Leitlinien 01/2021

zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten

Angenommen am 14. Dezember 2021

Version 2.0

Versionsverlauf

Version 2.0	14. Dezember 2021	Annahme der Leitlinien nach öffentlicher Konsultation
Version 1.0	14. Januar 2021	Annahme der Leitlinien für die öffentliche Konsultation

Inhaltsverzeichnis

1 EINLEITUNG 5

2 RANSOMWARE 8

2.1 Fall Nr. 01: Ransomware mit angemessener Sicherungskopie und ohne Exfiltration 9

2.1.1 Fall Nr. 01 – Vorherige Maßnahmen und Risikobewertung 9

2.1.2 Fall Nr. 01 – Schadensminderung und Pflichten 10

2.2 Fall Nr. 02: Ransomware ohne angemessene Sicherungskopie 11

2.2.1 Fall Nr. 02 – Vorherige Maßnahmen und Risikobewertung 11

2.2.2 Fall Nr. 02 – Schadensminderung und Pflichten 12

2.3 Fall Nr. 03: Ransomware mit Sicherungskopie und ohne Exfiltration in einem Krankenhaus 13

2.3.1 Fall Nr. 03 – Vorherige Maßnahmen und Risikobewertung 14

2.3.2 Fall Nr. 03 – Schadensminderung und Pflichten 14

2.4 Fall Nr. 04: Ransomware ohne Sicherungskopie und mit Exfiltration 15

2.4.1 Fall Nr. 04 – Vorherige Maßnahmen und Risikobewertung 15

2.4.2 Fall Nr. 04 – Schadensminderung und Pflichten 16

2.5 Organisatorische und technische Maßnahmen zur Vorbeugung/Minderung der Auswirkungen von Ransomware-Angriffen 16

3 ANGRIFFE mit Exfiltration von Daten 17

3.1 Fall Nr. 05: Exfiltration der Bewerbungsdaten von einer Website 18

3.1.1 Fall Nr. 05 – Vorherige Maßnahmen und Risikobewertung 18

3.1.2 Fall Nr. 05 – Schadensminderung und Pflichten 18

3.2 Fall Nr. 06: Exfiltration eines gehashten Passworts von einer Website 19

3.2.1 Fall Nr. 06 – Vorherige Maßnahmen und Risikobewertung 19

3.2.2 Fall Nr. 06 – Schadensminderung und Pflichten 20

3.3 Fall Nr. 07: Credential-Stuffing-Angriff auf eine Bankwebsite 21

3.3.1 Fall Nr. 07 – Vorherige Maßnahmen und Risikobewertung 21

3.3.2 Fall Nr. 07 – Schadensminderung und Pflichten 22

3.4 Organisatorische und technische Maßnahmen zur Vorbeugung/Milderung der Auswirkungen von Hackerangriffen 22

4 INTERNE MENSCHLICHE RISIKOQUELLE 23

4.1 Fall Nr. 08: Exfiltration von Geschäftsdaten durch einen Mitarbeiter 23

4.1.1 Fall Nr. 08 – Vorherige Maßnahmen und Risikobewertung 23

4.1.2 Fall Nr. 08 – Schadensminderung und Pflichten 24

4.2 Fall Nr. 09: Versehentliche Übermittlung von Daten an eine vertrauenswürdige Drittpartei 25

4.2.1 Fall Nr. 09 – Vorherige Maßnahmen und Risikobewertung 25

4.2.2 Fall Nr. 09 – Schadensminderung und Pflichten 26

4.3 Organisatorische und technische Maßnahmen zur Vorbeugung/Minderung der Auswirkungen interner menschlicher Risikoquellen 26
5 VERLORENE ODER GESTOHLENE GERÄTE UND PAPIERDOKUMENTE 27
5.1 Fall Nr. 10: Gestohlenes Gerät mit verschlüsselten personenbezogenen Daten 27
5.1.1 Fall Nr. 10 – Vorherige Maßnahmen und Risikobewertung 28
5.1.2 Fall Nr. 10 – Schadensminderung und Pflichten 28
5.2 Fall Nr. 11: Gestohlenes Gerät mit nicht verschlüsselten personenbezogenen Daten 28
5.2.1 Fall Nr. 11 – Vorherige Maßnahmen und Risikobewertung 28
5.2.2 Fall Nr. 11 – Schadensminderung und Pflichten 29
5.3 Fall Nr. 12: Gestohlene Papierakten mit sensiblen Daten 29
5.3.1 Fall Nr. 12 – Vorherige Maßnahmen und Risikobewertung 29
5.3.2 Fall Nr. 12 – Schadensminderung und Pflichten 30
5.4 Organisatorische und technische Maßnahmen zur Vorbeugung/Milderung der Auswirkungen von Verlust oder Diebstahl von Geräten 30
6 POSTVERSEHEN 31
6.1 Fall Nr. 13: Postversandfehler 31
6.1.1 Fall Nr. 13 – Vorherige Maßnahmen und Risikobewertung 31
6.1.2 Fall Nr. 13 – Schadensminderung und Pflichten 32
6.2 Fall Nr. 14: Versehentlicher Versand höchst vertraulicher personenbezogener Daten per E-Mail 32
6.2.1 Fall Nr. 14 – Vorherige Maßnahmen und Risikobewertung 32
6.2.2 Fall Nr. 14 – Schadensminderung und Pflichten 32
6.3 Fall Nr. 15: Versehentlicher Versand personenbezogener Daten per E-Mail 33
6.3.1 Fall Nr. 15 – Vorherige Maßnahmen und Risikobewertung 33
6.3.2 Fall Nr. 15 – Schadensminderung und Pflichten 33
6.4 Fall Nr. 16: Postversandfehler 34
6.4.1 Fall Nr. 16 – Vorherige Maßnahmen und Risikobewertung 34
6.4.2 Fall Nr. 16 – Schadensminderung und Pflichten 34
6.5 Organisatorische und technische Maßnahmen zur Vorbeugung/Milderung der Auswirkungen von Postversehen 34
7 Andere Fälle – Social Engineering 35
7.1 Fall Nr. 17: Identitätsdiebstahl 35
7.1.1 Fall Nr. 17 - Risikobewertung, Schadensminderung und Pflichten 36
7.2 Fall Nr. 18: Exfiltration von E-Mails 37
7.2.1 Fall Nr. 18 - Risikobewertung, Schadensminderung und Pflichten 37

DER EUROPÄISCHE DATENSCHUTZAUSSCHUSS –

gestützt auf Artikel 70 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden „DSGVO"),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 geänderten Fassung,[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 „Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung"[2] —

HAT FOLGENDE LEITLINIEN ANGENOMMEN:

1 EINLEITUNG

1. Mit der DSGVO wird in bestimmten Fällen die Anforderung eingeführt, dass eine Verletzung des Schutzes personenbezogener Daten der zuständigen nationalen Aufsichtsbehörde (im Folgenden „Aufsichtsbehörde") gemeldet werden muss und dass die Personen, deren personenbezogene Daten von der Verletzung betroffen sind, über die Verletzung benachrichtigt werden müssen (Artikel 33 und 34).

2. Die Artikel-29-Datenschutzgruppe hat bereits im Oktober 2017 einen *allgemeinen* Leitfaden zur Meldung von Verletzungen des Schutzes personenbezogener Daten erstellt, in dem die einschlägigen Abschnitte der DSGVO analysiert werden (Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250) (im Folgenden „Leitlinien WP250")[3]. In diesen Leitlinien wurden jedoch aufgrund ihres Charakters und des Zeitpunkts ihrer Veröffentlichung nicht alle praktischen Fragen hinreichend ausführlich behandelt. Daher bedarf es *praxisorientierter, fallbezogener* Leitlinien, die die bisherigen Erfahrungen der Aufsichtsbehörden seit Inkrafttreten der DSGVO berücksichtigen.

3. Dieses Dokument soll die Leitlinien WP250 ergänzen; es spiegelt die gemeinsamen Erfahrungen der Aufsichtsbehörden des EWR seit Inkrafttreten der DSGVO wider. Es soll den Verantwortlichen bei der

[1] Soweit in diesen Leitlinien auf „Mitgliedstaaten" Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten" zu verstehen.
[2] COM(2020) 264 final vom 24. Juni 2020.
[3] Artikel-29-Datenschutzgruppe WP250 rev.1 vom 6. Februar 2018, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 – vom EDSA gebilligt, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

Entscheidung helfen, wie sie mit Verletzungen des Schutzes von personenbezogenen Daten umgehen und welche Faktoren sie bei der Risikobewertung zu berücksichtigen haben.

4. Um eine Verletzung zu beheben, sollten der Verantwortliche und der Auftragsverarbeiter zunächst in der Lage sein, eine solche zu erkennen. In Artikel 4 Absatz 12 DSGVO wird eine „Verletzung des Schutzes personenbezogener Daten“ definiert als „eine Verletzung der Datensicherheit, die unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden”.

5. In ihrer Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten[4] und in ihren Leitlinien WP250 erläutert die WP29, dass Verletzungen des Schutzes personenbezogener Daten nach den folgenden drei bekannten Sicherheitskriterien kategorisiert werden können:

   - „Verletzung der Vertraulichkeit“ – die unbefugte oder unbeabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten,
   - „Verletzung der Integrität“ – die unbefugte oder unbeabsichtigte Änderung personenbezogener Daten,
   - „Verletzung der Verfügbarkeit“ – der unbefugte oder unbeabsichtigte Verlust des Zugangs zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten.[5]

6. Eine Verletzung kann potenziell eine Reihe von erheblichen nachteiligen Auswirkungen auf Einzelpersonen haben, die zu physischen, materiellen oder immateriellen Schäden führen können. Gemäß der DSGVO kann 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. Die Verletzung kann auch jeden anderen erheblichen wirtschaftlichen oder sozialen Nachteil für diese Personen bedeuten. Der Verantwortliche hat vor allem die Pflicht, 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 ist der Verantwortliche nach der DSGVO dazu verpflichtet:

   - jede Verletzung des Schutzes personenbezogener Daten zu dokumentieren, einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen,[6]

---

[4] G29 WP213 vom 25. März 2014, Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten, S. 5,https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Siehe Leitlinien WP250, S. 8. - Es ist zu berücksichtigen, dass eine Verletzung des Schutzes personenbezogener Daten entweder eine Kategorie oder mehrere Kategorien gleichzeitig oder kombiniert betreffen kann.

[6] Artikel 33 Absatz 5 DSGVO.

- die Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt,[7]
- die betroffene Person von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich eine hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.[8]

8. Verletzungen des Schutzes personenbezogener Daten sind ein Problem an sich, aber sie können auch auf ein anfälliges, möglicherweise veraltetes Datensicherheitssystem und auf Systemschwächen hindeuten, die behoben werden müssen. In der Regel ist es immer besser, Verletzungen des Schutzes personenbezogener Daten im Voraus vorzubeugen, da einige ihrer Folgen von Natur aus unumkehrbar sind. Bevor ein Verantwortlicher das Risiko, das sich aus einer durch einen Angriff verursachten Verletzung ergibt, *in vollem Umfang* bewerten kann, sollte die Ursache des Problems ermittelt werden, um festzustellen, ob die Schwachstellen, die zu dem Vorfall geführt haben, immer noch vorhanden sind und somit weiterhin ausgenutzt werden können. In vielen Fällen ist der Verantwortliche in der Lage zu erkennen, dass der Vorfall voraussichtlich ein Risiko mit sich bringt und daher zu melden ist. In anderen Fällen muss die Meldung nicht aufgeschoben werden, bis das Risiko und die Auswirkungen der Verletzung vollständig bewertet wurden, da die vollständige Risikobewertung parallel zur Meldung erfolgen kann und die so gewonnenen Informationen der Aufsichtsbehörde ohne unangemessene weitere Verzögerung schrittweise zur Verfügung gestellt werden können.[9]

9. Die Verletzung sollte gemeldet werden, wenn der Verantwortliche der Ansicht ist, dass sie voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Person mit sich bringt. Die Verantwortlichen sollten diese Bewertung zu dem Zeitpunkt vornehmen, zu dem sie von der Verletzung Kenntnis erlangen. Der Verantwortliche sollte nicht auf eine detaillierte forensische Untersuchung und (frühzeitige) Abhilfemaßnahmen warten, bevor er bewertet, ob die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein Risiko zur Folge hat und daher gemeldet werden sollte oder nicht.

