Cyber Sicherheit – Gibt es rechtliche Vorgaben und Standards?

Dr. Martin Eckert
Eric Neuenschwander

Der Oktober ist europäischer Cyber Security Monat: Die Botschaft des Globalen Cyber Security Monats ist die gemeinsame Verantwortung im Umgang mit moderner Informations- und Telekommunikationstechnik – STOP.THINK.CONNECT. In der Praxis stellt sich jedoch immer wieder die Frage, welche rechtlichen Vorgaben und Standards die IT-Sicherheit in Unternehmen aufweisen muss. Der vorliegende Beitrag zeigt nicht nur die für Unternehmen relevanten rechtlichen Bestimmungen auf, sondern enthält ebenso Empfehlungen zur Umsetzung von Cyber Risk Massnahmen.

Inhaltsverzeichnis

Einleitung

Die umfassende digitale Vernetzung – das Internet der Dinge und künstliche Intelligenz –machen uns Nutzer immer abhängiger von der Informations- und Kommunikationstechnik («IKT»). Diese bietet unzählige Chancen, birgt jedoch auch erhebliche Risiken in sich.

Im «Global Risk Report» des World Economic Forum von 2018 werden Cyber-Attacken und Datendiebstahl als zwei der fünf grössten globalen Hauptrisiken aufgeführt.[1]

In der Praxis stellt sich immer wieder die Frage, welche rechtlichen Vorgaben und Standards die IT-Sicherheit in Unternehmen aufweisen muss. Der vorliegende Beitrag zeigt nicht nur die für Unternehmen relevanten rechtlichen Bestimmungen auf, sondern erhält ebenso Empfehlungen zur Umsetzung von Cyber Risk Defense.

I. Schweiz

A. Nationale Strategie

Der Bundesrat ist sich der verstärkten digitalen Abhängigkeit von Schweizer Unternehmen und der intensivierten Bedrohungslage durch Cyber-Risiken bewusst. In der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022 werden Massnahmen aufgezeigt, die die Unabhängigkeit und Sicherheit der Schweiz wahren und vor Gefahren im Cyber-Raum schützen sollen.[2] Das Strategiepapier bietet wenig konkrete Handlungsanleitungen. Konzeptionell ist aber klar: Letztlich sind und bleiben die einzelnen Akteure in ihren eignen Sphären für ihren eigenen Schutz verantwortlich (Selbstverantwortung).

B. Datenschutzgesetz – Schutz von Personendaten

Da der gesetzliche Begriff von Personendaten weit gefasst ist[3], bearbeitet heute praktisch jedes Unternehmen Personendaten, sei es von Mitarbeitern, Kunden oder Lieferanten. Jede Bearbeitung von Personendaten in der Schweiz unterliegt den Bestimmungen des Schweizerischen Datenschutzgesetzes.[4] Entsprechend sollte der Schutz dieser Daten auf der Agenda der Geschäftsleitung und des Verwaltungsrates stehen.[5]

Wer Personendaten verarbeitet, muss dies rechtmässig tun und hat sich über die Richtigkeit der Daten zu vergewissern.[6] Das Gesetz schreibt vor, dass Personendaten durch angemessene technische und organisatorische Massnahmen[7] gegen unbefugtes Bearbeiten geschützt werden müssen. Welche Massnahmen zum Schutz der Personendaten konkret ergriffen werden müssen, wird in der Verordnung umschrieben. So

---

1 Top 5 Global Risks in Terms of Likelihood: Extreme weather events, natural disasters, cyberattacks, data fraud or theft, failure of climate change mitigation and adaptation. World Economic Forum, The Global Risks Report 2018, 13th Edition, online verfügbar unter: <http://www3.weforum.org/docs/WEF_GRR18_Report.pdf>.

2 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022, online verfügbar unter: <https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html>.

3 Gemäss Art. 3 lit. a DSG sind Personendaten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

4 SR 235.1 Bundesgesetz über den Datenschutz (DSG), vom 19. Juni 1992.

5 Siehe dazu weitere MME Magazinbeiträge: «Cyberrisiken sind heute Chefsache» sowie «Cybersicherheit im Verwaltungsrat von KMU», online verfügbar unter <https://www.mme.ch/de/magazin/>.

