HAW HAMBURG

BACHELORTHESIS
Karl Klemann

Die Rolle der DSGVO für das Risikomanagement in der IT-Sicherheit

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Karl Klemann

Die Rolle der DSGVO für das Risikomanagement in der IT-Sicherheit

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Angewandte Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Jens von Pilgrim
Zweitgutachter: Prof. Dr. Klaus-Peter Kossakowski

Eingereicht am: 16. Februar 2022

Karl Klemann

Thema der Arbeit

Die Rolle der DSGVO für das Risikomanagement in der IT-Sicherheit

Stichworte

Risiko, Risikomanagement, DSGVO, IT-Sicherheit, Schutzziele, Authentizität, Datenintegrität, Informationsvertraulichkeit, Verfügbarkeit, Verbindlichkeit, Anonymisierung, Pseudonymisierung

Kurzzusammenfassung

Diese Arbeit befasst sich mit der Bedeutung der DSGVO in Bezug auf das Risikomanagement in der IT-Sicherheit. Im Fokus steht dabei die Frage, ob Risikomanagement von der DSGVO abhängig ist.

Karl Klemann

Title of Thesis

The Function of the GDPR for Risk Management in IT Security

Keywords

Risk, Risk management, GDPR, IT security, Security Goals, Authenticity, Data integrity, Information confidentiality, Availability, Non repudiation, Anonymization, Pseudonymization

Abstract

This thesis investigates the function of the GDPR regarding risk management in IT security. The main question is whether risk management is dependent on the GDPR.

Inhaltsverzeichnis

Abbildungsverzeichnis ..... **vi**

Tabellenverzeichnis ..... **vii**

Abkürzungsverzeichnis ..... **viii**

1 Einleitung **1**

2 Risikomanagement in der IT-Sicherheit **2**

2.1 Die Definition von Risiko 2

2.2 Die Definition von Risikomanagement 6

2.3 IT-Sicherheit 8

2.3.1 Schutzziele in der IT-Sicherheit 10

2.4 Anforderungen und Vorgaben 13

2.4.1 Risikomanagement und die ISO/IEC 27000-Reihe 14

2.5 Kapitelzusammenfassung 16

3 DSGVO und Risikomanagement **18**

3.1 Die Datenschutz-Grundverordnung 18

3.1.1 Die Sicherheit von personenbezogenen Daten in der DSGVO 19

3.1.2 Die Rolle von Verfügbarkeit 21

3.1.3 Die Rolle von Pseudonymisierung 21

3.1.4 Informationsvertraulichkeit, Authentizität & Datenintegrität in Artikel 5 22

3.1.5 Die Rolle der Verbindlichkeit 23

3.1.6 Pflichten und Konsequenzen bei Datenschutzverletzungen 25

3.2 Die Bemessung von Bußgeldern in Deutschland 26

3.3 Der Fall des Berliner Kammergerichts 28

3.3.1 Der Vorfall und die anschließende Untersuchung 28

3.3.2 Erkenntnisse aus dem Vorfall und die Verbindung zur DSGVO 30

3.3.3 Die Folgen des Vorfalls ... 31
3.4 Die Perspektive von Unternehmen auf die DSGVO ... 32
3.4.1 Die Umfragen des Bitkom ... 32
3.4.2 Implikationen aus den Umfragen für das Risikomanagement ... 37
3.5 Kapitelzusammenfassung ... 38
4 Ableitungen für das Risikomanagement ... 40
4.1 Grundlegendes zu Angriffen ... 40
4.2 Erster Beispielfall - Ransomware ... 41
4.2.1 Szenario ... 42
4.2.2 Analyse ... 43
4.2.3 Grundlegende Lösungsansätze ... 45
4.3 Zweiter Beispielfall – Phishing ... 46
4.3.1 Szenario ... 47
4.3.2 Analyse ... 47
4.3.3 Grundlegende Lösungsansätze ... 49
4.4 Dritter Beispielfall - Spyware ... 50
4.4.1 Szenario ... 50
4.4.2 Analyse ... 51
4.4.3 Grundlegende Lösungsansätze ... 51
4.5 Vierter Beispielfall – Cross Site Scripting ... 52
4.5.1 Szenario ... 53
4.5.2 Analyse ... 54
4.5.3 Grundlegende Lösungsansätze ... 54
4.6 Kapitelzusammenfassung ... 55
5 Fazit ... 58
Literaturverzeichnis ... 59

Abbildungsverzeichnis

Abbildung 1: Herausforderungen bei der Umsetzung der DSGVO ..... .33
Abbildung 2: Aufwandseinschätzung bzgl. DSGVO. 34
Abbildung 3: Umsetzungsfortschritte von Unternehmen. 35
Abbildung 4: Forderungen von Unternehmen bzgl. Datenschutz. 36
Abbildung 5: Use Case Szenario 1. 43
Abbildung 6: Use Case Szenario 1 unter Berücksichtigung von Monitoring. 45
Abbildung 7: Sequenzdiagramm Szenario 4. 53

Tabellenverzeichnis

Tabelle 1: Schutzziele 10

Tabelle 2: Schutzziele und verwandte Artikel der DSGVO..... 19

Abkürzungsverzeichnis

Bitkom	Branchenverband der deutschen Informations- und Telekommunikationsbranche
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
EDPB	European Data Protection Board
EDSA	Europäischer Datenschutzausschuss
IKT	Informations- und Kommunikationstechnologie
IEC	Internationale Elektrotechnische Kommission
ISMS	Information Security Management System
ISO	Internationale Organisation für Normung
KFN	Kriminologisches Forschungsinstitut Niedersachsen
OWASP	Open Web Application Security Project
SSRF	Server-Side Request Forgery
XSS	Cross Site Scripting

1 Einleitung

Datenschutz ist bereits seit längerer Zeit ein Thema, das in der IT-Welt immer wieder in den Fokus gerät. Seit ihrer Einführung ist die Europäische Datenschutz-Grundverordnung (DSGVO) diesbezüglich die bedeutendste rechtliche Verordnung auf EU-Ebene. Dies macht sie zu einem wesentlichen Faktor, was den datenschutzkonformen Umgang mit personenbezogenen Daten angeht und verleiht ihr damit auch eine bedeutende Rolle für eine Vielzahl von Akteuren im öffentlichen und privaten Bereich. Dabei ist nicht nur der eigene rechtmäßige Umgang mit diesen Daten zu berücksichtigen, sondern auch der angemessene Schutz vor unbefugtem Zugriff. Dementsprechend darf sie in der IT-Sicherheit nicht vernachlässigt werden und muss beim Risikomanagement bedacht werden. In dieser Arbeit soll die konkrete Rolle der DSGVO für das Risikomanagement in der IT-Sicherheit elaboriert werden. Dabei sollen die Bedeutung von Vorgaben, Herausforderungen bei der Implementierung und auch mögliche Konsequenzen für Verstöße berücksichtigt werden. Ausgangspunkt für die Untersuchungen ist die Frage, ob sich Risikomanagement in einem Abhängigkeitsverhältnis zur DSGVO befindet. Grund für diese Annahme ist die Vermutung, dass Risikomanagement in Unternehmen durch die Vorgaben aus der DSGVO maßgeblich beeinflusst wird.

In den folgenden Kapiteln werden zunächst wesentliche Aspekte und Begriffe wie Risikomanagement und Schutzziele erläutert werden. Anschließend werden Zusammenhänge zwischen Risikomanagement und DSGVO elaboriert, indem ihre Inhalte mit bereits genannten Aspekten verknüpft werden. Diesbezüglich werden auch die Implementierung von Bußgeldern, ein Beispielfall für einen Angriff und die Perspektive von Unternehmen auf die DSGVO hinzugezogen. Schließlich werden anhand von spezifischen Beispielszenarien einige grundlegende Maßnahmen diskutiert, die zur Einhaltung der DSGVO beitragen können. Anhand der gesammelten Informationen aus diesen Kapiteln wird schließlich ein Fazit bezüglich der Rolle der DSGVO für das Risikomanagement in der IT-Sicherheit gezogen werden.

2 Risikomanagement in der IT-Sicherheit

Da sich diese Arbeit mit Risikomanagement in der IT-Sicherheit beschäftigt, ist es sinnvoll, zunächst einige grundlegende Begriffe zunächst zu erörtern, insbesondere *IT-Sicherheit* und *Risikomanagement* selbst. Dabei sollen nicht vollständige oder gar allgemeingültige Definitionen für diese Bereiche festgelegt werden, sondern es geht vielmehr darum, den Kontext dieser Arbeit darzulegen, um mögliche Missverständnisse frühzeitig aus dem Weg zu räumen. Wichtig ist es daher auch festzuhalten, dass die Begriffe vor allem in Zusammenhang mit Wirtschaftsunternehmen diskutiert werden, da dort ein Großteil der Datenverarbeitung stattfindet und sich bestimmte Teile der DSGVO, insbesondere was die Konsequenzen bei Fehlverhalten angeht, nicht gleichermaßen auf Unternehmen und Akteure wie z.B. öffentliche Einrichtungen beziehen. Primär wird sich dabei auf die Werke „IT-Sicherheit: Konzepte - Verfahren - Protokolle“ von Claudia Eckert und „IT-Risikomanagement mit System“ von Hans-Peter Königs konzentriert.

2.1 Die Definition von Risiko

Einer der zentralen Begriffe, die zunächst diskutiert werden müssen, ist der Begriff *Risiko*. Eckert geht hierbei zunächst auf Bedrohungen ein. Diese sind darauf ausgerichtet, Schwachstellen bzw. Verwundbarkeiten von Systemen auszunutzen um beispielsweise Datenintegrität, Verfügbarkeit oder Authentizität zu gefährden (Eckert, 2018, S. 17). Letztgenannte Begriffe werden in einem späteren Abschnitt dieser Arbeit genauer betrachtet werden.

Risiko selbst definiert Eckert mit den Worten:

„Unter dem Risiko (engl. risk) einer Bedrohung verstehen wir die Wahrscheinlichkeit (oder relative Häufigkeit) des Eintritts eines Schadensereignisses und die Höhe des potentiellen Schadens, der dadurch hervorgerufen werden kann.“ (Eckert, 2018, S. 17).

Aus dieser Definition ergibt sich die Feststellung, dass Risiken von Bedrohungen im Allgemeinen mit Wahrscheinlichkeit bzw. relativer Häufigkeit und Schadenshöhe von zwei

wesentlichen Faktoren abhängig sind. Jedoch ist diese Betrachtungsweise noch recht grob und für einen derartig zentralen Begriff in dieser Arbeit nicht ausreichend. Zudem wird auf Schadensereignisse, die eine wesentliche Rolle in dieser Definition spielen, nicht genauer eingegangen. Es ist daher sinnvoll, Risiko in einem Kontext zu behandeln, der direkt mit der DSGVO in Verbindung gesetzt werden kann. Königs konzentriert sich in seiner Betrachtung von Risiko in Bezug auf IT ebenfalls auf Wahrscheinlichkeit, allerdings mit einem anderen Fokus. Er verweist dabei auf folgende Definition:

„Risiko ist eine nach Wahrscheinlichkeit (Häufigkeit) und Konsequenz bewertete Bedrohung hinsichtlich der Abweichungen von erwarteten System-Zielen. Das (Downside-) Risiko betrachtet dabei stets die unerwünschten Abweichungen von den System-Zielen und deren Folgen.“ (Brühwiler, 2001, S. 8, zitiert nach Königs, 2017, S. 12).

Dieser Definition liegt die Überlegung zugrunde, dass sich bei Risiken im Bereich von IT und der Sicherheit von Informationen auf die negativen Abweichungen von Zielen konzentriert wird, die zu negativen Folgen führen, welche unter anderem auch als „Schäden[1]“ bezeichnet werden. Risiken werden hier explizit in einem negativen Kontext genannt, da sie sich von Chancen, bei denen positive Ergebnisse möglich sind, abgrenzen lassen und sich beides in der Regel nicht mit den gleichen Maßnahmen behandeln lässt. Allgemein können Abweichungen laut Königs von finanziellen bis hin zu technischen Aspekten breit gefächert sein, je nachdem auf welche Art von Risiken man sich konzentriert. Dabei erwähnt er explizit die Möglichkeit, die genannte Definition von Risiko auf die Sicherheit von Informationen anzuwenden, wobei hier die Abweichungen von Zielen wie Vertraulichkeit, Integrität, oder Verfügbarkeit im Vordergrund stehen. Als Beispiel für eine Abweichung vom Ziel Vertraulichkeit wird hier Datendiebstahl genannt. Zusätzlich dazu erwähnt er auch die Anwendung der Definition auf gesetzliche Vorlagen, wobei hier negative Konsequenzen zu erwarten sind, wenn sich nicht an die entsprechenden Anforderungen gehalten wird. Auftreten können Zielabweichungen insbesondere in Zusammenhang mit entsprechenden Bedrohungen, deren Gefahr auch davon abhängig

[1] (Königs, 2017, S. 12)

ist, ob entsprechende Maßnahmen gegen sie existieren. Ein System ist laut ihm nur dann sicher, wenn Zielabweichungen unmöglich sind (Königs, 2017, S. 11-15).

Bemerkenswert an der von Königs verwendeten Definition ist, dass sie in unterschiedlichen Kontexten angewendet und präzisiert werden kann. Im Rahmen dieser Arbeit ist dabei vor allem die Einhaltung von gesetzlichen Vorgaben, in diesem Fall die DSGVO, allerdings auch die Rolle von Informationssicherheit essenziell. In diesem Zusammenhang ist es auch wichtig festzuhalten, dass Risiko laut der Definition in Abhängigkeit von zuvor definierten System-Zielen steht. Die Ziele, die für diese Arbeit im Vordergrund stehen sollen, werden an späterer Stelle genauer erläutert. Ein Unterschied zur erstgenannten Definition ist zudem, dass hier Risiken selbst als Bedrohungen angesehen werden, die nach Wahrscheinlichkeit und Konsequenz bewertet werden. Deshalb wird auf diese Faktoren als nächstes eingegangen.

Bezüglich des Umgangs mit Risiko diskutiert Königs die Messbarkeit von Risiken vor allem anhand der Faktoren *Schadenshöhe* und *Wahrscheinlichkeit*, bemerkt aber, dass insbesondere simple Multiplikation schwerwiegenden Einschränkungen unterliegt, vor allem, was den Umgang mit besonders seltenen, aber dafür umso gravierenderen Schadensfällen angeht. Zudem sind ihm zufolge Einschätzungen bezüglich der Wahrscheinlichkeiten meist subjektiv beeinflusst von den am Risikomanagement beteiligten Personen, die unterschiedlich stark zu riskanten Aktionen tendieren. Dennoch unterstreicht er, dass Hilfsmittel wie Risiko-Bewertungs-Matrizen, die zwar nicht auf den einfachen Multiplikationen, aber zumindest auf den gleichen Faktoren basieren, nützlich für die Entscheidungsfindung sein können (Königs, 2017, S. 15-27).

Die soeben genannten Punkte unterstreichen die Komplexität der Berechenbarkeit von Risiken. Auch in Bezug auf die DSGVO muss daher bedacht werden, welche konkreten Informationen verfügbar sein müssen, damit die Auswirkungen für Entscheidungsträger greifbar werden. Auf diese Weise wäre es möglich, die DSGVO angemessen im Risikomanagement bei der IT-Sicherheit berücksichtigen zu können.

Wie im nächsten Kapitel ausführlich thematisiert wird, können durch Abweichung von Zielen bzw. Missachtung datenschutzrechtlicher Vorgaben Schäden in Form von Sanktionen entstehen. Eingegangen wird dann auch darauf, dass diese Sanktionen nicht immer gleich ausfallen und für die betroffenen Unternehmen teilweise schwer nachvollziehbar sind. *Schaden* bezieht

sich im Kontext dieser Arbeit daher primär auf finanzielle Einbußen für Unternehmen, die aus diesen Strafzahlungen resultieren, während *Schadenshöhe* sich dementsprechend auf den Betrag dieser Einbußen bezieht. Ein *Schadensereignis*, wie es in der Risikodefinition von Eckert bereits erwähnt wurde, wird hier als Ereignis angesehen, welches zu einem Schaden für das Unternehmen führt. Hierbei gilt zu bedenken, dass dies nicht automatisch der Fall ist, sobald die Abweichung von einem Ziel eingetreten ist, sondern erst, wenn dies auch explizit zu einem Schaden geführt hat. Was *Wahrscheinlichkeit* angeht, muss wie bereits von Königs angedeutet, bedacht werden, dass sie als Faktor schwer greifbar ist. Hierzu müsste es möglich sein, nicht nur zu wissen, mit welcher Wahrscheinlichkeit die behandelten Abweichungen auftreten, sondern auch, welcher Anteil davon überhaupt entdeckt wird. Zudem wird im Kapitel über IT-Sicherheit behandelt werden, dass man nicht davon ausgehen sollte, die Wahrscheinlichkeit von Abweichungen auf null zu reduzieren. Es ist daher nicht das Ziel dieser Arbeit, allgemeingültige Kalkulationen vorzugeben, die sämtliche Schadensfälle abdecken können, sondern vielmehr die wesentlichen Rahmenbedingungen zu thematisieren, welche sich in diesem Kontext mit der DSGVO ergeben. Entscheidend sind hierbei die möglichen Konsequenzen bei Nichteinhaltung der DSGVO und welche Maßnahmen getroffen werden können, um dies zu verhindern. In Kapitel 3 wird unter anderem darauf eingegangen werden, dass es ratsam ist, Entscheidungen bezüglich des Risikomanagements an dem jeweiligen Unternehmen auszurichten, da die Konsequenzen für die Nichteinhaltung der DSGVO abhängig von unterschiedlichen Faktoren, die die Umstände eines Vorfalls und die jeweiligen Unternehmen selbst betreffen, sehr unterschiedlich sein können.

Nachdem der Begriff *Risiko* nun bereits erörtert wurde, soll daher als nächstes der Begriff *Risikomanagement* behandelt werden.

2.2 Die Definition von Risikomanagement

Königs betont in seinen Ausführungen die Komplexität des Begriffs *Risikomanagement*. Im Zentrum seiner Ausführungen stehen dabei Risikoobjekte, d.h. schützenswerte Objekte, für die die behandelten Risiken zutreffen. Diese müssen beim Risikomanagement genau definiert und abgegrenzt werden. Gleiches gilt auch für den jeweiligen Kontext. Zum Beispiel ist es hier wichtig zu etablieren, ob man ein einzelnes oder wiederkehrendes Ereignis behandelt oder ob es einen spezifischen zeitlichen Rahmen gibt, in dem ein Ereignis geschehen kann. Wichtig sei es hierbei, dass Identifikation, Analyse und Bewertung von Risiken Beachtung finden, wobei bei der Risiko-Identifikation die Risiken bestimmt, bei der Risiko-Analyse mit ihren Eigenschaften erfasst und bei der Risiko-Bewertung anhand der zuvor definierten Kriterien interpretiert werden müssen (Königs, 2017, S. 11 & 45-64).

Hervorgehoben wird von Königs generell, dass Risikomanagement nicht als eine Reihe einzelner Punkte verstanden werden sollte, die immer in einer festen Reihenfolge einzeln abgearbeitet werden können:

„Der hier diskutierte Risikomanagement-Prozess muss als inhärent rekursiv aufgefasst werden, d. h., dass er mittels bedarfsabhängiger Rückkopplungen und Rekursionen der Komplexität und Dynamik heutiger Risikosituationen gerecht werden kann. Daher darf er vor allem nicht als eine rigide lineare Abfolge von einzelnen Aktivitäten und Subprozessen verstanden werden.“ (Königs, 2017, S. 45).

