BIANCHISCHWALD

NEWS

CYBERSECURITY UND COVID-19:

Die COVID-19-Krise bedeutet für Unternehmen grosse Anpassungen, die innert kürzester Zeit zu erfolgen haben. Als Reaktion wurde in vielen Fällen auf dezentrale Arbeitsweisen umgestellt. So vergrösserte sich die Abhängigkeit der Unternehmen von der Technologie. Ein Angriff von Cyberkriminellen könnte nun noch weitreichendere Folgen haben. Dies führt auch aus rechtlicher Sicht zu Handlungsbedarf.

Erschwerend kommt hinzu, dass die Auswahl der verwendeten Infrastruktur (Hardware, Software) in vielen Fällen nicht nach eingehender Prüfung erfolgte und die Mitarbeiter nicht angemessen eingeführt, geschult und auf mögliche Problembereiche sensibilisiert werden konnten.

Was ist Cybersecurity?
Unter Cybersecurity wird der Schutz von IT-Systemen bestehend aus Hardware, Software und den darin enthaltenen Daten verstanden. Diese Systeme sind einer Vielzahl von Bedrohungen unterschiedlicher Natur ausgesetzt. Das klassische Beispiel ist der Cyberkriminelle, welcher sich unerlaubt Zugang zu einem System verschafft, um entweder geheime Informationen auszuspionieren oder die Infrastruktur des Opfers zu blockieren oder gar zu zerstören. In den vergangenen Jahren haben insbesondere Fälle von Ransomware grosse Schäden angerichtet und entsprechende mediale Aufmerksamkeit erhalten. Bei einem solchen Angriff werden die Daten des Opfers technisch unlesbar gemacht. Um dies rückgängig zu machen, verlangt der Angreifer eine Gegenleistung (meist Geld oder Crypto-Währungen). Aus technischer Sicht ist zu beachten, dass scheinbar geringfügige Veränderungen der Infrastruktur substanzielle Risiken bewirken können, die nicht immer rechtzeitig erkannt werden. Als Beispiel: Verbinden sich die Mitarbeiter mit ihren privaten WiFi statt mit dem firmeninternen Netzwerk, entstehen zahlreiche weitere Angriffspunkte, die der Kontrolle des Cybersecurity-Verantwortlichen weitgehend entzogen sind. Dies gilt selbst dann, wenn über eine sichere Verbindung (z. B. über ein Virtual Private Network, kurz VPN) auf den Server zugegriffen wird.
Ebenso verbreitet sind Angriffe, die unter dem Oberbegriff «Social Engineering» zusammengefasst werden. Es geht jeweils um zwischenmenschliche Beeinflussungen durch Cyberkriminelle, die beim Opfer bestimmte Verhaltensweisen auslösen sollen. Ein bekanntes Beispiel sind sogenannte Phishing-Attacken. Der Angreifer gibt sich als eine legitime Institution aus, um das Opfer dazu zu verleiten, geheime Informationen (wie Passwörter, Bank- oder Kreditkartendaten) preiszugeben oder Zahlungen auszulösen. Unternehmen werden durch die nun eingeführten dezentralen Arbeitsweisen deutlich anfälliger auf solche Angriffe. Plötzlich werden alltägliche Interaktionen, die zuvor ausnahmslos im persönlichen Austausch erfolgten, über elektronische Kommunikationsmittel abgewickelt. Dadurch entsteht eine neue Angriffsfläche für Unternehmen.

Welche rechtlichen Aspekte sind bei Cybersecurity zu beachten?
Neben den betrieblichen und finanziellen Risiken sowie allfälligen Reputationsschäden bestehen im Hinblick auf Cybersecurity auch rechtliche Pflichten. Welche Pflichten im Einzelfall zu beachten sind, ist eine eigentliche Schlüsselfrage. Das Schweizer Recht kennt keine allgemeine Pflicht, die Integrität von IT-Systemen zu schützen. Stattdessen enthalten verschiedene Gesetze mit unterschiedlichen Regelungsgegenständen Vorschriften, die den Schutz von IT-Systemen ausdrücklich oder aber implizit voraussetzen.

