Serie Cyber-Sicherheit

Ein falscher Klick reicht

[06.10.2022] Cyber-Sicherheit ist kein Expertenthema, sondern geht alle an. In einer sechsteiligen Serie in Zusammenarbeit mit dem Hessen CyberCompetenceCenter wird Grundwissen vermittelt und praxisnah aufgezeigt, wie sich Kommunen schützen können.

Der Landkreis Anhalt-Bitterfeld in Sachsen-Anhalt, die Stadt Stralsund in Mecklenburg-Vorpommern und die Gemeinde Kammeltal in Bayern – drei Orte in Deutschland, die in Größe, Einwohnerzahl und Bekanntheitsgrad unterschiedlicher nicht sein könnten. Doch alle drei Kommunen haben eines gemeinsam: Sie wurden im vergangenen Jahr Opfer einer Ransomware-Attacke. Plötzlich konnten essenzielle Verwaltungsdienstleistungen nicht mehr erbracht werden. Zu den betroffenen Verwaltungsdienstleistungen zählten beispielsweise die Auszahlung von Sozialleistungen, das Beantragen von Ausweisen und Pässen ebenso wie die Anmeldung von Kraftfahrzeugen.
Cyber-Angriffe auf Ämter und Behörden sind längst Alltag geworden. Dennoch scheinen viele Kommunen das Thema nur zögerlich anzugehen. Die Herausforderung, vor die insbesondere kleine und mittlere Kommunen gestellt werden, ist groß: Technik, die immer wieder erneuert werden muss, Fachkräfte, die überall händeringend gesucht werden und gewachsene IT-Systeme, bei denen der Sicherheitsaspekt nicht immer mitgedacht wurde. Für Laien wirken die meist englischen Fachbegriffe und der technische Jargon zusätzlich abschreckend. Doch Cyber- und IT-Sicherheit ist kein Thema, das nur Fachkräfte etwas angeht. Alle Nutzerinnen und Nutzer von Endgeräten müssen sich mit dem Thema auseinandersetzen – denn ein falscher Klick reicht.

Lukratives Betätigungsfeld für Kriminelle

Um die angespannte Cyber-Bedrohungslage zu verstehen, muss man sich vom Bild des Hackers als einsamem Computer-Genie im Kapuzenpullover verabschieden. Lösegeldzahlungen und die Wahrscheinlichkeit, nicht gefasst zu werden, haben ein lukratives Betätigungsfeld für Kriminelle geschaffen. Erfolgreiche Cyber-Kriminelle benötigen heute keine besonderen IT-Kenntnisse mehr. Stattdessen können sie einzelne Dienstleistungen im Darknet einkaufen oder beauftragen. Angriffe setzen oft auf Quantität und Streuwirkung: Masse statt Klasse. Daneben gibt es auch hoch spezialisierte Angreifer, die von langer Hand planen und den Angriff individuell an das Ziel anpassen.
Mit fortschreitender Digitalisierung erhöht sich auch die Geschwindigkeit des digitalen Datenverkehrs und für Cyber-Kriminelle damit die Möglichkeit, an attraktive Daten zu gelangen. Wichtige Prozesse wie beispielsweise die Fernwartung von Systemen bieten neue Angriffsmöglichkeiten. Zahlreiche Menschen geben in sozialen Netzwerken wie LinkedIn, Facebook oder Instagram Informationen über sich preis. Diese können Cyber-Kriminelle nutzen, um die betreffende Person zu manipulieren, zu erpressen oder um sie zu unüberlegten Handlungen zu bringen. Während die meisten Standardarbeitsplätze mit grundlegenden Sicherheitsmaßnahmen wie zum Beispiel einem Viren-Scanner abgesichert werden, bleiben andere Systeme ungeschützt. Hierzu gehören (Dienst-) Handys und Tablets ebenso wie Router, Industrieanlagen, Smart-TV und die Heizung, die sich aus der Ferne steuern lässt.