An dieser Stelle muss betont werden, dass ein detaillierter Einbezug sämtlicher der von Königs genannten Aspekte den Rahmen dieser Arbeit sprengen würde, allerdings die hier genannten grundsätzlichen Aspekte des Risikomanagements, die von ihm betont werden, eine wichtige Rolle spielen. Grund dafür ist, dass nicht das Risikomanagement selbst der Hauptfokus dieser Arbeit sein soll, sondern die DSGVO und die Rolle, welche sie für das Risikomanagement in der IT-Sicherheit spielt. Im Zusammenhang mit dieser Arbeit lassen sich konkrete schützenswerte Risikoobjekte identifizieren. Hierbei handelt es sich um personenbezogene Daten, die dem Schutz der DSGVO unterliegen. Die Risiken, die im weiteren Verlauf dieser Arbeit diskutiert werden, werden also solche sein, die explizit mit personenbezogenen Daten zusammenhängen. Da bereits im Vorfeld erläutert wurde, dass sich Risiko sich auf potenzielle

Abweichungen von System-Zielen bezieht, wird zu einem späteren Zeitpunkt behandelt werden, welche Ziele mit Bezug auf personenbezogene Daten hierbei im Vordergrund stehen sollen und wie diese mit der DSGVO zusammenhängen.

Königs betont, dass eine Betrachtung des Risikomanagements im IT-Bereich nicht angemessen sein kann, falls Kontext und Umwelt eines Unternehmens nicht berücksichtigt werden. So sind laut ihm die gesetzlichen Anforderungen, die an Unternehmen gestellt werden von großer Bedeutung für das Risikomanagement und er erwähnt in diesem Kontext sogar explizit die zu diesem Zeitpunkt noch in Planung befindliche Datenschutz-Grundverordnung als Beispiel für derartige Anforderungen (Königs, 2017, S. 81-82 & 108-109).

Interessanterweise wird der Begriff Risikomanagement von Eckert nur kurz und dies ebenfalls im Kontext gesetzlicher Anforderungen erwähnt, und zwar in Bezug auf die Verpflichtung für Aktiengesellschaften und GmbHs, ein Risikomanagement zu implementieren, welche aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich hervorgeht. Auch wenn sie dabei feststellt, dass nicht genau festgelegt ist, wie derartige Systeme strukturiert sein müssten, so hat ein solches System zumindest über ein Frühwarnsystem und ein System für Revision und Controlling interner Prozesse zu verfügen (Eckert, 2018, S. 177). Für das Ziel dieser Arbeit ist es äußerst bemerkenswert, wie gesetzliche Vorgaben die Bedeutung von Risikomanagement durch verbindliche Anforderungen beeinflussen können, selbst wenn diese nicht explizit formuliert werden. Bereits in Bezug auf die Bedeutung von IT-Systemen ergänzt Eckert zudem, dass die Technologie eines Systems auch im Kontext der gesetzlichen Anforderungen zu betrachten ist und erwähnt explizit an dieser Stelle auch die DSGVO (Eckert, 2018, S. 3-4).

An dieser Stelle kann zunächst festgehalten werden, dass die Rolle der DSGVO darin zu bestehen scheint, dass sie wesentlichen Einfluss auf das Risikomanagement von Unternehmen ausüben kann. Dies würde ein einseitiges Abhängigkeitsverhältnis vom Risikomanagement zur DSGVO bedeuten. Jedoch bleibt vorerst abzuwarten, ob sich dieser Eindruck mit den weiteren Feststellungen in dieser Arbeit bestätigen wird. Zu diesem Zweck wird zu einem späteren Zeitpunkt ein Blick auf andere Anforderungen und Vorgaben geworfen, da auch die DSGVO in die Kategorie gesetzlicher Vorgaben fällt.

Nachdem nun also die ersten grundlegenden Begriffe behandelt wurden, soll im folgenden Abschnitt auf IT-Sicherheit eingegangen werden.

2.3 IT-Sicherheit

Claudia Eckert definiert die Rolle der IT-Sicherheit in der Wirtschaft folgendermaßen:

„IT-Sicherheit hat die Aufgabe, Unternehmen und deren Werte (Know-How, Kundendaten, Personaldaten) zu schützen und wirtschaftliche Schäden, die durch Vertraulichkeitsverletzungen, Manipulationen oder auch Störungen der Verfügbarkeit von Diensten des Unternehmens entstehen können, zu verhindern.“ (Eckert, 2018, S. 1).

Es lässt sich also festhalten, dass IT-Sicherheit für den Schutz diverser Unternehmensbereiche essenziell ist und personenbezogene Daten, die sowohl Personen innerhalb als auch außerhalb des Unternehmens betreffen, hierbei eine zentrale Rolle spielen.

Eckert führt weiterhin aus, dass es für Informations- und Kommunikationstechnologie (IKT) schwer ist, vollkommene Sicherheit vor Angriffen zu gewährleisten, weshalb es in der IT-Sicherheit Maßnahmen zur Verringerung von Risiken gibt (Eckert, 2018, S. 1). Wörtlich heißt es dazu:

„Da eine vollständige Vermeidung oder Verhinderung von Angriffen in der Praxis nicht möglich ist, umfasst das Gebiet der IT-Sicherheit insbesondere auch Maßnahmen und Konzepte, um das Ausmaß potentieller Schäden, die durch Sicherheitsvorfälle entstehen können, zu reduzieren und damit die Risiken beim Einsatz von IKT-Systemen zu verringern.“ (Eckert, 2018, S. 1).

Diese Aussage ist von entscheidender Bedeutung für die zuvor behandelten Themen und dabei vor allem für den Faktor *Wahrscheinlichkeit*, da hiermit impliziert wird, dass es eine hundertprozentige Wahrscheinlichkeit für mindestens einen erfolgreichen Angriff gibt. Die Frage wäre also nicht ob jemals ein Angriff erfolgreich sein wird, sondern wann dies geschieht und wie mit den Folgen bzw. Schäden umzugehen ist. Daher muss sich Risikomanagement vor allem darauf konzentrieren, Wahrscheinlichkeiten und Schäden soweit wie möglich abzumildern.

Eingegangen muss an dieser Stelle auch auf die erwähnten Angriffe. Diese werden von Eckert als nicht autorisierte Zugriffe bzw. Zugriffsversuche auf Systeme definiert. Dabei gibt es unterschiedlichste Varianten, die von unautorisierter Datengewinnung bis hin zur Modifikation

von Datenobjekten reichen. Aus diesen Angriffen resultieren die bereits zuvor genannten Bedrohungen (Eckert, 2018, S. 18-19).

Wichtig ist, dass Angriffe grundsätzlich nicht mit Risiken zu verwechseln sind, sondern vielmehr eine Quelle für Bedrohungen sind. Auch wenn in dieser Arbeit eine andere Risikodefinition als die von Eckert verwendet wird, in der auch eine andere Bedeutung von Bedrohung erkennbar ist, so werden Angriffe dennoch wie hier dargelegt aufgefasst werden. Dies liegt daran, dass es für die kausale Verbindung zwischen Bedrohung und Angriff nebensächlich ist, ob es sich bei einem Risiko selbst um eine Bedrohung oder um die Eigenschaft einer Bedrohung handelt. Entscheidend ist, dass Bedrohungen aus Angriffen hervorgehen. Risiken werden dementsprechend in dieser Arbeit als nach Wahrscheinlichkeit und Konsequenz bewertete Bedrohungen, welche aus unautorisierten Zugriffen und Zugriffsversuchen auf IT-Systeme resultieren, betrachtet.

Eine zentrale Rolle in der IT-Sicherheit spielt laut Eckert das IT-System, welches sie wie folgt definiert:

Ein IT-System ist ein geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen.“ (Eckert, 2018, S. 3).

Bei offenen Systemen handelt es sich hierbei in der Regel um verteilte, heterogene Systeme ohne zentrale Verwaltung, welche miteinander vernetzt sind und auf diese Weise untereinander kommunizieren können. Geschlossene Systeme hingegen sind homogen und werden zentral verwaltet, auf festgelegte Teilnehmer beschränkt und von anderen separiert. Allgemein werden von Eckert zwei wesentliche Aspekte für die Sicherheit von IT-Systemen dargelegt, *Sicherheitsanforderungen* und *Sicherheitseigenschaften*. Sicherheitsanforderungen sind dabei durch Schutzziele definiert, welche sich daraus ergeben, welche Daten und Informationen eines Systems vor unbefugtem Zugriff bewahrt werden müssen. Sicherheitseigenschaften hingegen sind dazu da, um genau diese Anforderungen zu erfüllen. Diese Sicherheitseigenschaften werden schließlich durch Angriffe auf das System herausgefordert (Eckert, 2018, S. 2-7). Besondere Aufmerksamkeit verdienen diesbezüglich die Schutzziele, welche von Eckert hervorgehoben werden, da sie einen wichtigen Ansatzpunkt dafür liefern, welche unterschiedlichen Aspekte der Sicherheit bei einem IT-System berücksichtigt werden sollten.

2.3.1 Schutzziele in der IT-Sicherheit

Bei den von Eckert beschriebenen Schutzzielen handelt es sich um unterschiedliche Faktoren, welche jeweils spezifischen Bereichen zugeordnet werden und die mit spezifischen Maßnahmen erreicht werden. Zur Veranschaulichung wurden die wichtigsten Aspekte dieser Schutzziele in die folgende Tabelle übertragen.

Tabelle 1: Schutzziele

Bezeichnung	**Bedeutung**	**Beispiele für Maßnahmen**
Authentizität	Identitäten können überprüft werden	Authentifikationsdaten (z.B. Benutzerkennung und Passwort, biometrische Daten)
Datenintegrität	Geschützte Daten können nicht unbefugt verändert werden	Spezifische Berechtigungsdefinitionen, eingeschränkte Methoden, kryptographische Hashfunktionen
Informationsvertraulichkeit	Einsicht nur mit entsprechender Berechtigung	Informationseinsicht nur nach erfolgreicher Identifikation, kryptographische Verschlüsselung beim Datentransfer
Verfügbarkeit	Authentifizierte Subjekte sollen ihre Rechte wahrnehmen können	Quoten für Ressourcenverwendung
Verbindlichkeit	Aktionen können eindeutig zugeordnet werden	Digitale Signaturen, Überwachung und Protokollierung
Anonymisierung und Pseudonymisierung	Daten sollen für Außen-stehende nicht mit Personen in Verbindung gesetzt werden können	Komplexe Datenverschlüsselung oder Verwendung von Zuordnungsvorschriften (z.B. Pseudonyme)

(vgl. Eckert, 2018, S. 8 ff)

Authentizität ist verifiziert, wenn Echtheit und Glaubwürdigkeit durch Überprüfung einer Identität (z.B. als Nutzer oder Administrator in einem System) mithilfe ihrer jeweiligen Authentifikationsdaten sichergestellt werden können. Diese bestehen in der Regel aus Benutzerkennung und Passwort, optional können allerdings auch biometrische Daten zur Bestätigung der Identität verwendet werden (Eckert, 2018, S. 8-9).

Datenintegrität zielt laut Eckert darauf ab, dass geschützte Daten durch unbefugten und/oder unerkannten Zugriff nicht verändert werden können. Mit der Implementierung von Berechtigungen z.B. für Lese- oder Schreibzugriffe oder Einschränkungen für Aktionen, damit Objekte nicht unbeschränkt verändert werden, kann eine wichtige Basis für Integrität geschaffen werden. Um dieses Ziel allerdings vollständig zu erreichen, empfiehlt sich nach Einschätzung von Eckert die Verwendung von speziellen, angepassten Methoden für die Nutzung von Objekten, um die Veränderungen in einem gewünschten Rahmen zu belassen. Zusätzlich muss gewährleistet sein, dass unerwünschte und nicht genehmigte Veränderungen, selbst wenn sie nicht verhindert werden können, zumindest im Nachhinein erkannt werden können. Mithilfe kryptographischer Hashfunktionen können solche Manipulationen festgestellt werden (Eckert, 2018, S. 9-10).

Informationsvertraulichkeit wiederum bedeutet, dass Einsicht in bestimmte Informationen nur mit der entsprechenden Berechtigung erfolgen kann und dies durch entsprechende Kontrollen überprüft wird. Mit diesen Berechtigungen kann gewährleistet werden, dass beispielsweise ein User nur exakt die Informationen erhält, die er auch erhalten soll oder ein Objekt mit einer hohen Sicherheitseinstufung nur für Administratoren zugänglich ist. Für die Übermittlung der Daten ist es erforderlich, diese kryptographisch zu verschlüsseln, damit sie, selbst wenn sie von anderen Subjekten abgefangen werden sollten, nicht zugänglich für diese sind (Eckert, 2018, S. 10-11).

Verfügbarkeit besteht, solange die mit bestimmten Rechten ausgestatteten Subjekte nach erfolgreicher Authentifizierung ihre jeweiligen Rechte auch wahrnehmen können (z.B. Einsicht bestimmter Dateien), ohne dass sie unrechtmäßig davon abgehalten werden können. Hierbei geht es häufig um den Zugang zu gemeinsamen Ressourcen, welche von den Prozessen eines oder mehrerer User genutzt werden. Bedacht werden muss hier laut Eckert allerdings auch, dass zwischen regulären und schädlichen Aktionen schwer unterschieden werden kann, falls

ein Angreifer ein System erfolgreich infiltriert haben sollte und eigenen Prozessen hohe Priorität einräumt. Um dies zu regulieren, können Maßnahmen wie Quoten eingesetzt werden, um die Nutzung z.B. der Rechenleistung einzuteilen. Auf diese Weise kann verhindert werden, dass einzelne Prozesse/User bestimmte Ressourcen allein kontrollieren (Eckert, 2018, S. 12).

Verbindlichkeit wird dadurch gewährleistet, dass sämtliche Aktionen (z.B. Veränderung von Daten) den jeweiligen Subjekten, die für sie verantwortlich sind, zugeordnet werden können. Für diesen Zweck werden digitale Signaturen verwendet, mit deren Hilfe sich Veränderungen, Transaktionen etc. nachvollziehen lassen. Zusätzlich dazu ist Verbindlichkeit auch bei der Verwendung von gemeinsamen Ressourcen im IT-Bereich (z.B. CPU) von Bedeutung. Damit nachverfolgt werden kann, wer zu welchem Zeitpunkt welche Ressourcen verwendet hat, werden Methoden zur Überwachung und Protokollierung von Aktivitäten eingesetzt (Eckert, 2018, S. 12-13).

Zusätzlich zu diesen wesentlichen Schutzzielen betont Eckert dabei noch die steigende Bedeutung von *Anonymisierung* und *Pseudonymisierung*[2]. Hierbei handelt es sich um die Verschlüsselung von personenbezogenen Daten, sodass es für Außenstehende nahezu unmöglich wird, diese Daten den jeweiligen Personen zuzuordnen. Bei der Anonymisierung werden dabei die Daten direkt verändert, sodass sie nur mit sehr hohem Ressourcenaufwand mit bestimmten Personen in Relation gesetzt werden können. Bei der Pseudonymisierung hingegen wird beispielsweise durch die Verwendung von Pseudonymen eine Zuordnungsvorschrift verwendet, sodass die Daten ohne das Wissen über jene Vorschrift nicht mehr den jeweiligen Personen zugeordnet werden können (Eckert, 2018, S. 13-14).

Bereits an dieser Stelle lässt sich erkennen, dass der Schutz von (personenbezogenen) Daten eine elementare Rolle in der IT-Sicherheit spielt. Die Bedeutung der Schutzziele als zentrale Aspekte bilden hier wichtige Punkte, an die sich später im Kontext der DSGVO anknüpfen lässt.

[2] Teilweise wird von Eckert ebenfalls der Begriff „Pseudomisierung“ verwendet, wobei keine inhaltlichen Unterschiede feststellbar sind (vgl. Eckert, 2018, S. 546).

Interessanterweise lässt sich auch eine Verbindung zwischen den von Eckert beschriebenen Schutzzielen und der von Königs verwendeten Risikodefinition erkennen, da wesentliche genannte Ziele wie Vertraulichkeit und Verfügbarkeit von Daten hierbei übereinstimmen. Risiken werden deshalb in dieser Arbeit im Kontext von Abweichungen mit negativen Konsequenzen behandelt. Der Fokus liegt dabei auf zwei Punkten. Dabei handelt es sich um Abweichungen von den dargelegten Schutzzielen und wie dies mit der Einhaltung der Vorgaben, welche aus der DSGVO hervorgehen, zusammenhängt. Der Zusammenhang zwischen den Schutzzielen und den Inhalten der DSGVO selbst wird anhand von einigen Artikeln in Kapitel 3 genauer untersucht. Dabei soll auch berücksichtigt werden, welche Konsequenzen bei einer Abweichung, d.h. Nichteinhaltung der DSGVO gesetzlich vorgesehen sind und welche expliziten Auswirkungen dies haben kann.

2.4 Anforderungen und Vorgaben

Neben den bisher genannten Aspekten von IT-Sicherheit sollte auch bedacht werden, dass für unterschiedliche Systeme womöglich noch zusätzliche Faktoren hinzukommen können, die spezifisch für das jeweilige System sind und auch von den Interessen der davon betroffenen Stakeholder abhängig sind.

Fabian et al. sehen die Definition von Sicherheitsanforderungen bei IT-Systemen daher als multilaterale Angelegenheit, da meist eine Vielzahl von Akteuren unterschiedliche und oft sogar gegensätzliche Interessen haben. Diese unterschiedlichen Sicherheitsziele müssen daher identifiziert werden, um anschließend jeweilige Konflikte zu behandeln und die Resultate in den Einklang mit den funktionalen Anforderungen des Systems gebracht werden. Essenziell sei dabei, dass diese Prozesse geschehen müssen, bevor das Design eines Systems festgelegt wird, da Sicherheitsanforderungen die funktionalen Anforderungen beeinflussen können, welche wiederum Auswirkungen auf das Design eines Systems haben (Fabian et al., 2010, S. 7-8).

Daraus resultiert, dass Sicherheitsanforderungen grundsätzlich im Vorfeld geklärt werden müssen und nicht im Nachhinein definiert werden sollten, weil dies sonst zu Konflikten mit der Funktionalität führen kann. Dies ist jedoch nur dann möglich, wenn die entsprechenden

Anforderungen keinen Veränderungen unterliegen, da es sich als schwierig erweisen kann, spezifische Standards zu berücksichtigen, welche erst nach dem Design des Systems oder sogar erst nach dessen Inbetriebnahme festgelegt werden.

Dies ist insofern von Bedeutung, da gesetzliche Vorgaben, die zu einem späteren Zeitpunkt verabschiedet werden, zusätzliche Anforderungen an die Sicherheit stellen können, mit denen im Vorfeld womöglich gar nicht gerechnet wurde. Da es sich bei der DSGVO um eine neue Verordnung handelt, muss also bedacht werden, dass sie bei der Planung vieler IT-Systeme noch nicht existierte und manche ihrer Anforderungen erst im Nachhinein in den Systemen angewendet wurden. Daher wird zu einem späteren Zeitpunkt die Perspektive von Unternehmen auf mögliche Probleme bei der Implementierung der DSGVO in den Vordergrund rücken.

Zunächst wird allerdings das Verhältnis zwischen Risikomanagement und einer bestimmten Reihe von Standards behandelt, um zu sehen, ob sich hier Anhaltspunkte ermitteln lassen, welche sich auch auf die Rolle der DSGVO übertragen lassen.

2.4.1 Risikomanagement und die ISO/IEC 27000-Reihe

Für den Fokus dieser Arbeit empfiehlt es sich, Risikomanagement im Kontext von anderen Vorgaben wie zum Beispiel von Gesetzen und international etablierten Standards zu betrachten. Dazu es nützlich, einen Blick auf Standards, die von der Internationalen Organisation für Normung (ISO) in Zusammenarbeit mit der Internationalen Elektrotechnischen Kommission (IEC) erstellt wurden, zu werfen. Hierbei handelt es sich um die Reihe 27000, welche spezifisch für Informationssicherheit konzipiert wurde. Innerhalb dieser Familie sind zum Beispiel ISO/IEC 27001 für die Darlegung von Anforderungen an ein Information Security Management System (ISMS) und vor allem ISO/IEC 27005 für die Präzisierung von Information Security Risk Management hervorzuheben (Klipper, 2015, S. 37-38).

