Ein Jahr nach dem Hackerangriff: Südwestfalen-IT zieht Bilanz

Unternehmen sieht sich zukunftssicher aufgestellt und dankt allen Beteiligten für ihren großen Einsatz

Siegen, 30. Oktober 2024 – Genau 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, was immense Auswirkungen auf die 72 Mitgliedskommunen aus dem Verbandsgebiet hatte. In den darauffolgenden Monaten arbeiteten sowohl die Mitarbeitenden der SIT als auch 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 01. Februar 2024 Geschäftsführer der Südwestfalen-IT ist. „Unser Dank gilt allen Beteiligten für ihre unermüdliche Unterstützung bei der Krisenbewältigung – und ebenso den Bürgerinnen und Bürgern, von denen streckenweise sehr viel Geduld und Verständnis gefordert war.“

Der Krisenmodus der SIT dauerte insgesamt 11 Monate an – zum 30.09.2024 konnte die Organisation in den Normalmodus wechseln. Zum jetzigen Zeitpunkt stehen nahezu 100% 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 bzw. Wochen erreicht. Lediglich vereinzelt sind noch kleine Restarbeiten zu erledigen, teilweise steht noch Zuarbeit externer Partner aus. Zudem konnten zahlreiche weitere Dienste bereitgestellt und neu eingerichtete Zugriffe für eine dreistellige Anzahl externer Webanwendungen ermöglicht werden.

SIT für die Zukunft aufgestellt

Gemeinsam mit externen IT- und Cyber-Security-Experten hat die SIT in den vergangenen Monaten bereits zahlreiche Sicherheitsvorkehrungen in allen aktuell eingesetzten Systemen implementiert. Zudem wurden die Erkenntnisse aus dem Vorfall genutzt, um die Sicherheit der IT-Systeme in allen Netzwerkbereichen weiter zu verstärken. Um einen möglichen Schaden auf einzelne Bereiche zu limitieren, werden die Systeme bspw. noch stärker segmentiert. Der VPN-Zugang wurde verbandsweit flächendeckend vereinheitlicht und nochmals extra gesichert (Multi-Faktor-Authentifizierung mit One-Time-Passwort und Zertifikat). Mittels leistungsstarker Software wurde im Bereich Virenschutz sowie Angriffserkennung und -abwehr aufgerüstet. Für Investitionen in die IT-Sicherheit sind für das Jahr 2025 Aufwendungen in hoch 6-stelliger Höhe kalkuliert. „Zu den konkreten bisherigen Kosten des Vorfalls lässt sich aktuell noch keine verlässliche Aussage treffen“, so Mirco Pinske. „Das Geschäftsjahr 2024 ist noch nicht abgeschlossen, es liegen also noch nicht alle Zahlen vor. Bis zum Stichtag 30. September 2024 fielen Zusatzaufwendungen in Höhe von ca. 2,8 Mio. Euro an.“

Die Infrastruktur wird – ebenso wie interne Strukturen und Prozesse – regelmäßig von externen Experten und Gutachtern auf Verbesserungspotential hin analysiert und auditiert. Eine 100-prozentige Sicherheit gegen solche Vorfälle gibt es allerdings nicht, so Mirco Pinske: „Cyberkriminelle passen ihre Angriffe kontinuierlich an neue Technologien und Verteidigungsmaßnahmen an, weshalb es unmöglich ist, zukünftige Angriffe völlig auszuschließen. Unsere Systeme entsprechen dem aktuellen Stand der

Technik, und wir arbeiten kontinuierlich daran, den Schutz weiter zu optimieren.“ Damit ein möglicher erneuter Angriff nicht mehr derartige Auswirkungen hat, hat die Südwestfalen-IT neben einer Vielzahl technischer Maßnahmen auch verschiedene Prozesse auf Managementebene eingeleitet. So wurde u.a. eine Kooperation mit anderen kommunalen IT-Dienstleistern in NRW angestoßen, um einander sowohl bei der Prävention als auch im Falle einer Cyberattacke noch besser unterstützen zu können.

