Interview

Wertvolle Lehren gezogen

[14.08.2024] Nach dem umfassenden Cyberangriff arbeitet der IT-Dienstleister Südwestfalen-IT an einer strategischen Neuausrichtung. Im Kommune21-Interview berichtet Geschäftsführer Mirco Pinske, wie die Aufarbeitung vorangeht und welche Konsequenzen bereits gezogen wurden

Herr Pinske, die Südwestfalen-IT (SIT) wurde im Oktober 2023 Opfer eines beispiellosen Hackerangriffs. Sie wurden im Februar dieses Jahres zum neuen Geschäftsführer bestellt – unter anderem mit der Aufgabe, den Vorfall umfassend aufzuarbeiten. Wie haben sich Ihre ersten Monate im Amt gestaltet?Eine wesentliche Aufgabe bestand für mich darin, mir zunächst ein umfassendes Bild von der Lage der SIT zu einem Zeitpunkt zu machen, in der sie noch voll auf Krisenbewältigung ausgerichtet war. Ich habe dabei großartige Mitarbeiterinnen und Mitarbeiter kennengelernt, die unter enormem Zeitdruck große Schwierigkeiten bewältigt und gezeigt haben, was sie können. Nach diesem Bewältigungssprint steht nun ein Marathon an, denn die SIT wird sich entwickeln müssen. Nach der akuten Bewältigung des Angriffs sind wir in eine neue Phase eingetreten, in der neben einer schonungslosen Fehleranalyse auch die strategische Neuausrichtung der SIT an vorderster Stelle steht. Welche Punkte haben Sie hier vor allem ausgemacht? Beispielhaft lassen sich zwei drängende Baustellen nennen: Erstens kämpft die SIT wie viele andere Unternehmen mit dem Fachkräftemangel – ein Begriff, der derzeit allzu geläufig ist, für uns aber ein zentrales Nadelöhr darstellt, das geweitet werden muss, damit wir unsere Aufgaben voll erfüllen können. So müssen wir diese zum Beispiel stärker im Sinne einer Serviceorientierung begreifen und Bearbeitungszeiten deutlich reduzieren. Um diesen Unternehmenswandel umzusetzen, investieren wir in Recruiting-Kampagnen und machen deutlich: Arbeiten für die Digitalisierung der öffentlichen Verwaltung ist nach wie vor eine immens wichtige und sinnstiftende Aufgabe, hadert aber mit einem schlechten Image von trägen Ämtern. Wir arbeiten daran, dieses Image auf unserer Seite abzulegen und zu zeigen, dass wir für unsere Kunden da sind. Zweitens werden sich strategische Überlegungen mit dem Software-Portfolio der SIT beschäftigen müssen. Denn dieses ist schlichtweg zu groß. Inzwischen bieten wir unseren Verbandsmitgliedern über 180 Fachverfahren an, das heißt, wir hosten und bieten Support für über 180 Softwareprogramme. Dieser Bestand ist historisch über die vergangenen Jahre gewachsen, auch aufgrund der Zusammenlegung zweier IT-Dienstleister zur SIT. Damit berücksichtigen wir noch heute zwar viele Sonderwünsche einzelner Kommunen, der damit verbundene Aufwand ist jedoch enorm und bindet Kapazitäten und Ressourcen, die an anderer Stelle besser investiert wären und dringend benötigt werden. Kurzum: Die Softwarelandschaft der öffentlichen Verwaltung wird sich deutlich verkleinern müssen. Das wird sich direkt auch auf eine Verbesserung der Sicherheit und des Service derjenigen Fachverfahren auswirken, auf die wir uns als Zweckverband dann einigen werden.„Neben einer schonungslosen Fehleranalyse steht die strategische Neuausrichtung an vorderster Stelle.“Damit hört die strategische Neuausrichtung vermutlich noch lange nicht auf… Nein, wir arbeiten außerdem an weiteren Maßnahmen, die für die SIT weitere Weichen stellen werden. So lassen wir uns von externen Unternehmen auditieren, um Schritte dafür abzuleiten, wie wir unsere Leistungsfähigkeit und Wettbewerbsfähigkeit nachhaltig steigern können. Außerdem werden wir in Kürze mit der Entwicklung eines neuen Leitbilds starten, das bis Ende dieses Jahres abgeschlossen sein soll. Unsere Grundhaltung ist dabei, Sicherheit als ständigen Prozess zu begreifen, eine zeitgemäße Unternehmenskultur zu etablieren und das operative Geschäft zu verbessern: mehr Service, schnellere Bearbeitungszeiträume und mehr Transparenz für unsere Kunden und Kommunen. Wie konnte es Ihren bisherigen Erkenntnissen nach überhaupt zu dem Angriff kommen