10. Wenn ein Verantwortlicher das Risiko selbst als unwahrscheinlich einschätzt, aber das Risiko dennoch eintritt, kann die zuständige Aufsichtsbehörde von ihren Abhilfebefugnissen Gebrauch machen und gegebenenfalls Sanktionen verhängen.

11. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte über Pläne und Verfahren für den Umgang mit eventuellen Verletzungen des Schutzes personenbezogener Daten verfügen. Organisationen sollten klare Meldepflichten haben und für bestimmte Aspekte des Wiederherstellungsprozesses zuständige Personen benennen.

12. Auch Schulungen und die Sensibilisierung für Datenschutzfragen der Mitarbeiter des Verantwortlichen und des Auftragsverarbeiters 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 Verantwortlichen und die Auftragsverarbeiter unerlässlich. Diese Schulungen sollten je nach Art der Verarbeitungstätigkeit und Größe des

[7] Artikel 33 Absatz 1 DSGVO.
[8] Artikel 34 Absatz 1 DSGVO.
[9] Artikel 33 Absatz 4 DSGVO.

Verantwortlichen regelmäßig wiederholt werden, wobei die neuesten Trends und die durch Cyberangriffe oder andere Sicherheitsvorfälle ausgelösten Warnmeldungen zu berücksichtigen sind.

13. Der Grundsatz der Rechenschaftspflicht und das Konzept des „Datenschutzes durch Technikgestaltung“ könnten eine Analyse beinhalten, die in das von den Verantwortlichen und den Auftragsverarbeitern erstellte „Handbuch zum Umgang mit Verletzungen des Schutzes personenbezogener Daten“ einfließt, mit dem die Fakten für jeden Aspekt der Verarbeitung in jeder wichtigen Verarbeitungsphase ermittelt werden sollen. Ein solches im Voraus erstelltes Handbuch wäre eine viel schnellere Informationsquelle, anhand derer die Verantwortlichen und die Auftragsverarbeiter die Risiken mindern und die Pflichten ohne unangemessene Verzögerung erfüllen könnten. Dadurch wird sichergestellt, dass im Falle einer Verletzung des Schutzes personenbezogener Daten die Mitarbeiter der Organisation über das weitere Vorgehen Bescheid wissen und der Vorfall wahrscheinlich schneller bewältigt werden kann, als wenn keine Abhilfemaßnahmen oder Pläne vorhanden sind.

14. Die im Folgenden dargestellten Fälle sind zwar fiktiv, beziehen sich aber auf typische Fälle aus der gemeinsamen Erfahrung der Aufsichtsbehörden hinsichtlich Meldungen über Verletzungen des Schutzes personenbezogener Daten. Die folgenden Analysen beziehen sich ausdrücklich auf die untersuchten Fälle, sollen aber den Verantwortlichen bei der Bewertung ihrer eigenen Verletzungen des Schutzes personenbezogener Daten behilflich sein. Jede Änderung der Umstände der nachstehend beschriebenen Fälle kann ein anderes oder höheres Risikoniveau zur Folge haben und somit andere oder zusätzliche Maßnahmen erfordern. In diesen Leitlinien werden die Fälle nach bestimmten Kategorien von Verletzungen (z. B. Ransomware-Angriffe) gegliedert. Bei einer bestimmten Kategorie von Verletzungen sind in jedem Fall bestimmte Maßnahmen zur Schadensminderung erforderlich. Diese Maßnahmen werden nicht notwendigerweise in jeder Fallanalyse, die zur gleichen Kategorie von Verletzungen gehört, wiederholt. Bei den Fällen, die derselben Kategorie angehören, werden nur die Unterschiede dargelegt. Daher sollte der Leser alle Fälle lesen, die zur jeweiligen Kategorie einer Sicherheitsverletzung gehören, um die richtigen Maßnahmen zu erkennen und zu unterscheiden.

15. Die interne Dokumentation einer Verletzung des Schutzes personenbezogener Daten ist unabhängig von den mit der Verletzung verbundenen Risiken in jedem einzelnen Fall erforderlich. Die im Folgenden vorgestellten Fälle sollen Aufschluss darüber geben, ob die Verletzung an die Aufsichtsbehörde gemeldet und die betroffenen Personen davon benachrichtigt werden müssen.

2 RANSOMWARE

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

2.1 Fall Nr. 01: Ransomware mit angemessener Sicherungskopie und ohne Exfiltration

Die Computersysteme eines kleinen Fertigungsunternehmens wurden einem Ransomware-Angriff ausgesetzt und die auf diesen Systemen gespeicherten Daten wurden verschlüsselt. Der Verantwortliche nutzte die Verschlüsselung von ruhenden Daten, d. h. alle Daten, auf die die Ransomware zugriff, wurden mit einem modernen Verschlüsselungsalgorithmus verschlüsselt gespeichert. Der Entschlüsselungsschlüssel wurde bei dem Angriff nicht beeinträchtigt, d. h. der Angreifer konnte weder auf ihn zugreifen noch ihn indirekt verwenden. Folglich hatte der Angreifer nur Zugriff auf verschlüsselte persönliche Daten. So waren weder das E-Mail-System des Unternehmens noch die Kundensysteme, über die darauf zugegriffen wurde, betroffen. Das Unternehmen nutzt das Fachwissen eines externen Cybersicherheitsunternehmens, um den Vorfall zu untersuchen. Es liegen Protokolle vor, die jeden Datenfluss, der das Unternehmen verlässt (einschließlich ausgehender E-Mails), aufzeichnen. Nach der Analyse der Protokolle und der von den Erkennungssystemen des Unternehmens erfassten Daten ergab eine interne Untersuchung mit Unterstützung des externen Cybersicherheitsunternehmens *eindeutig*, dass der Angreifer die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Anhand der Protokolle lässt sich keine Datenübermittlung nach außen im Zeitraum des Angriffs feststellen. Die von der Verletzung betroffenen personenbezogenen Daten betreffen Kunden und Mitarbeiter des Unternehmens – insgesamt einige Dutzend Personen. Eine Sicherungskopie war ohne Weiteres verfügbar, und die Daten wurden einige Stunden nach dem Angriff wiederhergestellt. Die Sicherheitsverletzung hatte keine Auswirkungen auf das Tagesgeschäft des Verantwortlichen. Es gab keine Verzögerungen bei den Zahlungen der Mitarbeiter oder der Bearbeitung von Kundenanfragen.

17. In diesem Fall wurden die folgenden Elemente der Definition einer „Verletzung des Schutzes personenbezogener Daten“ erkannt: Eine Verletzung des Schutzes personenbezogener Daten hatte eine unrechtmäßige Änderung und einen unbefugten Zugriff auf die gespeicherten personenbezogenen Daten zur Folge.

2.1.1 Fall Nr. 01 – Vorherige Maßnahmen und Risikobewertung

18. Wie bei jedem Risiko, das von externen Akteuren ausgeht, kann die Wahrscheinlichkeit, dass ein Ransomware-Angriff erfolgreich ist, drastisch reduziert werden, indem die Sicherheit des Datenkontrollumfelds verstärkt wird. Die meisten dieser Verletzungen können durch angemessene organisatorische, physische und technische Sicherheitsmaßnahmen verhindert werden. Beispiele für solche Maßnahmen sind ein angemessenes Patch-Management und die Verwendung eines geeigneten Anti-Malware-Erkennungssystems. Mit einer angemessenen und gesonderten Sicherungskopie können die Folgen eines erfolgreichen Angriffs gemindert werden, sollte es zu einem solchen kommen. Darüber hinaus hilft ein Programm zur Aus- und Weiterbildung und Sensibilisierung der Mitarbeiter für Sicherheitsfragen (security education, training, and awareness, SETA), 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, mit dem sichergestellt wird, 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 Verantwortliche die Sicherheitsverletzung untersuchen und die Art des Schadprogramms ermitteln, um die möglichen Folgen des Angriffs zu verstehen. Zu den zu berücksichtigenden Risiken gehört das Risiko, dass Daten exfiltriert wurden, ohne dass eine Spur in den Protokollen der Systeme hinterlassen wurde.

20. In diesem Beispiel hatte der Angreifer Zugriff auf personenbezogene Daten, wodurch die Vertraulichkeit des Geheimtextes, der personenbezogene Daten in verschlüsselter Form enthält, beeinträchtigt wurde. Die Daten, die möglicherweise exfiltriert wurden, können jedoch vom Angreifer vorerst nicht gelesen oder verwendet werden. Die vom Verantwortlichen verwendete Verschlüsselungstechnik entspricht dem Stand der Technik. Der zur Entschlüsselung benötigte Schlüssel wurde nicht beeinträchtigt und konnte vermutlich auch nicht auf anderem Wege ermittelt werden. Infolgedessen werden die Risiken hinsichtlich der Vertraulichkeit für die Rechte und Freiheiten natürlicher Personen auf ein Mindestmaß begrenzt, sofern keine kryptoanalytischen Fortschritte erzielt werden, die die verschlüsselten Daten in Zukunft verständlich machen.

21. Der Verantwortliche sollte das Risiko für den Einzelnen aufgrund der Verletzung abwägen.[10] In diesem Fall ergeben sich die Risiken für die Rechte und Freiheiten der betroffenen Personen offenbar aus der mangelnden Verfügbarkeit der personenbezogenen Daten, und die Vertraulichkeit der personenbezogenen Daten ist nicht beeinträchtigt.[11] In diesem Beispiel wurden die nachteiligen Auswirkungen der Sicherheitsverletzung relativ bald nach dem Eintreten der Verletzung gemindert. Mit einem angemessenen Sicherungssystem[12] lassen sich die Auswirkungen der Verletzung abmildern, und in diesem Fall war der Verantwortliche in der Lage, es wirksam zu nutzen.

22. Bezüglich der Schwere der Folgen für die betroffenen Personen konnten nur geringfügige Folgen festgestellt werden, da die betroffenen Daten innerhalb weniger Stunden wiederhergestellt wurden, die Verletzung keine Auswirkungen auf den täglichen Betrieb des 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 Pflichten

23. Ohne eine Sicherungskopie kann der 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 beeinträchtigten Systeme auf einen einwandfreien Zustand ohne Schadprogramme zurückgesetzt, die Schwachstellen behoben und die betroffenen Daten bald nach dem Angriff wiederhergestellt wurden. Ohne

---

[10] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Datenschutzgruppe nach Artikel 29 (Leitlinien zur Datenschutz-Folgenabschätzung) (DSFA) und die Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 rev. 01, – vom EDSA gebilligt, https://ec.europa.eu/newsroom/article29/items/611236, S. 9.

[11] Aus technischer Sicht ist die Verschlüsselung von Daten mit einem „Zugriff“ auf die Originaldaten verbunden, und im Falle von Ransomware mit der Löschung der Originaldaten, d. h. der Ransomware-Code muss auf die Daten zugreifen, um sie zu verschlüsseln und die Originaldaten zu löschen. Ein Angreifer kann vor der Löschung eine Kopie des Originals anfertigen, aber nicht immer werden personenbezogene Daten extrahiert. Im Laufe der Ermittlungen eines Verantwortlichen können neue Informationen zutage treten, die eine Änderung dieser Einschätzung erforderlich machen. Ein Zugriff, der zu einer unrechtmäßigen Zerstörung, einem Verlust, einer Änderung, einer unbefugten Weitergabe personenbezogener Daten oder zu einem Sicherheitsrisiko für eine betroffene Person führt, kann auch ohne Auswertung der Daten genauso schwerwiegend sein wie ein Zugriff mit Auswertung der personenbezogenen Daten.

[12] Sicherungsverfahren sollten strukturiert, einheitlich und wiederholbar sein. Beispiele für Sicherungsverfahren sind die 3-2-1-Methode und die Großvater-Vater-Sohn-Methode. Jede Methode sollte stets auf ihre Wirksamkeit in Bezug auf die Abdeckung und die Wiederherstellung von Daten getestet werden. Um die Integrität des Systems zu gewährleisten, sollten die Tests in regelmäßigen Abständen und insbesondere dann wiederholt werden, wenn sich der Verarbeitungsprozess oder die Umstände ändern.

eine Sicherungskopie gehen Daten verloren, und die Schwere des Schadens kann sich erhöhen, da auch Risiken oder Auswirkungen auf Einzelpersonen auftreten können.

