www.jusletter-it.eu

Daniel W. Seiler / Marcel Griesinger

Anforderungen an die Datensicherheit nach dem revidierten Datenschutzgesetz unter besonderer Berücksichtigung der Cyber-Sicherheit

Eine wirksame und effektive Sicherheitsstrategie von Unternehmen und staatlichen Stellen setzt wirksame Massnahmen zur Daten- und Cyber-Sicherheit voraus. Dabei gilt es neben zielführenden, konkreten Massnahmen auch die gesetzlichen Anforderungen umzusetzen. Der Beitrag von Seiler/Griesinger stellt die gesetzlichen Rahmenbedingungen zum Thema Daten- und Cybersicherheit dar und beschäftigt sich sodann mit konkreten technisch-organisatorischen Massnahmen, die in einem Datensicherheitskonzept enthalten sein sollten.

Beitragsart: Beiträge
Region: Schweiz
Rechtsgebiete: Datenschutz, IT-Recht

Zitiervorschlag: Daniel W. Seiler / Marcel Griesinger, Anforderungen an die Datensicherheit nach dem revidierten Datenschutzgesetz unter besonderer Berücksichtigung der Cyber-Sicherheit, in: Jusletter IT 26. April 2022

Inhaltsübersicht

I. Einleitung
II. Überblick zu den rechtlichen Grundlagen der Datensicherheit
1. Datenschutzgesetz (revDSG)
2. Vorentwurf der Verordnung zum revidierten Datenschutzgesetz (VE-VDSG)
3. Rechtsvergleich mit den Regelungen der EU-Datenschutzgrundverordnung (DSGVO)
III. Der Themenkomplex Cyber-Sicherheit
1. Cyberrisiken
2. Arten von Schutz-Massnahmen
3. Ausgewählte organisatorische Massnahmen
a) Bewusstsein des Managements über Risiken
b) Bewusstsein der Mitarbeitenden
c) Zuständigkeiten
d) Verhalten im Umgang mit E-Mail
e) Umgang mit Daten
f) Unternehmensinformationen im Internet
g) Passwörter
h) Zugriffsberechtigungen
i) IT-Dienstleister
4. Ausgewählte technische Massnahmen
a) Sicherheits-Updates
b) Regelmässige Datensicherung
c) Schutz vor Viren
d) Firewall
e) Fernzugriff
f) Cloud-Dienste
g) Log-Dateien
h) Netzsegmentierung
i) Verschlüsselung
IV. Grundelemente eines sog. Datensicherheitskonzept
V. Conclusio

I. Einleitung

[1] Die Bedeutung der Daten- und Cybersicherheit nimmt aus technischer, organisatorischer und rechtlicher Sicht stetig zu. Die Schweiz verfügt mit dem Nationalen Zentrum für Cybersicherheit (NCSC) über ein Kompetenzzentrum für Cybersicherheit, welches auch als Anlaufstelle für alle Fragen zur Cybersicherheit dient.[1]

[2] Die jüngsten geopolitischen Entwicklungen und Krisensituationen verdeutlichen, dass die Datensicherheit und mit ihr einhergehend die Cyber-Sicherheit zu zentralen Elementen der Sicherheitsstrategie von Unternehmen und staatlichen Einrichtungen gehören.[2] Vor diesem Hinter-

1 Vgl. Art. 12 Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020 (Stand am 1. April 2021), SR 120.73.

2 Vgl. u.a. Tätigkeitsbeschreibung des Nationalen Zentrums für Cybersicherheit https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/das-ncsc.html, zuletzt aufgerufen am 11. März 2022;Bericht zur Münchner Cyber Sicherheitskonferenz (MCSC) https://www.deutschlandfunk.de/cyber-attacken-ukraine-muenchner-cyber-sicherheits-konferenz-100.html, zuletzt aufgerufen am 13. März 2022; Bericht im Handelsblatt zur Gefahr von Cyberangriffen auf Bereich der kritischen Infrastruktur vom 22.2.2022 https://www.handelsblatt.com/politik/international/ukrainekrise-alarmstufe-rot-sicherheitsbehoerden-fuerchten-massive-attacken-russischer-hacker-auf-energie-versorgung/28092032.html, zuletzt aufgerufen am 13. März 2022; hinzuweisen ist aber auch darauf, dass vor dem Hintergrund des Krieges in der Ukraine aktuell kein Anstieg von Cyberangriffen auf die Schweiz festgestellt wur-

grund beschäftigt sich der nachfolgende Beitrag einerseits mit den rechtlichen Anforderungen an die Datensicherheit und andererseits besonders mit dem Themenkomplex Cyber-Sicherheit. Dabei wird neben dem rechtlichen Regelwerk auch zusammenfassend dargestellt, welche konkreten Handlungsweisen in der Praxis angezeigt sind und welche Grundelemente aus Sicht der Autoren in einem sog. Datensicherheitskonzept enthalten sein sollen.

II. Überblick zu den rechtlichen Grundlagen der Datensicherheit

[3] Die Datensicherheit ist in Art. 8 des revidierten Datenschutzgesetzes[3] (revDSG) geregelt. Darüber hinaus sind konkretisierende Regelungen in der Verordnung zum Datenschutzgesetz[4] (VDSG) vorgesehen. Die Verordnung befindet sich nach Abschluss der Vernehmlassung zum Vorentwurf zur VDSG im Oktober 2021 derzeit noch in der Ausarbeitung.

