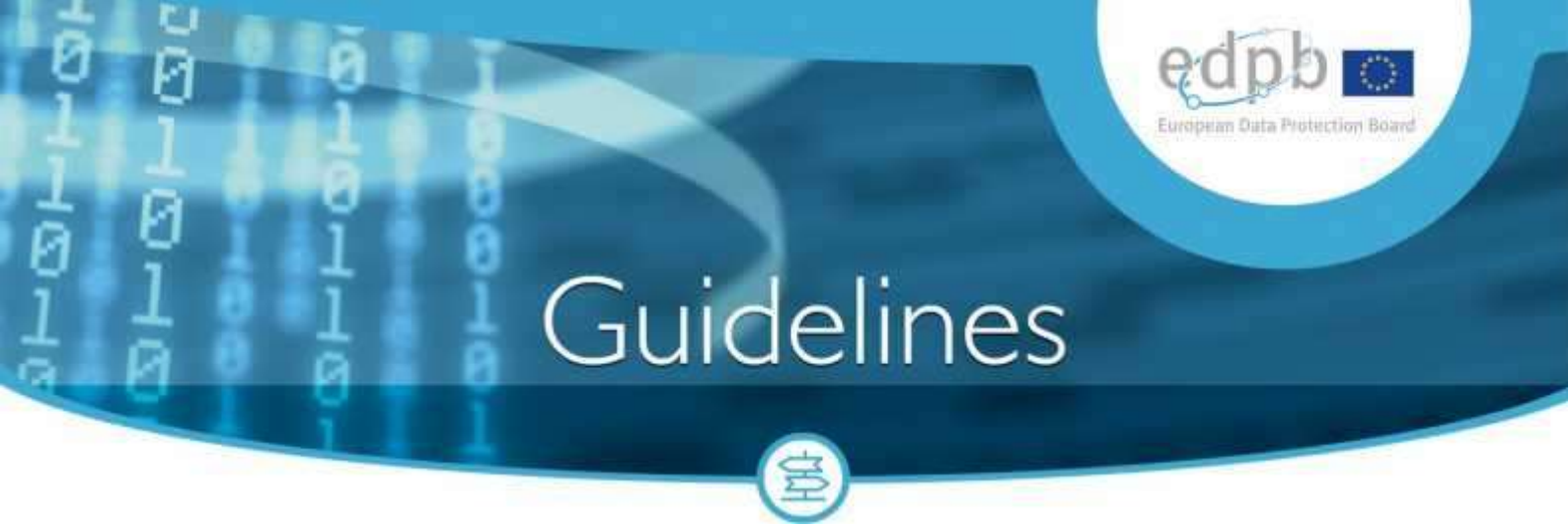

INOFFIZIELLE ÜBERSETZUNG
Die Fußnoten wurden entfernt, um den Textfluss wiederherzustellen und eine automatisierte Übersetzung per www.DeepL.com zu ermöglichen.

Leitlinien 01/2021

über Beispiele für die Benachrichtigung über Verletzungen des Schutzes personenbezogener Daten

Verabschiedet am 14. Dezember 2021

Die Entwurfsversion vom 14.01.2021 ist obsolet.
Es ist unklar, ob und wo Änderungen vorgenommen wurden.
Durch unterschiedliche Formatierungen sind selbst unveränderte Texte nicht zu erkennen.
Eine offizielle deutsche Übersetzung existiert nicht.
Jetzt muss jeder Rechtsanwender die 32 englischen Seiten Wort für Wort vergleichen.

Versionsgeschichte

Version 2.0	14 12 2021	Verabschiedung der Leitlinien nach öffentlicher Konsultation
Version 1.0	14 01 2021	Verabschiedung der Leitlinien für die öffentliche Konsultation

Inhaltsübersicht

1 EINFÜHRUNG 5

2 RANSOMWARE 8

2.1 FALL Nr. 01: Ransomware mit ordnungsgemäßer Sicherung und ohne Exfiltration 8

2.1.1 FALL Nr. 01 - Vorherige Maßnahmen und Risikobewertung 8

2.1.2 FALL Nr. 01 - Schadensminderung und Verpflichtungen 9

2.2 FALL Nr. 02: Ransomware ohne ordnungsgemäße Sicherung 10

2.2.1 FALL Nr. 02 - Vorherige Maßnahmen und Risikobewertung 10

2.2.2 FALL Nr. 02 - Schadensminderung und Verpflichtungen 11

2.3 FALL Nr. 03: Ransomware mit Backup und ohne Exfiltration in einem Krankenhaus 12

2.3.1 FALL Nr. 03 - Vorherige Maßnahmen und Risikobewertung 12

2.3.2 FALL Nr. 03 - Milderung und Verpflichtungen 12

2.4 FALL Nr. 04: Ransomware ohne Backup und mit Exfiltration 13

2.4.1 FALL Nr. 04 - Vorherige Maßnahmen und Risikobewertung 13

2.4.2 FALL Nr. 04 - Schadensminderung und Verpflichtungen 14

2.5 Organisatorische und technische Maßnahmen zur Vorbeugung / Abschwächung der Auswirkungen von Ransomware-Angriffen 14

3 Datenexfiltration ATTACKS 15

3.1 FALL Nr. 05: Exfiltration von Bewerbungsdaten von einer Website 15

3.1.1 FALL Nr. 05 - Vorherige Maßnahmen und Risikobewertung 15

3.1.2 FALL Nr. 05 - Milderung und Verpflichtungen 16

3.2 FALL Nr. 06: Exfiltration eines gehashten Passworts von einer Website 17

3.2.1 FALL Nr. 06 - Vorherige Maßnahmen und Risikobewertung 17

3.2.2 FALL Nr. 06 - Milderung und Verpflichtungen 17

3.3 FALL Nr. 07: Credential-Stuffing-Angriff auf eine Bank-Website 18

3.3.1 FALL Nr. 07 - Vorherige Maßnahmen und Risikobewertung 18

3.3.2 FALL Nr. 07 - Schadensminderung und Verpflichtungen 18

3.4 Organisatorische und technische Maßnahmen zur Vorbeugung / Abschwächung der Auswirkungen von Hackerangriffen 19

4 INTERNE MENSCHLICHE RISIKOQUELLE 20

4.1 FALL Nr. 08: Exfiltration von Geschäftsdaten durch einen Mitarbeiter 20

4.1.1 FALL Nr. 08 - Vorherige Maßnahmen und Risikobewertung 20

4.1.2 FALL Nr. 08 - Schadensminderung und Verpflichtungen 21

4.2 FALL Nr. 09: Versehentliche Übermittlung von Daten an eine vertrauenswürdige dritte Person 22

4.2.1 FALL Nr. 09 - Vorherige Maßnahmen und Risikobewertung 22

4.2.2 FALL Nr. 09 - Milderung und Verpflichtungen 22

4.3 Organisatorische und technische Maßnahmen zur Vermeidung/Minderung der Auswirkungen interner menschlicher Risikoquellen 22
5 VERLORENE ODER GESTOHLENE GERÄTE UND PAPIERDOKUMENTE 23
5.1 FALL Nr. 10: Gestohlenes Material mit verschlüsselten personenbezogenen Daten 24
5.1.1 FALL Nr. 10 - Vorherige Maßnahmen und Risikobewertung 24
5.1.2 FALL Nr. 10 - Schadensminderung und Verpflichtungen 24
5.2 FALL Nr. 11: Gestohlenes Material mit unverschlüsselten personenbezogenen Daten 25
5.2.1 FALL Nr. 11 - Vorherige Maßnahmen und Risikobewertung 25
5.2.2 FALL Nr. 11 - Schadensminderung und Verpflichtungen 25
5.3 FALL Nr. 12: Gestohlene Papierakten mit sensiblen Daten 25
5.3.1 FALL Nr. 12 - Vorherige Maßnahmen und Risikobewertung 26
5.3.2 FALL Nr. 12 - Milderung und Verpflichtungen 26
5.4 Organisatorische und technische Maßnahmen zur Verhinderung/Minderung der Auswirkungen von Verlust oder Diebstahl von Geräten 26
6 MISPOSTAL 27
6.1 FALL Nr. 13: Fehler bei der Postzustellung 27
6.1.1 FALL Nr. 13 - Vorherige Maßnahmen und Risikobewertung 27
6.1.2 FALL Nr. 13 - Milderung und Verpflichtungen 27
6.2 FALL Nr. 14: Versehentlich per Post verschickte streng vertrauliche personenbezogene Daten 28
6.2.1 FALL Nr. 14 - Vorherige Maßnahmen und Risikobewertung 28
6.2.2 FALL Nr. 14 - Milderung und Verpflichtungen 28
6.3 FALL Nr. 15: Versehentlich per Post übermittelte personenbezogene Daten 28
6.3.1 FALL Nr. 15 - Vorherige Maßnahmen und Risikobewertung 28
6.3.2 FALL Nr. 15 - Milderung und Verpflichtungen 29
6.4 FALL Nr. 16: Fehler bei der Postzustellung 29
6.4.1 FALL Nr. 16 - Vorherige Maßnahmen und Risikobewertung 29
6.4.2 FALL Nr. 16 - Schadensminderung und Verpflichtungen 30
6.5 Organisatorische und technische Maßnahmen zur Vorbeugung / Abschwächung der Auswirkungen von Falschparkern 30
7 Andere Fälle - Social Engineering 31
7.1 FALL Nr. 17: Identitätsdiebstahl 31
7.1.1 FALL Nr. 17 - Risikobewertung, Risikominderung und Verpflichtungen 31
7.2 FALL Nr. 18: E-Mail-Exfiltration 32
7.2.1 FALL Nr. 18 - Risikobewertung, Risikominderung und Verpflichtungen 32

DER EUROPÄISCHE DATENSCHUTZAUSSCHUSS

gestützt auf Artikel 70 (1e) der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom April27 2016 zum2016 Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden "DSGVO"),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018[1],

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

gestützt auf die Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel "Der Datenschutz als Pfeiler der Bürgerbeteiligung und das Konzept der EU für den digitalen Wandel - zwei Jahre Anwendung der Datenschutz-Grundverordnung"[2],

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN

1 EINFÜHRUNG

1. Die Datenschutz-Grundverordnung schreibt in bestimmten Fällen vor, dass eine Verletzung des Schutzes personenbezogener Daten der zuständigen nationalen Aufsichtsbehörde (nachstehend "Aufsichtsbehörde") gemeldet werden muss und dass die Personen, deren personenbezogene Daten von der Verletzung betroffen sind, über die Verletzung zu informieren sind (Artikel 33 und 34).

2. Die Artikel-29-Datenschutzgruppe hat bereits im Oktober 2017 einen *allgemeinen* Leitfaden zur Meldung von Datenschutzverletzungen erstellt, in dem die einschlägigen Abschnitte der DSGVO analysiert werden (Leitlinien zur Meldung von Datenschutzverletzungen im Rahmen der Verordnung (EU) 2016/679, WP 250) (im Folgenden "Leitlinien WP 250")[3]. Aufgrund ihrer Art und ihres Zeitpunkts wurden in dieser Leitlinie jedoch nicht alle praktischen Fragen hinreichend ausführlich behandelt. Daher ist ein *praxisorientierter, fallbezogener* Leitfaden erforderlich, der die Erfahrungen nutzt, die die ORKB seit der Anwendung der DSGVO gesammelt haben.

3. Dieses Dokument soll die Leitlinien WP 250 ergänzen und spiegelt die gemeinsamen Erfahrungen der ORKB des EWR seit dem Inkrafttreten der Datenschutzgrundverordnung wider. Es soll den für die Datenverarbeitung Verantwortlichen bei der Entscheidung helfen, wie sie mit Datenschutzverletzungen umgehen und welche Faktoren bei der Risikobewertung zu berücksichtigen sind.

4. Bei jedem Versuch, eine Datenschutzverletzung zu beheben, sollten der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter zunächst in der Lage sein, eine solche zu erkennen. Die Datenschutz-Grundverordnung definiert eine "Verletzung des Schutzes personenbezogener Daten" in Artikel 4 Absatz 12 als "eine Verletzung der Sicherheit, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum unbefugten Zugang zu übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten führt".

5. In ihrer Stellungnahme 03/2014 zur Meldung von Sicherheitsverletzungen [4]und in ihren Leitlinien erklärte die WP29250,, dass Sicherheitsverletzungen nach den folgenden drei bekannten Grundsätzen der Informationssicherheit kategorisiert werden können:

   - "Verletzung der Vertraulichkeit" - wenn es zu einer unbefugten oder versehentlichen Offenlegung personenbezogener Daten oder zum Zugriff auf diese Daten kommt.

- "Verletzung der Integrität" - wenn eine unbefugte oder versehentliche Änderung personenbezogener Daten vorliegt.
- "Verfügbarkeitsverletzung" - zufälliger oder unbefugter Verlust des Zugangs zu personenbezogenen Daten oder deren Vernichtung.[5]

6. Eine Datenschutzverletzung kann potenziell eine Reihe von erheblichen nachteiligen Auswirkungen auf Einzelpersonen haben, die zu physischem, materiellem oder immateriellem Schaden führen können. In der DSGVO wird erläutert, dass dies den Verlust der Kontrolle über ihre personenbezogenen Daten, die Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder Betrug, finanzielle Verluste, die unbefugte Aufhebung der Pseudonymisierung, Rufschädigung und den Verlust der Vertraulichkeit personenbezogener Daten, die unter das Berufsgeheimnis fallen, umfassen kann. Sie kann auch jeden anderen erheblichen wirtschaftlichen oder sozialen Nachteil für diese Personen umfassen. Eine der wichtigsten Pflichten des für die Datenverarbeitung Verantwortlichen ist es, diese Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewerten und geeignete technische und organisatorische Maßnahmen zu ergreifen, um ihnen zu begegnen.

7. Dementsprechend verlangt die Datenschutz-Grundverordnung von dem für die Verarbeitung Verantwortlichen, dass er:

   - jede Verletzung des Schutzes personenbezogener Daten zu dokumentieren, wobei die Fakten der Verletzung des Schutzes personenbezogener Daten, ihre Auswirkungen und die getroffenen[6] Abhilfemaßnahmen anzugeben sind;
   - die Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde melden, es sei denn, es ist unwahrscheinlich, dass die Verletzung des Schutzes personenbezogener Daten zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt[7];
   - die betroffene Person über die Verletzung des Schutzes personenbezogener Daten zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt[8].

8. Datenschutzverletzungen sind an sich schon ein Problem, aber sie können auch ein Symptom für ein anfälliges, möglicherweise veraltetes Datensicherheitssystem sein und auf Systemschwächen hinweisen, die behoben werden müssen. Generell gilt, dass es immer besser ist, Datenschutzverletzungen zu verhindern, indem man sich im Voraus darauf vorbereitet, da einige ihrer Folgen von Natur aus unumkehrbar sind. Bevor ein für die Verarbeitung Verantwortlicher das Risiko, das sich aus einer durch einen Angriff verursachten Sicherheitsverletzung ergibt, *in vollem Umfang* einschätzen kann, sollte die Ursache des Problems ermittelt werden, um festzustellen, ob die Schwachstellen, die zu dem Vorfall geführt haben, immer noch vorhanden und somit ausnutzbar sind. In vielen Fällen ist der für die Verarbeitung Verantwortliche in der Lage festzustellen, dass der Vorfall wahrscheinlich zu einem Risiko führt und daher gemeldet werden muss. In anderen Fällen muss die Meldung nicht aufgeschoben werden, bis das Risiko und die Auswirkungen der Sicherheitsverletzung vollständig bewertet worden sind, da die vollständige Risikobewertung parallel zur Meldung erfolgen kann und die so gewonnenen Informationen der Aufsichtsbehörde schrittweise und ohne unangemessene Verzögerung[9] zur Verfügung gestellt werden können.