Es muss an dieser Stelle jedoch betont werden, dass hier keine detaillierte Betrachtung dieser Standards vorgenommen wird, sondern exemplarisch beleuchtet werden soll, wie sich bestimmte Vorgaben auf das Risikomanagement auswirken können.

Sebastian Klipper kommt bei seiner Betrachtung der 27000 Reihe zu folgendem Ergebnis:

„Wer ISO/IEC 27001 nutzt, kommt nicht ohne Risikomanagement aus. Weder bei der Implementierung eines ISMS noch bei dessen Betrieb.“ (Klipper, 2015, S. 59).

Seiner Ansicht nach ist es dementsprechend nicht ersichtlich, warum der Risikomanagementprozess nicht bereits in ISO/IEC 27001 enthalten ist, sondern erst in ISO/IEC 27005. Hier wird in insgesamt zwölf Abschnitten und sieben Anhängen, auf deren genauere Betrachtung an dieser Stelle verzichtet wird, um nicht zu weit abzuschweifen, der Risikomanagementprozess in seiner Struktur und sämtlichen dazugehörigen Begriffen und Ergänzungen dargelegt. Zu beachten ist hierbei, dass dieser Prozess mit Bezug auf die ISO-Standards dabei an das jeweilige Unternehmen angepasst werden kann. Dementsprechend muss nicht alles detailgetreu übernommen werden, solange aus dem Prozess angemessene Sicherheitsmaßnahmen hervorgehen. Der laut Klipper womöglich wichtigste Aspekt dabei ist, welche Konsequenzen mit einem Schadensfall einhergehen. Daher sollte beim Risikomanagement Faktoren wie mögliche Gesetzesbrüche und die Höhe potenzieller Strafen eine entscheidende Rolle spielen (Klipper, 2015, S. 59-95).

Anhand dieses Beispiels wird deutlich, dass es nicht zwangsläufig einen strikt vorgegebenen Weg gibt, wie Standards implementiert werden, solange die entscheidenden Prinzipien berücksichtigt werden. Eine Implementierung kann dementsprechend in verschiedenen Unternehmen unterschiedlich ausfallen, die dennoch gleichermaßen korrekt sein können. Besonders interessant ist auch die Feststellung von Klipper, nach der die Anwendung bestimmter Standards ohne Risikomanagement nicht möglich ist. Bereits im Vorfeld wurde erwähnt, wie sich Risikomanagement an gegebenen Standards und gesetzlichen Vorgaben orientieren muss. Wenn man also diese beiden Punkte miteinander verknüpft, resultiert dies in einem gegenseitigen Abhängigkeitsverhältnis beider Faktoren aus Sicht der Unternehmen, da eine konsequente Umsetzung des einen Faktors ebenfalls die Berücksichtigung des anderen verlangt. Es sollte hierbei jedoch in Betracht gezogen werden, dass sich der Ansatz von Klipper spezifisch auf ISO/IEC 27001 konzentriert und nicht voreilig zu verallgemeinern ist. Da es sich bei der DSGVO um eine gesetzliche Verordnung handelt und Vorgaben aus ihr dementsprechend im Risikomanagement eines Unternehmens berücksichtigt werden sollten, ist zumindest diesbezüglich die Bedingung erfüllt. Zu klären ist allerdings noch, ob die Umsetzung der DSGVO selbst ebenfalls nur mithilfe von konsequentem Risikomanagement für Unternehmen möglich ist. Dieser Punkt wird

erst im folgenden Kapitel erörtert, wenn die DSGVO selbst in den Vordergrund rückt. Die Frage, ob dies auch für die Rolle der DSGVO zutrifft, muss an dieser Stelle daher vorerst offenbleiben.

2.5 Kapitelzusammenfassung

Bisher wurden einige grundlegende Verbindungen zwischen der Datenschutz-Grundverordnung, Risikomanagement und IT-Sicherheit behandelt, auch wenn an dieser Stelle vorerst noch nicht auf konkrete Details bezüglich der Inhalte der DSGVO eingegangen wurde. Um eine bessere Übersicht über die wichtigsten Begriffe, die in diesem Kapitel behandelt wurden, zu ermöglichen, werden ihre Zusammenhänge nochmals kurz zusammengefasst.

Im Zentrum stehen dabei vor allem personenbezogene Daten. Zum einen wurde thematisiert, wie Daten als schützenswertes Gut essenziell für die Sicherheitsanforderungen an ein System sind, zum anderen, wie dies durch Sicherheitseigenschaften eines Systems gewährleistet werden soll und wie unterschiedliche Schutzziele auf vielfältige Weise dafür sorgen sollen, dass die zu schützenden Daten stets geschützt und nur für rechtmäßige Nutzer unter entsprechenden Auflagen zur Verfügung stehen. Gefährdet werden diese Daten durch unautorisierte Zugriffe und Zugriffsversuche, die Angriffe genannt werden. Aus Angriffen auf IT-Systeme resultieren Risiken, deren Wahrscheinlichkeit und Folgen sich auf die Abweichungen von Ziele beziehen. Diese Ziele bestehen in diesem Fall aus den Schutzzielen, welche sich auf schützenswerte Objekte konzentrieren, bei denen es sich hierbei um personenbezogene Daten handelt. Die Aufgabe des Risikomanagements ist es die Wahrscheinlichkeiten und Schäden von Angriffen weitestgehend abzumildern. Dieser Prozess muss sich dabei kontinuierlich an wesentlichen Vorgaben und Standards orientieren, zu denen ebenfalls die DSGVO gehört. Zu bedenken gilt, dass ein System gemäß den Überlegungen von Königs nur dann wirklich sicher ist, wenn sämtliche Abweichungen von allen Zielen unmöglich sind. In diesem konkreten Fall würde dies bedeuten, dass alle Schutzziele jederzeit garantiert wären und keine Gefahr bestünde, gegen die Auflagen der DSGVO zu verstoßen. Allerdings wurde auch explizit behandelt, dass eine Abwehr von allen Angriffen nicht möglich sei, weshalb auch grundsätzlich mit der Abweichung von Zielen zumindest langfristig zu rechnen ist. Die im Vordergrund stehenden Folgen

jener Abweichungen sind dabei die Schäden, welche in Form von Strafzahlungen auftreten können, welche in der DSGVO verankert sind. Die Abweichung von einem Schutzziel verursacht im Kontext dieser Arbeit also nur dann explizit einen Schaden, wenn es tatsächlich zu einer Verurteilung kommt. Im nachfolgenden Kapitel werden Strafzahlungen selbst gesondert betrachtet werden. Außerdem wird ein Beispiel behandelt werden, bei dem jene Strafzahlungen nicht zur Geltung kamen und warum dies der Fall war.

Außerdem wurde ermittelt, dass Sicherheitsanforderungen unterschiedlichen Ursprungs, zu denen auch gesetzliche Anforderungen gehören, Schwierigkeiten bei ihrer Implementierung mit sich führen. Dies gilt insbesondere dann, wenn diese Anforderungen erst im Nachhinein auf ein bestehendes System angewendet werden sollen. Dabei können selbst Vorgaben, die die Details ihrer Implementierung offenlassen, von Bedeutung sein. Daher ist es an dieser Stelle naheliegend, sich mit den Inhalten der DSGVO zu beschäftigen, um zu analysieren, welche Vorgaben sich aus ihr ableiten lassen und wie ihre Inhalte mit den zuvor ermittelten Konzepten zusammenhängen. Im folgenden Kapitel wird daher die Datenschutz-Grundverordnung selbst in den Vordergrund rücken.

3 DSGVO und Risikomanagement

In diesem Kapitel sollen einige wesentliche Verbindungen zwischen der DSGVO und Risikomanagement aufgezeigt werden. Dazu wird gezielt auf einige spezifische Artikel eingegangen, aus denen Vorgaben für den Umgang mit personenbezogenen Daten hervorgehen, welche beim Risikomanagement bedacht werden müssen. Zusätzlich soll dieses Kapitel Probleme bei der Implementierung, sowie die möglichen Konsequenzen von Nichteinhaltung der DSGVO-Standards thematisieren. Außerdem wird Der Angriff auf das Berliner Kammergericht analysiert, welcher im folgenden Kapitel als Grundlage für einen Beispielfall dienen soll.

3.1 Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung ist auf EU-Ebene die bedeutendste rechtliche Grundlage zum Thema Datenschutz. Sie enthält elf Kapitel mit insgesamt neunundneunzig Artikeln, die von Grundsätzen und allgemeinen Pflichten bis hin zu Sanktionen bei Verstößen eine Vielzahl von Themen umfassen.

Im vorherigen Kapitel wurde für das Risikomanagement in der IT-Sicherheit die besondere Bedeutung von Schutzzielen in Bezug auf personenbezogene Daten hervorgehoben. Dementsprechend ist es notwendig, den Zusammenhang zwischen der DSGVO und diesen Schutzzielen zu ermitteln. Zusätzlich dazu werden einige weitere Artikel behandelt, die es im Kontext dieser Arbeit zu berücksichtigen gilt. Aus den gesammelten Ergebnissen kann anschließend die Rolle der DSGVO in diesem Zusammenhang abgeleitet werden. Es werden an dieser Stelle jedoch nur einige essenzielle Artikel vorgestellt, um den Rahmen dieser Arbeit nicht zu sprengen. Die Liste der angesprochenen Artikel erhebt dementsprechend auch keinen Anspruch auf Vollständigkeit was die Verbindungen zwischen den behandelten Schutzzielen und der DSGVO angeht. Es geht vielmehr darum, festzustellen, ob sich derartige Verbindungen erkennen lassen und welche Aussagen diesbezüglich für die Rolle der DSGVO beim Risikomanagement in der IT-Sicherheit gemacht werden können.

Bei genauerer Betrachtung lässt sich hierbei feststellen, dass solche Verbindungen zwischen DSGVO und Schutzzielen durchaus zu finden sind, allerdings in manchen Fällen komplex und nicht immer eindeutig. Daher wird in der folgenden Tabelle eine Übersicht über die im nachfolgenden Teil dieses Kapitels gesammelten Zusammenhänge dargestellt.

Tabelle 2: Schutzziele und verwandte Artikel der DSGVO

Bezeichnung	**Bedeutung**	**Relevante Artikel**
Authentizität	Identitäten können überprüft werden	Artikel 5
Datenintegrität	Geschützte Daten können nicht unbefugt verändert werden	Artikel 5 & 32
Informationsvertraulichkeit	Einsicht nur mit entsprechender Berechtigung	Artikel 5, 25 & 32
Verfügbarkeit	Authentifizierte Subjekte sollen ihre Rechte wahrnehmen können	Artikel 32
Verbindlichkeit	Aktionen können eindeutig zugeordnet werden	Artikel 13, 14 & 15
Anonymisierung und Pseudonymisierung	Daten sollen für Außen-stehende nicht mit Personen in Verbindung gesetzt werden können	Artikel 4, 25 & 32

(vgl. Eckert, 2018, S. 8 ff)

3.1.1 Die Sicherheit von personenbezogenen Daten in der DSGVO

Ein wesentlicher Artikel für den Datenschutz im Allgemeinen ist Artikel 25. Hier ist festgelegt, dass von den Verantwortlichen der Datenverarbeitung geeignete technische und

organisatorische Voreinstellungen getroffen werden sollen. Dies beinhaltet, dass nur für den Verarbeitungszweck notwendigen Daten genutzt, die Grundsätze der DSGVO umgesetzt und entsprechende Garantien in die Verarbeitung einbezogen werden sollen. Zu berücksichtigen sind hierbei unter anderem der Stand der Technik, die Kosten der Implementierung und die Eintrittswahrscheinlichkeiten und Schwere der verbundenen Risiken. Als ein Beispiel für entsprechende Maßnahmen wird explizit die Pseudonymisierung von Daten genannt. Außerdem soll ohne Zustimmung der jeweiligen Personen der Zugriff auf ihre persönlichen Daten keiner unbestimmten Zahl anderer Personen ermöglicht werden (Artikel 25 Absatz 1 & 2 DSGVO). Neben der erwähnten Pseudonymisierung ist bereits hier ein weiteres Schutzziel erkennbar, da der eingeschränkte Zugriff auf Daten einen eindeutigen Zusammenhang mit Informationsvertraulichkeit bedeutet.

Für diesen Artikel wurde später eine Reihe von Leitlinien vom European Data Protection Board (EDPB) veröffentlicht. Unter anderem wurde präzisiert, dass nicht die Umsetzung bestimmter technischer und organisatorischer Mittel vorgeschrieben wird, sondern diese an spezifische Verarbeitungsfälle angepasst und gegebenenfalls erweitert werden sollen (EDPB, 2020, S. 8). Dies bedeutet also einen gewissen Handlungsspielraum für die jeweiligen Unternehmen, was die Wahl der Mittel angeht, jedoch auch eine hohe Eigenverantwortung, jeweils die passenden Maßnahmen einzuleiten.

Auch zu Beginn von Kapitel IV Abschnitt 2, der sich mit der Rolle von Sicherheit von personenbezogenen Daten für Verantwortliche und Auftragsverarbeiter beschäftigt, wird ein direkter Bezug zu gleich mehreren der erwähnten Schutzziele hergestellt. So heißt es in Artikel 32, dass bei der Verarbeitung von personenbezogenen Daten die jeweils Verantwortlichen und Auftragsverarbeitenden geeignete Maßnahmen treffen müssen, um ein dem Risiko angemessenes Schutzniveau zu garantieren, wobei äußere Faktoren wie Kosten, Umfang und der Stand der Technik berücksichtigt werden sollen. Diese Maßnahmen sollen dabei explizit sicherstellen, dass Pseudonymisierung und Verschlüsselung von Daten, Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit von Systemen und Diensten gewährleistet wird. Zusätzlich wird verlangt, dass auch nach Zwischenfällen technischer Art, diese Aspekte möglichst schnell wieder herzustellen sind und Verfahren implementiert werden, die diese Maßnahmen überprüfen, bewerten und evaluieren (Artikel 32 Absatz 1 DSGVO).

Da bereits in diesem Absatz die Mehrheit der behandelten Schutzziele mit Ausnahme von Authentizität und Verbindlichkeit namentlich erwähnt werden, erscheint es deutlich, dass ein direkter Zusammenhang zwischen der Datenschutz-Grundverordnung und den behandelten Schutzzielen besteht. Allerdings lohnt sich an dieser Stelle ein genauerer Blick auf die Formulierungen, um sicherzustellen, dass die genannten Begriffe auch tatsächlich mit den jeweiligen Schutzzielen zusammenhängen.

3.1.2 Die Rolle von Verfügbarkeit

Im Falle des Schutzzieles der Verfügbarkeit muss wie zuvor erwähnt sichergestellt werden, dass autorisierte Nutzer ihre Rechte bezüglich der betroffenen Daten (z.B. Dateneinsicht) wahrnehmen können. Dies wird in Artikel 32 in zweierlei Weise hervorgehoben, zum einen wird Verfügbarkeit darauf bezogen, dass Systeme und Dienste die Verarbeitung von Daten sicherzustellen haben (Artikel 32 Absatz 1b) DSGVO) und zum anderen, dass auch nach physischen oder technischen Problemen die Verfügbarkeit von Daten und der Zugang zu ihnen schnellstmöglich herzustellen ist (Artikel 32 Absatz 1c) DSGVO). Daraus resultiert, dass auch dieses Schutzziel in der DSGVO repräsentiert wird, wobei bemerkenswerterweise aus dem zweiten Absatz hervorgeht, dass grundsätzliche Verfügbarkeit von Daten und der Zugang zu ihnen voneinander abgegrenzt werden, aber beides gleichermaßen eingefordert wird. Dementsprechend wird die Wahrung von Nutzungsrechten dadurch gesetzlich abgesichert, dass diese nicht nur theoretisch möglich sein sollen, sondern auch praktisch durchführbar sein müssen.

3.1.3 Die Rolle von Pseudonymisierung

Im Falle des Schutzziels der Anonymisierung und Pseudonymisierung ist der Zusammenhang dadurch gegeben, dass explizit die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten genannt wird (Artikel 32 Absatz 1a) DSGVO) und dies mit den im vorherigen Kapitel genannten Maßnahmen zum Erreichen dieses Ziels konform ist. Noch deutlicher wird der Zusammenhang in Artikel 4, wo der Begriff folgendermaßen definiert wird:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck: […] 5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;“ (Artikel 4 Absatz 5 DSGVO).

Auch wenn hier nicht explizit der Einsatz von Zuordnungsvorschriften benannt wird, so wird deutlich, dass Pseudonymisierung in der DSGVO mit der behandelten Bedeutung des Schutzziels übereinstimmt.

3.1.4 Informationsvertraulichkeit, Authentizität & Datenintegrität in Artikel 5

Doch auch jenseits dieses Artikels lassen sich einige Verbindungen erkennen. Dies betrifft beispielsweise die Schutzziele Informationsvertraulichkeit (Dateneinsicht nur mit Berechtigung) und Authentizität (Überprüfung von Identitäten für berechtigten Zugang) und Datenintegrität (Schutz von Daten vor unbefugter Veränderung). Zu beachten ist hierbei vor allem mit Artikel 5 einer der Grundsätze der DSGVO, in dem festgelegt ist, dass die Verantwortlichen für den Umgang mit personenbezogenen Daten durch Technikgestaltung und organisatorische Maßnahmen dafür Sorge tragen müssen, dass die Rechte der jeweiligen Personen ausreichend geschützt werden. Darunter fällt auch, dass entsprechende Maßnahmen getroffen werden, damit solche Daten nicht in die Hände von Unbefugten gelangen können bzw. unrechtmäßig verarbeitet, geschädigt oder vollständig vernichtet/verloren werden, wobei Integrität und Vertraulichkeit explizit erwähnt werden (Artikel 5 Absatz 1f) DSGVO). Hieraus ergibt sich ein klarer Auftrag für Unternehmen, geeignete Mittel zu wählen, um fremdem und unsachgemäßem Zugriff auf personenbezogene Daten entgegenzuwirken. Wichtig ist hierbei, dass die genannten Begriffe tatsächlich mit den jeweiligen Schutzzielen übereinstimmen. Der unsachgemäße Zugriff in Form von Manipulation oder Veränderung wäre ein Verstoß gegen das Prinzip der Datenintegrität, weshalb die Verbindung zu diesem Schutzziel eindeutig ist. Zudem lässt sich aus dem Artikel ebenfalls schließen, dass der Schutz vor fremdem Zugriff auch Maßnahmen

umfassen muss, die den Zugriff auf die jeweiligen Daten für Personen mit entsprechender Berechtigung gewähren, während Unbefugten dieser Zugriff verwehrt wird, was wiederum das Schutzziel der Informationsvertraulichkeit betrifft. Die Bedeutung der Authentizität hingegen erscheint nicht so eindeutig, wie die der anderen beiden Schutzziele. Um hier eine Verbindung herzustellen, sollte bedacht werden, wie die Vertraulichkeit von Daten gewährleistet werden kann, indem zwischen befugten und unbefugten Zugriffen unterschieden werden kann. Denn damit autorisierte Personen beweisen können, dass sie rechtmäßig auf bestimmte Daten zugreifen dürfen, müssen Authentifikationsverfahren implementiert werden, sodass sie anhand ihrer Authentifikationsdaten ihre Identität bestätigen können. Die aus Artikel 5 resultierenden Vorgaben lassen sich also auch mit Authentizität in Verbindung bringen, da die Gewährleistung von Vertraulichkeit nahelegt, dass die Identitäten von Usern überprüft werden kann und nur ausgewählte User Zugriff auf geschützte Daten erhalten.

