Informatik Spektrum (2020) 43:61–62
https://doi.org/10.1007/s00287-020-01238-7

FORUM

Incident Response und Recht

Ursula Sury[1]

Online publiziert: 30. Januar 2020

Cyberkrieg und Cryptotrojaner

Ein Mail kommt und wird vom Mitarbeiter geöffnet ... und schon ist es passiert. Dieser und viele andere Wege sind möglich, um auf ganz einfachem Weg Zugang zur IT eines Unternehmens zu bekommen und grundsätzlich zu schädigen. Schäden reichen von Verschlüsselungen verbunden mit Erpressungen über Datenklau und Datenzerstörung bis hin zur Übernahme von Steuerungen von Anlagen und Maschinen.

Insbesondere durch die immer weitere Einbindung von IOT und generell weitere Verknüpfungen mittels Digitalisierung werden die Angriffsflächen und somit die Risiken immer größer, Opfer einer Cyberattacke zu werden.

Incident Response und Governance

Unter Incident Response (Vorfallreaktion) versteht man die notwendige Reaktionsweise nach einer erfolgreichen Cyberattacke. Dazu benötigt man in aller Regel die Unterstützung durch eine spezialisierte Unternehmung. Es braucht technisches Spezialwissen, um Schäden zu beheben oder auch nur möglichst einzuschränken.

Solche Incidents möglichst zu verhindern, ist Aufgabe des Riskmanagements und der Informationssicherheit, organisatorisch bei den jeweiligen Verantwortlichen CISO (Chief Information Security Officer) zu verorten.

Im Rahmen der Unternehmensführung gehört die Vorwegnahme/Planung eines möglichen Incident Response zur Business Continuity Management (BCM) Planung.

✉ Ursula Sury
ursula.sury@hslu.ch

[1] Luzern, Schweiz

Verantwortung für Incident Management

Wer für Unternehmensführung verantwortlich ist, muss mit sämtlichen Risiken, die damit verbunden sind, adäquat umgehen. In der digitalisierten Welt sind Risiken hauptsächlich rund um den Umgang mit Informationen zu finden. Diese Informationen werden eben über IOT-Schnittstellen übertragen, sind in Servern gelagert, über Rechner verbunden. Kurz und gut: Sie sind digital vorhanden.

Das bedeutet, dass der Verwaltungsrat und die Geschäftsleitung sich mit diesen Hauptrisiken und damit verbundenen Maßnahmen vornehmlich beschäftigen sollten. Es müsste somit alles daran gesetzt werden, das Eintreten der Risiken zu vermeiden und ein realistisches BCM zu planen.

Nach Eintritt eines Incident ist unbedingt auch die Arbeit und Sensibilisierung des Verwaltungsrates und der Geschäftsleitung zu überprüfen.

Rechtsverletzungen rund um Daten und Informationen

Die beschädigten oder gestohlenen Informationen bei einem Incident könnten verschiedene Rechtsaspekte und somit auch verschiedene Personen betreffen.

Es können Geheimnisse publik gemacht oder gestohlen werden. Zu denken ist hier zum Beispiel an Fabrikationsgeheimnisse, wie Rezepte oder Geschäftsgeheimnisse und Umsatzzahlen. Dies kann strafbar sein und es muss mit Strafuntersuchungen gerechnet werden, insbesondere falls nicht genügende Sicherheitsmaßnahmen ergriffen wurden. Waren angemessene Sicherheitsmaßnahmen installiert, ist aber nicht mit einer Verurteilung der verantwortlichen Führungspersonen zu rechnen.

Falls Personendaten betroffen sind, kann es notwendig sein, nach DSGVO oder nach dem kommenden Datenschutzgesetz der Schweiz eine Meldung (DSGVO Art. 33 und Art. 34) bei der Datenschutzaufsichtsstelle zu machen. Der Art. 33 der DSGVO (Datenschutzgrundverordnung) sieht vor, dass bei einer Verletzung des Schutzes von personenbezogenen Daten der Verantwortliche dies innerhalb

von 72 h der zuständigen Aufsichtsbehörde mitzuteilen hat. Zur Erleichterung der Mitteilung haben die Aufsichtsbehörden umfangreiche Eingabemasken eingerichtet, die online bearbeitet werden können. Kommt es beim Betroffenen, Kunden oder Nutzer zu einer schwerwiegenden Verletzung, hat eine Information durch den Verantwortlichen gem. Art. 34 DSGVO sofort zu erfolgen. Bei einer entstandenen Datenpanne hat jeder Beteiligte zu wissen, an wen sich dieser im Ernstfall wenden muss. Schließlich handelt es sich um ihre persönlichen Informationen und somit Persönlichkeitsanteile, die durch die Malwareattacke betroffen und somit verletzt sind.

Auch hier ist mit möglichen Sanktionen als Konsequenz zu rechnen, wenn die Meldepflicht bei der Aufsichtsbehörde oder die Informationspflicht bei den Betroffenen durch die Verantwortlichen unterlassen wird.

Vererben der Probleme

Ist die Malware über Mail eingeschleppt worden, jedoch auch sonst, besteht die Gefahr, dass mögliche Außenkontakte, wie Kunden, Lieferanten, eigene Subunternehmen oder auch Dritte infiziert werden. Deshalb ist es auf dem Hintergrund der Schadenminderungspflicht wichtig, sofort zu reagieren und die Betroffenen zu informieren und nach Möglichkeit zu unterstützen, damit keine größeren Probleme entstehen.

Verhinderung an eigener Leistungsmöglichkeit und AGB

Wenn wegen des Informationsverlustes die eigene Leistungsmöglichkeit eingeschränkt oder unmöglich geworden ist, müssen die Kunden umgehend informiert werden. Da das Problem im Machtbereich des Lieferanten aufgetreten ist, ist zu klären, ob es sich um entschuldbare Verhinderung – analog höhere Gewalt – handelt, oder ob für Verspätungen oder Nichterfüllungen gehaftet werden muss. Grundsätzlich wird das Verschulden bei Unmöglichkeit vermutet. Hier wären sicher noch entsprechende Hinweise und Enthaltungen für Fahrlässigkeit in den Allgemeinen Geschäftsbedingungen von Vorteil.

Zusammenfassung

Unter Incident Response versteht man die Reaktion eines Unternehmens auf einen IT-Angriff. Dazu zählen alle organisatorischen und technischen Maßnahmen zur Abwehr und schnellen Eindämmung des Cyberangriffs, damit der Schaden möglichst gering bleibt. Digitale Angriffe sind heute so vielfältig wie die digitale Welt selbst. Dies macht die Ausarbeitung eines umfassenden Incident Response Plans für viele IT-Abteilungen auch zur Herausforderung. Mit einem ausgereiften und erprobten Incident Response Plan lassen sich der Erfolg der Angreifer und die Höhe des angerichteten Schadens jedoch minimieren.

Ursula Sury ist selbständige Rechtsanwältin in Luzern, Zug und Zürich (CH) und Vizedirektorin an der Hochschule Luzern – Informatik. Sie ist zudem Dozentin für Informatikrecht, Datenschutzrecht und Digitalisierungsrecht.