# Allgemeine Info Südwestfalen-IT/Angriff/ Forensik-Bericht

## Wer oder was ist Südwestfalen-IT?

Die Südwestfalen-IT ist ein kommunales Technologie-Unternehmen, das für mehrere Verwaltungen primär in Südwestfalen IT-Dienstleistungen anbietet, darunter z.B. Serverkapazitäten, E-Mail-Dienste und andere Kommunikationskanäle, Software u.a. Die Verwaltungen nutzen diese täglich und sind auf sie angewiesen, um verschiedenste Services wie das Ausstellen von Bescheinigungen, die KFZZulassung, die Veranlassung von Zahlungen etc. zu ermöglichen.

## Was genau ist passiert und wie wurde reagiert?

Die Südwestfalen-IT ist Opfer eines Cyberangriffs mit Ransomware (sog. Erpressungstrojaner) geworden. In der Nacht von Sonntag (29.10.2023) auf Montag (30.10.2023) wurden verschlüsselte Daten auf Servern der Südwestfalen-IT gefunden, die auf einen unautorisierten externen Zugriff hindeuten. Um die Weiterverbreitung der Schadsoftware innerhalb des Netzwerks zu verhindern, wurden die Verbindungen des Rechenzentrums zu und von allen Verbandskommunen und allen anderen Kunden und Partnern gekappt. Seitdem kann die Gemeinde Burbach nur in zum Teil noch immer sehr begrenztem Umfang oder vorerst gar nicht mehr auf unsere digitalen Anwendungen zugreifen. Die Erreichbarkeit über Telefon und E-Mail wurde zunächst über Notlösungen aufrecht gehalten, inzwischen ist die Verwaltung wieder über die bekannten Telefonnummern und E-Mail-Adressen erreichbar. Alle Informationen hierzu finden sich auf der eingerichteten Notfall-Homepage www.burbach-erleben.de

## Welche Ämter, Landkreise, Kommunen, Städte sind/waren von dem Angriff betroffen?

Primär betroffen sind 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 die Stadt Schwerte.

## Was hat es mit dem forensischen Bericht auf sich, der nun veröffentlicht wurde?

Der forensische Bericht legt die Umstände des Ransomware-Angriffs dar. Er wurde durch die Firma r-tec aus Wuppertal, einen vom BSI zertifizierten APT-Response-Dienstleister, im Auftrag der Südwestfalen-IT erstellt. Der forensische Bericht kann anderen helfen, aus dem Vorfall zu lernen.

## Wie konnte es zu dem Angriff kommen? Wurden alle Datenschutzrichtlinien und -standards eingehalten?

Die Umstände des Angriffs werden im forensischen Bericht dargelegt, eine Zusammenfassung der Erkenntnisse hat die Südwestfalen-IT in einer Pressemitteilung veröffentlicht. Es ist nun Aufgabe der Südwestfalen-IT, die vorgelegten Erkenntnisse auszuwerten und entsprechende Ableitungen zu treffen.

## Hat die Kommune einen Notfallplan für solche Vorfälle?

Als kleine Kommune sind die personellen, technischen und räumlichen Möglichkeiten, sich auf einen solchen Fall vorzubereiten begrenzt. Das war und ist auch der Grund, warum die Verantwortlichkeit bei in den Bereichen IT-Sicherheit und IT-Organisation größtenteils der Südwestfalen-IT (SIT) als kommunalen IT-Dienstleister übertragen wurde. Die gemeindeeigene IT-Stelle hat die SIT bei dieser Aufgabe unterstützt und hat ihr zugearbeitet. Die Einrichtung zusätzlicher / ergänzender Vorkehrungen zum Schutz vor einem Fremdzugriff auf die Systeme wären nicht zielführend gewesen, weil aufgrund der oben beschriebenen eingeschränkten Kapazitäten kein höherer Sicherheitsstandard erreicht worden wäre als den, den die SIT bieten kann. Nach dem Angriff und dem Ausfall der Systeme