24. Die rechtzeitige Wiederherstellung der Daten aus der sofort verfügbaren Sicherungskopie 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 Sicherheitsverletzung ab. Nach der DSGVO ist eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden zu melden. Daher ließe sich feststellen, dass eine Meldung nach mehr als 72 Stunden in keinem Fall ratsam ist, aber bei Fällen mit hohem Risikoniveau kann selbst die Einhaltung dieser Frist als unzureichend angesehen werden.

25. In diesem Fall hat der Verantwortliche nach einer detaillierten Folgenabschätzung und einer Vorfallreaktion festgestellt, dass es unwahrscheinlich ist, dass die Verletzung ein Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt; daher ist weder eine Benachrichtigung der betroffenen Personen noch eine Meldung der Verletzung an die Aufsichtsbehörde erforderlich. Wie alle Verletzungen des Schutzes personenbezogener Daten sollte sie jedoch gemäß Artikel 33 Absatz 5 dokumentiert werden. Unter Umständen muss die Organisation auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Gewährleistung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und verbessern (oder wird später von der Aufsichtsbehörde dazu aufgefordert). Im Rahmen dieser Aktualisierung und Behebung der Mängel sollte die Organisation die Sicherheitsverletzung gründlich untersuchen und die Ursachen und die vom Angreifer verwendeten Methoden ermitteln, um ähnliche Vorfälle in Zukunft zu verhindern.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	X	X

2.2 Fall Nr. 02: Ransomware ohne angemessene Sicherungskopie

Einer der von einem landwirtschaftlichen Unternehmen genutzten Computer war einem Ransomware-Angriff ausgesetzt 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 jeden Datenfluss, der das Unternehmen verlässt (einschließlich ausgehender E-Mails), aufzeichnen. Nach der Analyse der Protokolle und der von den Erkennungssystemen des Unternehmens erfassten Daten ergab eine interne Untersuchung mit Unterstützung des Cybersicherheitsunternehmens, dass der Angreifer die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Anhand der Protokolle lässt sich keine Datenübermittlung nach außen im Zeitraum des Angriffs feststellen. Die von der Verletzung betroffenen personenbezogenen Daten betreffen Mitarbeiter und Kunden des Unternehmens – insgesamt einige Dutzend Personen. Es waren keine besonderen Kategorien von Daten betroffen. Es war keine elektronische Sicherungskopie vorhanden. Der größte Teil der Daten wurde anhand von Sicherungskopien in Papierform wiederhergestellt. Die Wiederherstellung der Daten dauerte fünf Arbeitstage und führte zu geringfügigen Verzögerungen bei der Versendung der Bestellungen an die Kunden.

2.2.1 Fall Nr. 02 – Vorherige Maßnahmen und Risikobewertung

26. Der Verantwortliche hätte dieselben vorherigen Maßnahmen wie in Teil 2.1 und in Abschnitt 2.9 ergreifen sollen. Der größte Unterschied zum vorherigen Fall ist die fehlende elektronische Sicherungskopie und die fehlende Verschlüsselung von ruhenden Daten. Daraus ergeben sich wesentliche Unterschiede in den folgenden Schritten.

27. Bei der Risikobewertung sollte der Verantwortliche die Infiltrationsmethode untersuchen und die Art des Schadprogramms ermitteln, um die möglichen Folgen des Angriffs zu verstehen. In diesem Beispiel wurden die personenbezogenen Daten von der Ransomware verschlüsselt, ohne dass sie exfiltriert wurden. Die Risiken für die Rechte und Freiheiten der betroffenen Personen ergeben sich demnach offenbar aus der mangelnden Verfügbarkeit der personenbezogenen Daten, und die Vertraulichkeit der personenbezogenen Daten ist nicht beeinträchtigt. Eine sorgfältige Prüfung der Firewall-Protokolle und ihrer Auswirkungen ist für die Ermittlung des Risikos unerlässlich. Der Verantwortliche sollte die Ergebnisse dieser Prüfungen auf Anfrage vorlegen.

28. Er muss dabei berücksichtigen, dass im Falle eines ausgefeilten Angriffs die Schadsoftware die Möglichkeit hat, die Protokolldateien zu bearbeiten und die Spuren zu beseitigen. Da die Protokolle nicht an einen zentralen Protokollserver weitergeleitet oder repliziert werden, kann der Verantwortliche selbst nach einer sorgfältigen Prüfung, die ergibt, dass die personenbezogenen Daten nicht durch den Angreifer exfiltriert wurden, nicht behaupten, dass ein fehlender Protokolleintrag als Beweis dient, dass keine Exfiltration stattgefunden hat. Daher kann die Wahrscheinlichkeit einer Verletzung des Schutzes personenbezogener Daten nicht vollständig ausgeschlossen werden.

29. Der Verantwortliche sollte die Risiken einer Verletzung des Schutzes personenbezogener Daten bewerten,[13] wenn der Angreifer Zugriff auf die Daten hatte. Bei der Risikobewertung sollte der Verantwortliche auch die Art, die Sensibilität, den Umfang und den Kontext der von der Verletzung 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. Die Erhebung genauer Informationen über den unbefugten Zugriff ist entscheidend für die Bestimmung des Risikoniveaus und die Verhinderung eines neuen oder weiteren Angriffs. Wären die Daten aus der Datenbank kopiert worden, wäre dies natürlich ein risikoerhöhender Faktor gewesen. Wenn die Einzelheiten des unrechtmäßigen Zugriffs nicht bekannt sind, sollte das schlimmste Szenario in Betracht gezogen und das Risiko entsprechend bewertet werden.

31. Eine fehlende Sicherungsdatenbank kann als risikoerhöhender Faktor angesehen werden, je nachdem, wie schwerwiegend die Folgen für die betroffenen Personen sind, die sich aus der fehlenden Verfügbarkeit der Daten ergeben.

2.2.2 Fall Nr. 02 – Schadensminderung und Pflichten

32. Ohne eine Sicherungskopie kann der 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. E-Mails mit Auftragsbestätigungen). Ohne Sicherungskopie können Daten verloren gehen, und davon hängt die Schwere der Folgen für die betroffenen Personen ab.

33. Die Wiederherstellung der Daten sollte sich nicht als übermäßig problematisch erweisen,[14] wenn die Daten noch in Papierform vorliegen, aber angesichts der Tatsache, dass es keine elektronische

[13] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

[14] Dies hängt von der Komplexität und Struktur der personenbezogenen Daten ab. In den komplexesten Szenarien kann die Wiederherstellung der Datenintegrität, die Übereinstimmung mit den Metadaten, die Gewährleistung der richtigen Beziehungen innerhalb der Datenstrukturen und die Überprüfung der Datengenauigkeit erhebliche Ressourcen und Anstrengungen erfordern.

Sicherungsdatenbank gibt, wird eine Meldung an die Aufsichtsbehörde für notwendig erachtet, da die Wiederherstellung der Daten einige Zeit in Anspruch nimmt 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 Benachrichtigung der betroffenen Personen über die Verletzung des Schutzes personenbezogener Daten kann auch davon abhängen, wie lange die personenbezogenen Daten nicht verfügbar sind und welche Auswirkungen dies auf den Betrieb des Verantwortlichen haben könnte (z. B. Verzögerungen bei der Überweisung von Gehaltszahlungen für Arbeitnehmer). Da diese Verzögerungen bei Zahlungen und Lieferungen zu finanziellen Verlusten für die Personen führen können, deren Daten beeinträchtigt wurden, kann die Verletzung auch als ein hohes Risiko angesehen werden. Außerdem könnte es sich als unumgänglich erweisen, die betroffenen Personen zu benachrichtigen, 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. Unter Umständen muss das Unternehmen auch seine organisatorischen und technischen Maßnahmen und Verfahren zur Gewährleistung 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	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	X

2.3 Fall Nr. 03: Ransomware mit Sicherungskopie und ohne Exfiltration in einem Krankenhaus

Das Informationssystem eines Krankenhauses bzw. einer medizinischen Versorgungseinrichtung war einem Ransomware-Angriff ausgesetzt und ein erheblicher Teil der Daten wurde von dem Angreifer verschlüsselt. Die Einrichtung nutzt das Fachwissen eines externen Cybersicherheitsunternehmens, um ihr Netzwerk zu überwachen. Es liegen Protokolle vor, die jeden Datenfluss, der das Unternehmen verlässt (einschließlich ausgehender E-Mails), aufzeichnen. Nach der Analyse der Protokolle und der von den Erkennungssystemen der Einrichtung erfassten Daten ergab eine interne Untersuchung mit Unterstützung des Cybersicherheitsunternehmens, dass der Angreifer die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Anhand der Protokolle lässt sich keine Datenübermittlung nach außen im Zeitraum des Angriffs feststellen. Die von der Verletzung betroffenen personenbezogenen Daten betreffen Mitarbeiter der Einrichtung und Patienten – insgesamt Tausende von Personen. Es waren elektronische Sicherungskopien vorhanden. Der größte Teil der Daten konnte wiederhergestellt werden, 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 Leistungsniveaus aufgrund der Nichtverfügbarkeit der Systeme.

2.3.1 Fall Nr. 03 – Vorherige Maßnahmen und Risikobewertung

36. Der Verantwortliche hätte dieselben vorherigen Maßnahmen wie in Teil 2.1 und in Abschnitt 2.5 ergreifen sollen. Der größte Unterschied zum vorherigen Fall besteht darin, dass die Folgen für einen großen Teil der betroffenen Personen sehr schwerwiegend sind.[15]

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 Großteil der betroffenen Personen. Außerdem besteht ein hohes Restrisiko für die Vertraulichkeit der Patientendaten.

38. Wichtig sind die Art der Datenschutzverletzung sowie die Art, die Sensibilität und der Umfang der von der Verletzung 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 – Schadensminderung und Pflichten

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 Benachrichtigung der betroffenen Personen über die Sicherheitsverletzung ist aufgrund der Auswirkungen für die Patienten auch nach der Wiederherstellung der verschlüsselten Daten erforderlich. Es wurden zwar die Daten aller Patienten, die in den letzten Jahren im Krankenhaus behandelt wurden, verschlüsselt, aber nur die Patienten, die während des Ausfalls des Computersystems im Krankenhaus behandelt werden sollten, waren davon betroffen. Der Verantwortliche sollte diese Patienten direkt über die Datenschutzverletzung benachrichtigen. Eine direkte Benachrichtigung der anderen Patienten, von denen einige möglicherweise seit mehr als zwanzig Jahren nicht mehr im Krankenhaus waren, ist aufgrund der Ausnahmeregelung in Artikel 34 Absatz 3 Buchstabe c möglicherweise nicht erforderlich. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung[16] oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam 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 einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen. Er sollte gemäß Artikel 33 Absatz 5 dokumentiert, der Aufsichtsbehörde gemäß Artikel 33 Absatz 1 gemeldet und den betroffenen Personen gemäß Artikel 34 Absatz 1 zur Kenntnis gebracht werden. Die Organisation muss auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Gewährleistung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und verbessern.

---

[15] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

[16] In Erwägungsgrund 86 DSGVO heißt es: „Solche Benachrichtigungen der betroffenen Person sollten stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.“

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	✓

2.4 Fall Nr. 04: Ransomware ohne Sicherungskopie 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 Angreifer 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). Neben den grundlegenden Identitätsdaten sind auch Personalausweisnummern und Finanzdaten wie Kreditkartendaten von der Verletzung betroffen. Es gab zwar eine Sicherungsdatenbank, aber auch diese war vom Angreifer verschlüsselt worden.

2.4.1 Fall Nr. 04 – Vorherige Maßnahmen und Risikobewertung

41. Der Verantwortliche hätte dieselben vorherigen Maßnahmen wie in Teil 2.1 und in Abschnitt 2.5 ergreifen sollen. Zwar war eine Sicherungskopie vorhanden, aber auch diese war von dem Angriff betroffen. Allein diese Tatsache wirft Fragen über die Qualität der vorausgegangenen IT-Sicherheitsmaßnahmen des Verantwortlichen auf und sollte im Rahmen der Untersuchung genauer betrachtet werden, da bei einem sorgfältig geplanten Sicherungssystem mehrere Sicherungskopien ohne Zugriff vom Hauptsystem aus sicher aufbewahrt werden müssen, denn sie können andernfalls bei demselben Angriff beeinträchtigt werden. Außerdem können Ransomware-Angriffe tagelang unentdeckt bleiben, wobei selten genutzte Daten langsam verschlüsselt werden. Dies kann mehrere Sicherungskopien unbrauchbar machen. Daher sollten die Sicherungskopien auch in regelmäßigen Abständen und getrennt erstellt werden. Dies würde die Wahrscheinlichkeit einer Wiederherstellung erhöhen, wenn auch mit einem erhöhten Datenverlust.