1. Datenschutzgesetz (revDSG)

[4] Nach der Totalrevision des Datenschutzgesetzes[5] ist die Datensicherheit nunmehr in Art. 8 revDSG geregelt. Hiernach haben der Verantwortliche und der Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten (Art. 8 Abs. 1 revDSG). Dabei müssen es die Massnahmen ermöglichen, Verletzungen der Datensicherheit zu vermeiden (Art. 8 Abs. 2 revDSG). Der Gesetzgeber verfolgt dabei einen sog. risikobasierten Ansatz.[6] Die zu treffenden Massnahmen haben sich demnach am jeweiligen Risiko einer Verletzung der Datensicherheit zu orientieren.[7] Als mögliche Massnahmen im Sinne von Art. 8 Abs. 2 revDSG werden vom Gesetzgeber in der Botschaft zum revidierten Datenschutzgesetz beispielhaft die Pseudonymisierung von Personendaten, Massnahmen zur Wahrung der Vertraulichkeit und Verfügbarkeit von Systemen oder Diensten sowie Verfahren zur Prüfung und Analyse der Wirksamkeit von Sicherheitsmassnahmen genannt.[8] Ebenso wird das Vorhalten einer geeigneten Sicherheitsarchitektur für die jeweiligen Systeme angesprochen, um einen Verlust von Daten oder durch sog. Schadsoftware (Malware) zu verhindern.[9] Weitere, in der Praxis zur Anwendung kommende Standard-Massnahmen zur Gewährleistung der Datensicherheit sind u.a. Zugriffs- und Zugangsbeschränkungen, Schutzsoftware und Firewalls, Verschlüsselungen von Daten, Massnahmen zum Passwortschutz und zur Passwortsicherheit, Back-Ups, verschiede-

---

de, vgl. Medienmitteilung des NCSC https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/aktuelle_cyberlage.html, zuletzt aufgerufen am 14. März 2022; Medienmitteilung des deutschen Bundesamtes für Sicherheit in der Informationstechnik mit der Warnung vor dem Einsatz von Kaspersky-Virenschutzprodukten, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html, zuletzt aufgerufen am 15. März 2022.

3 Das revidierte Datenschutzgesetz wird zum 1. September 2023 in Kraft treten.

4 Die Verordnung zum revidierten Datenschutzgesetz wird ebenfalls am 1. September 2023 in Kraft treten.

5 Vgl. hierzu Griesinger, Ein Überblick über das neue Schweizer Datenschutzgesetz (DSG), PinG 2021, 43 f. sowie zum Ablauf des Gesetzgebungsverfahrens Griesinger, Überblick zum geplanten neuen Schweizer Datenschutzgesetz (DSG), PinG 2018, 175 f.

6 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7031.

7 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7031.

8 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7031.

9 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7031.

ne Serverstandorte mit der Erstellung umfangreicher Sicherheitskopien, physische Schliess- und Überwachungssysteme, Schutz- und Wachdienste, sichere Löschtechniken, sichere Regelungen und Techniken zur Datenvernichtung, Schulungsmassnahmen für Mitarbeitende, vertragliche Schutzmassnahmen, Sicherheitskonzepte und Weisungen, Protokollierung und Dokumentation von Sicherheitsmassnahmen, Aufnahme der Sicherheitsmassnahmen in Handbücher, Integration von Sicherheitsmassnahmen in Governance-Prozesse, Integration von Sicherheitsmassnahmen in interne als auch externe Audits, periodische Überprüfung der vorhandenen Sicherheitsmassnahmen, bspw. durch Penetration Tests oder im Rahmen sog. Bug-Bounty-Programme.[10]

[5] Die Botschaft betont die Wechselwirkungen aber auch die Verschiedenheiten zwischen den Begrifflichkeiten des Datenschutzes und der Datensicherheit. Die in Art. 8 revDSG normierte Datensicherheit zielt originär auf die Bearbeitung der Personendaten ab und fokussiert dabei auf die vom Verantwortlichen oder Auftragsbearbeiter umzusetzenden technischen und organisatorischen Massnahmen.[11] Es wird mithin auf den Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit von Personendaten abgestellt.[12]

[6] Gleichwohl stellt die Botschaft richtigerweise klar, dass der persönliche Datenschutz des Individuums nur dann wirksam umgesetzt werden kann, wenn gleichzeitig auch angemessene technische und organisatorische Massnahmen zur Wahrung der Datensicherheit erfolgen.[13]

[7] Gleichzeitig ist die Legaldefinition nach Art. 5 lit. g revDSG zu beachten, wonach eine Verletzung der Datensicherheit dann vorliegt, wenn eine Verletzung der Sicherheit gegeben ist, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Eine Verletzung der Datensicherheit ist bei den vorstehenden Vorgängen gegeben, unabhängig davon, ob die Begehung absichtlich oder widerrechtlich erfolgt.[14] Gleichzeitig ist es bereits ausreichend, wenn die (blosse) Möglichkeit besteht, dass Personendaten unbefugten Personen zugänglich wurden.[15]

[8] Schliesslich hält Art. 8 Abs. 3 revDSG die Verpflichtung des Bundesrats fest, Bestimmungen über die Mindestanforderungen an die Datensicherheit zu erlassen.

[9] Zu beachten ist weiterhin, dass bei einer Verletzung der Datensicherheit eine Meldepflicht nach Art. 24 revDSG an den EDÖB ausgelöst werden kann. Hiernach ist eine Meldepflicht im Fall einer Verletzung der Datensicherheit gegeben, wenn durch die Verletzung voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person entsteht.[16] Eine in den Grundzügen ähnliche Meldepflicht für den Fall von Cybersicherheits-Vorfällen bei Betrei-

10 Es ist zu beachten, dass es sich hierbei nicht um eine abschliessende Aufzählung handelt.

11 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7031.

12 Vgl. hierzu Rosenthal, Das neue Datenschutzgesetz, in: Jusletter vom 16. November 2020.

13 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7031.

14 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7020.

15 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7022; s.a. Bieri/Powell, Meldung von Verletzungen der Datensicherheit, AJP 2021, 781.

16 Vgl. hierzu auch Bieri/Powell, Meldung von Verletzungen der Datensicherheit, AJP 2021, 781 ff.; Griesinger, Ein Überblick über das neue Schweizer Datenschutzgesetz (DSG), PinG 2021, 46.

bern kritischer Infrastrukturen[17] befindet sich aktuell in der Vernehmlassung[18] und ist mittels der Revision des Informationsschutzgesetztes[19] angedacht. Auch hier ist, je nach Umständen, eine Meldung an den EDÖB vorgesehen[20]. Dies zeigt deutlich auf, dass Datenschutzverletzungen und Cybersicherheitsvorfälle eine hohe Gemeinsamkeit aufweisen, was bei der Umsetzung von technischen und organisatorischen Massnahmen zu beachten ist. Das Bewusstsein über diesen Zusammenhang kann es allenfalls erlauben, bestehende Prozesse und Vorkehrungen effizient anzupassen.

