RECHTSANWÄLTE

SCHELLENBERG WITTMER

FEBRUAR 2018

Newsletter

Autor:
Roland Mathys

ICT / DATENSCHUTZ

Prävention, Aktion, Reaktion – rechtlicher Umgang mit Cyberrisiken

Mit der zunehmenden Technologisierung der Wirtschaft verschiebt sich auch die Wirtschaftskriminalität immer stärker in die digitale Sphäre. Kaum ein Unternehmen wurde nicht schon Ziel oder gar Opfer eines Cyberangriffs. Das Bewusstsein der Unternehmen für diese neuartige Bedrohungsform nimmt zwar zu; dennoch fehlen oft klare Vorstellungen darüber, was zu deren Abwehr und Bewältigung vorgekehrt werden muss.

1 EINFÜHRUNG

Cyberangriffe haben in der jüngeren Vergangenheit erheblich an Verbreitung und Bedeutung gewonnen. Prominente Einzelfälle wie jener der *Ransomware* "Petya", welche die IT-Systeme zahlreicher Grossunternehmen vorübergehend lahmlegte, haben die Aufmerksamkeit für diese Gefährdungsform geschärft. Cyberangriffe finden aber tagtäglich statt. In Studien gaben fast 90 Prozent der befragten Unternehmen an, in den vergangenen zwölf Monaten von Cyberangriffen betroffen gewesen zu sein.

Cyberangriffe finden auf **nahezu alle Unternehmen** statt, unabhängig von Branche, Grösse oder Jurisdiktion. Der globale Finanzkonzern bleibt davon so wenig verschont wie das lokal tätige KMU. Entsprechend werden Cyberrisiken und -kriminalität heute in zahlreichen Untersuchungen als eine der **grössten Bedrohungen** für Unternehmungen eingestuft. Umso mehr erstaunt, dass Massnahmen zur Abwehr und Bewältigung von Cyberangriffen oft fehlen oder erst am Anfang stehen.

Deutlich zeigt sich dieser **Vollzugsnotstand** etwa bei der Dauer, die zwischen einem erfolgreichen Cyberangriff und dessen Entdeckung verstreicht: In etwa 85 Prozent aller Fälle wird eine erfolgreiche Cyberattacke erst nach fünf Monaten erkannt; durchschnittlich beträgt die Zeit, während der ein Angriff verborgen bleibt, gar etwa 250 Tage und somit rund acht Monate. Während dieser Zeit ist ein betroffenes Unternehmen besonders verletzlich, und die Angreifer können ihr Unwesen weitgehend ungestört treiben.

In diesem Newsletter soll aufgezeigt werden, wie mit Cyberrisiken **aus rechtlicher Sicht** umzugehen ist. Hierbei werden die drei Phasen der Prävention zur Abwehr von Angriffen, der unmittelbaren Aktion im Falle einer (erfolgreichen) Attacke sowie der Reaktion im Nachgang zu einem Angriff unterschieden.

2 PRÄVENTION

2.1 NOTWENDIGKEIT

Am Anfang jeder Verteidigungsstrategie gegenüber Cyberattacken sollte die Prävention stehen, also die Umsetzung von Massnahmen zur Verhinderung, dass Cyberangriffe ihr Ziel erreichen. Solche Massnahmen empfehlen sich nicht nur aus Gründen des Selbstschutzes und der Reputation eines Unternehmens, sondern sind teilweise auch gesetzlich vorgeschrieben und bilden somit Teil der **unternehmerischen Compliance**.

> "In etwa 85 Pozent aller Fälle wird eine erfolgreiche Cyberattacke erst nach fünf Monaten erkannt."

Eine allgemeine und umfassende **Pflicht zur Prävention** vor Cyberrisiken lässt sich den geltenden Gesetzen in der Schweiz nicht ausdrücklich entnehmen. Jedoch kann diese Aufgabe als Teil der Oberleitung der Gesellschaft (Art. 716a OR) und somit als **Pflicht des Verwaltungsrats** verstanden werden. Konkretisiert wird diese Aufgabe etwa durch den *Swiss Code of Best Practice for Corporate Governance* des Wirtschaftsdachverbands *economiesuisse*, wonach der Verwaltungsrat für ein dem Unternehmen angepasstes Risikomanagement und internes Kontrollsystem zu sorgen hat (Grundsatz 20). In der gegenwärtigen Bedrohungslage zählt die Prävention vor Cyberrisiken zu den vom Verwaltungsrat zu treffenden Massnahmen.