konnte die Gemeinde Burbach aufgrund des hohen Engagements der IT-Stelle und weiteren Mitarbeitenden relative schnell Parallelstrukturen aufbauen, um zunächst „Insellösungen“ (von den Strukturen der SIT unabhängige PCs) mit Internetzugang über ISDN herzurichten, damit zeitnah eine Not-Kommunikation mit den Bürgerinnen und Bürgern möglich war. Auch eine Notfall-Homepage wurde binnen Kürze aufgebaut und mit Inhalt gefüllt. Darüber hinaus war/ist die Gemeinde Burbach abhängig von den Fachverfahren, die über die SIT organisiert werden.

**Welche Konsequenzen zieht die Kommune aus dem Vorfall?**

Unsere Kommune wird gemeinsam mit der Südwestfalen-IT die Erkenntnisse aus dem forensischen Bericht auswerten. Entsprechende Konsequenzen werden dann im Verband gemeinsam beraten und umgesetzt.

**Aktueller Stand/Zeitplan Wie ist der aktuelle Stand bei der Wiederherstellung der Systeme? Welche Dienste sind verfügbar bzw. nicht verfügbar? Welche Fachanwendungen/Dienste stehen zur Verfügung, welche noch nicht?**

Unsere Verwaltung kann inzwischen wieder vollständig auf überprüfte und „saubere“ Rechner und einige benötigte Basis-Dienste und -Programme zugreifen, die für einen reibungslosen Ablauf benötigt werden. Viele Fachverfahren stehen allerdings weiterhin nicht zur Verfügung. Der digitale Betrieb der Außenstellen (Familienbüro, Tourist-Information) ist weiterhin eingeschränkt, die Bibliothek ist weiterhin geschlossen.

Generell gilt: Die Südwestfalen-IT hat die Voraussetzungen für den Basisbetrieb die ersten priorisierten Fachverfahren geschaffen – diese wurden bereits schrittweise in Betrieb genommen. Dazu gehören u.a. das Passwesen, das Melderegister (An- und Ummeldungen), die Beurkundung von Geburten und Sterbefällen etc. Das Bürgerbüro und das Standesamt können ihre Services nahezu vollständig wieder anbieten.

Basisbetrieb bedeutet, dass diese Fachverfahren teilweise mit reduzierter Funktionalität wieder anlaufen – sie werden also nach wie vor noch eingeschränkt sein. Wir bitten deshalb um Verständnis dafür, dass noch nicht alle Dienste sofort wieder angeboten werden können. Es kann weiterhin zu längeren Bearbeitungszeiten und Ausfällen kommen, während wir den Rückstau der in den vergangenen Wochen angefallenen Arbeiten erledigen.

Wann und in welcher Reihenfolge welche Dienste im Basisbetrieb für die Bürgerinnen und Bürger wieder verfügbar sind, teilen wir Ihnen über unsere Kommunikationskanäle mit. Bitte nutzen Sie bis dahin ggf. weiterhin die eingerichteten Behelfslösungen.

**Wie sieht der weitere Zeitplan aus? Wann können welche Verwaltungsdienste wieder regulär angeboten werden?**

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.

Darüber hinaus hat die Südwestfalen-IT gemeinsam mit den Kommunen die Priorisierung für eine zweite Welle von insgesamt 16 Fachverfahren vorgenommen. Basierend darauf hat die Südwestfalen-IT einen entsprechenden Plan erarbeitet, der den Kommunen Mitte Januar 2024 vorgelegt und von ihnen freigegeben wurde. Sobald die internen Tests und die Qualitätssicherung mit den Kommunen erfolgreich abgeschlossen sind, werden die Verfahren – wie auch in der ersten Welle – schrittweise für den Pilotbetrieb in einigen Kommunen freigegeben. Die Südwestfalen-IT wird uns als Kommune

informieren, sobald erste konkrete Zeitpläne absehbar sind. Auf Basis dessen informieren wir dann alle Bürgerinnen und Bürger.

