Recht

Rino Siffert

3. September 2024

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Stab FGG7 / ICT Warrior Academy
Kommando Cyber

HSLU Hochschule Luzern

Blockwoche Cyber Security

INHALT

Cybersicherheit und Recht

Schweiz

Blick über die Grenze

Schweiz

EU

AUSLEGEORDNUNG

CYBERSICHERHEIT UND RECHT

REGULIERUNG DES CYBERSPACE IN DER SCHWEIZ

- Bislang *kein* eigentliches *Cybersicherheitsgesetz*
- Zur Cybersicherheit gilt es v*erschiedene Rechtsgrundlagen/-gebiete* beachten, aus denen sich Handlungsanweisungen/-pflichten ergeben können
- Dies *erschwert eine umfassende Übersicht* über die Regulierung des Cyberspace in der Schweiz

DEFINITION DES BEGRIFFS «CYBERSICHERHEITSRECHT»

- Cybersicherheitsrecht =
  - *Interdisziplinäre Rechtsmaterie* in *Gesetzen und Verordnungen*, die Aspekte des *Privatrechts, öffentlichen Rechts und Strafrechts* umfasst
  - *Rechtliche Rahmenbedingungen*, die den Schutz von Computersystemen, Netzwerken und Daten vor Bedrohungen regeln, die Folgen von Cyberangriffen behandeln, die Einhaltung von IT-Sicherheitsanforderungen und daten- sowie informationsschutzrechtlichen Vorgaben adressieren
  - Es gibt zudem *sektorspezifische Regulierungen* (z.B. Banken oder Energieversorgung)
  - Im internationalen Kontext müssen Unternehmen zusätzlich *ausländische Rechtsvorschriften und internationale Standards* berücksichtigen

ÜBERSICHT DER BERÜHRTEN RECHTSGEBIETE

DATENSCHUTZRECHT (1/6)

Datenschutzgesetz (DSG) und *Verordnung über den Datenschutz (DSV)* bezwecken den *Schutz der Persönlichkeit* und der *Grundrechte von natürlichen Personen*, über die *Personendaten* bearbeitet werden

Datenschutz verlangt nach *Cybersicherheit* durch *technische sowie organisatorische Massnahmen*

Das DSG sieht eine *Meldepflicht bei einer Datenschutzverletzung* («*Databreach*») vor

Das DSG trat am 1. September 2023 in Kraft und ist inhaltlich stark von der EU-DSGVO beeinflusst

DATENSCHUTZRECHT (2/6)

- Datenschutzrechtliche Vorgaben an die Cybersicherheit:
  - Art. 8 Abs. 1 und 2 DSG verlangen, dass Entitäten, welche Personendaten verarbeiten, dem Risiko angemessen bestimmte *technische und organisatorische Massnahmen für die Sicherheit dieser Daten* ergreifen müssen, um so Verletzungen der Datensicherheit zu vermeiden
  - Seitens des Bundesrates wurde gestützt auf Art. 8 Abs. 3 DSG *detaillierte Bestimmungen über die Mindestanforderungen an die Datensicherheit* erlassen, welche sich in *Art. 3 ff. DSV* finden

DATENSCHUTZRECHT (3/6)

- Technische Massnahmen:
  - Der Schutz von Personendaten soll durch *Datenverschlüsselung* erreicht werden, um unbefugten Zugriff zu verhindern
  - Mittels *Zugriffskontrollen* sind Mechanismen zu implementieren, damit nur autorisierte Personen Zugang zu sensiblen Daten haben
  - Gilt auch Aspekte der *Netzwerksicherheit* zu beachten, damit nicht unbefugte Personen auf diese Daten zugreifen können (z.B. Schutz der IT-Infrastruktur durch Firewalls, Intrusion Detection Systeme (IDS), Durchführung von Updates zwecks Sicherstellung der Systemsicherheit)

DATENSCHUTZRECHT (4/6)

- Organisatorische Massnahmen:
  - Es müssen *Sicherheitsrichtlinien und -verfahren* zur Datensicherheit entwickelt und implementiert werden
  - Regelmässige *Schulungen für Mitarbeiter* zu den Themen Datenschutz und Cybersicherheit müssen durchgeführt werden, um das Bewusstsein und die Kompetenz zu erhöhen

DATENSCHUTZRECHT (5/6)

- Risikoanalysen und Datenschutz-Folgenabschätzungen:
  - Falls Personendaten bearbeitet werden, sind Unternehmen verpflichtet, regelmässige *Risikoanalysen* durchzuführen, um potenzielle *Schwachstellen in ihren Systemen zu identifizieren* und entsprechende *Massnahmen zu ergreifen*
  - Bei der Einführung neuer Systeme oder Prozesse, die personenbezogene Daten betreffen, müssen *Datenschutz-Folgenabschätzungen* durchgeführt werden, um die *Auswirkungen auf den Schutz der Daten zu bewerten* und *Massnahmen zur Risikominderung* zu ergreifen

DATENSCHUTZRECHT (6/6)

- Meldungen von Verletzungen der Datensicherheit:
  - Verletzungen der Datensicherheit («*Databreach*») müssen grundsätzlich dem *Eidgenössischen Datenschutzbeauftragten (EDÖB)* gemeldet werden (Art. 24 Abs. 1 DSG)
  - Es sind nur diejenigen Verletzungen der Datensicherheit meldepflichtig sind, welche dazu führen, dass *Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert oder Unbefugten offengelegt oder zugänglich gemacht werden und* dies wohl zu einem *hohen Risiko für die Persönlichkeit oder die Grundrechte von betroffenen Personen* führt

BEISPIELFALL

- Sachverhalt:
  - Eine Arztpraxis speichert die Gesundheitsdaten ihrer Patienten auf einem Server.
  - Bei einem Cyberangriff dringt ein Hacker in das System ein, stiehlt die sensiblen Gesundheitsdaten der Patienten und löscht alle Daten auf dem Server.
- Details des Vorfalls:
  - *Art des Verstosses*: Verlust und Diebstahl von sensiblen Gesundheitsdaten durch einen Cyberangriff.
  - *Ursache*: Hackerangriff auf den Praxis-Server.
  - *Betroffene*: Alle Patienten der Praxis, deren Gesundheitsdaten auf diesem Server gespeichert waren.
  - *Risiko*: Die entwendeten und gelöschten Daten enthalten sensible Informationen über die Gesundheit der Patienten. Dies stellt ein hohes Risiko für die Persönlichkeitsrechte der betroffenen Personen dar.