Eine Konkretisierung für Personendaten findet sich im **Datenschutzgesetz (DSG)**: Demnach müssen Personendaten durch geeignete technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSG); was das im Einzelnen umfasst, ergibt sich aus der zugehörigen Verordnung (**VDSG**; vgl. Art. 8 ff.). Im Entwurf zum revidierten DSG **(E-DSG)** wird der risikobasierte Ansatz bei der Datensicherheit stärker betont (vgl. Art. 7 E-DSG). Die Botschaft nennt als Beispiel ausdrücklich den Schutz gegen Schadsoftware (BBl 2017 6941 ff., 7031). Auch in der am 25. Mai 2018 in Kraft tretenden EU-Datenschutzgrundverordnung **(DSGVO)** wird die Datensicherheit als Grundsatz statuiert (Art. 32 DSGVO).

Ausdrückliche Vorschriften zur Prävention vor Cyberrisiken finden sich für einzelne Wirtschaftssektoren, insbesondere im **Finanzbereich**. Das Rundschreiben 2008/21 "Operationelle Risiken – Banken" der Eidgenössischen Finanzmarktaufsicht **(FINMA)** schreibt seit 1. Juli 2017 vor, dass die Geschäftsleitung ein Risikomanagement-Konzept für den Umgang mit Cyberrisiken implementieren muss (Grundsatz 4). Dieses Konzept soll mindestens die folgenden Aspekte abdecken:

- Identifikation der spezifischen Bedrohungspotenziale;
- Schutz der Geschäftsprozesse und der Technologieinfrastruktur;
- zeitnahe Erkennung und Aufzeichnung von Cyberattacken;
- Reaktion auf Cyberattacken durch rasche und gezielte Massnahmen;
- Sicherstellung einer zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyberattacken durch geeignete Massnahmen.

Zu den Aufgaben der Geschäftsleitung zählt gemäss Rundschreiben auch, die Wirksamkeit von Konzept und Massnahmen regelmässig durch Verwundbarkeitsanalysen und *Penetration Tests* zu überprüfen.

2.2 MASSNAHMEN

Das Arsenal präventiver Massnahmen zur Abwehr von Cyberrisiken ist gross. Zunächst sollte jedes Unternehmen ein **Cybersicherheits-Programm** aufsetzen. In diesem Programm werden grundlegende Zuständigkeiten geregelt (wie beispielsweise die Bezeichnung eines *Chief Information Security Officer* (CISO)). Die Involvierung des Top Managements ist hierbei zentral. Weiter legt das Programm Sicherheitsrichtlinien und Überwachungssysteme zur raschen Erkennung von Cyberattacken fest; gerade bei den Überwachungssystemen haben in jüngerer Zeit neue Lösungen den Markt erobert, die unter Einsatz von Mechanismen der künstlichen Intelligenz zu verlässlichen Befunden gelangen. Die eingerichteten Prozesse und Systeme sollten regelmässig auf ihre Wirksamkeit hin getestet werden, beispielsweise mittels simulierter Angriffe.

> "Ausdrückliche Vorschriften zur Prävention vor Cyberrisiken finden sich für einzelne Wirtschaftssektoren, insbesondere im Finanzbereich."

Jedes Unternehmen muss sich bewusst sein oder werden, welchen Risiken es ausgesetzt ist. Im Rahmen einer solchen **Risikobeurteilung** wird ein Inventar der sensitiven Daten und Infrastrukturen erstellt. Mögliche Bedrohungen und Angriffspotenziale werden identifiziert, wobei der Faktor Mensch und insbesondere das Potenzial unternehmensinterner Attacken nicht unterschätzt werden dürfen. Im Anschluss daran werden mittels *Gap*-Analyse Lücken und Schwachstellen im gegenwärtigen Schutz- und Abwehrsystem geortet und mit geeigneten technischen und/oder organisatorischen Massnahmen beseitigt. Bei verbleibenden Risiken ist ein Versicherungsschutz zu erwägen (vgl. dazu unten).

Die Risikobeurteilung soll nicht isoliert, sondern unter **Einbezug Dritter** erfolgen. Die Verträge mit Drittanbietern wesentlicher Dienstleistungen (z.B. Datenhosting) müssen gründlich darauf geprüft werden, ob dem Aspekt der Daten- und Informationssicherheit genügend Beachtung geschenkt wird. Anbieter businesskritischer Leistungen sollten einer eigentlichen *Cybersecurity Due Diligence* unterzogen werden.

Ein wesentliches Element der präventiven Massnahmen bildet die **Schulung** der Mitarbeitenden. Damit soll einerseits das Bewusstsein für das Bedrohungspotenzial von

Cyberrisiken geschärft werden; andererseits sollen den Mitarbeitern die wichtigsten Grundsätze zur Abwehr von Cyberattacken sowie zum richtigen Verhalten im Falle eines erfolgreichen Cyberangriffs vermittelt werden, wozu sich beispielsweise *Mock-Trainings* unter realitätsnahen Rahmenbedingungen besonders eignen.

Zu den vorbereitenden Massnahmen zählt schliesslich die Erstellung eines *Cyberincident Response Plan*, der das Vorgehen im Ernstfall schildert (vgl. sogleich).

3 AKTION

Jedes Unternehmen muss für den Fall gewappnet sein, dass eine Cyberattacke trotz präventiver Abwehrmassnahmen zum Ziel gelangt. Neben der **raschen Erkennung** eines erfolgreichen Angriffs steht das **richtige Verhalten im Ernstfall** im Vordergrund. Hierfür müssen die Zuständigkeiten klar geregelt und die Aufgaben definiert und zugeordnet sein.

3.1 TEAM

Im Ernstfall muss das *Incident Response Team* des Unternehmens sofort tätig werden. Dieses Team setzt sich zusammen aus Vertretern der Bereiche IT, Recht/Compliance, HR, Kommunikation, des von der Attacke betroffenen Fachbereichs sowie des Top Managements. Dem Team sollten auch ausgewählte externe Spezialisten (z.B. Cyberforensiker oder Rechtsanwälte) angehören.

3.2 AUFGABEN

Zu den Aufgaben des Teams zählen zunächst die Abschätzung der **Dimension des Cybervorfalls** sowie die **Ergreifung von Sofortmassnahmen** zur **Schadensminimierung** (z.B. Trennung aller Endgeräte vom Netz, um die Verbreitung von Schadsoftware zu verhindern). Sodann muss die *Business Continuity* notfallmässig und kurzfristig sichergestellt werden. Mittel- bis langfristig muss die Rückkehr zum ordentlichen Geschäftsbetrieb geplant und aufgesetzt werden.

Weiter muss das *Incident Response Team* prüfen, ob und wie der Vorfall intern und extern **kommuniziert** wird und ob behördliche Notifikationen notwendig sind (vgl. dazu sogleich). Auch stellt sich die Frage, in welchem Umfang eine **interne Untersuchung** des Vorfalls angestossen werden soll und ob weitere Schritte (z.B. Strafanzeige oder disziplinarische Massnahmen) geboten sind. Schliesslich sollte sich das Team mit der Frage auseinandersetzen, wie vergleichbare Vorfälle künftig verhindert werden können.

> "Neben der raschen Erkennung eines erfolgreichen Cyberangriffs steht das richtige Verhalten im Ernstfall im Vordergrund."

4 REAKTION

4.1 NOTIFIKATION

Nach Eintritt einer erfolgreichen Cyberattacke muss zeitnah geklärt werden, ob und wem der Vorfall gemeldet werden muss. Eine solche Notifikationspflicht kann sich zunächst aus dem **Datenschutzrecht** ergeben. Das geltende DSG statuiert keine ausdrückliche Pflicht, sicherheitsrelevante Vorfälle zu melden. Demgegenüber sieht der Entwurf zum revidierten DSG vor, dass unter gewissen Voraussetzungen der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte und allenfalls auch die betroffenen Personen über einen Cybervorfall "so rasch als möglich" informiert werden müssen (Art. 22 E-DSG). Analoges gilt unter der EU-Datenschutzgrundverordnung (vgl. Art. 33 f. DSGVO). Für einzelne Branchen bestehen überdies **Meldepflichten aufgrund von Spezialgesetzen** (z.B. für Fernmeldedienstanbieter, für Finanzmarktbeaufsichtigte oder im Gesundheitsbereich).

Eine Pflicht zur Bekanntgabe eines Cybervorfalls kann sich bei börsenkotierten Unternehmen auch aus den Vorschriften zur ***ad hoc* Publizität** ergeben. Demnach sind alle Informationen offenzulegen, die geeignet sind, den Aktienkurs eines Unternehmens erheblich zu beeinflussen. Auch dort, wo keine gesetzliche Notifikationspflicht besteht, kann sich eine Bekanntgabe empfehlen, beispielsweise aus Reputationsgründen, im Sinne einer *Best Practice* oder zur Minimierung potenzieller Schäden.

4.2 RECHTLICHE AUFARBEITUNG

Nach dem Eintritt eines Cybervorfalls muss das Unternehmen prüfen, welche rechtlichen Schritte gegen die Urheber des Angriffs ergriffen werden sollen. Hierbei stehen zivil- und strafrechtliche Massnahmen sowie einzelne Spezialbehelfe zur Verfügung.

Zivilrechtlich können Anspruchsgrundlagen für Unterlassungs-, Beseitigungs- oder Schadenersatzansprüche einerseits aus Vertragsverletzungen (z.B. von Kunden oder Lieferanten) oder aus unerlaubten Handlungen abgeleitet werden; hierbei liegt die Widerrechtlichkeit meist in der Begehung einer Straftat, einer Marken- oder Urheberrechtsverletzung, einer Persönlichkeits- oder Datenschutzverletzung oder in unlauterem Wettbewerb begründet. **Strafrechtlich** umfasst das Spektrum einerseits die spezifischen Cyberdelikte (z.B. Hacking, Datendiebstahl oder -beschädigung, Computerbetrug) und andererseits die "klassischen" Straftatbestände (z.B. Betrug, Erpressung, Nötigung, Urkunden- oder Geheimnisdelikte), oft auch in Kombination.

