Monthly
Newsletter
March 2023

IT Security and Cybercrime

Schellenberg Wittmer

Cybersicherheit – Zehn rechtliche Gebote zur Prävention

Roland Mathys

Key Take-aways

1.
Im Rahmen der Cyberprävention sind neben technischen und organisatorischen auch rechtliche Aspekte zu berücksichtigen. Dies wird heute noch zu wenig getan.

2.
Die wichtigsten rechtlichen Handlungsanweisungen lassen sich in zehn Punkten zusammenfassen und mit vertretbarem Aufwand umsetzen.

3.
Werden die präventiven rechtlichen Massnahmen vernachlässigt, riskiert ein Unternehmen vielseitige Nachteile von Vertragsverletzungen bis hin zu Sanktionen.

Einleitung

Cyberkriminalität ist in aller Munde. Es vergeht kaum ein Tag, an dem nicht ein grösseres Unternehmen oder eine Behörde Opfer einer Cyberattacke wird. Cyberangriffe werden heute als eines der **grössten Risiken aus Unternehmenssicht** wahrgenommen. Mit der ständig wachsenden Bedrohung durch Cyberattacken hat auch das Bewusstsein für präventive Massnahmen stark zugenommen. Dabei stehen technische und organisatorische Schritte im Vordergrund. **Rechtliche Massnahmen** im Umfeld der Cyberprävention werden demgegenüber **noch kaum getroffen** – zu Unrecht, denn auch hier bleibt viel zu tun, um für den Fall eines Cyberangriffs gewappnet zu sein. Im Folgenden werden die wichtigsten präventiven Empfehlungen aus rechtlicher Sicht im Sinne von zehn Handlungsgeboten zusammengefasst.

Der vertraglichen Dimension von Cybervorfällen wird kaum Beachtung geschenkt.

1 Informationssicherheit

Informationssicherheit wird primär als technisches Thema verstanden, hat aber auch eine rechtliche Dimension. Gemäss der EU-Datenschutzgrundverordnung (**DSGVO**) müssen angemessene technische und organisatorische Massnahmen zur **Gewährleistung der Datensicherheit** getroffen werden, ansonsten empfindliche Bussen in Millionenhöhe drohen. Auch unter dem künftigen Schweizer Datenschutzgesetz (**DSG**) wird die Nichteinhaltung von Mindestanforderungen an die Datensicherheit unter Strafe gestellt und mit Busse bis CHF 250'000 sanktioniert.

Ungenügende Informationssicherheit kann überdies zu einer Verletzung **strafrechtlich geschützter Geheimnisse** (z.B. Arztgeheimnis) führen und bei (Eventual-)Vorsatz sowie im Falle des Bankkundengeheimnisses sogar bei Fahrlässigkeit bestraft werden. Rechtliche Pflichten zur Gewährleistung der Informationssicherheit finden sich weiter in sektorspezifischen Regelungen (z.B. Finanzindustrie) sowie – speziell an Gesellschaftsorgane gerichtet – im *Swiss Code of Best Practice for Corporate Governance*.

2 Cyber Emergency Response Team

Ein Unternehmen sollte über ein Notfallteam verfügen, das bei einem Cybervorfall tätig werden und die notwendigen Massnahmen ergreifen kann. Ein solches Cyber Emergency Response Team (**CERT**) muss **im Vorfeld gebildet und instruiert** werden; hat sich der Cybervorfall bereits zugetragen, bleibt hierfür keine Zeit.

Das CERT muss sich aus den **richtigen Funktionen und Personen** zusammensetzen, damit es im Krisenfall gut funktioniert. Neben den Fachbereichen sollten Vertreter aus der Informationssicherheit, aus dem Kommunikationsbereich sowie von Legal/Compliance im CERT vertreten sein. Auch das Management eines Unternehmens muss in das CERT eingebunden werden. Je nach Grösse und Organisation eines Unternehmens sollten neben internen Spezialisten auch externe Dienstleister beigezogen werden (vgl. unten).