und wie konnte dieser eine derartige Wirkung entfalten? Zu den Ursachen des Angriffs haben wir zur vollen Transparenz einen umfassenden Bericht der externen IT-Experten veröffentlicht, die wir mit der forensischen Untersuchung beauftragt hatten. Die Angreifer konnten über eine Schwachstelle in einer VPN-Lösung in die Systeme der SIT eindringen, ihre Berechtigungen im Netzwerk erhöhen und so wichtige Systeme verschlüsseln und damit aushebeln. In der Folge fielen viele Softwarelösungen aus, die bei den Kommunen unseres Zweckverbands verwendet werden. Damit standen die Dienste – also die Fachverfahren – insgesamt 1,6 Millionen Bürgerinnen und Bürgern nicht mehr zur Verfügung. Der Angriff zeigt zum einen, wie wichtig die Arbeit der öffentlichen Verwaltung ist, da sie ein elementarer Bestandteil einer funktionierenden Gesellschaft und ihrer öffentlichen Ordnung ist. Er hat die Konsequenzen dessen schonungslos offengelegt, was passiert, wenn wir unsere IT-Sicherheit nicht täglich hinterfragen und optimieren: von der Auszahlung von Sozialhilfe, der Bewilligung von Aufenthaltstiteln bis hin zu der An- und Ummeldung von Wohnsitzen und vielen weiteren wichtigen Diensten waren kommunale Tätigkeiten kaum mehr möglich. Zum anderen steht die SIT nicht alleine da: Deutschlandweit hat die öffentliche Verwaltung einen großen Nachholbedarf an IT-Sicherheit, wie die zahlreichen Angriffe auf kommunale IT-Dienstleister zeigen. Diese neuralgischen Punkte gilt es in der Zukunft noch viel besser zu schützen und gegen Angriffe vorzubereiten. Von dem Angriff waren zahlreiche Kommunen im Verbandsgebiet betroffen, die monatelang keinerlei Fachverfahren nutzen konnten. Wie sind diese mit der Situation umgegangen? Der Ausfall der Systeme der SIT hat die Kommunen vor große Schwierigkeiten gestellt. Bei der Kommunikation in der Frühphase der Krise sind sicherlich Fehler gemacht worden, manches hätte besser laufen können: Prozesse mussten erst neu etabliert werden, was zunächst wertvolle Zeit gekostet hat. Dennoch haben wir versucht, den Kommunen so schnell wie möglich Behelfslösungen aufzuzeigen oder mit diesen abzustimmen. Viele weitere Workarounds fanden die Kommunen selbst. Lagen etwa Kontaktlisten noch in Papierform vor, konnte man in Teilen auf analoge „Papier und Stift“-Lösungen zurückgreifen. Bei komplexeren Dienstleistungen half die Landesregierung Nordrhein-Westfalen, die Geräte und Infrastruktur zur Verfügung stellte, auch die umliegenden Kommunen unterstützten im Rahmen von Amtshilfe. Dadurch konnten den betroffenen Kommunen funktionierende Arbeitsplätze außerhalb des Verbandsgebiets angeboten werden, was zum Beispiel die Kfz-Anmeldung als eines der ersten Fachverfahren wieder ermöglicht hat. Letztendlich standen die gesamte Krise hindurch immer die Kommunen im direkten Kontakt mit den Bürgerinnen und Bürgern. Dort, wo Behelfslösungen nicht griffen, mussten die Mitarbeitenden in den Rathäusern und Ämtern den – häufig verständlichen – Unmut abfedern und um Geduld bitten. Dafür gebührt ihnen unsere Anerkennung und ein großer Dank. Um den Kommunen in Zukunft besser helfen zu können, beginnen wir noch in diesem Jahr mit der Überarbeitung unserer Notfallpläne, um im Krisenfall schneller handlungsfähig zu sein. Das Ziel ist es, künftig die ersten Tage nach einem Angriff besser zu nutzen, um den Kommunen den Rücken freizuhalten und ein schnelleres Wiederanlaufen von Systemen zu ermöglichen. Auch das ist ein Bestandteil der strategischen Neuaufstellung der SIT. Wie ist die SIT vorgegangen, um die Kommunen auf dem Weg zum „Normalbetrieb“ zu unterstützen? Auf dem Weg zum Normalbetrieb galt es, die vielen Stationen dorthin überhaupt erst selbst zu identifizieren und zu bewältigen. Einen notwendigen Schritt stellte der so genannte Basisbetrieb im Dezember 2023 dar, mit dem als erstes die absolut essenziellen Fachverfahren wiederhergestellt wurden. Hierfür haben wir einen demokratischen Prozess etabliert und über diejenigen Fachverfahren abgestimmt, die Priorität haben sollten und welche die SIT für alle Kommunen als erstes wieder anbieten sollte. Ein heikler Moment: Denn für die Kommunen waren jeweils unterschiedliche Fachverfahren wichtig. Zudem nutzen die verwendeten Softwarelösungen häufig Schnittstellen zu anderen Programmen, sodass durch das schrittweise Anlaufen und anfängliche Fehlen wichtiger Schnittstellen die ersten Fachverfahren zunächst nur in ihrer absoluten Basisfunktionalität angeboten werden konnten. Es musste aber ein Anfang gemacht werden – und im Rückblick zeigt sich, dass die richtigen Fachverfahren

