2. IT-Sicherheit und Datenschutz

Mathias Lang

Key-Words: Cyberattacke, Datenverlust, IT-Sicherheit, Informationssicherheit, Datensicherheit, Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Intervenierbarkeit, Nicht-Verkettbarkeit, Datenschutz durch Technikgestaltung (data protection by design), datenschutzfreundliche Voreinstellungen (data protection by default), Stand der Technik, Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz, ISO/IEC 27001, ISO/IEC 27701, Data protection, Reputationsschutz, IT-SiG, Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG), DSGVO, Datenschutz-Folgeabschätzung, Meldepflichten, Betreiber Kritischer Infrastrukturen, Informationssicherheitsmanagementsystem, Standarddatenschutzmodell

2.1 Ausgangs-/Praxisfall

Einem Zeitarbeitsunternehmen werden über eine Hackerattacke Kunden- und Lieferantenlisten sowie Abmahnungen und Kündigungen entwendet.

Welche Maßnahmen müssen, insbesondere datenschutzrechtlich, ergriffen werden, und wie kann das Unternehmen in einem solchen Fall die Meldepflicht und Veröffentlichung nach der DSGVO evtl. von vorneherein verhindern?

Würden sich Besonderheiten ergeben, wenn ein „Betreiber Kritischer Infrastrukturen", wie etwa ein Energieversorgungsunternehmen einem Hackerangriff ausgesetzt worden wäre?

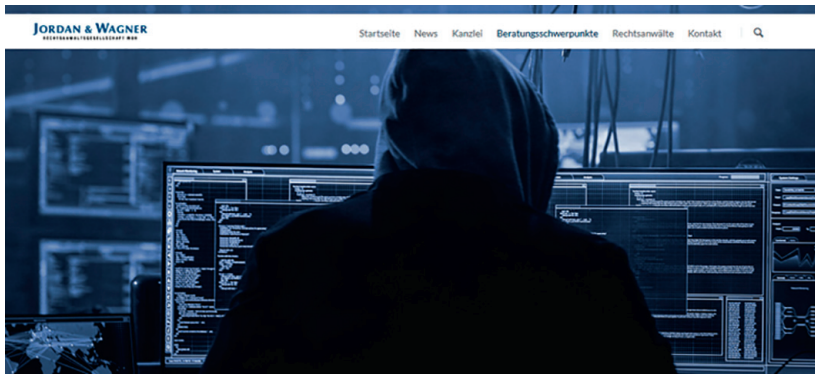

Abbildung 4

2.2 Rechtsrahmen und Zuständigkeiten

2.2.1 Begriff der IT-Sicherheit

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.[40]

Nach dieser Definition wird bereits deutlich, dass es 100%-ige IT-Sicherheit nicht geben kann.

Es geht bei diesem Bereich also um **Risikominimierung**.

Allerdings ist IT-Sicherheit nicht nur aufgrund regulatorischer Anforderungen für Unternehmen wichtig, die Medien berichten ständig von Sicherheitspannen im IT-Sektor, wie beispielsweise Datenverluste durch Hackerattacken, die für die betroffenen Unternehmen mit hohen Reputationsschäden verbunden sind und die sich entsprechend wirtschaftlich auswirken.

IT-Sicherheit ist damit gleichermaßen auch Reputationsschutz und eine Investition zur Abwehr von unkalkulierbaren Folgeschäden.

40 BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html, abgerufen am 30.06.2020.

Die Begriffe IT-Sicherheit, Informationssicherheit und Datensicherheit werden oft synonym benutzt, was jedoch nicht korrekt ist.

Während Datensicherheit den Bereich der personenbezogenen Daten i. S. der Datenschutzgesetze wie DSGVO und BDSG betrifft, geht Informationssicherheit begrifflich weiter und deckt darüber hinaus alle Informationen ab. IT-Sicherheit umfasst neben den gespeicherten Informationen auch die Informationstechnik, also die Systeme, Komponenten und Prozesse zum Verarbeiten der Informationen.

Gleichwohl haben die Begriffe eine gemeinsame Schnittmenge und sind zumindest teilweise deckungsgleich. Wie bereits aus der eingangs zitierten Definition hervorgeht, bestehen folgende Funktionsziele:

Vertraulichkeit, **Integrität** und **Verfügbarkeit**.

- Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.[41]
- Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.[42]
- Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.[43]

Zu beachten ist an dieser Stelle, dass der Datenschutz darüber hinaus weitere Schutzziele definiert, wie Transparenz, Intervenierbarkeit, Nicht-Verkettbarkeit. Hierzu im Weiteren mehr.

Die gesetzlichen und regulatorischen Parameter der IT-Sicherheit werden im Nachfolgenden dargestellt.

41 BSI: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817314, abgerufen am 30.06.2020.

42 BSI: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288, abgerufen am 30.06.2020.

43 BSI: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817314, abgerufen am 30.06.2020.

2.2.2 IT-Sicherheitsgesetz(e) und Gesetz zur Umsetzung der NIS-Richtlinie (EU) 2016/1148

2.2.2.1 IT-Sicherheitsgesetz[44]

Die Bezeichnung des Gesetzes ist leicht irreführend. Es regelt nämlich nicht allgemeinverbindlich die IT-Sicherheit.

Das IT-Sicherheitsgesetz ist ein Artikelgesetz. Neben dem BSI-Gesetz werden auch das Energiewirtschaftsgesetz, das Telemediengesetz, das Telekommunikationsgesetz und weitere Gesetze geändert und ergänzt.

Hauptsächlich betroffen sind sog. „Betreiber Kritischer Infrastrukturen", deren Ausfall oder Beeinträchtigung ernsthafte Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere schwerwiegende Folgen für das Allgemeinwohl haben würden.

Dies sind insbesondere die Bereiche

- Energie,
- Informationstechnik und Telekommunikation,
- Transport und Verkehr,
- Gesundheit,
- Wasser,
- Ernährung,
- Finanz- und Versicherungswesen.

Welche Unternehmen letztendlich dazu zählen, wird durch Rechtsverordnung bestimmt.[45]

Ausgenommen sind lediglich Kleinunternehmen.

Die „Betreiber Kritischer Infrastrukturen" treffen zahlreiche Sicherungspflichten. Bei Sicherheitsverstößen bestehen auch gesonderte Meldepflichten an die Aufsichtsbehörden.

Allerdings sind auch Telekommunikationsunternehmen und Webseitenbetreibe unmittelbar betroffen.

Webseitenbetreiber – also Anbieter geschäftsmäßig erbrachter Telemediendienste – müssen seit Inkrafttreten des Gesetzes technische und organisatorische Maßnahmen nach dem Stand der Technik ergreifen, um sowohl un-

44 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2015).

45 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Art. 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist.

erlaubte Zugriffe auf ihre technischen Einrichtungen und Daten als auch Störungen zu verhindern.

Die entsprechenden Regelungen, die in § 13 (7) TMG ihre konkrete Ausprägung haben, sind ab 01.12.2021 in § 19 (1) u. (4) TTDSG[46] zu finden.

2.2.2.2 Gesetz zur Umsetzung der NIS-Richtlinie (EU) 2016/1148

Das Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union[47] wurde am 29.06.2017 verkündet und setzte die vorgenannte Richtlinie (NIS-Richtlinie) in nationales Recht um.

Zwar handelt es sich im Verhältnis zum IT-Sicherheitsgesetz um ein eigenständiges Gesetz, gleichwohl ist es ebenfalls ein Artikelgesetz und ergänzt sowie erweitert zumindest teilweise das IT-Sicherheitsgesetz, insbesondere im BSI-Gesetz.

In diesem Gesetz werden die **Meldepflichtpflichten** auf Digitale Dienste wie Online-Marktplätze, Suchmaschinen und Cloud-Computing-Dienste erweitert und die Mindestanforderungen für deren IT-Sicherheit definiert.
Hinsichtlich der Digitalen Dienste sind die Vorschriften seit dem 10. Mai 2018 anwendbar. Allerdings ist mit einer Novellierung des Gesetzes zu rechnen, da die NIS-Richtlinie auf Europaebene überarbeitet wird.