42. Diese Verletzung betrifft nicht nur die Verfügbarkeit von Daten, sondern auch die Vertraulichkeit, da der Angreifer möglicherweise Daten auf dem Server geändert und/oder kopiert hat. Die Art der Sicherheitsverletzung bringt daher ein hohes Risiko mit sich.[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 Daten von Ausweisdokumenten und Finanzdaten wie Kreditkartendaten betroffen. Eine Verletzung des Schutzes dieser Arten personenbezogener Daten stellt für sich genommen ein hohes Risiko dar, und wenn die Daten zusammen verarbeitet werden, könnten sie unter anderem für Identitätsdiebstahl oder Betrug verwendet werden.

44. Aufgrund einer fehlerhaften Serverlogik oder organisatorischer Kontrollen waren die Sicherungsdateien durch die Ransomware beeinträchtigt, wodurch die Wiederherstellung der Daten verhindert und das Risiko erhöht wurde.

45. Diese Verletzung des Schutzes personenbezogener Daten stellt ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen dar, da sie sowohl zu materiellem (z. B. finanziellem Verlust, da Kreditkartendaten

[17] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

betroffen waren) als auch zu immateriellem Schaden (z. B. Identitätsdiebstahl oder Betrug, da Personalausweisdaten betroffen waren) führen könnte.

2.4.2 Fall Nr. 04 – Schadensminderung und Pflichten

46. Die betroffenen Personen müssen unbedingt benachrichtigt werden, damit sie die erforderlichen Maßnahmen ergreifen können, um materiellen Schaden abzuwenden (z. B. Sperrung ihrer Kreditkarten).

47. Neben der Dokumentation der Verletzung gemäß Artikel 33 Absatz 5 ist in diesem Fall auch eine Meldung an die Aufsichtsbehörde erforderlich (Artikel 33 Absatz 1), und der Verantwortliche ist auch verpflichtet, die betroffenen Personen über die Verletzung zu benachrichtigen (Artikel 34 Absatz 1). Letzteres könnte individuell erfolgen, jedoch sollte der Verantwortliche Personen, für die keine Kontaktdaten verfügbar sind, durch eine öffentliche Bekanntmachung benachrichtigen, sofern eine solche Bekanntmachung 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 Verantwortlichen angezeigt wird und genaue Verweise auf die einschlägigen Bestimmungen der DSGVO enthält. Unter Umständen muss das Unternehmen auch seine organisatorischen und technischen Maßnahmen und Verfahren zur Gewährleistung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und verbessern.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	✓

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

48. Die Tatsache, dass ein Ransomware-Angriff stattfinden konnte, ist in der Regel ein Zeichen für eine oder mehrere Schwachstellen im System des 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 Evaluierung des Datensicherheitssystems – unter besonderer Berücksichtigung 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 erschöpfend oder vollständig. Ziel ist es vielmehr, Ideen zur Vorbeugung und mögliche Lösungen aufzuzeigen. Jede Verarbeitungstätigkeit ist anders, daher sollte der Verantwortliche entscheiden, welche Maßnahmen für die jeweilige Situation am besten geeignet sind).

- Gewährleistung der Aktualität der Firmware, des Betriebssystems und der Anwendungssoftware auf den Servern, Client-Rechnern, aktiven Netzwerkkomponenten und allen anderen Rechnern im selben lokalen Netz (einschließlich Wi-Fi-Geräten). Sicherstellung, 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,
- Entwurf und Organisation von Verarbeitungssystemen und Infrastrukturen zur Segmentierung oder Isolierung von Datensystemen und Netzwerken, um die Ausbreitung von Schadprogrammen innerhalb des Unternehmens und auf externe Systeme zu verhindern,

- Vorhandensein eines aktuellen, sicheren und getesteten Sicherungsverfahrens. Medien für mittel- und langfristige Sicherungskopien sollten von der betrieblichen Datenspeicherung getrennt und auch im Falle eines erfolgreichen Angriffs für Dritte unzugänglich aufbewahrt werden (z. B. tägliche stufenweise Sicherung und wöchentliche Vollsicherung),
- Besitz/Beschaffung einer angemessenen, aktuellen, wirksamen und integrierten Anti-Malware-Software,
- Vorhandensein einer angemessenen, aktuellen, wirksamen und integrierten Firewall sowie eines Angriffserkennungs- und -präventionssystems sowie Leitung des Netzwerkverkehrs durch die Firewall bzw. das Angriffserkennungssystem, auch im Fall von Arbeit im Home Office oder von mobiler Arbeit (z. B. durch Nutzung von VPN-Verbindungen zu organisatorischen Sicherheitsmechanismen beim Internetzugriff),
- Schulung der Mitarbeiter in den Methoden zur Erkennung und Abwehr von IT-Angriffen. Der Verantwortliche sollte Mittel zur Verfügung stellen, um festzustellen, ob die über andere Kommunikationsmittel erhaltenen E-Mails und Nachrichten authentisch und vertrauenswürdig sind. Die Mitarbeiter sollten darin geschult werden, zu erkennen, wann ein solcher Angriff stattgefunden hat, wie das Endgerät aus dem Netz genommen werden kann und dass sie verpflichtet sind, dies unverzüglich dem Sicherheitsbeauftragten zu melden,
- Betonung der Notwendigkeit, den Typ des Schadprogramms zu identifizieren, um die Folgen des Angriffs zu erkennen und die richtigen Maßnahmen zur Minderung des Risikos zu finden. Sollte ein Ransomware-Angriff erfolgreich gewesen sein und keine Sicherheitskopie vorhanden sein, können Tools wie die des Projekts „no more ransom“ (nomoreransom.org) eingesetzt werden, um Daten wiederherzustellen. Sollte jedoch eine Sicherungskopie vorhanden sein, ist es ratsam, die Daten daraus 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-Notfallteams (Computer Security Incident Response Team, CSIRT) oder eines Reaktionsteams für IT-Sicherheitsvorfälle (Computer Emergency Response Team, CERT) innerhalb der Organisation oder Beitritt zu einem gemeinsamen CSIRT/CERT. Erstellung eines Reaktionsplans für Cybervorfälle, eines Plans für die Datenwiederherstellung im Falle eines Systemabsturzes und eines Plans zur Aufrechterhaltung des Geschäftsbetriebs sowie Sicherstellung, dass diese sorgfältig getestet werden,
- bei der Bewertung von Gegenmaßnahmen sollte die Risikoanalyse überprüft, getestet und aktualisiert werden.

3 ANGRIFFE MIT EXFILTRATION VON DATEN

50. Angriffe, die Schwachstellen in Diensten ausnutzen, die der Verantwortliche Dritten über das Internet anbietet, beispielsweise durch Injektionsangriffe (z. B. SQL-Injection, Path Traversal), Angriffe auf Websites und ähnliche Methoden, können insofern Ransomware-Angriffen ähneln, als das Risiko von der Handlung eines unbefugten Dritten ausgeht. Diese Angriffe zielen jedoch in der Regel darauf ab, personenbezogene Daten zu kopieren, zu exfiltrieren und für einen böswilligen Zweck zu missbrauchen. Es handelt sich also in erster Linie um Verletzungen der Vertraulichkeit und möglicherweise auch der Integrität von Daten. Sofern sich der Verantwortliche der Merkmale dieser Art von Verletzungen 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 der Bewerbungsdaten von einer Website

Eine Arbeitsvermittlungsstelle fiel einem Cyberangriff, bei dem ein Schadcode auf ihrer Website platziert wurde, zum Opfer. Durch diesen Schadcode wurden personenbezogene Daten, die über Online-Bewerbungsformulare übermittelt und auf dem Webserver gespeichert wurden, für Unbefugte zugänglich. Es sind 213 solcher Formulare möglicherweise betroffen, wobei nach Analyse der betroffenen Daten festgestellt wurde, dass keinerlei besondere Datenkategorien von der Verletzung betroffen waren. Das installierte Schadsoftware-Toolkit enthielt Funktionen, die es dem Angreifer ermöglichten, den Verlauf der Exfiltration zu löschen sowie 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 Verantwortlichen ist äußerst wichtig, da die meisten dieser Verletzungen verhindert werden können, indem sichergestellt wird, dass alle Systeme ständig aktualisiert, sensible Daten verschlüsselt und Anwendungen nach hohen Sicherheitsstandards wie starke Authentifizierung, Maßnahmen gegen Brute-Force-Angriffe, „Maskierung“ oder „Bereinigung“[18] von Benutzereingaben usw. entwickelt werden. Regelmäßige IT-Sicherheitsaudits, 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 findet sich in Abschnitt 3.7).

52. Zu Beginn der Untersuchung der Verletzung sollte der Verantwortliche stets die Art des Angriffs und dessen Methoden ermitteln, um zu beurteilen, welche Maßnahmen zu ergreifen sind. Damit dies schnell und wirksam geschieht, sollte der Verantwortliche einen Reaktionsplan für den Vorfall aufstellen, in dem die schnellen und notwendigen Schritte festgelegt sind, um den Vorfall unter Kontrolle zu bringen. In diesem Fall war die Art der Verletzung ein risikoerhöhender Faktor, da nicht nur die Vertraulichkeit der Daten eingeschränkt wurde, sondern der Infiltrator auch die Möglichkeit hatte, Änderungen im System vorzunehmen, wodurch auch die Integrität der Daten gefährdet wurde.

53. Die Art, die Sensibilität und der Umfang der von der Verletzung betroffenen personenbezogenen Daten sollten bewertet werden, um festzustellen, inwieweit die betroffenen Personen von der Verletzung berührt sind. Es waren zwar keine besonderen Kategorien personenbezogener Daten betroffen, aber die Daten, auf die zugegriffen wurde, enthalten umfangreiche personenbezogene Informationen aus den Online-Formularen, und diese Daten könnten in vielerlei Hinsicht missbraucht werden (gezielte Werbung, Identitätsdiebstahl usw.), sodass die Schwere der Auswirkungen das Risiko für die Rechte und Freiheiten der betroffenen Personen erhöhen dürfte.[19]

3.1.2 Fall Nr. 05 – Schadensminderung und Pflichten

54. Soweit möglich, sollte die Datenbank nach der Behebung des Problems mit der in einer Sicherungskopie gespeicherten Datenbank verglichen werden. Die aus der Sicherheitsverletzung gewonnenen Erfahrungen sollten für die Aktualisierung der IT-Infrastruktur genutzt werden. Der Verantwortliche sollte alle betroffenen

[18] Die Maskierung oder Bereinigung von Benutzereingaben ist eine Form der Eingabevalidierung, mit der sichergestellt wird, dass nur korrekt formatierte Daten in ein Informationssystem eingegeben werden.

[19] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

IT-Systeme in einen sauberen Zustand versetzen, die Schwachstelle beheben und neue Sicherheitsmaßnahmen, z. B. Prüfungen der Integrität von Daten und Sicherheitsaudits einführen, um ähnliche Verletzungen des Schutzes personenbezogener Daten in Zukunft zu vermeiden. Wurden personenbezogene Daten nicht nur exfiltriert, sondern auch gelöscht, muss der Verantwortliche systematisch Maßnahmen ergreifen, um die personenbezogenen Daten in dem Zustand wiederherzustellen, in dem sie sich vor der Verletzung befanden. Es kann notwendig sein, vollständige Sicherungen und schrittweise Änderungen durchzuführen und dann möglicherweise die Verarbeitung seit der letzten schrittweisen Sicherung zu wiederholen, was voraussetzt, dass der Verantwortliche in der Lage ist, die seit der letzten Sicherung vorgenommenen Änderungen zu replizieren. Hierfür könnte es erforderlich sein, dass das System des Verantwortlichen so ausgelegt ist, dass es die täglichen Eingabedateien für den Fall aufbewahrt, dass sie erneut verarbeitet werden müssen, und es bedarf einer robusten Speichermethode und einer angemessenen Aufbewahrungsstrategie.