Perspektivisch sieht Mirco Pinske 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 NIS-2-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 NIS-2 werden.“

Größter Angriff auf kommunale Verwaltung

Der Ransomware-Angriff auf die Südwestfalen-IT war bundesweit der bisher größte und komplexeste Vorfall dieser Art. Bevor wiederhergestellte bzw. wiederanlaufende Server in Betrieb genommen wurden, zurückgesicherte Daten freigegeben wurden oder Fachverfahren wieder ans Netz gebracht wurden, mussten jeweils umfangreiche organisatorische und technische Sicherheitsanforderungen erfüllt werden. Dies erforderte Zeit und Sorgfalt.

Der Wiederanlauf der rund 160 Fachverfahren wurde gemeinsam mit den Verbandskommunen priorisiert – diese Anwendungen sind oftmals stark individualisiert, was die Komplexität erhöht und eine enge Zuarbeit von Kunden, Herstellern und externen IT-Dienstleistern erfordert. Parallel dazu mussten laufende Aufgaben erledigt und Anforderungen erfüllt werden, bspw. die Vorbereitung und Durchführung der Europawahl, umfassende Updates für hochrelevante Verfahren zu festgelegten Stichtagen (Bürgerdienste wie Einwohnermeldeamt, Standesamt etc.) sowie laufende Audits.

Auch die Zusammenarbeit in der öffentlichen Verwaltung inkl. der Abstimmungsarbeit mit Gremien, Behörden und Interessengruppen birgt eine relevante zeitliche Komponente. „Natürlich unterscheiden sich auch die internen Kapazitäten der einzelnen Verbandskommunen“, so SIT-Geschäftsführer Mirco Pinske. „Dennoch haben wir im Vergleich zu ähnlich gelagerten Fällen in anderen Kommunen Deutschlands bei höherer Komplexität weniger Zeit benötigt, bis alle Dienstleistungen wieder angeboten werden konnten.“

Der Vorfall in Zahlen

- Die Südwestfalen-IT hat **72 Verbandsmitglieder**. Diese bedient sie über **22.000 Arbeitsplätze** mit IT-Infrastruktur und mit rund **160 Fachverfahren**, die nach dem Angriff ausgefallen waren. Zudem versorgt die SIT weitere Kunden wie Tourismusverbände, Zweckverbände für Abfallwirtschaft, Feuerwehren, Stadtwerke etc. mit IT-Dienstleistungen.
- Insgesamt waren **1,6 Millionen Bürgerinnen und Bürger** von den Folgen des Angriffs betroffen.
- Der Angriff betraf **1.463 Server**, davon mussten 871 neu aufgesetzt werden und 592 vor der Wiederinbetriebnahme aufbereitet werden (umfassende forensische Prüfung, Ausstattung mit neuen Betriebssystemen und Sicherheits-Features).

- Die über **700 Daten-Backups** waren von dem Angriff nicht betroffen, mussten aber alle einzeln geprüft und wieder eingespielt werden.
- Es wurde eine hohe dreistellige Anzahl von **Verbindungen zu externen Webanwendungen** wie bspw. Online-Vergabeportalen, Plattformen zur Marketing-Automation oder dem Portal der NRW-Landwirtschaftskammer geprüft und wieder eingerichtet.
- In Summe arbeiteten rund **170 Personen** bei der Südwestfalen-IT an der Bewältigung der Auswirkungen des Cyberangriffs. Über **50 externe Partner** galten für die Krisenbewältigung als essentiell und mussten entsprechend intensiv eingebunden und koordiniert werden, darunter Behörden wie das BSI sowie Bundes-/Landesministerien, IT-Dienstleister und Forensiker, Hersteller und Hardware-Lieferanten und Auditoren.
- Insgesamt wendete allein die SIT-Belegschaft für die reine Bewältigung der Krise bei der SIT rund **43.000 Arbeitsstunden** auf. Zudem gab es **210 Austauschrunden** mit den Gremien und ähnlichen Formaten/Gruppen der Zweckverbandsmitglieder, um gemeinsam Lösungen zu finden und umzusetzen.