Die **Rolle der Juristen** im CERT besteht darin, bei einem Cybervorfall alle notwendigen rechtlichen Schritte zeitnah und in der richtigen Abfolge in die Wege zu leiten. Dazu zählen die Kontaktierung der Cyberversicherung (vgl. unten), die Meldung von Datenschutzverletzungen an Behörden und betroffene Personen, die Einleitung einer internen Untersuchung, die Einreichung einer Strafanzeige oder die Vorbereitung der Abwehr von Drittansprüchen.

3 Externe Spezialisten

Externe Dienstleister wie Sicherheitsfachleute, IT Forensiker, "Verhandler" bei Lösegeldforderungen und Anwälte sollten frühzeitig an Bord geholt werden. Mit diesen Dienstleistern sollten **Mandatsvereinbarungen** getroffen und Prüfungen auf Interessenkonflikte vorgenommen werden. Beginnt ein Unternehmen hiermit erst nach Eintritt eines Cybervorfalls, geht wertvolle Zeit verloren; zudem befindet sich das Unternehmen in einer ungünstigen Verhandlungsposition.

Für alle Dienstleister sind die **Kontaktstellen und -wege** festzulegen (je nach Bedarf inkl. Pikettverfügbarkeit). Weiter sollten die Dienstleister mit den spezifischen Gegegebenheiten eines Unternehmens sowie den massgeblichen Prozessen (vgl. unten) vertraut gemacht werden, um im Notfall rasch einsatzfähig zu sein.

4 Prozesse, Richtlinien und Vorlagen

Als Teil der Vorbereitung auf einen Cybervorfall sollten relevante Prozesse dokumentiert und Richtlinien erstellt sein. Dies gilt namentlich für das **Vorgehen bei Meldung einer Datenschutzverletzung**, die innert kurzer Frist nach Kenntnis eines Vorfalls und dessen Tragweite erfolgen muss. Wichtig sind weiter sicherheitsrelevante Richtlinien, z.B. Anweisungen an Mitarbeitende zum Umgang mit Cyberrisiken. Zudem sollten Vorlagen für die interne und externe Kommunikation vorbereitet werden, die im Bedarfsfalle rasch an die spezifischen Umstände des eingetretenen Cybervorfalls angepasst werden können.

Die einmal erstellte Dokumentation ist **laufend zu prüfen und aktualisieren**, beispielsweise wenn neue Bedrohungsszenarien aufkommen, Änderungen an der IT-Infrastruktur vorgenommen werden oder neue gesetzliche Vorgaben einzuhalten sind. Die erwähnten Unterlagen dienen einerseits dazu, bei einem Cybervorfall rasch, planmässig und zielgerichtet agieren zu können und damit die Auswirkungen des Vorfalls zu minimieren. Andererseits verfolgt die Dokumentation den Zweck, die Einhaltung von Mindestanforderungen an die Datensicherheit und die Umsetzung diesbezüglicher Massnahmen nachweisen zu können.

5 Compliance

Unternehmen, die bei Datenschutzbehörden **nicht im Fokus** stehen, vernachlässigen zuweilen die Datenschutz-Compliance. Dies kann sich bei Eintritt eines Cybervorfalls aber rasch ändern, wenn ein Unternehmen plötzlich im Scheinwerferlicht der Behörden erscheint. Stellt sich dann heraus, dass das betroffene Unternehmen Datenschutzvorgaben nicht gesetzeskonform umgesetzt hat, droht weiteres Ungemach.

Beispielhaft sei der Fall eines Unternehmens angeführt, das aufgrund einer Verletzung der Datensicherheit eine Meldung an die Datenschutzbehörde in einem EU-Mitgliedstaat vornahm. Bei der Aufarbeitung dieser Meldung ergab sich, dass auch die Datenschutzhinweise auf der Website angepasst, ein EU-Vertreter bestellt und ein Verzeichnis von Verarbeitungstätigkeiten erstellt werden mussten.