9. Die Verletzung sollte gemeldet werden, wenn der für die Verarbeitung Verantwortliche der Ansicht ist, dass sie wahrscheinlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Person führen wird. Die für die Verarbeitung Verantwortlichen sollten diese Bewertung zu dem Zeitpunkt vornehmen, zu dem sie von der Verletzung Kenntnis erlangen. Der für die Verarbeitung Verantwortliche sollte nicht erst eine eingehende kriminaltechnische Untersuchung und (frühzeitige) Abhilfemaßnahmen abwarten, bevor er beurteilt, ob die Datenschutzverletzung wahrscheinlich zu einem Risiko führt und daher zu melden ist oder nicht.

10. Wenn ein Kontrolleur das Risiko selbst als unwahrscheinlich einschätzt, es sich aber herausstellt, dass das

Risiko eintritt, kann die zuständige ORKB von ihren Korrekturbefugnissen Gebrauch machen und Sanktionen beschließen

11. Jeder für die Verarbeitung Verantwortliche und jeder Auftragsverarbeiter sollte über Pläne und Verfahren für den Umgang mit etwaigen Datenschutzverletzungen verfügen. Organisationen sollten klare Berichtslinien und Personen haben, die für bestimmte Aspekte des Wiederherstellungsprozesses verantwortlich sind

12. Schulungen und Sensibilisierung des Personals des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters für Datenschutzfragen mit Schwerpunkt auf dem Umgang mit Verletzungen des Schutzes personenbezogener Daten (Erkennung von Verletzungen des Schutzes personenbezogener Daten und weitere zu ergreifende Maßnahmen usw.) sind für die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter ebenfalls unerlässlich. Diese Schulungen sollten je nach Art der Verarbeitungstätigkeit und der Größe des für die Verarbeitung Verantwortlichen regelmäßig wiederholt werden und die neuesten Trends und Warnungen vor Cyberangriffen oder anderen Sicherheitsvorfällen behandeln.

13. Der Grundsatz der Rechenschaftspflicht und das Konzept des "eingebauten Datenschutzes" könnten eine Analyse beinhalten, die in das eigene "Handbuch für den Umgang mit Verletzungen des Schutzes personenbezogener Daten" des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters einfließt, das darauf abzielt, Fakten für jede Facette der Verarbeitung in jeder wichtigen Phase des Vorgangs zu schaffen. Ein solches Handbuch, das im Voraus erstellt wird, würde eine viel schnellere Informationsquelle darstellen, die es den für die Verarbeitung Verantwortlichen und den Datenverarbeitern ermöglicht, die Risiken zu mindern und die Verpflichtungen ohne unangemessene Verzögerung zu erfüllen. Dies würde sicherstellen, dass im Falle einer Verletzung des Schutzes personenbezogener Daten die Mitarbeiter der Organisation wissen, was zu tun ist, und dass der Vorfall wahrscheinlich schneller bewältigt werden kann, als wenn es keine Abhilfemaßnahmen oder keinen Plan gäbe.

14. Die im Folgenden dargestellten Fälle sind zwar fiktiv, beruhen aber auf typischen Fällen aus der kollektiven Erfahrung der SA mit Meldungen von Datenschutzverletzungen. Die angebotenen Analysen beziehen sich ausdrücklich auf die untersuchten Fälle, sollen aber den für die Datenverarbeitung Verantwortlichen eine Hilfestellung bei der Bewertung ihrer eigenen Datenschutzverletzungen bieten. Jegliche Änderung der Umstände in den nachstehend beschriebenen Fällen kann zu einem anderen oder höheren Risikoniveau führen, so dass andere oder zusätzliche Maßnahmen erforderlich sind. Diese Leitlinien strukturieren die Fälle nach bestimmten Kategorien von Datenschutzverletzungen (z. B. Ransomware-Angriffe). Bestimmte Maßnahmen zur Risikominderung sind in jedem Fall erforderlich, wenn es um eine bestimmte Kategorie von Sicherheitsverletzungen geht. Diese Maßnahmen werden nicht notwendigerweise bei jeder Fallanalyse, die zur gleichen Kategorie von Verstößen gehört, wiederholt. Bei den Fällen, die zur selben Kategorie gehören, werden nur die Unterschiede aufgezeigt. Daher sollte der Leser alle Fälle lesen, die zu der jeweiligen Kategorie von Verstößen gehören, um alle richtigen Maßnahmen zu erkennen und zu unterscheiden.

15. Die interne Dokumentation einer Datenschutzverletzung ist eine Verpflichtung, die unabhängig von den mit der Verletzung verbundenen Risiken besteht und in jedem einzelnen Fall durchgeführt werden muss. Die im Folgenden dargestellten Fälle sollen Aufschluss darüber geben, ob die Datenschutzverletzung der Aufsichtsbehörde gemeldet und den betroffenen Personen mitgeteilt werden muss oder nicht.

2 RANSOMWARE

16. Ein häufiger Grund für die Meldung einer Datenschutzverletzung ist ein Ransomware-Angriff auf den für die Datenverarbeitung Verantwortlichen. In diesen Fällen verschlüsselt ein bösartiger Code die personenbezogenen Daten, und anschließend verlangt der Angreifer von dem für die Verarbeitung Verantwortlichen ein Lösegeld im Austausch für den Entschlüsselungscode. Diese Art von Angriffen kann in der Regel als eine Verletzung der Verfügbarkeit eingestuft werden, oft kann aber auch eine Verletzung der Vertraulichkeit vorliegen.

2.1 FALL Nr. 01: Ransomware mit ordnungsgemäßer Sicherung und ohne Exfiltration

Die Computersysteme eines kleinen Fertigungsunternehmens waren einem Ransomware-Angriff ausgesetzt, und die auf diesen Systemen gespeicherten Daten wurden verschlüsselt. Der für die Datenverarbeitung Verantwortliche verwendete eine Verschlüsselung im Ruhezustand, d. h. alle Daten, auf die die Ransomware zugriff, wurden mit einem modernen Verschlüsselungsalgorithmus in verschlüsselter Form gespeichert. Der Entschlüsselungsschlüssel wurde bei dem Angriff nicht kompromittiert, d. h. der Angreifer konnte weder auf ihn zugreifen noch ihn indirekt verwenden. Folglich hatte der Angreifer nur Zugriff auf verschlüsselte persönliche Daten. Insbesondere waren weder das E-Mail-System des Unternehmens noch die Client-Systeme, über die darauf zugegriffen wurde, betroffen. Das Unternehmen nutzt die Expertise eines externen Cybersecurity-Unternehmens, um den Vorfall zu untersuchen. Es liegen Protokolle vor, die alle Datenströme nachverfolgen, die das Unternehmen verlassen haben (einschließlich ausgehender E-Mails). Nach der Analyse der Protokolle und der von den Erkennungssystemen des Unternehmens gesammelten Daten hat eine interne Untersuchung mit Unterstützung des externen Cybersicherheitsunternehmens *mit Sicherheit* ergeben, dass der Täter die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Aus den Protokollen geht hervor, dass im Zeitraum des Angriffs kein Datenfluss nach außen stattfand. Die von der Sicherheitsverletzung betroffenen personenbezogenen Daten beziehen sich auf Kunden und Mitarbeiter des Unternehmens, insgesamt einige Dutzend Personen. Eine Sicherungskopie war ohne weiteres verfügbar, und die Daten wurden wenige Stunden nach dem Angriff wiederhergestellt. Die Sicherheitsverletzung hatte keine Auswirkungen auf das Tagesgeschäft des für die Verarbeitung Verantwortlichen. Es gab keine Verzögerungen bei der Bezahlung von Mitarbeitern oder der Bearbeitung von Kundenanfragen.

17. In diesem Fall wurden die folgenden Elemente aus der Definition einer "Verletzung des Schutzes personenbezogener Daten" umgesetzt: Eine Verletzung der Sicherheit führte zu einer unrechtmäßigen Änderung und einem unbefugten Zugriff auf gespeicherte personenbezogene Daten.

2.1.1 FALL Nr. 01 - Vorherige Maßnahmen und Risikobewertung

18. Wie bei allen Risiken, die von externen Akteuren ausgehen, kann die Wahrscheinlichkeit, dass ein Ransomware-Angriff erfolgreich ist, drastisch reduziert werden, indem die Sicherheit der Datenkontrollumgebung verstärkt wird. Die meisten dieser Verstöße können verhindert werden, indem geeignete organisatorische, physische und technologische Sicherheitsmaßnahmen getroffen werden. Beispiele für solche Maßnahmen sind eine angemessene Patch-Verwaltung und der Einsatz eines geeigneten Anti-Malware-Erkennungssystems. Eine ordnungsgemäße und getrennte Datensicherung trägt dazu bei, die Folgen eines erfolgreichen Angriffs abzumildern, sollte es dazu kommen. Darüber hinaus kann ein Programm zur Sicherheitsschulung, -ausbildung und -aufklärung (SETA) der Mitarbeiter dazu beitragen, diese Art von Angriffen zu verhindern und zu erkennen. (Eine Liste empfehlenswerter Maßnahmen findet sich in Abschnitt 2.5.) Zu den wichtigsten Maßnahmen gehört ein angemessenes Patch-Management, das sicherstellt, dass die Systeme auf dem neuesten Stand sind und alle bekannten Schwachstellen der eingesetzten Systeme behoben werden, da die meisten Ransomware-Angriffe bekannte Schwachstellen ausnutzen.

19. Bei der Risikobewertung sollte der für die Verarbeitung Verantwortliche die Sicherheitsverletzung

untersuchen und die Art des bösartigen Codes ermitteln, um die möglichen Folgen des Angriffs zu verstehen. Zu den zu berücksichtigenden Risiken gehört das Risiko, dass Daten exfiltriert wurden, ohne eine Spur in den Protokollen der Systeme zu hinterlassen.

20. In diesem Beispiel hatte der Angreifer Zugriff auf personenbezogene Daten, und die Vertraulichkeit des Chiffriertextes, der personenbezogene Daten in verschlüsselter Form enthält, war gefährdet. Allerdings können die Daten, die möglicherweise exfiltriert wurden, zumindest vorläufig nicht vom Täter gelesen oder verwendet werden. Die von dem für die Datenverarbeitung Verantwortlichen verwendete Verschlüsselungstechnik entspricht dem Stand der Technik. Der Entschlüsselungsschlüssel wurde nicht kompromittiert und konnte vermutlich auch nicht auf anderem Wege ermittelt werden. Folglich sind die Risiken für die Vertraulichkeit derdie Rechte und Freiheiten natürlicher Personen auf ein Minimum reduziert werden, ohne dass ein kryptoanalytischer Fortschritt erzielt wird, der die verschlüsselten Daten in Zukunft verständlich macht.

21. Der für die Verarbeitung Verantwortliche sollte das Risiko für den Einzelnen aufgrund der Sicherheitsverletzung berücksichtigen[10]. In diesem Fall scheinen die Risiken für die Rechte und Freiheiten der betroffenen Personen aus der mangelnden Verfügbarkeit der personenbezogenen Daten zu resultieren, und die Vertraulichkeit der personenbezogenen Daten ist nicht gefährdet[11]. In diesem Beispiel wurden die nachteiligen Auswirkungen der Datenschutzverletzung relativ bald nach dem Eintreten der Verletzung gemildert. Ein angemessenes Backup-System[12] mildert die Auswirkungen der Verletzung, und in diesem Fall war der für die Verarbeitung Verantwortliche in der Lage, es effektiv zu nutzen.

22. Was die Schwere der Folgen für die betroffenen Personen betrifft, so konnten nur geringfügige Folgen festgestellt werden, da die betroffenen Daten innerhalb weniger Stunden wiederhergestellt wurden, die Sicherheitsverletzung keine Auswirkungen auf das Tagesgeschäft des für die Verarbeitung Verantwortlichen hatte und sich nicht wesentlich auf die betroffenen Personen auswirkte (z. B. Zahlungen der Mitarbeiter oder Bearbeitung von Kundenanfragen).

2.1.2 FALL Nr. 01 - Schadensminderung und Verpflichtungen

23. Ohne ein Backup kann der für die Verarbeitung Verantwortliche nur wenige Maßnahmen ergreifen, um den Verlust personenbezogener Daten zu beheben, und die Daten müssen erneut erhoben werden. In diesem speziellen Fall konnten die Auswirkungen des Angriffs jedoch wirksam eingedämmt werden, indem alle kompromittierten Systeme auf einen sauberen Zustand zurückgesetzt wurden, von dem bekannt ist, dass er frei von bösartigem Code ist, die Schwachstellen behoben und die betroffenen Daten bald nach dem Angriff wiederhergestellt wurden. Ohne ein Backup sind die Daten verloren und der Schweregrad kann sich erhöhen, da auch Risiken oder Auswirkungen auf Einzelpersonen auftreten können.

24. Die Rechtzeitigkeit einer effektiven Datenwiederherstellung aus dem sofort verfügbaren Backup ist eine Schlüsselvariable bei der Analyse der Sicherheitsverletzung. Die Festlegung eines angemessenen Zeitrahmens für die Wiederherstellung der gefährdeten Daten hängt von den besonderen Umständen der jeweiligen Verletzung ab. Die Datenschutz-Grundverordnung besagt, dass eine Verletzung des Schutzes personenbezogener Daten unverzüglich und, soweit möglich, spätestens nach 72 Stunden gemeldet werden muss. Daher könnte man zu dem Schluss kommen, dass eine Überschreitung der 72-Stunden-Frist in jedem Fall nicht ratsam ist, aber bei Fällen mit hohem Risikoniveau kann selbst die Einhaltung dieser Frist als unbefriedigend angesehen werden.