BEISPIELFALL

- Meldepflicht:
  - Da der Verlust und Diebstahl der Daten durch den Cyberangriff ein hohes Risiko für die Persönlichkeitsrechte der betroffenen Personen darstellt, ist die Arztpraxis gemäss Artikel 24 Abs. 1 DSG verpflichtet, diesen Vorfall dem EDÖB zu melden.
- Elektronisches Meldeformular:
  - Die Meldung kann über das vom EDÖB bereitgestellte elektronische Meldeformular unter folgender Adresse erfolgen:

    https://databreach.edoeb.admin.ch/report

INFORMATIONSSICHERHEITSRECHT (1/4)

Informationssicherheitsgesetz (ISG) regelt die *sichere Bearbeitung der Informationen* sowie den *sicheren Einsatz der Informatikmittel für alle Behörden und Organisationen des Bundes* zwecks Stärkung der Informationssicherheit

Fokus auf die *kritischen Informationen und Systeme* sowie auf die *Standardisierung der Massnahmen*

ISG sieht eine *Meldepflicht für Cyberangriffe für die Betreiber kritischer Infrastrukturen* vor

Das ISG trat am 1. Mai 2023 in Kraft / weitere Bestimmungen folgen im Jahr 2025

INFORMATIONSSICHERHEITSRECHT (2/4)

- IKT-Grundschutz in der Bundesverwaltung:
  - Das *BACS* legt mittels *Verwaltungsverordnungen den «Grundschutz» der Informatikmittel und Vorgaben zur Netzwerksicherheit in der Bundesverwaltung* fest (Art. 29 Abs. 1 ISV i.V.m. Art. 17 Abs. 1 und Art. 18 Abs. 1 und 2 ISG)
  - Wurde mit der Weisung «Si001 – IT-Grundschutz in der Bundesverwaltung» gemacht:
    - Verbindliche Festlegung der *minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben* im Bereich Informatiksicherheit
    - Für *Informatikschutzobjekte in der Bundesverwaltung ist IKT-Grundschutz* umzusetzen
    - *Umsetzung* der Sicherheitsvorgaben und -massnahmen sind durch die *Verwaltungseinheiten zu dokumentieren und zu überprüfen*

INFORMATIONSSICHERHEITSRECHT (3/4)

- Meldepflicht von Cyberangriffen auf kritische Infrastrukturen:
  - Art. 74*a* ff. ISG sehen bei einem *Cyberangriff eine Meldepflicht* für Betreiberinnen und Betreiber von kritischen Infrastrukturen vor
  - Als *Betreiber kritischer Infrastrukturen* gelten Hochschulen, Banken, Versicherungen, Organisationen der Sicherheit und Rettung, Trink- und Abwasserversorgung, Energieversorgung, öffentlicher Verkehr, Zivilluftfahrt, Fernmeldedienste und Gesundheitseinrichtungen
  - Art. 74e Abs. 2 ISG umschreibt den *Inhalt der Meldung*

INFORMATIONSSICHERHEITSRECHT (4/4)

- Meldepflicht von Cyberangriffen auf kritische Infrastrukturen:
  - Der konkrete Umfang und Inhalt der zu meldenden Informationen wird in der *Cybersicherheitsverordnung* präzisiert und vom BACS in einem Formular in den sog. «Cyber Security Hub» übernommen sowie Erkenntnisse daraus publiziert
  - Als Anreiz wird im Rahmen der technischen Analyse des gemeldeten Angriffs eine Unterstützung durch das *Computer Emergency Response Team (CERT) des BACS* im Sinne einer *Soforthilfe im Notfall vorgesehen*
  - *Zur Ahndung einer Meldepflichtverletzung gibt es auch eine Strafbestimmung*

BEISPIELFALL

- Sachverhalt:
  - Ein Krankenhaus, das als kritische Infrastruktur gilt, wird Opfer eines Cyberangriffs. Hacker installieren eine Ransomware, die alle Patientendaten sowie Verwaltungsdaten verschlüsselt und fordern ein Lösegeld, um die Daten wieder freizugeben. Das Krankenhaus ist durch den Angriff quasi handlungsunfähig.
- Details des Vorfalls:
  - *Art des Angriffs*: Ransomware-Angriff auf die IT-Systeme des Krankenhauses.
  - *Ursache*: Unzureichende IT-Sicherheitsmassnahmen ermöglichten den Zugriff.
  - *Betroffene*: Alle Patienten und Mitarbeiter des Krankenhauses, da sowohl medizinische als auch administrative Daten betroffen sind.
  - *Risiko*: Der Angriff gefährdet Gesundheitsversorgung der Patienten und ist ein erhebliches Risiko für die Persönlichkeitsrechte/Schutz sensibler Daten. Die Sicherheit und Funktionsfähigkeit einer kritischen Infrastruktur wird beeinträchtigt.

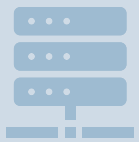
BEISPIELFALL

- Meldepflicht:
  - Gemäss Art. 74*a* und 74*b* Abs. 1 Bst. f ISG ist das Krankenhaus eine Betreiberin einer kritischen Infrastruktur und muss Cyberangriff melden
  - Die Meldung muss Informationen über den Vorfall und seine Auswirkungen enthalten (vgl. Art. 74e Abs. 2 ISG und CSV)
  - Meldung erfolgt im Idealfall über den «Cyber Security Hub»
- Unterstützung durch das CERT:
  - Nach der Meldung wird das Krankenhaus vom Computer Emergency Response Team (CERT) des BACS unterstützt.
  - Das CERT hilft bei der Analyse des Angriffs und leistet nötigenfalls Soforthilfe.
  - Bei den nach der Vorfallbewältigung nötigen Arbeiten zur Wiederherstellung der Daten und Wiederaufbau der Systeme unterstützt das BACS nur beratend.

