Rechtliche Verpflichtungen nach einem Cyber-Security-Vorfall

Unternehmen, die von einem Cyber-Angriff heimgesucht wurden, unterliegen bereits heute einer gesetzlichen Informationspflicht. Damit endet die Verantwortung aber noch nicht.

Nach den jüngsten weltweiten Cyber-Attacken durch den Krypto-Trojaner WannaCry ist die Debatte um den Stellenwert von IT-Sicherheit und den Umgang mit Sicherheitslücken erneut entbrannt. Auch die diesmal nicht betroffenen Unternehmen sollten den vom WannaCry-Angriff ausgehenden Weckruf ernst nehmen und ihre Sicherheitsmaßnahmen evaluieren. Zudem sollten sie wissen, was zu tun ist, wenn sie tatsächlich Opfer eines digitalen Angriffs geworden sind.

Umfassende Meldepflichten für Sicherheitslücken

Der aktuelle Fall zeigt, dass Staat und Wirtschaft vertrauensvoll zusammenarbeiten müssen, um flächendeckende Angriffe auf IT-Systeme im Vorfeld zu verhindern. Aus diesem Grund hat nun auch der Verfassungsschutz zusammen mit BSI, Bundeskriminalamt und Bundesnachrichtendienst sowie einigen Wirtschaftsverbänden die **„Initiative Wirtschaftsschutz"** (*www.wirtschaftsschutz.info*) gegründet. Auf einer Internetseite werden Unternehmen Ratschläge gegeben, wie man sich vor Angriffen schützen und an wen sie sich im Notfall wenden können.

Diese Zusammenarbeit ist wichtig, denn beim WannaCry-Angriff wurde eine Sicherheitslücke in alten Windows-Systemen ausgenutzt, welche der US-Geheimdienst NSA entdeckte, aber nicht dem Hersteller meldete, sondern im Gegenteil für die eigenen Zwecke nutzte. Im August 2016 wurde die NSA jedoch selbst angegriffen und die Hacker erbeuteten etliche „Cyberwaffen". Doch erst viel später erfuhr der Windows-Hersteller Microsoft von der Lücke in seinem System und stellte im März 2017 ein Update zur Verfügung.

Da viele Systeme aber noch nicht aktualisiert waren, konnten die Kriminellen diese Lücke bis dahin ausnutzen. Sie verschlüsselten mit einer Erpressungssoftware, die Daten, um diese nur gegen eine Art Lösegeldzahlung wieder freizugeben. Vor diesem Hintergrund forderte unter anderem der Telekom-Chef Timotheus Höttgens eine Meldepflicht für Sicherheitslücken, die auch für staatliche Sicherheitsbehörden gelten solle. Welche Melde- und sonstigen Pflichten jedoch bereits heute bestehen, soll nachfolgend gezeigt werden.

Prävention statt Reaktion

Zuerst sind Unternehmen jedoch angehalten vorbeugend Maßnahmen zu ergreifen, um derartige Security Vorfälle und Datenpannen zu verhindern. Dies ergibt sich für alle Unternehmen aus den allgemeinen Sorgfaltspflichten, aber auch aus der neuen EU-Datenschutzgrundverordnung (DSGVO). Die ab dem 25. Mai 2018 geltende DSGVO sieht vor, dass die Verarbeitung personenbezogener Daten – zumindest bei „risikobehafteter" Datenverarbeitung – auch durch eine so genannte Datenschutzfolgeabschätzung begleitet und durch technische und organisatorische Maßnahmen geschützt wird.

Bei diesem **„Privacy Impact Assessment"** (*www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/RadioFrequencyIdentification/PIA/pia_node.html*) müssen die Auswirkungen der Datenverarbeitung für Betroffene evaluiert und effektive Maßnahmen der IT-Sicherheit etabliert werden. Betreiber kritischer Infrastrukturen müssen sogar präventive Schutzmaßnahmen nach dem „Stand der Technik" implementieren, um die kritische Infrastruktur vor einem Cyber-Angriff zu schützen.

Auch organisatorische Maßnahmen sind notwendig

Um im Falle einer erfolgreichen Attacke und dem Eintritt einer Meldepflicht die gesetzlichen Anforderungen überhaupt erfüllen zu können, bedarf es auch organisatorischer Strukturen innerhalb des Unternehmens. Diese sollen eine schnelle Ermittlung der Einzelheiten des Angriffs, seiner Folgen, sowie etwaiger zukünftiger Gegenmaßnahmen erlauben. Die klare Benennung eines oder mehrerer Verantwortlicher wie Datenschutzbeauftragter oder Security Officer sowie Schulungen der Mitarbeiter zur IT-Sicherheit und entsprechende interne Prozesse sind hierfür zwingend notwendig.

Melde- und Informationspflichten in Bezug auf Datenschutz und IT-Sicherheit

Unternehmen, die Opfer eines IT-Angriffs oder einer Datenpanne geworden sind, treffen bereits jetzt eine Reihe von Melde- und Informationspflichten. Durch die Meldung von Vorfällen an die Aufsichtsbehörden sollen mögliche oder bereits existierende Bedrohungen festgestellt, beziehungsweise ihnen entgegengewirkt werden. Dies erfolgt auch, um die Konsequenzen für die Betroffenen möglichst zu reduzieren.

