IT-Sicherheit

Potsdam zieht den Stecker

[15.03.2023] Ende 2022 nahm die brandenburgische Landeshauptstadt Potsdam ihre IT-Systeme vom Netz, um einer Cyber-Attacke zu entgehen. Bürgermeister Mike Schubert fordert mehr Unterstützung für die Kommunen durch Land und Bund. Andernfalls könnten diese IT- und Datensicherheit nicht mehr gewährleisten.

Die Kette der Meldungen über Cyber-Angriffe auf Kommunen und auch Organisationen wie Hochschulen reißt nicht ab. Die Folgen beschäftigen die Betroffenen oft wochen- und monatelang. Kurz vor dem Jahreswechsel, am 29. Dezember 2022, hat es eine große Kommune und Landeshauptstadt erwischt: Nach Warnungen durch Landes- und Bundeskriminalamt vor einer bevorstehenden Cyber-Attacke nahm die Stadt Potsdam ihre IT-Systeme vorsorglich vom Netz. Betroffen waren der gesamte E-Mail-Verkehr der Verwaltung und sämtliche Verfahrenssoftware. Anträge für Ausweisdokumente, An- und Ummeldungen, Kfz-Angelegenheiten, standesamtliche Urkunden – nichts ging mehr. Auch die städtischen Unternehmen hatten aus Sicherheitsgründen ihre Internet-Verbindungen offline gestellt. „Im Potsdamer Rathaus war es zu Beginn der IT-Krise so, als hätte jemand virtuell die Tür verschlossen und den Schlüssel abgezogen“, beschreibt Oberbürgermeister Mike Schubert den Zustand.

Nach dem Angriff ist vor dem Angriff – 2020 und 2022

Im Januar 2020 gab es schon einmal ein Angriff auf Potsdams IT, der die Verwaltung längere Zeit lahmlegte. Auch damals hatte die brandenburgische Landeshauptstadt ihre Verbindung zum Internet präventiv gekappt. Bei dem Angriff hatten Hacker eine bereits bekannte Sicherheitslücke in der Citrix-Software genutzt. Citrix war auch schon bei anderen schwerwiegenden Attacken – etwa auf die Städte Frankfurt am Main und Bad Homburg, das Kammergericht Berlin oder die Universität Gießen – das Einfallstor.
In Potsdam ergab eine IT-forensische Untersuchung, dass die technischen Sicherheitssysteme den Citrix-Angriff erfolgreich abgewehrt hatten. Folgenlos war der Vorfall aber nicht: Noch ein Jahr später waren iKfz-Services und der Antrag zum Bewohnerparken offline. Auch die vollständige Aufarbeitung zog sich hin. Der Berliner Tagesspiegel berichtet im Januar 2023, also drei Jahre später, dass „nach wie vor offen“ sei, ob die von der DSGVO vorgesehene Dokumentation des Vorfalls abgeschlossen sei. Ob die unter dem Eindruck des Angriffs neu geschaffenen IT-Stellen inzwischen alle besetzt sind, ist nach Tagesspiegel-Angaben ebenfalls unklar.
Dennoch haben die Erfahrungen mit dem Citrix-Vorfall und die danach getroffenen Vorkehrungen dazu beigetragen, dass Potsdam bei dem neuerlichen Angriff im Dezember 2022 schnell reagieren konnte. Bei der Bewältigung der Lage habe der Verwaltungsstab auf Ausweich- und Bypass-Szenarien zurückgegriffen, die im Zuge des Vorfalls von 2020 erarbeitet wurden, heißt es von der Stadt. Auch die bereits erfolgte Dokumentation helfe bei der erneut notwendigen Überprüfung der Systeme.

Der lange Weg zurück ans Netz

Mit dem Erfahrungswissen von 2020 begann Potsdam sofort nach dem Vorfall im Dezember 2022 mit umfangreichen Sicherheitstests und machte sich daran, Ausweichlösungen zu schaffen. Mitte Januar 2023 konnte die Verwaltung wieder E-Mails empfangen, auch erste Dienste wurden hochgefahren. Nachdem