2. Vorentwurf der Verordnung zum revidierten Datenschutzgesetz (VE-VDSG)

[10] Nach der Verabschiedung des neuen Datenschutzgesetzes am 25. September 2020 wurden auch die dazugehörigen Ausführungsbestimmungen, die Verordnung zum Datenschutzgesetz, überarbeitet und als Vorentwurf (VE-VDSG), in die Vernehmlassung gegeben. Das Vernehmlassungsverfahren endete am 14. Oktober 2021. Es ist damit zu rechnen, dass am VE-VDSG noch zahlreiche Anpassungen vorgenommen werden. Aus der Praxis wurde unter anderem Kritik geäussert, dass der Vorentwurf zu detaillierte und umfangreiche Vorgaben – insbesondere für kleinere und mittelständische Unternehmen – enthalte.[21]

[11] Im Vorentwurf zur revidierten Verordnung zum Datenschutzgesetz (VE-VDSG)[22] sind im ersten Kapitel in Abschnitt 1 in den Art. 1 bis 5[23] Regelungen zur Datensicherheit formuliert. Dabei sind in Art. 1 VE-VDSG Kriterien beschrieben, die festlegen sollen, ob die technisch-organisatorischen Massnahmen angemessen sind, um die Datensicherheit zu gewährleisten. Entscheidende Kriterien hiernach sollen Zweck, Art, Umfang und Umstände der Datenbearbeitung (lit. a), die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und die entsprechenden Auswirkungen auf die betroffene Person (lit. b), der Stand der Technik (lit. c) und die Implementierungskosten (lit. d) sein. Gleichzeitig sollen die Massnahmen nach Art. 1 Abs. 2 VE-VDSG in angemessenen Abständen überprüft werden.

[12] Weiterhin legt Art. 2 VE-VDSG Schutzziele fest, die durch die Massnahmen zur Gewährleistung der Datensicherheit erreicht werden sollen. Dies erfolgt unter der Einschränkung der Ange-

17 Vgl. Medienmitteilung «Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe eröffnet» vom 12. Januar 2022, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-86768.html zuletzt aufgerufen am 14. März 2022.

18 Als kritische Infrastrukturen werden typischerweise Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. für das Wohlergehen der Bevölkerung sind.

19 Informationssicherheitsgesetz (ISG) vom 18. Dezember 2020, BBl 2020 9975.

20 Vgl. Art. 74a ff. ISG der Vernehmlassungsvorlage.

21 Vgl. beispielsweise die Vernehmlassungsantwort der Swico (Schweizerischer Verband der Digital-Wirtschaft), https://www.swico.ch/media/filer_public/be/a8/bea85870-1fec-4f27-b224-9be038d6815d/vernehmlassung_-vdsg.pdf, zuletzt aufgerufen am 14. März 2022 und die Kritik von Glatthaar zum VE-VDSG vom 12. September 2021, https://datenrecht.ch/taeglich-gruesst-das-murmeltier-gedanken-zum-vorentwurf-der-datenschutz-verordnung/, zuletzt aufgerufen am 14. März 2022.

22 Der **Vorentwurf** zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz sowie der **erläuternde Bericht** zur Eröffnung des Vernehmlassungsverfahrens zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz kann aufgerufen werden über https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-84103.html, zuletzt aufgerufen am 14. März 2022.

23 Im 1. Abschnitt zur Datensicherheit regelt Art. 1 VE-VDSG die Grundsätze, Art. 2 VE-VDSG die Schutzziele, Art. 3 VE-VDSG die Protokollierung, Art. 4 VE-VDSG das Bearbeitungsreglement von privaten Personen und Art. 5 VE-VDSG das Bearbeitungsreglement von Bundesorganen.

messenheit der Massnahmen. Als Schutzziele nennt Art. 2 VE-VDSG dabei die Zugriffskontrolle, die Zugangskontrolle, die Datenträgerkontrolle, die Speicherkontrolle, die Benutzerkontrolle, die Transportkontrolle, die Eingabekontrolle, die Bekanntgabekontrolle, die Wiederherstellung, die Verfügbarkeit und Zuverlässigkeit des Systems als auch die Erkennung von Verletzungen der Datensicherheit.

[13] Darüber hinaus sind in Art. 3 VE-VDSG Protokollierungspflichten vorgesehen, wenn trotz der vorgesehenen Massnahmen des Verantwortlichen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht. In diesem Fall hat der private Verantwortliche nach Art. 3 VE-VDSG die Vorgänge des Speicherns, des Veränderns, des Lesens, der Bekanntgabe, der Löschung und der Vernichtung zu protokollieren. Bundesorgane (und deren Auftragsbearbeiter) haben nach Art. 3 Abs. 2 VE-VDSG die Vorgänge des Speicherns, des Veränderns, der Bekanntgabe, der Löschung und der Vernichtung zu protokollieren.

[14] Der Vorentwurf hat in der Vernehmlassung von Seiten der Praxis einige Kritik erfahren. Unter anderem wurde vorgebracht, dass der Vorentwurf zu stark regulierend wirke und dass insbesondere im Hinblick auf die Datensicherheit zu hohe Anforderungen gestellt würden.[24]

[15] Schliesslich ist in Art. 4 VE-VDSG geregelt, dass Verantwortliche und Auftragsbearbeiter im Fall der umfangreichen Bearbeitung von besonders schützenswerten Personendaten oder bei Durchführung eines Profiling mit hohem Risiko ein Reglement erstellen müssen. Dabei wird in Art. 4 Abs. 2 VE-VDSG der Inhalt des Reglements (Bearbeitungszweck, Kategorien betroffener Personen und bearbeiteter Personendaten, Aufbewahrungsdauer und Kriterien für die Festlegung dieser Dauer, interne Organisation, Herkunft der Personendaten und Art ihrer Beschaffung, technisch-organisatorische Massnahmen zur Gewährleistung der Datensicherheit, Zugriffsberechtigungen sowie Art und Umfang der Zugriffe, Datenbearbeitungsverfahren und Verfahren zur Ausübung des Auskunftsrechts) vorgegeben. Zudem ist in Art. 4 Abs. 3 VE-VDSG die Pflicht zur regelmässigen Aktualisierung des Reglements festgehalten.