25. In diesem Fall kam der für die Verarbeitung Verantwortliche nach einer detaillierten Folgenabschätzung und einem Verfahren zur Reaktion auf den Vorfall zu dem Schluss, dass die Verletzung wahrscheinlich kein Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, so dass keine Mitteilung an die betroffenen Personen erforderlich ist und die Verletzung auch nicht der Aufsichtsbehörde gemeldet werden muss. Wie alle Datenschutzverletzungen sollte sie jedoch gemäß Artikel 33 Absatz 5 dokumentiert

werden. Die Organisation muss möglicherweise auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Handhabung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und verbessern (oder wird später von der ORKB dazu aufgefordert). Im Rahmen dieser Aktualisierung und Nachbesserung sollte die Organisation die Verletzung gründlich untersuchen und die Ursachen und die vom Täter verwendeten Methoden ermitteln, um ähnliche Vorfälle in Zukunft zu verhindern.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen
	X	X

2.2 FALL Nr. 02: Ransomware ohne ordnungsgemäße Sicherung

Einer der von einem landwirtschaftlichen Unternehmen genutzten Computer wurde Opfer eines Ransomware-Angriffs und seine Daten wurden vom Angreifer verschlüsselt. Das Unternehmen nutzt das Fachwissen eines externen Cybersicherheitsunternehmens, um sein Netzwerk zu überwachen. Es liegen Protokolle vor, die alle Datenströme, die das Unternehmen verlassen (einschließlich ausgehender E-Mails), aufzeichnen. Nach der Analyse der Protokolle und der Daten, die die anderen Erkennungssysteme gesammelt haben, hat die interne Untersuchung mit Unterstützung des Cybersecurity-Unternehmens ergeben, dass der Täter die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Aus den Protokollen geht hervor, dass im Zeitraum des Angriffs kein Datenfluss nach außen stattfand. Die von der Sicherheitsverletzung betroffenen personenbezogenen Daten beziehen sich auf die Mitarbeiter und Kunden des Unternehmens, insgesamt einige Dutzend Personen. Es waren keine besonderen Kategorien von Daten betroffen. Es lag keine elektronische Sicherungskopie vor. Der größte Teil der Daten wurde anhand von Sicherungskopien in Papierform wiederhergestellt. Die Wiederherstellung der Daten dauerte 5 Arbeitstage und führte zu geringfügigen Verzögerungen bei der Auslieferung von Bestellungen an Kunden.

2.2.1 FALL Nr. 02 - Vorherige Maßnahmen und Risikobewertung

26. Der für die Verarbeitung Verantwortliche sollte dieselben vorherigen Maßnahmen ergriffen haben, wie sie in Teil 2.1. und in Abschnitt
2.9. Der Hauptunterschied zum vorherigen Fall ist das Fehlen eines elektronischen Backups und das Fehlen einer Verschlüsselung im Ruhezustand. Dies führt zu kritischen Unterschieden bei den folgenden Schritten.

27. Bei der Risikobewertung sollte der für die Verarbeitung Verantwortliche die Methode des Eindringens untersuchen und die Art des Schadcodes ermitteln, um die möglichen Folgen des Angriffs zu verstehen. In diesem Beispiel verschlüsselte die Ransomware die personenbezogenen Daten, ohne sie zu exfiltrieren. Die Risiken für die Rechte und Freiheiten der betroffenen Personen ergeben sich also aus der mangelnden Verfügbarkeit der personenbezogenen Daten, und die Vertraulichkeit der personenbezogenen Daten ist nicht gefährdet. Eine gründliche Prüfung der Firewall-Protokolle und ihrer Auswirkungen ist für die Bestimmung des Risikos von wesentlicher Bedeutung. Der für die Verarbeitung Verantwortliche sollte die tatsächlichen Ergebnisse dieser Untersuchungen auf Anfrage vorlegen.

28. Der für die Verarbeitung Verantwortliche muss bedenken, dass die Schadsoftware bei einem raffinierten Angriff in der Lage ist, Protokolldateien zu bearbeiten und die Spuren zu beseitigen. Da die Protokolle nicht an einen zentralen Protokollserver weitergeleitet oder repliziert werden, kann der für die Verarbeitung Verantwortliche selbst nach einer gründlichen Untersuchung, bei der festgestellt wurde, dass die personenbezogenen Daten nicht durch den Angreifer exfiltriert wurden, nicht behaupten, dass das Fehlen eines Protokolleintrags beweist, dass keine Exfiltration stattgefunden hat, so dass die Wahrscheinlichkeit

einer Verletzung der Vertraulichkeit nicht völlig ausgeschlossen werden kann.

29. Der für die Verarbeitung Verantwortliche sollte die Risiken dieser Verletzung bewerten, [13]wenn der Angreifer Zugang zu den Daten hatte. Bei der Risikobewertung sollte der für die Verarbeitung Verantwortliche auch die Art, die Sensibilität, den Umfang und den Kontext der von der Sicherheitsverletzung betroffenen personenbezogenen Daten berücksichtigen. In diesem Fall sind keine besonderen Kategorien personenbezogener Daten betroffen, und die Menge der verletzten Daten und die Zahl der betroffenen Personen ist gering.

30. Das Sammeln genauer Informationen über den unbefugten Zugriff ist der Schlüssel zur Bestimmung des Risikoniveaus und zur Verhinderung eines neuen oder weiteren Angriffs. Wenn die Daten aus der Datenbank kopiert worden wären, wäre dies natürlich ein risikoerhöhender Faktor gewesen. Wenn man sich über die Einzelheiten des unrechtmäßigen Zugriffs nicht sicher ist, sollte das schlimmste Szenario in Betracht gezogen und das Risiko entsprechend bewertet werden.

31. Das Fehlen einer Sicherungsdatenbank kann als risikoerhöhender Faktor betrachtet werden, je nachdem, wie schwerwiegend die Folgen für die betroffenen Personen sind, die sich aus der mangelnden Verfügbarkeit der Daten ergeben.

2.2.2 FALL Nr. 02 - Schadensminderung und Verpflichtungen

32. Ohne eine Sicherungskopie kann der für die Verarbeitung Verantwortliche nur wenige Maßnahmen ergreifen, um den Verlust personenbezogener Daten zu beheben, und die Daten müssen erneut erhoben werden, es sei denn, es steht eine andere Quelle zur Verfügung (z. B. Auftragsbestätigungs-E-Mails). Ohne ein Backup können Daten verloren gehen, und die Schwere der Verletzung hängt von den Auswirkungen für die betroffenen Personen ab.

33. Die Wiederherstellung der Daten sollte sich nicht als übermäßig problematisch er[14]weisen, wenn die Daten noch in Papierform vorliegen, aber angesichts des Fehlens einer elektronischen Sicherungsdatenbank wird eine Meldung an die ORKB für notwendig erachtet, da die Wiederherstellung der Daten einige Zeit in Anspruch genommen hat und zu Verzögerungen bei der Auslieferung der Bestellungen an die Kunden führen könnte und eine beträchtliche Menge an Metadaten (z. B. Protokolle, Zeitstempel) möglicherweise nicht abrufbar ist.

34. Die Unterrichtung der betroffenen Personen über die Sicherheitsverletzung kann auch davon abhängen, wie lange die personenbezogenen Daten nicht verfügbar sind und welche Schwierigkeiten sich daraus für den für die Verarbeitung Verantwortlichen ergeben könnten (z. B. Verzögerungen bei der Überweisung von Arbeitnehmerzahlungen). Da diese Verzögerungen bei Zahlungen und Lieferungen zu finanziellen Verlusten für die Personen führen können, deren Daten kompromittiert wurden, könnte man auch argumentieren, dass die Verletzung wahrscheinlich zu einem hohen Risiko führt. Auch könnte es sich als unumgänglich erweisen, die betroffenen Personen zu informieren, wenn ihr Beitrag zur Wiederherstellung der verschlüsselten Daten erforderlich ist.

35. Dieser Fall dient als Beispiel für einen Ransomware-Angriff mit einem Risiko für die Rechte und Freiheiten der betroffenen Personen, der jedoch kein hohes Risiko darstellt. Er sollte gemäß Artikel 33 Absatz 5 dokumentiert und der Aufsichtsbehörde gemäß Artikel 33 Absatz 1 gemeldet werden. Die Organisation muss möglicherweise auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Handhabung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und verbessern (oder wird von der Aufsichtsbehörde dazu aufgefordert).

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

		X

2.3 FALL Nr. 03: Ransomware mit Backup und ohne Exfiltration in einem Krankenhaus

Das Informationssystem eines Krankenhauses/Gesundheitszentrums war einem Ransomware-Angriff ausgesetzt, und ein erheblicher Teil der Daten wurde von dem Angreifer verschlüsselt. Das Unternehmen nutzt das Fachwissen eines externen Cybersicherheitsunternehmens, um sein Netzwerk zu überwachen. Es liegen Protokolle vor, die alle Datenströme, die das Unternehmen verlassen (einschließlich ausgehender E-Mails), aufzeichnen. Nach der Analyse der Protokolle und der Daten, die die anderen Erkennungssysteme gesammelt haben, hat die interne Untersuchung mit Unterstützung des Cybersecurity-Unternehmens ergeben, dass der Täter die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Aus den Protokollen geht hervor, dass im Zeitraum des Angriffs kein Datenfluss nach außen stattfand. Die von der Sicherheitsverletzung betroffenen personenbezogenen Daten beziehen sich auf Mitarbeiter und Patienten, d. h. auf Tausende von Personen. Backups waren in elektronischer Form verfügbar. Der größte Teil der Daten wurde wiederhergestellt, aber dieser Vorgang dauerte zwei Arbeitstage und führte zu erheblichen Verzögerungen bei der Behandlung der Patienten, da Operationen abgesagt bzw. verschoben wurden, und zu einer Verringerung des Dienstleistungsniveaus aufgrund der Nichtverfügbarkeit der Systeme.

2.3.1 FALL Nr. 03 - Vorherige Maßnahmen und Risikobewertung

36. Der für die Verarbeitung Verantwortliche sollte dieselben vorherigen Maßnahmen ergriffen haben, wie sie in Teil und2.1. in Abschnitt
2.5. Der Hauptunterschied zum vorhergehenden Fall ist die große Schwere der Folgen für einen erheblichen Teil der betroffenen[15] Personen.

37. Die Menge der verletzten Daten und die Zahl der betroffenen Personen sind hoch, da Krankenhäuser in der Regel große Datenmengen verarbeiten. Die Nichtverfügbarkeit der Daten hat große Auswirkungen auf einen erheblichen Teil der betroffenen Personen. Darüber hinaus besteht ein schwerwiegendes Restrisiko für die Vertraulichkeit der Patientendaten.

38. Wichtig sind die Art der Verletzung, die Art, die Sensibilität und der Umfang der betroffenen personenbezogenen Daten. Auch wenn eine Sicherungskopie der Daten vorhanden war und diese innerhalb weniger Tage wiederhergestellt werden konnte, besteht aufgrund der schwerwiegenden Folgen für die betroffenen Personen, die sich aus der mangelnden Verfügbarkeit der Daten zum Zeitpunkt des Angriffs und in den folgenden Tagen ergeben, ein hohes Risiko.

2.3.2 FALL Nr. 03 - Milderung und Verpflichtungen

39. Eine Meldung an die Aufsichtsbehörde wird als notwendig erachtet, da besondere Kategorien personenbezogener Daten betroffen sind und die Wiederherstellung der Daten lange dauern könnte, was zu erheblichen Verzögerungen bei der Patientenversorgung führen würde. Die Unterrichtung der betroffenen Personen über die Sicherheitsverletzung ist aufgrund der Auswirkungen für die Patienten auch nach der Wiederherstellung der verschlüsselten Daten erforderlich. Während die Daten aller Patienten, die in den letzten Jahren im Krankenhaus behandelt wurden, verschlüsselt wurden, waren nur die Patienten betroffen, die während der Zeit, in der das Computersystem nicht verfügbar war, im Krankenhaus behandelt werden sollten. Der für die Verarbeitung Verantwortliche sollte diese Patienten direkt über die Datenverletzung informieren. Eine direkte Mitteilung an die anderen Patienten, von denen einige möglicherweise seit mehr als zwanzig Jahren nicht mehr im Krankenhaus behandelt wurden, ist aufgrund der Ausnahme in Artikel 34 Absatz 3 Buchstabe c nicht erforderlich. In einem solchen Fall muss stattdessen eine öffentliche Mitteilung [16]oder eine ähnliche Maßnahme erfolgen, durch die die betroffenen Personen

auf ebenso wirksame Weise informiert werden. In diesem Fall sollte das Krankenhaus den Ransomware-Angriff und seine Auswirkungen öffentlich machen.

40. Dieser Fall dient als Beispiel für einen Ransomware-Angriff mit hohem Risiko für die Rechte und Freiheiten der betroffenen Personen. Er sollte gemäß Artikel 33 Absatz 5 dokumentiert, der Aufsichtsbehörde gemäß Artikel 331 gemeldet und den betroffenen Personen gemäß Artikel 341 mitgeteilt werden. Die Organisation muss auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Handhabung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und nachbessern.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

2.4 FALL Nr. 04: Ransomware ohne Backup und mit Exfiltration

Der Server eines öffentlichen Verkehrsunternehmens war einem Ransomware-Angriff ausgesetzt und seine Daten wurden vom Angreifer verschlüsselt. Nach den Ergebnissen der internen Untersuchung hat der Täter die Daten nicht nur verschlüsselt, sondern auch exfiltriert. Bei den verletzten Daten handelte es sich um personenbezogene Daten von Kunden und Mitarbeitern sowie von mehreren Tausend Personen, die die Dienste des Unternehmens in Anspruch nahmen (z. B. beim Online-Kauf von Tickets). Über die grundlegenden Identitätsdaten hinaus sind auch Ausweisnummern und Finanzdaten wie Kreditkartendaten von dem Verstoß betroffen. Es gab eine Backup-Datenbank, die jedoch ebenfalls vom Angreifer verschlüsselt wurde.

2.4.1 FALL Nr. 04 - Vorherige Maßnahmen und Risikobewertung

41. Der für die Verarbeitung Verantwortliche sollte dieselben vorherigen Maßnahmen ergriffen haben, wie sie in Teil und2.1. in Abschnitt
2.5. Obwohl ein Backup vorhanden war, war auch dieses von dem Angriff betroffen. Allein diese Regelung wirft Fragen über die Qualität der bisherigen IT-Sicherheitsmaßnahmen des für die Verarbeitung Verantwortlichen auf und sollte im Rahmen der Ermittlungen näher untersucht werden, da bei einem gut konzipierten Backup-System mehrere Backups sicher und ohne Zugriff vom Hauptsystem aus gespeichert werden müssen, da sie sonst bei demselben Angriff kompromittiert werden könnten. Außerdem können Ransomware-Angriffe tagelang unentdeckt bleiben, indem sie selten genutzte Daten langsam verschlüsseln. Dies kann mehrere Backups unbrauchbar machen, so dass Backups auch in regelmäßigen Abständen und isoliert erstellt werden sollten. Dies würde die Wahrscheinlichkeit einer Wiederherstellung erhöhen, auch wenn dabei mehr Daten verloren gehen.

42. Diese Verletzung betrifft nicht nur die Datenverfügbarkeit, sondern auch die Vertraulichkeit, da der Angreifer möglicherweise Daten auf dem Server geändert und/oder kopiert hat. Daher ist die Art der Verletzung mit einem hohen Risiko verbunden[17].

43. Die Art, die Sensibilität und der Umfang der personenbezogenen Daten erhöhen die Risiken zusätzlich, da die Zahl der betroffenen Personen und die Gesamtmenge der betroffenen personenbezogenen Daten hoch ist. Neben grundlegenden Identitätsdaten sind auch Ausweisdokumente und Finanzdaten wie Kreditkartendaten betroffen. Eine Datenschutzverletzung in Bezug auf diese Datenarten stellt an sich schon ein hohes Risiko dar, und wenn sie zusammen verarbeitet werden, könnten sie für folgende Zwecke verwendet werden
- unter anderem - Identitätsdiebstahl oder Betrug.

44. Aufgrund einer fehlerhaften Serverlogik oder organisatorischer Kontrollen wurden die Sicherungsdateien

von der Ransomware befallen, wodurch die Wiederherstellung der Daten verhindert und das Risiko erhöht wurde.