priorisiert wurden. Darüber hinaus erhielten die Kommunen regelmäßige Status-Updates und Informationen direkt von uns sowie über die kommunalen IT-Verantwortlichen, mit denen wir schon früh einen Krisenstab gebildet haben. Dieser Austausch war für die Bestandsaufnahme der in den Kommunen plötzlich entstandenen Baustellen wie auch der täglich neuen Entwicklungen bei der SIT wesentlich, da so trotz eingeschränkter Kommunikationsmöglichkeiten ein Informationsfluss aufgebaut werden konnte. Sind die Auswirkungen des Angriffs in der Zwischenzeit überall behoben? Inzwischen sind zahlreiche Fachverfahren wieder voll hergestellt und wir gehen davon aus, dass bis Oktober dieses Jahres alle Fachverfahren wieder in vollem Umfang angeboten werden können. Insgesamt sind dabei zwei Dinge hervorzuheben: Bei der Aufarbeitung des Angriffs galt immer der Grundsatz: Sicherheit vor Schnelligkeit. Das hatte einerseits zur Folge, dass sich manche Einschränkungen länger hinzogen als ursprünglich gedacht, weil wiederhergestellte Fachverfahren zunächst in kleinem Kreis bei ausgewählten Pilotkommunen getestet werden mussten. Gleichzeitig hat dies aber auch dazu geführt, dass die Fachverfahren, die ausgerollt wurden, wirklich funktionierten und auf eine sichere Basis gestellt waren. Dieser Arbeitsschritt erweist sich rückblickend als besonders wichtig, weil damit eine solide Grundlage geschaffen war, die Basisfunktionalität immer weiter auszuweiten, um einen echten „Normalbetrieb“ zu erreichen. Der zweite Punkt betrifft die relative Schnelligkeit des Wiederaufbaus der SIT-Systeme. Auch wenn die betroffenen Kommunen einige Wochen warten mussten, bis die ersten priorisierten Fachverfahren im Basisbetrieb wieder angeboten werden konnten, dauerte es bei vergleichbaren Angriffen auf die öffentliche Verwaltung in Deutschland um ein Vielfaches länger. Wie bewerten Sie also den Umgang Ihres Hauses mit der Krise? Angesichts des großen Effekts eines solchen Cyberangriffs hat die SIT – sowohl aus eigener Kraft wie auch mit der Hilfe wichtiger externer Experten – relativ schnell aus der unmittelbaren Krisenbewältigung herausgefunden. Zudem gingen keine Daten verloren, da die SIT über Back-ups verfügte, die von dem Angriff nicht betroffen waren. Sie hat die Verschlüsselung der Systeme schnell erkannt und konnte die Angreifer früh stören. Damit