Börsen-Zeitung
Zeitung für die Finanzmärkte
Ausgabe 10 vom 14.01.2017, Seite 9

RECHT UND KAPITALMARKT

Cyberkriminalität: Gewappnet für den Ernstfall?

Unternehmen drohen Reputationsschäden, Schadenersatzverpflichtungen und Bußgelder – Neue Rahmenbedingungen

Von Jan Geert Meents, Jan Pohle und Christian Schoop *)

Börsen-Zeitung, 14.1.2017

Immer wieder erschüttern spektakuläre Straftaten im Zusammenhang mit Cyberkriminalität die Wirtschaftswelt, zum Teil mit erheblichen finanziellen Schäden. So zuletzt in dem medienträchtigen Fall einer Cyber-Attacke auf über 900 000 DSL-Router oder die jüngst bekannt gewordenen Angriffe auf Yahoo, bei denen Hacker Daten von über einer Milliarde Kunden erlangten.

Die zunehmende Digitalisierung und Vernetzung wirtschaftlicher Prozesse schafft enorme Anreize für Kriminelle, schnelle Beute zu machen. Dies stellt für Unternehmen eine große organisatorische und personelle Herausforderung dar. Unternehmen drohen im Zusammenhang mit Cyberangriffen nicht nur der Verlust von Geschäfts- und Betriebsgeheimnissen, sondern bei nicht hinreichender Vorsorge oder einem nicht ordnungsgemäßen Verhalten im Ernstfall Reputationsschäden, Schadenersatzverpflichtungen und Bußgelder.

Der Begriff der Cyberkriminalität umfasst Taten, bei denen der Computer oder das Internet als Tatmittel oder als Tatobjekt eingesetzt wird. Der Schaden durch Cyberkriminalität für Unternehmen in Deutschland wird auf jährlich 51 Mrd. Euro geschätzt. Experten gehen von einer großen Dunkelziffer aus, weil oftmals aus (falsch verstandener) unternehmerischer Sorge vor Reputationseinbußen wegen eines publik gewordenen Cyberangriffs auf eine Anzeige verzichtet wird.

Es besteht für Unternehmen gleich welcher Branche und Größe die Gefahr, mit Angriffen konfrontiert zu werden. Hierzu zählen exemplarisch die Infiltrierung mit Schadsoftware (beispielsweise von sogenannter Ransomware, die im Jahr 2014 die IT-Struktur von Sony Pictures beschädigte), Phishing (also Erlangung persönlicher Kunden- und/oder vertraulicher Unternehmensdaten) und gegebenenfalls die anschließende Erpressung des Unternehmens mit der Drohung, gestohlene Daten zu veröffentlichen.

Unternehmen müssen sich dieser Herausforderung annehmen und zum einen Vorsorge vor einem Cyberangriff betreiben und sich aber zum anderen für den Ernstfall rüsten. Hierbei kommt der Beachtung verschiedener Rechtspflichten und der Zusammenarbeit mit den zuständigen Behörden national wie international eine herausgehobene Bedeutung zu.

Aufgerüstet

Staatliche Stellen haben das Thema Cyberkriminalität erkannt und sich zunehmend besser aufgestellt. Das Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI) als Bundesbehörde hat inzwischen weitreichende Aufgaben in der Bekämpfung der Cyberkriminalität. Die Bundesregierung räumt dem Thema IT-Sicherheit oberste Priorität ein und hat – neben rechtlichen Rahmenbedingungen – unter anderem die Weiterentwicklung des Nationalen Cyber-Abwehrzentrums sowie die Einrichtung von mobilen Einsatztruppen des BSI beschlossen. Daneben bestehen beim Bundeskriminalamt, dem Bundesamt für Verfassungsschutz und den Nachrichtendiensten (BND und MAD) spezialisierte Einheiten. Auch die Länder haben bei Staatsanwaltschaften und Landeskriminalämtern teilweise entsprechende Zentralstellen zur Bekämpfung von Cyberkriminalität geschaffen – so etwa in Berlin, Hessen, Nordrhein-Westfalen und Bayern. Diese Zentralstellen ermitteln bei besonders bedeutenden Verfahren im Bereich der (organisierten) Cyberkriminalität.

Doch auch die Strafverfolgungsbehörden stoßen im Bereich der Cyberkriminalität regelmäßig an ihre Grenzen. Zum einen erfasst das am analogen Weltbild orientierte Strafgesetzbuch nicht sämtliche Verhaltensweisen der Täter eines Cyberangriffs als strafbar. Zum anderen sind die strafprozessualen Voraussetzungen für Ermittlungsmaßnahmen, wie etwa die Durchsuchung von Cloud-Storage-Diensten, nach wie vor zum Teil ungeklärt. Auch erweisen sich Ermittlungstätigkeiten aufgrund des häufigen Auslandsbezuges und der mangelnden Unterstützungsbereitschaft ausländischer Provider als schwierig, weil formalisierte Rechtshilfeverfahren viel Zeit in Anspruch nehmen. Die Strafverfolgungsbehörden bedienen sich daher regelmäßig einer informellen Ebene des Austausches mit ausländischen Behörden, um ein schnelles operatives Tätigwerden zu erreichen.