Mit Hessen3C Cyber-Gefahren abwehren

In Erkenntnis dieser wachsenden Bedrohungslage hat das Hessische Ministerium des Innern und für Sport im April 2019 das Hessen CyberCompetenceCenter (Hessen3C) eingerichtet. Dessen Aufgabe ist es, die Sicherheit in der Informationstechnik des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren sowie die Effizienz der Bekämpfung der Cyber-Kriminalität zu steigern. Hessen3C arbeitet hierzu eng mit der hessischen Polizei, dem Landesamt für Verfassungsschutz Hessen und dem Hessischen Landeskriminalamt zusammen. Hessen3C ist die gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) benannte zentrale Kontaktstelle für die Entgegennahme landesbezogener KRITIS-Meldungen und vertritt das Land Hessen im Nationalen Cyber-Abwehrzentrum.
Unter Wahrung des Selbstverwaltungsprinzips können hessische Kommunen und ihre Eigenbetriebe – auf freiwilliger Basis und ohne Kostenbeteiligung – Leistungen des Hessen3C nutzen. Zu diesen Leistungen gehören Beratungs- und Awareness-Veranstaltungen für Mitarbeiterinnen und Mitarbeiter, ein werktäglicher Schwachstellenbericht mit verifizierten Informationen zu aktuellen Schwachstellen in Hard- und Software sowie Warnungen bei akuten Cyber-Bedrohungen. Hessen3C warnt teilnehmende Kommunen zudem vor durch Diebstahl oder Datenlecks kompromittierten dienstlichen E-Mail-Adressen. Bei IT-Sicherheitsvorfällen erreichen Betroffene über die rund um die Uhr an sieben Tagen die Woche besetzte Notfall-Hotline das im Hessen3C integrierte CERT-Hessen, das bei IT-Sicherheitsvorfällen zum Krisen-Management berät, gemeinsam mit den Verantwortlichen (bei Bedarf auch durch ein mobiles Team vor Ort) die Angriffswege analysiert und zu gesetzlichen Meldepflichten sowie der Erstattung von Strafanzeige informiert.

Übungen bereiten auf den Ernstfall vor

Gemeinsam mit ekom21, dem BSI-zertifizierten kommunalen IT-Dienstleister in Hessen, hat das Land Hessen das Kommunale Dienstleistungszentrum Cyber-Sicherheit (KDLZ-CS) sowie das Hessische Cyber-Abwehrausbildungszentrum Land/Kommunen (HECAAZ L/K) entwickelt. Die beiden sich ergänzenden Angebote orientieren sich an den Standards des BSI. Das KDLZ-CS steht seit 2016 zur Verfügung. Basierend auf einer Ist-Analyse zur Cyber-Sicherheit der teilnehmenden Kommune wird ein konkreter Maßnahmenplan zur Stärkung der Widerstandsfähigkeit gegen Cyber-Angriffe entwickelt. Bis zum 31. Juli 2022 haben 330 der insgesamt 443 hessischen Kommunen am Programm KDLZ-CS teilgenommen. 60 Gemeinden und fünf Landkreise haben inzwischen fortgeschrittene Maßnahmen durchgeführt.
Das HECAAZ L/K bereitet Bedienstete aus den Bereichen Verwaltungsleitung, Organisation und IT-Betrieb in realistischen Übungsszenarien auf den Ernstfall vor: einen Cyber-Angriff auf die Kommune. In den Schulungsveranstaltungen lernen die kommunalen Entscheider Maßnahmen des Business Continuity Managements (BCM) kennen. Anhand praktischer Übungen werden Notfallpläne und Strategien entwickelt. So sollen die Kommunen auch nach einem Cyber-Angriff schnell wieder arbeitsfähig sein. Kommunale Cyber-Sicherheit und Resilienz betrifft alle. Die Bürgerinnen und Bürger sind darauf angewiesen, dass die über 10.000 deutschen Kommunen den wachsenden Bedrohungen aus dem Cyber-Raum gewachsen sind und ihre Widerstandskraft gegen Angreifer stärken.

()

Das Hessen CyberCompetenceCenter (Hessen3C)
Dieser Beitrag ist in der Ausgabe Oktober 2022 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Hessen CyberCompetenceCenter