Wann und in welcher Reihenfolge welche Dienste im Basisbetrieb für die Bürgerinnen und Bürger wieder verfügbar sind, teilen wir Ihnen über unsere Kommunikationskanäle mit. Bitte nutzen Sie bis dahin ggf. weiterhin die eingerichteten Behelfslösungen.

**Wann wird eine vollständige Wiederherstellung aller Systeme voraussichtlich beendet sein? Wann ist mit einem „Normal-Betrieb" in den betroffenen Kommunen zu rechnen?**

Viele Hauptanliegen der Bürgerinnen und Bürger können durch den Basisbetrieb der Fachverfahren bzw. etablierte Behelfslösungen wieder bearbeitet werden. Der Zeitpunkt, ab wann ein Normalbetrieb läuft, ist derzeit leider noch nicht absehbar.

**In Kommune X kann die Dienstleistung Y schon wieder angeboten werden – warum bei anderen noch nicht? Was unterscheidet die Situation der jeweiligen Kommunen?**

Viele Kommunen im Verbandsgebiet sind unterschiedlich stark betroffen, und auch der Roll-Out der entsprechenden Fachanwendungen erfolgt schrittweise. Die verschiedenen Dienstleistungen von Kreisen, Städten und Gemeinden erfordern unterschiedliche Fachanwendungen. Deshalb gibt es bei der Wiederinbetriebnahme unterschiedliche zeitliche Abläufe und Stände.

Wann und in welcher Reihenfolge welche Dienste im Basisbetrieb für die Bürgerinnen und Bürger wieder verfügbar sind, teilen wir Ihnen über unsere Kommunikationskanäle mit.

**Warum dauert die Wiederherstellung der Arbeitsfähigkeit/der Systeme so lange?**

Bei dem Ransomware-Angriff auf die Südwestfalen-IT handelt es sich um den bundesweit größten Vorfall dieser Art bisher. Der Fall wird auch durch die hinzugezogene Staatsanwaltschaft als hochkomplex betrachtet.

Die Dauer des Wiederanlaufprozesses hängt in hohem Maß von der Art des Angriffs sowie der Größe und Komplexität des Unternehmens ab. Die Südwestfalen-IT hat 72 Verbandsmitglieder und bedient diese über 22.000 Arbeitsplätze mit IT-Infrastruktur und 160 Fachverfahren. Darüber hinaus bedient sie weitere, externe Kunden mit IT-Dienstleistungen. Bevor wiederhergestellte bzw. wiederanlaufende Server in Betrieb genommen werden oder zurückgesicherte Daten freigegeben werden können, müssen umfangreiche organisatorische und technische Sicherheitsanforderungen erfüllt werden. Dies erfordert Zeit und Sorgfalt.

In Summe arbeiten rund 170 Personen bei der Südwestfalen-IT an der Bewältigung der Auswirkungen des Cyberangriffs, unterstützt werden sie hierbei von neun externen Dienstleistern.

**Wie kann ich die Verwaltung meiner Stadt erreichen? Wo erhalte ich neue Informationen?**

Unsere Notfall-Website finden Sie unter der Adresse www.burbach-erleben.de. Dort erhalten Sie immer eine Übersicht der aktuellen Informationen. Außerdem halten wir Sie über unsere Social-Media-Kanäle auf Facebook (www.facebook.com/genmeindeburbach) und Instagram (www.instagram.com/gemeindeburbach) sowie über Veröffentlichungen in der Tagespresse auf dem Laufenden.

**Wie sieht es mit Bescheiden/Anträgen/Genehmigungen/etc. aus, die an Fristen gebunden waren und deren Fristen aufgrund des Hackerangriffs nicht eingehalten werden konnten (beispielsweise bei Bußgeldbescheiden)?**

Bei Fragen zu Einzelfällen sollte die zuständige Fachstelle kontaktiert werden.

