Serie Cyber-Sicherheit

Kommunikation in der Krise

[24.03.2023] Die Kommunikation nach einem Cyber-Angriff trägt entscheidend dazu bei, wie die Krise innerhalb der Kommune sowie von Bürgern und Medien wahrgenommen wird. Auch wenn es kein Patentrezept gibt, sollten also entsprechende Vorkehrungen getroffen werden.

Der Wunsch, bei einem Cyber-Angriff nicht aus einer dynamischen Lage zu kommunizieren, ist verständlich. Doch wer nicht kommuniziert, riskiert, dass es andere tun. Spekulationen, Gerüchte und Falschinformationen verbreiten sich sehr schnell. Ihre Auswirkungen sind nicht immer einzuschätzen. Gleichzeitig haben Führungskräfte in einer Krise viele Entscheidungen zu treffen, sodass die interne und externe Kommunikation darunter leiden. Das Thema Kommunikation ist daher unabdingbarer Teil des Business Continuity Managements (BCM) und sollte mit mindestens einer Person sowie einem Vertreter im Notfallstab personell eingeplant sein. Krisenkommunikation hat zum Ziel, bei allen Beteiligten den gleichen Informations- und Wissensstand zu schaffen. Medien, Beschäftigte sowie die Bevölkerung sind möglichst umfassend, aktuell, widerspruchsfrei und wahrheitsgemäß zu informieren. In den meisten Fällen ist es empfehlenswert, dass die Beschäftigten die Informationen zeitgleich mit der Öffentlichkeit erhalten. Sofern ein Abfluss von Daten nicht ausgeschlossen werden kann, sollte der Datenschutzbeauftragte in die Kommunikation eingebunden werden. Krisenkommunikation folgt aufgrund der Dynamik der Lageentwicklung keinem Patentrezept. Aus diesem Grund können hier nur Hilfestellungen und Anregungen für eine erfolgreiche Krisenkommunikation gegeben werden. **Allgemeine Mittel der Krisenkommunikation** Bei einem IT-Sicherheitsvorfall kommt erschwerend hinzu, dass die Telefonanlage und der Zugriff auf das E-Mail-Konto oftmals ebenfalls betroffen sind. Für den Notfall müssen daher immer aktuelle Kontaktinformationen von Presse- und Medienvertretern, Beschäftigten, Dienstleistern und Partnern ausgedruckt vorliegen. Ein dienstliches Endgerät, welches für den Notfall bereitgehalten wird, oder eine Regelung zum sicheren Einsatz eines privaten Endgeräts sollten ebenfalls berücksichtigt werden. Zu den allgemeinen Mitteln der Krisenkommunikation gehören Telefon, E-Mail, soziale Medien, eine extra eingerichtete Notfall-Hotline sowie die Internet-Seite mit Informationen zum Notfall und einer Sonderseite mit häufig gestellten Fragen. Sollte die reguläre Website durch den Cyber-Angriff betroffen sein, lohnt sich die Einrichtung einer alternativen Notfall-Internet-Seite, die primär der Krisenkommunikation dient. Sobald das im BCM festgelegte Notfall-Management angelaufen ist und die ersten Erkenntnisse gesichert sind, bieten sich eine Pressemitteilung, ein Interview oder eine Pressekonferenz an. Die Erklärung sollte folgende Fragen beantworten: Was und wann ist es passiert, wer oder was ist zu Schaden gekommen, mit welchen Auswirkungen ist zu rechnen, was wurde bisher unternommen und was sind die nächsten Schritte? **Mitarbeitende informieren** Für die Beschäftigten ist ein akuter Cyber-Angriff nicht immer ersichtlich. Für einen Mitarbeitenden kann es zunächst so aussehen, dass nur Log-in und Telefon nicht funktionieren. Das gilt insbesondere für die Mitarbeitenden im Homeoffice. Die hierdurch entstehende Unsicherheit ist sofort zu minimieren. Wichtig ist zunächst die Information, dass es zu einem Cyber-Angriff kam und Maßnahmen ergriffen werden. Auch Informationen über einen möglichen Zeitraum sind hilfreich. Ist es für die Mitarbeiterinnen und Mitarbeiter beispielsweise sinnvoll zu warten? Gibt es Aufgaben, die ohne IT bearbeitet werden können oder sind die Beschäftigten nach Hause zu schicken? Diese Fragen können im Rahmen der Erstellung eines BCM erörtert werden. Besonders wichtig ist es, rasch relevante Informationen für Beschäftigte mit Außenkontakt bereitzustellen. So benötigen die Mitarbeiterinnen und Mitarbeiter im Bürgerbüro Informationen, ob sie die Wartenden