GESELLSCHAFTSRECHT

Die *Verantwortung des Verwaltungsrats* als Aufsichts- und Kontrollorgan einer Aktiengesellschaft und seine Haftung als Organ sind im Obligationenrecht (OR) geregelt (Art. 716*a*, 717 und 754 OR)

Zu den *unübertragbaren und unentziehbaren* Aufgaben des Verwaltungsrats gemäss Art. 716*a* OR gehören die *Oberleitung des Unternehmens*, die *Bestimmung einer geeigneten Organisation* und die *Ernennung der Geschäftsführung*



Diese Verantwortung erstreckt sich auch auf die *Oberleitung und Organisation sowie die Erteilung von Weisungen mit Blick auf die Cybersicherheit*
Diese Aufgaben können *nicht delegiert* werden
Für die Auswahl der konkreten technischen und organisatorischen Sicherheitsmassnahmen kann der Verwaltungsrat auch *externe technische und juristische Spezialisten beiziehen*

BEISPIELFALL

- Sachverhalt:
  - Ein Maschinenbauunternehmen betreibt seit Jahren eine veraltete IT-Infrastruktur
  - Der Verwaltungsrat und die Geschäftsleitung des Unternehmens haben trotz wiederholter Warnungen des internen IT-Teams keine ausreichenden Cybersicherheitsmassnahmen implementieren lassen
  - Investitionen in IT-Sicherheit wurden aus Kostengründen stets verschoben
  - Unternehmen wird Opfer eines Ransomware-Angriffs, es werden sämtliche Daten verschlüsselt und ein Lösegeld für die Freigabe der Daten verlangt
  - Da keine aktuellen Backups existieren und der Betrieb vollständig zum Erliegen kommt, zahlt das Unternehmen das Lösegeld
  - Die Zahlung und die daraus resultierenden Verluste führen zu einem erheblichen finanziellen Schaden für das Unternehmen

BEISPIELFALL

- <u>Details des Vorfalls:</u>
  - *Art des Angriffs*: Ransomware-Angriff auf die IT-Systeme des Unternehmens
  - *Ursache*: Mangelnde Wartung der IT-Infrastruktur und Unterlassung notwendiger Cybersicherheitsmassnahmen durch den Verwaltungsrat und die Geschäftsleitung
  - *Betroffene*: Das Unternehmen, seine Aktionäre und Gläubiger, da der Vorfall zu erheblichen finanziellen Verlusten geführt hat
  - *Risiko*: Der Angriff gefährdet die finanzielle Stabilität des Unternehmens und stellt ein erhebliches Risiko für die Erfüllung von Verpflichtungen gegenüber Aktionären und Gläubigern dar

BEISPIELFALL

- Verletzung der Sorgfaltspflicht:
  - Der Verwaltungsrat und die Geschäftsleitung haben es versäumt:
    - die notwendigen Cybersicherheitsmassnahmen zu ergreifen, obwohl sie dafür verantwortlich sind,
    - die IT-Sicherheit des Unternehmens zu überwachen, und
    - sicherzustellen, dass angemessene Schutzmassnahmen vorhanden sind
  - Dies stellt eine Verletzung der Sorgfalts- und Treuepflichten gemäss Artikel 716*a* und 717 OR dar
  - Insbesondere haben sie ihre unübertragbare Verantwortung für die Cyber-Sicherheitsstrategie des Unternehmens vernachlässigt

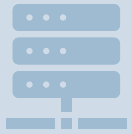
BEISPIELFALL

- <u>Haftung:</u>
  - Aufgrund der fahrlässigen Vernachlässigung der Sorgfaltspflichten könnten die Mitglieder des Verwaltungsrats und die Geschäftsleitung haftbar gemacht werden
  - Sie haften gegenüber dem Unternehmen, den Aktionären und den Gläubigern für den entstandenen Schaden, der auf die mangelhafte IT-Sicherheit und die daraus resultierenden Auswirkungen des Cyberangriffs zurückzuführen ist

VERTRAGSRECHT (1/4)

Mit Blick auf die Cybersicherheit in Unternehmen beizieht sich das *Vertragsrecht* auf die *rechtlichen Aspekte, die bei der Gestaltung, Verhandlung und Durchsetzung von Verträgen mit Kunden, Lieferanten und Partnern* im Zusammenhang mit der *Sicherheit von Informationssystemen und Daten* berücksichtigt werden müssen

Vertragsrecht erfasst die Vereinbarungen und Bestimmungen, die zwischen den Parteien getroffen werden,
- um *angemessene Massnahmen zum Schutz vor Cyberangriffen vorzusehen* sowie
- die *Verantwortlichkeiten und Haftung* im Falle von Sicherheitsvorfällen *festzulegen*



Cybersicherheitsklauseln in Verträgen mit IT-Leistungserbringern spielen eine nicht zu unterschätzende Rolle beim Schutz vor diesen Bedrohungen, indem sie darauf a*bzielen, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen sowie die damit einhergehende Compliance sicherzustellen* und *Haftungsrisiken zu adressieren*

VERTRAGSRECHT (2/4)

- Vielzahl von Vertragsarten im IT-Bereich:
  - Verträge mit Hardware- und Netzwerkanbietern sind eigentliche *Kauf-, Miet- oder Miet-Kaufverträge*
  - Falls die Hardware oder die Netzwerkinfrastruktur speziell nach den Bedürfnissen und Weisungen des Unternehmens zusammengestellt werden, so kann ein *Werkvertrag* vorliegen
  - Sollte die Hardware oder das Netzwerk gewartet oder repariert werden, so kann es sich je nach Ausgestaltung des Vertrags und der darin enthaltenen Pflichten, um einen *Auftrag oder Werkvertrag* handeln
  - Bei Verträgen über den Erwerb von Software kann bei Standardsoftware das *Kaufvertragsrecht* und bei individuell hergestellter Software das *Werkvertragsrecht* zur Anwendung kommen.
  - Falls aber eine Software lediglich genutzt werden soll, so wird dem Unternehmen meist mittels eines *Lizenzvertrags* ein Nutzungsrecht an dieser vertraglich eingeräumt

VERTRAGSRECHT (3/4)

- Vertragliche Regelung der Cybersicherheit:
  - Verträge *klar und präzise* formulieren, um Missverständnisse zu vermeiden und damit Parteien ihre Verpflichtungen verstehen und erfüllen
  - Es können folgende *Aspekte der Cybersicherheit vertraglich geregelt* werden:
    - *Vertraulichkeit*: Es muss vertraglich sichergestellt werden, dass *vertrauliche Daten und Informationen geschützt* und *nicht unbefugt offengelegt* werden
    - *Integrität*: Vertrag muss *Integrität der Daten und Informationen* adressieren, um sicherzustellen, dass sie *nicht unbemerkt manipuliert oder verändert* werden
    - *Verfügbarkeit*: *Systeme, Dienste und Daten müssen jederzeit verfügbar* sein und es sollen keine unnötigen Ausfallzeiten auftreten
    - *Compliance*: Anforderungen an die *Einhaltung von Gesetzen, Vorschriften oder sektor- bzw. branchenspezifischen Standards* im Bereich der Cybersicherheit
    - *Haftung*: Der Vertrag hat festzulegen, *wer für Schäden oder Verluste* infolge von Sicherheitsverletzungen oder Cyberbedrohungen *verantwortlich* ist

VERTRAGSRECHT (4/4)

- Nutzung einer vertraglichen Cybersicherheitsklausel:
  - Gibt *Muster-Cybersicherheitsklausel* für Verträge mit IT-Dienstleistern

    https://www.bkb.admin.ch/dam/bkb/de/dokumente/Oeffentliches_Beschaffungswesen/Mustervertragsklausel_Cyberangriff_20240101b_d.docx.download.docx/Mustervertragsklausel_Cyberangriff_20240101b_d.docx
  - Diese sind im Sinne einer *Maximalvariante* verfasst
  - Können nicht unbesehen übernommen werden, sondern *müssen* jeweils mit Blick auf die Natur des Vertrages sowie dem Ergebnis der Vertragsverhandlungen auf die konkreten Verhältnisse *angepasst werden*
  - Falls der IT-Leistungserbringer einen *Subunternehmer* zur Vertragserfüllung beizieht, so ist die Cybersicherheitsklausel entsprechend zu erweitern

BEISPIELFALL

- Sachverhalt:
  - Ein Unternehmen, das Softwarelösungen für Finanzdienstleister entwickelt, steht kurz vor dem Abschluss eines grossen Projekts, bei dem eine massgeschneiderte Software für einen Kunden erstellt werden soll
  - Das Projekt umfasst die Entwicklung der Software, die Bereitstellung der notwendigen Hardware, den Aufbau einer sicheren Netzwerkstruktur und den fortlaufenden Support und die Wartung der Systeme
- Details der Vertragsgestaltung:
  - *Vertraulichkeit*: Im Vertrag mit dem Kunden wird eine strenge *Vertraulichkeitsklausel* aufgenommen, die sicherstellt, dass alle sensiblen Finanzdaten und Informationen des Kunden während und nach der Projektlaufzeit geschützt sind. Alle beteiligten *Parteien*, einschliesslich der *Subunternehmer*, sind vertraglich zur *Geheimhaltung verpflichtet*.

BEISPIELFALL

- Details der Vertragsgestaltung:
  - *Integrität*: Im Vertrag mit dem Softwareentwickler wird festgelegt, dass *Mechanismen implementiert* werden, um die *Integrität der Daten zu gewährleisten* (z.B. regelmässige Sicherheitsüberprüfungen und die Implementierung von Verschlüsselungen, um unbefugte Änderungen an den Daten zu verhindern)
  - *Verfügbarkeit*: Der Vertrag mit dem Netzwerkdienstleister enthält Regelungen zur *Sicherstellung der Systemverfügbarkeit*. Es werden klare Service Level Agreements (SLAs) vereinbart, die garantieren, dass die Systeme eine sehr hohe Betriebszeit erreichen. Es werden auch Regelungen zu Reaktionszeiten im Falle von Ausfällen festgelegt

BEISPIELFALL

- Details der Vertragsgestaltung:
  - *Haftung*: In allen Verträgen wird klar definiert, *wer im Falle von Sicherheitsverletzungen oder Cyberangriffen haftet* (z.B. Vertrag mit dem Softwareentwickler sieht vor, dass dieser für alle durch Sicherheitslücken in der entwickelten Software verursachten Schäden haftet)
  - *Compliance*: Der Vertrag mit dem Kunden enthält Bestimmungen, die sicherstellen, dass *alle Softwareentwicklungsprozesse und die Datenverarbeitung den geltenden gesetzlichen und regulatorischen Anforderungen entsprechen* (z.B. umfasst branchenspezifische Datenschutzvorgaben und Anforderungen an die Archivierung und Beweissicherung)

BEISPIELFALL

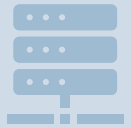
- Details der Vertragsgestaltung:
  - *Information Security Management*: Der Kunde wird verpflichtet, ein internes Information Security Management (ISM) einzuführen, um sicherzustellen, dass alle vertraglich vereinbarten Sicherheitsmassnahmen im Unternehmen umgesetzt und überwacht werden (z.B. regelmässige Audits und Schulung der Mitarbeiter in Bezug auf Cybersicherheit)

ARBEITSRECHT

Sowohl den *Arbeitnehmern als auch den Arbeitgebern* kommen zur *Vermeidung und zur Bekämpfung von Cyberrisiken Rechte und Pflichten* zu

Arbeitgeber hat im Rahmen ihrer *allgemeinen Fürsorgepflicht* die Personendaten der Mitarbeitenden zu schützen (vgl. Art. 328 OR).