55. Da die Verletzung des Schutzes personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, sollten die betroffenen Personen auf jeden Fall darüber benachrichtigt werden (Artikel 34 Absatz 1), was wiederum bedeutet, dass die zuständige(n) Aufsichtsbehörde(n) in Form einer Meldung über die Verletzung des Schutzes personenbezogener Daten einbezogen werden sollten. Die Dokumentation der Verletzung ist nach Artikel 33 Absatz 5 DSGVO verpflichtend und erleichtert die Bewertung der Situation.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der 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 Kochwebsite zu erhalten. Die Benutzer durften nur beliebige Pseudonyme als Benutzernamen wählen. Von der Verwendung von E-Mail-Adressen zu diesem Zweck wurde abgeraten. Die in der Datenbank gespeicherten Passwörter wurden mit einem starken Algorithmus gehasht und das Salt wurde nicht beeinträchtigt. Betroffene Daten: gehashte Passwörter von 1200 Benutzern. Zur Sicherheit benachrichtigte der Verantwortliche die betroffenen Personen per E-Mail über die Verletzung 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 Sensibilität und den Umfang der personenbezogenen Daten verringert. Dieser Fall bringt keine Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich.

57. Darüber hinaus wurden keine Kontaktinformationen (z. B. E-Mail-Adressen oder Telefonnummern) betroffener Personen preisgegeben, weshalb für die betroffenen Personen kein erhebliches Risiko besteht, Opfer von Betrugsversuchen zu werden (z. B. durch den 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 kann,[20] wenn aufgrund der Art der Website und der Daten, auf die zugegriffen wird, besondere Kategorien personenbezogener Daten offengelegt werden 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, werden erfolgreiche Brute-Force-Angriffe auf die Anmeldung verhindert, wodurch die Risiken, die sich aus der Tatsache ergeben, dass die Angreifer die Benutzernamen bereits kennen, weitgehend verringert werden.

3.2.2 Fall Nr. 06 – Schadensminderung und Pflichten

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 durch die Verletzung verursachte Schäden zu vermeiden, indem sie zum Beispiel ihr Passwort ändern. In diesem Fall war die Benachrichtigung nicht obligatorisch, kann aber in vielen Fällen empfehlenswert sein.

60. Der Verantwortliche sollte die Schwachstelle beheben und neue Sicherheitsmaßnahmen wie etwa systematische Sicherheitsaudits der Website einführen, um ähnliche Verletzungen des Schutzes personenbezogener Daten in Zukunft zu vermeiden.

61. Die Verletzung sollte gemäß Artikel 33 Absatz 5 dokumentiert werden, eine Benachrichtigung oder Meldung ist jedoch nicht erforderlich.

62. Außerdem ist es in jedem Fall ratsam, die betroffenen Personen über eine Verletzung des Schutzes von Passwörtern zu benachrichtigen, auch wenn die Passwörter unter Verwendung eines mit einem Salt versehenen Hashwerts mit einem Algorithmus gespeichert wurden, der dem Stand der Technik entspricht. Vorzugsweise sollten Authentifizierungsmethoden verwendet werden, die eine Verarbeitung der Passwörter auf der Serverseite überflüssig machen. 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	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	X	X

[20] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

3.3 Fall Nr. 07: Credential-Stuffing-Angriff auf eine Bankwebsite

Eine Bank wurde Opfer eines Cyberangriffs auf eine ihrer Online-Banking-Websites. Der Angriff zielte darauf ab, alle möglichen Nutzerkennungen aufzuzählen, die ein festgelegtes triviales Passwort verwenden. Die Passwörter bestehen aus 8 Ziffern. Aufgrund einer Sicherheitslücke auf der Website konnten in einigen Fällen personenbezogene Daten (Name, Vorname, Geschlecht, Geburtsdatum und -ort, Steuernummer, Nutzerkennungen) an den Angreifer weitergegeben werden, auch wenn das verwendete Passwort nicht korrekt war oder das Bankkonto nicht mehr aktiv war. Dadurch waren rund 100 000 Datensubjekte betroffen. Von diesen loggte sich der Angreifer erfolgreich in etwa 2000 Konten ein, die das vom Angreifer ausprobierte triviale Passwort benutzten. Im Nachhinein war der Verantwortliche in der Lage, alle unrechtmäßigen Anmeldeversuche zu ermitteln. Der Verantwortliche konnte bestätigen, dass gemäß den Überprüfungen zur Betrugsbekämpfung keine Vorgänge von diesen Konten während des Angriffs durchgeführt wurden. Die Bank hatte Kenntnis von der Verletzung des Schutzes personenbezogener Daten, da ihr Sicherheitseinsatzzentrum eine hohe Anzahl von Login-Anfragen auf der Website feststellte. Daraufhin deaktivierte der Verantwortliche die Anmeldefunktion auf der Website und erzwang die Rücksetzung der Passwörter der angegriffenen Konten. Der Verantwortliche hat nur die Nutzer der betroffenen Konten über die Verletzung des Schutzes personenbezogener Daten benachrichtigt, d. h. die Nutzer, deren Passwörter missbraucht wurden oder deren Daten offengelegt wurden.

3.3.1 Fall Nr. 07 – Vorherige Maßnahmen und Risikobewertung

63. Es sei darauf hingewiesen, dass Verantwortliche, die mit hochsensiblen personenbezogenen Daten[21] umgehen, eine größere Verantwortung in Bezug auf die Gewährleistung einer angemessenen Datensicherheit haben, z. B. durch ein Sicherheitseinsatzzentrum und andere Maßnahmen zur Vorbeugung, Erkennung und Reaktion auf Vorfälle. Werden diese höheren Standards nicht erfüllt, führt dies mit Sicherheit zu strengeren Maßnahmen bei der Untersuchung durch eine Aufsichtsbehörde.

64. Die Verletzung betrifft nicht nur Finanzdaten, sondern auch Informationen über die Identität und die Nutzerkennung, was sie besonders schwerwiegend macht. Die Zahl der betroffenen Personen ist hoch.

65. Die Tatsache, dass es in einem so sensiblen Umfeld zu einer Verletzung kommen konnte, deutet auf erhebliche Datensicherheitslücken im System des Verantwortlichen hin und kann ein Indikator dafür sein, dass die Überprüfung und Aktualisierung der betroffenen Maßnahmen gemäß Artikel 24 Absatz 1, Artikel 25 Absatz 1 und Artikel 32 Absatz 1 DSGVO „erforderlich“ ist. Anhand der verletzten Daten können die betroffenen Personen eindeutig identifiziert werden. Sie enthalten auch andere Informationen über die betroffenen Personen (z. B. Geschlecht, Geburtsdatum und -ort) und können vom Angreifer dazu verwendet werden, die Passwörter der Kunden zu erraten oder eine an die Bankkunden gerichtete Spear-Phishing-Kampagne durchzuführen.

[21] Dazu gehören Informationen über die betroffenen Personen in Bezug auf Zahlungsmethoden wie Kartennummern, Bankkonten, Online-Zahlungen, Gehaltsabrechnungen, Kontoauszüge, Wirtschaftsanalysen oder andere Angaben, die wirtschaftliche Informationen über die betroffenen Personen liefern können.

66. Deshalb wurde davon ausgegangen, dass die Verletzung des Schutzes personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten aller betroffenen Personen mit sich bringt.[22] Somit sind sowohl materielle (z. B. finanzielle Verluste) als auch immaterielle Schäden (z. B. Identitätsdiebstahl oder Betrug) als Folge denkbar.

3.3.2 Fall Nr. 07 – Schadensminderung und Pflichten

67. Die in der Fallbeschreibung genannten Maßnahmen des Verantwortlichen sind angemessen. Nach der Verletzung des Schutzes personenbezogener Daten hat er auch die Schwachstelle auf der Website behoben und weitere Schritte unternommen, um ähnliche künftige Verletzungen des Schutzes personenbezogener Daten zu verhindern, z. B. die Hinzufügung 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 Meldung an die Aufsichtsbehörde sind in diesem Szenario nicht optional. Darüber hinaus sollte der Verantwortliche alle 100 000 betroffenen Personen (einschließlich der betroffenen Personen, deren Konten nicht angegriffen wurden) gemäß Artikel 34 DSGVO benachrichtigen.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	✓

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

69. Ebenso wie im Falle von Ransomware-Angriffen ist eine Neubewertung der IT-Sicherheit für Verantwortliche in ähnlichen Fällen unabhängig vom Ausgang und den Folgen des Angriffs obligatorisch.

70. Empfehlenswerte Maßnahmen:[23]

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

- modernste Verschlüsselung und Schlüsselverwaltung, 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. Authentifizierungsmethoden, die eine Verarbeitung von Passwörtern auf der Serverseite überflüssig machen, sind zu bevorzugen,
- Aufrechterhaltung der Aktualität des Systems (Software und Firmware). Sicherstellung, dass alle IT-Sicherheitsmaßnahmen vorhanden und 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 im Einklang mit Artikel 5 Absatz 2 DSGVO nachweisen zu können, sollte der Verantwortliche Aufzeichnungen über alle durchgeführten Aktualisierungen führen, einschließlich des Zeitpunkts, zu dem sie durchgeführt wurden,

[22] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

[23] Zur sicheren Entwicklung von Webanwendungen siehe auch https://www.owasp.org/index.php/Main_Page.

- Verwendung starker Authentifizierungsmethoden wie Zwei-Faktor-Authentifizierung und Authentifizierungsserver, ergänzt durch eine moderne Passwortpolitik,
- Zu den Standards für eine sichere Entwicklung gehören die Filterung (soweit möglich unter Verwendung von Whitelists) und Maskierung 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,
- starke Benutzerrechte und Zugangskontrollpolitik,
- Einsatz angemessener, aktueller, wirksamer und integrierter Firewall-, Angriffserkennungs- und anderer Perimeterschutzsysteme,
- systematische IT-Sicherheitsprüfungen und Schwachstellenanalysen (Penetrationstests),
- regelmäßige Überprüfungen und Tests, um sicherzustellen, dass Sicherungskopien 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. Bei Verletzungen des Schutzes personenbezogener Daten ist menschliches Versagen besonders hervorzuheben, da es häufig vorkommt. Da diese Arten von Verletzungen sowohl beabsichtigt als auch unbeabsichtigt erfolgen können, können die Verantwortlichen die Schwachstellen nur sehr schwer erkennen und Maßnahmen zu deren Vermeidung ergreifen. Auf der Internationalen Konferenz der Datenschutzbeauftragten wurde die Bedeutung solcher menschlicher Faktoren erkannt und im Oktober 2019 eine Entschließung angenommen, in der die Rolle des menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten behandelt wird.[24] Darin wird betont, dass geeignete Schutzmaßnahmen ergriffen werden sollten, um menschliches Versagen zu verhindern, und es wird eine nicht erschöpfende Liste solcher Schutzmaßnahmen und Ansätze aufgeführt.

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

Der Angestellte eines Unternehmens kopiert während seiner Kündigungsfrist Geschäftsdaten aus der Datenbank des Unternehmens. Der Angestellte hat nur zur Erfüllung seiner Arbeitsaufgaben Zugriff auf die Daten. Monate später, nachdem er gekündigt hat, nutzt er die so gewonnenen Daten (grundlegende Kontaktdaten) für einen neuen Datenverarbeitungsprozess, für den er der Verantwortliche ist und der dazu dient, 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 die Kontaktinformationen der Kunden des Unternehmens kopiert, da er für seine Aufgaben rechtmäßigen Zugriff auf diese Informationen benötigte – und hatte. Da die meisten Aufgaben im Bereich der Kundenbetreuung in irgendeiner Form den Zugriff der Angestellten auf personenbezogene Daten erfordern, sind diese Verletzungen des Schutzes personenbezogener Daten möglicherweise am schwierigsten zu verhindern. Beschränkungen des Zugriffs können die Arbeit des betreffenden Angestellten

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

einschränken. Gut durchdachte Zugangsstrategien und eine ständige Kontrolle können jedoch zur Vermeidung solcher Verletzungen beitragen.