6 Art. 4 DSG.

7 TOMs (Technische und organisatorische Massnahmen).

statuiert Art. 8 VDSG[8] die Pflicht, für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten, besorgt zu sein, um so einen angemessenen Datenschutz zu gewährleisten (Datensicherheit).[9] Dies umfasst insbesondere die Pflicht, die Datenverarbeitungssysteme gegen folgende Risiken zu schützen:

- Unbefugte oder zufällige Vernichtung,
- Zufälliger Verlust,
- Technische Fehler,
- Fälschung, Diebstahl oder widerrechtliche Verwendung,
- Unbefugtes Änderung, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.

Durch die Vorgabe, dass IT-Systeme dem gegenwärtigen Stand der Technik entsprechen müssen, schafft der Gesetzgeber die Pflicht zur Implementierung von Sicherheitsmassnahmen. Bei der Umsetzung der Vorgaben aus dem Datenschutzgesetz und der entsprechenden Verordnung ist der sogenannte «risk-based approach» zu empfehlen, d.h. der Aufwand darf auf das Risiko abgestimmt werden. Das Risiko ist dabei jeweils aus der Optik der betroffenen Personen zu beurteilen. Weiter sollten die Massnahmen schon aus Haftungsgründen dokumentier werden (sog. TOMs, technische und organisatorische Massnahmen).

Nicht zu vergessen ist dabei die Verantwortlichkeit eines Auftraggebers, wenn er die Bearbeitung von Personendaten auf Dritte überträgt. Bei Hinzuziehen eines Providers muss sich der Auftraggeber vergewissern, dass der Provider die Datensicherheit gewährleisten kann.[10]

Das Datenschutzgesetz bietet somit einen ersten Anhaltspunkt, welche Massnahmen zu ergreifen sind um Daten vor unberechtigtem Missbrauch zu schützen. Das Gesetz aus dem Jahre 1992 bietet noch keine konkrete Handlungsanweisung, wie mit den Cyber-Risiken der heutigen Zeit umzugehen ist.[11]

C. Praktische Vorgaben für KMUs

1. MELANI-Merkblatt

Die Cyber Security Praxis wird in der Schweiz geprägt von MELANI. MELANI ist die seit 2004 tätige Melde- und Analysestelle Informationssicherung, welche vom Bundesrat mit dem Schutz der kritischen Infrastrukturen beauftragt ist.[12] MELANI bietet aber auch KMUs Hilfestellungen in Form von Merkblättern über Informationssicherheit, Berichten über die wichtigsten Tendenzen und Entwicklungen im Bereich IKT und ein Meldeformular, um Vorfälle auf freiwilliger Basis zu melden. MELANI bietet aber auch Unterstützung bei der technischen Analyse von Vorfällen.[13] Im Gegensatz zur EU[14] gibt es in der Schweiz zurzeit keine Meldepflicht von Datenschutzverstössen, eine solche ist jedoch im revidierten Datenschutzgesetz vorgesehen, sofern eine

8 SR 235.11 Verordnung zum Bundesgesetz über den Datenschutz (VDSG), vom 14. Juni 1993.
9 Siehe dazu auch: EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, August 2015.
10 Art. 10a DSG.
11 Das aktuelle Datenschutzgesetz befindet sich zurzeit in Revision. Weitere Ausführungen zu den Neuerungen im E-DSG sind in der entsprechenden Fachliteratur zu finden.
12 https://www.isb.admin.ch/isb/de/home/themen/melani.html.
13 Alle sechs Monate veröffentlicht MELANI einen Halbjahresbericht, welcher die über die wichtigsten Cybervorfälle in der Schweiz und International informiert: <https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte.html>.
14 Art. 33 EU-DSGVO.