3.1.5 Die Rolle der Verbindlichkeit

Als letztes Schutzziel verbleibt demnach Verbindlichkeit, für das es deutlich schwieriger ist, einen direkten Bezug zu erkennen. In Zusammenhang mit der Verarbeitung von personenbezogenen Daten würde dies bedeuten, dass Aktionen, die mit solchen Daten zusammenhängen (z.B. Dateneinsicht), entsprechend zugeordnet werden können. Obwohl der Begriff zwar in der DSGVO erwähnt wird, geschieht dies jedoch anstatt im Kontext der Zuordnung von Aktionen in anderen Zusammenhängen, beispielsweise der Verbindlichkeit von internen Vorschriften von Unternehmen und Rechtsverbindlichkeit wie es in Artikel 47 der DSGVO erwähnt wird (Artikel 47 DSGVO). Um hier mögliche Verbindungen aufzeigen zu können, muss sich also auf die Bedeutung des Schutzzieles konzentriert werden und nicht auf seine Bezeichnung.

Fündig wird man hier vor allem in Kapitel III, in dem die Rechte von betroffenen Personen dargelegt werden. In Abschnitt 2 finden sich dazu bedeutende Ausführungen über die Informationspflicht bei der Erhebung von personenbezogenen Daten in Artikel 13 und 14. Im erstgenannten wird dabei festgehalten, welche Informationen betroffenen Personen bei der Erhebung ihrer Daten mitgeteilt werden müssen. Darunter fallen unter anderem die Kontaktinformationen von verantwortlichen Personen in diesem Zusammenhang, was ebenfalls etwaige

Datenschutzbeauftragte miteinschließt, andere Empfänger der Daten und Verwendungszwecke, wobei hier auch angegeben werden muss, ob diese Daten auch für andere Zwecke als die, für die sie ursprünglich erhoben wurden verarbeitet werden sollen (Artikel 13 Absatz 1a) - c) & e) & 3 DSGVO). Artikel 14 konzentriert sich auf ähnliche Fälle, bei denen die Daten allerdings nicht bei den betroffenen Personen selbst erhoben wurden. Auch hier gilt es die betroffenen Personen über weitestgehend ähnliche Sachverhalte aufzuklären, die insbesondere auch die bereits für Artikel 13 besprochenen Informationen betreffen (Artikel 14 Absatz 1 a) - c) & e) & 4 DSGVO). Wie an dieser Stelle bereits deutlich wird, spielt Transparenz eine wichtige Rolle. Dies wird auch im folgenden Artikel 15 deutlich, der die Rechte von betroffenen Personen konkretisiert, im Bedarfsfall darüber informiert zu werden, ob und für welche Zwecke diese Informationen verarbeitet werden, welche Kategorien personenbezogener Daten verarbeitet werden und vor allem auch, wem die Daten offengelegt worden sind bzw. offengelegt werden. Dies schließt ebenfalls internationale Empfänger außerhalb der EU mit ein (Artikel 15 Absatz 1 a) - c) DSGVO). Entscheidend für den Kontext der Verbindlichkeit ist hier, dass Empfänger von Daten während der Verarbeitung bekannt gegeben werden müssen, falls dies von den betroffenen Personen verlangt wird. Damit dies möglich ist, muss nämlich bekannt sein, wer die Empfänger dieser Daten waren. Zwar lässt sich aus den genannten Artikeln nicht ableiten, dass jederzeit stets die individuelle Person bekannt gemacht werden muss, welche einen Auftrag verarbeitet, jedoch ist die Festlegung, dass sämtliche Empfänger bekannt gemacht werden müssen, Grund genug, entsprechende Maßnahmen zu implementieren, die sicherstellen, dass es keinerlei Zugriffe auf die jeweiligen Daten geben kann, die unerwünscht und unbekannt sind. Dies legt nahe, dass sämtliche Zugriffe auf personenbezogene Daten im Zuge der Verarbeitung erkannt und zugewiesen werden können sollten, damit die Partei, welche die Aktionen durchgeführt hat und die jeweiligen Aktionen selbst festgehalten werden können. Die Bedeutung des Schutzziels Verbindlichkeit in der DSGVO ist dementsprechend zwar nicht explizit hervorgehoben, allerdings durch die dargelegten Anforderungen bezüglich Transparenz und Informationspflicht relevant, um diese erfüllen zu können. Es liegt dabei auch im Interesse der Verantwortlichen, festhalten zu können, wer auf welche Weise auf bestimmte Daten zugegriffen hat, da zumindest Informationen, die die Dateneinsicht betreffen im Bedarfsfall an die betroffenen Personen übermittelt werden müssen und alle Verstöße diesbezüglich auf die Verantwortlichen zurückfallen würden.

Zusammenfassend lässt sich bereits an dieser Stelle festhalten, dass sich zu allen behandelten Schutzzielen eine Verbindung erkennen lässt, auch wenn diese nicht immer eindeutig ist. Bemerkenswert ist hierbei vor allem, dass aus der DSGVO vor allem die Forderungen hervorgehen, die Rechte von Personen in Bezug auf ihre persönlichen Daten zu wahren, indem z.B. entsprechende Maßnahmen auf organisatorischer und technischer Ebene getroffen werden. Die Details für die Umsetzung solcher Maßnahmen werden jedoch offengelassen. Die Verantwortung, die geeigneten Mittel zu finden obliegt damit den Verantwortlichen für die Datenverarbeitung. Ein Unternehmen, das mit personenbezogenen Daten arbeitet, muss also selbst herausfinden, welche Anstrengungen nötig sind, um rechtlich auf der sicheren Seite zu sein.

3.1.6 Pflichten und Konsequenzen bei Datenschutzverletzungen

Zusätzlich zu den bisher besprochenen Inhalten ergeben sich aus der DSGVO Vorgaben, die es zu beachten gilt, wenn die getroffenen Schutzmaßnahmen fehlschlagen sollten.

Artikel 33 behandelt beispielsweise eine Meldepflicht von Verletzungen des Schutzes von personenbezogenen Daten. Hierbei gilt, dass binnen 72 Stunden nachdem die Verantwortlichen von einer Datenschutzverletzung erfahren haben, die dafür zuständigen Aufsichtsbehörden informieren müssen. In diesem Artikel ist außerdem festgehalten, dass die Benachrichtigung der Behörden nach Möglichkeit Informationen über Ursache, Auswirkungen, Schutzmaßnahmen enthalten sollen, sowie die Möglichkeit, mit der für den Datenschutz verantwortlichen Person in Kontakt zu treten (Artikel 33 DSGVO). Dabei kann es sich beispielsweise auch um einen benannten Datenschutzbeauftragten handeln, welcher unter anderem dafür verantwortlich ist, mit Aufsichtsbehörden zu kooperieren (Artikel 39 Absatz 1 d) DSGVO). Jene Datenschutzbeauftragte sollen vor allem in Bezug auf ihre Qualifikationen und ihr Wissen über Datenschutz ausgewählt werden (Artikel 37 Absatz 5), was bedeutet, dass nur spezielle Fachkräfte für eine derartige Position in Frage kommen. Es gilt daher bei der Einhaltung der DSGVO nicht allein darum Datenschutzverletzungen gegenüber personenbezogenen Daten zu vermeiden, sondern auch die entsprechenden Vorkehrungen zu treffen für den Fall, dass die eigenen Schutzanstrengungen vergebens waren.

Von großer Bedeutung sind allerdings auch die Konsequenzen von Verstößen gegen die DSGVO. Dabei liegt es in der Verantwortung der zuständigen Behörden, entsprechende Verstöße abhängig von Kriterien wie z.B. ob dem Fehlverhalten Fahrlässigkeit oder Vorsätzlichkeit zugrunde lag, zu sanktionieren. So kann auch explizit die Nichtbefolgung einer verbindlichen Anweisung einer Aufsichtsbehörde eine Strafzahlung verursachen. Artikel 25 erhält hierbei auch zusätzliche Bedeutung, da die in diesem Artikel behandelten technischen und organisatorischen Maßnahmen ebenfalls als Faktoren hinzugezogen werden können (Artikel 83 Absatz 1 & 2 DSGVO). Von großer Relevanz dürfte für Unternehmen selbstverständlich die Höhe einer möglichen Strafe sein. Diese können stark variieren, da sie sich auch an der Größe eines Unternehmens orientieren und im Extremfall daher bis zu 20 Millionen Euro oder bis zu 4% ihres weltweit erwirtschafteten Jahresumsatzes betragen. Die Mitgliedsstaaten haben jedoch einen gewissen Handlungsspielraum bezüglich der Umsetzung, z.B. ob derartige Geldbußen ebenfalls gegen öffentliche Institutionen verhängt werden können (Artikel 83 Absatz 4, 5, 6 & 7 DSGVO). Auf diese Weise ist gewährleistet, dass die Sanktionen Unternehmen jeglicher Größe empfindlich treffen können, um die Einhaltung der DSGVO zu forcieren.

Diese Bußgelder, welche bereits zuvor als Schäden im Zusammenhang mit der Abweichung von Schutzzielen erwähnt wurden, haben für Unternehmen eine große Bedeutung. Wie diese Sanktionen in Deutschland ausfallen können, wird daher im folgenden Abschnitt des Kapitels behandelt werden.

3.2 Die Bemessung von Bußgeldern in Deutschland

Auf Basis von Artikel 83 wurde von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein Konzept zur Bußgeldzumessung erstellt, welches explizit für die Sanktionierung von Unternehmen konzipiert wurde und auch nur in derartigen Fällen zur Anwendung kommen soll. Dieses Konzept ist allerdings nicht darauf ausgelegt, dauerhaft die Grundlage für Strafzahlungen zu bilden und kann von den Datenschutzaufsichtsbehörden des Bundes und der einzelnen Bundesländer verändert oder aufgehoben werden. Spätestens jedoch mit der Veröffentlichung der verbindlichen Leitlinien für die Festsetzung von Geldbußen durch den Europäische Datenschutzausschuss (EDSA) wird das Konzept

seine Gültigkeit verlieren (DSK, 2019, S. 1-2). Es ist daher davon auszugehen, dass das gegenwärtige Konzept nicht langfristig zur Anwendung kommen wird. Allerdings kann es dennoch als wertvolle Informationsquelle für diese Arbeit dienen, da es sich nahe an den Vorgaben aus der DSGVO orientiert und sich auch zukünftige Bußgeldkonzepte zumindest diesen Vorgaben unterwerfen müssen.

Die Zuweisung von Bußgeldern soll gemäß dem Konzept in mehreren Schritten erfolgen, um für jeden individuellen Fall eine angemessene Sanktion zu ermöglichen.

Diese Schritte orientieren sich stark an Artikel 83 der DSGVO, da hier unter anderem die Größe des Unternehmens, also der jährliche Umsatz berücksichtigt wird. Allerdings wird der Umsatz auch ins Verhältnis zu dem mittleren Jahresumsatz und dem darauf basierenden wirtschaftlichen Grundwert von Unternehmen ähnlicher Größe gesetzt. Eine Ausnahme besteht hierbei für Unternehmen mit einem jährlichen Umsatz von mehr als 500 Millionen Euro, da ab hier der vorgesehene prozentuale Bußgeldrahmen von bis zu 4%, der aus Artikel 83 hervorgeht, angewendet wird. Ebenfalls auf Artikel 83 basiert der Einbezug der Umstände des Vorfalls, sodass der bis hierhin ermittelte Betrag mit einem Faktor multipliziert wird, der sich an der Schwere der Tat orientiert. Hierbei spielt vor allem eine Rolle, ob es sich um vorsätzliche Schuld handelt und ob es sich um einen materiellen oder lediglich einen formellen Verstoß handelt. Also je schwerer die jeweilige Tat angesehen wird, desto höher kann dabei der Faktor ausfallen. Abschließend können weitere Faktoren hinzugezogen werden, wie z.B. Verfahrenslänge oder die Gefahr von Insolvenz für das Unternehmen (DSK, 2019, S. 2-8).

Ein Beispiel für die Verhängung von Bußgeldern in Deutschland ist die Strafe von über 900.000 Euro, die im September 2021 in Hamburg gegen die Vattenfall Europe Sales GmbH verhängt wurde. Als ausschlaggebender Grund für die Verurteilung wurde dabei mangelnde Transparenz beim Vergleich von Kundendaten angegeben (EDPB, 2021). Derartige Strafen können allerdings auch deutlich höher ausfallen. Ein besonders schwerwiegendes Urteil wurde beispielsweise im selben Jahr in Irland gegen WhatsApp Ireland Ltd. verhängt. Auch hier war mangelnde Transparenz maßgeblich entscheidend für die Verurteilung, wobei vor allem Intransparenz beim Austausch von Nutzerdaten mit anderen Unternehmen des Facebook-Konzerns im Vordergrund stand. Das Bußgeld betrug insgesamt 225 Millionen Euro (Data Protection Commission, 2021).

Wie sich an dieser Stelle bestätigt, kann also der Verstoß gegen die DSGVO schwere finanzielle Konsequenzen für Unternehmen bedeuten. Es wird jedoch auch ersichtlich, dass es einen gewissen Spielraum für die Anwendung von Bußgeldern gibt. Insbesondere der Einbezug von fallspezifischen Umständen sorgt dafür, dass sich potenzielle Strafzahlungen nur schwer im Vorfeld abschätzen lassen können. Aus diesem Grund sollten nicht nur präventive Maßnahmen im Risikomanagement berücksichtigt werden, sondern auch die notwendigen Reaktionen. Von wesentlicher Bedeutung ist hierbei auch, dass angemessenes Verhalten (insbesondere die notwendigen Meldungen an die zuständigen Behörden) verantwortungsvollen Umgang mit dem Vorfall zeigt, das Unterlassen einer Meldung hingegen einen weiteren Verstoß gegen die DSGVO bedeuten würde.

3.3 Der Fall des Berliner Kammergerichts

Welche Auswirkungen Sicherheitslücken haben können, lässt sich am besten anhand eines Beispiels darlegen. In jüngerer Vergangenheit ist IT-Sicherheit in Deutschland oft im Zusammenhang mit Störfällen, Cyberangriffen oder ähnlichen Vorfällen in die Schlagzeilen geraten. Einer dieser Vorfälle fand im Jahre 2019 beim Berliner Kammergericht statt.

3.3.1 Der Vorfall und die anschließende Untersuchung

Am 25.09.2019 meldete das Berliner Kammergerichts eine mögliche Infizierung ihres Netzwerkes mit Malware. Aus dem veröffentlichten Bericht von T-Systems, die mit der Untersuchung dieses Falls betraut wurden, geht hervor, dass es sich dabei um eine Infektion mit TrickBot und Emotet Schadsoftware handelte, die vermutlich am 20.09. stattfand. Dies ist insofern von Bedeutung, da dies auch eine Gefahr für die Daten innerhalb des Netzwerks darstellte. Die Malware Emotet wird dazu eingesetzt, um andere Malware, wie in diesem Falle TrickBot den Zugang zu einem Netwerk zu ermöglichen. Diese kann daraufhin mit diversen Modulen unterschiedliche Konsequenzen wie zum Beispiel Datenabfluss verursachen. Auf dem betroffenen System wurden entsprechende Module identifiziert, welche dafür konzipiert waren,

Systeminformationen und Passwörter weiterzuleiten. Ob und welche Daten letztendlich gestohlen bzw. manipuliert wurden, konnte nicht festgestellt werden (T-SYSTEMS, 2019, S. 4-10 & 13). Interessant ist dieser Fall für diese Arbeit vor allem auch, weil trotz der umfassenden Analyse der ausschlaggebende Grund für den Vorfall nicht restlos geklärt werden konnte. Dennoch können einige wichtige Erkenntnisse aus ihm gewonnen werden.

Aufgrund von bekannten Vorgängen mit der verwendeten Schadsoftware wurde gemutmaßt, dass Makros in Worddokumenten verwendet wurden, wobei nicht mit Sicherheit gesagt werden konnte, auf welche Weise diese Dokumente in das System gelangt waren und wie diese Makros aktiviert wurden. Dennoch wurden zwei mögliche Infektionswege ermittelt. Beim ersten handelt es sich um den Anhang eines entsprechenden Dokuments an eine E-Mail, was laut Bericht eine gängige Vorgehensweise für den Einsatz von Emotet ist. Da jedoch in keiner Mail auf dem Rechner, von dem aus sich die Schadsoftware verbreitet hatte, Mails mit derartigen Anhängen gefunden wurden, wurde auch über die Involvierung von Mails, die über eine Webmail Website geöffnet wurden, spekuliert. Jedoch ließen sich auch hierfür keine eindeutigen Beweise finden. Als zweiter Infektionsweg hingegen wurde die Verbreitung einer schädlichen Datei über einen mobilen Datenträger diskutiert. In diesem Fall hätte ein solcher Datenträger an den betroffenen Rechner angeschlossen werden und die Malware sich im Netzwerk des Kammergerichts ausbreiten können (T-SYSTEMS, 2019, S. 9-11). Obwohl die tatsächliche Ursache also nicht festgelegt werden konnte, bietet dieser Bericht wertvolle Informationen darüber, wie der Vorfall zustande gekommen sein könnte. Hinzu kommen noch weitere Einsichten in die Sicherheitsmängel, die in diesem Bericht festgehalten wurden.

Von großer Bedeutung sind hierbei vor allem die Beobachtungen, die T-Systems bezüglich der IT-Infrastruktur und den Sicherheitsmaßnahmen, machte. So wurde im Fazit des Berichts explizit hervorgehoben, dass aufgrund von diversen Faktoren wie fehlender Proxy Logdaten und mangelnder Filterung am Gateway aus einem Standardvorfall ein schwerwiegender Fall wurde. Zusätzlich dazu wurden Probleme bei der angewendeten Endpoint Protection Lösung der Firma McAfee festgestellt, welche die Malware hätte erkennen sollen, da sie zum Zeitpunkt des Vorfalls bereits bekannt war (T-SYSTEMS, 2019, S. 13-14).

3.3.2 Erkenntnisse aus dem Vorfall und die Verbindung zur DSGVO

Aus diesem Beispiel lässt sich erkennen, wie eine Vielzahl von Faktoren mit dem Schutz von personenbezogenen Daten zusammenhängen können. Es wird beispielsweise deutlich, dass die Sicherheit von Daten von mehreren Parteien abhängig sein kann, in diesem Fall betrifft dies vor allem das Kammergericht, McAfee und T-Systems, die jeweils für die Infrastruktur, die Sicherheitssoftware und die Untersuchung des Vorfalls verantwortlich waren. Aus der Untersuchung ergaben sich dann Empfehlungen für das Kammergericht, um das Netzwerk in Zukunft besser schützen zu können. Zudem aktualisierte McAfee die verwendete Software (T-SYSTEMS, 2019, S. 4 & 13-14).

Dieses Beispiel zeigt anschaulich, wie so ein Vorfall geschehen und durch Mängel begünstigt werden kann sowie welche Konsequenzen daraus gezogen werden können. Des Weiteren ist erwähnenswert, dass es in diesem Fall um mehr als die bloße Abwehr einer Schadsoftware geht, die zur Gefahr für personenbezogene Daten werden kann. Denn wie bereits erwähnt wurde, hatten mangelnde Sicherheitsmaßnahmen dazu geführt, dass die Malware nicht nur nicht erkannt wurde, sondern sich auch ausbreiten konnte, ohne dass die damit verbundenen Vorgänge entsprechend dokumentiert wurden. Daraus lassen sich zwei wichtige Erkenntnisse ableiten: 1. Selbst wenn ein Vorfall nicht verhindert werden kann, sollte also zumindest dafür Sorge getragen werden, die Auswirkungen derartiger Vorfälle so gering wie möglich zu halten. 2. Ist es zweckmäßig, ein System so aufzubauen, dass Informationen über Vorgänge, welche mit diesen Vorfällen zusammenhängen, durch entsprechende Maßnahmen wie zum Beispiel dem Erstellen von Event Logs festgehalten werden können. Auf diese Weise könnte das System im Nachhinein mithilfe dieser Informationen optimiert werden, um für ähnliche Vorfälle in Zukunft besser vorbereitet zu sein.