gibt es zwar aktuell noch Einschränkungen, diese sind aber nicht irreversibel und können nun schrittweise abgebaut werden. Bei allen Anstrengungen und Fehlern können wir heute immer noch sagen: Wir gehen davon aus, dass keine Daten abgeflossen sind. Die Daten der Bürgerinnen und Bürger sind sicher, und wir tun alles dafür, dass sich ein solcher Angriff nicht wiederholen kann. Welche Konsequenzen haben Sie aus Ihrer Abarbeitung abgeleitet, um einen Vorfall solchen Ausmaßes künftig bestmöglich auszuschließen? Der Angriff hat die SIT und die betroffenen Kommunen zwar schwer getroffen. Wir haben uns unserer Verantwortung aber gestellt und wertvolle Lehren daraus gezogen, dabei unsere IT-Sicherheit komplett aufgerollt und neu aufgesetzt. Nötige Veränderungsprozesse, die sonst womöglich Jahre gedauert hätten, wurden in Rekordzeit umgesetzt. Bei dieser „Schockmodernisierung“ sind wir davon ausgegangen, dass die Gefahr eines Angriffs hoch bleibt – eine Einschätzung, die unter anderem auch das BSI teilt und momentan die gesamte deutsche Gesellschaft herausfordert. Das Ziel muss darin bestehen, Angriffe früh zu erkennen, einzugrenzen und schnell zu unterbinden. Hierzu haben wir wichtige kurz- und mittelfristige Maßnahmen bereits umgesetzt oder arbeiten mit Hochdruck an einer Realisierung noch in diesem Jahr. Dazu gehören etwa die Etablierung einer neuen, verbesserten Netzwerksegmentierung und Systemhärtung, die Einführung besserer Firewalls, eine flächendeckend eingeführte Multifaktorauthentifizierung, die Absicherung von Nutzerkonten und weitere Maßnahmen. Darüber hinaus sind zusätzliche Investitionen geplant, die dazu dienen, die Systeme der SIT nachhaltig abzusichern, und auch in Zukunft wirksam gegen neue Angriffe schützen werden. Wie geht es nun weiter? Die nächsten Monate werden wegweisend sein und ich bin mir sicher, dass wir einen guten Weg finden werden, die SIT so aufzustellen, dass sie mit den kommenden Herausforderungen umgehen kann. Damit werden wir besser denn je aufgestellt sein, sichere Softwarelösungen für die digitale Verwaltung anzubieten. Die ersten wichtigen Schritte auf diesem Weg sind gemacht und ich freue mich darauf, unsere alten wie auch neuen Aufgaben mit neuem

Rückenwind aufzunehmen.

()

Dieser Beitrag ist in der September-Ausgabe von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit,