IT-RECHT

INCIDENT RESPONSE – AUF CYBERANGRIFFE RICHTIG REAGIEREN

Viele Hacker-Angriffe auf Unternehmen kommen zunächst unspektakulär daher. Die Folgen können jedoch gravierend sein. Unternehmen sind gut beraten, in die Sicherheit ihrer IT zu investieren.

▸ Es beginnt vielleicht mit einer harmlos aussehenden E-Mail: „Unter diesem Link kannst du dir die Bilder des letzten Firmenausflugs herunterladen.“, verspricht der Verfasser. Ein Klick auf den Link führt jedoch nicht zu dem erhofften Fotoalbum. Stattdessen erscheint eine Fehlermeldung im Browser, der Mitarbeiter klickt auf „Abbrechen“ und schließt das Browser-Fenster. Und dann passiert: Nichts. Kein plötzlich schwarzer Bildschirm, kein spektakulärer Hinweis, dass man gehackt wurde, keine über den Bildschirm flimmernden Totenköpfe oder Vergleichbares. Kurz öffnet sich das Konsolen-Fenster, in dem ein paar Zeilen mit kryptischen Computerbefehlen erscheinen. Dann verschwindet auch dieses Fenster wieder. Danach gibt es keine besonderen Vorkommnisse.

So oder so ähnlich können Hacker-Angriffe auf private und öffentliche Unternehmen beginnen, die dann tage- oder sogar monatelang unentdeckt ablaufen. Denn mit Klick auf den Link hat der Mitarbeiter unbewusst ein Schadprogramm heruntergeladen. Dieses verbreitet sich nun im gesamten Firmennetzwerk und beginnt damit, wichtige Daten des Unternehmens zu kompromittieren. Denkbar sind beispielsweise Übertragung der Daten ins Ausland oder, genauso schlimm, die Verschlüsselung sämtlicher Daten des Unternehmens.

Bemerkt wird der Angriff oft erst Monate später. Dann sperrt das Schadprogramm zum Beispiel den Zugang zu den Unternehmensdaten und fordert dazu auf, Lösegeld für die Entschlüsselung der Daten zu zahlen. Eine Entschlüsselung der Daten ohne Zahlung des Lösegeldes ist in vielen Fällen nicht oder nur mit hohem finanziellen Aufwand möglich.

Bekannte Bedrohungslage – Oft mangelhafte Vorbereitung

Zwar sind sich viele Unternehmen der aktuell hohen Bedrohungslage bewusst. Die Bereitschaft, in die Sicherheit der eigenen IT-Landschaft zu investieren steigt jedoch nur langsam an. Dabei werden Angriffe wie der oben beschriebene immer häufiger. Attacken auf die Uniklinik in Düsseldorf sowie auf Impfstoffentwickler und Impfzentren führen vor Augen, dass die IT-Landschaft ein verletzliches Rückgrat sowohl der öffentlichen Daseinsvorsorge als auch der Privatwirtschaft darstellt.

Deshalb ist es wichtig, vorbeugende Maßnahmen zur Verbesserung der IT-Sicherheit zu treffen. Unternehmen können so das Risiko, Opfer einer Cyber-Attacke zu werden, effektiv reduzieren. Ganz ausschließen lässt sich dieses Risiko jedoch mit wirtschaftlich vertretbaren Mitteln nicht. Daher sollten ergänzende Maßnahmen zum Umgang mit einem solchen Angriff getroffen werden.

Erfahrungsgemäß treffen Cyber-Attacken Unternehmen oft völlig unvermittelt. Gerade Unternehmen, die bereits einige Schutzmaßnahmen ergriffen haben, rechnen umso weniger mit einem tatsächlich erfolgreichen Angriff. Unabhängig von den Maßnahmen zum Schutz gegen solche Angriffe, herrscht in vielen Unternehmen nach einem Angriff „Kopflosigkeit“. Dabei gibt es unmittelbar nach einem erfolgten Angriff viele Möglichkeiten, Schäden zu begrenzen. Ergänzend haben Unternehmen eventuelle behördliche Informationspflichten zu prüfen, deren Existenz jedoch häufig unbekannt ist. In Unkenntnis der Rechtslage gehen Unternehmen dann hohe Bußgeldrisiken ein.

Minimierung von Schäden durch Incident Response Management

Um für den Ernstfall vorbereitet zu sein empfiehlt sich daher, einen sogenannten Incident Response Plan (IRP) zu erstellen. Dieser sollte auf das Unternehmen individuell zugeschnitten sein und die wirtschaftlichen und rechtlichen Besonderheiten berücksichtigen. In einem solchen IRP sollte ein Krisenteam benannt sein, das im Fall eines Angriffs alle Vorgänge im Zusammenhang mit dem Angriff bearbeitet bzw. koordiniert. Daneben sollte dieses Team die interne Kommunikation der einzelnen Fachabteilungen mit der Unternehmensleitung steuern sowie die externe Kommunikation mit Technikern, Anwälten und Versicherungen übernehmen. Auf diese Weise werden die Fachabteilungen entlastet, sodass das operative Tagesgeschäft – so gut es geht – fortgeführt werden kann.