[16] Art. 5 VE-VDSG enthält die Regelung für das Bearbeitungsreglement von Bundesorganen. Ein solches Reglement muss von Bundesorganen (und deren Auftragsbearbeitern) erstellt werden, wenn besonders schützenswerte Personendaten bearbeitet werden, ein Profiling durchgeführt wird, es zur Datenbearbeitungen nach Art. 34 Abs. 2 lit. c revDSG kommt, wenn Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen Personendaten zugänglich gemacht werden oder wenn zusammen mit anderen Bundesorgangen ein Informationssystem betrieben oder Datenbestände bewirtschaftet werden. Das Reglement hat dabei den Inhalt gemäss Art. 4 Abs. 2 VE-VDSG aufzuweisen und muss nach Art. 5 Abs. 3 VE-VDSG regelmässig aktualisiert werden.

3. Rechtsvergleich mit den Regelungen der EU-Datenschutzgrundverordnung (DSGVO)

[17] In der DSGVO ist die Datensicherheit in Art. 32 geregelt. Die Regelung aus Art. 8 revDSG ähnelt Art. 32 DSGVO. Die Vorschrift in der DSGVO ist indessen im Hinblick auf die beispielhafte Umschreibung technisch-organisatorischer Massnahmen detaillierter ausgestaltet. In Art. 32

[24] Vgl. bspw. die Kritik von Glatthaar zum VE-VDSG vom 12. 9.2021, https://datenrecht.ch/taeglich-gruesst-das-murmeltier-gedanken-zum-vorentwurf-der-datenschutzverordnung/, zuletzt aufgerufen am 14. März 2022.

Abs. 1 DSGVO ist ein nicht abschliessender Katalog möglicher Massnahmen (bspw. die Pseudonymisierung und Verschlüsselung personenbezogener Daten)aufgelistet. Eine entsprechende Aufzählung wird jedoch im Schweizer Recht durch den VE-VDSG vorgenommen. Gleichzeitig wird in Art. 32 Abs. 3 DSGVO ausdrücklich darauf hingewiesen, dass Verhaltensregeln oder eine Zertifizierung[25] als Nachweis für die Einhaltung der erforderlichen technisch-organisatorischen Massnahmen dienen können.

[18] Gesamthaft ist festzustellen, dass eine starke Angleichung zwischen der Regelung im revDSG und der Regelung in der DSGVO stattgefunden hat.[26] Dies ist vom Schweizer Gesetzgeber auch bewusst so erfolgt. Es sollte eine «Kompatibilität mit der DSGVO» erzielt werden.[27]

III. Der Themenkomplex Cyber-Sicherheit

1. Cyberrisiken

[19] Cyberrisiken haben in den letzten Jahren markant zugenommen, was den wirtschaftlichen und politischen Entscheidungsträgern sowie der breiten Öffentlichkeit insbesondere auch durch nationale und internationale Vorfälle mit grossen Auswirkungen bewusst wurde.[28] Dabei waren beispielsweise Websiten nicht mehr erreichbar oder auch gesamte Netzwerke von Unternehmen durch Cyberangriffe betroffen. Nebst finanziellen Schäden gelangen oft auch vertrauliche Informationen in falsche Hände – dies mit gravierenden Folgen: Verlust von Daten, Ausfall von Systemen, Datenschutzverletzungen oder Reputationsschäden. Um in die IT-Systeme einzudringen, zielt die Täterschaft mehrheitlich darauf ab, Mitarbeitende dazu zu verleiten, beispielsweise einen E-Mail-Anhang zu öffnen, einen Link anzuklicken, Passwörter anzugeben oder eine Zahlung vorzunehmen.[29]

[20] Cyberrisiken sind somit längst keine theoretischen Risiken mehr, was beispielsweise auch durch die Tatsache zu erkennen ist, dass sich selbst die Organisation der Vereinten Nationen (UNO) dazu veranlasst sah, im Bericht der offenen Arbeitsgruppe der UN festzuhalten, dass «Infrastruktur des Gesundheitssektors einschliesslich medizinischen Dienstleistungen und Einrichtungen» kritische Infrastruktur darstelle und daher nicht angegriffen werden dürfen – dies umfasst auch Cyberangriffe.[30] Auch Kriege werden abseits der sichtbaren Kriegsschauplätze zunehmend im Cyberspace ausgefochten, dies bisweilen unter der Beteiligung von nichtstaatlichen Akteuren, wie z.B. dem Hackerkollektiv «Annonymous». Diese unübersichtliche Lage mit erhöhten schädlichen Aktivitäten im Cyberspace vergrössert das Risiko von direkten, indirekten und auch unabsichtlichen Auswirkungen auf kritische Infrastrukturen, Unternehmen und die Gesellschaft.

---

25 Bei Einhaltung bestimmter Vorgaben, vgl. dazu Art. 32 Abs. 3 DSGVO sowie Art. 40 und 42 DSGVO.

26 Botschaft Totalrevision Datenschutzgesetz, BBl 2017 7031.

27 Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz vom 23. Juni 2021, S. 10, aufrufbar unter https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-84103.html, zuletzt aufgerufen am 14. März 2022.

28 Vgl. Halbjahresbericht 2021/1 des NCSC: https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/lageberichte/NCSC_2021-1_HJB_DE.pdf.download.pdf/NCSC_2021-1_HJB_DE.pdf, zuletzt aufgerufen am 14. März 2022.

29 NCSC – Verhaltensregeln E-Mail: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/verhalten-bei-e-mail.html, zuletzt aufgerufen am 14. März 2022.

30 Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (A/76/135).

Cyberrisiken sollten daher Teil des Risikomanagements jedes Unternehmens sein. Die folgende Übersicht von ausgewählten technischen und organisatorischen Massnahmen soll Vorschläge und konkrete Hilfestellungen bieten, um derartigen Risiken besser zu begegnen.[31] Selbstverständlich ist in jedem Fall eine Anpassung derartiger Massnahmen auf den konkreten Einzelfall und die individuelle Risikosituation vorzunehmen. Weite Teile der nachstehenden Informationen, Massnahmen und Umsetzungshinweise stammen ursprünglich vom NCSC und werden mit dessen freundlicher Genehmigung vorliegend verwendet.[32]

2. Arten von Schutz-Massnahmen

[21] Im Umgang mit Daten- und Cyberrisiken kommen technische und organisatorische Schutzmassnahmen zur Reduktion der Risiken zur Anwendung:

[22] Organisatorische Massnahmen erhöhen oder gewährleisten die Informations- bzw. Datensicherheit. Sie stellen sicher, dass die Zuständigkeiten innerhalb des Unternehmens in Bezug auf die Informations- und Datensicherheit festgelegt sind.