45. Diese Datenschutzverletzung stellt ein hohes Risiko für die Rechte und Freiheiten des Einzelnen dar, da sie wahrscheinlich sowohl zu materiellem (z. B. finanziellem Verlust, da Kreditkartendaten betroffen waren) als auch zu immateriellem Schaden (z. B. Identitätsdiebstahl oder Betrug, da Identitätskartendaten betroffen waren) führen könnte.

2.4.2 FALL Nr. 04 - Schadensminderung und Verpflichtungen

46. Die betroffenen Personen müssen unbedingt informiert werden, damit sie die notwendigen Schritte unternehmen können, um materiellen Schaden zu vermeiden (z. B. Sperrung ihrer Kreditkarten).

47. Neben der Dokumentation der Verletzung gemäß Artikel 33 Absatz 5 ist in diesem Fall auch eine Benachrichtigung der Aufsichtsbehörde obligatorisch (Artikel 33 Absatz 1), und der für die Verarbeitung Verantwortliche ist auch verpflichtet, die betroffenen Personen über die Verletzung zu informieren (Artikel 341). Letzteres könnte auf individueller Basis erfolgen, aber bei Personen, für die keine Kontaktdaten verfügbar sind, sollte der für die Verarbeitung Verantwortliche dies öffentlich tun, sofern eine solche Mitteilung keine zusätzlichen negativen Folgen für die betroffenen Personen nach sich ziehen kann, z. B. durch eine Mitteilung auf seiner Website. Im letzteren Fall ist eine präzise und klare Mitteilung erforderlich, die gut sichtbar auf der Homepage des für die Verarbeitung Verantwortlichen erscheint und genaue Hinweise auf die einschlägigen Bestimmungen der Datenschutzgrundverordnung enthält. Die Organisation muss möglicherweise auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Handhabung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und verbessern.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

2.5 Organisatorische und technische Maßnahmen zur Vorbeugung / Abschwächung der Auswirkungen von Ransomware-Angriffen

48. Die Tatsache, dass ein Ransomware-Angriff stattgefunden haben könnte, ist in der Regel ein Zeichen für eine oder mehrere Schwachstellen im System des für die Verarbeitung Verantwortlichen. Dies gilt auch für Ransomware-Fälle, in denen personenbezogene Daten zwar verschlüsselt, aber nicht exfiltriert wurden. Unabhängig vom Ausgang und den Folgen des Angriffs kann die Bedeutung einer umfassenden Bewertung des Datensicherheitssystems - mit besonderem Schwerpunkt auf der IT-Sicherheit - nicht genug betont werden. Die festgestellten Schwachstellen und Sicherheitslücken sind unverzüglich zu dokumentieren und zu beheben.

49. Empfehlenswerte Maßnahmen:

(Die Aufzählung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Ziel ist es vielmehr, Präventionsideen und mögliche Lösungen aufzuzeigen. Jede Verarbeitungstätigkeit ist anders, daher sollte der für die Verarbeitung Verantwortliche entscheiden, welche Maßnahmen für die jeweilige Situation am besten geeignet sind).

- Aktualisierung der Firmware, des Betriebssystems und der Anwendungssoftware auf den Servern, den Client-Rechnern, den aktiven Netzwerkkomponenten und allen anderen Rechnern im selben LAN (einschließlich Wi-Fi-Geräten). Sicherstellen, dass geeignete IT-Sicherheitsmaßnahmen vorhanden sind,

dass sie wirksam sind und dass sie regelmäßig aktualisiert werden, wenn sich die Verarbeitung oder die Umstände ändern oder weiterentwickeln. Dazu gehört auch die Führung detaillierter Protokolle darüber, welche Patches zu welchem Zeitpunkt angewendet wurden.

- Entwicklung und Organisation von Verarbeitungssystemen und Infrastrukturen zur Segmentierung oder Isolierung von Datensystemen und Netzwerken, um die Ausbreitung von Malware innerhalb des Unternehmens und auf externe Systeme zu verhindern.
- Das Vorhandensein eines aktuellen, sicheren und getesteten Sicherungsverfahrens. Medien für mittel- und langfristige Backups sollten von der betrieblichen Datenspeicherung getrennt und auch im Falle eines erfolgreichen Angriffs für Dritte unerreichbar aufbewahrt werden (z. B. tägliche inkrementelle Sicherung und wöchentliche Vollsicherung).
- Besitz/Beschaffung einer geeigneten, aktuellen, wirksamen und integrierten Anti-Malware-Software.
- Vorhandensein einer geeigneten, aktuellen, wirksamen und integrierten Firewall und eines Systems zur Erkennung und Verhinderung von Eindringlingen. Leiten des Netzwerkverkehrs durch die Firewall/das Intrusion Detection System, auch im Falle von Home Office oder mobiler Arbeit (z. B. durch VPN-Verbindungen zu organisatorischen Sicherheitsmechanismen beim Zugriff auf das Internet).
- Schulung der Mitarbeiter in den Methoden zur Erkennung und Verhinderung von IT-Angriffen. Der für die Verarbeitung Verantwortliche sollte Mittel bereitstellen, mit denen festgestellt werden kann, ob E-Mails und Nachrichten, die über andere Kommunikationsmittel eingehen, authentisch und vertrauenswürdig sind. Die Mitarbeiter sollten darin geschult werden, zu erkennen, wann ein solcher Angriff stattgefunden hat, wie der Endpunkt aus dem Netz genommen werden kann und dass sie verpflichtet sind, dies sofort dem Sicherheitsbeauftragten zu melden.
- Betonen Sie die Notwendigkeit, den Typ des bösartigen Codes zu identifizieren, um die Folgen des Angriffs zu erkennen und die richtigen Maßnahmen zur Risikominderung treffen zu können. Wenn ein Ransomware-Angriff erfolgreich war und keine Sicherungskopie vorhanden ist, können Tools wie die des Projekts "no more ransom" (nomoreransom.org) eingesetzt werden, um Daten wiederherzustellen. Falls jedoch ein sicheres Backup vorhanden ist, ist es ratsam, die Daten von diesem wiederherzustellen.
- Weiterleitung oder Replikation aller Protokolle an einen zentralen Protokollserver (möglicherweise einschließlich der Signierung oder kryptografischen Zeitstempelung von Protokolleinträgen).
- Starke Verschlüsselung und mehrstufige Authentifizierung, insbesondere für den administrativen Zugang zu IT-Systemen, angemessene Schlüssel- und Passwortverwaltung.
- Regelmäßige Schwachstellen- und Penetrationstests.
- Einrichtung eines Computer Security Incident Response Team (CSIRT) oder Computer Emergency Response Team (CERT) innerhalb des Unternehmens oder Beitritt zu einem kollektiven CSIRT/CERT. Erstellen Sie einen Notfallplan, einen Notfallwiederherstellungsplan und einen Geschäftskontinuitätsplan, und stellen Sie sicher, dass diese gründlich getestet werden.
- Bei der Bewertung von Gegenmaßnahmen sollte die Risikoanalyse überprüft, getestet und aktualisiert werden.

3 ANGRIFFE ZUR DATENEXFILTRATION

50. Angriffe, die Schwachstellen in Diensten ausnutzen, die der für die Verarbeitung Verantwortliche Dritten über das Internet anbietet, z. B. durch Injektionsangriffe (z. B. SQL-Injection, Path Traversal), Kompromittierung von Websites und ähnliche Methoden, können insofern Ransomware-Angriffen ähneln, als das Risiko von der Aktion eines unbefugten Dritten ausgeht, doch zielen diese Angriffe in der Regel darauf ab, personenbezogene Daten zu kopieren, zu exfiltrieren und für einen böswilligen Zweck zu missbrauchen. Es handelt sich also hauptsächlich um Verstöße gegen die Vertraulichkeit und möglicherweise auch gegen die Datenintegrität. Wenn sich der für die Verarbeitung Verantwortliche der

Merkmale dieser Art von Verstößen bewusst ist, stehen ihm zahlreiche Maßnahmen zur Verfügung, die das Risiko einer erfolgreichen Durchführung eines Angriffs erheblich verringern können.

3.1 FALL Nr. 05: Exfiltration von Bewerbungsdaten von einer Website

Ein Arbeitsvermittler wurde Opfer eines Cyberangriffs, bei dem ein bösartiger Code auf seiner Website platziert wurde. Dieser Schadcode machte personenbezogene Daten, die über Online-Bewerbungsformulare eingegeben und auf dem Webserver gespeichert wurden, für Unbefugte zugänglich. 213 solcher Formulare sind möglicherweise betroffen, aber nach der Analyse der betroffenen Daten wurde festgestellt, dass keine besonderen Datenkategorien von der Verletzung betroffen waren. Das installierte Malware-Toolkit verfügte über Funktionen, die es dem Angreifer ermöglichten, die Historie der Datenexfiltration zu löschen und die Verarbeitung auf dem Server zu überwachen und persönliche Daten zu erfassen. Das Toolkit wurde nur einen Monat nach seiner Installation entdeckt.

3.1.1 FALL Nr. 05 - Vorherige Maßnahmen und Risikobewertung

51. Die Sicherheit der Umgebung des für die Verarbeitung Verantwortlichen ist äußerst wichtig, da die meisten dieser Verstöße verhindert werden können, indem sichergestellt wird, dass alle Systeme ständig aktualisiert, sensible Daten verschlüsselt und Anwendungen nach hohen Sicherheitsstandards entwickelt werden, wie z. B. starke Authentifizierung, Maßnahmen gegen Brute-Force-Angriffe, "Flucht" oder "Bereinigung" von [18]Benutzereingaben usw. Regelmäßige IT-Sicherheitsprüfungen, Schwachstellenbewertungen und Penetrationstests sind ebenfalls erforderlich, um diese Art von Schwachstellen im Voraus zu erkennen und zu beheben. In diesem speziellen Fall hätten Tools zur Überwachung der Dateiintegrität in der Produktionsumgebung helfen können, die Code-Injektion zu entdecken. (Eine Liste empfehlenswerter Maßnahmen ist in Abschnitt 3.7 zu finden).

52. Der für die Verarbeitung Verantwortliche sollte die Untersuchung des Verstoßes immer mit der Ermittlung der Art des Angriffs und seiner Methoden beginnen, um zu beurteilen, welche Maßnahmen zu ergreifen sind. Damit dies schnell und effizient geschieht, sollte der für die Verarbeitung Verantwortliche über einen Plan zur Reaktion auf einen Vorfall verfügen, in dem die raschen und notwendigen Schritte zur Beherrschung des Vorfalls festgelegt sind. In diesem speziellen Fall war die Art des Verstoßes ein risikoerhöhender Faktor, da nicht nur die Vertraulichkeit der Daten beeinträchtigt wurde, sondern der Eindringling auch die Möglichkeit hatte, Änderungen im System vorzunehmen, so dass auch die Datenintegrität in Frage gestellt wurde.

53. Die Art, die Sensibilität und der Umfang der von der Sicherheitsverletzung betroffenen personenbezogenen Daten sollten bewertet werden, um festzustellen, in welchem Umfang die betroffenen Personen von der Sicherheitsverletzung betroffen sind. Obwohl keine besonderen Kategorien personenbezogener Daten betroffen waren, enthalten die abgerufenen Daten erhebliche Informationen über die Personen aus den Online-Formularen, und diese Daten könnten auf verschiedene Weise missbraucht werden (gezielte Werbung, Identitätsdiebstahl usw.), so dass die Schwere der Folgen das Risiko für die Rechte und Freiheiten der betroffenen[19] Personen erhöhen sollte.

3.1.2 FALL Nr. 05 - Milderung und Verpflichtungen

54. Wenn möglich, sollte die Datenbank nach der Behebung des Problems mit der in einem sicheren Backup gespeicherten Datenbank verglichen werden. Die aus der Sicherheitsverletzung gewonnenen Erfahrungen sollten bei der Aktualisierung der IT-Infrastruktur genutzt werden. Der für die Datenverarbeitung Verantwortliche sollte alle betroffenen IT-Systeme in einen bekanntermaßen sauberen Zustand versetzen, die Schwachstelle beheben und neue Sicherheitsmaßnahmen einführen, um ähnliche Datenschutzverletzungen in Zukunft zu vermeiden, z. B. Dateiintegritätsprüfungen und Sicherheitsaudits.

Wenn personenbezogene Daten nicht nur exfiltriert, sondern auch gelöscht wurden, muss der für die Verarbeitung Verantwortliche systematische Maßnahmen ergreifen, um die personenbezogenen Daten in dem Zustand wiederherzustellen, in dem sie sich vor der Verletzung befanden. Es kann erforderlich sein, vollständige Sicherungen und inkrementelle Änderungen vorzunehmen und dann möglicherweise die Verarbeitung seit der letzten inkrementellen Sicherung zu wiederholen - was voraussetzt, dass der für die Verarbeitung Verantwortliche in der Lage ist, die seit der letzten Sicherung vorgenommenen Änderungen zu replizieren. Dies könnte erfordern, dass der für die Verarbeitung Verantwortliche das System so gestaltet, dass die täglichen Eingabedateien für den Fall, dass sie erneut verarbeitet werden müssen, aufbewahrt werden, und erfordert eine robuste Speichermethode und eine geeignete Aufbewahrungsrichtlinie.

55. Da die Verletzung wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, sollten die betroffenen Personen auf jeden Fall darüber informiert werden (Artikel 34 Absatz 1), was natürlich bedeutet, dass auch die zuständige(n) Aufsichtsbehörde(n) in Form einer Meldung über die Datenschutzverletzung einbezogen werden sollten. Die Dokumentation der Datenschutzverletzung ist gemäß Artikel 33 Absatz 5 DSGVO obligatorisch und erleichtert die Bewertung der Situation.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

3.2 FALL Nr. 06: Exfiltration eines gehashten Passworts von einer Website

Eine SQL-Injection-Schwachstelle wurde ausgenutzt, um Zugriff auf eine Datenbank des Servers einer Koch-Website zu erhalten. Die Benutzer durften nur beliebige Pseudonyme als Benutzernamen wählen. Von der Verwendung von E-Mail-Adressen für diesen Zweck wurde abgeraten. Die in der Datenbank gespeicherten Passwörter wurden mit einem starken Algorithmus gehasht, und das Salt wurde nicht kompromittiert. Betroffene Daten: gehashte Passwörter von 1.200 Benutzern. Zur Sicherheit informierte der für die Verarbeitung Verantwortliche die betroffenen Personen per E-Mail über die Sicherheitsverletzung und forderte sie auf, ihre Passwörter zu ändern, insbesondere wenn das gleiche Passwort für andere Dienste verwendet wurde.

3.2.1 FALL Nr. 06 - Vorherige Maßnahmen und Risikobewertung

56. In diesem besonderen Fall ist die Vertraulichkeit der Daten gefährdet, aber die Passwörter in der Datenbank wurden mit einer aktuellen Methode gehasht, was das Risiko im Hinblick auf die Art, die Empfindlichkeit und den Umfang der personenbezogenen Daten verringern würde. Dieser Fall birgt keine Risiken für die Rechte und Freiheiten der betroffenen Personen.