# Individuell beantworten Datenabfluss und -veröffentlichung / Datenverlust

### Sind (personenbezogene) Daten abgeflossen? Wurden (personenbezogene) Daten im Darknet veröffentlicht? Kann eine nachträgliche Veröffentlichung personenbezogener Daten von den Angreifenden stattfinden?

Bei der forensischen Analyse durch externe, BSI-zertifizierte Cyber-Security-Experten (Firma r-tec) konnten keine Hinweise für einen Abfluss von Daten festgestellt werden. Darüber hinaus wird seit dem Vorfall das Darkweb auf Hinweise auf einen Datenabfluss beobachtet. Auch dabei konnten keine Hinweise für einen Datenabfluss festgestellt werden. Eine absolute Garantie, dass keine Daten abgeflossen sind, kann trotz allem nicht gegeben werden. Eine potenzielle Veröffentlichung von Daten bleibt möglich, wird aber durch die Firma r-tec nach aktuellem Stand für unwahrscheinlich gehalten.

### Was kann ich tun, um mich/meine Daten zu schützen?

Generell empfehlen wir Ihnen, sich in allen Online-Umgebungen sehr vorsichtig zu verhalten und folgende Empfehlungen zu beachten:

- Nutzen Sie den Empfehlungen des BSI folgend komplexe, sichere Passwörter. Nutzen Sie, wo möglich, eine Zwei-Faktor-Authentisierung (2FA), um Ihre Daten, Konten bei Online-Zahlungsdiensten, Konten bei Shopping-Anbietern etc. zusätzlich abzusichern.
- Halten Sie Ihr Betriebssystem und die Softwareanwendungen sowie den Virenschutz auf dem aktuellsten Stand.
- Seien Sie wachsam beim Öffnen von E-Mail-Anhängen, beim Anklicken von Verlinkungen sowie bei Downloads – egal, ob Sie per Mail, Social Media, Messenger-App oder SMS von unbekannten Nummern kontaktiert werden.

Umfangreiche Empfehlungen finden Sie auch auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI):

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-undVerbraucher/Informationen-und-Empfehlungen/CyberSicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoertererstellen_node.html

### Sind bei dem Angriff Daten verloren gegangen, z.B. aus wichtigen Projekten der Kommunen?

Nach gegenwärtigem Kenntnisstand können die Datenstände aus Back-Ups wieder hergestellt werden.

# Ransom Note/Lösegeld

### Wurde ein Lösegeld gefordert? Wie hoch? Wie wurde reagiert?

Die Angreifer stellten gegenüber der Südwestfalen-IT keine direkte Lösegeldforderung, sondern boten eine Kontaktaufnahme zu den Modalitäten einer Wiederherstellung und einer damit verbundenen Lösegeldzahlung an. Die Südwestfalen-IT entschied im Einvernehmen mit den Behörden, keinen Kontakt aufzunehmen. Es kommt für eine öffentlich-rechtliche Organisation nicht infrage, Geschäfte mit kriminellen Organisationen zu tätigen.

### Wäre es nicht finanziell günstiger gewesen, einfach das Lösegeld zu zahlen?

Unternehmen, die Lösegeld bezahlen, werden oft erneut gehackt. Darüber hinaus besteht auch bei Zahlung keine Sicherheit, dass alles wieder hergestellt werden kann. Und schließlich muss das System ohnehin wieder neu aufgebaut werden, um derartige Verwundbarkeiten in Zukunft auszuschließen.

### Werden die Täter zur Rechenschaft gezogen?

Die Südwestfalen-IT hat Anzeige bei den zuständigen Behörden gestellt.

## Schadensersatz/rechtliche Aspekte

### Wer haftet für den entstandenen Schaden?

Die Südwestfalen-IT wird hierzu gemeinsam mit den dem Zweckverband angehörenden Kommunen eine verbandsweite Lösung erarbeiten.

### Können/werden die Kommunen die SIT wegen mangelnder Sicherheitsvorkehrungen verklagen?

Hierzu stehen die Kommunen derzeit mit der Südwestfalen-IT im Austausch.