Verletzung der Datensicherheit zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.[15]

Ein von MELANI erarbeitetes Merkblatt stellt eine Konkretisierung der vom DSG geforderten technischen und organisatorischen Massnahmen dar und bietet KMUs eine Hilfestellung zwecks Erhöhung der Informationssicherheit in ihrer Systemlandschaft.[16] Das Merkblatt adressiert einerseits organisatorische Massnahmen und anderseits Massnahmen auf technischer Ebene und weist aber zu Recht darauf hin, dass weder die einen noch die anderen Massnahmen für sich alleine genügen, die Informationssicherheit in einem Netzwerk zu gewährleisten. Die technischen Vorkehrungen bilden einen wichtigen Teil der IT-Sicherheit, jedoch können diese nur geplant und umgesetzt werden, wenn in einem Unternehmen einerseits ein Bewusstsein für Cyber-Risiken und anderseits auf Stufe Geschäftsleitung und Verwaltungsrat ein entsprechendes Verantwortungsbewusstsein besteht. Das Risiko, Opfer einer Cyber-Attacke zu werden, wird jedoch stark unterschätzt. Studien belegen jedoch, dass rund ein Drittel der Schweizer KMUs schon von Cyber-Attacken betroffen waren (Malware wie Viren oder Trojaner).[17] Trotzdem sahen es 2017 immer noch nur gerade 4% der rund 300 befragten KMU-CEOs als grosse Gefahr an, durch einen Cyber-Angriff mindestens einen Tag lang ausser Gefecht gesetzt zu werden.

2. Cybersecurity Check

Viele Schweizer KMUs wissen nicht oder nur ungenügend, wie das Thema Cyber-Security am besten angegangen werden kann und entsprechend richten sich Hacker immer mehr auf diese sog. «low hangig fruits» aus, also nicht ausreichend geschützte, kleinere Unternehmen.[18] Aufgrund dieser Problematik entwickelte eine Fachgruppe aus den wichtigsten Verbänden und Gruppierungen aus dem IT-Bereich einen Schnelltest, welcher KMUs ermöglichen soll, sich rasch ins Bild setzen zu können, ob ihre technischen, organisatorischen und mitarbeiterbezogenen Massnahmen zum Schutz vor Cyberrisiken ausreichen.

Unter dem Link www.cybersecurity-check.ch ist ein in 12 Themen und insgesamt 34 Fragen unterteilter Fragebogen abrufbar, der auch für den IT-Laien verständlich ist. Was mit Cybersecurity, Firewall, Administrationsrecht und Daten-Back-up-Prozess gemeint ist, wird aber vorausgesetzt. Der Test ermöglicht es Unternehmen, rasch und kostenlos die eigene Cyberresilienz zu überprüfen.

D. Kritische Infrastrukturen

1. MELANI

Die Cyberrisiken betreffen Bürger, private Unternehmen und Bundesbetriebe gleichermassen. Der Schutz vor Cyber-Attacken ist gemäss schweizerischem Konzept eine gemeinsame Verantwortung von Staat, Gesellschaft und Wirtschaft ist. Die grundsätzliche Verantwortung zum Eigenschutz liegt bei den einzelnen Bürgern und Unternehmen. Nur dort, wo die Funktion von kritischen Infrastrukturen zum Wohle der Allgemeinheit

---

15 Art. 22 E-DSG.

16 Melde- und Analysestelle Informationssicherung MELANI, Merkblatt Informationssicherheit für KMUs, Version v2.0, online verfügbar unter <https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html>.

17 Cyberrisiken in Schweizer KMUs, Markt- und Sozialforschungsinstitut gfs-zürich, online verfügbar unter <https://ictswitzerland.ch/media/dateien/Studien/Schlussbericht_Cyberrisk_KMU_2017.pdf>.

18 Medienmitteilung Cyber Security, ICTswitzerland, 03.09.2018.

gewährleistet bleiben muss, ist der Staat in der Verantwortung, basierend auf dem Auftrag aus der Bundesverfassung und dem Landesversorgungsgesetz.[19]

Entsprechend liegt der zweite Fokus der Dienstleistungen von MELANI grundsätzlich im Schutz von kritischen Infrastrukturen. Dazu gehören z. B. Energie- und Wasserversorger, Telekommunikationsunternehmen, Banken, Spitäler, usw., die vom Funktionieren von Informations- und Kommunikationsinfrastrukturen abhängen. MELANI steht Betreibern von kritischen Infrastrukturen mit Mitteln und Wissen unterstützend zur Seite.