Mit Bezug auf die DSGVO lässt sich sagen, dass es eine eindeutige Verbindung zu Artikel 25 gibt. Bemerkenswert ist an dieser Stelle vor allem, dass die geforderten datenschutzfreundlichen Voreinstellungen anscheinend in mehrfacher Hinsicht nicht gegeben waren, wobei für die Auswahl der Mittel primär das Kammergericht verantwortlich war, allerdings auch die Verantwortung von McAfee bedacht werden sollte, da die Software dieser Firma nicht in der Lage war, eine bekannte Angriffsform zu erkennen. Bemerkenswert ist zudem, dass die Meldung der Infektion -vorausgesetzt, der geschätzte Zeitpunkt sollte korrekt sein – erst fünf Tage später

erfolgte und es demnach davon abhängig wäre, ob die Infektion tatsächlich erst später bemerkt wurde, um die gemäß Artikel 33 geforderte Frist von 72 Stunden nicht zu überschreiten. Dies erscheint allerdings realistisch, da es sich beim 20.09.2019 um einen Freitag handelte und in den folgenden beiden Tagen aufgrund des Wochenendes der Schaden vom Personal vorerst hätte unbemerkt bleiben können. Bezüglich der Schutzziele lässt sich in Hinsicht auf den Bericht nicht eindeutig sagen, welche verletzt wurden. Dies liegt daran, dass nicht erwähnt wurde, ob mithilfe der genannten TrickBot-Module auch personenbezogene Daten selbst abgeflossen sind oder Passwörter gestohlen wurden, welche den Zugriff auf personenbezogene Daten ermöglichen. Beide Möglichkeiten würden jedoch einen Verstoß gegen die Informationsvertraulichkeit bedeuten, da hier unautorisierte Personen Dateneinsicht bekommen bekämen. Bei einer Manipulation von Daten wäre ebenfalls die Datenintegrität betroffen. Zusätzlich müsste mit einem Verstoß gegen die Verbindlichkeit gerechnet werden, da entsprechende Zugriffe mit gestohlenen Passwörtern nicht eindeutig hätten zugeordnet werden können. Ob die womöglich betroffenen (personenbezogenen) Daten anonymisiert bzw. pseudonymisiert waren, geht aus dem Bericht nicht hervor.

3.3.3 Die Folgen des Vorfalls

In Anbetracht dieser Umstände ist es interessant zu sehen, dass das gesamte Ausmaß des Vorfalls noch immer nicht vollständig erfasst wurde. Aus einem Artikel der Deutschen Welle aus dem Jahr 2020 geht hervor, dass die Möglichkeit und der Umfang von Datenabfluss nicht restlos geklärt werden konnte und die Aufklärung einen Zeitaufwand von zwei Jahren und eine zweistellige Millionensumme benötigt. Des Weiteren wurde erwähnt, dass zumindest vorerst keine gravierenden Sanktionen als Reaktion auf den Vorfall erlassen wurden. So konnte beispielsweise kein Bußgeld gegen das Kammergericht verhängt werden, da es sich um eine öffentliche Einrichtung handelt (Kuhn, 2020). Bedacht werden sollte hierbei, dass dies gemäß Artikel 83 Absatz 7 theoretisch möglich wäre, wie bereits zuvor erwähnt wurde, diese Option allerdings nicht von Deutschland implementiert wurde.

Wie dieses Beispiel zeigt, kann selbst ein teilweise unaufgeklärter Fall wertvolle Informationen über die Auswirkungen von Sicherheitslücken liefern. Diese lassen sich zu einem großen Teil

auch auf das Risikomanagement in Unternehmen anwenden, denn auch wenn das Kammergericht selbst nicht zu einer Strafzahlung verurteilt werden konnte, sollten sich Unternehmen nicht darauf verlassen, ebenfalls so glimpflich davonzukommen, da sie nicht den Schutz einer öffentlichen Einrichtung genießen. Im folgenden Kapitel werden daher grundlegenden Lösungsansätze in einem auf diesem Vorfall basierenden Fallbeispiel behandelt.

Insgesamt konnten in diesem Kapitel wesentliche Zusammenhänge zwischen den zuvor behandelten Schutzzielen als wesentlichem Aspekt des Risikomanagements in der IT-Sicherheit und der DSGVO dargelegt werden. Zudem wurde festgestellt, dass die Nichtbeachtung der gesetzlichen Vorgaben schwere finanzielle Schäden zur Folge haben kann. Derartige Missachtungen können unter anderem aus der Abweichung von Schutzzielen entstehen, weshalb ein eindeutiger Bezug zur Risikodefinition von Königs besteht. Ziel des Risikomanagements muss es an dieser Stelle sein, die Vorgaben der DSGVO zu berücksichtigen, damit finanzielle Schäden verhindert werden können. Kapitel 4 wird sich daher mit einigen Beispielfällen beschäftigen, um unterschiedliche Angriffe darzulegen und wie mit ihnen umgegangen werden kann.

3.4 Die Perspektive von Unternehmen auf die DSGVO

Da die Vorgaben der DSGVO insbesondere für Unternehmen von großer Bedeutung sind, vor allem, was die Konsequenzen bei Nichteinhaltung angeht, wird an dieser Stelle ein Blick auf deren Perspektive geworfen. Besonders interessant ist es hierbei zu sehen, ob die Implementierung von den Unternehmen mit Schwierigkeiten verbunden wird und ob sich hieraus Auswirkungen auf das Risikomanagement ableiten lassen.

3.4.1 Die Umfragen des Bitkom

Der Branchenverband der deutschen Informations- und Telekommunikationsbranche (Bitkom) hat seit der Einführung der DSGVO Umfragen bei über 500 Unternehmen unterschiedlicher Größe in Deutschland durchgeführt, aus denen bemerkenswerte Erkenntnisse hervorgehen.

In einer der Umfragen, welche seit 2019 jährlich durchgeführt wurde, standen die Herausforderungen bezüglich der DSGVO im Vordergrund (Abbildung 1). Hierbei wurde durchgehend Rechtsunsicherheit am häufigsten von allen Herausforderungen genannt, wobei der Prozentsatz zwischen 2019 und 2021 von 68% auf 78% stieg. Ebenfalls häufig wurden mangelnde Umsetzungshilfen durch Aufsichtsbehörden (66% in 2021) und eine zu hohe Anzahl an notwendigen Änderungen und Anpassungen (74% in 2021) bei der Umsetzung der DSGVO genannt. Ein zusätzlicher Faktor, der erst ab 2020 berücksichtigt wurde, ist die uneinheitliche Auslegung der DSGVO innerhalb der DSGVO, was 52% der Unternehmen im Jahre 2021 angaben (Streim & Weiß, 2021).

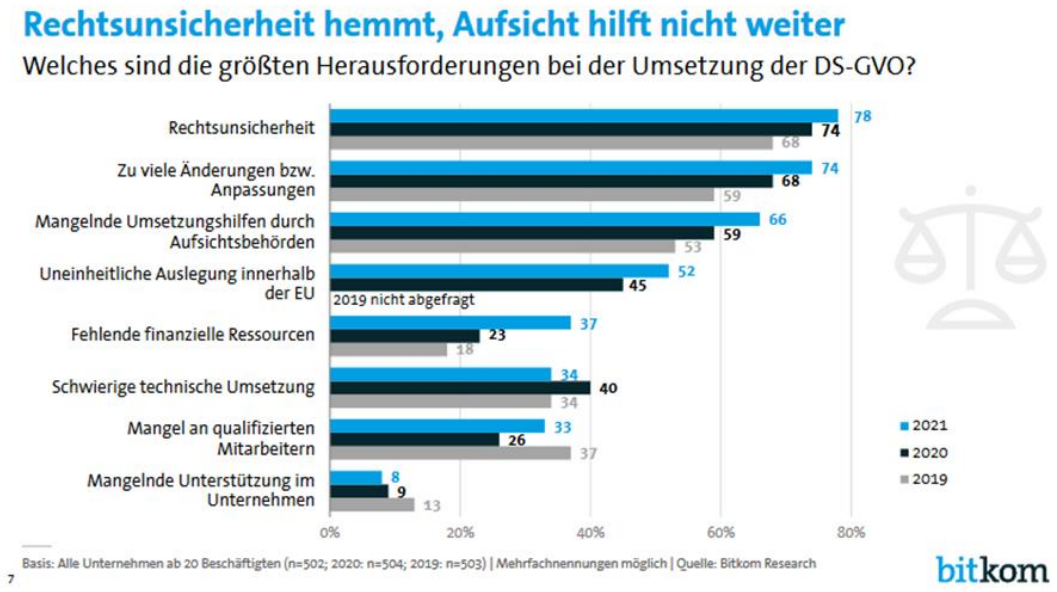

Abbildung 1: Herausforderungen bei der Umsetzung der DSGVO (Dehmel, 2021, S. 7)

Schon aus diesen Daten lässt sich eindeutig erkennen, dass die Implementierung der DSGVO zu Komplikationen bei vielen Unternehmen geführt hat, die bis heute nicht entscheidend geklärt werden konnten. Besonders bemerkenswert ist an dieser Stelle, dass die Nennung von Herausforderungen in beinahe allen Punkten seit 2019 zugenommen hat und die Tendenz dementsprechend negativ einzuschätzen ist. Doch auch andere Ergebnisse der Bitkom-Untersuchung zeugen von Problemen.

Eines dieser Probleme, welches Teil der Untersuchungen war, ist der zusätzliche Aufwand, der durch die Umsetzung der DSGVO bereits entstanden ist und auch in Zukunft bestehen wird (Abbildung 2). So gaben 32% der Unternehmen an, dass sie nicht nur zusätzlichen Aufwand durch die Implementierung hätten, sondern sogar mit steigendem Aufwand rechnen müssten. Weitere 42% klagten zumindest über zusätzlichen Aufwand, der zwar nicht steigen, aber auch nicht geringer werden würde. Besonders bezeichnend ist ebenfalls, dass kein einziges Unternehmen angab, weniger Aufwand seit der Einführung der DSGVO zu haben (Streim & Weiß, 2021).

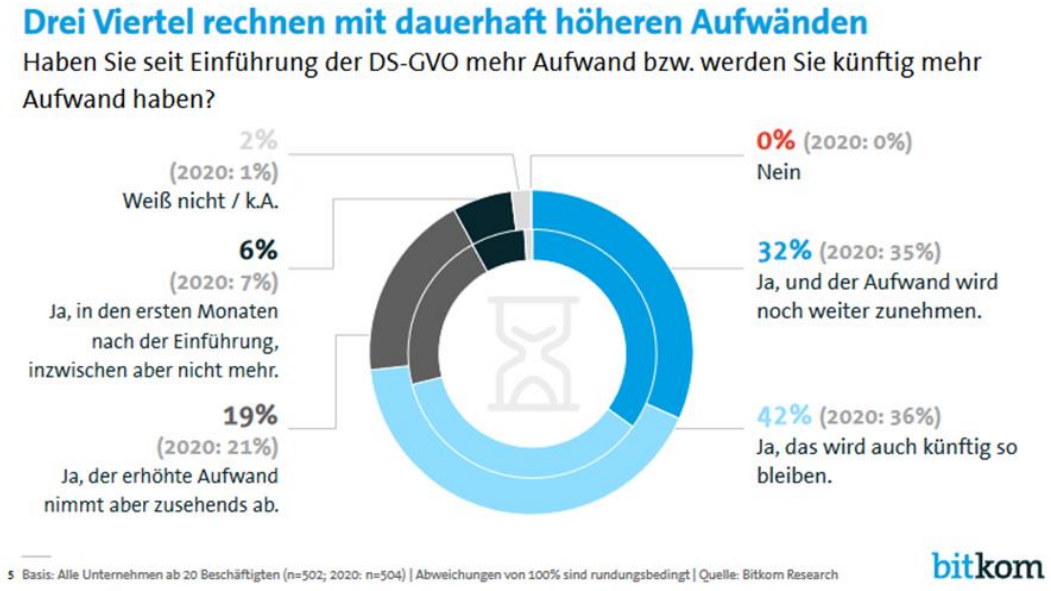

Abbildung 2: Aufwandseinschätzung bzgl. DSGVO (Dehmel, 2021, S. 5)

Es ist also davon auszugehen, dass für sämtliche Unternehmen grundsätzlich ein Mehraufwand durch die Einführung der DSGVO verursacht wurde. Außerdem lässt sich auch hier erkennen, dass die Aussichten für die Zukunft als tendenziell negativ angesehen werden, was den Aufwand angeht.

Durch den zusätzlichen Aufwand gilt es auch zu bedenken, ob die Implementierung von Seiten der Unternehmen bereits vollständig erfolgen konnte. Dies wurde in einer weiteren Umfrage (Abbildung 3) überprüft, in der im Jahr 2021 65% der Unternehmen angaben, die Datenschutzgrundverordnung mittlerweile komplett umgesetzt zu haben. Zumindest hier ist die Tendenz positiv, da der Prozentsatz mit 57% im Jahr 2020 geringer war. Bemerkenswert ist an dieser Stelle, dass vor allem kleinere Unternehmen die DSGVO noch nicht vollständig umsetzen konnten. So hatten im Jahre 2021 lediglich 58% der kleineren Unternehmen die Umsetzung nach eigenen Angaben abgeschlossen, während es bei den größten Unternehmen 90% waren. Bezüglich der Gründe, warum die Umsetzung noch nicht (vollständig) erfolgen konnte, gaben 82% der Unternehmen an, dass sie durch Corona dazu gezwungen wurden, sich zunächst auf andere Dinge zu konzentrieren. Allerdings waren auch 77% dieser Unternehmen der Ansicht, dass die Umsetzung der DSGVO gar nicht möglich sei. Ein Mangel an Personal war immerhin noch für 61% ein wesentlicher Grund. Interessanterweise nannten 47% dieser Unternehmen als Grund die Problematik von fortlaufenden Anpassungen, die durch Urteile und Empfehlungen der Aufsicht verursacht werden (Streim & Weiß, 2021).

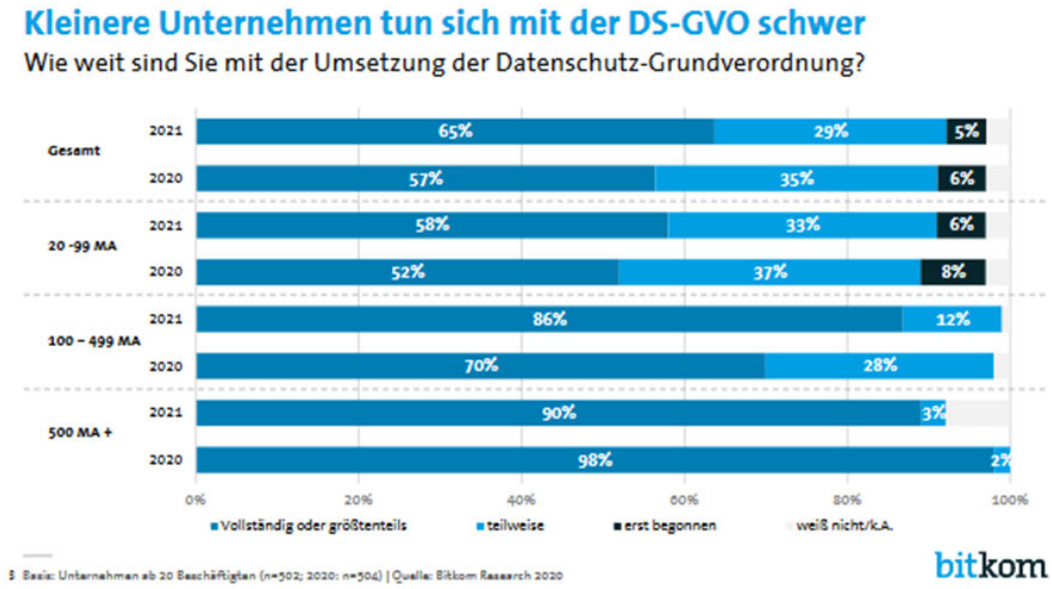

Abbildung 3: Umsetzungsfortschritte von Unternehmen (Dehmel, 2021, S. 3)

Durch diese Umfrage lässt sich erkennen, dass der Aufwand durch die Implementierung problematischer wird, je kleiner ein Unternehmen ist. Dies legt zumindest die Korrelation zwischen Unternehmensgröße und Möglichkeit, die DSGVO umzusetzen, nahe. Besonders bedeutend ist ebenfalls, dass für viele Unternehmen eine komplette Umsetzung unmöglich erscheint. Möglich wäre, dass das zuvor genannte Hindernis der Rechtsunsicherheit hier einen wichtigen Faktor darstellt und/oder die ebenfalls genannte kontinuierliche Anpassung einer vollständigen Implementierung im Wege steht.

In Zusammenhang mit den bisher genannten Aspekten ergeben sich auch einige Forderungen durch die Unternehmen an die Bundesregierung (Abbildung 4). Laut Bitkom verlangen dabei 89% der befragten Unternehmen eine Anpassung der DSGVO, auch wenn keine spezifischen Details genannt werden, wie diese auszusehen hätten. Interessant ist auch die Forderung mit der zweitgrößten Unterstützung (68% der Unternehmen), nämlich eine stärkere Vereinheitlichung der Vorgaben auf europäischer Ebene (Streim & Weiß, 2021).

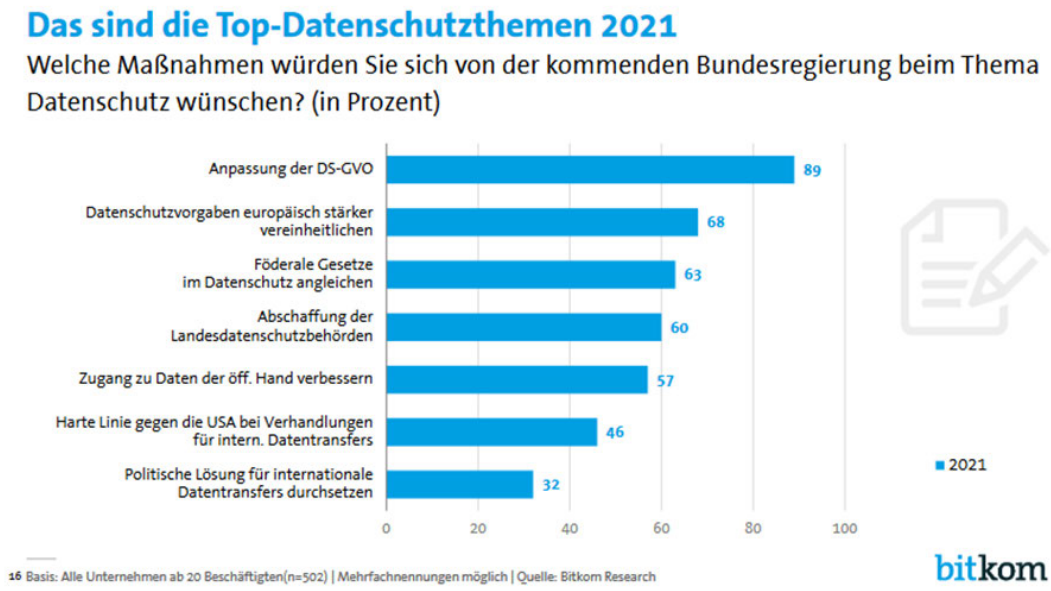

Abbildung 4: Forderungen von Unternehmen bzgl. Datenschutz (Dehmel, 2021, S. 16)

Die Aktualität dieser Daten unterstreicht den Eindruck, dass die DSGVO eine bedeutende Rolle für den Datenschutz spielt, die allerdings aus Sicht nahezu aller Unternehmen

verbesserungswürdig ist. Entscheidend ist auch, welche Bedeutung diese Ergebnisse in Bezug auf das Risikomanagements haben.

