Cyber-Sicherheit

Im Worst Case erreichbar bleiben

[10.08.2023] Bei einem erfolgreichen Cyber-Angriff droht nicht nur ein Abfluss sensibler Daten – auch die Kommunikation einer Behörde bricht dann oft abrupt ab. Ein durchdachter Notfallplan und eine robust geplante IT bauen vor.

Die öffentliche Verwaltung setzt zunehmend auf digitale Kommunikationskanäle. Angesichts der zunehmenden Bedrohungslage ist es für Behörden mittlerweile eine große Herausforderung, ihre vertraulichen Informationen vor unbefugtem Zugriff, Datenlecks oder anderen Sicherheitsrisiken zu schützen. Selbst wenn Behörden alle notwendigen Maßnahmen ergreifen, um Systeme und IT-Infrastrukturen optimal zu schützen, kann eine erfolgreiche Cyber-Attacke nie ganz ausgeschlossen werden. Notfallpläne können in einer solchen Situation dazu beitragen, die Erreichbarkeit und Handlungsfähigkeit von Behörden abzusichern.
Da sie im Ernstfall unverzichtbar sind, werden Notfallpläne für die Verfügbarkeit von digitalen Kommunikationswegen in Deutschland auch gesetzlich eingefordert. So legt das IT-Sicherheitsgesetz 2.0 (IT-SiG), das zuletzt im Jahr 2021 aktualisiert wurde, fest, dass Betreiber Kritischer Infrastrukturen – darunter auch einige Behörden – Vorkehrungen treffen müssen, um die IT-Sicherheit zu gewährleisten. Darunter fällt auch das Erstellen von Notfallplänen für den Fall von Angriffen oder sonstigen Störungen. Um eine resiliente, IT-SIG-konforme Verfügbarkeit der Kommunikation zu erreichen, empfiehlt sich als erster Schritt eine umfassende Risikoanalyse. Dabei können Schwachstellen identifiziert und mögliche Auswirkungen auf die Abläufe einer Behörde skizziert werden. Zusätzlich sollten Behörden ein Incident Response Team ernennen, das im Falle eines Cyber-Angriffs die Maßnahmen koordiniert. So sind die Zuständigkeiten klar definiert und die Behörde kann mit einem koordinierten Prozess schnell auf Bedrohungen reagieren.

Ungestörter Kommunikationsfluss

Im Falle eines Angriffs, der die ganze IT-Infrastruktur lahmlegt, endet zunächst auch die digitale Kommunikation. Schon Teilausfälle können zu Flaschenhals-Effekten führen, die Arbeitsabläufe in der gesamten Organisation abbremsen. Deshalb gehört ein funktionierender IT-Verfügbarkeitsplan, der den resilienten Informationsfluss während einer Cyber-Attacke regelt, zwingend in jeden Notfallplan.
Eine digitale Behördenkommunikation sollte eine Reihe von Eigenschaften aufweisen, die es erleichtern, bei einem Cyber-Angriff die interne und externe Kommunikation aufrechtzuerhalten beziehungsweise zügig wiederherzustellen. So sollten Kommunikationsmittel robust gegen Angriffe und Störungen sein. IT-Sicherheit ist die Grundlage, um deren Verfügbarkeit sicherzustellen. So sollten Cyber-Sicherheits-Technologien etwa über Schutzmechanismen gegen Distributed-Denial-of-Service(DDoS)-Angriffe verfügen. Sie müssen außerdem in der Lage sein, unerlaubtes Eindringen in die Infrastruktur sowie andere verdächtige Aktivitäten zu erkennen und abzuwehren. Virenscanner oder die Verwendung von Zwei-Faktor-Authentifizierung erschweren es Kriminellen, in die Systeme von Behörden einzudringen oder Ransomware einzuschleusen. Insbesondere Ransomware-Angriffe, bei denen Hacker die Blockade von Systemen als Erpressungsszenario einsetzen, stellen eine veritable Gefahr für die Verfügbarkeit digitaler Verwaltungsprozesse dar.

Robust durch Redundanz

Ein weiterer Weg, um die digitale Kommunikation abzusichern, ist Redundanz: Ein System mit redundanten Kommunikationswegen und -infrastrukturen bietet die Option, auf alternative Kanäle auszuweichen, wenn der Hauptkommunikationsweg durch einen Angriff beeinträchtigt ist. Dies kann beispielsweise durch mehrere Internet-Anbindungen, redundante Leitungen und Server oder den Einsatz von verschiedenen Kommunikationsplattformen und -diensten erreicht werden. Ideal sind hier browserbasierte Lösungen, die auch ohne Clients funktionieren und einen verschlüsselten Datenaustausch ermöglichen. Auf diese Weise bleiben Behörden auch dann kommunikationsfähig, wenn der Rest der IT-Infrastruktur lahmgelegt ist.
Zudem sollten Kommunikationsmittel so ausgelegt sein, dass nach dem Ernstfall der Betrieb schnell wieder aufgenommen werden kann. Auf Basis regelmäßiger und vor allem automatisch erstellter Back-ups ist es möglich, Systeme und Daten in kurzer Zeit wiederherzustellen, Kommunikationswege wieder verfügbar zu machen und das Risiko eines umfangreichen Datenverlusts zu minimieren.
Die Verwendung von sicheren Verschlüsselungstechnologien schützt darüber hinaus die Integrität und Vertraulichkeit der übertragenen Daten. Eine durchgängige Ende-zu-Ende-Verschlüsselung stellt sowohl bei der Übertragung als auch bei der Speicherung sicher, dass auch sensible Informationen vollständig geschützt sind.

()

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, FTAPI Software