Mitarbeiter müssen gestützt auf ihre *arbeitsrechtliche Sorgfalts- und Treuepflicht* gemäss Art. 321e OR Schaden bei der arbeitgebenden Unternehmung abwenden



Unternehmensintern muss daher beispielsweise dafür gesorgt werden, dass im Arbeitsalltag keine Malware oder Ransomware auf das Computersystem der Arbeitgeberin heruntergeladen und installiert wird

BEISPIELFALL

- Sachverhalt
  - Ein Mitarbeiter eines Finanzdienstleistungsunternehmens erhält während der Arbeitszeit eine E-Mail, die angeblich von einem Geschäftspartner stammt
  - Ohne den Absender oder den Anhang zu prüfen, öffnet der Mitarbeiter die Datei, die Malware enthält
  - Diese Malware verbreitet sich schnell im Unternehmensnetzwerk, verschlüsselt Daten und fordert Lösegeld

BEISPIELFALL

- Pflichten des Arbeitgebers/Fürsorgepflicht (Art. 328 OR)
  - Der Arbeitgeber hat sicherzustellen, dass die IT-Infrastruktur des Unternehmens gegen Cyberangriffe geschützt ist, was unter anderem was folgt beinhaltet:
    - Regelmässige Sicherheitsupdates und Wartung der IT-Systeme
    - Bereitstellung von Schulungen und Ressourcen für Mitarbeiter, um sie für Cyberrisiken zu sensibilisieren
    - Implementierung von Sicherheitsrichtlinien, die den Umgang mit verdächtigen E-Mails und Dateien regeln
  - In diesem Fall hat der Arbeitgeber versäumt, ausreichende Schulungen zur Erkennung von Phishing-E-Mails und zur sicheren Nutzung von IT-Systemen anzubieten

BEISPIELFALL

- Pflichten des Arbeitnehmers/Sorgfalts- und Treuepflicht (Art. 321e OR)
  - Der Mitarbeiter ist verpflichtet, vorsichtig und gewissenhaft mit der IT-Infrastruktur des Unternehmens umzugehen, um Schäden zu vermeiden und hierzu gehört:
    - Verdächtige E-Mails oder Links nicht ohne Überprüfung zu öffnen.
    - Unverzüglich den IT-Support zu informieren, wenn verdächtige Aktivitäten bemerkt werden
  - In diesem Fall hat der Mitarbeiter seine Sorgfaltspflicht verletzt, indem er unvorsichtig auf einen unsicheren Link geklickt und so den Cyberangriff ermöglicht hat.

BEISPIELFALL

- Folgen:
  - Durch das unvorsichtige Verhalten des Mitarbeiters kommt es zu einem erheblichen Sicherheitsvorfall, der das Unternehmen finanziell belastet und das Vertrauen der Kunden gefährdet
  - Da der Arbeitgeber jedoch auch seiner Fürsorgepflicht nicht vollständig nachgekommen ist, könnte eine Mitschuld vorliegen
- Schlussfolgerung:
  - Dieses Fallbeispiel zeigt, wie wichtig es ist, dass sowohl Arbeitgeber als auch Arbeitnehmer ihre jeweiligen Pflichten ernst nehmen, um Cyberrisiken zu minimieren
  - Der Arbeitgeber muss proaktiv Sicherheitsmassnahmen implementieren und Mitarbeiter schulen, während die Mitarbeiter ihre Sorgfaltspflicht beachten und verantwortungsvoll handeln müssen

STRAFRECHT (1/3)

Delikte im digitalen Raum werden allgemein als *Computerdelikte* bezeichnet

Man unterscheidet zwischen:
(i) Delikten, die darauf abzielen, Daten und Systeme zu schädigen (sog. *Computerdelikte i.e.S.*) oder
(ii) Delikte, die mittels Computern begangen werden (sog. *Computerdelikte i.w.S.*)

Cyberkriminalität umfasst sämtliche Computerdelikte, welche mit dem Hilfsmittel des Internets begangen werden

STRAFRECHT (2/3)

- <u>Computerdelikte im engeren Sinn (Art.143 ff. StGB):</u>
  - Unbefugte Datenbeschaffung (Art. 143 StGB)
  - Unbefugtes Eindringen in Datenverarbeitungssysteme (Art. 143bis StGB)
  - Datenbeschädigung/Computersabotage (Art. 144bis Ziff. 1 StGB)
  - Herstellen von datenschädigenden Programmen (Art. 144bis Ziff. 2 StGB)
  - Computerbetrug (Art. 147 StGB)
  - Unbefugtes Beschaffen von Personendaten (Art. 179^{novies} StGB)
- <u>Computerdelikte im weiteren Sinn:</u>
  - Gewaltdarstellungen
  - Ehrverletzungen
  - Pornografie

STRAFRECHT (3/3)

- Ethical Hacking:
  - Ethical Hacking hat zum Ziel, auf Sicherheitslücken von Systemen aufmerksam zu machen
  - Experten werden eingeladen, Sicherheitskonzepte auf die Probe zu stellen
- Bug Bounty Programme:
  - Bug Bounty Programme laden im Unterschied zu Ethical Hacking eine *Vielzahl von Hackern* dazu ein, sich in die Systeme einzuschleichen oder ein Schlupfloch ausfindig zu machen
  - Anbieter locken teils mit beträchtlichen Belohnungen
- Fehlende Strafbarkeit sowie zivilrechtliche Haftbarkeit:
  - Strafrechtlich nicht belangbar, da die Einladung zum Hacken eine *Einwilligung* darstellt und dieser Rechtfertigungsgrund den Straftatbestand aufhebt