73. Im Rahmen der Risikobewertung sind wie üblich die Art der Verletzung sowie die Art, die Sensibilität und der Umfang der betroffenen personenbezogenen Daten zu berücksichtigen. Bei dieser Art von Verletzungen handelt es sich in der Regel um Verletzungen der Vertraulichkeit, da die Datenbank meistens unversehrt bleibt und ihr Inhalt „lediglich" zur weiteren Verwendung kopiert wird. Auch die Menge der betroffenen Daten ist in der Regel gering oder mittelgroß. In diesem Fall waren keine besonderen Kategorien personenbezogener Daten betroffen, da der Angestellte lediglich die Kontaktinformationen von Kunden benötigte, um nach seinem Ausscheiden aus dem Unternehmen mit ihnen in Kontakt treten zu können. Daher sind die betroffenen Daten nicht sensibel.

74. Auch wenn sich das einzige Ziel des ehemaligen Mitarbeiters, der die Daten böswillig kopiert hat, darauf beschränken mag, die Kontaktinformationen der Kunden des Unternehmens für seine eigenen kommerziellen Zwecke zu erlangen, kann der Verantwortliche das Risiko für die betroffenen Personen nicht als gering einstufen, da er keine Gewissheit über die Absichten des Mitarbeiters hat. Somit könnten die Folgen der Verletzung zwar darauf beschränkt sein, dass die Kunden einer unangemessenen Eigenwerbung durch den ehemaligen Mitarbeiter aussetzt werden, ein weiterer und schwerwiegenderer Missbrauch der gestohlenen Daten ist jedoch nicht ausgeschlossen, je nach dem Zweck der von dem ehemaligen Mitarbeiter vorgenommenen Verarbeitung.[25]

4.1.2 Fall Nr. 08 – Schadensminderung und Pflichten

75. Die Minderung der nachteiligen Auswirkungen der Verletzung 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 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, Daten auf Wechseldatenträger zu kopieren oder herunterzuladen, können hilfreich sein.

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

77. Da die Verletzung kein großes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt, reicht eine Meldung an die Aufsichtsbehörde aus. Die Benachrichtigung der betroffenen Personen könnte jedoch auch für den Verantwortlichen von Vorteil sein, da es möglicherweise besser ist, wenn sie von dem Unternehmen von dem Datenleck erfahren als von dem ehemaligen Mitarbeiter, der versucht, sie zu kontaktieren. Die Dokumentation von Verletzungen des Schutzes personenbezogener Daten gemäß Artikel 33 Absatz 5 ist gesetzlich vorgeschrieben.

[25] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen", siehe Fußnote 10.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	X

4.2 Fall Nr. 09: Versehentliche Übermittlung von Daten an eine vertrauenswürdige Drittpartei

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

4.2.1 Fall Nr. 09 – Vorherige Maßnahmen und Risikobewertung

78. Hier ist die Verletzung nicht auf eine vorsätzliche Handlung eines Mitarbeiters zurückzuführen, sondern auf ein unbeabsichtigtes menschliches Versagen, das durch Unachtsamkeit verursacht wurde. Diese Art von Verletzungen kann vermieden oder in ihrer Häufigkeit verringert werden, indem a) Schulungs-, Aufklärungs- und Sensibilisierungsprogramme durchgeführt werden, bei 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 erfolgen.

79. Diese Verletzung des Schutzes personenbezogener Daten betrifft nur die Vertraulichkeit der Daten, die Integrität und die Verfügbarkeit der Daten bleiben unangetastet. Die Verletzung des Schutzes personenbezogener Daten betraf nur etwa zwei Dutzend Kunden, weshalb die Menge der betroffenen Daten als gering angesehen werden kann. Außerdem enthalten die betroffenen personenbezogenen Daten keine sensiblen Daten. Die Tatsache, dass sich der Datenverarbeiter sofort nach Bekanntwerden der Verletzung mit dem Verantwortlichen in Verbindung gesetzt hat, kann als risikomindernder Faktor betrachtet werden. (Die Möglichkeit, dass Daten an andere Versicherungsvermittler übermittelt wurden, sollte ebenfalls geprüft werden, und falls sich dies bestätigt, sollten geeignete Maßnahmen ergriffen werden). Da nach der Verletzung des Schutzes personenbezogener Daten geeignete Maßnahmen ergriffen wurden, wird sie wahrscheinlich keine Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen haben.

80. Die Kombination aus der geringen Zahl der betroffenen Personen, der sofortigen Aufdeckung der Verletzung und den Maßnahmen, die zur Minimierung der Auswirkungen ergriffen wurden, führt dazu, dass dieser besondere Fall kein Risiko darstellt.

4.2.2 Fall Nr. 09 – Schadensminderung und Pflichten

81. Darüber hinaus spielen auch andere risikomindernde Umstände eine Rolle: Der Versicherungsvermittler ist an das Berufsgeheimnis gebunden, er selbst hat das Problem dem Verantwortlichen gemeldet und die Datei auf Aufforderung gelöscht. Eine Sensibilisierung und möglicherweise zusätzliche Schritte bei der Überprüfung von Dokumenten, die personenbezogene Daten enthalten, werden wahrscheinlich dazu beitragen, ähnliche Fälle in Zukunft zu vermeiden.

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

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	X	X

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

83. Eine Kombination der nachstehend genannten Maßnahmen, die je nach den Besonderheiten des Falles angewandt werden, sollte dazu beitragen, die Wahrscheinlichkeit einer ähnlichen Verletzung zu verringern.

84. Empfehlenswerte Maßnahmen:

(*Die Aufzählung der folgenden Maßnahmen ist keineswegs erschöpfend oder vollständig. Ziel ist es vielmehr, Ideen zur Vorbeugung und mögliche Lösungen aufzuzeigen. Jede Verarbeitungstätigkeit ist anders, daher sollte der 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 robuster und wirksamer Praktiken, Verfahren und Systeme zum Schutz von Daten und Privatsphäre,[27]
- Bewertung der Praktiken, Verfahren und Systeme zum Schutz der Privatsphäre, um eine fortlaufende Wirksamkeit zu gewährleisten,[28]
- Erstellung angemessener Zugangskontrollstrategien und Erzwingen der Einhaltung der Regeln durch die Benutzer,
- Anwendung von Techniken, die eine Benutzerauthentifizierung beim Zugriff auf sensible persönliche Daten erzwingen,

[26] Abschnitt 2 Unterabschnitt i der Entschließung zur Rolle des menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten.
[27] Abschnitt 2 Unterabschnitt ii der Entschließung zur Rolle des menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten.
[28] Abschnitt 2 Unterabschnitt iii der Entschließung zur Rolle des menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten.

- Deaktivierung des unternehmensbezogenen Kontos des Nutzers, sobald die Person das Unternehmen verlässt,
- Überprüfung ungewöhnlicher Datenflüsse zwischen dem Dateiserver und den Arbeitsplätzen der Mitarbeiter,
- Einrichtung der I/O-Schnittstellensicherheit im BIOS oder durch den Einsatz von Software, die die Nutzung von Computerschnittstellen kontrolliert (Sperren oder Entsperren von z. B. USB/CD/DVD usw.),
- Überprüfung der Zugriffsrichtlinien der Mitarbeiter (z. B. Protokollierung des Zugriffs auf sensible Daten und Anforderung an den Nutzer, einen geschäftlichen Grund anzugeben, damit dieser für Audits zur Verfügung steht),
- Deaktivierung offener Cloud-Dienste,
- Verbieten und Verhindern des Zugriffs auf bekannte offene E-Mail-Dienste,
- Deaktivierung der Bildschirmdruckfunktion im Betriebssystem,
- Durchsetzung einer Strategie des aufgeräumten Schreibtisches,
- automatisches Sperren aller Computer nach einer bestimmten Zeit der Inaktivität,
- Verwendung von Mechanismen (z. B. (drahtlose) Token zur Anmeldung/zum Öffnen gesperrter Konten) für schnelle Benutzerwechsel in gemeinsam genutzten Umgebungen,
- Verwendung spezieller Systeme für die Verwaltung personenbezogener Daten, die angemessene Zugangskontrollmechanismen anwenden und menschliche Fehler, wie etwa das Senden von Mitteilungen an die falsche Person, verhindern. Die Verwendung von Tabellenkalkulationen und anderen Bürodokumenten ist kein geeignetes Mittel für die Verwaltung von Kundendaten.

5 VERLORENE ODER GESTOHLENE GERÄTE UND PAPIERDOKUMENTE

85. Häufig kommt es zum Verlust oder Diebstahl von tragbaren Geräten. In diesen Fällen muss der 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 sind von Bedeutung für die möglichen Auswirkungen einer Verletzung des Schutzes personenbezogener Daten. Die Risikobewertung ist unter Umständen schwierig, da das Gerät nicht mehr verfügbar ist.

86. Diese Art von Verletzungen kann immer als Verletzung der Vertraulichkeit eingestuft werden. Gibt es jedoch keine Sicherungskopie der gestohlenen Datenbank, kann es sich bei der Verletzung auch um eine Verletzung der Verfügbarkeit und der Integrität handeln.

87. Die folgenden Szenarien zeigen, wie die oben genannten Umstände die Wahrscheinlichkeit und Schwere einer Verletzung des Schutzes personenbezogener Daten beeinflussen.

5.1 Fall Nr. 10: Gestohlenes Gerät 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 Bildung der Kinder. Sowohl die verschlüsselten Tablets, die zum Zeitpunkt des Einbruchs ausgeschaltet waren, als auch die App waren durch ein starkes Passwort geschützt. Sicherungsdaten waren für den Verantwortlichen wirksam und ohne Weiteres verfügbar. Kurz nachdem die Kindertagesstätte von dem Einbruch erfahren hatte, ordnete sie remote an, die Geräte aufzuräumen.

5.1.1 Fall Nr. 10 – Vorherige Maßnahmen und Risikobewertung

88. In diesem Fall hat der Verantwortliche angemessene Maßnahmen ergriffen, um die Folgen einer möglichen Verletzung des Schutzes personenbezogener Daten 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 empfehlenswerter Maßnahmen findet sich in Abschnitt 5.7).

89. Nachdem er von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt hat, sollte der Verantwortliche die Risikoquelle, die Systeme zur Unterstützung der Datenverarbeitung, die Art der betroffenen personenbezogenen Daten und die möglichen Auswirkungen der Verletzung des Schutzes personenbezogener Daten auf die betroffenen Personen bewerten. Bei der oben beschriebenen Verletzung des Schutzes personenbezogener Daten wären die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten betroffen gewesen. Aufgrund der angemessenen Maßnahmen des Verantwortlichen vor und nach der Verletzung kam es jedoch zu keiner dieser Beeinträchtigungen.

5.1.2 Fall Nr. 10 – Schadensminderung und Pflichten

90. Die Vertraulichkeit der persönlichen Daten auf den Geräten war aufgrund des starken Passwortschutzes sowohl auf den Tablets als auch in den Apps nicht gefährdet. Die Tablets waren so eingerichtet, dass die Festlegung eines Passworts zugleich die Verschlüsselung der Daten auf dem Gerät bedeutet. Dies wurde noch dadurch verstärkt, dass der Verantwortliche versuchte, sämtliche Daten von den gestohlenen Geräten aus der Ferne zu löschen.

91. Aufgrund der getroffenen Maßnahmen blieb auch die Vertraulichkeit der Daten gewahrt. Außerdem gewährleistete die Datensicherung die ständige Verfügbarkeit der personenbezogenen Daten, sodass keine potenziellen negativen Auswirkungen hätten auftreten können.

92. Aufgrund dieser Tatsachen war es unwahrscheinlich, dass die oben beschriebene Verletzung des Schutzes personenbezogener Daten zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führte, weshalb keine Meldung an die Aufsichtsbehörde oder Benachrichtigung der betroffenen Personen erforderlich war. Allerdings muss auch diese Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 Absatz 5 dokumentiert werden.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	X	X

5.2 Fall Nr. 11: Gestohlenes Gerät mit nicht verschlüsselten personenbezogenen Daten

Das Notebook eines Mitarbeiters eines Dienstleistungsunternehmens wurde gestohlen. Das gestohlene Notebook enthielt Namen, Vornamen, Geschlecht, Adressen und Geburtsdaten von mehr als 100 000 Kunden. Da das Gerät gestohlen wurde, 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. Persönliche Daten konnten aus täglichen erstellten Sicherungskopien wiederhergestellt werden.