3.4.2 Implikationen aus den Umfragen für das Risikomanagement

Aus den gesammelten Ergebnissen lässt sich einiges ableiten, was für diese Arbeit relevant ist. Wie aus diesem kurzen Einblick in die Perspektive der Unternehmen hervorgeht, wird die DSGVO als große Herausforderung betrachtet, wobei von einem Ende der genannten Probleme in Anbetracht der letzten Umfragen vorerst nicht zu rechnen ist. Insbesondere dadurch, dass Unsicherheit bezüglich der DSGVO eher zu- als abgenommen hat, wird ein Bedarf an Hilfestellungen bezüglich der Umsetzung in Unternehmen deutlich. Unterstützt wird diese Annahme durch die hohe Unzufriedenheit bezüglich der Unterstützung durch die Aufsichtsbehörden. Ebenfalls zu nennen ist der zusätzliche Aufwand für die Unternehmen, der mit der Zeit womöglich in vielen Fällen eher zu- als abnehmen wird. Da auch ein Mangel an geeignetem Personal eine Rolle für die fehlende Umsetzung spielt, wird das Problem vieler Unternehmen, die Anforderungen erfüllen zu können, deutlich. Die hohen Anforderungen an Datenschutzbeauftragte nach Artikel 37 liefern einen Indikator dafür, dass entsprechende Stellen auch nur von hochqualifiziertem Personal besetzt werden kann, welches womöglich für viele Unternehmen nicht in ausreichender Anzahl verfügbar ist.

Insgesamt implizieren die Umfrageergebnisse, dass es noch Optimierungsbedarf bezüglich des Risikomanagements gibt. Vor allem die gravierende Rechtsunsicherheit macht dies deutlich, denn solange Unklarheit herrscht, an welche exakten Vorgaben man sich zu halten hat, kann nicht feststehen, wie dies genau geschehen soll. Auch muss angenommen werden, dass der zusätzliche Aufwand, von dem in der Umfrage die Rede ist, zumindest teilweise beim Risikomanagement entsteht, da mit der DSGVO ein bedeutender zusätzlicher Faktor berücksichtigt werden muss.

Mit der genannten Unsicherheit geht offensichtlich auch eine gewisse Unzufriedenheit einher, was die Forderungen nach einer Anpassung der DSGVO und einer stärkeren Vereinheitlichung der Vorgaben auf europäischer Ebene zeigt. Aus den Veröffentlichungen des Bitkom geht allerdings nicht hervor, welche Vorgaben nach Ansicht der Unternehmen vereinheitlicht werden

sollten. Einer der wesentlichen Punkte der DSGVO, bei denen die Mitgliedsstaaten der EU einen gewissen Spielraum bei der Umsetzung haben, ist, wie bereits zuvor erwähnt, Artikel 83, der die Verhängung von Bußgeldern behandelt. Auch wenn aus der Umfrage des Bitkom keine Klarheit darüber herrscht, ob der Wunsch nach einer Vereinheitlichung der Vorgaben auf europäischer Ebene sich direkt auf die landesspezifischen Implementierungen bestimmter Aspekte der DSGVO, so könnte Artikel 83 ein entscheidender Faktor sein. Immerhin kann eine unterschiedliche Anwendung von Bußgeldern in den jeweiligen Mitgliedsstaaten bedeuten, dass die Konsequenzen von Missachtung des Datenschutzes sehr unterschiedlich ausfallen können. Ein Beispiel hierfür ist der zuvor behandelte Fall des Berliner Kammergerichts, da in Deutschland Behörden von Bußgeldzahlungen nicht betroffen sind und dies auf einer landesspezifischen Umsetzung von Artikel 83 beruht. Bereits zuvor wurde betont, dass finanzielle Einbußen eine gewichtige Rolle beim Risikomanagement spielen können. Sollte sich also zeigen, dass die Konsequenzen bei Verstößen auf lange Sicht tatsächlich in den jeweiligen Ländern deutlich unterschiedlich ausfallen würden, so müsste das Risikomanagement in Bezug auf die DSGVO dementsprechend landesspezifisch angepasst werden.

Besorgniserregend ist jedoch auch die Ansicht vieler Unternehmen, dass die DSGVO nicht vollständig für sie umsetzbar sei. Dies offenbart tiefgreifende Probleme, die möglichst direkt behandelt werden müssten. Das hohe Maß an Unzufriedenheit mit der unzureichenden Unterstützung durch die Aufsichtsbehörden impliziert auch hier, dass diese Probleme kurzfristig nicht mit öffentlicher Hilfe gelöst werden können. Solange die DSGVO von vielen Unternehmen nicht umgesetzt werden kann, muss also auch davon ausgegangen werden, dass das Risikomanagement bezüglich des Datenschutzes in diesen Unternehmen stark eingeschränkt ist.

3.5 Kapitelzusammenfassung

Bezüglich der Rolle der DSGVO wurden in diesem Kapitel einige wesentliche Feststellungen gemacht. Zum einen wurde an einigen Beispielen aufgezeigt, wie sich mehrere Artikel der DSGVO direkt mit den behandelten Schutzzielen in Verbindung setzen lassen, zum anderen wurde deutlich, dass auch weitere Inhalte relevant für das Risikomanagement sind. Ein wesentlicher Faktor sind hierbei die Anforderungen an datenschutzfreundliche Voreinstellungen in

technischer und organisatorischer Hinsicht. Insbesondere weil hier keine expliziten Vorgaben für entsprechende Maßnahmen und Technologien gemacht werden, bedeutet dies eine umso größere Verantwortung für Unternehmen, diese selbst festzulegen und damit die Wahrscheinlichkeiten von Verstößen gegen die DSGVO zu verringern.

Von zentraler Bedeutung sind auch die möglichen Schäden in Form der erwähnten Bußgelder nach Artikel 83. Jedoch lässt sich selbst mithilfe des Konzeptes für Bußgeldzumessung in Deutschland für Unternehmen nicht präzise abschätzen, welche Sanktionen ihnen bei Fehlverhalten drohen. Wichtig ist allerdings, dass eigenes Verhalten die Höhe des Bußgeldes und damit die Schadenshöhe entscheidend beeinflussen kann. Dies bedeutet also, dass auch wenn alle präventiven Maßnahmen fehlgeschlagen sind, entsprechendes Verhalten wie die Einhaltung der Meldepflicht womöglich strafmildernd ausgelegt werden kann, weshalb auch dies beim Risikomanagement berücksichtigt werden sollte.

Zusätzlich wurde die DSGVO als große Herausforderung für Unternehmen identifiziert, die laut Umfragen des Bitkom für manche dieser Unternehmen nur schwer oder gar nicht vollständig umsetzbar ist. Da bereits die Notwendigkeit, gesetzliche Vorgaben zu berücksichtigen etabliert wurde, impliziert dies gravierende Schwierigkeiten beim Risikomanagement.

Insgesamt wurde vor allem konkretisiert, welche Einflüsse die DSGVO auf das Risikomanagement haben kann. Auf den ersten Blick verstärkt dies den Eindruck eines einseitigen Abhängigkeitsverhältnisses vom Risikomanagement zur DSGVO. Jedoch muss auch die (fehlende) Umsetzung der Unternehmen berücksichtigt werden. Denn solange es von Unternehmen zu keiner vollständigen Umsetzung der DSGVO kommt, sei es aus Personalmangel, Rechtsunsicherheit oder anderen Gründen, kann ihre Zielsetzung in Bezug auf Datenschutz nicht gewährleistet werden. Da eine vollständige Umsetzung allerdings auf Risikomanagement beruht, wird auf diese Weise auch die Abhängigkeit der DSGVO vom Risikomanagement zumindest mit Bezug auf Unternehmen deutlich.

Im folgenden Kapitel werden nun einige Angriffe vorgestellt. Im Vordergrund soll dabei stehen, wie diese eine Gefahr für die behandelten Schutzziele darstellen. Anschließend werden einige Szenarien behandelt, die sich auf diese Angriffe und ihre Verbindung zur DSGVO beziehen. Zudem werden grundlegende Ansätze erörtert, wie mit derartigen Angriffen umgegangen werden kann.

4 Ableitungen für das Risikomanagement

In diesem Kapitel sollen die in den vorherigen Kapiteln gesammelten Informationen miteinander verknüpft und auf Beispielszenarien, die mit Verstößen gegen die DSGVO zu tun haben, angewendet werden. Dabei gilt es festzustellen, mit was für Angriffen Unternehmen konfrontiert werden können, welchen Bezug dies zur DSGVO und den behandelten Schutzzielen haben kann und wie diesen Angriffen beim Risikomanagement begegnet werden kann. Auf diese Weise soll die Rolle der DSGVO in konkreten Situationen sowie welche Herausforderungen und Grenzen diesbezüglich erkennbar sind, ermittelt werden.

Die Darstellung von Angriffen in den jeweiligen Szenarien dient dabei in erster Linie der Veranschaulichung. Aufgrund der Beschränkungen für eine solche Arbeit werden nur grundlegende Lösungsansätze und ihre wesentlichen Aspekte dargelegt. Auf einen Leitfaden für die Implementierung wird an dieser Stelle dementsprechend verzichtet, da die konkreten Umstände einer Implementierung auch immer kontextabhängig sind. Zunächst werden jedoch einige grundlegende Aspekte von Angriffen behandelt.

4.1 Grundlegendes zu Angriffen

Bisher wurden Angriffe vor allem als Quelle von Risiken behandelt, ohne näher auf sie einzugehen. An dieser Stelle soll ein grundlegender Überblick über Angriffe im Allgemeinen geschaffen werden, um die Komplexität über dieses Thema zu verdeutlichen.

Das Open Web Application Security Project (OWASP) erwähnt beispielsweise in ihren Top Ten unter anderem auch explizit Schwachstellen gegenüber spezifischen Angriffsformen. In der aktuellen Version aus dem Jahr 2021 wird dabei zur Version aus dem Jahre 2017 deutlich, dass innerhalb weniger Jahre gravierende Veränderungen stattgefunden haben und nahezu alle Ränge anders besetzt sind. So wird erkennbar, wie bestimmte Angriffsformen an Bedeutung gewinnen, wie Server-Side Request Forgery (SSRF) oder verlieren (OWASP, 2021a). Auch ohne hier tiefer ins Detail zu gehen, wird ersichtlich, dass es bei Angriffen auch innerhalb

weniger Jahre zu bedeutsamen Veränderungen kommen kann und nicht mit Stagnation zu rechnen ist.

Deutlicher wird dies noch in einem aktuellen Lagebericht über die IT-Sicherheit in Deutschland des Bundesamtes für Sicherheit und Informationstechnik. Hier ist unter anderem festgehalten, dass im letzten Berichtszeitraum, durchschnittlich 394.000 neue Schadprogramm-Varianten pro Tag bekannt wurden, was einen Anstieg von ca. 22 Prozent zum vorherigen Zeitraum bedeutete. In diesem Zusammenhang wurde ebenfalls berichtet, dass auch die Opfer von Angriffen mit derartigen Schadprogrammen Verstöße gegen die DSGVO begehen würden, wenn sie ihrer Meldepflicht nicht nachkämen, was wiederum zu Ordnungsstrafen durch die Behörden oder Erpressungen durch die Angreifer führen könnte (BSI, 2021, S. 9-14). Dies verdeutlicht zum einen die Bedeutung von Artikel 33 für Unternehmen und zum anderen die wachsende Anzahl von Angriffen mit Schadprogrammen.

Unter den verschiedenen Angriffsvarianten finden sich auch Sonderfälle, deren individuelle Betrachtung an dieser Stelle nicht möglich ist, da für sie in der Regel eine besondere kontextabhängige Auseinandersetzung mit der DSGVO notwendig wäre. Ein Beispiel hierfür stellen sogenannte Zero Day Exploits dar. Hierbei handelt es sich um Code mit dessen Hilfe Sicherheitslücken ausgenutzt werden, bevor Hersteller darauf reagieren können (Fox, 2009). Angesichts der großen Anzahl von Angriffen wird also nicht auf alle verschiedenen Angriffe und deren Varianten eingegangen, weshalb in den folgenden Beispielfällen nur einige exemplarisch behandelt werden.

4.2 Erster Beispielfall - Ransomware

Als erstes Beispiel soll ein Szenario dienen, welches sich in wesentlichen Punkten an dem Vorfall beim Berliner Kammergericht orientiert. Dadurch, dass im Untersuchungsbericht die tatsächliche Ursache nicht restlos geklärt werden konnte (T-SYSTEMS, 2019, S. 10), wird es hierbei nicht darum gehen, die genauen Ereignisse zu rekapitulieren bzw. reproduzieren, sondern potenzielle Abläufe darzustellen und zu analysieren, welche Schwachpunkte ermittelt werden können bzw. wie mit diesen umgegangen werden kann.

4.2.1 Szenario

Für diesen Fall wird ein vereinfachtes Modell für das System verwendet, welches aus Benutzerschnittstelle, Applikationsschicht und Datenhaltungssystem besteht und sich damit an der 3-Schichten Architektur orientiert.

Im Kontext (personenbezogener) Daten ist selbstverständlich das Datenhaltungssystem als Angriffsziel von enormer Bedeutung. Hierbei gibt es eine Vielzahl von Möglichkeiten, wie es bedroht werden kann. Beispielsweise könnten durch einen Angriff mit Ransomware, wichtige Daten unbrauchbar gemacht werden. In dem Bericht des Kriminologischen Forschungsinstituts Niedersachsen (KFN) werden Ransomware-Angriffe als Einsätze von Schadsoftware bezeichnet, mit welchen Daten auf infizierten Systemen verschlüsselt werden. Die Angreifer verlangen für die Aufhebung der Verschlüsselung dann in der Regel ein Lösegeld. Laut Bericht war ca. ein Achtel der Unternehmen innerhalb der letzten zwölf Monate vor Durchführung der Umfrage Opfer eines solchen Angriffes geworden (Dreißigacker et al., 2020, S. 99 & 107).

Besonders bei den Nutzerschnittstellen besteht das Risiko, dass Angriffe ermöglicht werden, die das System von innen bedrohen. Einige Möglichkeiten wurden dabei bereits im Bericht über den Fall des Berliner Kammergerichts genannt. Zum einen wäre da der Angriff über einen fremden Datenträger mit schädlichem Inhalt und zum anderen als Anhang an eine E-Mail, welche über eine Webmailseite geöffnet wurde. In beiden Fällen hätte sich eine Infektion über den Fileserver ausbreiten können (T-SYSTEMS, 2019, S. 10-11). Es gilt zu beachten, dass in solchen Fällen, der erfolgreiche Angriff von der (unfreiwilligen) Mitarbeit der Benutzer eines Systems abhängig wäre. Dementsprechend ist der Schutz vor derartigen Attacken vom Risikobewusstsein der jeweiligen User abhängig.

Vereinfacht lässt sich dies in einem simplen Use Case Diagramm darstellen.

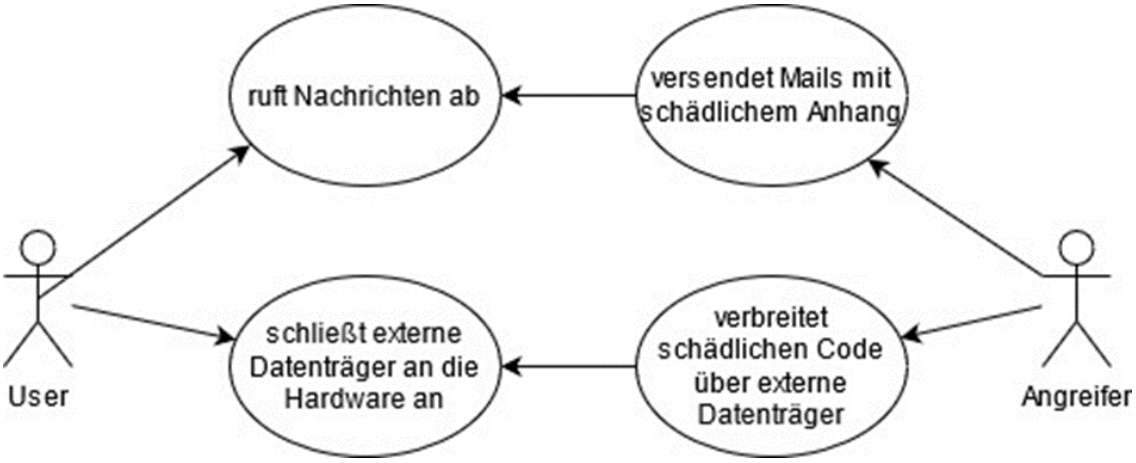

Abbildung 5: Use Case Szenario 1

Wie in dieser Darstellung deutlich wird, geht es hier primär um zwei Akteure, deren Aktionen miteinander zusammenhängen. Ganz konkret geht es dabei um die zwei genannten Fälle: 1. Ein User ruft Nachrichten ab, bei denen es sich um Mails mit schädlichem Anhang eines Angreifers handeln kann. 2. Ein User schließt einen fremden Datenträger, welcher womöglich schädlichen Code eines Angreifers enthält, an die IT-Infrastruktur an.

4.2.2 Analyse

Anders als bei einem Hackerangriff, der allein von außen erfolgt, ist bei den beiden oben genannten Bedrohungen das Zusammenspiel zwischen Angreifer und User entscheidend. Dementsprechend können etwaige Abwehrmaßnahmen für derartige Fälle sich darauf konzentrieren, dieses Zusammenspiel zu vermeiden, indem der User nicht den Erwartungen des Angreifers entsprechend handelt. Allerdings lässt sich daraus auch ableiten, dass menschliches Versagen ein enormes Gefahrenpotenzial bietet, dass auf unterschiedlichen Wegen systembedrohend sein kann.

Dabei ist es nicht immer möglich, zu unterscheiden, ob es sich bei diesem Versagen um unbewusste Fehler handelt, die beispielsweise auf Unwissen gegenüber möglichen Angriffen beruhen oder um mehr oder weniger bewusst eingegangene Risiken handelt. Im Falle eines fremden

Datenträgers, der an ein System angeschlossen wurde und der auf diese Weise Schaden anrichten konnte, ist beispielsweise beides möglich. Ungeschultes Personal könnte entweder vollkommen naiv gegenüber den Gefahren sein, aber auch das Risiko zu gering einschätzen und den Datenträger aus Neugier trotzdem öffnen. Generell gilt es derartige Fehlerquellen bestmöglich zu behandeln. Ganz konkret sollten grundsätzliche Aspekte bei Mitarbeiterschulungen, die möglichst das gesamte Personal betreffen, vermittelt werden. Jedoch ist dies kein Ersatz für geschultes Fachpersonal, welches für die allgemeine Sicherheit und/oder den Datenschutz verantwortlich ist, wie beispielsweise ein entsprechend qualifizierter Datenschutzbeauftragter, wie er in Artikel 37 beschrieben wird. Zudem muss bedacht werden, dass solange es sich um ein vermeidbares Risiko handelt, die konkrete Ursache für einen Fehler zwar nicht irrelevant ist, der entstandene Schaden jedoch von weitaus größerer Bedeutung ist. Sollte es allerdings im Anschluss an einen Angriff festgestellt werden, dass es dabei auch intern datenschutzrechtliche Verstöße gegeben hat, muss mit weiteren Konsequenzen gerechnet werden.

Einen weiteren entscheidenden Aspekt zur Bekämpfung von Angriffen, der hier zum Tragen kommt, nämlich Monitoring wird auch von Claudia Eckert genannt. Hierbei handelt es sich um die Überwachung der eigenen Ressourcen, um mögliche Angriffsfälle durch Eingriffe zu verhindern (Eckert, 2018, S. 20). Auch in den OWASP Top 10 wird mangelhaftes Monitoring, auch mit Verweis auf eine hohe Dauer bis etwaige Gefahren erkannt wurden und die dementsprechende zu langsame Reaktion, um den Angriff abzuwehren, erwähnt (OWASP, 2021b). Eine wichtige Herausforderung ist hierbei allerdings, auf der einen Seite die Sicherheit der eigenen Ressourcen zu gewährleisten, während gleichzeitig der Datenschutz bezüglich der gespeicherten Daten, aber auch die der Nutzer eines Systems gewahrt wird.