Strafrecht
Vorab verdienen diejenigen Regeln besondere Beachtung, deren Verletzung strafrechtliche Konsequenzen haben können. Zu den bekanntesten Beispielen gehört der Schutz des Berufsgeheimnisses, des Fabrikations- und Geschäftsgeheimnisses oder des Bankkundengeheimnisses. Weniger offensichtlich ist, dass mit der ungenügenden Sicherung von IT-Systemen z. B. auch der Tatbestand der ungetreuen Geschäftsbesorgung erfüllt sein kann. Weiter ist auch die Verletzung gewisser datenschutzrechtlicher Bestimmungen unter Strafe gestellt.
Diese Strafbestimmungen stellen meist nur die vorsätzliche Tatbegehung unter Strafe, und oft wird zudem der Strafantrag einer berechtigten Person vorausgesetzt. Das Risiko einer Verurteilung ist deshalb fast immer gering. Nichtsdestotrotz ist eine rechtliche Überprüfung angesichts der möglichen einschneidenden Folgen empfehlenswert.

Zivilrecht und Verwaltungsrecht
Auch im Zivil- und Verwaltungsrecht gibt es zahlreiche Bestimmungen, welche die Integrität von IT-Systemen vorschreiben oder voraussetzen. Nachfolgend werden einige dieser Bestimmungen exemplarisch herausgegriffen, welche für die überwiegende Mehrheit der Schweizer Unternehmen relevant sind.

Zu erwähnen ist vorab die Gesetzgebung zum Datenschutz, namentlich das Schweizer Datenschutzgesetz und die dazugehörige Verordnung. Es handelt sich um eine wichtige Rechtsquelle im Zusammenhang mit dem Schutz von IT-Systemen. Sie schreibt für Personendaten ausdrücklich vor, dass diese Informationen durch angemessene technische Massnahmen gegen unbefugtes Bearbeiten zu schützen sind. Aufgrund der breiten Definition des Begriffs «Personendaten» betrifft diese Pflicht fast ausnahmslos alle Unternehmen, unabhängig von deren rechtlicher Organisationsform.

Auch die Geschäftsbücherverordnung enthält Grundsätze, die bei der elektronischen Aufbewahrung von Unterlagen zu beachten sind. Im Hinblick auf die Cybersecurity ist primär die Pflicht bedeutsam, die Integrität (Echtheit und Unverfälschbarkeit) und Verfügbarkeit der Unterlagen sicherzustellen. Dies ist von sämtlichen Unternehmen einzuhalten, welche der obligationenrechtlichen Pflicht zur Buchführung unterstehen. In diesem Zusammenhang sind auch steuer- und sozialversicherungsrechtliche Aufbewahrungspflichten zu nennen.

Daneben bestehen diverse Industrie- und Best-Practice-Standards. Zu denken ist etwa an Vorschriften für Finanzinstitute oder ISO-Zertifizierungen, welche Datenschutz- und weitere relevante Standards vorgeben. Darüber hinaus sind allenfalls auch Vorgaben nicht-staatlicher Organisationen zu beachten, die weitere Pflichten in Form von Selbstregulierung vorschreiben (z. B. Geheimhaltungspflichten).

Weiter ergibt sich oft auch aus Verträgen die Pflicht, die Sicherheit von IT-Systemen zu gewährleisten. Besonders naheliegend sind Geheimhaltungspflichten, die in Verträgen als Nebenpflicht vereinbart werden oder gar die Hauptpflicht darstellen (sog. Non-Disclosure Agreement oder Confidentiality Agreement). Darüber hinaus können auch weitere vertraglich übernommene Pflichten (mittelbar) voraussetzen, dass die Sicherheit der IT-Systeme zu gewährleisten ist. So kann z. B. die Pflicht bestehen, über die im Rahmen des Vertrags ausgeführten Tätigkeiten Rechenschaft abzulegen. Dies ist nur möglich, wenn die dazu benötigten elektronischen Unterlagen entsprechend gesichert sind.

Das vorrangige Risiko, welches mit der Verletzung von zivilrechtlichen Normen einhergeht, ist die mögliche Schadenersatzpflicht. Die Höhe des Schadenersatzes bemisst sich anhand des Schadens, welcher durch die Verletzung der Norm verursacht wurde. Bei vertraglichen Verpflichtungen besteht ausserdem das Risiko einer allfälligen Konventionalstrafe.

Die unterlassene Sicherung von IT-Systeme kann eine Pflichtverletzung der Organe einer Kapitalgesellschaft darstellen (Verwaltungsrat der Aktiengesellschaft sowie der Geschäftsführung der GmbH). Die Mitglieder des Aufsichtsorgans unterstehen einer strengen Sorgfaltspflicht und haben die Interessen der Gesellschaft nach Treu und Glauben zu wahren. Im Fall der Delegation der operativen Geschäftsführung sind die beauftragten Personen gehörig zu beaufsichtigen. Eine derartige Pflichtverletzung kann die Haftung der Organe mit ihrem persönlichen Vermögen begründen.