5.2.1 Fall Nr. 11 – Vorherige Maßnahmen und Risikobewertung

93. Der Verantwortliche hat keine vorherigen Sicherheitsmaßnahmen getroffen, weshalb die auf dem gestohlenen Notebook gespeicherten personenbezogenen Daten für den Dieb oder jede andere Person, die später in den Besitz des Geräts gelangt, leicht zugänglich waren.

94. Diese Verletzung des Schutzes personenbezogener Daten 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 stellt die Identifizierung der betroffenen Personen ebenfalls ein Problem dar, was die Schwere der Verletzung zusätzlich erhöht. Die beträchtliche Zahl der betroffenen Personen erhöht das Risiko, dennoch waren keine besonderen Kategorien personenbezogener Daten von der Verletzung betroffen.

96. Bei der Risikobewertung[29] sollte der Verantwortliche die möglichen Folgen und nachteiligen Auswirkungen der Verletzung der Vertraulichkeit berücksichtigen. Die Verletzung des Schutzes personenbezogener Daten kann dazu führen, dass die betroffenen Personen aufgrund der auf dem gestohlenen Gerät gespeicherten Daten Opfer eines Identitätsbetrugs werden, weshalb das Risiko als hoch einzustufen ist.

5.2.2 Fall Nr. 11 – Schadensminderung und Pflichten

97. Die Aktivierung der Geräteverschlüsselung und die Verwendung eines starken Passwortschutzes für die gespeicherte Datenbank hätten verhindern können, dass die Verletzung des Schutzes personenbezogener Daten ein Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt.

98. Aufgrund dieser Umstände sind nicht nur die Meldung an die Aufsichtsbehörde, sondern auch die Benachrichtigung der betroffenen Personen erforderlich.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	✓

5.3 Fall Nr. 12: Gestohlene Papierakten mit sensiblen Daten

Aus einer Rehabilitationseinrichtung für Drogenabhängige wurde ein Patientenbuch in Papierform gestohlen. Das Buch enthielt grundlegende Identitäts- und Gesundheitsdaten der Patienten, die in die Rehabilitationseinrichtung aufgenommen wurden. Die Daten wurden 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 Verantwortliche verfügte weder über ein Zugangskontrollsystem noch über eine andere Sicherheitsmaßnahme für die Papierdokumentation.

5.3.1 Fall Nr. 12 – Vorherige Maßnahmen und Risikobewertung

99. Der Verantwortliche hat keine vorherigen Sicherheitsmaßnahmen getroffen, weshalb die in diesem Buch gespeicherten personenbezogenen Daten für die Person, die es gefunden hat, leicht zugänglich waren. Außerdem ist der Mangel an Sicherungsdaten angesichts der Art der in dem Buch gespeicherten personenbezogenen Daten ein sehr ernster Risikofaktor.

[29] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

100. Dieser Fall dient als Beispiel für eine mit hohem Risiko behaftete Verletzung des Schutzes personenbezogener Daten. Aufgrund fehlender angemessener Sicherheitsvorkehrungen gingen sensible Gesundheitsdaten gemäß Artikel 9 Absatz 1 DSGVO verloren. Da es sich in diesem Fall um eine besondere Kategorie personenbezogener Daten handelte, wurde das potenzielle Risiko für die betroffenen Personen erhöht, was von dem für die Risikobewertung Verantwortlichen ebenfalls berücksichtigt werden sollte.[30]

101. Diese Verletzung betrifft die Vertraulichkeit, Verfügbarkeit und Integrität der betroffenen personenbezogenen Daten. Die Verletzung der ärztlichen Schweigepflicht kann dazu führen, dass unbefugte Dritte Zugang zu den privaten medizinischen Patientendaten erhalten, was schwerwiegende Folgen für das Privatleben 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 – Schadensminderung und Pflichten

102. Bei der Bewertung der Sicherungsmaßnahmen sollte auch die Art des zu sichernden Objekts berücksichtigt werden. Da das Patientenbuch 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 versperrten Zimmer sowie eine angemessene Zugangskontrolle mit Authentifizierung beim Zugriff darauf hätten die Verletzung des Schutzes personenbezogener Daten verhindern können.

103. Die oben beschriebene Verletzung des Schutzes personenbezogener Daten kann schwerwiegende Folgen für die betroffenen Personen haben; daher ist die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen über die Verletzung erforderlich.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	chrichtigung der betroffenen Personen
✓	✓	✓

5.4 Organisatorische und technische Maßnahmen zur Vorbeugung/Milderung der Auswirkungen von Verlust oder Diebstahl von Geräten

104. Eine Kombination der nachstehend genannten Maßnahmen, die je nach den Besonderheiten des Falles angewandt werden, sollte dazu beitragen, die Wahrscheinlichkeit einer ähnlichen Verletzung zu verringern.

105. Empfehlenswerte Maßnahmen:

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

- Aktivierung der Geräteverschlüsselung (z. B. Bitlocker, Veracrypt oder DM-Crypt),
- Verwendung eines Passcodes/Passworts auf allen Geräten. Verschlüsselung aller mobilen elektronischen Geräte dahin gehend, dass zur Entschlüsselung die Eingabe eines komplexen Passworts erforderlich ist,
- Verwendung einer mehrstufigen Authentifizierung,
- Aktivierung von Lokalisierungsfunktionen für hochmobile Geräte, damit diese im Fall von Verlust oder Verlegen lokalisiert werden können,

[30] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

- Verwendung einer Software/Anwendung zur Verwaltung mobiler Geräte (Mobile Devices Management, MDM) und Lokalisierung. Einsatz von Blendschutzfiltern. Abschaltung aller unbeaufsichtigten Geräte,
- soweit möglich und für die betreffende Datenverarbeitung geeignet, Speicherung der personenbezogenen Daten nicht auf einem mobilen Gerät, sondern auf einem zentralen Back-End-Server,
- wenn der Arbeitsplatz mit dem Unternehmensnetzwerk verbunden ist, Durchführung einer automatischen Sicherung von den Arbeitsordnern, sofern es unvermeidbar ist, dass dort personenbezogene Daten gespeichert werden,
- Verwendung eines sicheren VPN (das z. B. einen separaten zweiten Authentifizierungsschlüssel für den Aufbau einer sicheren Verbindung erfordert), um mobile Geräte mit Back-End-Servern zu verbinden,
- Bereitstellung von physischen Schlössern für Mitarbeiter, damit diese die von ihnen verwendeten mobilen Geräte physisch sichern können, wenn sie unbeaufsichtigt sind,
- angemessene Regulierung der Gerätenutzung außerhalb des Unternehmens,
- angemessene Regulierung der Gerätenutzung innerhalb des Unternehmens,
- Verwendung von MDM-Software/Anwendungen und Aktivierung der ferngesteuerten Löschfunktion,
- Verwendung eines zentralisierten Geräteverwaltungssystems mit minimalen Rechten für die Endnutzer zur Installation von Software,
- Installation von physischen Zugangskontrollen,
- Vermeidung der Speicherung sensibler Informationen auf mobilen Geräten oder Festplatten. Wenn auf das interne System des Unternehmens zugegriffen werden muss, sollten sichere Kanäle verwendet werden, wie bereits erwähnt.

6 POSTVERSEHEN

106. Die Risikoquelle ist auch in diesem Fall ein internes menschliches Versagen, wobei hier jedoch keine böswillige Handlung zu der Verletzung führte. Sie ist das Ergebnis von Unachtsamkeit. Der Verantwortliche kann im Nachhinein nur wenig unternehmen, weshalb die Vorbeugung in diesen Fällen noch wichtiger ist als bei anderen Arten von Sicherheitsverletzungen.

6.1 Fall Nr. 13: Postversandfehler

Zwei bestellte Schuhe wurden von einem Einzelhandelsunternehmen verpackt. Durch menschliches Versagen wurden zwei Packzettel verwechselt, sodass beide Produkte und die dazugehörigen Packzettel an die falsche Person geschickt wurden. Somit erhielten die beiden Kunden die Bestellungen des jeweils anderen, einschließlich der Packzettel mit den personenbezogenen Daten. Nach Bekanntwerden der Verletzung des Schutzes personenbezogener Daten rief der Verantwortliche die Bestellungen zurück und schickte sie an die richtigen Empfänger.

6.1.1 Fall Nr. 13 – Vorherige Maßnahmen und Risikobewertung

107. Die Zettel enthielten die für eine ordnungsgemäße 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 zu erheblichen negativen Auswirkungen führen könnte, betroffen waren, die Verletzung nicht auf einen systematischen Fehler des 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 – Schadensminderung und Pflichten

108. Der Verantwortliche sollte für eine kostenlose Rücksendung der Gegenstände und der dazugehörigen Zettel sorgen und die falschen Empfänger auffordern, alle etwaigen Kopien der Zettel, die die personenbezogenen Daten der anderen Person enthalten, zu vernichten bzw. zu löschen.

109. Auch wenn die Verletzung 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	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	X	X

6.2 Fall Nr. 14: Versehentlicher Versand höchst vertraulicher personenbezogener Daten per E-Mail

Die Abteilung für Beschäftigung einer öffentlichen Verwaltung schickte eine E-Mail-Nachricht über bevorstehende Schulungen an die Personen, die in ihrem System als Arbeitssuchende registriert waren. Versehentlich wurde dieser E-Mail ein Dokument mit den persönlichen Daten all dieser Arbeitssuchenden (Name, E-Mail-Adresse, Postadresse, Sozialversicherungsnummer) beigefügt. Die Zahl der betroffenen Personen beläuft sich auf mehr als 60 000. Die Behörde 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. Es sollte die Einführung zusätzlicher Kontrollmechanismen in Betracht gezogen werden.

111. Die Zahl der betroffenen Personen ist beträchtlich, und die Einbeziehung ihrer Sozialversicherungsnummer zusammen mit anderen, grundlegenderen personenbezogenen Daten erhöht das als hoch einzustufende Risiko zusätzlich.[31] Die eventuelle Weitergabe der Daten durch einen der Empfänger kann von dem Verantwortlichen nicht verhindert werden.

6.2.2 Fall Nr. 14 – Schadensminderung und Pflichten

112. Wie bereits erwähnt, gibt es nur begrenzte Mittel, um die Risiken einer derartigen Verletzung wirksam zu mindern. Der Verantwortliche hat zwar um die Löschung der Nachricht gebeten, aber er kann 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	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	✓

[31] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen“, siehe Fußnote 10.

6.3 Fall Nr. 15: Versehentlicher Versand personenbezogener Daten per E-Mail

Eine Teilnehmerliste für einen Kurs in englischer Rechtssprache, der fünf Tage lang in einem Hotel stattfindet, wird versehentlich an 15 ehemalige Teilnehmer des Kurses und nicht an das Hotel geschickt. Die Liste enthält Namen, E-Mail-Adressen und Ernährungsvorlieben der 15 Teilnehmer. Nur zwei Teilnehmer haben Angaben zu ihren Ernährungsvorlieben gemacht und angegeben, dass sie eine Laktoseintoleranz haben. Keiner der Teilnehmer hat eine geschützte Identität. Der Verantwortliche entdeckt den Fehler unmittelbar nach dem Versenden der Liste und informiert die Empfänger über den Fehler und bittet sie, die Liste zu löschen.

6.3.1 Fall Nr. 15 – Vorherige Maßnahmen und Risikobewertung

114. Für die Übermittlung Nachrichten mit personenbezogenen Daten hätten strenge Regeln eingeführt werden müssen. Es sollte die Einführung zusätzlicher Kontrollmechanismen 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. Zu den personenbezogenen Daten gehören sensible Daten über die Ernährungsvorlieben von zwei Teilnehmern. Auch wenn es sich bei der Information, dass jemand laktoseintolerant ist, um Gesundheitsdaten handelt, ist das Risiko, dass diese Daten in nachteiliger Weise verwendet werden, als relativ gering anzusehen. Obwohl 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 Fall kein Risiko festgestellt werden, dass die Verletzung einen physischen, materiellen oder immateriellen Schaden für die betroffene Person aufgrund der unbefugten Weitergabe von Informationen über Laktoseintoleranz zur Folge hat. Im Gegensatz zu einigen anderen Ernährungsvorlieben kann die Laktoseintoleranz normalerweise nicht mit religiösen oder weltanschaulichen 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 – Schadensminderung und Pflichten

116. Zusammenfassend lässt sich feststellen, dass die Verletzung keine wesentlichen Auswirkungen auf die betroffenen Personen hatte. Die Tatsache, dass sich der Verantwortliche sofort nach Bekanntwerden des Fehlers mit den Empfängern in Verbindung gesetzt hat, kann als mildernder Umstand betrachtet werden.