BEISPIELFALL

- Sachverhalt
  - Ein Anwalt speichert sensible Mandantendaten auf seinem Laptop
  - Diese Daten umfassen vertrauliche Informationen über laufende Rechtsstreitigkeiten, persönliche Dokumente und finanzielle Daten der Mandanten
  - Der Laptop ist zwar passwortgeschützt, aber es wurden keine zusätzlichen Sicherheitsmassnahmen wie Verschlüsselung oder regelmässige Backups implementiert
  - Eines Tages wird der Laptop in einem Café gestohlen, als der Anwalt ihn unbeaufsichtigt lässt
  - Der Dieb kann das Passwort leicht umgehen und hat nun Zugriff auf alle gespeicherten Mandantendaten
  - Diese Daten könnten nun missbraucht oder veröffentlicht werden, was erhebliche Schäden für die betroffenen Mandanten bedeutet

BEISPIELFALL

- Pflichten/Verantwortlichkeiten gemäss Art. 321 StGB
  - *Vertraulichkeit*: Der Anwalt ist gemäss Berufsgeheimnis verpflichtet, die ihm anvertrauten Informationen zu schützen. Dazu gehört auch der Einsatz angemessener Cybersicherheitsmassnahmen
  - *Schutzvorkehrungen*: Angemessene Schutzvorkehrungen hätten in diesem Fall eine *Datenverschlüsselung* und *sichere Speicherung der Daten auf einem zentralen, gut gesicherten Server* beinhalten können

BEISPIELFALL

- Folgen:
  - Durch die unzureichende Absicherung der sensiblen Daten hat der Anwalt das Berufsgeheimnis verletzt
  - Dies könnte nicht nur strafrechtliche Konsequenzen für den Anwalt haben, sondern auch das Vertrauen seiner Mandanten zerstören und zu erheblichen rechtlichen und finanziellen Schäden führen
- Schlussfolgerung:
  - Fall zeigt die Bedeutung von Cybersicherheitsmassnahmen zur Wahrung des Berufsgeheimnisses und wie der sorglose Umgang mit vertraulichen Informationen schwerwiegende Folgen haben kann
  - Betont Notwendigkeit, dass Berufsgeheimnisträger geeignete Massnahmen ergreifen müssen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen, die ihnen anvertraut wurden, zu gewährleisten

BRANCHENSPEZIFISCHE REGULIERUNGEN

Cybersicherheit wird in *zahlreiche Sektoren durch zusätzliche Bestimmungen* reguliert (z.B. Banken, Versicherungen, Energieversorgung)

Solche Vorgaben sollen einen *angemessenen Schutz von Unternehmensdaten und der IT-Sicherheit des Unternehmens* bewirken

FINANZWESEN (1/3)

- Die *FINMA kontrolliert und beaufsichtigt* als Finanzmarktaufsichtsbehörde der Schweiz alle Bereiche des *Finanzwesens*
- Darunter fallen *Banken, Versicherungen, Börsen, Wertpapierhäuser sowie kollektive Kapitalanlagen und Prüfgesellschaften*
- Anlässlich der Revision des *Rundschreibens 2008/21 von 2019* hat die FINMA verschiedene *Ergänzungen im Bereich der Cyberrisiken* in das Dokument aufgenommen
- Nach diesen Regeln ist die *Vorgehensweise bei Cyberrisiken zu dokumentieren*

FINANZWESEN (2/3)

- Die *Dokumentation* soll mindestens folgende Aspekte abdecken:
  - Identifikation der spezifischen Bedrohungspotenziale durch Cyberattacken
  - Schutz der Geschäftsprozesse und der Technologieinfrastruktur
  - Zeitnahe Erkennung und Aufzeichnung von Cyberattacken
  - Reaktion auf Cyberattacken mit zeitnahen und gezielten Massnahmen
  - Sicherstellung der zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyberattacken
- Die Finanzdienstleister sind verpflichtet, *regelmässige Verwundbarkeitsanalysen und Penetrationstests* durchzuführen; hierfür bedarf es qualifiziertes Personal und angemessene Ressourcen

FINANZWESEN (3/3)

- Meldepflicht von Cyberangriffen für von der FINMA überwachte Unternehmen:
  - Unternehmen, die unter die Aufsicht der FINMA fallen, sind dazu verpflichtet, Cyberangriffe an die Behörde zu melden
  - Zwecks Gewährleistung der Integrität und Stabilität des Finanzmarkts
  - Bei der Meldung eines Cyberangriffs müssen betroffene Unternehmen detaillierte Informationen bereitstellen
  - Unternehmen müssen erläutern, welche *Massnahmen* sie implementiert haben, um Vorfälle in Zukunft zu verhindern
  - Die FINMA überwacht die Einhaltung dieser Vorschriften streng und kann bei Nichteinhaltung Sanktionen verhängen

ENERGIEVERSORGUNGSUNTERNEHMEN (1/2)

- Das *revidierte Bundesgesetz über die Stromversorgung (StromVG) sowie die Stromversorgungsverordnung (StromVV)* traten per 1. Juli 2024 in Kraft
- Mit dieser Gesetzgebung wurden *verbindliche Anforderungen an die Informationssicherheit der IT und OT* (Operationale Technologie) der *Schweizer Energieversorgungsunternehmen* erlassen
- *Stromerzeuger, Netzbetreiber, Speicherbetreiber und Dienstleister in der Schweiz* müssen zum *Schutz vor Cyberbedrohungen den in der StromVV gemachten Vorgaben* nachkommen
- Das *zu erreichende Schutzniveau hängt jeweils von der Leistungsfähigkeit* der Systeme *ab*

ENERGIEVERSORGUNGSUNTERNEHMEN (2/2)

- Die Massnahmen zur Erreichung des Schutzniveaus werden aus dem *IKT-Minimalstandard des Bundesamt für wirtschaftliche Landesversorgung (BWL)* abgeleitet
- Der *Eidgenössische Elektrizitätskommission (ElCom)* obliegt die *Überwachung* der Massnahmenumsetzung mittels jährlicher Selbsteinschätzung, Sensibilisierungsgespräche sowie Audits zu technischen Aspekten bei Auffälligkeiten
- Es ist hierfür eine *Übergangsfrist von maximal 24 Monaten* nach Inkrafttreten des StromVG und der StromVV vorgesehen
- Die Kosten für die rechtlich festgelegte Umsetzung von Cybersicherheitsmassnahmen sind für die Netzbetreiber *anrechenbare Netzkosten*

