Emerging Risks

Cyber Risks

Letzte Anpassung September 2018

Private und öffentliche Unternehmen sind heute in allen Bereichen ihrer Geschäftstätigkeit auf IT-Systeme angewiesen und entsprechend anfällig auf entsprechende Störungen verursacht durch Cyber-Risiken. Die Komplexität der Informationssicherheit ist noch nicht vollständig erkannt, und entsprechende Risiken werden oft unterschätzt. Informationssicherheit umfasst unter anderem den Schutz der Vertraulichkeit von Informationen und Daten (Confidentiality), den Schutz vor unbefugter Veränderung von Daten (Integrity) und die Gewährleistung der Verfügbarkeit von kritischen IT-Systemen, wie beispielsweise Zahlungssysteme. Folgende Risikobereiche lassen sich identifizieren:

- Ausfall oder Unterbrechung von kritischen Infrastrukturen der Informations- und Kommunikationstechnologie (Critical Information Infrastructure = CII-Breakdown)
- Online Daten- und Informationssicherheit (Online data and information security , z.B. Cloud Computing) in Bezug auf möglichen Datenverlust
- Informationsdiebstahl (Cyber theft)
- Informationsspionage (Cyber espionage)
- Informationskrieg und Terror (Cyber war and Cyber terrorism)

Gefahren aus dem Internet sind vielfältig und umfassen neben den traditionellen Viren, Würmern, Trojanischen Pferden und Spyware, welche zu unwiederbringlichem Verlust von Daten, zur Beeinträchtigung der Privatsphäre, zum Verlust von Geschäftsgeheimnissen, Informationen zu Handelspartnern führen können, auch Aktivitäten wie Phishing von Daten, die beispielsweise zu Kreditkartenmissbrauch führen können, Spammails, die häufig nur lästig sind und kostbare Arbeitszeit stehlen, sowie «Cryptolocker» – auch Verschlüsselungsviren, Erpressungstrojaner oder Ransomware genannt – , welche die Dateien unlesbar machen und meist gegen Bezahlung eines Lösegelds in der Internet-Währung «Bitcoin» wieder entschlüsselt werden können. Details zu den einzelnen Gefahren sind in den folgenden Quellen aufgeführt:

- Die Melde- und Analysestelle MELANI
  bietet aktuelle Informationen zur Sicherheit von Computersystemen und des Internets sowie zum Schutz der schweizerischen kritischen Infrastrukturen (https://www.melani.admin.ch/melani/de/home.html).

Beispiele aus MELANI:
Neben den ausführlichen Halbjahresberichten hat die Melde- und Analysestelle Informationssicherung MELANI kürzlich folgende Newsletters und Blogs publiziert (aus MELANI Halbjahresbericht 2/2017):

- Wieder vermehrt betrügerische Anrufe bei Firmen (05.07.2018)
  In den letzten Tagen mehren sich wiederum Anrufe bei potenziellen Opferfirmen, in denen sich Angreifer als Bankmitarbeiter ausgeben. Die Anrufer bitten um die Ausführung von Zahlungen oder geben vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll.
- Datenabflüsse, Crimeware und Angriffe auf industrielle Kontrollsysteme – Themen im MELANI-Halbjahresbericht (26.04.18)

Der am 26. April 2018 veröffentlichte 26. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cyber-Vorfällen der zweiten Jahreshälfte 2017 im In- und Ausland. Im Fokus stehen unter anderem der verbreitete Einsatz von Crimeware sowie Angriffe auf industrielle Kontrollsysteme.

– 70'000 Zugangsdaten zu Internet-Diensten gestohlen (05.12.2017)
  Der Melde- und Analysestelle Informationssicherung MELANI wurde wiederum eine Liste mit Zugangsdaten bestehend aus Login und Passwort gemeldet. Diesmal handelt es sich um 70'000 Datensätze.
– Verschlüsselungstrojaner und missbräuchliche Mails im Namen von Behörden im Vormarsch (02.11.2017)
  Der am 2. November 2017 veröffentlichte 25. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cyber-Vorfällen der ersten Jahreshälfte 2017 im In- und Ausland. Im Schwerpunktthema widmet sich der Bericht den Verschlüsselungstrojanern «Wanna Cry» und «NotPetya».

