SIT

Ransomware-Angriff auf IT-Dienstleister

[01.11.2023] Der kommunale IT-Dienstleister Südwestfalen IT wurde Opfer eines Cyber-Angriffs. Infolgedessen sind vor allem in Südwestfalen und im Ruhrgebiet viele Kommunen nur schwer erreichbar, Verwaltungen bleiben geschlossen.

„Es ist keine Frage, dass ein Cyber-Angriff erfolgreich sein wird, die Frage ist lediglich, wann“ – dieser Satz ist fast schon ein Mantra unter IT-Sicherheits-Experten. Am Montag wurde der kommunale IT-Dienstleister Südwestfalen-IT (SIT) aus Siegen Ziel einer Ransomware-Attacke. Dadurch ist die Handlungsfähigkeit zahlreicher kommunaler Verwaltungen beeinträchtigt. Primär betroffen sind nach Angaben von SIT die 72 Mitgliedskommunen aus dem Verbandsgebiet in Südwestfalen, darunter die Landkreise Hochsauerlandkreis, Märkischer Kreis, Olpe, Siegen-Wittgenstein, Soest sowie mehrere Kommunen im Rheinisch-Bergischen Kreis und einige externe Kunden im Bundesgebiet. Die Verwaltungen können derzeit nicht auf die üblicherweise von der SIT bereitgestellten Fachverfahren und Infrastrukturen zugreifen und sind in ihren Dienstleistungen für die Bürger stark eingeschränkt.
Der IT-Dienstleister gibt an, dass in der Nacht von Sonntag auf Montag verschlüsselte Daten auf dessen Servern gefunden wurden, die auf einen unautorisierten externen Zugriff hindeuten. Unmittelbar im Anschluss hätten die Techniker noch in der Nacht mit der Analyse und ersten Schritten der Schadensbegrenzung begonnen. Dazu gehörte auch, die Verbindungen des Rechenzentrums zu und von allen Verbandskommunen zu kappen, um eine Weiterverbreitung des Erpressungstrojaners innerhalb des Netzwerks zu verhindern. SIT steht in Kontakt mit dem LKA, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie externen Sicherheitsdienstleistern, um schnellstmöglich Klarheit hinsichtlich des Ursprungs des Angriffs zu bekommen, das Ausmaß des Angriffs zu ermitteln und die Infrastruktur der SIT zu härten. Zur möglichen Dauer des Ausfalls wurden noch keine Angaben gemacht.

Auf unbestimmte Zeit geschlossen

Wie die Folgen bei den Kommunen und für Bürgerinnen und Bürger konkret aussehen, zeigt eine Meldung aus dem Märkischen Kreis. Dort bleibe die Kreisverwaltung auf vorerst unbestimmte Zeit ganz geschlossen. Zwar seien die eigenen Systeme gut vor Cyber-Angriffen geschützt (wir berichteten), vorsichtshalber habe man diese jedoch heruntergefahren, derzeit würden die Systeme und Fachanwendungen geprüft. Die Mitarbeiterinnen und Mitarbeiter seien telefonisch erreichbar, aber nicht per E-Mail. Die Homepage sei ebenfalls offline , auch Termine könnten aktuell nicht vereinbart werden. Seine Kunden bittet die Kreisverwaltung, nicht zu den Zulassungsstellen zu kommen und auch nicht in anderen Angelegenheiten das Kreishaus aufzusuchen. Ähnlich verfährt der Kreis Soest, wo nur in wenigen Bereichen die Dienstgeschäfte weiterlaufen wie bisher. Der WDR meldete, dass sich in einigen Fällen auch Zahlungen von Ämtern verzögern könnten, zudem sollen auch die Computersysteme in Krankenhäusern teilweise nicht mehr funktionieren.
Dass öffentliche Verwaltungen oder ihre Dienstleister Ziel von Angriffen durch Cyberkriminelle werden, ist inzwischen keine Seltenheit mehr. So musste im Juli 2021 infolge des Cyber-Angriffs auf die Kreisverwaltung im Landkreis Anhalt-Bitterfeld der Katastrophenfall ausgerufen werden (wir berichteten), die Landeshauptstadt Potsdam wurde 2020 und 2022 angegriffen und brauchte lange für die Aufarbeitung (wir berichteten), ebenfalls 2022 wurde der Rhein-Pfalz-Kreis Opfer einer Ransomware-Attacke, bei der auch sensible Daten gestohlen und später im Darknet veröffentlicht wurden (wir berichteten).

(sib)

Stichwörter: IT-Sicherheit, Cybersicherheit, Märkischer Kreis, Kreis Soest