57. Darüber hinaus wurden keine Kontaktinformationen (z. B. E-Mail-Adressen oder Telefonnummern) betroffener Personen kompromittiert, was bedeutet, dass für die betroffenen Personen kein erhebliches Risiko besteht, Opfer von Betrugsversuchen zu werden (z. B. Erhalt von Phishing-E-Mails oder betrügerischen Textnachrichten und Anrufen). Es waren keine besonderen Kategorien von personenbezogenen Daten betroffen.

58. Einige Benutzernamen könnten als personenbezogene Daten betrachtet werden, aber das Thema der Website lässt keine negativen Assoziationen zu. Es ist jedoch zu beachten, dass sich die Risikobewertung ändern[20] kann, wenn die Art der Website und die Daten, auf die zugegriffen wird, besondere Kategorien personenbezogener Daten offenbaren könnten (z. B. die Website einer politischen Partei oder einer Gewerkschaft). Die Verwendung einer modernen Verschlüsselung könnte die nachteiligen Auswirkungen

der Sicherheitsverletzung abmildern. Wenn sichergestellt wird, dass nur eine begrenzte Anzahl von Anmeldeversuchen zulässig ist, wird verhindert, dass Brute-Force-Angriffe erfolgreich sind, wodurch das Risiko, dass Angreifer die Benutzernamen bereits kennen, weitgehend verringert wird.

3.2.2 FALL Nr. 06 - Milderung und Verpflichtungen

59. Die Benachrichtigung der betroffenen Personen könnte in einigen Fällen als mildernder Umstand angesehen werden, da die betroffenen Personen auch in der Lage sind, die notwendigen Schritte zu unternehmen, um weitere Schäden durch die Sicherheitsverletzung zu vermeiden, indem sie zum Beispiel ihr Passwort ändern. In diesem Fall war die Benachrichtigung nicht obligatorisch, kann aber in vielen Fällen als gute Praxis angesehen werden.

60. Der für die Verarbeitung Verantwortliche sollte die Schwachstelle beheben und neue Sicherheitsmaßnahmen ergreifen, um ähnliche Datenschutzverletzungen in Zukunft zu vermeiden, z. B. systematische Sicherheitsaudits der Website.

61. Der Verstoß sollte gemäß Artikel 33 Absatz 5 dokumentiert werden, eine Benachrichtigung oder Mitteilung ist jedoch nicht erforderlich.

62. Außerdem ist es in jedem Fall ratsam, die betroffenen Personen über eine Verletzung des Schutzes von Passwörtern zu informieren, auch wenn die Passwörter unter Verwendung eines gesalzenen Hashwerts mit einem Algorithmus gespeichert wurden, der dem Stand der Technik entspricht. Die Verwendung von Authentifizierungsmethoden, die die Verarbeitung von Passwörtern auf der Serverseite überflüssig machen, ist vorzuziehen. Die betroffenen Personen sollten die Möglichkeit haben, geeignete Maßnahmen in Bezug auf ihre eigenen Passwörter zu ergreifen.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen
	X	X

3.3 FALL Nr. 07: Credential-Stuffing-Angriff auf eine Bank-Website

Eine Bank wurde Opfer eines Cyberangriffs auf eine ihrer Online-Banking-Webseiten. Ziel des Angriffs war es, alle möglichen Benutzerkennungen mit einem festgelegten trivialen Kennwort zu ermitteln. Die Passwörter bestehen aus 8 Ziffern. Aufgrund einer Schwachstelle in der Website wurden in einigen Fällen Informationen über betroffene Personen (Name, Vorname, Geschlecht, Geburtsdatum und -ort, Steuernummer, Benutzerkennungen) an den Angreifer weitergegeben, auch wenn das verwendete Passwort nicht korrekt oder das Bankkonto nicht mehr aktiv war. Dies betraf etwa 100.000 betroffene Personen. Von diesen loggte sich der Angreifer erfolgreich in etwa 2.000 Konten ein, die das vom Angreifer versuchte Trivialpasswort benutzten. Im Nachhinein war der für die Verarbeitung Verantwortliche in der Lage, alle unrechtmäßigen Anmeldeversuche zu identifizieren. Der für die Verarbeitung Verantwortliche konnte bestätigen, dass laut Betrugsbekämpfungsprüfungen während des Angriffs keine Transaktionen von diesen Konten durchgeführt wurden. Die Bank war sich der Datenschutzverletzung bewusst, da ihr Sicherheitszentrum eine hohe Anzahl von Login-Anfragen auf der Website feststellte. Als Reaktion darauf deaktivierte der für die Verarbeitung Verantwortliche die Möglichkeit, sich auf der Website anzumelden, indem er sie ausschaltete, und erzwang die Zurücksetzung der Passwörter der kompromittierten Konten. Der für die Verarbeitung Verantwortliche teilte die Sicherheitsverletzung nur den Nutzern mit, deren Konten kompromittiert wurden, d. h. den Nutzern, deren Passwörter kompromittiert wurden oder deren Daten offengelegt wurden.

3.3.1 FALL Nr. 07 - Vorherige Maßnahmen und Risikobewertung

63. Es ist wichtig zu erwähnen, dass für die Verarbeitung Verantwortliche, die mit sehr persönlichen Daten umgehen[21], eine größere Verantwortung für die Gewährleistung einer angemessenen Datensicherheit haben, z. B. durch ein Sicherheitszentrum und andere Maßnahmen zur Vorbeugung, Aufdeckung und Reaktion auf Vorfälle. Die Nichteinhaltung dieser höheren Standards wird mit Sicherheit zu ernsteren Maßnahmen bei der Untersuchung durch eine ORKB führen.

64. Die Sicherheitsverletzung betrifft nicht nur Finanzdaten, sondern auch Identitäts- und Benutzer-ID-Informationen, was sie besonders schwerwiegend macht. Die Zahl der betroffenen Personen ist hoch.

65. Die Tatsache, dass es in einem so sensiblen Umfeld zu einer Sicherheitsverletzung kommen konnte, deutet auf erhebliche Datensicherheitslücken im System des für die Verarbeitung Verantwortlichen hin und kann ein Indikator für einen Zeitpunkt sein, an dem die Überprüfung und Aktualisierung der betroffenen Maßnahmen gemäß Artikel (241), (251) und (321) der Datenschutz-Grundverordnung "erforderlich" ist. Die verletzten Daten ermöglichen die eindeutige Identifizierung der betroffenen Personen und enthalten weitere Informationen über sie (einschließlich Geschlecht, Geburtsdatum und -ort); außerdem können sie vom Angreifer verwendet werden, um die Passwörter der Kunden zu erraten oder eine an die Bankkunden gerichtete Spear-Phishing-Kampagne durchzuführen.

66. Aus diesen Gründen wurde davon ausgegangen, dass die Datenschutzverletzung wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten aller betroffenen Personen führen würde[22]. Daher ist das Auftreten von materiellem (z. B. finanziellem Verlust) und immateriellem Schaden (z. B. Identitätsdiebstahl oder Betrug) ein denkbares Ergebnis.

3.3.2 FALL Nr. 07 - Schadensminderung und Verpflichtungen

67. Die in der Fallbeschreibung genannten Maßnahmen des für die Verarbeitung Verantwortlichen sind angemessen. Nach der Sicherheitsverletzung hat er auch die Schwachstelle auf der Website behoben und weitere Schritte unternommen, um ähnliche Datenschutzverletzungen in Zukunft zu verhindern, wie z. B. das Hinzufügen einer Zwei-Faktor-Authentifizierung auf der betroffenen Website und die Umstellung auf eine starke Kundenauthentifizierung.

68. Die Dokumentation der Sicherheitsverletzung gemäß Artikel 33 Absatz 5 DSGVO und die Benachrichtigung der Aufsichtsbehörde sind in diesem Szenario nicht optional. Darüber hinaus sollte der für die Verarbeitung Verantwortliche alle 100.000betroffenen Personen (einschließlich der betroffenen Personen, deren Konten nicht kompromittiert wurden) gemäß Artikel 34 DSGVO benachrichtigen.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

3.4 Organisatorische und technische Maßnahmen zur Vorbeugung / Abschwächung der Auswirkungen von Hackerangriffen

69. Wie im Falle von Ransomware-Angriffen ist eine Neubewertung der IT-Sicherheit für die für die Verarbeitung Verantwortlichen in ähnlichen Fällen unabhängig vom Ergebnis und den Folgen des Angriffs obligatorisch.

70. Empfehlenswerte Maßnahmen:[23]

(*Die Aufzählung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Ziel ist es vielmehr, Präventionsideen und mögliche Lösungen aufzuzeigen. Jede Verarbeitungstätigkeit ist anders, daher sollte der für die Verarbeitung Verantwortliche entscheiden, welche Maßnahmen für die jeweilige Situation am besten geeignet sind*).

- Verschlüsselung und Schlüsselverwaltung auf dem neuesten Stand der Technik, insbesondere bei der Verarbeitung von Passwörtern, sensiblen oder finanziellen Daten. Kryptographisches Hashing und Salting für geheime Informationen (Passwörter) ist immer der Verschlüsselung von Passwörtern vorzuziehen. Die Verwendung von Authentifizierungsmethoden, die die Verarbeitung von Passwörtern auf der Serverseite überflüssig machen, ist vorzuziehen.
- Das System auf dem neuesten Stand halten (Software und Firmware). Sicherstellung, dass alle IT-Sicherheitsmaßnahmen vorhanden sind, dass sie wirksam sind und dass sie regelmäßig aktualisiert werden, wenn sich die Verarbeitung oder die Umstände ändern oder weiterentwickeln. Um die Einhaltung von Artikel 5 Absatz 1 Buchstabe f gemäß Artikel 5 Absatz 2 DSGVO nachweisen zu können, sollte der für die Verarbeitung Verantwortliche Aufzeichnungen über alle durchgeführten Aktualisierungen führen, einschließlich des Zeitpunkts, zu dem sie vorgenommen wurden.
- Einsatz starker Authentifizierungsmethoden wie Zwei-Faktor-Authentifizierung und Authentifizierungsserver, ergänzt durch eine aktuelle Passwortpolitik.
- Zu den Standards für eine sichere Entwicklung gehören die Filterung von Benutzereingaben (soweit möglich unter Verwendung von Whitelists), die Umgehung von Benutzereingaben und Maßnahmen zur Verhinderung von Brute-Force-Eingaben (z. B. Begrenzung der maximalen Anzahl von Wiederholungsversuchen). "Web Application Firewalls" können bei der wirksamen Anwendung dieser Technik helfen.
- Strenge Richtlinien für die Verwaltung von Benutzerrechten und Zugriffskontrolle.
- Einsatz geeigneter, aktueller, wirksamer und integrierter Firewall-, Intrusion-Detection- und anderer Perimeterschutzsysteme.
- Systematische IT-Sicherheitsprüfungen und Schwachstellenbewertungen (Penetrationstests).
- Regelmäßige Überprüfungen und Tests, um sicherzustellen, dass Backups zur Wiederherstellung von Daten, deren Integrität oder Verfügbarkeit beeinträchtigt wurde, verwendet werden können.
- Keine Sitzungs-ID in der URL im Klartext.

4 INTERNE MENSCHLICHE RISIKOQUELLE

71. Die Rolle des menschlichen Versagens bei Verstößen gegen den Schutz personenbezogener Daten muss hervorgehoben werden, da sie häufig vorkommt. Da diese Art von Verstößen sowohl absichtlich als auch unabsichtlich erfolgen kann, ist es für die für die Datenverarbeitung Verantwortlichen sehr schwierig, die Schwachstellen zu erkennen und Maßnahmen zu ihrer Vermeidung zu ergreifen. Die Internationale Konferenz der Datenschutzbeauftragten hat erkannt, wie wichtig es ist, sich mit solchen menschlichen Faktoren zu befassen, und im Oktober eine Entschließung zur Rolle menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten angenommen2019[24]. In dieser Entschließung wird betont, dass geeignete Schutzmaßnahmen ergriffen werden sollten, um menschliches Versagen zu verhindern, und sie enthält eine nicht erschöpfende Liste solcher Schutzmaßnahmen und Ansätze.

4.1 FALL Nr. 08: Exfiltration von Geschäftsdaten durch einen Mitarbeiter

Der Mitarbeiter eines Unternehmens kopiert während seiner Kündigungsfrist Geschäftsdaten aus der Datenbank des Unternehmens. Der Angestellte ist nur zur Erfüllung seiner Aufgaben berechtigt, auf die Daten zuzugreifen. Monate später, nachdem er gekündigt hat, nutzt er die so gewonnenen Daten (grundlegende Kontaktdaten), um eine neue Datenverarbeitung zu speisen, für die er der Verantwortliche ist, um die Kunden des Unternehmens zu kontaktieren und sie für sein neues Geschäft zu gewinnen.

4.1.1 FALL Nr. 08 - Vorherige Maßnahmen und Risikobewertung

72. In diesem speziellen Fall wurden keine vorherigen Maßnahmen ergriffen, um zu verhindern, dass der

Angestellte Kontaktinformationen der Kunden des Unternehmens kopiert, da er für seine Aufgaben legitimen Zugang zu diesen Informationen brauchte - und hatte. Da die meisten Aufgaben im Bereich der Kundenbetreuung in irgendeiner Form den Zugriff der Mitarbeiter auf personenbezogene Daten erfordern, lassen sich diese Datenverstöße möglicherweise am schwersten verhindern. Beschränkungen des Zugriffs können die Arbeit des betreffenden Mitarbeiters einschränken. Gut durchdachte Zugriffsrichtlinien und eine ständige Kontrolle können jedoch dazu beitragen, solche Verstöße zu verhindern.

73. Wie üblich sind bei der Risikobewertung die Art der Verletzung sowie die Art, die Sensibilität und der Umfang der betroffenen personenbezogenen Daten zu berücksichtigen. Bei dieser Art von Verstößen handelt es sich in der Regel um Verstöße gegen die Vertraulichkeit, da die Datenbank in der Regel unversehrt bleibt und ihr Inhalt "lediglich" zur weiteren Verwendung kopiert wird. Auch die Menge der betroffenen Daten ist in der Regel gering oder mittelgroß. Im vorliegenden Fall waren keine besonderen Kategorien personenbezogener Daten betroffen, der Mitarbeiter benötigte lediglich die Kontaktinformationen von Kunden, um nach seinem Ausscheiden aus dem Unternehmen mit ihnen in Verbindung treten zu können. Die betroffenen Daten sind daher nicht sensibel.

74. Auch wenn sich das einzige Ziel des ehemaligen Mitarbeiters, der die Daten böswillig kopiert hat, darauf beschränken mag, die Kontaktdaten der Kunden des Unternehmens für seine eigenen kommerziellen Zwecke zu erlangen, kann der für die Verarbeitung Verantwortliche das Risiko für die betroffenen Personen nicht als gering einstufen, da er keine Gewissheit über die Absichten des Mitarbeiters hat. Während sich die Folgen des Verstoßes auf die unangemessene Selbstvermarktung des ehemaligen Mitarbeiters beschränken könnten, ist ein weiterer und schwerwiegenderer Missbrauch der gestohlenen Daten nicht ausgeschlossen, je nach dem Zweck der von dem ehemaligen Mitarbeiter vorgenommenen Verarbeitung[25].