Mit der seit 1. November 2017 revidierten Verordnung über Internet-Domains **(VID)** wurde ein neues Instrument geschaffen, um **Domainnamen rechtswidriger Webseiten zu sperren**. Die Regelung findet Anwendung auf Webseiten der *Top-Level Domains* .ch und .swiss, über die *Phishing* betrieben oder Schadsoftware verbreitet wird oder die solche Handlungen unterstützen.

Weiter besteht die Möglichkeit, Cybervorfälle jeglicher Art der Melde- und Analysestelle Informationssicherung MELANI (www.melani.admin.ch) oder der nationalen Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK (www.kobik.ch) zu melden. Aufgrund der grossen Zahl von Meldungen und der beschränkten Ressourcen wird es diesen Institutionen jedoch oft nicht möglich sein, gemeldete Vorfälle im Detail zu untersuchen.

Wie dargelegt steht zwar ein grosses Arsenal an rechtlichen Massnahmen zur Verfügung; jedoch lassen die inhärenten Umstände und besonderen Herausforderungen der Cyberkriminalität, insbesondere die Anonymität und Virtualität der Täterschaft, die internationale Dimension und der Faktor Zeit, die Durchsetzung dieser Massnahmen oft als wenig erfolgversprechend erscheinen.

4.3 VERSICHERUNG

Auch bei umfassenden Präventionsmassnahmen kann der Eintritt eines Cybervorfalls nicht gänzlich ausgeschlossen werden, womit sich die Frage nach der Versicherbarkeit von Cyberrisiken stellt. Der **Markt für Cyberversicherungen** ist in der Schweiz noch relativ jung, aber im Wachstum begriffen. Die bisher verfügbaren Versicherungsmodelle decken Drittschäden (z.B. Haftpflichtfälle) und/oder "Eigenschäden" des betroffenen Unternehmens (z.B. Kosten für Krisenmanagement, Kosten zur Datenwiederherstellung oder Folgen eines Betriebsunterbruchs) ab.

Bei Cyberversicherungen sollte im Einzelnen **geprüft** werden, welche Risiken abgedeckt sind, welche Sorgfaltspflichten auf Seiten des Versicherungsnehmers vorausgesetzt werden (insbesondere präventive technische und organisatorische Massnahmen) und welche Obliegenheiten den Versicherungsnehmer im Schadensfall treffen (z.B. Anzeige- oder Notifikationspflichten).

5 AUSBLICK UND FAZIT

In der Schweiz können derzeit zahlreiche **politische Vorstösse** im Bereich Cyberkriminalität beobachtet werden. Diese reichen von der Schaffung spezifischer Kompetenzzentren und zentraler Anlauf- und Koordinationsstellen bis hin zur Einführung neuer Meldepflichten (z.B. für Betreiber kritischer Infrastrukturen). Der Handlungsbedarf wurde somit auch bei Gesetzgeber und Behörden erkannt.

Bei den Unternehmen in der Schweiz kann eine erhöhte Sensibilisierung für Cyberrisiken konstatiert werden. Jedoch **hapert es oft noch bei der Umsetzung** entsprechender Massnahmen. Der proaktive Umgang mit Cyberrisiken bildet je länger je mehr einen zentralen Pfeiler der Governance und Compliance jedes Unternehmens.

Kontakte

Der Inhalt dieses Newsletter stellt keine Rechts- oder Steuerauskunft dar und darf nicht als solche verwendet werden. Sollten Sie eine auf Ihre persönlichen Umstände bezogene Beratung wünschen, wenden Sie sich bitte an Ihre Kontaktperson bei Schellenberg Wittmer oder an eine der folgenden Personen:

In Zürich:

Roland Mathys
Partner
roland.mathys@swlegal.ch

Peter Burckhardt
Partner
peter.burckhardt@swlegal.ch

In Genf:

Benjamin Borsodi
Partner
benjamin.borsodi@swlegal.ch

Louis Burrus
Partner
louis.burrus@swlegal.ch

SCHELLENBERG WITTMER AG / Rechtsanwälte

ZÜRICH / Löwenstrasse 19 / Postfach 2201 / 8021 Zürich / Schweiz / T +41 44 215 5252

GENF / 15bis, rue des Alpes / Postfach 2088 / 1211 Genf 1 / Schweiz / T +41 22 707 8000

SINGAPUR / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapur 049909 / www.swlegal.sg

www.swlegal.ch