Weitere Rechtsfragen
Im Zusammenhang mit dezentralen Arbeitsweisen und der verstärkten Nutzung von Technologie stellt sich eine Reihe weiterer Rechtsfragen, die über die Kernfragen der Cybersecurity hinausreichen:

- Dürfen die privaten elektronischen Geräte der Mitarbeiter (Laptop, Mobiltelefon) für geschäftliche Zwecke genutzt werden? Was ist zu beachten? Besteht ein Anspruch auf Entschädigung?
- Ist es zulässig, Unterlagen in der «Cloud» abzulegen? Was ist dabei zu beachten? Muss in jedem Fall eine Papierkopie aufbewahrt werden?
- Kann ein Dokument auch ohne eigenhändige Unterschrift rechtsgültig unterzeichnet werden?

Viele Anbieter von Waren und Dienstleistungen erwägen derzeit, ihr Angebot über neue Vertriebswege anzubieten. Eine verbreitete Möglichkeit ist der Vertrieb über das Internet. Bei der Implementierung eines Online-Shops in der Schweiz sind verschiedene rechtliche Vorgaben zu beachten (vgl. eingehend den BianchiSchwald Newsletter zu E-Commerce).

Was ist zu tun?
Die Entwicklung von IT-Systemen erfährt regelmässig grundlegende Veränderungen. Dies führt dazu, dass sich auch die Bedrohungslage äusserst dynamisch entwickelt. Als Folge bedarf der Schutz der IT-Systeme der fortlaufenden Überprüfung. Die Prüfung der rechtlichen Pflichten hinsichtlich der Cybersecurity erlaubt es dem Unternehmen, angemessene Massnahmen zu definieren. Diese rechtliche Analyse der Ausgangsla-

ge ist deshalb ein wichtiger Bestandteil jeder Cybersecurity-Strategie, die in periodischen Abständen auf ihre Aktualität und allfälligen Anpassungsbedarf hin überprüft werden sollte.

Die als Reaktion auf die COVID-19-bedingten Einschränkungen eingeführten dezentralen Arbeitsweisen führen zu zusätzlichem Überprüfungsbedarf bei der Cybersecurity-Strategie. Ausgehend von den konkret getroffenen Massnahmen sollte geprüft werden, ob damit Handlungsbedarf bei der Cybersecurity geschaffen wurde. Als Hilfestellung zur Prüfung können folgende Fragen dienen:

- Wurde im Unternehmen ein neues IT-System eingeführt, welches einen zentralen Prozess betrifft oder das aus sonstigen Gründen eine wichtige Funktion für das Unternehmen wahrnimmt?
- Wurden die Mitarbeiter angemessen in das neue IT-System eingeführt?
- Sind alle Mitarbeiter über die zusätzlichen Risiken für die Sicherheit von IT-Systemen informiert?
- Ist es vorgesehen, die Wirksamkeit des Schutzes der IT-Systeme zu testen?

Darüber hinaus lohnt es sich gerade bei einer krisenbedingten Anpassung des Geschäftsmodells ganz besonders, allfällige rechtliche Herausforderungen frühzeitig zu erkennen und Lösungen zu erarbeiten.

Bei Fragen oder Unklarheiten wenden Sie sich bitte an Ihre Kontaktperson bei BianchiSchwald.

CHRISTOPH GASSER
Rechtsanwalt, Dr. iur.
LL.M. University of Michigan
Nebenamtlicher Richter am Bundespatentgericht
Partner

ADRIAN TRUTMANN
Rechtsanwalt, MLaw
Associate

THIERRY BURNENS
Rechtsanwalt, M.A. HSG
CIPP/E
Associate

BIANCHISCHWALD GMBH
mail@bianchischwald.ch
bianchischwald.ch

GENF
5, rue Jacques-Balmat
Postfach 5839
CH-1211 Genf 11
T +41 58 220 36 00
F +41 58 220 36 01

ZÜRICH
St. Annangasse 9
Postfach 1162
CH-8021 Zürich
T +41 58 220 37 00
F +41 58 220 37 01

LAUSANNE
12, avenue des Toises
Postfach 5410
CH-1002 Lausanne
T +41 58 220 36 70
F +41 58 220 36 71

BERN
Elfenstrasse 19
Postfach 133
CH-3000 Bern 15
T +41 58 220 37 70
F +41 58 220 37 71