RECHTSANWÄLTE

SCHELLENBERG WITTMER

FEBRUAR 2019

Newsletter

Autoren:
Roland Mathys, LL.M. (LSE)
Andreas Hösli, LL.M.

ICT / WHITE-COLLAR CRIME AND COMPLIANCE

Reaktion auf Cyberattacken – Was ist zu tun?

Die Risiken durch gezielte Cyberangriffe auf Unternehmen sowie deren Top-Management nehmen laufend zu. Während das Gefahrenpotenzial vermehrt erkannt wird, herrscht bei Unternehmen häufig Unsicherheit über den konkreten Handlungsbedarf und insbesondere darüber, ob im Ernstfall die Behörden (insbesondere spezialisierte Cyber-Strafverfolgungsbehörden oder die Meldestelle MELANI) einzuschalten sind.

1 CYBERATTACKEN ALS EXISTENZIELLES RISIKO

Beinahe täglich ist in der Presse von **Cyberangriffen** zu lesen. Längst ist Cyberkriminalität zu einem attraktiven Businessmodell für immer professioneller agierende Täter geworden, die oft **gezielt Unternehmen** sowie deren **Top-Management** ins Visier nehmen.

Publik gewordene Vorfälle wie die schwere Beeinträchtigung oder gar vorübergehende Lahmlegung der IT-Infrastruktur zahlreicher Unternehmen sowie öffentlicher Einrichtungen wie Spitäler durch Verschlüsselungssoftware (Stichwort *NotPetya*) haben das **Bewusstsein** für die Problematik auf Managementstufe erhöht, wenngleich es bei der Umsetzung konkreter Massnahmen teilweise hapert. Nebst massiven **finanziellen Einbussen** (teilweise im dreistelligen Millionenbereich) wie auch **Reputationsschäden** für die betroffenen Unternehmen können Angriffe auf kritische Infrastrukturen schwerwiegende gesellschaftliche Folgen haben. Sodann bestehen berechtigte Sorgen aufgrund möglicher **Bussen** bei Datenabflüssen (EU Datenschutzgrundverordnung, **DSGVO**). Deshalb stellen Cybergefahren für Unternehmen **operationelle Risiken** dar, die im Falle der Realisierung existenzbedrohende Ausmasse annehmen können und daher durch entsprechendes Risikomanagement zu adressieren sind. Die Dimension der Schadensszenarien macht deutlich, dass es sich hierbei um eine **Managementaufgabe** handelt.

2 KREATIVE ANGREIFER

Die **Angriffsmethoden** sind vielfältig und nutzen insbesondere IT-Sicherheitslücken (in Soft- oder Hardware), ungenügende Passwörter sowie die "Schwachstelle Mensch" aus. Ferner bietet die oftmals geringe IT-Sicherheit bei mit dem Internet verbundenen Gegenständen (*Internet of Things*, z.B. Sicherheitskameras) erhebliche Angriffsflächen. Gängige Vorgehensweisen sind *Distribu-*

ted Denial of Service (DDoS) Attacken (Überschwemmung eines Systems mit sehr grossen Datenmengen zwecks Überlastung und zeitweiser Lahmlegung desselben) oder *Phishing* (betrügerisches Erschleichen vertraulicher Daten, z.B. mittels fingierter E-Mails). Das Erwirken nicht autorisierter Zahlungen (vermeintlich auf Anweisung der Geschäftsleitung) ist als CEO-Betrug bekannt geworden. In jüngerer Zeit vermehrt zu beobachten sind erpresserische Forderungen etwa in Form von *Ransomware*-Attacken, wobei mittels Schadsoftware fremde Daten oder ganze Systeme verschlüsselt werden und für die Entschlüsselung ein Lösegeld (z.B. in Form einer Kryptowährung wie *Bitcoin*) verlangt wird.

"Cyberattacken nehmen oft gezielt Unternehmen sowie deren Top-Management ins Visier."

Wie in unserem **Newsletter vom Februar 2018** skizziert kommt im rechtlichen Umgang mit Cyberrisiken der **Prävention**, der **Aktion** sowie der **Reaktion** zentrale Bedeutung zu. Gerade beim praktischen Umgang mit dem letzten Aspekt besteht indes in vielen Unternehmen eine erhebliche Unsicherheit. Insbesondere stellt sich bei Eintritt eines Cybervorfalls oft die Frage, ob eine Meldung an Behörden angezeigt bzw. sinnvoll ist, und an wen man sich am besten wendet.

3 GENERELL KEINE MELDEPFLICHT

Bei Eintritt eines bedeutsamen Cybervorfalls ist das (idealerweise bestehende) *Computer Security Incident/Emergency Response Teams* (CSIRT/CERT) des Unternehmens für die Ergreifung der notwendigen Sofortmassnahmen zur Schadensminderung und Wiederherstellung des ordentlichen Geschäftsganges zuständig.

Abgesehen von allfälligen *ad hoc* Meldepflichten börsenkotierter Unternehmen sowie Notifikationspflichten für bestimmte Branchen aufgrund von Spezialgesetzen (z.B. für regulierte Finanzinstitute, Fernmeldedienstanbieter oder im Gesundheitsbereich tätige Unternehmen) besteht bei einer Cyberattacke derzeit grundsätzlich **keine Meldepflicht** an eine Schweizer Behörde. Hingegen kann eine solche Notifikationspflicht bei mit einem Cybervorfall einhergehenden **Datenschutzverletzungen** unter der DSGVO gelten, was auch für das derzeit in Revision befindliche schweizerische Datenschutzgesetz (**DSG**) geplant ist.

4 MELDUNG AN MELANI

Cybervorfälle können der Melde- und Analysestelle Informationssicherung des Bundes (**MELANI**) per Meldeformular mitgeteilt werden (www.melani.admin.ch). Dies kann auch anonym geschehen, was MELANI allerdings eine Antwort verunmöglicht. Solche Meldungen – jährlich rund 8'000 – tragen dazu bei, dass MELANI über ein gut informiertes Lagebild betreffend Cyberangriffe in der Schweiz verfügt. Zudem betreibt MELANI eine Plattform, über die **Phishing-Aktivitäten** gemeldet werden können (www.antiphishing.ch), was regelmässig zur zeitnahen Deaktivierung von Phishing-Websites in der Schweiz führt. Unabhängig von MELANI bietet Art. 15 der Verordnung über Internet-Domains (**VID**) bei Missbrauchsverdacht (insbesondere *Phishing* und Verbreitung von *Malware*) die Möglichkeit der Blockierung von Domain-Namen via Registerbetreiberin (SWITCH).

Der Auftrag von MELANI besteht primär im Schutz und in der Unterstützung ausgewählter **Betreiber kritischer Infrastrukturen** (u.a. aus den Bereichen Finanz, Energie, Telekommunikation, Gesundheit). Diesem beschränkten Teilnehmerkreis bietet MELANI Unterstützung bei der Bewältigung von Cybervorfällen, insbesondere durch technische Analysen des MELANI zugehörigen **GovCERT** (CERT des Bundes). Zudem ermöglicht MELANI den vertraulichen Austausch mit anderen Betreibern kritischer Infrastrukturen. Sonstigen Betroffenen (etwa Privaten und KMU, die keine kritischen Infrastrukturen betreiben) stehen die Dienstleistungen von MELANI grundsätzlich nicht (oder nur auf einer *Best-Effort* Basis) zur Verfügung (der Aufgabenbereich von MELANI soll in Zukunft erweitert werden, vgl. hierzu "Ausblick" unten). Auch nimmt MELANI keine eigentlichen Ermittlungshandlungen vor; hierfür sind die Strafverfolgungsbehörden zuständig.

5 EINSCHALTUNG DER STRAFBEHÖRDEN

5.1 STRAFVERFOLGUNG 2.0

Strafverfolgung im digitalen Raum stellt die Behörden vor grosse und neuartige Herausforderungen. Die Täterschaft handelt hochprofessionell, häufig aus dem Ausland und oft im sogenannten *Darknet*. Zudem stellen sich zahlreiche **neue rechtliche Fragen**, die höchstrichterlicher Klärung harren, z.B. im Zusammenhang mit der Beschlagnahmefähigkeit von Daten.

"Besondere Cyber-Strafverfolgungsbehörden verfügen über spezifisches Know-How."

Um der zunehmenden Verlagerung der Kriminalität in den digitalen Raum gerecht zu werden, bestehen in zahlreichen Kantonen wie auch beim Bund **spezielle Cyber-Einheiten**, die spezifisch mit der Untersuchung von Cyberstraftaten beauftragt sind. Der Kanton Zürich verfügt bereits seit 2013 über ein eigenes **Kompetenzzentrum Cybercrime** mit Spezialisten aus Staatsanwaltschaft und Polizei. Dieses weist beachtliche Ermittlungserfolge vor, wie z.B. die Restitution entwendeter Bitcoins an Geschädigte in mehreren Fällen. Im Jahr 2017 wurden 240 Verfahren abgeschlossen, davon 23% per Strafbefehl, 10% mit Anklage und 67% mit Einstellung oder Sistierung.