2. IKT-Minimalstandard des BWL

Zum Schutz einer funktionierenden schweizerischen Informations- und Kommunikationsinfrastruktur hat das Bundesamt für wirtschaftliche Landesversorgung (BWL) einen IKT-Minimalstandard erarbeitet. Es handelt sich dabei um eine Empfehlung und Richtschnur zur Verbesserung der IKT-Resilienz.[20] Der Minimalstandard richtet sich in erster Linie an die Betreiber der kritischen Infrastrukturen, er soll aber bewusst allen interessierten Unternehmen eine Hilfestellung und konkrete Handlungsanweisung bieten. Ein Self-Assessment Tool kann Unternehmen bei einer Standortbestimmung der eigenen IKT-Struktur helfen. [21]

Das Dokument bietet den Anwendern 106 konkrete Handlungsanweisungen zur Verbesserung der eigenen IKT-Resilienz, welche in die Themenbereiche «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen» gegliedert sind. Es geht somit nicht um den Schutz der IT-Infrastruktur im engeren Sinn, sondern um die – auch vom DSG geforderten – technischen und organisatorischen Massnahmen, um die eigenen Systeme zu schützen. Der Minimalstandard basiert auf dem NIST Cybersecurity Framework, einem Richtlinienpapier des amerikanischen National Institute of Standards and Technology (NIST)[22], welches amerikanischen Unternehmen helfen soll, Cyber-Attacken besser zu erkennen, identifizieren und entsprechend darauf reagieren. Aufgrund des globalen Charakters der Richtlinie dienen die Sicherheitsempfehlungen dem schweizerischen IKT-Minimalstandard als Basis.

E. Branchenspezifische Vorgaben

Beim IKT-Minimalstandard vom BWL handelt es sich um eine allgemein gehaltene Richtlinie, um damit möglichst viele Unternehmen mit unterschiedlichen Anforderungen anzusprechen. In Zusammenarbeit mit einzelnen Verbänden arbeitet das BWL aber an Spezifizierungen der Minimalstandards für einzelne Branchen. Diese branchenspezifischen Standards können sodann von den Verbänden für ihre Mitglieder – im Gegensatz zu den allgemeinen IKT-Minimalstandard – für verbindlich erklärt werden. Im Bereich der Stromversorgung ist dies bereits geschehen. Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) hat im Juli 2018 ein «Handbuch Grundschutz» für die Strombranche veröffentlicht, welches Teil des bestehenden Regelwerks für die Elektrizitätsversorgung wurde.[23] Weitere Standards für die Trinkwasserversorgung, die Erdgas- und Erdölversorgung sowie die Lebensmittelversorgung sind in Ausarbeitung.

---

19 Art. 57, 102 BV; Bundesgesetz über die wirtschaftliche Landesversorgung (LVG).

20 Die Minimalstandards sind für die Unternehmen der kritischen Infrastrukturen derzeit nicht verbindlich, aber der Bund hat mit dem LVG die Möglichkeit, präventive Massnahmen vorzuschreiben, siehe Art. 5 Abs. 4 LVG.

21 Online verfügbar unter: <https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html>.

22 Online verfügbar unter: <https://www.nist.gov/cyberframework>.

23 Handbuch Grundschutz für «Operational Technology» in der Stromversorgung, Juli 2018, online verfügbar unter

Im vergangenen Jahr hat auch die Eidgenössische Finanzmarktaufsicht FINMA neue Vorgaben zum Thema Cyber Security für Banken erlassen, die per 1. Juli 2017 in Kraft getreten sind. Im revidierten Rundschreiben 2008/21 über operationelle Risiken von Banken speziell auch IT- und Cyberrisiken adressiert und die Liste der Risiken im Risikomanagementgrundsatz 4 betreffend die Technologieinfrastruktur ergänzt. Gefordert wird vor allem die Geschäftsleitung: Sie hat sowohl ein allgemeines IT-Risikomanagement-Konzept als auch ein Risikomanagement-Konzept speziell für den Umgang mit Cyber-Risiken zu erstellen und zu implementieren.[24]

II. Europa

Das europäische Recht hat direkt (extraterritoriale Anwendbarkeit der DSGVO) oder indirekt (Orientierung der Praxis und Rechtsprechung an EU-Praxis) eine Ausstrahlung auf die schweizerischen Unternehmen. Insofern lohnt sich ein Blick auf die europäische Cyber-Security Regulierungslandschaft.