4.1.2 FALL Nr. 08 - Schadensminderung und Verpflichtungen

75. Die Milderung der nachteiligen Auswirkungen des Verstoßes in dem oben genannten Fall ist schwierig. Möglicherweise müssen sofortige rechtliche Schritte eingeleitet werden, um den ehemaligen Mitarbeiter daran zu hindern, die Daten weiter zu missbrauchen und zu verbreiten. In einem nächsten Schritt sollte das Ziel darin bestehen, ähnliche Situationen in Zukunft zu vermeiden. Der für die Verarbeitung Verantwortliche könnte versuchen, den ehemaligen Mitarbeiter anzuweisen, die Verwendung der Daten einzustellen, aber der Erfolg dieser Maßnahme ist bestenfalls zweifelhaft. Geeignete technische Maßnahmen wie die Unmöglichkeit des Kopierens oder Herunterladens von Daten auf Wechseldatenträger können helfen.

76. Es gibt keine "Einheitslösung" für diese Art von Fällen, aber ein systematischer Ansatz kann helfen, sie zu verhindern. So kann das Unternehmen beispielsweise in Erwägung ziehen - wenn möglich - Mitarbeitern, die ihre Kündigungsabsicht bekundet haben, bestimmte Formen des Zugangs zu entziehen oder Zugangsprotokolle zu erstellen, damit unerwünschte Zugriffe protokolliert und gekennzeichnet werden können. Der mit den Mitarbeitern geschlossene Vertrag sollte Klauseln enthalten, die solche Handlungen untersagen.

77. Da die betreffende Verletzung kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, reicht eine Meldung an die Aufsichtsbehörde aus. Die Unterrichtung der betroffenen Personen könnte jedoch auch für den für die Verarbeitung Verantwortlichen von Vorteil sein, da es besser sein könnte, dass sie von dem Unternehmen über das Datenleck erfahren als von dem ehemaligen Mitarbeiter, der versucht, sie zu kontaktieren. Dokumentation von Datenschutzverletzungen gemäß Artikel 33
(5) ist eine gesetzliche Verpflichtung.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen
		X

4.2 FALL Nr. 09: Versehentliche Übermittlung von Daten an eine vertrauenswürdige dritte Person

Ein Versicherungsvertreter stellte fest, dass er aufgrund der fehlerhaften Einstellungen einer per E-Mail erhaltenen Excel-Datei Zugang zu Informationen über zwei Dutzend Kunden hatte, die nicht zu seinem Zuständigkeitsbereich gehörten. Er ist an das Berufsgeheimnis gebunden und war der einzige Empfänger der E-Mail. Die Vereinbarung zwischen dem für die Verarbeitung Verantwortlichen und dem Versicherungsvertreter verpflichtet den Vertreter, dem für die Verarbeitung Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich zu melden. Daher meldete der Vertreter den Fehler unverzüglich dem für die Verarbeitung Verantwortlichen, der die Datei korrigierte und sie erneut verschickte, wobei er den Vertreter aufforderte, die frühere Nachricht zu löschen. Gemäß der oben genannten Vereinbarung muss der Beauftragte die Löschung in einer schriftlichen Erklärung bestätigen, was er auch tat. Die gewonnenen Informationen umfassen keine besonderen Kategorien personenbezogener Daten, sondern lediglich Kontaktdaten und Daten über die Versicherung selbst (Versicherungsart, Betrag). Nach der Analyse der von der Verletzung betroffenen personenbezogenen Daten stellte der für die Verarbeitung Verantwortliche keine besonderen Merkmale auf Seiten der Personen oder des für die Verarbeitung Verantwortlichen fest, die das Ausmaß der Auswirkungen der Verletzung beeinflussen könnten.

4.2.1 FALL Nr. 09 - Vorherige Maßnahmen und Risikobewertung

78. Hier ist der Verstoß nicht auf eine vorsätzliche Handlung eines Mitarbeiters zurückzuführen, sondern auf einen unbeabsichtigten menschlichen Fehler, der durch Unachtsamkeit verursacht wurde. Diese Art von Verstößen kann vermieden oder in ihrer Häufigkeit verringert werden, indem a) Schulungs-, Aufklärungs- und Sensibilisierungsprogramme durchgesetzt werden, in denen die Mitarbeiter ein besseres Verständnis für die Bedeutung des Schutzes personenbezogener Daten erlangen, b) der Dateiaustausch per E-Mail reduziert wird und stattdessen z. B. spezielle Systeme für die Verarbeitung von Kundendaten verwendet werden, c) Dateien vor dem Versand doppelt geprüft werden, d) die Erstellung und der Versand von Dateien getrennt werden.

79. Diese Datenschutzverletzung betrifft nur die Vertraulichkeit der Daten, die Integrität und die Zugänglichkeit der Daten bleiben unangetastet. Die Datenverletzung betraf nur etwa zwei Dutzend Kunden, so dass die Menge der betroffenen Daten als gering angesehen werden kann. Außerdem enthalten die betroffenen personenbezogenen Daten keine sensiblen Daten. Die Tatsache, dass der Datenverarbeiter den für die Verarbeitung Verantwortlichen unverzüglich nach Bekanntwerden der Datenschutzverletzung kontaktiert hat, kann als risikomindernder Faktor betrachtet werden. (Die Möglichkeit, dass Daten an andere Versicherungsvertreter übermittelt wurden, sollte ebenfalls geprüft werden, und falls sich dies bestätigt, sollten geeignete Maßnahmen ergriffen werden). Aufgrund der angemessenen Maßnahmen, die nach der Datenschutzverletzung ergriffen wurden, wird diese wahrscheinlich keine Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen haben.

80. Die Kombination aus der geringen Anzahl der betroffenen Personen, der sofortigen Entdeckung der Sicherheitsverletzung und den Maßnahmen, die zur Minimierung der Auswirkungen ergriffen wurden, machen diesen besonderen Fall zu einem Risiko.

4.2.2 FALL Nr. 09 - Milderung und Verpflichtungen

81. Darüber hinaus spielen auch andere risikomindernde Umstände eine Rolle: Der Bedienstete ist an das Berufsgeheimnis gebunden, er selbst hat das Problem dem für die Verarbeitung Verantwortlichen gemeldet und die Datei auf Anfrage gelöscht. Eine Sensibilisierung und möglicherweise zusätzliche Schritte bei der Überprüfung von Dokumenten mit personenbezogenen Daten werden wahrscheinlich dazu beitragen,

ähnliche Fälle in Zukunft zu vermeiden.

82. Außer der Dokumentation des Verstoßes gemäß Artikel 33 Absatz 5 sind keine weiteren Maßnahmen erforderlich.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen
	X	X

4.3 Organisatorische und technische Maßnahmen zur Vermeidung/Minderung der Auswirkungen interner menschlicher Risikoquellen

83. Eine Kombination der unten genannten Maßnahmen - die je nach den Besonderheiten des Falles angewandt werden - sollte dazu beitragen, die Wahrscheinlichkeit eines erneuten Verstoßes zu verringern.

84. Empfehlenswerte Maßnahmen:

(*Die Aufzählung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Ziel ist es vielmehr, Präventionsideen und mögliche Lösungen aufzuzeigen. Jede Verarbeitungstätigkeit ist anders, daher sollte der für die Verarbeitung Verantwortliche entscheiden, welche Maßnahmen für die jeweilige Situation am besten geeignet sind.*)

- Regelmäßige Durchführung von Schulungs-, Aufklärungs- und Sensibilisierungsprogrammen für Mitarbeiter in Bezug auf ihre Datenschutz- und Sicherheitspflichten sowie die Erkennung und Meldung von Bedrohungen für die Sicherheit personenbezogener Daten[26]. Entwicklung eines Sensibilisierungsprogramms, um die Mitarbeiter an die häufigsten Fehler zu erinnern, die zu Verletzungen des Schutzes personenbezogener Daten führen, und daran, wie diese vermieden werden können.
- Einführung solider und wirksamer Praktiken, Verfahren und Systeme[27] zum Schutz von Daten und Privatsphäre.
- Evaluierung der Datenschutzpraktiken, -verfahren und -systeme, um eine kontinuierliche Wirksamkeit[28] zu gewährleisten.
- Festlegung angemessener Zugangskontrollrichtlinien und Erzwingen der Einhaltung der Regeln durch die Benutzer.
- Anwendung von Techniken zur Erzwingung der Benutzerauthentifizierung beim Zugriff auf sensible persönliche Daten.
- Deaktivierung des unternehmensbezogenen Kontos des Benutzers, sobald die Person das Unternehmen verlässt.
- Überprüfung des ungewöhnlichen Datenflusses zwischen dem Dateiserver und den Arbeitsplätzen der Mitarbeiter.
- Einrichtung der E/A-Schnittstellensicherheit im BIOS oder durch den Einsatz von Software, die die Verwendung von Computerschnittstellen kontrolliert (Sperren oder Entsperren z. B. von USB/CD/DVD usw.).
- Überprüfung der Zugriffsrichtlinien der Mitarbeiter (z. B. Protokollierung des Zugriffs auf sensible Daten und Verpflichtung des Benutzers zur Eingabe eines geschäftlichen Grundes, damit dieser für Audits zur Verfügung steht).
- Deaktivierung offener Cloud-Dienste.
- Verbot und Verhinderung des Zugangs zu bekannten offenen Postdiensten.
- Deaktivierung der Funktion "Bildschirm drucken" in OS.
- Durchsetzung einer Clean-Desk-Politik.
- Automatisches Sperren aller Computer nach einer bestimmten Zeit der Inaktivität.

- Verwendung von Mechanismen (z. B. (drahtloses) Token zur Anmeldung/zum Öffnen gesperrter Konten) für schnelle Benutzerwechsel in gemeinsam genutzten Umgebungen.
- Verwendung spezieller Systeme für die Verwaltung personenbezogener Daten, die geeignete Zugangskontrollmechanismen anwenden und menschliche Fehler, wie das Versenden von Mitteilungen an die falsche Person, verhindern. Die Verwendung von Tabellenkalkulationen und anderen Bürodokumenten ist kein geeignetes Mittel zur Verwaltung von Kundendaten.

5 VERLORENE ODER GESTOHLENE GERÄTE UND PAPIERDOKUMENTE

85. Ein häufiger Fall ist der Verlust oder Diebstahl von tragbaren Geräten. In diesen Fällen muss der für die Verarbeitung Verantwortliche die Umstände des Verarbeitungsvorgangs berücksichtigen, z. B. die Art der auf dem Gerät gespeicherten Daten sowie die unterstützenden Anlagen und die vor der Verletzung getroffenen Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus. All diese Elemente wirken sich auf die potenziellen Auswirkungen der Datenverletzung aus. Die Risikobewertung könnte sich als schwierig erweisen, da das Gerät nicht mehr verfügbar ist.

86. Diese Art von Verstößen kann immer als Verstoß gegen die Vertraulichkeit eingestuft werden. Wenn es jedoch keine Sicherungskopie der gestohlenen Datenbank gibt, kann es sich auch um eine Verletzung der Verfügbarkeit und der Integrität handeln.

87. Die nachstehenden Szenarien zeigen, wie die oben genannten Umstände die Wahrscheinlichkeit und Schwere einer Datenschutzverletzung beeinflussen.

5.1 FALL Nr. 10: Gestohlenes Material mit verschlüsselten personenbezogenen Daten

Bei einem Einbruch in eine Kindertagesstätte wurden zwei Tablets gestohlen. Auf den Tablets befand sich eine App, die personenbezogene Daten über die Kinder, die die Kindertagesstätte besuchen, enthielt. Es handelte sich um Namen, Geburtsdaten und persönliche Daten über die Ausbildung der Kinder. Sowohl die verschlüsselten Tablets, die zum Zeitpunkt des Einbruchs ausgeschaltet waren, als auch die App waren durch ein starkes Passwort geschützt. Back-up-Daten standen dem für die Verarbeitung Verantwortlichen tatsächlich und ohne Weiteres zur Verfügung. Nachdem die Kindertagesstätte von dem Einbruch erfahren hatte, gab sie kurz nach der Entdeckung des Einbruchs aus der Ferne den Befehl, die Tablets zu löschen.

5.1.1 FALL Nr. 10 - Vorherige Maßnahmen und Risikobewertung

88. In diesem speziellen Fall hat der für die Verarbeitung Verantwortliche angemessene Maßnahmen ergriffen, um die Auswirkungen einer potenziellen Datenschutzverletzung zu verhindern und abzumildern, indem er das Gerät verschlüsselte, einen angemessenen Passwortschutz einführte und eine Sicherungskopie der auf den Tablets gespeicherten Daten anfertigte. (Eine Liste ratsamer Maßnahmen ist in Abschnitt 5.7 zu finden).

89. Nach Bekanntwerden einer Datenschutzverletzung sollte der für die Verarbeitung Verantwortliche die Risikoquelle, die Systeme zur Unterstützung der Datenverarbeitung, die Art der betroffenen personenbezogenen Daten und die möglichen Auswirkungen der Datenschutzverletzung auf die betroffenen Personen bewerten. Die oben beschriebene Datenschutzverletzung hätte die Vertraulichkeit, die Verfügbarkeit und die Integrität der betroffenen Daten betroffen, doch aufgrund der angemessenen Maßnahmen des für die Verarbeitung Verantwortlichen vor und nach der Datenschutzverletzung ist keines dieser Probleme aufgetreten.

5.1.2 FALL Nr. 10 - Schadensminderung und Verpflichtungen

90. Die Vertraulichkeit der persönlichen Daten auf den Geräten war aufgrund des starken Passwortschutzes sowohl auf den Tablets als auch auf den Apps nicht gefährdet. Die Tablets waren so eingerichtet, dass das Festlegen eines Passworts auch bedeutet, dass die Daten auf dem Gerät verschlüsselt sind. Dies wurde noch dadurch verstärkt, dass der Kontrolleur versuchte, alles von den gestohlenen Geräten aus der Ferne zu löschen.

91. Aufgrund der getroffenen Maßnahmen blieb auch die Vertraulichkeit der Daten gewahrt. Außerdem gewährleistete die Sicherung die ständige Verfügbarkeit der personenbezogenen Daten, so dass keine potenziellen negativen Auswirkungen eintreten konnten.

92. Aufgrund dieser Tatsachen war es unwahrscheinlich, dass die oben beschriebene Datenschutzverletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führte, weshalb keine Benachrichtigung der ORKB oder der betroffenen Personen erforderlich war. Allerdings muss auch diese Datenverletzung gemäß Artikel 33 Absatz 5 dokumentiert werden.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen
	X	**X**

5.2 FALL Nr. 11: Gestohlenes Material mit unverschlüsselten personenbezogenen Daten

Das elektronische Notebook eines Mitarbeiters eines Dienstleistungsunternehmens wurde gestohlen. Das gestohlene Notebook enthielt Namen, Vornamen, Geschlecht, Adressen und Geburtsdaten von mehr als 100000 Kunden. Da das gestohlene Gerät nicht mehr verfügbar war, konnte nicht festgestellt werden, ob auch andere Kategorien personenbezogener Daten betroffen waren. Der Zugriff auf die Festplatte des Notebooks war nicht durch ein Passwort geschützt. Die persönlichen Daten konnten aus den täglich verfügbaren Backups wiederhergestellt werden.

5.2.1 FALL Nr. 11 - Vorherige Maßnahmen und Risikobewertung

93. Da der für die Verarbeitung Verantwortliche keine vorherigen Sicherheitsmaßnahmen ergriffen hatte, waren die auf dem gestohlenen Notebook gespeicherten personenbezogenen Daten für den Dieb oder jede andere Person, die später in den Besitz des Geräts kam, leicht zugänglich.

