Pressemitteilung

Südwestfalen-IT: Forensik-Bericht liefert Erkenntnisse zu Ransomware-Angriff – neuer Geschäftsführer der Südwestfalen IT arbeitet Vorfall auf

Siegen, 25. Januar 2024 – Am 29. Oktober 2023 wurde die Südwestfalen-IT Opfer einer kriminellen Cyberattacke. Nun legt das Unternehmen den forensischen Bericht über den Tathergang vor. Demnach konnten die Angreifer über eine VPN-Lösung eindringen und weitere Hürden überwinden, um die Ransomware auszuführen. Durch die unverzügliche Reaktion der Südwestfalen-IT wurde der Angriff erfolgreich gestoppt und das Schadensausmaß effektiv begrenzt. Es kam mit hoher Wahrscheinlichkeit zu keinem Abfluss von Daten, auch die Back-Ups waren nicht betroffen. Alle Sicherheitslücken sind beim Wiederanlaufen geschlossen worden. Der mit den Kreisen und Kommunen abgestimmte Zeitplan der Südwestfalen-IT sieht vor, die ersten wesentlichen Fachverfahren bis Ende Q1 2024 in den Normalbetrieb zu überführen. Zum 01. Februar 2024 wird Mirco Pinske neuer Geschäftsführer der Organisation – ihm obliegen auch die Aufarbeitung des Vorfalls sowie das Ableiten entsprechender Konsequenzen.

„Die Südwestfalen-IT wurde Opfer eines kriminellen, professionell ausgeführten Ransomware-Angriffs, der beträchtliche Auswirkungen sowohl auf uns als auch unsere Kunden und die Bürgerinnen und Bürger mit sich brachte. 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 beginnt der neue Geschäftsführer Mirco Pinske seine Arbeit bei der Südwestfalen-IT. Zu seinen vordringlichsten Aufgaben gehört auch, den gesamten Vorfall umfassend aufzuarbeiten und die entsprechenden Konsequenzen abzuleiten und umzusetzen. „Die Aufgabe des neuen Geschäftsführers der Südwestfalen-IT ist es, mit allen verfügbaren Mitteln dafür zu sorgen, einen Vorfall solchen Ausmaßes künftig bestmöglich auszuschließen“, so Melcher.

Angriff auf zentrale Windows-Domäne

Die ersten verschlüsselten Dateien bemerkte die Südwestfalen-IT in der Nacht von Sonntag, 29. Oktober 2023 auf Montag, den 30. Oktober 2023. Die Datei-Endung .akira weist auf die Ransomware-Gruppe „Akira“ hin. Den Zugang zum internen Netzwerk erlangten die Angreifer 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 nicht abschließend aufgeklärt werden. Laut Forensik-Bericht könnte eine Brute-Force-Attacke stattgefunden haben. Sicherheitslücken in der intra.lan ermöglichten es den Angreifern, die Rechte bis zur Domain-Administrationsberechtigung zu erhöhen. Die Aktivitäten der Angreifer konzentrierten sich auf die Windows-Domäne intra.lan, die zentrale Systeme und wichtige Fachverfahren für alle Kunden der Südwestfalen-IT verwaltet. Andere Domänen waren nicht betroffen.

Schnelle Reaktion verhinderte weitere Ausbreitung

Die Südwestfalen-IT dämmte den Angriff durch unverzügliches Herunterfahren und Isolieren der betroffenen Systeme ein. Direkt danach wurden externe, BSI-zertifizierte Cyber-Security-Experten mit der forensischen Untersuchung und dem Wiederaufbau der Infrastruktur beauftragt.

Erkenntnisse aus Forensik-Bericht bei Wiederaufbau berücksichtigt

„Fakt ist, dass das Rechenzentrum nicht in der Lage war, den Angriff abzuwehren.“ so Theo Melcher. „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."

Keine Hinweise auf Datenabfluss und Datenverlust

Bei den intensiven forensischen Untersuchungen durch die beauftragten Cyber-Security-Experten sowie dem kontinuierlichen Monitoring des Darkwebs mittels einer Spezialsoftware konnten keine Hinweise auf einen Datenabfluss oder eine Datenveröffentlichung gefunden werden. Die Datenrücksicherungen der Südwestfalen-IT sind intakt und werden den Kommunen schrittweise wieder zur Verfügung gestellt.

Weitere Maßnahmen und Zeitplan für Wiederanlaufen der Fachverfahren

Für den langfristigen Betrieb hat die Südwestfalen-IT wesentliche Änderungen in der System-Architektur geplant, um das System robuster zu gestalten und derartige Vorfälle künftig bestmöglich auszuschließen. Mit den Kreisen und Kommunen hat die Südwestfalen-IT einen Zeitplan abgestimmt. Danach werden die ersten wesentlichen Fachverfahren, die bislang im Basisbetrieb laufen, bis zum Ende des ersten Quartals 2024 in den Normalbetrieb überführt werden. Darüber hinaus werden im ersten Quartal 2024 weitere priorisierte Fachverfahren in den Basisbetrieb gehen.