Im IRP sollte außerdem ein möglichst detaillierter Ablaufplan festgehalten werden, der die nach einem Angriff erforderlichen Aktionen aufführt und die jeweils verantwortlichen Mitarbeiter benennt. Auf diese Weise kann auf einen Angriff so effektiv und effizient wie möglich reagiert werden.

Zu den unmittelbar erforderlichen Aktionen zählt, die Vertiefung des Cyber-Schadens zu verhindern. Hier ist entweder die Unterstützung der hauseigenen IT-Abteilung oder eines externen IT-Dienstleisters gefragt. Wenn abzusehen ist, dass die eigene IT-Abteilung mit derartigen Maßnahmen überfordert ist, sollte bereits im Voraus ein externer Dienstleister identifiziert werden, der im Ernstfall rasch unterstützen kann.

Auch die Etablierung eines regelmäßigen Cyber-Drills, also einer „Trocken“-Übung des Ernstfalls, an der das Krisenteam sowie die Unternehmensleitung teilnehmen, optimiert die Reaktionsgeschwindigkeit im Ernstfall nachhaltig.

Bußgelder vermeiden durch rechtskonforme Meldung an Behörden

Des Weiteren ist es zwingend erforderlich, den Status quo unmittelbar nach dem Angriff zu dokumentieren. Dies erleichtert einerseits eine Liquidation des eingetretenen Schadens über eine Cyber-Versicherung sowie die eventuelle Geltendmachung von Schadenersatzansprüchen vor Gericht. Andererseits ist eine umfassende Dokumentation des Angriffs die Grundlage für die behördlichen Meldepflichten, die das Unternehmen treffen.

Zu den behördlichen Meldepflichten gehören die Informationspflichten aus der Datenschutzgrundverordnung. Hier gilt es, auf der Grundlage einer rechtlichen Risikoabwägung zu entscheiden, ob nur die Aufsichtsbehörde oder aber auch (sämtliche) betroffene Kunden des Unternehmens informiert werden müssen.

Darüber hinaus zählen beispielsweise Gas- Wasser- oder Stromversorger, Kliniken, Pharmaunternehmen und Labore sowie Apotheken, große Lebensmittel-Hersteller und Händler, Banken, IT-Dienstleister wie Server-Farmen und Hosting-Betreiber als sogenannte Betreiber kritischer Infrastrukturen (KRITIS). Diese KRITIS-Betreiber sowie Anbieter digitaler Dienste treffen zusätzliche Informationspflichten aus dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz). Zahlungsdienstleister müssen Meldungen gemäß dem Zahlungsdiensteaufsichtsgesetz abgeben, börsennotierte Unternehmen trifft eventuell die Pflicht zu einer ad-hoc-Mitteilung. Die rechtskonforme inhaltliche Ausgestaltung der jeweiligen Meldung und deren fristgerechte Abgabe sind dabei von zentraler Bedeutung. Werden Meldungen verspätet, gar nicht oder nicht rechtskonform abgegeben drohen hohe Bußgelder. Daneben hat die Ausgestaltung der Meldung auch erheblichen Einfluss auf die Reputation des Unternehmens, insbesondere bei der Mitteilung an betroffene Kunden sowie bei ad-hoc-Mitteilungen.

Die Behandlung dieser Meldepflichten sollte daher im individuellen Fall gründlich abgewogen werden, um Reputationsschäden so gering wie möglich zu halten und trotzdem alle rechtlichen Verpflichtungen zu erfüllen.

DIE AUTOREN

Dr. Carsten Ulbricht ist Rechtsanwalt und Partner bei der Kanzlei Menold Bezler in Stuttgart. Er berät zu allen rechtlichen Themen des Internet, mobiler und sozialer Medien und rund um die Digitalisierung von Unternehmensprozessen und Produkten. Die Schwerpunkte liegen dabei auf IT- und Internetrecht, Datenschutzrecht bzw. Urheber-, Wettbewerbs- und Markenrecht. Neben der Prüfung der Rechtskonformität von Geschäftsmodellen, liegt ein wesentlicher Fokus auf der Vertragsgestaltung (einschließlich dem Entwurf von AGB und anderen Verträgen).

Carlo Kunz ist Rechtsanwalt bei der Kanzlei Menold Bezler Rechtsanwälte in Stuttgart. Er ist dort mit dem gesamten Gebiet des IT-Rechts betraut. Er berät insbesondere zum Datenschutzrecht sowie zu den Themen Cyber-Security, IT-Compliance und der Verfolgung von IT-Straftaten. Daneben ist er auch mit der gerichtlichen und außergerichtlichen Vertretung in Medien- und Urheberrechtsstreitigkeiten befasst.

www.menoldbezler.de