94. Diese Datenschutzverletzung betrifft die Vertraulichkeit der auf dem gestohlenen Gerät gespeicherten Daten.

95. Das Notebook, auf dem sich die personenbezogenen Daten befanden, war in diesem Fall angreifbar, da es weder über einen Passwortschutz noch über eine Verschlüsselung verfügte. Das Fehlen grundlegender Sicherheitsmaßnahmen erhöht das Risikoniveau für die betroffenen Personen. Darüber hinaus ist auch die Identifizierung der betroffenen Personen problematisch, was ebenfalls die Schwere der Sicherheitsverletzung erhöht. Die beträchtliche Anzahl der betroffenen Personen erhöht das Risiko, dennoch waren keine besonderen Kategorien personenbezogener Daten von der Datenverletzung betroffen.

96. Bei der Risikobewertung sollte [29]der für die Verarbeitung Verantwortliche die möglichen Folgen und nachteiligen Auswirkungen der Verletzung der Vertraulichkeit berücksichtigen. Infolge der Verletzung der Vertraulichkeit können die betroffenen Personen Opfer eines Identitätsbetrugs werden, der sich auf die auf dem gestohlenen Gerät vorhandenen Daten stützt, so dass das Risiko als hoch einzustufen ist.

5.2.2 FALL Nr. 11 - Schadensminderung und Verpflichtungen

97. Durch die Aktivierung der Geräteverschlüsselung und die Verwendung eines starken Passwortschutzes für die gespeicherte Datenbank hätte verhindert werden können, dass die Datenverletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

98. Aufgrund dieser Umstände ist die Benachrichtigung der Aufsichtsbehörde erforderlich, und auch die betroffenen Personen müssen benachrichtigt werden.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

5.3 FALL Nr. 12: Gestohlene Papierakten mit sensiblen Daten

Aus einer Reha-Einrichtung für Drogenabhängige wurde ein Logbuch in Papierform gestohlen. Das Buch enthielt grundlegende Identitäts- und Gesundheitsdaten der Patienten, die in die Reha-Einrichtung eingewiesen wurden. Die Daten waren nur auf Papier gespeichert, und den behandelnden Ärzten stand keine Sicherungskopie zur Verfügung. Das Buch wurde nicht in einer verschlossenen Schublade oder einem Raum aufbewahrt, und der für die Datenverarbeitung Verantwortliche verfügte weder über ein Zugangskontrollsystem noch über andere Sicherungsmaßnahmen für die Papierdokumentation.

5.3.1 FALL Nr. 12 - Vorherige Maßnahmen und Risikobewertung

99. Der für die Verarbeitung Verantwortliche hat keine vorherigen Sicherheitsmaßnahmen getroffen, so dass die in diesem Buch gespeicherten personenbezogenen Daten für die Person, die es gefunden hat, leicht zugänglich waren. Außerdem macht die Art der in dem Buch gespeicherten personenbezogenen Daten das Fehlen von Sicherungsdaten zu einem sehr ernsten Risikofaktor.

100. Dieser Fall dient als Beispiel für eine hochriskante Datenverletzung. Aufgrund des Versagens angemessener Sicherheitsvorkehrungen gingen sensible Gesundheitsdaten gemäß Artikel (91) der DSGVO verloren. Da es sich in diesem Fall um eine besondere Kategorie personenbezogener Daten handelte, war das potenzielle Risiko für die betroffenen Personen erhöht, was von dem für die Verarbeitung Verantwortlichen bei der Risikobewertung ebenfalls berücksichtigt werden sollte[30].

101. Diese Verletzung betrifft die Vertraulichkeit, Verfügbarkeit und Integrität der betroffenen personenbezogenen Daten. Durch die Verletzung der Vertraulichkeit wird die ärztliche Schweigepflicht gebrochen, und unbefugte Dritte können Zugang zu den privaten medizinischen Informationen der Patienten erhalten, was schwerwiegende Auswirkungen auf das persönliche Leben der Patienten haben kann. Die Verletzung der Verfügbarkeit kann auch die Kontinuität der Behandlung der Patienten stören. Da die Änderung/Löschung von Teilen des Buchinhalts nicht ausgeschlossen werden kann, ist auch die Integrität der personenbezogenen Daten gefährdet.

5.3.2 FALL Nr. 12 - Milderung und Verpflichtungen

102. Bei der Bewertung der Sicherungsmaßnahmen sollte auch die Art des unterstützenden Gutes berücksichtigt werden. Da das Patiententagebuch ein physisches Dokument war, hätte seine Sicherung anders organisiert werden müssen als die eines elektronischen Geräts. Die Pseudonymisierung der Patientennamen, die Aufbewahrung des Buches in einem gesicherten Raum und in einer verschlossenen Schublade oder einem Zimmer sowie eine angemessene Zugangskontrolle mit Authentifizierung beim Zugriff auf das Buch hätten die Datenverletzung verhindern können.

103. Die oben beschriebene Datenschutzverletzung kann schwerwiegende Auswirkungen auf die betroffenen Personen haben; daher ist die Benachrichtigung der Aufsichtsbehörde und die Mitteilung der Verletzung an die betroffenen Personen obligatorisch.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

5.4 Organisatorische und technische Maßnahmen zur Verhinderung/Minderung der Auswirkungen von Verlust oder Diebstahl von Geräten

104. Eine Kombination der unten genannten Maßnahmen - die je nach den Besonderheiten des Falles angewandt werden - sollte dazu beitragen, die Wahrscheinlichkeit eines erneuten Verstoßes zu verringern.

105. Empfehlenswerte Maßnahmen:

(*Die Aufzählung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Ziel ist es vielmehr, Präventionsideen und mögliche Lösungen aufzuzeigen. Jede Verarbeitungstätigkeit ist anders, daher sollte der für die Verarbeitung Verantwortliche entscheiden, welche Maßnahmen für die jeweilige Situation am besten geeignet sind.*)

- Aktivieren Sie die Verschlüsselung des Geräts (z. B. Bitlocker, Veracrypt oder DM-Crypt).
- Verwenden Sie auf allen Geräten einen Passcode/Passwort. Verschlüsseln Sie alle mobilen elektronischen Geräte so, dass zur Entschlüsselung die Eingabe eines komplexen Passworts erforderlich ist.
- Verwenden Sie eine mehrstufige Authentifizierung.
- Schalten Sie die Funktionen hochmobiler Geräte ein, mit denen sie bei Verlust oder Verlegung geortet werden können.
- Verwenden Sie MDM (Mobile Devices Management) Software/App und Lokalisierung. Verwenden Sie Blendschutzfilter. Schließen Sie alle unbeaufsichtigten Geräte.
- Wenn möglich und für die jeweilige Datenverarbeitung angemessen, speichern Sie personenbezogene Daten nicht auf einem mobilen Gerät, sondern auf einem zentralen Back-End-Server.
- Wenn der Arbeitsplatz mit dem Firmen-LAN verbunden ist, führen Sie eine automatische Sicherung von den Arbeitsordnern durch, sofern es unvermeidlich ist, dass dort persönliche Daten gespeichert sind.
- Verwenden Sie ein sicheres VPN (das z. B. einen separaten zweiten Authentifizierungsschlüssel für den Aufbau einer sicheren Verbindung erfordert), um mobile Geräte mit Backend-Servern zu verbinden.
- Stellen Sie den Mitarbeitern physische Schlösser zur Verfügung, damit sie die von ihnen verwendeten mobilen Geräte physisch sichern können, wenn sie unbeaufsichtigt sind.
- Ordnungsgemäße Regelung der Gerätenutzung außerhalb des Unternehmens.
- Ordnungsgemäße Regelung der Gerätenutzung innerhalb des Unternehmens.
- Verwenden Sie eine MDM-Software/App und aktivieren Sie die Fernlöschfunktion.
- Verwenden Sie eine zentralisierte Geräteverwaltung mit einem Minimum an Rechten für die Endnutzer zur Installation von Software.
- Installieren Sie physische Zugangskontrollen.
- Vermeiden Sie es, sensible Informationen auf mobilen Geräten oder Festplatten zu speichern. Wenn ein Zugriff auf das interne System des Unternehmens erforderlich ist, sollten sichere Kanäle verwendet werden, wie bereits erwähnt.

6 MISPOSTAL

106. Die Risikoquelle ist auch in diesem Fall ein internes menschliches Versagen, aber hier führte keine böswillige Handlung zu dem Verstoß. Sie ist das Ergebnis von Unachtsamkeit. Der für die Verarbeitung Verantwortliche kann im Nachhinein nur wenig unternehmen, so dass die Vorbeugung in diesen Fällen noch wichtiger ist als bei anderen Arten von Verstößen.

6.1 FALL Nr. 13: Fehler bei der Postzustellung

Zwei Bestellungen für Schuhe wurden von einem Einzelhandelsunternehmen verpackt. Durch menschliches Versagen wurden zwei Packscheine vertauscht, so dass beide Produkte und die entsprechenden Packscheine an die falsche Person geschickt wurden. Das bedeutet, dass die beiden Kunden die Bestellungen des jeweils anderen erhalten haben, einschließlich der Lieferscheine mit den personenbezogenen Daten. Nachdem der für die Datenverarbeitung Verantwortliche von dem Verstoß erfahren hatte, rief er die Bestellungen zurück und schickte sie an die richtigen Empfänger.

6.1.1 FALL Nr. 13 - Vorherige Maßnahmen und Risikobewertung

107. Die Rechnungen enthielten die für eine erfolgreiche Lieferung erforderlichen personenbezogenen Daten (Name, Adresse sowie den gekauften Artikel und dessen Preis). Es ist wichtig zu ermitteln, wie der menschliche Fehler überhaupt passieren konnte und ob er in irgendeiner Weise hätte verhindert werden können. In dem beschriebenen Fall ist das Risiko gering, da keine besonderen Kategorien personenbezogener Daten oder andere Daten, deren Missbrauch erhebliche negative Auswirkungen haben könnte, betroffen waren, die Verletzung nicht auf einen systematischen Fehler des für die Verarbeitung Verantwortlichen zurückzuführen ist und nur zwei Personen betroffen sind. Es konnten keine negativen Auswirkungen auf die Personen festgestellt werden.

6.1.2 FALL Nr. 13 - Milderung und Verpflichtungen

108. Der für die Verarbeitung Verantwortliche sollte eine kostenlose Rücksendung der Sendungen und der dazugehörigen Rechnungen vorsehen und die falschen Empfänger auffordern, alle etwaigen Kopien der Rechnungen, die die personenbezogenen Daten der anderen Person enthalten, zu vernichten/zu löschen.

109. Auch wenn die Sicherheitsverletzung selbst kein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt und daher die Benachrichtigung der betroffenen Personen gemäß Artikel 34 DSGVO nicht vorgeschrieben ist, kann die Benachrichtigung der betroffenen Personen nicht vermieden werden, da ihre Mitarbeit erforderlich ist, um das Risiko zu mindern.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen
	X	X

6.2 FALL Nr. 14: Versehentlich per Post verschickte streng vertrauliche personenbezogene Daten

Die Arbeitsvermittlungsstelle einer öffentlichen Verwaltung schickte eine E-Mail-Nachricht über bevorstehende Schulungen an die in ihrem System als Arbeitsuchende registrierten Personen. Versehentlich wurde dieser E-Mail ein Dokument beigefügt, das die persönlichen Daten all dieser Arbeitssuchenden (Name, E-Mail-Adresse, Postanschrift, Sozialversicherungsnummer) enthielt. Die Zahl der betroffenen Personen beläuft sich auf mehr als 60000. Das Amt hat sich daraufhin mit allen Empfängern in Verbindung gesetzt und sie gebeten, die vorherige Nachricht zu löschen und die darin enthaltenen Informationen nicht zu verwenden.

6.2.1 FALL Nr. 14 - Vorherige Maßnahmen und Risikobewertung

110. Für die Übermittlung solcher Nachrichten hätten strengere Regeln eingeführt werden müssen. Die Einführung zusätzlicher Kontrollmechanismen muss in Betracht gezogen werden.

111. Die Zahl der betroffenen Personen ist beträchtlich, und die Einbeziehung ihrer Sozialversicherungsnummer sowie anderer grundlegender personenbezogener Daten erhöht das als hoch[31] einzustufende Risiko zusätzlich. Die eventuelle Weitergabe der Daten durch einen der Empfänger kann von dem für die Verarbeitung Verantwortlichen nicht verhindert werden.

6.2.2 FALL Nr. 14 - Milderung und Verpflichtungen

112. Wie bereits erwähnt, sind die Mittel zur wirksamen Minderung der Risiken einer ähnlichen Verletzung begrenzt. Obwohl der für die Verarbeitung Verantwortliche um die Löschung der Nachricht gebeten hat, kann er die Empfänger nicht dazu zwingen, und folglich kann er auch nicht sicher sein, dass sie der Aufforderung nachkommen.

113. Die Durchführung aller drei unten aufgeführten Maßnahmen sollte in einem solchen Fall selbstverständlich sein.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

6.3 FALL Nr. 15: Versehentlich per Post übermittelte personenbezogene Daten

Eine Teilnehmerliste für einen Kurs in Rechtsenglisch, der tagelang5 in einem Hotel stattfindet, wird versehentlich an 15 ehemalige Teilnehmer des Kurses statt an das Hotel geschickt. Die Liste enthält Namen, E-Mail-Adressen und Essensvorlieben der 15 Teilnehmer. Nur zwei Teilnehmer haben ihre Essensvorlieben angegeben, da sie eine Laktoseintoleranz haben. Keiner der Teilnehmer hat eine geschützte Identität. Der für die Verarbeitung Verantwortliche entdeckt den Fehler unmittelbar nach dem Versand der Liste und informiert die Empfänger über den Fehler und fordert sie auf, die Liste zu löschen.

6.3.1 FALL Nr. 15 - Vorherige Maßnahmen und Risikobewertung

114. Für die Übermittlung von Nachrichten, die personenbezogene Daten enthalten, hätten strenge Regeln eingeführt werden müssen. Die Einführung zusätzlicher Kontrollmechanismen muss in Betracht gezogen werden.

115. Die Risiken, die sich aus der Art, der Sensibilität, dem Umfang und dem Kontext der personenbezogenen Daten ergeben, sind gering. Die personenbezogenen Daten umfassen sensible Daten über die Ernährungsvorlieben von zwei der Teilnehmer. Auch wenn es sich bei der Information, dass jemand eine Laktoseintoleranz hat, um Gesundheitsdaten handelt, ist das Risiko, dass diese Daten in einer nachteiligen Weise verwendet werden, als relativ gering anzusehen. Während bei Gesundheitsdaten in der Regel davon ausgegangen wird, dass die Verletzung wahrscheinlich zu einem hohen Risiko für die betroffene Person führt[32], kann in diesem speziellen Fall kein Risiko festgestellt werden, dass die Verletzung zu physischen, materiellen oder immateriellen Schäden der betroffenen Person aufgrund der unbefugten Offenlegung von Informationen über Laktoseintoleranz führt. Im Gegensatz zu einigen anderen Lebensmittelpräferenzen kann Laktoseintoleranz normalerweise nicht mit religiösen oder philosophischen Überzeugungen in Verbindung gebracht werden. Auch die Menge der verletzten Daten und die Zahl der betroffenen Personen ist sehr gering.

6.3.2 FALL Nr. 15 - Milderung und Verpflichtungen

116. Zusammenfassend kann festgestellt werden, dass der Verstoß keine wesentlichen Auswirkungen auf die betroffenen Personen hatte. Die Tatsache, dass der für die Verarbeitung Verantwortliche die Empfänger unverzüglich nach Bekanntwerden des Fehlers kontaktiert hat, kann als mildernder Umstand betrachtet werden.

117. Wird eine E-Mail an einen falschen/unbefugten Empfänger gesendet, wird empfohlen, dass der für die Verarbeitung Verantwortliche den unbeabsichtigten Empfängern eine Follow-up-E-Mail in Bcc-Format sendet, in der er sich entschuldigt, die Löschung der betreffenden E-Mail anordnet und die Empfänger darauf hinweist, dass sie nicht berechtigt sind, die ihnen mitgeteilten E-Mail-Adressen weiter zu verwenden.

118. Aufgrund dieser Tatsachen war es unwahrscheinlich, dass diese Datenschutzverletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führte, weshalb keine Benachrichtigung der ORKB oder der betroffenen Personen erforderlich war. Allerdings muss auch diese Datenschutzverletzung gemäß

Artikel 33 Absatz 5 dokumentiert werden.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen
	X	X

6.4 FALL Nr. 16: Fehler bei der Postzustellung

Ein Versicherungskonzern bietet Kfz-Versicherungen an. Dazu verschickt sie regelmäßig angepasste Beitragspolicen per Post. Das Schreiben enthält neben dem Namen und der Anschrift des Versicherungsnehmers das Kfz-Kennzeichen ohne maskierte Ziffern, die Versicherungstarife des laufenden und des nächsten Versicherungsjahres, die ungefähre Jahresfahrleistung und das Geburtsdatum des Versicherungsnehmers. Gesundheitsdaten gemäß Artikel 9 DSGVO, Zahlungsdaten (Bankverbindung), Wirtschafts- und Finanzdaten sind nicht enthalten.

Die Briefe werden von automatischen Kuvertiermaschinen verpackt. Aufgrund eines mechanischen Fehlers werden zwei Briefe für verschiedene Versicherungsnehmer in einen Umschlag gesteckt und per Briefpost an einen Versicherungsnehmer verschickt. Der Versicherungsnehmer öffnet den Brief zu Hause und wirft einen Blick auf seinen korrekt zugestellten Brief sowie auf den fehlerhaft zugestellten Brief eines anderen Versicherungsnehmers.

6.4.1 FALL Nr. 16 - Vorherige Maßnahmen und Risikobewertung

119. Das fehlerhaft zugestellte Schreiben enthält Name, Anschrift, Geburtsdatum, unkenntlich gemachte Kfz-Kennzeichen und die Einstufung des Versicherungstarifs des laufenden und des nächsten Jahres. Die Auswirkungen auf den Betroffenen sind als mittel einzustufen, da nicht öffentlich zugängliche Informationen wie das Geburtsdatum oder unkenntlich gemachte Kfz-Kennzeichen sowie Angaben zur Erhöhung der Versicherungstarife dem unbefugten Empfänger bekannt gegeben werden. Die Wahrscheinlichkeit, dass diese Daten missbraucht werden, wird als gering bis mittel eingeschätzt. Zwar werden viele Empfänger das fälschlicherweise erhaltene Schreiben wahrscheinlich im Müll entsorgen, in Einzelfällen kann jedoch nicht völlig ausgeschlossen werden, dass das Schreiben in sozialen Netzwerken gepostet oder der Versicherungsnehmer kontaktiert wird.

6.4.2 FALL Nr. 16 - Schadensminderung und Verpflichtungen

120. Der für die Verarbeitung Verantwortliche sollte sich das Originaldokument auf eigene Kosten zurücksenden lassen. Der falsche Empfänger sollte außerdem darüber informiert werden, dass er die gelesenen Informationen nicht missbrauchen darf.

121. Es wird wahrscheinlich nie möglich sein, einen Zustellungsfehler bei einer Massensendung mit vollautomatischen Maschinen vollständig zu vermeiden. Im Falle einer erhöhten Häufigkeit ist jedoch zu prüfen, ob die Kuvertiermaschinen korrekt eingestellt und gewartet sind oder ob ein anderes systemisches Problem zu einem solchen Verstoß führt.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen
		X

6.5 Organisatorische und technische Maßnahmen zur Vorbeugung / Abschwächung der Auswirkungen von Falschparkern

122. Eine Kombination der unten genannten Maßnahmen - die je nach den Besonderheiten des Falles

angewandt werden - sollte dazu beitragen, die Wahrscheinlichkeit eines erneuten Verstoßes zu verringern.

123. Empfehlenswerte Maßnahmen:

(*Die Aufzählung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Ziel ist es vielmehr, Präventionsideen und mögliche Lösungen aufzuzeigen. Jede Verarbeitungstätigkeit ist anders, daher sollte der für die Verarbeitung Verantwortliche entscheiden, welche Maßnahmen für die jeweilige Situation am besten geeignet sind.*)

- Festlegung genauer Standards - ohne Interpretationsspielraum - für den Versand von Briefen/E-Mails.
- Angemessene Schulung des Personals für den Versand von Briefen/E-Mails.
- Beim Senden von E-Mails an mehrere Empfänger werden diese standardmäßig im Feld "bcc" aufgeführt.
- Beim Versand von E-Mails an mehrere Empfänger ist eine zusätzliche Bestätigung erforderlich, und diese werden nicht im Feld "bcc" aufgeführt.
- Anwendung des Vier-Augen-Prinzips.
- Automatische Adressierung statt manueller, wobei die Daten aus einer verfügbaren und aktuellen Datenbank entnommen werden; das automatische Adressierungssystem sollte regelmäßig auf versteckte Fehler und falsche Einstellungen überprüft werden.
- Anwendung der Nachrichtenverzögerung (z.B. kann die Nachricht innerhalb einer bestimmten Zeitspanne nach Anklicken der Schaltfläche "Drücken" gelöscht / bearbeitet werden).
- Deaktivierung der automatischen Vervollständigung bei der Eingabe von E-Mail-Adressen.
- Sensibilisierungsveranstaltungen zu den häufigsten Fehlern, die zu einer Verletzung des Schutzes personenbezogener Daten führen.
- Schulungen und Handbücher über den Umgang mit Vorfällen, die zu einer Verletzung des Schutzes personenbezogener Daten führen, und darüber, wer zu informieren ist (Einbeziehung des DSB).

7 ANDERE FÄLLE - SOCIAL ENGINEERING

7.1 FALL Nr. 17: Identitätsdiebstahl

Das Kontaktzentrum eines Telekommunikationsunternehmens erhält einen Telefonanruf von jemandem, der sich als Kunde ausgibt. Der vermeintliche Kunde fordert das Unternehmen auf, die E-Mail-Adresse zu ändern, an die von nun an die Rechnungsdaten gesendet werden sollen. Der Mitarbeiter des Kontaktzentrums überprüft die Identität des Kunden, indem er nach bestimmten persönlichen Daten fragt, wie sie in den Verfahren des Unternehmens festgelegt sind. Der Anrufer gibt die Steuernummer und die Postanschrift des angefragten Kunden korrekt an (da er Zugang zu diesen Elementen hatte). Nach der Überprüfung nimmt der Betreiber die gewünschte Änderung vor, und von da an werden die Rechnungsdaten an die neue E-Mail-Adresse gesendet. Das Verfahren sieht keine Benachrichtigung des früheren E-Mail-Kontakts vor. Im darauffolgenden Monat wendet sich der rechtmäßige Kunde an das Unternehmen und erkundigt sich, warum er keine Rechnungen an seine E-Mail-Adresse erhält, und leugnet jeden Anruf von ihm, in dem er die Änderung des E-Mail-Kontakts fordert. Später stellt das Unternehmen fest, dass die Informationen an einen unrechtmäßigen Nutzer gesendet wurden, und macht die Änderung rückgängig.

7.1.1 FALL Nr. 17 - Risikobewertung, Risikominderung und Verpflichtungen

124. Dieser Fall dient als Beispiel dafür, wie wichtig vorherige Maßnahmen sind. Unter Risikoaspekten stellt die

Sicherheitsverletzung ein hohes Risiko dar33 , da die Rechnungsdaten Aufschluss über das Privatleben der betroffenen Person geben können (z. B. Gewohnheiten, Kontakte) und zu materiellem Schaden führen könnten (z. B. Stalking, Gefährdung der körperlichen Unversehrtheit). Die bei diesem Angriff erlangten personenbezogenen Daten können auch verwendet werden, um die Übernahme von Konten in dieser Organisation zu erleichtern oder weitere Authentifizierungsmaßnahmen in anderen Organisationen auszunutzen. In Anbetracht dieser Risiken sollte die "geeignete" Authentifizierungsmaßnahme eine hohe Messlatte erfüllen, je nachdem, welche personenbezogenen Daten als Ergebnis der Authentifizierung verarbeitet werden können.

125. Infolgedessen sind sowohl eine Meldung an die ORKB als auch eine Mitteilung an die betroffene Person durch den für die Verarbeitung Verantwortlichen erforderlich.

126. Das bisherige Verfahren zur Kundenvalidierung muss im Lichte dieses Falles eindeutig verfeinert werden. Die zur Authentifizierung verwendeten Methoden waren nicht ausreichend. Die böswillige Partei war in der Lage, sich als der beabsichtigte Nutzer auszugeben, indem sie öffentlich zugängliche Informationen und Informationen, zu denen sie anderweitig Zugang hatte, nutzte.

127. Die Verwendung dieser Art der statischen wissensbasierten Authentifizierung (bei der sich die Antwort nicht ändert und die Informationen nicht "geheim" sind, wie es bei einem Passwort der Fall wäre) wird nicht empfohlen.

128. Stattdessen sollte die Organisation eine Form der Authentifizierung verwenden, bei der ein hohes Maß an Vertrauen besteht, dass es sich bei dem authentifizierten Nutzer um die gewünschte Person und nicht um eine andere handelt. Die Einführung einer "Out-of-band"-Multifaktor-Authentifizierungsmethode würde das Problem lösen, z. B. zur Überprüfung der Änderungsanforderung, indem eine Bestätigungsanfrage an den früheren Kontakt gesendet wird, oder indem zusätzliche Fragen gestellt und Informationen verlangt werden, die nur auf den früheren Rechnungen sichtbar sind. Es liegt in der Verantwortung des für die Verarbeitung Verantwortlichen zu entscheiden, welche Maßnahmen er einführen will, da er die Einzelheiten und Anforderungen seines internen Betriebs am besten kennt.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen

7.2 FALL Nr. 18: E-Mail-Exfiltration

Eine Verbrauchermarktkette entdeckte Monate 3nach ihrer Konfiguration, dass einige E-Mail-Konten verändert und Regeln erstellt worden waren, so dass jede E-Mail, die bestimmte Ausdrücke enthielt (z. B. "Rechnung", "Zahlung", "Banküberweisung", "Kreditkartenauthentifizierung", "Bankkontodaten"), in einen unbenutzten Ordner verschoben und außerdem an eine externe E-Mail-Adresse weitergeleitet wurde. Außerdem war zu diesem Zeitpunkt bereits ein Social-Engineering-Angriff durchgeführt worden, d. h. der Angreifer, der sich als Lieferant ausgab, hatte die Bankverbindung des Lieferanten in seine eigene umgewandelt. Schließlich waren zu diesem Zeitpunkt bereits mehrere gefälschte Rechnungen verschickt worden, die die neue Bankverbindung enthielten. Das Überwachungssystem der E-Mail-Plattform gab schließlich eine Warnung zu den Ordnern aus. Das Unternehmen konnte nicht feststellen, wie der Angreifer überhaupt Zugang zu den E-Mail-Konten erlangen konnte, vermutete aber, dass eine infizierte E-Mail dafür verantwortlich war, dass die für die Zahlungen zuständige Benutzergruppe Zugang erhielt.

Durch die stichwortartige Weiterleitung von E-Mails erhielt der Angreifer Informationen über 99 Beschäftigte: Name und Lohn eines bestimmten Monats bei 89 betroffenen Personen; Name, Familienstand, Anzahl der Kinder, Lohn, Arbeitszeiten und restliche Informationen über den Gehaltseingang von 10 Beschäftigten, deren Verträge beendet wurden. Der für die Verarbeitung Verantwortliche benachrichtigte nur die 10 Arbeitnehmer, die zu der letztgenannten Gruppe gehörten.

7.2.1 FALL Nr. 18 - Risikobewertung, Risikominderung und Verpflichtungen

129. Auch wenn der Angreifer wahrscheinlich nicht darauf abzielte, personenbezogene Daten zu sammeln, da die Sicherheitsverletzung sowohl zu materiellem (z. B. finanziellem Verlust) als auch zu immateriellem Schaden (z. B. Identitätsdiebstahl oder Betrug) führen könnte oder die Daten zur Erleichterung anderer Angriffe (z. B. Phishing) verwendet werden könnten, stellt die Verletzung des Schutzes personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen dar. Daher sollte die Sicherheitsverletzung allen 99 Mitarbeitern mitgeteilt werden und nicht nur den 10 Mitarbeitern, deren Gehaltsdaten durchgesickert sind.

130. Nach Bekanntwerden des Verstoßes erzwang der für die Verarbeitung Verantwortliche eine Passwortänderung für die kompromittierten Konten, blockierte den Versand von E-Mails an das E-Mail-Konto des Angreifers, benachrichtigte den Dienstanbieter der vom Angreifer verwendeten E-Mail über seine Aktionen, entfernte die vom Angreifer aufgestellten Regeln und verfeinerte die Warnmeldungen des Überwachungssystems, so dass eine Warnung ausgegeben wird, sobald eine automatische Regel erstellt wird. Alternativ könnte der für die Verarbeitung Verantwortliche den Benutzern das Recht entziehen, Regeln für die Weiterleitung festzulegen, so dass das IT-Dienstleistungsteam dies nur noch auf Anfrage tun muss, oder er könnte eine Richtlinie einführen, wonach die Benutzer die für ihre Konten festgelegten Regeln einmal pro Woche oder in Bereichen, in denen Finanzdaten verarbeitet werden, häufiger überprüfen und darüber Bericht erstatten müssen.

131. Die Tatsache, dass eine Sicherheitsverletzung so lange unentdeckt bleiben konnte und die Tatsache, dass über einen längeren Zeitraum hinweg Social Engineering zur Veränderung weiterer Daten hätte eingesetzt werden können, hat erhebliche Probleme im IT-Sicherheitssystem des für die Verarbeitung Verantwortlichen aufgezeigt. Diese sollten unverzüglich angegangen werden, z. B. durch verstärkte Automatisierungsprüfungen und Änderungskontrollen sowie Maßnahmen zur Erkennung von und Reaktion auf Vorfälle. Kontrollstellen, die mit sensiblen Daten, Finanzinformationen usw. umgehen, tragen eine größere Verantwortung für die Gewährleistung einer angemessenen Datensicherheit.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Notifizierung an SA	Mitteilung an die betroffenen Personen