Neue rechtliche Rahmenbedingungen sollen diese Probleme in den kommenden Jahren abmildern. Neben dem 2015 in Kraft getretenen IT-Sicherheitsgesetz auf Bundesebene wird im Frühjahr 2018 die EU-Datenschutzgrundverordnung nationales Recht. Mit der EU-Richtlinie zur Netz- und Informationssicherheit (kurz: NIS-Richtlinie) ist ein neues Instrumentarium zur europaweit koordinierten Bekämpfung von Cyberkriminalität geschaffen worden. Die NIS-Richtlinie wird spätestens 2018 in nationales Recht umgesetzt, seit Dezember 2016 liegt ein Gesetzesentwurf vor. Dies ist mit Blick auf die Unterschiede zu rechtlichen Rahmenbedingungen auf nationaler Ebene begrüßenswert.

Sowohl die NIS-Richtlinie als auch das sich hiermit teilweise überschneidende IT-Sicherheitsgesetz sehen eine Mitwirkungspflicht der Betreiber sogenannter kritischer Infrastrukturen vor. Hierzu zählen neben ausgewählten Branchen wie etwa dem Finanz-, Energie-, Verkehrs- und Versicherungswesen auch IT-Dienstleister. Diese sind verpflichtet, Mindeststandards für IT-Sicherheit einzuhalten, um die Begehung von

Computerstraftaten zu erschweren, und im Falle gravierender IT-Sicherheitsvorfälle solche den IT-Sicherheitsbehörden zu melden.

Chefsache

IT-Sicherheit ist aus Unternehmenssicht eine Führungsaufgabe, weil IT-Sicherheit für das Bestehen des Unternehmens von Bedeutung ist. Für internationale Unternehmen stellt die Gewährleistung von IT-Sicherheit zudem eine komplexe Aufgabe mit vielfältigen Rechtspflichten und Best Practices in verschiedenen Ländern dar. Auch infolge von Mitwirkungs-, Melde- und Sorgfaltspflichten muss Cybersicherheit im Unternehmen höchste Priorität haben. Sämtliche Unternehmen – und nicht nur solche, die sich digitaler Geschäftsmodelle bedienen – haben ihre rechtliche Compliance im nationalen und internationalen Datenverkehr fortlaufend zu kontrollieren und zu verbessern. Neben diesen präventiven Maßnahmen erfordert Cyberabwehr eine vorausschauende Projektplanung in Gestalt von Notfallplänen für den Krisenfall mit klaren Zuständigkeiten und Verantwortlichkeiten sowie klar definierten Verhaltensstandards. Im Vorfeld werden so gerade auch im Krisenfall drohende Reputationsschäden minimiert.

Schnelle Reaktion

Sollte trotz getroffener Präventivmaßnahmen der Ernstfall eintreten, ist eine frühzeitige Zusammenarbeit mit den Strafverfolgungs- und IT-Sicherheitsbehörden angezeigt. Die Staatsanwaltschaft kann umgehend etwa wegen der Straftatbestände des Computerbetruges, des Ausspähens und Abfangens von Daten, der Fälschung beweiserheblicher Daten bzw. der Täuschung im Rechtsverkehr sowie der Datenveränderung und der Computersabotage, aber auch wegen klassischer Straftaten wie der Erpressung Ermittlungsmaßnahmen durchführen. So kann der drohende Verlust von wichtigen Beweismitteln vermieden werden. Bei der Unterrichtung der Behörden gilt daher: Je schneller die Anzeige erfolgt, desto besser ist der Ermittlungserfolg.

Sofern ein Unternehmen zum Kreis der Betreiber kritischer Infrastrukturen gehört, ist gegenüber den IT-Sicherheitsbehörden eine Meldung vorzunehmen. Bei Finanzdienstleistern und Versicherungen sind Aufsichtsbehörden – etwa die BaFin – zu informieren und das weitere Vorgehen mit diesen abzustimmen. Sofern Kundendaten betroffen sind, kann eine unverzügliche Unterrichtung der Behörden oder der Kunden gefordert sein. Dies nicht zuletzt auch, um ein mögliches Schadenersatzrisiko zu minimieren. Wenn beim Diebstahl von Kundendaten Kunden und Datenschutzbeauftragte zu unterrichten sind, hat dies in enger Abstimmung mit den jeweiligen Behörden zu erfolgen, um den Erfolg möglicher Ermittlungsmaßnahmen nicht zu vereiteln.

*) Dr. Jan Geert Meents, Jan Pohle und Dr. Christian Schoop sind Partner von DLA Piper.

ID: 2017010050