A. Europäische Datenschutz-Grundverordnung (DSGVO)

Mit der DSGVO sollte der Datenschutz europaweit vereinheitlicht werden und die Verordnung regelt, wie personenbezogene Daten von betroffenen Personen verarbeitet werden dürfen. Im Rahmen der Verordnung müssen die betroffenen Unternehmen diverse Dokumentations-, Melde- und Genehmigungspflichten erfüllen und die DSGVO enthält somit einige Aspekte, die auch die Cyber-Security betreffen.[25]

Neben den allgemeinen Grundsätzen, welche bei der Bearbeitung von Personendaten zu befolgen sind (Treu und Glauben, Rechtmässigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht), sind insbesondere die folgenden Vorgaben für die Cyber-Security relevant:

— Dokumentationspflicht (Art. 5 Abs. 2 DSGVO)

  Das in der DSGVO verankerte «accountability»-Prinzip führt faktisch zu einer Beweislastumkehr bei Datenschutzverstössen. Die DSGVO fordert, dass ein Verantwortlicher jederzeit die Einhaltung des Gesetzes nachweisen können muss. Kommt es zu einer Cyber-Attacke und somit einem Verlust von Personendaten, muss nicht die Aufsichtsbehörde den Verstoss nachweisen, sondern es liegt am betroffenen Unternehmen, die rechtskonforme Verarbeitung der Daten nachzuweisen. Ein Unternehmen muss also die getroffenen Massnahmen zum Schutz vor Cyber-Attacken jederzeit dokumentieren.

— Meldepflicht von Datenschutzverstössen (Art. 33 und 34 DSGVO)

  Gemäss Art. 4 Nr. 12 DSGVO liegt eine Datenschutzverletzung vor bei einer «*Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden*». Bei Vorliegen einer Verletzung muss ein Unternehmen die zuständige Aufsichtsbehörde (möglichst innert 72 Stunden) informieren. Die Meldung kann nur unterbleiben, falls «*die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt*».

<https://www.strom.ch/fileadmin/user_upload/Dokumente_Bilder_neu/010_Downloads/Handbuch/Grundschutz_OT_in_der_Stromversorgung.pdf>.

[24] Für weitere Informationen, siehe: MARTIN ECKERT, Cyberrisiken und Cyber Security – Neue Vorgaben der FINMA für Banken, September 2017.

[25] Zur DSGVO im Allgemeinen wird auf die unzähligen Fachartikel verwiesen, der vorliegende Beitrag beleuchtet die für Cyber-Security relevanten DSGVO Aspekte.

Falls die Datenschutzverletzung «*voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten*» des Betroffenen bedeutet, so sind die betroffenen Personen unverzüglich ebenso von der Datenschutzverletzung «*in klarer und einfacher Sprache*» zu unterrichten (Art. 34 DSGVO).

— Datenschutz-Folgeabschätzung (Art. 35 DSGVO)

Wenn eine Datenverarbeitung «*voraussichtlich ein hohes Risiko*» zur Folge hat, muss ein Unternehmen eine Datenschutzfolgeabschätzung durchführen, um so die möglichen Risiken der Datenverarbeitung zu erkennen und entsprechende technische und organisatorische Massnahmen zu ergreifen, um den Schutz der Daten sicherzustellen.[26]

B. NIS Direktive

Die NIS-Richtlinie[27] hat zum Ziel, ein höheres Niveau der Netz- und Informationssicherheit in der gesamten EU zu schaffen. Dies soll dadurch erreicht werden, dass die Cyber-Security in Infrastruktursektoren, welche stark IKT abhängig sind, verbessert wird. Entsprechend richtet sich die Richtlinie an die Betreiber wesentlicher Dienste[28], welche in der EU niedergelassen sind sowie an Anbieter digitaler Dienste, welche Dienstleistungen für Personen innerhalb der EU anbieten.

