Cyberattacken

Meldung bei den Behörden?

Risiken durch Cyberangriffe auf Schweizer Unternehmen sowie deren Top-Management nehmen stetig zu. Für Firmen ist die Frage nach dem rechtlichen Handlungsbedarf im Ernstfall daher von grosser Wichtigkeit.

→ VON ROLAND MATHYS UND ANDREAS HÖSLI

DIE AUTOREN

Roland Mathys, Andreas Hösli
Rechtsanwalt Roland Mathys ist Co-Leiter der Rechtskommission von swissICT und leitet als Partner das Praxisteam ICT, Daten, Digital und Cyber der Anwaltskanzlei Schellenberg Wittmer.
Co-Autor Andreas Hösli ist ebenfalls Rechtsanwalt bei Schellenberg Wittmer und Spezialist für Mandate im Bereich Cyber- und Wirtschaftskriminalität. Die Rechtskommission von swissICT berichtet in der Kolumne «Recht & IT» über aktuelle juristische Themen im digitalen Bereich.
→ **www.swissict.ch**

Als Trittbrettfahrer der zunehmenden Digitalisierung haben sich professionelle Hacker auf gezielte Cyberattacken auf Unternehmen und deren Top-Management spezialisiert. Vorfälle wie die schwerwiegende Beeinträchtigung und teilweise Lahmlegung der IT-Infrastruktur grosser Unternehmen und öffentlicher Einrichtungen wie beispielsweise Spitäler durch die Verschlüsselungs-Malware NotPetya veranschaulichen, wie gross die Risiken sind. Nebst finanziellen Einbussen, etwa infolge eines Angriffs mit Ransomware, der Beeinträchtigung des Geschäftsbetriebs und der Beschädigung respektive des Verlusts sensitiver Daten stellen insbesondere mögliche Reputationsschäden hohe Risiken dar. Diese gilt es, durch das Management adäquat zu adressieren. Für Unternehmen und Organisationen ist es daher entscheidend zu wissen, welche rechtlichen Handlungsoptionen (und auch -pflichten) bei Cybervorfällen bestehen.

MELDEPFLICHT: NEIN, ABER …

Zunächst stellt sich bei einem Cybervorfall die Frage, ob dieser einer Behörde zu melden ist, und wenn ja, welcher. Nach heutiger Gesetzeslage besteht im Falle eines Cybervorfalls grundsätzlich keine Meldepflicht an eine Schweizer Behörde. Eine Ausnahme hiervon bilden sektorspezifische Meldepflichten aufgrund von Spezialgesetzen für Anbieter kritischer Infrastrukturen. Hierzu zählen etwa regulierte Finanzinstitute oder Unternehmen im Telekommunikations- sowie im Gesundheitsbereich.

Zudem kann eine Pflicht zur Notifikation innerhalb von nur 72 Stunden bei mit einem Cybervorfall einhergehenden Datenschutzverletzungen unter der EU-Datenschutz-Grundverordnung (DSGVO) bestehen. Die Einführung einer solchen Pflicht ist auch für das in Revision befindliche Schweizer Datenschutzgesetz (DSG) vorgesehen.

KOOPERATION MIT MELANI

Auf freiwilliger Basis können Cybervorfälle per Meldeformular der Melde- und Analysestelle Informationssicherung des Bundes (MELANI) gemeldet werden. Solche Meldungen ermöglichen es der Behörde, sich ein gut informiertes Lagebild über Cyberangriffe in der Schweiz zu verschaffen. Aktive Unterstützung bei der Bewältigung des Vorfalls bietet MELANI heute indes im Regelfall nur den Betreibern kritischer Infrastrukturen. Derzeit wird erwogen, das Mandat von MELANI auf Leistungen zu erweitern, die sich an die gesamte Wirtschaft richten.

> «In jedem Fall sollten die Strafverfolgungsbehörden rasch informiert werden»
>
> Roland Mathys

UMGEHEND STRAFANZEIGE STELLEN

Zur rechtlichen Aufarbeitung eines erfolgten (oder noch andauernden) Cyberangriffs kann es angezeigt sein, Strafanzeige bei einer spezialisierten Cyberstrafverfolgungsbehörde einzureichen. In vielen Kantonen und auf Bundesebene existieren fachkundige Stellen, deren Einbezug zur Eruierung der Täterschaft und zur Rückführung entwendeter Vermögenswerte zum Beispiel in Form von Bitcoins hilfreich sein kann. Oftmals besteht jedoch eine gewisse Zurückhaltung, aktiv auf Strafverfolgungsbehörden zuzugehen, da Cyberangriffe sensitive Bereiche des Unternehmens wie deren IT-Infrastruktur betreffen. Solchen Bedenken kann man dadurch begegnen, dass man mit der zuständigen Staatsanwaltschaft vorab das Gespräch sucht. Dies trägt dazu bei, dass die Reputation des betroffenen Unternehmens keinen Schaden nimmt. In jedem Fall sollten die Strafverfolgungsbehörden möglichst schnell involviert werden, um die Erfolgschancen der Ermittlungen zu erhöhen.

FAZIT

Unternehmen sind gut beraten, sich technisch, organisatorisch und rechtlich auf Cyberangriffe vorzubereiten, um im Notfall rasch und adäquat reagieren zu können. Bei einem Vorfall ist umgehend zu prüfen, ob eine Meldepflicht besteht und ob Strafanzeige gestellt werden soll. ←