[23] Technische Massnahmen erhöhen oder gewährleisten die Sicherheit der IT-Infrastruktur an sich. Sie leisten einen wesentlichen Beitrag zur Gewährleistung der Informationssicherheit und werden typischerweise durch organisatorische Massnahmen ergänzt. Obwohl die technischen Risiken von IT-Systemen einen wichtigen Teil der Informationssicherheit darstellen, sollte ein Unternehmen seinen Fokus nicht auf diesen Teil der Risiken beschränken oder gar die IT-Abteilung als alleinigen Risikoträger benennen. Denn die Verantwortung für das Risikomanagement, die Klassifizierung und Kategorisierung von Informationen sowie ein abgestufter Aufwand an bereitgestellten Sicherheitsmassnahmen sind Kernaufgaben der Oberleitung des Unternehmens.[33]

[24] Die Arten derartiger Massnahmen lassen sich zwar nicht immer scharf voneinander trennen und weisen oft Aspekte beider Elemente auf. Völlige Sicherheit kann niemals durch technische bzw. organisatorische Massnahmen erreicht werden. Oft sind nicht die Massnahmen das schwächste Glied, sondern der Mensch. Sind beispielweise Mitarbeitende nicht im sicheren Umgang mit IT-Systemen geschult, kann dies die Wirksamkeit der nachfolgend beschriebenen Massnahmen erheblich schwächen. Eine sinnvolle Kombination verschiedener technischer und organisatorischer Massnahmen leistet jedoch einen wesentlichen Beitrag zur Sicherheit im Unternehmen und kann das Risiko von Vorfällen erheblich mindern. Wichtig ist in jedem Fall eine auf den konkreten Fall und das Risiko angemessene Ausgestaltung der getroffenen Massnahmen sowie deren regelmässige Überprüfung.[34]

---

31 Die Übersicht in diesem Kapitel hat keinen abschliessenden Charakter.

32 Weitergehende Informationen sowie Detailhinweise und technische Grundlagen des NCSC finden sich unter: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen.html, zuletzt aufgerufen am 14. März 2022.

33 Vgl. Art. 716 OR, Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches(Fünfter Teil: Obligationenrecht OR) vom 30. März 1911 (Stand am 1. Januar 2022), SR 220.

34 NCSC – Cyberangriffe gegen Firmen – Das müssen Sie wissen: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/cyberangriffe-gegen-firmen.html, zuletzt aufgerufen am 14. März 2022.

3. Ausgewählte organisatorische Massnahmen

a) Bewusstsein des Managements über Risiken

[25] Das Management eines Unternehmens sollte die Abhängigkeit der Geschäftsprozesse von der IT bewerten und kennen. Dazu gehören Abklärungen zu den Auswirkungen eines Systemausfalls oder der Nichtverfügbarkeit einer Datenspeicherung, zu finanziellen und betrieblichen Folgen und zu notwendigen Massnahmen, die zu treffen sind.[35]

b) Bewusstsein der Mitarbeitenden

[26] Die Sensibilisierung aller Mitarbeitenden im Umgang mit IT-Systemen ist von zentraler Bedeutung. Das Personal sollte regelmässig im Umgang mit möglichen Gefahren in der digitalen Welt geschult werden. Dazu gehört insbesondere auch eine Sensibilierung betreffend Umgang mit E-Mails und dem Internet sowie die Kenntnis entsprechder Prozesse und Vorgaben des Unternehmens.[36]

c) Zuständigkeiten

[27] Mitarbeitende müssen wissen, an wen sie sich wenden können, wenn sie Fragen zur IT-Sicherheit haben (z.B. wenn sie eine verdächtige E-Mail erhalten) oder wen sie im Falle eines IT-Sicherheitsvorfalls informieren müssen. Dazu ist es nützlich, frühzeitig einen Reaktionsplan für Sicherheitsvorfälle zu entwickeln und diesen regelmässig auf seine Wirksamkeit zu überprüfen und anzupassen, z.B. mit Übungen.[37]

d) Verhalten im Umgang mit E-Mail

[28] Die E-Mail ist nach wie vor das wichtigste Einfallstor für Schadsoftware und Betrugsversuche. Ein sorgfältiger Umgang mit E-Mails trägt daher wesentlich zur Daten- und Cybersicherheit des Unternehmens bei. Dabei sollten folgende Punkte im Rahmen von Sensibilisierungsmassnahmen sowie internen Regelungen beachtet werden: Im Umgang mit E-Mails unbekannten Ursprungs ist es besonders wichtig, dass sich Mitarbeitende nicht überrumpeln lassen. Denn Cyberkriminelle lassen sich immer neue Szenarien einfallen, um die Opfer zu einer unüberlegten Reaktion unter Zeitdruck zu bewegen. Vorsicht ist immer dann geboten, wenn der Empfänger der E-Mails aufgefordert wird, z.B. dringend einen Link anzuklicken oder einen angeblich wichtigen Anhang zu öffnen – dem sollte keinesfalls nachgekommen werden. Potenziell bösartige E-Mail-Anhänge sollten daher bereits vom E-Mail-Server des Unternehmens blockiert oder gefiltert werden[38]. Aber selbst E-Mails von bekannten Absendern können gefährlich sein, da sich

35 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

36 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

37 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

38 Eine Liste mit potenziell bösartigen Dateierweiterungen stellt das GovCERT des NCSC zur Verfügung: https://www.govcert.ch/downloads/blocked-filetypes.txt, zuletzt aufgerufen am 14. März 2022.

