Cyberkriminalität und unternehmerische Verantwortung

Von RA lic. jur. Ursula Sury

Cybercrime ist auch in der Schweiz sehr präsent. Oft wissen Betroffene (noch) nicht, dass sie Opfer einer Attacke wurden und, dass dies für das Unternehmen und deren Leitung Konsequenzen haben kann.

Gegenüber Kunden, Lieferanten, Mitarbeitern und Dritten stehen Geschäftsleitung und Verwaltungsrat in der Verantwortung. Insbesondere statuiert Art. 716a Abs. 1 Ziff. 5 OR, dass der Verwaltungsrat die Gesetzmässigkeit in der eigenen Organisation persönlich sicherstellt. Daten müssen vor Zugriff unberechtigten Personen geschützt werden, damit u. a. kein Amts- (Art. 320 StGB), Berufs- (Art. 321 StGB), Fabrikations- oder Betriebs- (Art. 162 StGB) sowie Datenschutzgeheimnis (Art 35 DSG) offenbart wird. Allenfalls muss ein Verwaltungsrat mit zivilrechtlicher Verantwortung (Art. 754 OR) rechnen.

Nachfolgende Ausführungen geben einen kurzen Überblick zur Cyberkriminalität, die unternehmerische Verantwortung und wie technisch und organisatorisch vorzugehen ist.

Digitale Taten und Anzahl Opfer steigen

Ende August wurde bekannt, dass das Schweizer Grossunternehmen Habasit Opfer eines Ransomware-Angriffs wurde. Durch diesen «Data leak» wurden grosse Mengen an vertraulichen Daten des Schweizer Industrie-Konzerns im Darknet veröffentlicht. Dabei handelte es sich um besonders schützenwerte Daten, wie Vergütungen der Angestellten und des Managements, Mitarbeiterbewertungen aber auch Daten aus dem Rechnungswesen und Signaturen des höheren Kaders.

Dieses Vorgehen ist Standard bei Cyber-Piraten. Im August wurde unter anderem bereits eine Gemeindeverwaltung im Kanton Waadt, die Klinikgruppe Pallas oder die Universität Liechtenstein Opfer eines Ransomware-Angriffs. Weitere Bekanntheit erlangte der Angriff auf Comparis im Juli.

Was ist Cybercrime?

Als digitale Kriminalität, sog. Cybercrime oder High-Tech Crime, gelten Straftaten, die im digitalen Raum, also mit Informations- und Kommunikationstechnik begangen werden.

Straftaten werden also nach dem Modus Operandi, der Art der Tatdurchführung, als Cybercrime klassifiziert. Somit gelten alle illegalen Aktivitäten, welche mithilfe digitaler Technologie durchgeführt werden als Cybercrime.

Aktuelle Herausforderung

Ransomware-Attacken zeigen auf, wie Cyberkriminalität an Bedeutung gewinnt.

Mit der polizeilichen Kriminalstatistik (PKS) 2020 wurden erstmals gesamtschweizerische Zahlen veröffentlicht. So wurden 24'398 Cybercrime-Straftaten erfasst. Der Anteil der Cyberkriminalität beträgt heute 31,6% aller im Jahre 2020 erfassten Straftaten. Durch die Verschiebung unserer Lebensrealitäten in digitale Sphären ist mit einem starken Anstieg der Cyber-Kriminalität zu rechnen.

Empfohlenes Vorgehen: Cyber Incident Response

Da Angriffe auf Unternehmen immer komplexer und zielgerichteter werden, muss sich ein Unternehmen heute entsprechend organisieren, um sich vor einem potentiellen Cyberangriff/Datenverletzung zu schützen (Prevent) oder einen Angriff überhaupt erst zu erfassen (Detect). Falls es zu einem Angriff kommt, muss im Vorhinein geklärt sein, wie ein

Unternehmen mit diesem Ereignis umgeht (respond) und wie man für zukünftige Angriffe reagieren muss (revocer). Dieser Prozess wird «Cyber Incident response» genannt.

I. Prevent

Ein Cyberangriff kann nicht mit Sicherheit verhindert werden, allerdings kann das Risiko durch präventive Massnahmen drastisch minimiert werden.

a. Technische Vorkehrungen

Es müssen griffige technische Massnahmen getroffen werden (regelmässige Sicherheitsupdates der Betriebssysteme, aktuelle Virenschutzprogramme, Firewalls, 2-Faktor-Authentifizierungen, regelmässige Backups der Daten).

b. Sensibilisierung

Die Mitarbeiter müssen sensibilisiert werden. Trotz der ganzen Digitalisierung bildet der Mensch immer noch den grössten Schwachpunkt im System. Es ist daher besonders wichtig, ein Bewusstsein in technischer und sozialer Hinsicht zu schaffen. Dazu müssen intern Weisungen erteilt und Mitarbeiter müssen entsprechend geschult werden.

c. Organisatorische Massnahmen

Zudem ist es wichtig, dass ein Unternehmen sich organisatorisch vorbereitet, indem Verfahren oder Anleitungen ausgearbeitet werden, sollte der Fall eintreffen, Opfer eines Cyber-Deliktes zu werden. Dabei muss die Vorgehensweise für verschiedene Szenarien bei einem IT-Sicherheitsvorfall definiert werden. Für eine schnellere Reaktion müssen die Rollen und Kompetenzen zum Voraus klar geregelt sein.