Die **Bundesanwaltschaft** führt in ihrem Zuständigkeitsbereich mehrere komplexe Verfahren im Zusammenhang mit Cyberkriminalität. Die Bundeskriminalpolizei verfügt über eine eigene Abteilung IT-Forensik/Cybercrime. Ferner betreibt das Bundesamt für Polizei (**Fedpol**) eine Plattform, auf der verdächtige Cybervorfälle gemeldet werden können (www.cybercrime.admin.ch).

5.2 STRAFANZEIGE

Bei schwerwiegenden Cyberangriffen ist zu erwägen, ob zusätzlich zur eigenen Aufarbeitung des Vorfalls (z.B. im Rahmen einer internen Untersuchung) sowie einer allfälligen Meldung an MELANI die Einschaltung der **Strafverfolgungsbehörden** angezeigt ist.

Während das betroffene Unternehmen (bzw. dessen CSIRT/CERT) sich insbesondere auf die Abwehr eines (möglicherweise andauernden) Cyberangriffs und die Wiederherstellung des ordentlichen Geschäftsgangs fokussiert, besteht

die primäre Aufgabe der Strafverfolgungsbehörden in der **Beweissicherung** sowie der **Lokalisierung und Identifizierung** der mutmasslichen Täterschaft. Dies kann im Hinblick auf die **Restituierung** allfällig entwendeter Vermögenswerte sehr hilfreich sein.

Bei den Ermittlungen wird häufig von **geheimen Überwachungsmassnahmen** (vgl. Art. 269 ff. Strafprozessordnung, StPO; Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BÜPF) Gebrauch gemacht. Zu denken ist etwa an die Erhebung noch nicht abgerufener E-Mails auf dem Server des Providers im Sinne einer Echtzeitüberwachung.

> "Eine spezifische Meldepflicht für Cybervorfälle besteht in den meisten Fällen nicht."

Die Erfolgschancen einer Strafuntersuchung sind im Regelfall erheblich höher, wenn Cyberattacken **sehr zeitnah** zur Anzeige gebracht werden. Die besonderen Cyber-Staatsanwaltschaften sind darauf spezialisiert, im Ernstfall umgehend Ermittlungen aufzunehmen. Dabei arbeiten sie im Idealfall eng mit den IT-Spezialisten des betroffenen Unternehmens zusammen. Regelmässig hilfreiche **Beweismittel** sind unter anderem die in den Cybervorfall involvierten IP-Adressen und URLs, Randdaten oder Logfiles.

Obwohl verlässliche Statistiken fehlen, ist bei Cyberangriffen auf Unternehmen von einer **hohen Dunkelziffer** auszugehen. Einerseits wird nicht jeder Angriff identifiziert; andererseits sind viele Unternehmen gerade im Hinblick auf **mögliche Reputationsschäden** zurückhaltend, Vorfälle den Behörden zur Kenntnis zu bringen. Kommt es infolge einer Strafuntersuchung zu einer Gerichtsverhandlung, ist diese grundsätzlich öffentlich, wodurch allenfalls sensitive Informationen des betroffenen Unternehmens publik werden können. Zudem handelt es sich bei den in Frage kommenden Straftatbeständen - wie z.B. den Computerstraftatbeständen (Art. 143, 143bis, 144bis, 147 und 150 Strafgesetzbuch, StGB), Betrug (Art. 146 StGB), Erpressung (Art. 156 StGB), oder wirtschaftlicher Nachrichtendienst (Art. 273 StGB) - teilweise um grundsätzlich unabhängig vom Willen des Anzeigeerstatters zu untersuchende Offizialdelikte. Sodann haben Unternehmen verständlicherweise eine gewisse Zurückhaltung, sensitive Informationen (etwa betreffend die eigene IT-Infrastruktur) mit Aussenstehenden zu teilen. Diesen Bedenken kann entgegengewirkt werden, indem nach Möglichkeit das **informelle Vorgespräch** mit der Staatsanwaltschaft gesucht wird. In diesem Rahmen ist etwa die Bereitschaft der Staatsanwaltschaft abzuklären, einer allfälligen späteren Desinteresse-Erklärung des anzeigeerstattenden Unternehmens zu entsprechen. Ferner ist unter Umständen die Beschränkung des Akteneinsichtsrechts zum Schutz privater Geheimhaltungsinteressen des Unternehmens (Art. 108 StPO) zu erwägen.

