SIT

Ein Jahr nach dem Ransomware-Angriff

[04.11.2024] Ein Jahr nach der Cyberattacke auf die Südwestfalen-IT haben die Mitarbeitenden gemeinsam mit den IT-Teams betroffener Kommunen die Systeme wiederhergestellt. Um künftig besser gegen Cyberbedrohungen geschützt zu sein, fordert Geschäftsführer Mirco Pinske klarere gesetzliche Regelungen – etwa die Berücksichtigung kommunaler IT-Dienstleister in der NIS2-Richtlinie.

Ein Jahr ist es her, dass die Südwestfalen-IT (SIT) von kriminellen Hackern angegriffen wurde: In der Nacht auf den 30. Oktober 2023 verschlüsselte eine Ransomware-Gruppe die Systeme. 72 Mitgliedskommunen aus dem Verbandsgebiet waren nach Angaben des IT-Zweckverbandes betroffen. Bei dem Angriff wurde offensichtlich eine VPN-Schwachstelle ausgenutzt. Die Auswirkungen waren immens: Die betroffenen Verwaltungen konnten nicht auf die von der SIT bereitgestellten Fachverfahren und Infrastrukturen zugreifen, Verwaltungsleistungen für Bürger und Unternehmen konnten über längere Zeit gar nicht oder nur eingeschränkt erbracht werden. Vielerorts blieben Bürgerbüros in den Tagen nach dem Angriff ganz geschlossen, manche Kommunen haben behelfsmäßige Mailadressen und Websites eingerichtet, um mit Bürgerinnen und Bürgern in Kontakt zu bleiben und um zu kommunizieren, welche Leistungen wie erbracht werden können.

11 Monate Notfallmodus

In den darauffolgenden Monaten arbeiteten die Mitarbeitenden der SIT und die IT-Verantwortlichen der betroffenen Kommunen und deren Teams mit größtem Einsatz und unter enormem Zeitdruck daran, die Systeme so schnell wie möglich wieder zum Laufen zu bringen. „Ich war beeindruckt von der Kooperation und der Hilfe der Kommunen untereinander, beispielsweise bei der Etablierung von Behelfslösungen“, so Mirco Pinske, der seit Februar 2024 Geschäftsführer der Südwestfalen-IT ist.

Der Krisenmodus der SIT dauerte insgesamt 11 Monate an – Ende September 2024 konnte die Organisation in den Normalmodus wechseln. Zum jetzigen Zeitpunkt stehen nach Angaben von SIT nahezu 100 Prozent des Produktportfolios von rund 160 Anwendungen wieder im vollen Funktionsumfang zur Verfügung. Für die von den Zweckverbandsmitgliedern als besonders prioritär eingestuften Anwendungen – darunter fallen Bürger-, Finanz- und Sozialdienste – wurde der Normalbetrieb bereits vor mehreren Monaten beziehungsweise Wochen erreicht. „Lediglich vereinzelt“, so SIT, seien noch Restarbeiten zu erledigen. Zudem seien auch zahlreiche weitere Dienste bereitgestellt und neu eingerichtete Zugriffe für eine dreistellige Anzahl externer Webanwendungen ermöglicht worden.

Zu den konkreten Kosten des Vorfalls lasse sich abschließend noch keine verlässliche Aussage treffen, da das Geschäftsjahr noch nicht abgeschlossen ist. „Bis zum Stichtag 30. September 2024 fielen Zusatzaufwendungen in Höhe von circa 2,8 Millionen Euro an“, so Pinske.

Sicherheitsvorkehrungen verschärft

SIT berichtet, dass in den vergangenen Monaten zahlreiche Sicherheitsvorkehrungen in allen aktuell eingesetzten Systemen implementiert worden seien. Dabei wurden auch externe IT- und Cyber-Security-Experten hinzugezogen. So seien die Systeme noch stärker segmentiert worden, um in Zukunft mögliche Schäden auf einzelne Bereiche einzugrenzen. Der VPN-Zugang sei verbandsweit flächendeckend vereinheitlicht und mit einer Multi-Faktor-Authentifizierung mit One-Time-Passwort und Zertifikat abgesichert worden. Zudem komme leistungsstarke Software im Bereich Virenschutz sowie Angriffserkennung und -abwehr zum Einsatz. Die Infrastruktur werde – ebenso wie interne Strukturen und Prozesse – regelmäßig von externen Experten und Gutachtern auf Verbesserungspotenzial hin analysiert und auditiert. Für Investitionen in die IT-Sicherheit sind laut SIT für das Jahr 2025 Aufwendungen in hoch sechsstelliger Höhe kalkuliert.

Ein erneuter Angriff kann nie völlig ausgeschlossen werden. Um mögliche Auswirkungen einzugrenzen, hat SIT neben den technischen Maßnahmen auch verschiedene Prozesse auf Managementebene eingeleitet. So wurde eine Kooperation mit anderen kommunalen IT-Dienstleistern in NRW angestoßen, um einander bei der Prävention und im Falle einer Cyberattacke besser unterstützen zu können.

Handlungsbedarf auf regionaler und nationaler Ebene

Über ihre 72 Verbandsmitglieder bedient SIT über 22.000 Arbeitsplätze mit IT-Infrastruktur und mit rund 160 Fachverfahren, die nach dem Angriff ausgefallen waren. Zudem versorgt SIT weitere Kunden wie Tourismusverbände, Zweckverbände für Abfallwirtschaft, Feuerwehren und Stadtwerke mit IT-Dienstleistungen. Insgesamt waren nach SIT-Angaben rund 1,6 Millionen Bürgerinnen und Bürger von den Folgen des Angriffs betroffen. Damit war der Ransomware-Angriff auf SIT bundesweit der bisher größte und komplexeste Vorfall dieser Art.

Nicht nur deswegen sieht Mirco Pinske perspektivisch auch regionalen und nationalen Handlungsbedarf: „Die Vielfalt der Anwendungen muss reduziert werden, für gleichartige Aufgaben darf es im Verbandsgebiet auch nur jeweils ein System geben. Das würde auch im Krisenfall die Zeit bis zu einer erfolgreichen Wiederherstellung verkürzen.“ Zudem fordert er, IT-Sicherheit ganz offiziell zur Chefsache zu machen: „In der NIS2-Richtlinie verpasst der Gesetzgeber nach aktuellem Stand die Gelegenheit, eine verbindliche Gesetzesgrundlage für kommunale IT-Dienstleister zu schaffen. Die Regeln müssen klarer gefasst werden, und wir würden es begrüßen, dass auch kommunale IT-Dienstleister Gegenstand der NIS2 werden.“

(sib)

Stichwörter: IT-Sicherheit, Südwestfalen-IT (SIT), Ransomware