Die NIS-Richtlinie schreibt den betroffenen Unternehmen Sicherheitsanforderungen vor, deren Umsetzung von den EU-Mitgliedstaaten sicherzustellen sind[29]:

— Geeignete technische und organisatorische Maßnahmen zur Sicherung der Netzwerke und Informationssysteme;

— Einbeziehung der neuesten Entwicklungen und Berücksichtigung möglicher Risiken der Systeme;

— Ergreifung geeigneter Maßnahmen, um Sicherheitsvorfälle zu verhindern oder mindestens die Auswirkungen zu minimieren, um die Geschäftskontinuität zu gewährleisten; und

— Benachrichtigung der zuständigen Behörde in Bezug auf die sicherheitsrelevanten Ereignisse, die einen wesentlichen Einfluss auf die Geschäftskontinuität haben.

Um die geforderte Cyberresilienz zu erreichen, fordert die Richtlinie in Artikel 19 die Verwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit der Netze und Informationssystemen. Ausserdem verpflichtet die Richtlinie jeden EU-Mitgliedstaat, eine oder mehrere nationale Behörden zu benennen, welche für die Sicherheit der Netz- und Informationssysteme zuständig ist.[30] Um ein hohes Sicherheitsniveau zu erreichen, muss zudem jedes EU-Land eine nationale Strategie zur Sicherheit

---

26 Eine Übersicht zu den Leitlinien der Artikel-29-Arbeitsgruppe betreffend Datenschutz-Folgeabschätzung und den Positiv- und Negativlisten der Aufsichtsbehörden ist zu finden unter: <http://datenrecht.ch/datenschutz-folgenabschaetzung-leitlinien-der-artikel-29-arbeitsgruppe/>.

27 EU-Richtlinie 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

28 Gem. Art. 5 Abs. 2 der Richtlinie stellt ein Betreiber wesentlicher Dienste einen Dienst bereit, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist, die Bereitstellung des Dienstes von Netz- und Informationssystemen abhängig ist und ein Sicherheitsvorfall eine erhebliche Störung des Dienstes bewirken würde.

29 Art. 14 NIS-Richtlinie. Die EU-Mitgliedstaaten hatten bis zum 9. Mai 2018 Zeit, die Richtlinie in nationales Recht umzusetzen und müssen die Massnahmen ergreifen, um deren Durchsetzung zu gewährleisten und haben bis 9. November 2018 Zeit, um die Betreiber wesentlicher Dienste zu ermitteln.

30 Art. 8 NIS-Richtlinie.

der Netz- und Informationssysteme festlegen, welche die strategischen Ziele sowie konkrete politische Massnahmen vorsieht.

C. EU Cybersecurity Act

Im Rahmen eines Reformpakets der Europäischen Kommission wurden 2017 Massnahmen zur Stärkung der Vorschriften zur Cyber-Security verabschiedet. Die Massnahmen stützen sich insbesondere auf die oben erwähnte NIS-Richtlinie. Mittels einer Verordnung sollen IT-Produkte und Dienstleistungen für Bürger, Unternehmen und die Verwaltung sicherer zu machen.[31] Insbesondere beabsichtigt die Kommission, dadurch das Vertrauen in das Internet der Dinge zu stärken. Der Vorschlag basiert insbesondere auf drei Initiativen:

- Einrichtung einer schlagkräftigen EU-Agentur für Cyber-Security;
- Einführung eines EU-weiter Zertifizierungssystems für Cyber-Security;
- Rasche Umsetzung der NIS-Richtlinie.

Der EU Cyber Security Act sieht vor, die bestehende Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) weiter auszubauen, sodass diese den Mitgliedstaaten und Unternehmen helfen kann, sich gegen Cyber Attacken zu wehren. ENISA soll die gegenseitige Anerkennung und Neuentwicklung von Zertifizierungsschemata koordinieren und die verschiedenen bestehenden Zertifizierungen für IT-Infrastrukturen, Produkte, Dienstleistungen und Systeme in der EU harmonisieren. So soll ein funktionierender digitaler Binnenmarkt in der EU geschaffen werden. Zur Finalisierung und Inkraftsetzung der Verordnung, müssen der Rat der Europäischen Union und das Europäische Parlament eine Einigung über den endgültigen Text erzielen. Die entsprechenden Verhandlungen begannen am 13. September 2018. Der österreichische Ratsvorsitz ist bestrebt, die Verordnung bis Ende des Jahres fertigzustellen.[32]