Der Bezug zur den verletzten Schutzzielen ist abhängig von der Art des Angriffes. Bei einer Verwendung von Ransomware, welche die Daten auf dem System verschlüsselt, ist eindeutig die Datenintegrität durch die Manipulation von Daten betroffen. Jedoch ist auch eine Einschränkung der Verfügbarkeit zu nennen, da die manipulierten Daten zumindest vorerst nicht zur autorisierten Nutzung zur Verfügung stünden. Wie im vorherigen Kapitel dargelegt wurde, sind diese Schutzziele vor allem durch ihre explizite Erwähnung in Artikel 32 durch die DSGVO abgedeckt. In diesem und Artikel 25 finden sich zudem die Aufforderungen, Maßnahmen zum Schutz von Daten einzuleiten, sowohl auf technischer als auch organisatorischer

Ebene (Artikel 25 Absatz 1 & 2, Artikel 32 Absatz 1 DSGVO). Gerade die organisatorischen Mittel sind insbesondere in einem Fall, in dem unbekannte Datenträger an ein System angeschlossen wurden, nicht gegeben.

4.2.3 Grundlegende Lösungsansätze

Die wichtigsten Stichpunkte, aus denen sich Gegenmaßnahmen für derartige Angriffe ableiten lassen, wurden bereits zuvor genannt. Zunächst sind hier grundlegende Mitarbeiterschulungen zu nennen, damit vermeidbare Fehler, wie das Verwenden von fremden Datenträgern, die womöglich schädliche Dateien enthalten und dementsprechend niemals an die IT-Infrastruktur angeschlossen werden sollten, solange es keine vollständige Klarheit über die Inhalte gibt. Noch wichtiger ist allerdings konsequentes Monitoring. Diesem muss vor allem deshalb eine zentrale Rolle zukommen, weil es nicht nur die Überwachung der eigenen Ressourcen ermöglicht, sondern auch im Verdachtsfall Eingriffe ermöglicht. Mit Bezug auf das zuvor verwendete Use Case Diagramm lässt sich dafür eine leichte Ergänzung vornehmen, die allerdings genauer erläutert werden sollte, um Missverständnisse zu vermeiden.

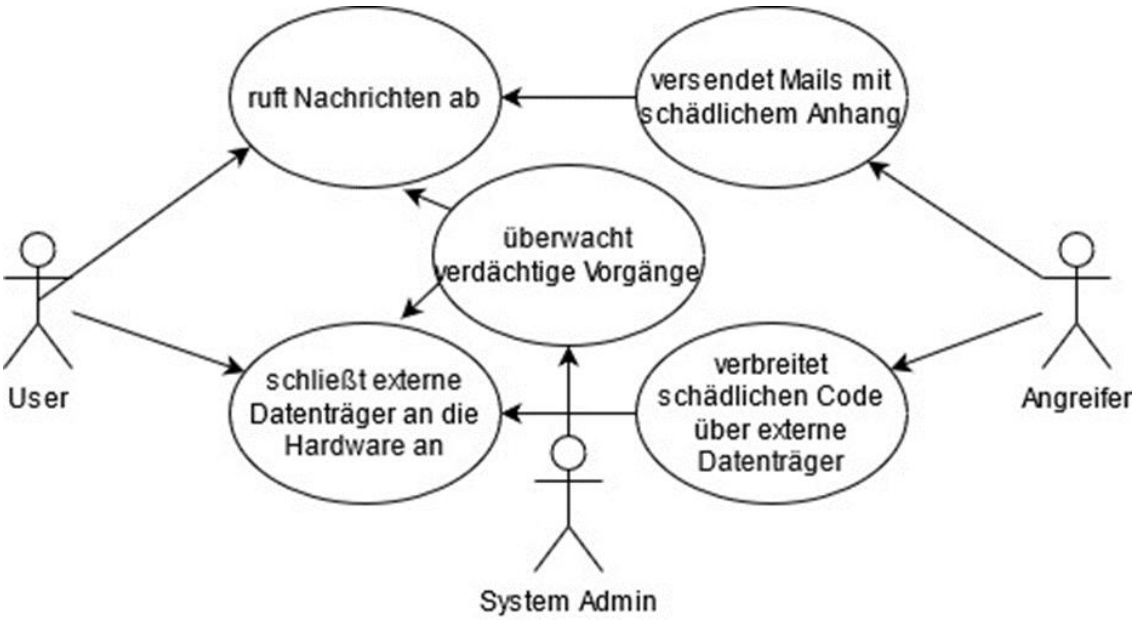

Abbildung 6: Use Case Szenario 1 unter Berücksichtigung von Monitoring

Wie sich erkennen lässt, wird das Monitoring durch einen System Administrator durchgeführt, der explizit verdächtige Vorgänge überwacht, um im Bedarfsfall eingreifen zu können. Hierbei muss allerdings festgehalten werden, dass es gewisse Grenzen gibt, die eingehalten werden müssen. So kann Monitoring nur dann stattfinden, wenn dabei die Datenschutzrechte der betroffenen User gewahrt werden, was in derartigen Fällen beispielsweise beim Zugriff auf Nachrichten zutreffen kann. Falls ein Angriff jedoch bereits erfolgreich war, sollte er zumindest gemeldet werden, um wenigstens Artikel 33 der DSGVO zu erfüllen.

4.3 Zweiter Beispielfall – Phishing

Wie im ersten Beispiel bereits dargestellt, hängt die Gefahr eines Angriffes nicht immer nur vom Angreifer selbst, sondern oftmals auch von den Personen innerhalb eines Systems und deren Verhalten ab. Der nächste Beispielfall konzentriert sich deshalb auf ein Phänomen, mit dem viele Menschen beruflich oder privat schon einmal in Kontakt gekommen sein dürften: Es handelt sich hierbei um das sogenannte „Phishing“.

Bei Phishing-Angriffen wird gezielt versucht, an Zugangsdaten von Personen zu gelangen um diese dann anschließend selbst verwenden zu können. Im Gegensatz zu Angriffen, bei denen sich Angreifer durch Hacking direkt selbst unbefugten Zugang zu einem System verschaffen, werden hierbei beispielsweise Mails oder gefälschte Webseiten eingesetzt, um User zur Angabe ihrer Zugangsdaten zu verleiten (Eckert, 2018, S. 22-23 & 26).

Auch wenn viele Angriffe dieser Art schnell erkannt werden können, darf die Gefahr, die von Phishing ausgeht, nicht unterschätzt werden, da bereits ein einzelner erfolgreicher Angriff weitreichende Konsequenzen haben kann. Aus einer Befragung des KFN geht hervor, dass Phishing eine der häufigsten Angriffsarten war, denen Unternehmen innerhalb der letzten zwölf Monate vor Durchführung der Umfrage zum Opfer gefallen waren. Insgesamt waren dabei über ein Fünftel der 4.981 befragten Unternehmen von mindestens einem solchen Angriff in diesem Zeitraum betroffen gewesen (Dreißigacker et al., 2020, S. 99-101 & 107).

Besondere Gefahr durch Phishing-Angriffe ist auch für personenbezogene Daten gegeben, wenn sich Außenstehende auf diese Weise Zugangsdaten verschaffen können, welche ihnen

den Zugriff auf beispielsweise Kundendaten, Patientenakten oder ähnliche Informationen ermöglichen.

4.3.1 Szenario

Auch für diesen Fall reicht ein vereinfachtes Modell eines Systems basierend auf dem Client-Server-Modell, welches also aus einem zentralen Server und mehreren Clients besteht. Ein User kann dabei über einen Client mithilfe individueller Zugangsdaten auf den Server zugreifen und auf diese Weise Daten abrufen.

Ein Angreifer mit dem Ziel, ebenfalls Zugriff auf die geschützten Daten auf dem Server zu erhalten, könnte nun versuchen, sich die Zugangsdaten eines Users zu verschaffen, um dieses Ziel zu erreichen.

Zu diesem Zweck könnten mehrere Varianten von Phishing-Angriffen genutzt werden, wie beispielsweise Mails, in denen Personen mithilfe eines Links zu einer gefälschten Version des Anmeldeformulars für den Server weitergeleitet würden. Ein User, welcher hierdurch erfolgreich getäuscht wurde, könnte nun seine persönlichen Zugangsdaten angeben, welche auf diese Weise in die Hände des Angreifers gelangen würden. Anschließend könnte der Angreifer die Zugangsdaten selbst verwenden, um Zugriff auf den Server und somit die geschützten Daten zu erhalten.

4.3.2 Analyse

In diesem Fallbeispiel ist erneut das Zusammenspiel zwischen Angreifer und User entscheidend für den Erfolg des Angriffs. Wichtig sind hierbei zwei wesentliche Faktoren. Erstens hängt dieser Erfolg von der Überzeugungskraft der verwendeten Täuschung ab, wobei der Angriff trotzdem von der unfreiwilligen Kooperation des Opfers abhängig ist. Diese Kooperation bildet den zweiten Faktor und auch derjenige, den man im Risikomanagement eher beeinflussen kann. Dazu müsste die gezielte Abwehr solcher Angriffe unter anderem darin bestehen, dass das Personal nicht von derartigen Betrugsversuchen getäuscht wird. Bedacht werden sollte

vor allem auch, dass die Gefahr nicht von einem einzelnen, sondern wahrscheinlich von mehreren Angriffen ausgehen kann, von denen bereits ein einzelner Erfolg dem Angreifer ermöglicht, sein Ziel zu erreichen.

Mit Bezug zu den Schutzzielen muss an dieser Stelle erwähnt werden, dass Authentizität zwar theoretisch erfüllt ist, da Identitäten überprüft werden können, dies aber dennoch nicht verhindern könnte, dass die betreffenden personenbezogenen Daten in die Hände von unbefugten Personen gelangen oder von diesen verändert werden können, sollten diese sich der Zugangsdaten von autorisierten Usern bemächtigen. Auf diese Weise wäre zumindest das Ziel der Informationsvertraulichkeit verletzt, da die Rechte nicht von den Personen ausgeübt wurden, für die sie vorgesehen waren. Relevant ist daher auch das Schutzziel der Verbindlichkeit, da die Aktionen des Angreifers nicht transparent zugeordnet werden könnten. Im Falle einer Datenmanipulation wäre zudem auch die Datenintegrität betroffen. Davon abhängig, ob die personenbezogenen Daten, auf die der Angreifer Zugriff erhalten würde, zumindest anonymisiert oder pseudonymisiert wurden, wäre auch das diesbezügliche Schutzziel betroffen. Damit muss unterschieden werden zwischen der unerlaubten Einsicht in Daten und der Möglichkeit, diese zuordnen zu können, da davon unterschiedliche Schutzziele abhängen. Die Verbindungen zur DSGVO sind ähnlich wie im vorherigen Fall, insbesondere was Artikel 25 und 32 betrifft. Zusätzlich muss hier jedoch die Hervorhebung von Pseudonymisierung als ausdrücklich genannte Maßnahme zur datenschutzfreundlichen Voreinstellung betont werden (Artikel 25 Absatz 1 DSGVO). Daraus kann geschlossen werden, dass bei einem erfolgreichen Angriff mit Zugriff auf personenbezogene Daten zumindest dann ein Verstoß eines Unternehmens gegen die DSGVO vorliegen würde, wenn keine Maßnahmen getroffen wären, die die Zuordnung von Daten mit Personen verhindern könnten. Bezüglich der Verbindlichkeit wäre die DSGVO betroffen, da nicht gewährleistet werden könnte gemäß Artikel 15, die Betroffenen darüber informieren zu können, ob und für welche Zwecke deren Informationen verarbeitet wurden und wem ihre Daten offengelegt wurden (Artikel 15 Absatz 1 a) & c) DSGVO).

4.3.3 Grundlegende Lösungsansätze

Zu Versuchen, Phishing-Angriffe zu unterbinden würde bedeuten, Angreifer davon abhalten zu wollen z.B. gefälschte Webseiten zu erstellen, Mails zu versenden, die zu diesen Seiten führen etc., was unmöglich sein dürfte. Um den Gefahren von Phishing zu begegnen, ist es daher notwendig, sich auf die Maßnahmen zu konzentrieren, die intern durchgeführt werden können, um diese Angriffe abzuwehren. Um Phishing entgegenzuwirken ist also eine gewisse Grundkompetenz für den Umgang mit sensiblen Informationen notwendig, die von allen Usern verinnerlicht wurde. Um dies zu erreichen, bieten sich wie auch bereits im vorherigen Fall erwähnt, grundlegende Mitarbeiterschulungen an, in denen dem das Personal Kenntnisse über die Gefahren solcher Angriffe und wie diese vermieden werden können, vermittelt werden. Bei den Maßnahmen gegen Phishing sollte außerdem bedacht werden, dass es sich nicht um eine gleichbleibende Bedrohung handelt, sondern dass stets neue Angriffsvarianten entwickelt werden können. Sollten neue Bedrohungen dieser Art bekannt werden, muss dementsprechend über sie aufgeklärt werden. Da sich aus der DSGVO gemäß Artikel 25 auch eine Verantwortung ergibt, Unbefugten einen solchen Zugriff nicht zu ermöglichen und dafür die geeigneten Maßnahmen zu treffen, ist es wichtig festzuhalten, dass eigenes Fehlverhalten auch hier weitreichende Auswirkungen auf den Datenschutz zur Folge hat.

Präventivmaßnahmen allein sind allerdings nicht ausreichend. Sollte trotz aller Vorsicht ein Angriff erfolgreich sein, gilt es schnellstmöglich zu handeln, um eventuelle Schäden möglichst gering zu halten. Angestellte müssen daher unverzüglich die jeweiligen Verantwortlichen wie z.B. Datenschutzbeauftragte informieren, falls sie Opfer von Phishing wurden. Eine schnelle Reaktion kann dazu führen, dass entsprechende Nutzerkonten, auf die der Angreifer Zugriff hat, gesperrt werden und der Schaden möglichst gering ausfällt. Ebenso sollten die Daten wie in der Analyse des Szenarios besprochen möglichst anonymisiert oder pseudonymisiert werden. Zusätzlich müssen die Verantwortlichen die zuständigen Behörden informieren, um ihre Meldepflicht gemäß Artikel 33 der DSGVO zu wahren.

4.4 Dritter Beispielfall - Spyware

Im vorherigen Fall wurde bereits erläutert, dass der Diebstahl von Passwörtern und Zugangsdaten generell verheerende Folgen für den Datenschutz hat. Neben Phishing gibt es allerdings noch andere Möglichkeiten, wie derartige Informationen in falsche Hände geraten können.

Eine dieser Möglichkeiten nennt sich Spyware. Dabei handelt es sich um Programme, die für die Angreifer in Systemen oder einzelnen Rechnern beispielsweise Zugangsdaten, Informationen über Aktivitäten oder vertrauliche Daten, bei denen es sich selbstverständlich auch um personenbezogene Daten handeln kann, sammelt. Welche Gefahr genau von einer Spyware ausgeht, hängt also von ihrer spezifischen Funktion ab. In diesem Fall soll sich daher mit der Gefahr, die von Spyware ausgeht, auseinandergesetzt werden und wie dies den Datenschutz betrifft. Spyware kann auf unterschiedliche Weise in ein System eingeschleust werden. Denkbar wären beispielsweise Situationen wie im ersten Fallbeispiel, bei dem das schädliche Programm über einen fremden Datenträger oder den Anhang einer Mail eingeschleust wurde. Ebenfalls möglich wäre, dass Spyware bei der Installation einer anderen Software auf ein einen Rechner gelangt und anschließend mit der Sammlung von Daten beginnt (Eckert, 2018, S. 24-25, & Dreißigacker et al., 2020, S. 99-101 & 107).

Um Redundanzen mit dem ersten Beispielfall jedoch zu vermeiden, wird sich hierbei primär darauf konzentriert, welche Probleme Spyware verursachen kann, wenn sie bereits erfolgreich eingeschleust wurde.

4.4.1 Szenario

Gegeben sei erneut ein einfaches Modell basierend auf der 3-Schichten-Architektur wie bei 4.1.1. Sollte es einem Angreifer gelingen Spyware auf dem Rechner eines Users zu platzieren, könnte diese durch Überwachung von Login-Prozessen die Zugangsdaten dieses Users aufzeichnen, welche den Zugriff auf die Datenbank ermöglichen. Diese Zugangsdaten könnten dann an den Angreifer weitergeleitet werden, welcher auf diese Weise Zugriff auf die Datenbanken und damit auf die dort verfügbaren Daten erhält. Alternativ könnte Spyware wie

erwähnt auch dazu verwendet werden, um direkt personenbezogene Daten in einem System zu sammeln und diese an den Angreifer übermitteln.

4.4.2 Analyse

Ein wichtiger Aspekt dieses Falles ist, dass die Bedrohung durch Spyware direkte und indirekte Auswirkungen auf den Schutz personenbezogener Daten haben kann. Während der Diebstahl von Zugangsdaten eines Users zunächst nur die Möglichkeit schafft, dass bestimmte personenbezogene Daten in die Hände eines Angreifers gelangen, wäre das Sammeln von Daten auf einem Rechner oder in einem Netzwerk bereits eine direkte Bedrohung. In beiden Fällen besteht jedoch eine denkbar große Gefahr für den Datenschutz. Zusätzlich sollte bedacht werden, dass Spyware auf unterschiedliche Art und Weise auf einen Rechner bzw. in ein System gelangen kann. Was die Schutzziele angeht, können hier weitestgehend ähnliche Verletzungen wie im zweiten Beispielfall auftreten. Der wesentliche Unterschied ist jedoch, dass Daten auf zweierlei Weise gefährdet werden könnten. Falls ein Angreifer Spyware nutzen würde, um zunächst Zugangsdaten zu stehlen, um dann auf Datenbanken zuzugreifen, wären wie im vorherigen Fall womöglich Datenintegrität, Verbindlichkeit, Informationsvertraulichkeit, sowie Anonymisierung und Pseudonymisierung betroffen. Sollte die Spyware nur personenbezogene Daten weiterleiten, wären davon unmittelbar nur die drei letztgenannten Ziele betroffen. Da der Fall in der Art, wie die Schutzziele verletzt werden können, dem vorherigen ähnelt, sind auch die entsprechenden Verbindungen zur DSGVO bezüglich Artikel 15, 25 und 32 wieder gegeben. Es sollte beispielsweise bedacht werden, ob aufgrund der Vorgaben, die aus Artikel 25 resultieren, die Abwehr von Spyware aktuellen technischen Standards entsprechen.

4.4.3 Grundlegende Lösungsansätze

Wie bereits festgestellt wurde ist im Gegensatz zu den vorangegangenen Fällen der Angreifer nicht zwangsläufig von der unfreiwilligen Mitarbeit seiner Opfer abhängig. Dieser Faktor bedeutet einen signifikanten Unterschied, welcher beim Risikomanagement bedacht werden sollte. Dies bedeutet nicht, dass die bereits vorgestellten Sicherheitsvorkehrungen hier nicht

zum Tragen kommen sollten, da eine Involvierung menschlicher Fehler seitens des Personals ebenfalls zur Infiltration eines Systems führen kann, es ist jedoch nicht der einzige Faktor. Eine weitere Option wäre der flächendeckende Einsatz von technischen Maßnahmen, die in der Lage sein sollten, möglichst aktuelle Spywarevarianten zu entdecken. Zudem ist auch hier konsequentes Monitoring ratsam, insbesondere was die grundsätzliche Überwachung von Zugriffen auf Datenbanken angeht. Sollte es beispielsweise zu außerplanmäßig vielen Zugriffen auf personenbezogene Daten kommen, könnte so entsprechend schnell reagiert werden und im Verdachtsfall weitere Schritte eingeleitet werden. Zu diesen Schritten wie z.B. Sperrung des infiltrierten Benutzerkontos muss allerdings auch die entsprechende Meldung gemäß Artikel 33 DSGVO folgen.

4.5 Vierter Beispielfall – Cross Site Scripting

Im abschließenden Beispiel soll es um Cross Site Scripting (XSS) gehen, was bereits in vergangenen Jahren einen eigenen Eintrag in den OWASP Top 10 hatte. Mittlerweile wird es dort als Teil von Injection aufgelistet und steht damit stellvertretend für eine Kategorie verschiedener Schwachstellen, die auf Platz drei der aktuellen OWASP Top 10 rangiert (OWASP, 2021a & OWASP, 2021c).