kurz darauf ein Virenscanner anschlug, wurden die Server erneut vom Landesverwaltungsnetz Brandenburg getrennt, die E-Mail-Kommunikation wurde ab- und das Landeskriminalamt Brandenburg eingeschaltet. Inzwischen hat sich aber herausgestellt, dass die besorgniserregende Symptomatik auf eine Fehlkonfiguration zurückging.
Im Verlauf des Monats Februar konnten dann tatsächlich eine Reihe von Bürgerdienstleistungen wieder angeboten werden, darunter so wichtige Leistungen wie Wohngeldanträge, standesamtliche Beurkundungen und die Abholung von Ausweisen. Bei den Leistungen rund ums Kfz räumt das Rathaus selbst noch mögliche Verzögerungen im Betriebsablauf ein. Um den inzwischen aufgelaufenen Rückstau an Vorgängen abzuarbeiten, ist in den kommenden Wochen und Monaten eine Aufstockung des Personals geplant.
Parallel zur Wiederherstellung der Arbeitsfähigkeit der Verwaltung arbeitete man in Potsdam an einer besseren Absicherung der IT. Viele Details sind dazu nicht bekannt, offenbar aus Sicherheitsgründen. Vorgesehen ist vor allem ein „dauerhafter Informations- und Statusabgleich mit angeschlossenen Netzen auf Landes- und Bundesebene“. Bei dieser 24/7-Überwachung der IT-Systeme wird Potsdam von einem externen Dienstleister unterstützt. Die Rund-um-die Uhr-Kontrolle sei in einer ersten Stufe bereits angelaufen und sei auch Bedingung für das sukzessive Wiederhochfahren der Netzwerke gewesen, so der Oberbürgermeister.

Aufarbeitung wird dauern

Das präventive Not-Aus für Potsdams Verwaltungsdienste im Dezember 2022 konnte einen Datenverlust oder Datendiebstahl verhindern – anders als in anderen Fällen, wo Bürgerdaten sogar im Darknet landeten. So beispielsweise geschehen nach einer Ransomware-Attacke auf die Verwaltung des Rhein-Pfalz-Kreises (wir berichteten). In Potsdam ist die Verwaltung gut zehn Wochen nach dem Angriff zumindest in Teilen wieder arbeitsfähig, mit einer erneuten Abschaltung der Dienste wird vorerst nicht gerechnet. Dennoch sind die Folgen des Vorfalls noch lange nicht behoben.
Und es zeichnet sich ab: Ohne Hilfe von außen hätte die Landeshauptstadt die Lage wohl nicht bewältigen können. Nach Angaben des Rathauses waren an der Aufarbeitung zahlreiche externe Kräfte beteiligt. IT-Sicherheitsfirmen und IT-Forensiker, das Bundesamt für Sicherheit in der Informationstechnik (BSI) in beratender und technisch unterstützender Funktion, das Ministerium des Innern und für Kommunales des Landes Brandenburg, das LKA Brandenburg, der Brandenburgische IT-Dienstleister ZIT-BB, der Zweckverband Digitale Kommunen Brandenburg (DIKOM) und die Bundeswehr arbeiteten oder arbeiten mit. Dazu kommen hohe Kosten. Für die IT-Sicherheit rechnet die Stadt künftig zusätzlich mit zwei bis drei Millionen Euro im Jahr, um das derzeitige Sicherheitsniveau zu halten und perspektivisch weiterzuentwickeln.

Kommunen nicht alleine lassen

Gegen Cyber-Kriminalität könne man sich nicht abschotten, so Oberbürgermeister Schubert, sondern sich nur vorbereiten. Doch diese Vorbereitung erfordere erhebliche Anstrengungen. Kommunen könnten eine umfassende IT-Sicherheit auf adäquatem Niveau auf Dauer nicht alleine gewährleisten, betonte Schubert. Er appelliere an Land und Bund, für Kommunen mehr Geld bereitzustellen, aber auch langfristige Kooperationen und einen kontinuierlichen, ebenenübergreifenden fachlichen Austausch für die Cyber-Sicherheit zu garantieren. Datensicherheit sei eine elementare staatliche Aufgabe. Allerdings, so Schubert, werden die Kommunen diesen wichtigen Bestandteil der Daseinsvorsorge für die Bürgerinnen und Bürger auf Dauer nicht alleine gewährleisten können. Auch das Präsidium des Städte- und Gemeindebundes Brandenburg, dem Schubert angehört, will sich noch einmal verstärkt mit der Diskussion um das Thema Datensicherheit und den Folgen der Digitalisierung befassen.

()

Stichwörter: IT-Sicherheit, Potsdam, Cyber-Sicherheit