einige Schadprogramme von selbst mittels E-Mail verbreiten, ohne dass dies dem Absender bewusst ist. Daher ist z.B. immer dann Vorsicht geboten, wenn bereits vorhandene E-Mails plötzlich aus dem Zusammenhang gerissen werden, dies kann ein Hinweis auf Schadprogramme sein. Schadsoftware wird häufig auch mittels Office-Dokumenten via E-Mail verbreitet. In den meisten Fällen wird hierbei die Makrofunktion ausgenutzt.[39] Daher sollte die Ausführung von Makrofunktion deaktiviert und alle E-Mail-Anhänge, die Makros enthalten (z.B. Word-, Excel- oder PowerPoint-Anhänge mit Makros) blockiert werden. Mitarbeitende sollten auch darauf aufmerksam gemacht werden, dass entsprechende Warnmeldungen in Office-Programmen nicht ignoriert werden dürfen.[40]

e) Umgang mit Daten

[29] Für den Umgang mit Daten und Informationen sollten im Unternehmen verbindliche Regeln erlassen werden, welche auch in organisatorischer und technischer Hinsicht konsequent um- und durchgesetzt werden. Für sensible Daten (z.B. schützenswerte Personendaten oder auch geistiges Eigentum) sollte genau geregelt werden, wie diese gespeichert und elektronisch übermittelt werden dürfen. Für die Weitergabe von Unternehmensinformationen sollten klare Richtlinien bestehen.[41]

f) Unternehmensinformationen im Internet

[30] Kriminelle sind stets auf der Suche nach brauchbaren Informationen über potenzielle Opfer. Daher sollte genau bedacht werden, welche Informationen z.B. auf der eigenen Website oder in sozialen Medien verbreitet werden. Nutzen und Risiken von frei verfügbaren Informationen des Unternehmens sollten sorgfältig gegeneinander abgewogen werden. Dazu sollte im Unternehmen auch bestimmt werden, wie Mitarbeitende mit Unternehmensinformationen umgehen dürfen, z.B. bei der privaten Nutzung sozialer Medien.[42]

g) Passwörter

[31] Schlecht gewählte oder zu kurze Passwörter stellen ein erhebliches Sicherheitsrisiko für Unternehmen dar. Daher sollten verbindliche Vorgaben im Unternehmen zur Nutzung von Passwörtern bestehen. Diese sollten folgende Grundlagen enthalten: Die Mindestlänge des Passworts sollte 12 Zeichen betragen und aus Klein- und Grossbuchstaben, Zahlen und Sonderzeichen bestehen. Passworte dürfen nicht mehrfach verwendet und auch nicht weitergegeben werden. Wenn immer möglich, sollte die sogenannte Zwei-Faktor-Authentifizierung aktiviert werden, so dass zusätzlich zum eigentlichen Passwort ein weiterer Faktor (Einmalpasswort, SMS-Code usw.) zur

39 Makros werden zur Automatisierung von Office-Dokumenten verwendet. Sie können aber auch zur Verbreitung von Malware genutzt werden.

40 NCSC – Verhaltensregeln E-Mail: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/verhalten-bei-e-mail.html, zuletzt aufgerufen am 14. März 2022.

41 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

42 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

Authentifizierung notwendig ist. Sehr wichtig ist zudem auch, sicherzustellen, dass Passwörter geändert bzw. Zugriffe deaktiviert werden, wenn Mitarbeitende das Unternehmen verlassen.[43]

h) Zugriffsberechtigungen

[32] Nur sehr wenige Mitarbeitende benötigen umfangreiche Administratorrechte, dafür besteht oftmals zu wenig Bewusstsein. Mitarbeitende sollten in IT-Systemen daher nur so viele Rechte besitzen, wie für die Erledigung der konkreten Arbeit unbedingt notwendig sind. Insbesondere sollten Rechte zur Installation von Software nur sehr restriktiv vergeben werden.[44]

i) IT-Dienstleister

[33] Viele Unternehmen lagern ihre IT zunehmend an spezialisierte IT-Dienstleister aus. Die Verantwortlichkeiten zwischen Unternehmen und IT-Dienstleister müssen klar definiert werden. Haftungsfragen für den Fall, dass Sicherheitsvorschriften missachtet oder die IT-Sicherheit anderweitig vernachlässigt werden, sollten im Vertrag geregelt werden. Sicherheitsüberlegungen sollten aber bereits beim Beschaffungsprozess von IT-Systemen eine wichtige Rolle spielen. Dabei sollte es nicht nur um Überlegungen bezüglich Inbetriebnahme gehen, sondern Risiken über den gesamten Lebenszyklus eines Systems, einschliesslich Wartung und Ausserbetriebnahme bedacht werden. Ein wichtiges Element einer solchen Einschätzung kann beispielweise der Zeitraum sein, für welchen Sicherheitsaktualisierungen des Herstellers garantiert werden. Ein oft vergessener Aspekt ist auch die Stilllegung (von Teilen) der IT-Infrastruktur; hierbei sollte u.a. festgelegt werden, wie vertrauliche Informationen zuverlässig von den betroffenen Systemen entfernt werden und wie mit vorhandenen Datensicherungen umgegangen werden soll. Zertifizierungen nach anerkannten Datenschutz- und Informationssicherheitsstandards oder Prüfberichte von unabhängigen Dritten können bei der Auswahl des IT-Dienstleisters hilfreich sein. Es empfiehlt sich, IT-Dienstleister vorgängig nachweisen zu lassen, dass sie die technischen und fachlichen Anforderungen erfüllen und die von Unternehmen benötigte Verfügbarkeit und Sicherheit gewährleisten können. Dies sollte von einer unabhängigen Stelle überprüft oder bestätigt werden. Auch die Erfüllung der vertraglich vereinbarten Leistungen sollte periodisch und unabhängig überprüft werden[45]. Der IT-Dienstleister sollte einen ISAE 3402 Type 2 (International Standard on Assurance Engagements) Prüfbericht vorlegen können.[46] Dieser Bericht einer unabhängigen Prüfstelle behandelt ausgewählte Aspekte der Sicherheit, Verfügbarkeit, Integrität und Vertraulichkeit, was die Einschätzung des entsprechenden IT-Dienstleisters auf Sicherheit erleichtern kann.[47]

---

43 NCSC – Schützen Sie Ihre Konten/Passwörter: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihre-konten.html, zuletzt aufgerufen am 14. März 2022.

44 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

45 Zum Beispiel auf der Grundlage von COBIT (Control Objectives for Information and Related Technology, https://www.isaca.org/resources/cobit) der Information Systems Audit and Control Association (ISACA, https://www.isaca.org/).