EU-REGULIERUNGEN

AUSWAHL

EU NIS-2 RL (1/6)

- Im *Mai 2022* einigten sich die EU-Mitgliedstaaten und das EU-Parlament nach langen Verhandlungen auf die *NIS-2-Richtlinie* (Richtlinie (EU) 2022/2555; «*Directive on measures for a high common level of cybersecurity across the Union*»)
- Eine *überarbeitete Version* der RL für Netz- und Informationssicherheit (NIS-I-Richtlinie)
- *Mitgliedstaaten* haben rund 18 bis 24 Monate Zeit, um die neuen Elemente der Richtlinie in *nationales Recht umzusetzen*
- Die neuen umfassenden Regelungen für Cyber-Sicherheit für EU-Unternehmen werden *ab Herbst 2024* gelten (Deadline: 17. Oktober 2024)

EU NIS-2 RL (2/6)

- RL soll bei Mitgliedsstaaten sowohl ein *einheitliches Verständnis* als auch *Anforderungsniveau der Cybersicherheitsmassnahmen* schaffen
- Wird vorgegeben, welche *Sparten/Unternehmen* überhaupt unter diese gesetzlichen Anforderungen fallen und strengere Cybersicherheitsstandards berücksichtigen müssen:
  - Auswahl anhand der *Unternehmensgrösse* (mehr als 50 Mitarbeitende, Jahresumsatz oder Jahresbilanz von mehr als 10 Millionen Euro und Zugehörigkeit zu einem kritischen oder wichtigen Sektor)
  - *Wichtige Sektoren* (z.B. Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, öffentliche Verwaltung)
  - Wichtige Sektoren als *kritische Einrichtungen* (z.B. Postdienste, Abfallbewirtschaftung, Warenhersteller)

EU NIS-2 RL (3/6)

- Bringt für Unternehmen eine Vielzahl neuer Pflichten und Anforderungen mit sich:
  - *Unternehmen* muss sich selbst in die *unterschiedlichen Stufen einordnen* (KRITIS bzw. «besonders wichtige Einrichtung» oder «wichtige» Einrichtung) und sich bei der zuständigen Behörde innerhalb von drei Monaten nach Identifikation registrieren
  - «Besonders wichtige» Einrichtungen müssen am *Informationsaustausch über eine zentrale Austauschplattform* teilnehmen
  - Unternehmen müssen sich mit den neuen *strengen Sicherheitsanforderungen* im Rahmen von NIS-2 auseinandersetzen

EU NIS-2 RL (4/6)

- *Risikomanagement* für Informationssicherheit als Grundpfeiler der NIS-2-Compliance:
  - Erfasste Unternehmen sind verpflichtet, *angemessene und verhältnismässige technische, operative und organisatorische Massnahmen* zu ergreifen, um Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder zu minimieren
  - Durch ein *strukturiertes Risikomanagement* können Unternehmen potenzielle Bedrohungen und Schwachstellen in ihren Netz- und Informationssystemen frühzeitig erkennen
  - Dies umfasst sowohl *interne als auch externe Bedrohungen*, wie etwa Cyberangriffe, Datenschutzverletzungen, Systemausfälle oder menschliches Versagen

EU NIS-2 RL (5/6)

- Informationssicherheitsstandards in Lieferketten sicherstellen:
  - *Sicherheit in der Lieferkette* ist ein wichtiger Aspekt der NIS-2-Anforderungen
  - Unternehmen müssen sicherstellen, dass ihre *Geschäftspartner und Dienstleister angemessene Sicherheitsvorkehrungen für ihre Informationssicherheit* treffen
  - Dies kann zum Beispiel den *Abschluss vertraglicher Vereinbarungen* umfassen, in denen *Sicherheitsanforderungen festgelegt* werden
  - Auch *Zertifizierungen* spielen eine wichtige Rolle, um die *Erfüllung von Standards nachzuweisen*

EU NIS-2 RL (6/6)

- Sicherheitsvorfälle melden und angemessen behandeln:
  - Unternehmen, die als *Betreiber Kritischer Infrastruktur* in den Anwendungsbereich der NIS-2 fallen, müssen ihre nationale Cybersecurity-Behörde *unverzüglich* über signifikante Störungen, Vorfälle und Bedrohungen ihrer kritischen Dienstleistungen *unterrichten*
  - Im Rahmen der Umsetzung der NIS-2 muss das Unternehmen auch ein effektives *Sicherheitsprogramm mit klaren Richtlinien und Verfahren für den Umgang mit Sicherheitsvorfällen* implementieren

EU NIS-2 RL (7/7)

- Sanktionen bei Verstössen gegen NIS-2:
  - *Geldstrafen*, aber auch andere Massnahmen möglich
  - *Umfang der Sanktionen* hängt von der *Schwere des Verstosses und den spezifischen Umständen* ab
  - Ähnlich wie bei der DSGVO sind konkrete finanzielle Werte als *Bussgeldobergrenze* angegeben (bis maximal EUR 10'000'000 oder 2% des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens)

EU-AI-ACT (1/7)

- *EU Artificial Intelligence Act («AI Act»)* wurde entwickelt, um die *KI zu regulieren*, Vertrauen in KI-Systeme zu schaffen und sicherzustellen, dass diese ethisch und sicher eingesetzt werden
- KI-System = ein maschinengestütztes System, das durch Verarbeitung von Eingaben selbstständig Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, um physische oder virtuelle Umgebungen zu beeinflussen

EU-AI-ACT (2/7)

- KI-Technologien werden demnach in *vier verschiedene Risikokategorien* zugeordnet entsprechend dem Grad ihrer *Risiken für Gesundheit, Sicherheit und Grundrechte*:
  1. *Unvertretbares Risiko*:
     - KI-Systeme, die eine erhebliche Bedrohung für Sicherheit, Lebensgrundlagen oder Rechte der Menschen darstellen (z. B. KI-gestützte soziale Bewertungssysteme durch Regierungen), sind grundsätzlich verboten
  2. *Hohes Risiko*:
     - KI-Systeme, die in kritischen Infrastrukturen, Bildungs- und Beschäftigungsentscheidungen, Strafverfolgung, Migration und in anderen sensiblen Bereichen eingesetzt werden, werden als «hochriskant» eingestuft
     - Diese Systeme unterliegen strengen Anforderungen, wie etwa einer umfassenden Risikobewertung, Transparenzvorgaben und kontinuierlichem Monitoring