2.2.2.3 IT-Sicherheitsgesetz 2.0[48]

Am 28.05.2021 ist das sog. IT-Sicherheitsgesetz 2.0 weitgehend in Kraft getreten. Teile davon treten zum 01.12.2021 in Kraft.[49] Es löst das IT-Sicherheitsgesetz[50] nicht vollständig ab, sondern beinhaltet – wiederum als Artikelgesetz – Erweiterungen und Modifikationen in mehreren Gesetzen, insbesondere dem BSI-Gesetz. Allerdings soll nun erstmals ein ganzheitlicher Ansatz der IT-Sicherheit erfolgen, was sich insbesondere an der ausführlicheren Begriffsbestimmung der Sicherheit in der Informationstechnik im BSI-Gesetz und einer Befugnis des BSI Anordnungen gegen Anbieter von Telemediendiensten zu treffen, zeigt.

46 BGBl. I 2021, S. 1122 ff.
47 BGBl. I 2017, 1885 ff.
48 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2021).
49 Art. 1 Nummer 4, 6 und 12.
50 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2015).

Neben einer Ausweitung der Befugnisse und der Zuständigkeit des BSI wird der Bußgeldrahmen drastisch erhöht, die Pflichten für Betreiber kritischer Infrastrukturen erweitert und der Katalog der Betreiber kritischer Infrastrukturen um den Sektor der „Siedlungsabfallentsorgung" ergänzt.

Außer den Betreibern Kritischer Infrastrukturen werden nun Unternehmen im besonderen öffentlichen Interesse in den Anwendungsbereich samt Meldepflichten und Mindestanforderungen einbezogen.

Unternehmen im besonderen öffentlichen Interesse sind solche, die – ohne Betreiber Kritischer Infrastrukturen zu sein – große Bedeutung in Bezug auf die IT-Sicherheit in Deutschland haben und folgenden Gruppen zuzuordnen sind:
1.) Rüstung und IT-Produkte für staatliche Verschlusssachen

Herstellung von Rüstungsgütern (Waffen, Munition, Rüstungsmaterial und Wehrtechnik), sowie IT-Produkte für staatliche Verschlusssachen.

2.) Erhebliche volkswirtschaftliche Bedeutung

Unternehmen, die aufgrund ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland zählen und deshalb von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind, sowie deren Zulieferer, wenn sie aufgrund ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind.

3.) Gefahrstoffe der oberen Klasse

Betreiber von Betriebsbereichen der oberen Klasse mit gefährlichen Stoffen im Sinne der Störfall-Verordnung oder diesen gleichgestellten Betreibern.

Eine Konkretisierung der Unternehmen soll durch Verordnung bestimmt werden.

2.2.3 DSGVO

Weitaus allgemeinverbindlicher rückt im Bereich der Datensicherheit der technische und organisatorische Datenschutz in der DSGVO stärker als bisher in den Vordergrund.

Art. 25 DSGVO gibt den **Datenschutz durch Technikgestaltung** (data protection by design) und durch **datenschutzfreundliche Voreinstellungen** (data protection by default) vor. Maßstab ist hier u. a. der Stand der Technik.

Art. 32 DSGVO verlangt hinsichtlich der Sicherheit der Verarbeitung geeignete technische und organisatorische Maßnahmen, um ein dem Risiko an-

gemessenes Schutzniveau zu gewährleisten und bezieht sich wiederum u. a. auf den Stand der Technik.

Schließlich verlangt Art. 35 DSGVO unter bestimmten Bedingungen eine **Datenschutz-Folgenabschätzung** (DSFA).

Eine DSFA ist eine spezielle Vorgehensweise zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann.[51]

Sie beginnt mit einer Evaluierung des Risikos. Führt diese zum Ergebnis, dass ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten gegeben ist, muss die DSFA durchgeführt werden. Dies wird unterstellt, soweit umfangreich besondere Kategorien personenbezogener Daten verarbeitet werden, Profiling- und Scoring-Verfahren zum Einsatz kommen oder eine systematische und umfassende Überwachung öffentlich zugänglicher Bereiche erfolgt.

Die DSFA muss enthalten:

1) Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
2) Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
3) Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
4) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

51 Kurzpapier Nr. 5 Datenschutz- Folgenabschätzung nach Art. 35 DSGVO, S.1 https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf, abgerufen am 30.06.2020.