46 Auch bekannt als SOC-2-Bericht (Service Organization Control).

47 NCSC – Empfehlungen für die Zusammenarbeit mit IT Providern: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/zusammenarbeit-it-provider.html, zuletzt aufgerufen am 14. März 2022.

4. Ausgewählte technische Massnahmen

a) Sicherheits-Updates

[34] Veraltete Software ist ein beliebtes und effektives Einfallstor für Schadsoftware. Es sollte daher unbedingt sichergestellt werden, dass alle Computer, Smartphones, Tablets und Server im Netzwerk des Unternehmens automatisch Sicherheitsupdates des jeweiligen Betriebssystems umgehend anwenden. Jede installierte Software (z.B. Webbrowser, Fachapplikationen etc.) sollte ebenfalls möglichst umgehend aktualisiert werden. Auch Geräte wie Drucker, Scanner, Router, usw. sollten immer unverzüglich auf dem neuesten Stand gehalten werden.[48]

b) Regelmässige Datensicherung

[35] Unternehmen sollten über einen definierten Prozess zur regelmässigen Datensicherung (Backup) verfügen und diesen konsequent umsetzen. Datensicherungen sollten regelmässig überprüft werden, um sicherzustellen, dass diese ordnungsgemäss zur Verfügung stehen und funktionieren. Das Importieren von Datensicherungen sollte ebenso regelmässig geübt werden, damit das Verfahren bekannt ist. Datensicherungen sollten offline gespeichert werden, also auf einem externen Medium wie z.B. einer externen Festplatte. Auch sollte das Medium nach dem Sicherungsvorgang vom Computer getrennt werden, denn im Falle eines Angriffs durch sog. Ransomware[49] können sonst auch die Datensicherungen unbrauchbar werden. Zudem sollten ältere Datensicherungen für eine angemessen lange Zeit lang aufbewahrt werden.[50]

c) Schutz vor Viren

[36] Auf jedem Computer im Unternehmen muss ein Virenschutz installiert sein. Dieser sollte regelmässig aktualisiert werden, vorzugsweise mehrmals täglich. Auch sollten automatisch vollständige Systemüberprüfungen durch den Virenschutz im Hintergrund ausgeführt werden. Der Virenschutz darf sich zudem nicht vom Nutzer des Computers deaktivieren lassen.[51]

d) Firewall

[37] Im Unternehmen muss auf jedem Computer eine Firewall aktiviert sein. Das Unternehmensnetz sollte auch vor dem Internet mit einer zusätzlichen Firewall geschützt werden. Dabei sollte mit sog. Firewall-Regeln definiert werden, welche ein- und ausgehenden Verbindungen erlaubt sein sollen. Die Protokolldateien der Firewall sollten regelmässig auf Auffälligkeiten und Anomalien analysiert werden.

---

48 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

49 Bei Verschlüsselungstrojanern (auch «Ransomware» oder «Erpressungstrojaner» genannt) handelt es sich um Schadsoftware, welche Dateien auf dem Computer des Opfers sowie auf verbundenen Netzlaufwerken verschlüsselt und somit für das Opfer unbrauchbar macht. Die Cyberkriminellen verlangen für den notwendigen Schlüssel zur Entschlüsselung vom Opfer ein Lösegeld, oftmals in Form von Kryptowährungen.

50 NCSC – Sichern Sie Ihre Daten regelmässig: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/ks-daten.html, zuletzt aufgerufen am 14. März 2022.

51 NCSC – Sorgen Sie für Virenschutz: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/ks-virenschutz.html, zuletzt aufgerufen am 14. März 2022.

e) Fernzugriff

[38] Wenn Mitarbeiter von aussen auf Ihr Unternehmensnetzwerk zugreifen müssen (z.B. auf Geschäftsreisen, im Home-Office usw.), sollte dies nur über ein virtuelles privates Netzwerk (VPN)[52] möglich sein, welches durch eine Zwei-Faktor-Authentifizierung geschützt ist. Dies gilt auch für den Zugriff von externen IT-Dienstleistern und Administratoren.[53]

f) Cloud-Dienste

[39] Bei der Nutzung von Cloud-Diensten muss zwar nicht selbst eine teure IT-Infrastruktur betrieben werden. Gleichwohl gilt es bei der Nutzung von Cloud-Diensten, besondere Vorsicht walten zu lassen. Sensible Daten sollten niemals in der Cloud gespeichert werden, sondern nur lokal. Es empfiehlt sich, beim Anbieter vor Vertragsabschluss die wichtigsten Sicherheitsvorkehrungen (Datenzugriff, Datensicherung usw.) abzufragen.[54]

g) Log-Dateien

[40] Sogenannte Log-Dateien[55] sind bei der Nachbereitung eines IT-Vorfalls von zentraler Bedeutung. Unternehmen sollten daher sicherstellen, dass kritische Systeme wie z.B. Buchhaltungssoftware, Domänencontroller, Firewalls oder E-Mail-Server solche Protokolldateien erstellen. Diese Log-Dateien sollten zudem regelmässig auf Unstimmigkeiten überprüft und mindestens sechs Monate lang aufbewahrt werden.[56]

h) Netzsegmentierung

[41] Unternehmensnetzwerke sollten getrennte Netze z.B. für Produktion, Personaldaten, Buchhaltung etc. aufweisen. So kann vermieden werden, dass z.B. nicht mehr aktualisierbare Fachapplikationen zum Einfallstor auf das ganze Unternehmensnetzwerk werden.[57]

---

52 Ein VPN ermöglicht durch Verschlüsselung des Datenverkehrs eine sichere Kommunikation zwischen Computern/Servern über öffentliche Netzwerke (z.B. das Internet).

53 NCSC – Home Office – Sicherer Umgang mit Fernzugriffen: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/home-office.html, zuletzt aufgerufen am 14. März 2022.

54 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

55 Eine Logdatei enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem.

56 NCSC – Ransomware – Was nun?: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html, zuletzt aufgerufen am 14. März 2022.