III. Empfehlungen zur Umsetzung von Cyber Defense Massnahmen

Um eine wirksame Cyber Security in einem Unternehmen umzusetzen, empfehlen wir in einem ersten Schritt, überhaupt erst ein Bewusstsein für die eigene Angreifbarkeit zu schaffen. So müssen sich Unternehmen fragen, wo ihre Risiken liegen. Was sind die digitalen «Kronjuwelen» des eigenen Unternehmens? Wo würde ein Angriff den grössten Schaden anrichten? Dabei sollte man nicht nur an finanzielle Risiken (z.B. als Folge eines Betriebsunterbruchs) denken, sondern ebenso auch an Reputations- und Compliance-Risiken.

In Bezug auf Cyber Security sind Unternehmen in erster Linie selbst gefordert und das eigenverantwortliche Handeln spielt eine grosse Rolle. Gefordert ist insbesondere der Verwaltungsrat. Er trägt die Oberverantwortung für das Risk Management und kann die Verantwortung für die Cybersicherheit nicht an den CIO delegieren. Wer als Verwaltungsrat nichts unternimmt, riskiert im Rahmen der Organhaftung persönlich belangt zu werden. Was muss im Verwaltungsrat eines KMU konkret vorgekehrt werden? Im Vordergrund steht die Schaffung klarer Prozesse und entsprechenden Verantwortlichkeiten. Die nachfolgende Checkliste soll eine nicht abschliessende Übersicht bieten:

---

31 Proposal 9350/18 for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

32 Siehe dazu: <http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0225%28COD%29>.

— Cyber-Risiken gehören auf die Traktandenliste des Verwaltungsrates (Risk Management, IKS)

— Initialisierung der Prüfung von Sofortmassnahmen

— Initialisierung einer Risikoanalyse

— Set-the tone at the top

— Erarbeitung eines Sicherheitskonzepts (Ziele, Verantwortlichkeiten, Definition von Sicherheitsstandards)

— Kontrolle der Umsetzung von technischen und organisatorischen Massnahmen

— Notfallpläne

— Dokumentation

Massnahmen und Verantwortlichkeiten sind schon aus Haftungsgründen sauber zu dokumentieren (Datensicherheitskonzept; Business Continuity; Weisungen für Mitarbeiter; Notfallpläne). Die entsprechenden Konzepte müssen aber vor allem gelebt werden. Sind Prozesse und Verantwortlichkeiten zwar sauber dokumentiert, aber werden nicht entsprechend umgesetzt, kann kein wirksamer Schutz bestehen.

Mitarbeiterschulung ist ein wesentliches Element im Gesamtkonzept Cyber Security von einem Unternehmen: Das schwächste Glied ist der Mensch. Vieles wird von den Mitarbeitenden nicht hinterfragt, E-Mails mit problematischen Anhängen werden unbedacht geöffnet, wenn kein Bewusstsein für die möglichen Gefahren geschaffen wird. Eine Kombination aus gesundem Menschenverstand und geschärftem Bewusstsein für Cyber Risiken kann bereits sehr viel bewirken.

Aufwand und Ertrag sind beim Thema Cyber Risk eine besondere Herausforderung. Technisch ist ein 100%iger Schutz nicht möglich. Die Rest-Risiken können mit Cyber Risk Versicherungen abgedeckt werden.[33]

MME unterstützt Sie beim juristisch verlässlichen Auf- und Umsetzen von Cyber Risk Defence Massnahmen. Für die operative und technische Umsetzung arbeiten wir mit erprobten Partnern Hand in Hand.

Ihr Team

Dr. Martin Eckert
Legal Partner

+41 44 254 99 66
martin.eckert@mme.ch

Eric Neuenschwander
Legal Associate

+41 44 254 99 66
eric.neuenschwander@mme.ch

[33] Siehe dazu: «Wie können Cyber Risiken versichert werden?», <https://www.mme.ch/de/magazin/wie_koennen_cyber_risiken_versichert_werden/>.