Werden keine Maßnahmen zur Eindämmung des Risikos ergriffen, ist die Aufsichtsbehörde zu konsultieren, bevor die Daten verarbeitet werden.

Bei jeder Verletzung des Schutzes personenbezogener Daten ergibt sich aus Art. 33 DSGVO eine Meldepflicht binnen 72 Stunden an die Aufsichtsbehörde, bei Fristüberschreitungen ist der Meldung eine Begründung beizufügen.

Die Meldung muss enthalten:

1) Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
3) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
4) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Diese Meldepflicht entfällt, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Dies wird nur dann der Fall sein, wenn zuvor eine DSFA vorgenommen wurde und entsprechende Maßnahmen nachweisbar ergriffen wurden, um das Risiko auszuschließen. Zu denken ist hier etwa an geeignete Verschlüsselungs-, sowie Anonymisierungs-, Pseudonymisierungsverfahren.

Es sind weiter unverzüglich Abhilfemaßnahmen zu ergreifen.

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so ist/sind die betroffene(n) Person(en) in klarer und einfacher Sprache unverzüglich über die Art der Verletzung, ihrer wahrscheinlichen Folgen, der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen zu benachrichtigen. Außerdem sind der Name und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen anzugeben.

Die Benachrichtigung ist bei Vorliegen einer der folgenden Voraussetzungen entbehrlich:

- Der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung.
- Der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht.
- Wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

2.2.4 Stand der Technik

Der Stand der Technik wird in der DSGVO als auch im IT-SiG im Rahmen der Anforderung zur IT-Sicherheit als Maßstab genannt. Was dieser letztendlich beinhaltet, ist jedoch nicht verbindlich vorgegeben. Es handelt sich somit um einen **unbestimmten Rechtsbegriff**, der folglich durch die zuständigen Behörden und Gerichte auszulegen sein wird.

Dabei kann auf Normen und Methoden aus dem relevanten Bereich zurückgegriffen werden.

Das BSI führt hierzu aus:

> „Stand der Technik" ist ein gängiger juristischer Begriff, der nicht allgemeingültig und abschließend definiert ist. Da die technische Entwicklung schneller ist als die Gesetzgebung, hat es sich bewährt, in Gesetzen den Begriff „Stand der Technik" zu verwenden, statt zu versuchen, konkrete technische Anforderungen festzulegen. Was zu einem bestimmten Zeitpunkt „Stand der Technik" ist, lässt sich z. B. anhand existierender nationaler oder internationaler Standards oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln.[52]

52 BSI: https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Neuregelungen_KRITIS/B3S/b3s.html, abgerufen am 30.06.2020.

2.2.4.1 ISO/IEC 27001

Die Internationale Organisation für Standardisierung (ISO) ist die internationale Vereinigung von Normungsorganisationen und erarbeitet internationale Normen in allen Bereichen.

Die International Electrotechnical Commission (IEC), zu Deutsch: Internationale Elektrotechnische Kommission ist eine internationale Normungsorganisation für Normen im Bereich der Elektrotechnik und Elektronik. Einige Normen werden gemeinsam mit der ISO entwickelt.

So wurde im Bereich der Informations- und IT-Sicherheit von beiden Organisationen gemeinsam die 27000-Reihe entwickelt.

Die ISO/IEC 27001 gilt dabei als international anerkannter Standard.

ISO/IEC 27001 ist auch als DIN-Norm umgesetzt (DIN EN ISO/IEC 27001:2017-06).

Hauptgegenstand der Norm ist die Einführung und ständige Überwachung eines Informationssicherheit-Managementsystems (ISMS), welches dem Zweck dient, die Informationssicherheit/IT-Sicherheit und deren Funktionsziele in einem Unternehmen zu gewährleisten.

Dabei ist die ISO/IEC 27001 bewusst sehr allgemein gehalten, um den individuellen Anforderungen eines Unternehmens Raum zu lassen. Die Norm soll grundsätzlich auf alle Unternehmen in jeder Organisationsform anwendbar sein.

Eine Zertifizierung ist möglich und allgemein anerkannt.

Das über 30-seitige Hauptdokument ist unterteilt in 10 Abschnitte oder Kapitel und zwei Anhänge mit jeweils normativen und informativen Inhalten.

Abbildung 5