57 NSCS – Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/news/news-archiv/sicherheitsrisiko-durch-ransomware.html, zuletzt aufgerufen am 14. März 2022.

i) Verschlüsselung

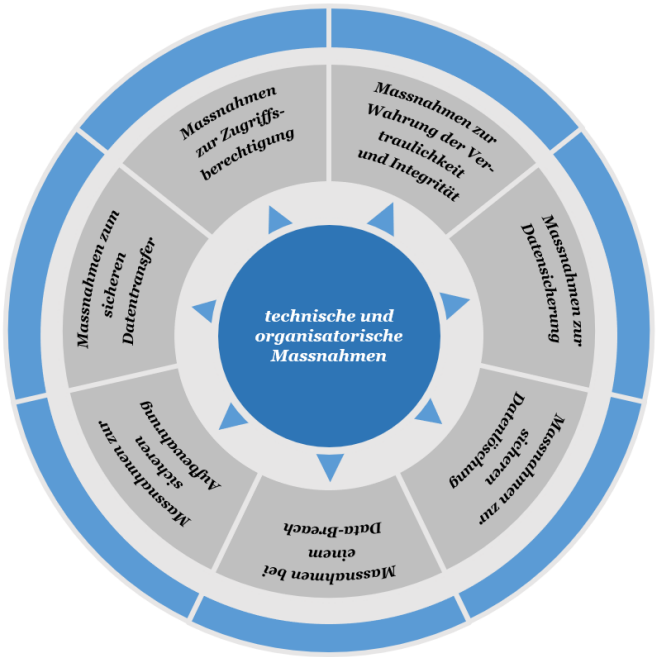
[42] Wichtige Daten sollten stets verschlüsselt gespeichert und transportiert bzw. übermittelt werden, vor allem bei der Nutzung von Cloud-Diensten und bei der Nutzung von mobilen Geräten.[58]

IV. Grundelemente eines sog. Datensicherheitskonzept

[43] Ein Datensicherheitskonzept ist stets an den jeweiligen Sicherheitsbedürfnissen des Anwenders orientiert. Gleichwohl sind bestimmte Grundelemente in allen Datensicherheitskonzepten vorzuhalten.

[44] Neben einer Präambel mit Einleitung und der Benennung der gesetzlichen Grundlage empfiehlt es sich, zunächst einen Überblick über die relevanten Definitionen und Begrifflichkeiten zu geben. Wesentlicher Schwerpunkt eines Sicherheitskonzepts ist sodann die Darstellung der technischen und organisatorischen Massnahmen zwecks der Wahrung der Datensicherheit. Zudem kann auf Massnahmen zur Sicherstellung der Betroffenenrechte eingegangen werden.

[45] Die folgenden Massnahmen-Kategorien werden als technische und organisatorische Massnahmen im Rahmen eines Datensicherheitskonzepts empfohlen:



58 NCSC – Schützen Sie Ihr KMU: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html, zuletzt aufgerufen am 14. März 2022.

V. Conclusio

[46] Datensicherheit und Cybersicherheit stellen sich als zentrale und wesentlich Bestandteile eines funktionierenden Risikomanagements und Schutzkonzepts für Unternehmen ebenso wie für staatliche Stellen dar. Aus Anwendersicht ist nach Auffassung der Autoren sicherzustellen, dass die rechtlichen Anforderungen und die technischen und organisatorischen Umsetzungen Hand in Hand gehen. Dazu ist erforderlich, dass diese zentrale Schnittstelle so ausgestaltet ist, dass die aktuellen Entwicklungen beider Fachbereiche stets berücksichtigt werden. Um einen hinreichenden Sicherheitsstandard zu gewährleisten, ist bei den Sicherheitsmassnahmen regelmässig der Status «State oft the Art» einzuhalten. Die technische und organisatorische Umsetzung dieses Standards bedarf gleichzeitig aber auch einer hinreichenden rechtlichen Grundlage und Absicherung. Dies kann beispielsweise durch ein fundiertes Sicherheitskonzept erfolgen. Gleichzeitig gilt es, neue Entwicklungen und Risiken zu erkennen und die Sicherheitsstrategien bzw. -Massnahmen entsprechend anzupassen. Eine solche Sicherheits- und Risiko-Awareness wird vom Normgeber mit seiner Regelung zur Datensicherheit vorausgesetzt. Ein zentraler Aspekt bei all den vorgenannten Elementen ist die Awareness und die Unterstützung durch das Management eines Unternehmens. Denn Daten- und Cybersicherheit ist kein reines IT-Thema; es würde einer Good-Governance widersprechen, derartige Themen und Verantwortlichkeiten auf rein operativer Ebene anzusiedeln. Vielmehr ist es in der Verantwortung der Oberleitung (Verwaltungsrat) eines jeden Unternehmens, Risiken adäquat einzuschätzen, entsprechende Strategien und Massnahmen zu treffen und die notwendige Organisation festzulegen, um unter anderem auch die Daten- und Cybersicherheit zu gewährleisten.[59]

[47] Es wird für die Umsetzung konkreter Praxismassnahmen zudem zu beobachten sein, wie die revidierte VDSG genau ausgestaltet ist. Dies betrifft insbesondere die Fragestellung zu den Bearbeitungsreglementen. Die Fragestellungen rund um die Massnahmen der Datensicherheit sind hingegen bereits durch Praxisbedürfnisse zur Datensicherheit weitgehend vorgegeben. Mitunter scheint sogar vorstellbar, dass die Praxisbedürfnisse an die Datensicherheit über die im VE-VDSG formulierten Anforderungen hinausgehen, beispielsweise in Form von geplanten externen Überprüfungen von IT-Sicherheitsarchitekturen oder in Form von ungeplanten externen Überprüfungen von IT-Sicherheitsarchitekturen im Rahmen sog. Bug-Bounty-Programme.

Daniel W. Seiler, lic. iur., IT-Projektleiter am Nationalen Zentrum für Cyber-Sicherheit (NCSC) und Gastdozent an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) sowie an der Universität St. Gallen (HSG), unterrichtet als Experte im IT- und Datenschutzrecht.

Marcel Griesinger, Rechtsanwalt und Inhaber der Rechtsanwaltskanzlei Griesinger, die auf Corporate Privacy Law spezialisiert ist, Dozent an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW), Praxis- und Lehrtätigkeit im Wirtschafts- und Datenschutzrecht.

59 Art. 716 OR.