Südwestfalen-IT

Angreifer nutzten VPN-Schwachstelle aus

[30.01.2024] Ein Forensik-Bericht liefert jetzt Erkenntnisse zu dem Ransomware-Angriff auf die Südwestfalen-IT im Oktober 2023. Demnach nutzten die Angreifer eine Schwachstelle in einer VPN-Lösung aus, um in das Netzwerk des IT-Dienstleisters einzudringen.

Ende Oktober vergangenen Jahres wurde der kommunale IT-Dienstleister Südwestfalen-IT Opfer einer Cyber-Attacke (wir berichteten). Nun hat das Unternehmen einen forensischen Bericht über den Tathergang vorgelegt. Zugang zum internen Netzwerk erlangten die Angreifer dem Bericht zufolge über eine softwarebasierte VPN-Lösung mit einer Zero-Day-Schwachstelle, die keine Multifaktor-Authentifizierung erforderte. Auf welchem Weg die dafür benötigten Zugangsdaten abgegriffen wurden, konnte laut Bericht nicht abschließend aufgeklärt werden. Sicherheitslücken in der Windows-Domäne intra.lan, die zentrale Systeme und wichtige Fachverfahren für alle Kunden der Südwestfalen-IT verwaltet, ermöglichten es den Angreifern, die Rechte bis zur Domain-Administrationsberechtigung zu erhöhen. Andere Domänen waren nicht betroffen.

Durch unverzügliches Herunterfahren und Isolieren der betroffenen Systeme sei es jedoch gelungen, den Angriff einzudämmen und das Schadensausmaß zu begrenzen, teilt Südwestfalen-IT weiter mit. So seien mit hoher Wahrscheinlichkeit keine Daten abgeflossen, auch die Back-ups seien nicht betroffen. Alle Sicherheitslücken konnten nach Angaben des IT-Dienstleisters beim Wiederanlaufen der Systeme geschlossen werden. Der mit den Kommunen abgestimmte Zeitplan sehe nun vor, die ersten wesentlichen Fachverfahren bis Ende des ersten Quartals dieses Jahres in den Normalbetrieb zu überführen.

„Höchste Priorität haben weiterhin die zügige Wiederherstellung und der sichere Wiederaufbau der Systeme für operative Betriebsfunktionen“, so Verbandsvorsteher Theo Melcher. „Dabei müssen wir uns auch fragen, wie es dazu kommen konnte – das sind wir unseren Kunden und allen Bürgerinnen und Bürgern schuldig.“ Zum 01. Februar 2024 beginne der neue Geschäftsführer Mirco Pinske seine Arbeit bei der Südwestfalen-IT. Zu seinen vordringlichsten Aufgaben gehöre es, den gesamten Vorfall umfassend aufzuarbeiten und die entsprechenden Konsequenzen abzuleiten, um einen Vorfall solchen Ausmaßes künftig bestmöglich auszuschließen.

„Fakt ist, dass das Rechenzentrum nicht in der Lage war, den Angriff abzuwehren“, so Theo Melcher weiter. „Die Erkenntnisse aus dem forensischen Bericht werden nun genutzt, um die Sicherheit der IT-Systeme in allen Netzwerkbereichen und Domänen weiter zu verstärken. Zugleich kann der forensische Bericht anderen helfen, aus dem Vorfall bei der Südwestfalen-IT zu lernen. Die Transparenz, die wir durch die Veröffentlichung des Berichts herstellen, nutzt allen.“

(bw)

Stichwörter: IT-Sicherheit,