Welche Informationspflichten im Einzelfall greifen, hängt von der Art und Weise des Cyber-Security-Vorfalls ab. Bei einer „Datenpanne", also der unrechtmäßigen Erlangung von personenbezogenen Daten von Kunden, greifen vorrangig die datenschutzrechtlichen Regelungen. Aktuell enthält das Bundesdatenschutzgesetz (BDSG),

welches wegen der ab 25.05.2018 geltenden EU-Datenschutzgrundverordnung gerade reformiert wird, in Paragraf 42a BDSG beziehungsweise den Paragrafen 66 und 67 BDSG-neu eine Meldepflicht, die immer dann eingreift, wenn besonders sensible Informationen unrechtmäßig einem Dritten zur Kenntnis gelangen und dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Typischer Beispielsfall eines meldepflichtigen „Data Breach" ist das Hacken von (Kunden-)Datenbanken. In diesem Fall müssen sowohl die zuständige Datenschutzaufsichtsbehörde als auch die betroffenen Personen unverzüglich informiert werden. Darüber hinaus ist der Aufsichtsbehörde mitzuteilen, welche Maßnahmen ergriffen werden um in Zukunft solche Vorfälle zu verhindern.

Verschärfte Regelungen für Betreiber kritischer Infrastrukturen

Welch gravierende Auswirkungen ein Cyber-Security-Vorfall für das gesellschaftliche Zusammenleben haben kann, hat der WannaCry-Angriff sehr deutlich in Großbritannien gezeigt, wo zahlreiche Krankenhäuser lahmgelegt wurden. Um solche Zustände zu vermeiden, hat der deutsche Gesetzgeber im Jahr 2015 das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (sog. IT-Sicherheitsgesetz) verabschiedet. Dieses musste jedoch bereits im Jahr 2017 an die europäische Richtlinie zur Netzwerk- und Informationssystemsicherheit (NIS-Richtlinie) angepasst werden. Das IT-Sicherheitsgesetz hat zum Ziel präventiv Schutzmaßnahmen nach dem „Stand der Technik" zu implementieren, um kritische Infrastrukturen vor einem Cyber-Angriff zu schützen und dadurch die Versorgungssicherheit der Bevölkerung zu gewährleisten. Es richtet sich daher allerdings nur an die Betreiber Kritischer Infrastrukturen, wie etwa Strom- und Wasserversorgung, Finanzen, Ernährung oder eben auch Gesundheitsversorgung. Zudem sind solche Betreiber von kritischen Infrastrukturen erst ab einer gewissen Größe betroffen.

Wird ein Betreiber Opfer eines Cyber-Security-Vorfalles oder liegt ein versuchter Angriff vor, treffen diesen besondere Meldepflichten. Der Betreiber muss die Angriffe der zuständigen Aufsichtsbehörde, in der Regel dem Bundesamt für Sicherheit in der Informationstechnik (BSI), melden. Diese Meldungen müssen ausführlich sein, um eine Verfolgung der Attacken und die Entwicklung wirksamer Schutzmaßnahmen zu ermöglichen.

Nach **Paragraf 8b Abs. 4 des Gesetzes für das Bundesamt für Sicherheit** (*www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Meldeformular_BSIG8b_Muster.pdf?__blob=publicationFile&v=3*) in der Informationstechnik (BSIG) müssen dann

Angaben zur Störung, den technischen Rahmenbedingungen, der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten sein. Atom-, Energiewirtschafts-, und Telekommunikationsgesetz enthalten beispielsweise in dem IT-Sicherheitskatalog der Bundesnetzagentur ähnliche Pflichten.

Nachforschungspflichten

Allein mit der Meldung eines Cyber-Security-Vorfalles an die zuständige Behörde endet die Verantwortung des betroffen Unternehmens aber nicht. Vielmehr muss der Vorfall, insbesondere wenn er erfolgreich war, fachmännisch aufbereitet werden, um die Sicherheitslücke zu schließen und zukünftige Angriffe über denselben Angriffsvektor zu erschweren. Um mögliche Spuren, die der Angreifer hinterlassen hat, nicht zu verwischen, sollten möglichst Forensik-Spezialisten mit einbezogen werden.

Da der Eingriff in fremde Systeme in den meisten Fällen auch Strafgesetze verletzt, kann hier auch die Staatsanwaltschaft eingebunden werden. So haben bereits einige Bundesländer, wie etwa Nordrhein-Westfalen, spezielle Anlaufstellen wie etwa die **„Zentral- und Ansprechstelle Cybercrime"** (ZAC, *www.polizei-bw.de/Dienststellen/LKA/Seiten/ZAC-Infoseite.aspx*) gegründet. Von Köln aus ermitteln die Staatsanwälte der ZAC und stehen Unternehmen dabei rund um die Uhr zur Verfügung.

Zertifizierungen für mehr IT-Sicherheit

Ein Weg zu mehr IT-Sicherheit ist es, das Management der Informationssicherheit an dem international anerkannten **ISO 27001-Standard** auszurichten (*www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html*). Die Bundesnetzagentur (BNetzA) ordnet die Zertifizierung nach ISO 27001 bis 2018 für die Strom- und Gasnetzbetreiber in ihrem IT-Sicherheitskatalog sogar ausdrücklich an. Des Weiteren verweist auch die BaFin in ihren MaRisk auf gängige IT-Standards wie ISO 27001 oder die BSI-Grundschutzkataloge. Diese aktuellen Frameworks zur Cyber-Security können daher auch anderen Unternehmen als „Ideengeber" für die Gestaltung der internen Prozesse dienen. Als „ISMS-light-Ansatz" kann KMUs etwa der **„VdS 3473"** (*https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf*) empfohlen werden, welcher in der Regel eine Vorstufe für eine mögliche ISO/IEC 27001 und BSI IT-Grundschutz-Zertifizierung darstellt.

Michael Rath, Christian Kuß