nach Hause schicken müssen. Sie sollten zudem Rückfragen zur Dauer des Ausfalls beantworten können. In größeren Verwaltungen kann es auch notwendig sein, eine Anrufkette festzulegen und interne Multiplikatoren zu nutzen. Beschäftigte, die von zu Hause aus arbeiten, dürfen dabei nicht vergessen werden. **Externe Kommunikation** Jeder Mitarbeitende ist eine potenzielle Informationsquelle: vom internen Flurfunk über Messenger-Apps und private Konten auf sozialen Netzwerken bis hin zur inoffiziellen Informationsquelle für Journalistinnen und Journalisten. Mitarbeitende sollten nur Informationen erhalten, die auch für Externe geeignet sind. Wenn es sich um sensible, nicht zur Veröffentlichung bestimmte Informationen handelt, sollte explizit darauf hingewiesen werden. Es ist nicht immer notwendig, Details zu kommunizieren, es sei denn, es sind persönliche Daten, die persönliche Sicherheit oder die persönliche Situation der Beschäftigten betroffen. Die externe Kommunikation umfasst Journalistinnen und Journalisten, Medien, Bevölkerung, Dienstleister, Lieferanten, Aufsichtsbehörden, Polizei und Versicherung. Für die Kommunikation mit Medienvertretern sollten ein fester Ansprechpartner und ein Vertreter benannt werden. Daneben sollte ein Monitoring der Berichterstattung und der Beiträge in sozialen Medien stattfinden. Auch die Kommunikation Externer untereinander sollte nicht aus den Augen verloren werden. Neben der Verteilung von Informationen über Presse und Medien sollten Bürgerinnen und Bürger über die Internet-Seite der Kommune und gegebenenfalls die kommuneeigenen Kanäle in den sozialen Netzwerken Zugriff auf aktuelle Informationen haben. Eine eigene Unterseite für häufig gestellte Fragen kann die Kommunikation entlasten. Bei besonders schweren Fällen sollten im BCM Mittel und Ressourcen für eine Notfall-Hotline eingeplant werden. Dienstleister und Lieferanten müssen über Verzögerungen in Kenntnis gesetzt werden. In Fällen, in denen eine Ausbreitung der Schad-Software auf Dienstleister und Lieferanten möglich ist, müssen diese frühzeitig informiert werden, um ihre eigenen Systeme eng überwachen zu können. **Offen und wahrheitsgemäß informieren** Die Zentralen Ansprechstellen Cybercrime (ZACs) in den Landeskriminalämtern sind nicht nur im Notfall einzuschalten, viele ZACs bieten auch Kennenlern- und Beratungsgespräche an. Die Polizei stimmt die Pressearbeit mit den Verantwortlichen in der Kommune ab und erteilt in den frühen Phasen der Ermittlung keine proaktiven Presseauskünfte. Einige Kommunen haben Cyber-Versicherungen abgeschlossen. Hier ist zu prüfen, ab wann der Vertrag eine Einbindung der Versicherung erfordert und wie diese zu erfolgen hat. Auch diese Informationen sollten in Papierform vorliegen. Die Kommunikation über den Cyber-Angriff kann auch noch lange nach dem akuten Krisenereignis notwendig sein, beispielsweise dann, wenn gestohlene Daten von Mitarbeitenden oder Bürgerinnen und Bürgern im Darknet auftauchen oder für Fachverfahren essenzielle Datenbanken verloren sind und sich diese Verfahren daher verzögern. Die anhaltende Bedrohung durch Cyber-Angriffe ist den Menschen heute bewusster als jemals zuvor. Eine offene, umfassende, aktuelle, widerspruchsfreie und wahrheitsgemäße Kommunikation hat sich bewährt. Es empfiehlt sich, entsprechende Vorkehrungen zu treffen – von der Einplanung in den Krisenstab über das Grundverständnis von Cyber-Angriffsarten bis hin zu ausgedruckt vorliegenden Verträgen und Informationen. Die Kommunikation kann Art und Umfang, in der eine Krise die Wahrnehmung einer Kommune verändert, entscheidend beeinflussen.

()

Weitere Teile der Serie Cyber-Sicherheit
Das Hessen CyberCompetenceCenter (Hessen 3C)

Stichwörter: IT-Sicherheit, Hessen CyberCompetenceCenter, Hessen CyberCompetenceCenter (Hessen3C) Serie Cyber-Sicherheit