Etwas ältere, aber illustrative Beispiele sind:

– Der Cyber-Angriff auf die Wasserversorgung in Queensland/Australien. Ein entlassener Angestellter der Stadtwerke einer Gemeinde wollte sich rächen und drang mit Hilfe seines Laptops über eine drahtlose Verbindung in das Wasserkontrollsystem seines ehemaligen Arbeitgebers ein. Er öffnete Schleusentore, woraufhin sich grosse Mengen Abwasser in das örtliche Flusssystem ergossen.
– Cyber-Attacken gegen Google und andere US-Konzerne – angeblich von chinesischen Hackern durchgeführt – haben Bedenken in den USA über die nationale Sicherheit und die Wirtschaft hervorgerufen. Cyber-Angriffe waren auf das amerikanische Militär und Verteidigungsinstitutionen fokussiert. Die Attacken aus China gegen Google und andere Unternehmen haben den Diebstahl geistigen Eigentums im grossen Massstab als Ziel. Eine kürzlich durchgeführte Studie ergab, dass die Kosten dieser wirtschaftlichen Angriffe hunderte von Milliarden Dollar betragen können.
– Haftungsrisiken von Social-Networking-Sites, wie Facebook oder Twitter: Sowohl Arbeitnehmer als auch Arbeitgeber können sich durch den Einsatz von Social-Networking-Medien am Arbeitsplatz in einer schwierigen Lage befinden. Beispiel: Ein Manager sendet über Facebook eine «Freundschaftsanfrage» an Mitarbeiter/Innen, was in letzter Zeit ein zu beobachtender Trend ist. Online-Beziehungen zwischen einem Vorgesetzten und einem Mitarbeiter können in Zukunft – nicht nur in den USA – vermehrt zu rechtlichen Ansprüchen führen. Zu denken ist hier an verschiedene Arten von Belästigungen, z. B. von sexuellen Übergriffen bis hin zur Rassen-, bzw. Geschlechter- oder religiösen Diskrimination oder auch in Bezug auf ungerechtfertigte Kündigung.

Meldungen über Diebstahl, Verfälschung oder Zerstörung persönlicher, elektronisch gespeicherter Daten, wie Kreditkarten-Informationen oder auch medizinische Daten (z. B. in Spitälern) durch Hacker haben in letzter Zeit zugenommen. Jedes Unternehmen und generell Organisationen mit einer grossen Menge gespeicherter persönlicher Daten (z.B. Mitarbeiter-, Kunden-, Patientendaten) sind hiervon betroffen. Diese Unternehmen sind verpflichtet, entsprechende Massnahmen zum Schutz der persönlichen Daten, der Datensicherheit und deren Wiederherstellung zu implementieren und zu unterhalten (Sorgfaltspflicht). Dies beinhaltet auch regelmässige Updates oder den Ersatz von Software um allfällige Sicherheitslücken zu schliessen. Die «Wanna-Cry»-Attacke vom Mai 2017 hat deutlich aufgezeigt, dass es unabdingbar ist, die Software regelmässig zu überprüfen und entsprechende Anpassungen vorzunehmen. Diese Attacke hat Dutzende von Spitälern in Grossbritannien lahmgelegt sowie bei der Deutschen Bahn zu Ausfällen und beim Automobilhersteller Renault zu Produktionsbeeinträchtigungen geführt. Beim englischen nationalen Gesundheitsdienst (NHS) laufen knapp 5 Prozent der Computer auf dem praktisch ungeschützten Betriebssystem Windows XP.

Zudem verschärfen sich die rechtlichen Anforderungen, wie z. B. im Fall eines Datenverlusts vorgegangen werden muss. In Amerika müssen alle betroffenen Personen über den Vorfall informiert werden, und in vielen Fällen muss ein «Credit Watch» offeriert werden, was den Missbrauch von Kreditkarten verhindern soll. Diese Massnahmen führen zu Folgekosten.

ASA | SVV

Risikowahrnehmung
Unbestritten ist die Abhängigkeit der Wirtschaft von Informationssystemen. In der Tagespresse werden regelmässig Berichte über Störungen und widerrechtliche Angriffe auf Informationssysteme aller Art publiziert.

Haftpflichtrechtliche Relevanz
Es besteht eine Tendenz aus den USA bzw. aus UK, dass vermehrt Schadenersatzklagen als Folge des Verlustes von (vertraulichen) Daten erhoben werden. Dieser Trend kann auch in Europa (bzw. in der Schweiz) beobachtet werden. Die Haftpflicht aus der rechtswidrigen Beeinträchtigung von kritischen Infrastrukturen, Computern, Netzwerken, Daten etc. ist sicher gegeben, auch wenn die Täter schwer zu ermitteln sein werden.
Die Haftpflicht aus der Sorgfaltspflichtverletzung von Informationssystem-Betreibern und IT-Serviceprovidern (ISP) für Folgeschäden ist ebenfalls gut denkbar (z. B. Personenschäden in Spitälern, aber auch Sachschäden oder Umweltbeeinträchtigungen).