EU-AI-ACT (3/7)

- KI-Technologien werden demnach in vier verschiedene Risikokategorien zugeordnet entsprechend dem Grad ihrer Risiken für Gesundheit, Sicherheit und Grundrechte:
  3. *Begrenztes Risiko*:
     - KI-Systeme, die ein geringeres Risiko darstellen, müssen bestimmte Transparenzanforderungen erfüllen
     - Beispielsweise müssen Benutzer darüber informiert werden, dass sie mit einer KI interagieren, wenn dies nicht offensichtlich ist (z. B. bei Chatbots)
  4. *Minimales Risiko*:
     - Für KI-Systeme, die in alltäglichen Anwendungen wie Spam-Filtern oder KI-basierten Videospielen eingesetzt werden, gelten keine spezifischen Anforderungen, da das Risiko als gering eingeschätzt wird
- *Je Kategorie* gelten unterschiedliche *Verbote bzw. Compliance- und Informationspflichten*

EU-AI-ACT (4/7)

- *Zeitliche Staffelung* bei Umsetzung der Vorschriften (je nach Risikoprofil des KI-Systems):
  - *1. August 2024*: Inkrafttreten EU-AI-Act
  - *2. Februar 2025*: Vorschriften für verbotene KI-Systeme («Social Scoring», «Predictive Policing») umsetzen oder letztere aus Verkehr nehmen
  - *2. August 2025*: Unternehmen müssen EU-AI-Act «*compliant*» sein, andernfalls Sanktionen
  - *2. August 2026*: Gewisse Hochrisiko-KI-Systeme müssen Anforderungen EU-AI-Act entsprechen
  - *2. August 2027*: Längere Umsetzungsfrist für spezifische Hochrisiko-KI-Systeme

EU-AI-ACT (5/7)

- Situation in der Schweiz:
  - *Kein AI Act*
  - *Geltende rechtlichen Bestimmungen anwendbar KI* (z.B. Roboter verursacht Schaden: Wiedergutmachung gemäss dem Haftpflichtrecht)
  - Gibt in der Schweiz bereits die vom *Bund herausgegebenen Leitlinien für Künstliche Intelligenz* vom 25. November 2020 als Rahmen für die ethische und verantwortungsvolle Nutzung von KI in der Schweiz
  - Bundesrat hat das *UVEK und das EDA beauftragt, bis Ende 2024 eine umfassende Analyse über den Regulierungsbedarf* der künstlichen Intelligenz *in der Schweiz* zu erstellen

EU-AI-ACT (6/7)

- Situation in der Schweiz:
  - AI Act hat eine *über die Grenzen der EU hinausgehende Wirkung* und gilt somit *auch für Schweizer Unternehmen, die in der EU tätig sind, oder deren KI-Produkte in der EU verwendet* werden
  - Im EU-Markt tätige, Schweizer Unternehmen, müssen neben den Anforderungen des Schweizer Datenschutzgesetzes (DSG) und der Datenschutz-Grundverordnung der EU (DSGVO), zusätzlich die *Regelungen des AI Act* beachten

EU-AI-ACT (7/7)

- Sanktionen und Strafen:
  - *Sanktionen* bei Verstössen gegen den AI Act sind *erheblich*
  - Administrative Bussen gegen das fehlbare Unternehmen *von bis zu 35 Millionen Euro oder 7% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres* umfassen (je nachdem, welcher Betrag höher ist)
  - Hohen Strafen unterstreichen die *Bedeutung der Einhaltung der neuen Vorschriften und die Notwendigkeit*, entsprechende *Compliance-Massnahmen zu implementieren*

EU CYBERSICHERHEITSGESETZ (EU CYBERSECURITY ACT)

- *Inkrafttreten*: Das EU-Cybersicherheitsgesetz trat im Juni 2019 in Kraft
- *Zweck*: Es legt den rechtlichen Rahmen für die Cybersicherheit in der EU fest und stärkt die Rolle der Europäischen Agentur für Cybersicherheit (ENISA)
- *Schwerpunkte*:
  - Gesetz schafft eine dauerhafte Mandatierung und eine erweiterte Rolle der ENISA, damit diese die EU-Mitgliedstaaten, Institutionen und Unternehmen in Fragen der Cybersicherheit unterstützen kann
  - Gesetz enthält ein EU-weites Cybersicherheitszertifizierungssystem für Produkte, Dienstleistungen und Prozesse
- *Ziel*: Verbesserung der Cybersicherheit in der EU durch Schaffung eines gemeinsamen Zertifizierungsrahmens und Unterstützung der Mitgliedstaaten bei der Bekämpfung von Cyberbedrohungen

EU CYBER RESILIENCE ACT (CRA)

- *Inkrafttreten*: Gesetz über die Cyber-Resilienz soll in der zweiten Hälfte des Jahres 2024 in Kraft treten, und die Hersteller müssen bis 2027 konforme Produkte auf den EU-Markt bringen
- *Zweck:* Cybersicherheit von vernetzten Produkten (Hardware und Software) in der gesamten EU zu verbessern
- *Schwerpunkte:*
  - Hersteller von vernetzten Produkten müssen bestimmte Cybersicherheitsanforderungen erfüllen, bevor diese Produkte auf den Markt gebracht werden dürfen
  - Anforderungen an das Sicherheitsdesign und die laufende Sicherheitswartung (Updates)
- *Ziel:* Verbesserung der Widerstandsfähigkeit von vernetzten Produkten gegen Cyberangriffe und Schaffung eines einheitlichen Regelwerks für die Cybersicherheit von Produkten im EU-Binnenmarkt