5.3 RECHTSHILFE 2.0

Bedingt durch die transnational operierende Täterschaft hängen die Erfolgsaussichten von Strafuntersuchungen oft wesentlich vom Funktionieren der **Rechtshilfe** mit anderen Ländern ab. Hierzu liegen je nach Staat stark unterschiedliche Erfahrungswerte vor.

In diesem Zusammenhang ist namentlich das für die Schweiz am 1. Januar 2012 in Kraft getretene Übereinkommen über Computerkriminalität des Europarats (*Convention on Cybercrime*, **CCC**), welches z.B. auch die USA, Australien und Japan unterzeichnet haben, einschlägig. Das CCC bezweckt u.a. die Erleichterung der Rechtshilfe im Cyberbereich. Insbesondere sieht Art. 32 lit. b CCC den **direkten Zugriff** auf (oder den Empfang von) im Hoheitsgebiet eines anderen Vertragsstaates befindliche Daten vor, sofern die **Zustimmung** der zur Weitergabe der betreffenden Daten befugten Person (z.B. ausländischer Internetservice-Provider, der sich in den Datenverwendungsrichtlinien gegenüber seinen Kunden ein solches Recht vorbehalten hat) vorliegt. Der hoheitliche Zugriff (d.h. ohne Zustimmung) durch Schweizer Strafbehörden auf im Ausland domizilierte Anbieter ist indes nach bundesgerichtlicher Rechtsprechung aufgrund des **Territorialitätsprinzips** unzulässig, da hierfür der Weg der internationalen Rechtshilfe in Strafsachen vorgesehen ist (BGE 141 IV 108).

Aus umgekehrter Perspektive (Datenzugriff ausländischer Behörden auf in der Schweiz gelegene Daten) sieht der im März 2018 in den USA in Kraft getretene *Clarifying Lawful Overseas Use of Data Act* (**CLOUD Act**) für amerikanische Strafverfolgungsbehörden den Zugriff (via Provider) auf ausserhalb der USA lokalisierte Daten vor. Ein derart vorgenommener hoheitlicher Zugriff auf in der Schweiz lokalisierte Daten steht in einem potenziellen Spannungsverhältnis zu Art. 271 StGB (verbotene Handlungen für einen fremden Staat).

6 AUSBLICK

Im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018-2022 (NCS II) sind insbesondere der Aufbau eines **Cybersecurity-Kompetenzzentrums** auf Bundesebene sowie einer Cyber-Truppe der Armee vorgesehen. Erste strategische Entscheide hierzu wurden vom Bundesrat Ende Januar 2019 getroffen. Insbesondere soll der Auftrag der MELANI so erweitert werden, dass Dienstleistungen für die gesamte Wirtschaft angeboten und Warnungen und Informationen an die Bevölkerung herausgegeben werden können. Ferner soll das beim Eidgenössischen Finanzdepartement anzusiedelnde Kompetenzzentrum bei der Bewältigung von Cyber-Vorfällen **Weisungsbefugnisse** gegenüber anderen Bundesstellen erhalten. Sodann wird die **Einführung einer Meldepflicht** bei Cyberangriffen (insbesondere für Betreiber kritischer Infrastrukturen) erwogen. Auch international ist eine erhebliche **gesetzgeberische Dynamik** zu beobachten.

7 FAZIT

Angesichts der voranschreitenden Digitalisierung müssen sich Unternehmen (und Private) darauf einstellen, dass Risiken durch **Cyberattacken in Zukunft weiter zunehmen**. Im Ernstfall ist rasch und entschieden vorzugehen. Während Meldungen an MELANI insbesondere für Betreiber kritischer Infrastrukturen sinnvoll sind, ist die Einschaltung der Strafverfolgungsbehörden für jedes von einer Cyberattacke betroffene Unternehmen (und Private) eine ernstzunehmende Option, die es sehr zeitnah zu prüfen gilt.

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, LL.M. (LSE)
Partner
roland.mathys@swlegal.ch

Andreas Hösli, LL.M.
Associate
andreas.hoesli@swlegal.ch

In Genf:

Louis Burrus
Partner
louis.burrus@swlegal.ch

Clara Poglia, MAS in Criminology
Partnerin
clara.poglia@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