6 Behörden

Neben der Einbindung externer Experten in das CERT sollten auch Kontakte zu den bei einem Cybervorfall zuständigen Behörden aufgebaut und gepflegt werden. Hierzu zählen namentlich **Datenschutz-, Straf- und weitere Aufsichtsbehörden** (z.B. im Finanzbereich).

Zunächst muss das Unternehmen sondieren, welche Behörden **örtlich und sachlich zuständig** sind. Kann ein Unternehmen an verschiedene Stellen gelangen, fragt sich, welche Behörde über die grösste Sachkompetenz und Erfahrung im Umgang mit Cybervorfällen verfügt; bei Strafbehörden trifft dies regelmässig für Behörden jener Kantone zu, die eigene Dezernate für Cyberkriminalität gebildet haben. Innerhalb der zuständigen Behörde sollten auch die massgeblichen **Ansprechpersonen** mitsamt Kontaktmöglichkeiten in Erfahrung gebracht werden, um einen möglichst direkten Zugang zu gewährleisten.

Weiter empfiehlt sich, mit den Behördenvertretern im Rahmen der Cyberprävention den **Austausch** zu suchen. Dies erlaubt den Behörden, mehr über das Unternehmen zu erfahren und abzuschätzen, wie kritisch ein Cyberangriff ausfallen kann. Teils besprechen Unternehmen (z.B. Betreiber kritischer Infrastrukturen) die Abläufe, nach denen bei einem Cybervorfall gehandelt wird, mit den Behörden vor. Nach unserer Erfahrung zeigen sich Behörden einem solchen Austausch gegenüber meist aufgeschlossen und kooperativ.

7 Verträge

Cybersicherheit bildet direkt oder indirekt immer häufiger Gegenstand vertraglicher Vereinbarungen. Die Verträge mit den wichtigsten Geschäftspartnern sollten im Hinblick auf **Bestimmungen rund um die Cybersicherheit** geprüft werden, um Vertragsverletzungen zu vermeiden.

Diese Prüfung sollte klären, ob ein Vertrag **Mindestvorgaben** an die Cybersicherheit vorschreibt, und ob das eigene Unternehmen diese einhält. Weiter sollte im Vorfeld Klarheit darüber bestehen, ob ein Cybervorfall (evtl. abhängig von der Schwere) eine **Vertragsverletzung** darstellt, und welche Rechtsfolgen daran gekoppelt sind. Wichtig ist auch die Kenntnis darüber, ob (und innert welcher Frist) der Vertragspartner über einen Cybervorfall zu **informieren** ist.

All diese Erkenntnisse sollten in einem **Inventar** festgehalten werden, das regelmässig aktualisiert wird und auch *offline* (z.B. in Papierform) griffbereit ist. Vorfälle, bei denen der Zugriff auf solche Unterlagen genau daran scheiterte, dass diese im Zuge einer Attacke mit Ransomware verschlüsselt wurden, entbehren nicht einer gewissen Ironie, treten in der Praxis aber leider auf.

Eine Cyberversicherung kann ein Restrisiko decken, ist aber kein Allheilmittel.

8 Lieferketten und Dienstleister

Häufig besteht eine **Sicherheitslücke** nicht beim angegriffenen Unternehmen selbst, sondern in dessen Lieferkette bzw. bei einem (IT-)Dienstleister (z.B. Cloud-Provider oder Softwarelieferant). In Bezug auf geschäftskritische Dritte muss deshalb neben der technischen eine vertragliche *Due Diligence* stattfinden.

Im Rahmen der **vertraglichen Due Diligence** ist der Vertrag mit dem Dritten insbesondere auf folgende Themen hin zu analysieren: Sicherheitsstandards und -massnahmen, Zertifizierungen, Audit-Rechte, Verwundbarkeitstests, Sorgfaltsmassstab, vertragliche Zusicherungen und Garantien, Informationspflicht (z.B. Einsicht in den forensischen Bericht), Unterstützungspflicht bei Cybervorfällen und Entgeltlichkeit, Rechtsbehelfe (z.B. Haftung, ausserordentliche Kündigung), Versicherungsdeckung und andere Sicherheiten.