117. Wird eine E-Mail an einen falschen/unbefugten Empfänger gesendet, wird empfohlen, dass der Verantwortliche eine Folge-E-Mail mit der Funktion für Blindkopien an die unbeabsichtigten Empfänger sendet, in der er sich entschuldigt, die Löschung der betreffenden E-Mail fordert und den Empfängern mitteilt, dass sie nicht berechtigt sind, die ihnen mitgeteilten E-Mail-Adressen weiter zu verwenden.

118. Aufgrund dieser Tatsachen war es unwahrscheinlich, dass die Datenschutzverletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führte, weshalb keine Meldung an die Aufsichtsbehörde oder Benachrichtigung die betroffenen Personen erforderlich war. Allerdings muss auch diese Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 Absatz 5 dokumentiert werden.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	X	X

[32] Siehe Leitlinien WP 250, S. 27.

6.4 Fall Nr. 16: Postversandfehler

Eine Versicherungsgruppe bietet Kfz-Versicherungen an. Dazu verschickt sie regelmäßig angepasste Beitragspolicen per Post. Das Schreiben enthält neben dem Namen und der Adresse des Versicherungsnehmers das Kfz-Kennzeichen ohne maskierte Ziffern, die Versicherungstarife des laufenden und des nächsten Versicherungsjahres, die ungefähre Jahreskilometerleistung und das Geburtsdatum des Versicherungsnehmers. Gesundheitsdaten im Sinne von Artikel 9 DSGVO, Zahlungsdaten (Bankverbindung), wirtschaftliche und finanzielle Daten 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 Post an einen Versicherungsnehmer verschickt. Der Versicherungsnehmer öffnet den Brief zu Hause und wirft einen Blick auf seinen korrekt zugestellten Brief sowie auf den falsch zugestellten Brief eines anderen Versicherungsnehmers.

6.4.1 Fall Nr. 16 – Vorherige Maßnahmen und Risikobewertung

119. Der falsch zugestellte Brief enthält den Namen, die Adresse, das Geburtsdatum, das unmaskierte 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 über die Erhöhung der Versicherungstarife dem unberechtigten Empfänger offenbart werden. Die Wahrscheinlichkeit, dass diese Daten missbraucht werden, wird als gering bis mittel eingeschätzt. Zwar werden viele Empfänger den fälschlicherweise erhaltenen Brief wahrscheinlich im Müll entsorgen, doch kann in Einzelfällen nicht völlig ausgeschlossen werden, dass der Brief in sozialen Netzwerken gepostet oder der Versicherungsnehmer kontaktiert wird.

6.4.2 Fall Nr. 16 – Schadensminderung und Pflichten

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

121. Vermutlich wird es nie möglich sein, einen Postzustellungsfehler 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 eine solche Verletzung zur Folge hat.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	X

6.5 Organisatorische und technische Maßnahmen zur Vorbeugung/Milderung der Auswirkungen von Postversehen

122. Eine Kombination der nachstehend genannten Maßnahmen, die je nach den Besonderheiten des Falles angewandt werden, sollte dazu beitragen, die Wahrscheinlichkeit einer ähnlichen Verletzung zu verringern.

123. Empfehlenswerte Maßnahmen:

(*Die Aufzählung der folgenden Maßnahmen ist keineswegs erschöpfend oder vollständig. Ziel ist es vielmehr, Ideen zur Vorbeugung und mögliche Lösungen aufzuzeigen. Jede Verarbeitungstätigkeit ist anders, daher*

sollte der Verantwortliche entscheiden, welche Maßnahmen für die jeweilige Situation am besten geeignet sind.)

- Festlegung genauer Vorgaben – ohne Interpretationsspielraum – für den Versand von Briefen/E-Mails,
- angemessene Schulung des Personals für den Versand von Briefen/E-Mails,
- standardmäßige Auflistung von Empfängern im Feld „Bcc“ beim Versand von E-Mails an mehrere Empfänger,
- erforderliche zusätzliche Bestätigung beim Versand von E-Mails an mehrere Empfänger, die nicht im Feld „Bcc“ aufgeführt sind,
- Anwendung des Vier-Augen-Prinzips,
- automatische Adresseingabe anstelle der manuellen Eingabe, wobei die Daten aus einer verfügbaren und aktuellen Datenbank entnommen werden; das automatische Adressierungssystem sollte regelmäßig überprüft werden, damit versteckte Fehler und falsche Einstellungen erkannt werden,
- Anwendung der Nachrichtenverzögerung (z. B. die Nachricht kann innerhalb einer bestimmten Zeitspanne nach Anklicken der Drucktaste gelöscht/bearbeitet werden),
- Deaktivierung der automatischen Vervollständigung bei der Eingabe von E-Mail-Adressen,
- Veranstaltungen zur Sensibilisierung für die häufigsten Fehler, 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 benachrichtigen ist (Einbeziehung des behördlichen Datenschutzbeauftragten).

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, die in den Verfahren des Unternehmens festgelegt sind. Der Anrufer macht korrekte Angaben zur Steuernummer und Postadresse des gewünschten Kunden (da er Zugang zu diesen Informationen hatte). Nach der Validierung nimmt der Mitarbeiter die gewünschte Änderung vor, und die Rechnungsdaten werden an die neue E-Mail-Adresse gesendet. Bei diesem Verfahren ist keine Sendung der Benachrichtigung an die bisherige E-Mail-Adresse vorgesehen. Im darauffolgenden Monat wendet sich der rechtmäßige Kunde an das Unternehmen und fragt, warum er keine Rechnungen an seine E-Mail-Adresse erhält, und bestreitet, dass er angerufen und die Änderung der E-Mail-Adresse verlangt hat. 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, Schadensminderung und Pflichten

124. Dieser Fall dient als Beispiel für die Bedeutung von vorherigen Maßnahmen. Die Verletzung stellt unter dem Risikoaspekt ein hohes Risiko dar,[33] da die Abrechnungsdaten Aufschluss über das Privatleben der betroffenen Person geben können (z. B. Gewohnheiten, Kontakte) und zu einem materiellen Schaden führen könnten (z. B. Stalking, Gefährdung der körperlichen Integrität). Die bei diesem Angriff erlangten personenbezogenen Daten können auch verwendet werden, um die Übernahme von Konten in diesem Unternehmen zu erleichtern oder weitere Authentifizierungsmaßnahmen in anderen Unternehmen auszunutzen. In Anbetracht dieser Risiken sollte die „angemessene" Authentifizierungsmaßnahme hohe Anforderungen erfüllen, je nachdem, welche personenbezogenen Daten infolge der Authentifizierung verarbeitet werden können.

125. Folglich sind sowohl eine Meldung an die Aufsichtsbehörde als auch eine Benachrichtigung der betroffenen Person durch den Verantwortlichen erforderlich.

126. Das bisherige Verfahren zur Kundenvalidierung muss im Hinblick auf diesen Fall eindeutig verfeinert werden. Die zur Authentifizierung verwendeten Methoden waren nicht ausreichend. Der böswillige Angreifer war in der Lage, sich als der vorgesehene Nutzer auszugeben, indem er öffentlich zugängliche Informationen und Informationen, auf die er anderweitig Zugriff hatte, nutzte.

127. Die Verwendung dieser Art von statischer wissensbasierter 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 das Unternehmen eine Form der Authentifizierung verwenden, bei der mit hoher Wahrscheinlichkeit davon ausgegangen werden kann, dass es sich bei dem authentifizierten Nutzer um die gewünschte Person und nicht um eine andere handelt. Die Einführung einer mehrstufigen Authentifizierungsmethode außerhalb der Bandbreite würde das Problem lösen, z. B. um die Änderungsanforderung zu überprüfen, indem eine Bestätigungsanfrage an die bisherige E-Mail-Adresse gesendet wird oder indem zusätzliche Fragen gestellt und Informationen verlangt werden, die nur auf den früheren Rechnungen sichtbar sind. Es obliegt dem Verantwortlichen zu entscheiden, welche Maßnahmen er einführen will, da er die Details und Anforderungen seiner internen Abläufe am besten kennt.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	✓

[33] Für Leitlinien zu Verarbeitungen, die „wahrscheinlich ein hohes Risiko mit sich bringen", siehe Fußnote 10.

7.2 Fall Nr. 18: Exfiltration von E-Mails

Eine Supermarktkette entdeckte drei Monate nach ihrer Einrichtung, dass einige E-Mail-Konten verändert und Befehle erstellt worden waren, damit 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 auf seine eigene geändert. Schließlich waren zu diesem Zeitpunkt bereits mehrere gefälschte Rechnungen mit der neuen Bankverbindung verschickt worden. Das Überwachungssystem der E-Mail-Plattform gab schließlich eine Warnung in Bezug auf die Ordner aus. Das Unternehmen konnte nicht feststellen, wie der Angreifer überhaupt Zugang zu den E-Mail-Konten erlangen konnte, vermutete aber, dass dies auf eine infizierte E-Mail zurückzuführen war, mit der Zugang zur für den Zahlungsverkehr zuständigen Benutzergruppe gewährt wurde.

Durch die schlagwortbasierte Weiterleitung von E-Mails erhielt der Angreifer folgende Daten von 99 Arbeitnehmern: Name und Lohn eines bestimmten Monats von 89 betroffenen Personen, Name, Familienstand, Anzahl der Kinder, Lohn, Arbeitszeiten und restliche Daten über den Gehaltseingang von 10 Arbeitnehmern, deren Verträge beendet wurden. Der Verantwortliche benachrichtigte nur die 10 Arbeitnehmer, die zu der letztgenannten Gruppe gehören.

7.2.1 Fall Nr. 18 - Risikobewertung, Schadensminderung und Pflichten

129. Auch wenn der Angreifer wahrscheinlich nicht zum Ziel hatte, personenbezogene Daten zu erheben, ist die Verletzung des Schutzes personenbezogener Daten voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden, da die Verletzung 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. Daher sollte die Datenschutzverletzung allen 99 Arbeitnehmern mitgeteilt werden und nicht nur den 10 Arbeitnehmer, deren Gehaltsdaten offengelegt wurden.

130. Sobald der Verantwortliche von der Verletzung erfuhr, veranlasste er eine Passwortänderung für die angegriffenen 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 Handlungen, entfernte die vom Angreifer eingerichteten Regeln und verfeinerte die Warnmeldungen des Überwachungssystems, damit eine Warnung ausgegeben wird, sobald eine automatische Regel erstellt wird. Stattdessen könnte der Verantwortliche den Nutzern das Recht entziehen, Weiterleitungsregeln festzulegen, wodurch das IT-Dienstleistungsteam dies nur noch auf Anfrage tun müsste, oder er könnte eine Politik einführen, wonach die Nutzer die in ihren Konten festgelegten Regeln einmal pro Woche oder in Bereichen, in denen Finanzdaten verarbeitet werden, häufiger überprüfen und darüber Bericht erstatten sollten.

131. Die Tatsache, dass eine Verletzung so lange unentdeckt bleiben konnte, und die Tatsache, dass in einem längeren Zeitraum Social Engineering zur Änderung weiterer Daten hätte eingesetzt werden können, machte erhebliche Probleme im IT-Sicherheitssystem des Verantwortlichen deutlich. Diese sollten unverzüglich behandelt werden, z. B. durch die Verstärkung von Automatisierungsprüfungen und Änderungskontrollen sowie Maßnahmen zur Erkennung von und Reaktion auf Vorfälle. Verantwortliche, die mit sensiblen Daten, Finanzdaten usw. umgehen, tragen eine größere Verantwortung für die Gewährleistung einer angemessenen Datensicherheit.

Erforderliche Maßnahmen auf der Grundlage der ermittelten Risiken		
Interne Dokumentation	Meldung an die Aufsichtsbehörde	Benachrichtigung der betroffenen Personen
✓	✓	✓