Grundsätzlich werden bei Cross Site Scripting eingegebene Daten eines Angreifers, die an einen Web-Server gesendet wurden, weder geprüft noch gefiltert und anschließend an die Web-Browser von anderen Usern gesendet, wo sie weiterverarbeitet werden. Hierdurch kann Scriptcode im Browser dieser User ausgeführt werden. Auf diese Weise können beispielsweise manipulierte Web-Seiten angezeigt werden, bei denen durch das Anklicken eines Links schädlicher Code ausgeführt wird. Ziel solcher Angriffe sind häufig nutzerspezifische Informationen, die der Identifizierung dienen, wie z.B. Cookies, auf die der Angreifer Zugriff erhält, nachdem der Schadcode erfolgreich ausgeführt wurde (Eckert, 2018, S. 164-168).

Im folgenden Szenario wird Cross Site Scripting anhand eines vereinfachten Beispiels dargestellt, das auf den obigen Informationen beruht. Hierbei wird auch der Zusammenhang mit personenbezogenen Daten und der DSGVO berücksichtigt.

4.5.1 Szenario

Für dieses Szenario ist ein Web-Server eines Unternehmens, ein User-Client und ein Angreifer gegeben. Der Angreifer übermittelt seinen schädlichen Code an den Web-Server. Von dort aus gelangt der Code an einen User, in dessen Browser er ausgeführt wird. Dies wiederum ermöglicht dem Angreifer Zugriff auf Cookies, die der Authentifizierung des Users dienen. Der Angreifer kann anschließend mithilfe jener Cookies sich gegenüber dem Server als der User ausgeben und dort dessen Rechte ausüben. Wichtig ist an dieser Stelle noch, dass der Angreifer, wenn er sich als ein bestimmter User ausgeben kann über dessen Rechte auf dessen persönliche Daten und womöglich an weitere personenbezogene Daten gelangen kann, die eigentlich vor fremdem Zugriff geschützt sein sollten.

Zur Veranschaulichung wird dies in einem einfachen Sequenzdiagramm dargestellt.

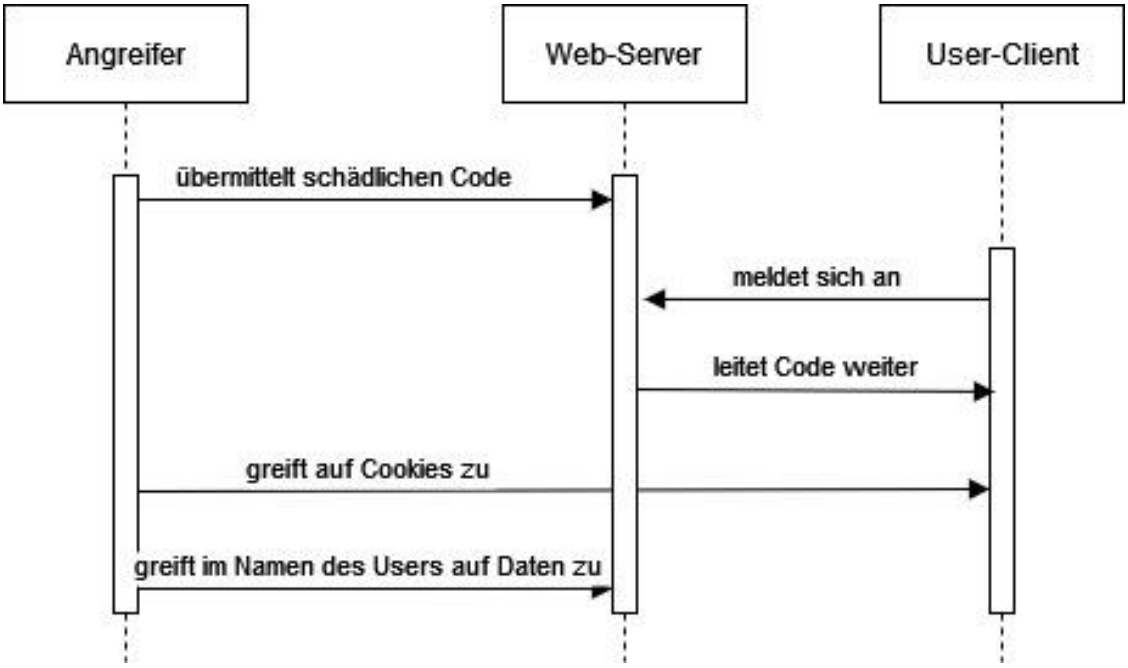

Abbildung 7: Sequenzdiagramm Szenario 4

An diesem Beispiel lässt sich erkennen, wie ein Angreifer einen Server verwendet, um von dort seinen Code zu verteilen. Der User-Client steht hier nur stellvertretend für eine beliebige Anzahl von Clients, die durch denselben XSS-Angriff betroffen sein können.

4.5.2 Analyse

Auch wenn hier erneut erkennbar ist, dass durch einen erfolgreichen Angriff personenbezogene Daten in die Hände von Unbefugten gelangen können, besteht doch ein wichtiger Unterschied zu den vorherigen Beispielen. Dieser besteht darin, dass ein Angreifer auf zweierlei Weise Zugriff zu personenbezogenen Daten erhalten kann. Sollte sich der Angreifer zum Beispiel mithilfe der Cookies als ein angemeldeter User auf dem Web-Server eines Unternehmens ausgeben können, so könnte er zum einen auf dessen persönliche Informationen im Nutzerprofil zugreifen, zum anderen aber möglicherweise auch auf Daten, welche auf den Datenbanken des Unternehmens gespeichert sind, falls dieser User die entsprechenden Berechtigungen dafür besitzt. Zudem muss bedacht werden, dass sowohl User innerhalb und außerhalb des Unternehmens von solchen Angriffen betroffen sein können, was den Umgang mit derartigen Angriffen erschweren könnte. Bei den Schutzzielen fällt vor allem auf, wie Informationsvertraulichkeit dadurch unterminiert wird, indem eine ursprünglich überprüfte Identität, die über Berechtigungen zur Einsicht bestimmter Daten verfügt, von einem Angreifer übernommen und missbraucht werden kann. Auch hier zeigt sich wieder, dass selbst wenn Authentizität theoretisch gegeben ist, gestohlene Identifikationsdaten dazu führen können, dass andere Schutzziele verletzt werden. Wie in vorangegangenen Fällen können anschließend auch wieder Datenintegrität, Verbindlichkeit sowie Anonymisierung und Pseudonymisierung verletzt werden. Im Kontext der DSGVO sind demnach auch erneut vor allem Artikel 15, 25 & 32 zu bedenken.

4.5.3 Grundlegende Lösungsansätze

Ein wichtiger Anteil der Abwehr von XSS-Angriffen ist mit der Entwicklung der betreffenden Web-Anwendungen verbunden. Dabei muss vor allem die Injektion mit schädlichem Code verhindert werden, indem bestimmte Zeichen aus einer Eingabe herausgefiltert werden können,

damit keinerlei bösartige Scripte übermittelt werden. Doch auch von Seiten der User können Maßnahmen getroffen werden. Dafür müsste die Ausführung von Skriptsprachen im Browser deaktiviert werden, damit entsprechende Skriptbefehlen aus dem schädlichen Code, der vom Server übermittelt wurde, nicht ausgeführt werden können (Eckert, 2018, S. 168).

Während der eine Teil also sich explizit auf die Programmierung konzentriert, hängt der andere wiederum mit den Usern und deren Bewusstsein für derartige Angriffe zusammen. User, die zum jeweiligen Unternehmen gehören, könnten noch entsprechend geschult werden, aber dies wäre nicht bei anderen Usern wie z.B. Kunden der Fall. Hier müsste davon ausgegangen werden, dass selbst entsprechende Warnungen vor XSS-Angriffen unbeachtet bleiben können. Entscheidend wäre also vor allem die Berücksichtigung von derartigen Angriffen bei der Programmierung, um die Sicherheit von personenbezogenen Daten und deren Verarbeitung gemäß Artikel 32 zu erfüllen.

Dennoch sollte auch hier der Fall bedacht werden, dass die präventiven Maßnahmen womöglich nicht ausreichend sind. Problematisch ist hierbei die Möglichkeit, dass ein Angreifer, der sich bereits als ein bestimmter User ausgeben konnte, unmittelbar danach Einsicht in vertrauliche Daten haben könnte. Eine Reaktion auf einen erfolgreichen Angriff ist dementsprechend schwierig. Sollte der Angreifer die Rechte eines Users für den Zugriff auf besonders große Datenmengen missbrauchen und versuchen, diese herunterzuladen, könnte womöglich der erhöhte Datenverkehr Verdacht erregen, aber auch wenn in solch einen spezifischen Fall noch eingegriffen werden könnte, so ist dies auch nur eine Ausnahme. Dieses Beispiel zeigt daher auch auf, dass manche Angriffe im Nachhinein schwer zu erkennen sind. Selbstverständlich muss auch hier die Meldepflicht gemäß Artikel 33 berücksichtigt werden, falls ein erfolgreicher Angriff bekannt werden sollte.

4.6 Kapitelzusammenfassung

In diesem Kapitel wurde behandelt, wie komplex Angriffe in Bezug auf die Verletzung von Schutzzielen, der DSGVO und Risikomanagement sein können. Auch wenn dabei Aspekte aus den Beispielfällen auf den ersten Blick redundant erscheinen mögen, lassen sich hieraus

wichtige Erkenntnisse gewinnen. Zum Beispiel wird deutlich, wie unterschiedliche Angriffe ähnliche Konsequenzen haben können, insbesondere was die verletzten Schutzziele angeht. Mit Hinblick auf den Bericht des BSI, lässt sich daraus schließen, dass auch wenn es viele Angriffsvarianten gibt und stetig neue entwickelt werden, so bleiben die daraus resultierenden Risiken häufig ähnlich. Dies bedeutet allerdings nicht, dass alle Fälle gleich sind. So gab es bei den Beispielfällen stets auch individuelle Aspekte, die berücksichtigt werden sollten. So wurde anhand von Spyware gezeigt, wie mit einer Angriffsform unterschiedlich vorgegangen werden kann und teilweise unterschiedliche Schutzziele dadurch verletzt werden. Dies wiederum bedeutet, dass Angriffsformen unterschiedlich eingesetzt werden können und dabei nicht exakt die gleichen Auswirkungen haben. Allgemein kommt dem verantwortungsbewussten Umgang von Personal eine hohe Bedeutung zu. Mehrfach wurde in den Beispielen deutlich, wie Angriffe durch menschliches Fehlverhalten erst ermöglicht werden. Dies stimmt auch mit einer Einschätzung des BSI überein. Hiernach ergibt sich für Cyber-Angriffe eine wachsende Bedeutung des Faktors „Mensch“ (BSI, 2021, S. 10).

Die DSGVO stellt in Zusammenhang mit Angriffen das Risikomanagement vor große Herausforderungen. So gibt es klare Vorgaben, was den Schutz von Daten angeht, jedoch wenig Hinweise dazu, wie genau diese Hinweise eingehalten werden sollen. Da es durch die Vielzahl von Angriffen und deren Varianten kaum möglich sein dürfte, gegen alle Angriffe gleichermaßen geschützt zu sein, müssen vor allem bei den präventiven Maßnahmen Prioritäten gesetzt werden. Hierbei sollte es sich um einen rekursiven Prozess handeln, da stetig neue Angriffsvarianten entwickelt werden und neue Angriffsformen an Bedeutung gewinnen können, weshalb gegebenenfalls Maßnahmen ergänzt oder neu hinzugefügt werden müssen. Wie bereits erwähnt muss dennoch damit gerechnet werden, dass auf lange Sicht einer oder mehrere Angriffe erfolgreich sein werden. Doch auch wenn diese Möglichkeit bestehen mag, ist dies kein Grund, alle Anstrengungen einzustellen. So geht aus Artikel 32 schließlich explizit hervor, dass neben dem Stand der Technik auch unter anderem Implementierungskosten und Eintrittswahrscheinlichkeiten berücksichtigt werden können, um geeignete Maßnahmen zu einzuleiten (Artikel 32 Absatz 1 DSGVO). Somit ist davon auszugehen, dass Unternehmen nicht bei jedem erfolgreichen Angriff damit rechnen müssen, zu Strafzahlungen verurteilt zu werden, solange sie darlegen können, dass ihre Maßnahmen angemessen waren. Daher bedeutet nicht jede Verletzung eines Schutzzieles durch einen Angreifer auch ein Schadensereignis für ein Unternehmen.

Doch muss an dieser Stelle erneut betont werden, dass der Umgang mit der DSGVO innerhalb von Unternehmen nicht allein auf Maßnahmen beruhen sollte, die sich auf die Abwehr von Angriffen konzentrieren. So sollten auch Maßnahmen implementiert werden, die die Auswirkungen von Angriffen einschränken können, da auch davon abhängig sein kann, welche Schutzziele verletzt werden und wie stark. Auch hier ist entscheidend, dass davon eine Verhinderung oder wenigstens Abmilderung von Bußgeldern abhängig sein kann. Eine wichtige und einfach zu implementierende Maßnahme des Risikomanagements wurde dabei in allen Beispielen erwähnt. Sollte trotz aller Anstrengungen ein erfolgreicher Angriff eine Verletzung des Datenschutzes zur Folge haben, müssen die dafür zuständigen Behörden gemäß Artikel 33 DSGVO schnellstmöglich davon in Kenntnis gesetzt werden und sachdienliche Informationen zu diesem Vorfall übermittelt werden, um zumindest diesbezüglich die DSGVO einzuhalten.

Insgesamt wurde auch an diesen Beispielfällen der Einfluss der DSGVO durch ihre Vorgaben auf das Risikomanagement belegt. Jedoch gibt es auch Anzeichen dafür, wie zumindest aus der Perspektive von Unternehmen die DSGVO vom Risikomanagement abhängig ist. So wird im Kontext von Angriffen deutlich, wie von der Priorisierung, Entwicklung und Implementierung von Maßnahmen, die Teil des Risikomanagements sind, abhängt, ob die DSGVO überhaupt angemessen umgesetzt werden kann.

5 Fazit

Zu Beginn dieser Arbeit wurde die Frage gestellt, ob sich Risikomanagement in der IT-Sicherheit in einem Abhängigkeitsverhältnis zur DSGVO befindet. Diese Frage kann zwar bejaht werden, jedoch ist damit das Verhältnis nicht vollständig beschrieben.

Im Verlauf dieser Arbeit wurde die vielschichtige Rolle der DSGVO behandelt. Im Vordergrund stehen vor allem Inhalte wie die direkten Vorgaben zum Datenschutz oder die Konsequenzen in Form von Strafzahlungen. Insbesondere letztere sind dabei entscheidend, da sie in diesem Kontext die Schäden beim Risikomanagement darstellen. Allerdings muss auch behandelt werden, dass die Vorgaben nicht die Details der Implementierung vorgeben, was wiederum eine Herausforderung für die Verantwortlichen der Verarbeitung von personenbezogenen Daten darstellt. Dies wird auch dadurch deutlich, dass eine Vielzahl von Unternehmen die DSGVO als große Herausforderung und manche sie sogar als unmöglich vollständig implementierbar ansehen. Es wurde allerdings auch erörtert, dass die DSGVO ohne den Einsatz von Risikomanagement nicht umsetzbar ist. Das Verhältnis zwischen Risikomanagement und der DSGVO ist demnach von einer beidseitigen Abhängigkeit geprägt.

Abschließend ist zu konstatieren, dass es eine Reihe weiterer Aspekte gibt, die genauer untersucht werden könnten. Diese könnten sich beispielsweise auf die bereits erwähnten Zero Day Exploits im Kontext der DSGVO konzentrieren. Gleichermaßen könnten auch genauer untersucht werden, welchen langfristigen Einfluss Strafzahlungen, die aufgrund der DSGVO verhängt werden, auf Risikomanagement in Unternehmen haben.

Literaturverzeichnis

BSI (2021). *Die Lage der IT-Sicherheit in Deutschland 2021*. Abgerufen am 10.01.2022, von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf;jsessionid=48FE902071CFBA4C845144AEA042C96B.internet461?__blob=publicationFile&v=3

Data Protection Commission (2021, 02. September). *Data Protection Commission announces decision in WhatsApp inquiry*. Abgerufen am 10.01.2022, von https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry

Dehmel, S. (2021, 15. September). *Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers* [Vorlesungsfolien]. Bitkom e.V. Abgerufen am 1. November 2021, von https://www.bitkom.org/sites/default/files/2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf

Dreißigacker, A., von Skarczinski, B. & Wollinger, G. R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland - Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019* (Forschungsbericht Nr. 152). KFV e.V. https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf

DSK (2019). *Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen*. Abgerufen am 10.11.2021, von https://lfd.niedersachsen.de/startseite/infothek/datenschutzkonferenz/konzept_zur_bussgeldzumessung/konzept-zur-bussgeldzumessung-in-verfahren-gegen-unternehmen-192565.html

Eckert, C. (2018). *IT-Sicherheit*: *Konzepte - Verfahren - Protokolle*. (10. Aufl.). Berlin, Boston: De Gruyter Oldenbourg. DOI: 10.1515/9783110563900

EDPB (2020). *Leitlinien 4/2019 zu Artikel 25 - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Version 2.0*. Abgerufen am 20.12.2021, von https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf

EDPB (2021, 14. Oktober). *Hamburg DPA: Penalty against Vattenfall Europe Sales GmbH.* Abgerufen am 10.01.2022, von https://edpb.europa.eu/news/national-news/2021/hamburg-dpa-penalty-against-vattenfall-europe-sales-gmbh_de

Fabian, B., Gürses, S., Heisel, M., Santen, T. & Schmidt, H. (2010). A comparison of security requirements engineering methods. In: *Requirements Engineering 15*, Nr. 1, S. 7–40. DOI: 10.1007/s00766-009-0092-x

Fox, D. (2009). Zero Day Exploits. in: *Datenschutz und Datensicherheit - DuD.* Wiesbaden: Springer Gabler, Vol. 33, No. 4 (2009), S. 250. DOI: 10.1007/s11623-009-0060-0

Klipper, S. (2015). *Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010.* (2. Aufl.). Springer Vieweg. DOI: 10.1007/978-3-658-08774-6

Königs, H. (2017). *IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken.* (5. Aufl.). Springer Vieweg. DOI: 10.1007/978-3-658-12004-7

Kuhn, J. (2020, 6. Februar). Datenschutz - Cyberangriff auf das Berliner Kammergericht. *Deutschlandfunk*. Abgerufen am 20.10.2021, von https://www.deutschlandfunk.de/datenschutz-cyberangriff-auf-das-berliner-kammergericht-100.html

OWASP (2021a). *OWASP Top Ten*. Abgerufen am 29.12.2021, von https://owasp.org/www-project-top-ten/

OWASP (2021b). *A09:2021 – Security Logging and Monitoring Failures.* Abgerufen am 29.12.2021, von https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/

OWASP (2021c). *A03:2021 – Injection.* Abgerufen am 29.12.2021, von https://owasp.org/Top10/A03_2021-Injection/

Streim, A. & Weiß, R. (2021, September 15). *Datenschutz setzt Unternehmen unter Dauerdruck*. Bitkom e.V. Abgerufen am 1. November 2021, von https://www.bitkom.org/Presse/Presseinformation/Datenschutz-setzt-Unternehmen-unter-Dauerdruck

T-Systems (2019). *Forensics Report. Vorläufiger forensischer Abschlussbericht zur Untersuchung des Incidents beim Berliner Kammergericht*. Abgerufen am 26.07.2021, von https://www.berlin.de/sen/justva/presse/pressemitteilungen/2020/pm-11-2020-t-systems-forensik_bericht_public_v1.pdf

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr. Amtsblatt der Europäischen Union. Abgerufen am 18.07.2021, von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

Ort	Datum	Unterschrift im Original