Wenn der Vertrag in diesen Punkten **keine ausreichenden Regelungen** enthält, wird eine (Neu-)Verhandlung empfohlen. Führt dies nicht zu einer Besserung, sollte auch die Vertragsbeendigung (bzw. der Verzicht auf den Vertragsschluss) kein Tabu darstellen.

9 Training und Bewusstseinsbildung

Der Faktor Mensch bildet eines der häufigsten Einfallstore für Cyberangriffe, sei es über Phishing-Attacken, vireninfizierte Dateianhänge oder ausgeklügeltes *Social Engineering*. Entsprechend bedeutsam ist es, das Bewusstsein über Cyberattacken zu schärfen, typische Angriffsmuster aufzuzeigen und die richtige Verhaltensweise zu schulen. Solche **Trainings** müssen regelmässig und angesichts des technischen Fortschritts mit jeweils aktualisiertem Inhalt stattfinden.

Schulungen zählen zu den **organisatorischen Massnahmen** zur Gewährleistung der Informationssicherheit. Deren Vernachlässigung ist datenschutzrechtlich somit als Verletzung der Datensicherheit mit entsprechenden Konsequenzen einzustufen.

10 Versicherung

Trotz aller präventiven Massnahmen verbleibt ein **Restrisiko**; hier bietet eine (Cyber)versicherung allenfalls Deckung. Keinesfalls sollte man sich aber nur auf die Versicherung verlassen und die zuvor geschilderten präventiven Massnahmen vernachlässigen.

Zunächst fragt sich, ob und unter welchen Voraussetzungen Cybervorfälle überhaupt vom Versicherungsschutz erfasst werden. Regelmässig verlangen die Versicherungsunternehmen den Nachweis eines **technischen Mindestschutzniveaus**. Zu prüfen ist sodann, welche **Schadensarten** (z.B. Lösegeldzahlungen, indirekte Schäden infolge Betriebsunterbruch, Aufwände im Zusammenhang mit der Einreichung einer Strafanzeige) gedeckt sind.

Auch sollte sich ein Unternehmen bereits im Voraus kundig machen, welche **Obliegenheiten im Schadensfall** zu beachten sind. Hierzu zählen neben der Schadensanzeige typischerweise Dokumentationspflichten, Massnahmen zur Schadensminderung oder die Zusammenarbeit mit vorgegebenen externen Dienstleistern.

Schliesslich empfiehlt sich, verschiedene Anbieter von Cyberversicherungen einem Vergleich und **Benchmarking** hinsichtlich zentraler Leistungsmerkmale zu unterziehen. Beträchtliche Unterschiede bestehen etwa in der Zeitdauer bis zur Kostengutsprache, die nach unserer Erfahrung von weniger als einer Stunde bis hin zu mehreren Tagen reichen kann.

Fazit

Neben technischen sind auch rechtliche Massnahmen im Rahmen der Cyberprävention von fundamentaler Bedeutung. Die meisten dieser Vorkehrungen stellen keine *Rocket Science* dar und lassen sich mit überschaubarem Aufwand umsetzen. Umso wichtiger ist, diesen Aspekten gebührend Beachtung zu schenken.

Roland Mathys
Partner Zürich
roland.mathys@swlegal.ch

Peter Burckhardt
Partner Zürich
peter.burckhardt@swlegal.ch

Louis Burrus
Partner Genf
louis.burrus@swlegal.ch

Clara Poglia
Partnerin Genf
clara.poglia@swlegal.ch

Schellenberg Wittmer AG
Rechtsanwälte

Zürich
Löwenstrasse 19
Postfach 2201
8021 Zürich / Schweiz
T +41 44 215 5252
www.swlegal.ch

Genf
15bis, rue des Alpes
Postfach 2088
1211 Genf 1 / Schweiz
T +41 22 707 8000
www.swlegal.ch

Singapur
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapur 049909
T +65 6580 2240
www.swlegal.sg