Im April 2016 wurde die EU-Datenschutz-Richtlinie verabschiedet und gilt ab 25. Mai 2018 unmittelbar in allen Mitgliedstaaten der EU. Erwartet wird, dass die Verpflichtung, über schwere Datenschutzverletzungen zu informieren, aber auch die vorgesehene maximale Höhe der Strafe von 4% des Umsatzes, zu einem erhöhten Risikobewusstsein und als Folge davon zu einer verstärkten Nachfrage nach Versicherungslösungen in Europa führen wird.

Haftpflichtversicherungstechnische Relevanz
Betriebshaftpflichtversicherung:
Personen- und Sachschäden als Folge der Störung von Informationssystemen sind versichert. Es handelt sich aber um ein weniger wahrscheinliches Szenario, da mittlerweile die Informationssicherheit einen hohen Stellenwert in der Firmenpolitik aller Art von Unternehmungen hat. Reine Vermögensschäden aus der Unterbrechung von kritischen Informationssystemen können teilweise versichert werden.

In denjenigen Fällen, wo Cyber Risiken nicht explizit ausgeschlossen sind (z.B. AVB Betriebshaftpflicht-Versicherung), sind Ansprüche aus der gesetzlichen Haftpflicht für Personen- oder Sachschäden mitversichert (silent cyber cover).

Risiken	Schaden / Deckung	AVB BH-Versicherung
Gesetzliche Haftpflicht für Persönlichkeitsverletzungen	Entschädigung Dritter für Personenschäden aufgrund der fahrlässigen Bekanntgabe von geheimen/persönlichen Informationen	
	Entschädigung Dritter für reine Vermögensschäden aufgrund der fahrlässigen Bekanntgabe von geheimen/persönlichen Informationen	
Gesetzliche Haftpflicht für Verletzungen der Computersicherheit	Entschädigung Dritter für Personen-/ Sachschäden aufgrund mangelhafter Netzwerksicherheit des VN	

ASA | SVV

Risiken	Schaden / Deckung	AVB BH-Versicherung
	Entschädigung Dritter für reine Vermögensschäden aufgrund mangelhafter Netzwerksicherheit des VN	
Schäden an Daten/Informationen des VN ohne Beschädigung von Hardware	Kosten für die Wiederherstellung von durch eine Computerattacke gestohlenen, zerstörten oder korrupten Daten	
Ertragsausfälle des VN als Folge – von Computerattacken – der Unterbrechung der Infrastruktur (z.B. Strom)	Ertragsausfälle als Folge der Unterbrechung von IT bzw. mangelhafter Umgang mit vertraulichen Informationen	
Mehrausgaben des VN aufgrund von gegen ihn gerichteten erpresserischen Computerattacken	Ermittlungskosten und Entschädigung von Erpressungsforderungen	
Identitätsdiebstahl	Kosten/Ausgaben aufgrund des Identitätsdiebstahls	

Versichert Nicht versichert

Berufshaftpflichtversicherung (IT-Dienstleistungsunternehmen, Soft-/Hardware-Herstellung etc.):
Vermögensschäden durch fehlerhaftes Erbringen von Dienstleistungen sind versicherbar. In der Regel sehen die Dienstleistungsverträge aber Haftungsbeschränkungen vor.

Vermehrt werden international, aber auch im schweizerischen Versicherungsmarkt, spezielle Cyber-Versicherungen angeboten. Diese Produkte decken in der Regel die Aufwendungen für die Wiederherstellung der eigenen Daten und Ertragsausfälle aus der Betriebsunterbrechung (First Party-Deckung) sowie Ansprüche Dritter aus der gesetzlichen Haftpflicht (Third Party-Deckung) für Schäden im Zusammenhang beispielsweise mit der Verletzung von Persönlichkeitsrechten und dem Missbrauch von Kreditkarteninformationen.

D&O-Haftpflichtversicherung
Inadäquate Kontrolle und Sicherheitsstandards können zu grossen finanziellen Schäden bis hin zum Konkurs des Unternehmens führen. Als Folge davon sind Klagen gegen die Verantwortlichen der Unternehmen denkbar. Die Versicherungspolicen sehen in der Regel keinen Ausschluss für Schäden im Zusammenhang mit mangelhafter Informationssicherheit vor.

Zeithorizont für versicherte Ansprüche
Aktuelles Problem – Ansprüche aus diesen vielfältigen Risiken sind jederzeit zu erwarten.