verändern oder verloren gehen.**

123 Sich hieraus ergebende Schäden, die durch Cyberpolicen versichert werden können, sind unter anderem der Software- und Datenwiederherstellungsaufwand, erhöhte Betriebskosten, Betriebsunterbrechungskosten, Ausfallkosten durch Beauftragung externer Dienstleister, Kosten für Sachverständige, Berater (IT-Forensik), Rechtsanwälte und Wirtschaftsprüfer, Kosten für einen im Nachgang des Schadens erhöhten Werbeaufwand, Kosten für den Regress beim Schädiger (soweit dieser identifiziert wurde), Aufwand für Systemverbesserungen, um gleichläufige Schäden zukünftig zu verhindern, sowie Leistungen bei erpresserischer Bedrohung und Vertragsstrafen.

### 2. Versicherungsschutz für Haftpflichtansprüche

124 Gefahren, die eine Haftpflicht gegenüber Dritten auslösen können, sind unter anderem die Verletzung von Datenschutz- oder Vertraulichkeitspflichten, die unbefugte Nutzung eines fremden Computersystems oder Netzwerks oder die unbeabsichtigte Übertragung eines Computervirus auf das System eines Dritten.

---

[164] *Kerst,* WM 2010, 594 (597).
[165] *Kerst,* WM 2010, 594 (598).