II. Detect

Eine gute Vorbereitung nützt wenig, wenn eine Cyberattacke zu spät festgestellt wird. Darum müssen die Systeme ständig beobachtet werden.
Wurde auf Dateien oder Protokolle zugegriffen oder wurden solche erstellt, verändert kopiert oder sogar gelöscht?

Mit den Spezialisten sind Prozesse auszuarbeiten, um ungewöhnliche Vorkommnisse festzustellen und eine rasche Rückmeldung an die Verantwortlichen zu gewährleisten.

III. Response

Die eingangs geschilderten Vorfälle zeigen v. a. eines auf: Oftmals ist das Verhalten in der Organisation für den Ernstfall nicht klar. Es müsste innert kurzer Zeit folgendes geschehen:

a. Unmittelbare Reaktion nach Feststellung

Wurde eine Angriff auf das System festgestellt, gilt es die infizierten Systeme schnellstmöglich vom Netzwerk zu trennen, um weiteren Schaden zu vermeiden.

b. Ursache ermitteln

Die Ursache oder der Auslöser des Vorfalls muss gesucht, gefunden und aus dem System entfernt werden. Erst dann kann das betroffene Teilsystem wieder integriert werden. Da in der Regel eine schnelle Reaktion erforderlich ist, muss schon vor dem Sicherheitsfall feststehen, welche externen Partner man zur Hilfe heranziehen kann.

c. Abwägen, ob Behörden zu informieren sind

Nach Bekanntwerden eines Sicherheitsvorfalls mit potenziell weit reichenden Folgen ist u.U. innert 72 Stunden eine Mitteilung abzugeben.

Da ein Sicherheitsvorfall in der Regel eine Straftat darstellt, ist es ratsam die zuständige Strafverfolgungsbehörde zu informieren und mit deren Cybercrime-Spezialisten zusammenzuarbeiten.

Unabhängig von einer Anzeige bei der Strafverfolgungsbehörde, sind Sofortmassnahmen zum Schutze Personendaten etwaiger betroffenen Personen zu treffen. Gegenüber den betroffenen Personen, besteht auch eine Meldepflicht, wenn es der Schutz der Personendaten erfordert. Dies ist beispielsweise der Fall, wenn Zugangsdaten abgegriffen wurden und folglich Passwörter geändert werden müssen.

Mit Inkrafttreten des neuen Datenschutzgesetzes 2022 muss eine Datenschutzverletzung dem EDÖB (Eidgenössischer Datenschutz und Öffentlichkeitsberater) gemeldet werden, wenn ein hohes Risiko für negative Folgen für die betroffene Person besteht (Art. 24 nDSG).

Allerding sieht das neue Datenschutzgesetz keine Sanktion für die Verletzung der Meldepflicht vor.

IV. Recover

a. Beweise sichern

Für den Nachweis und eine spätere Analyse empfiehlt es sich eine Kopie des betroffenen Systems zu erstellen. Weiter wird eine Meldung an den Hersteller des Produkts/Systems empfohlen dessen Schwachstelle ausgenutzt wurde, somit können andere potentiell Betroffene (Hersteller sowie Nutzer) entsprechend reagieren.

b. Kontinuierliche Verbesserung

Die gewonnen Erkenntnisse aus einem solchen Vorfall sollten in die Vervollständigung und Aktualisierung der internen festgelegten Vorgehensweise für solche Sicherheitsvorfälle fliessen.

Fazit - Zukunftsaussichten

Grundsätzlich kann jedes Unternehmen Ziel eines Cyberangriffes werden. Die Gefahr nimmt mit der fortschreitenden Digitalisierung laufend zu.

Unternehmen müssen sich die Frage stellen, ob ihre interne Organisation und IT-Systeme auf einen solchen Sicherheitsvorfall vorbereitet sind und sie im Ernstfalle adäquat reagieren könnten. Der Schaden für das Unternehmen ist umso grösser, falls es sich erst im Ernstfall mit dieser Problematik befasst. Dazu ist mit negativer Publizität zu rechnen, wenn zu spät oder zögerlich reagiert wurde.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und Vizedirektorin an der Hochschule Luzern – Informatik. Sie ist zudem Dozentin für Informatikrecht in verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.