Ausfallsicherheit in der Zentralen Leitstelle Ostthüringen

Manfred Hofmeier · Andreas Rieb · Tamara Gurschler

Universität der Bundeswehr München
{manfred.hofmeier | andreas.rieb | tamara.gurschler}@unibw.de

Zusammenfassung

Im vorliegenden Beitrag wird die Kurzfassung einer Fallstudie zur IT-Sicherheit in Kritischen Infrastrukturen beschrieben. Gegenstand dieses Beitrags ist die IT-Sicherheit der Zentralen Leitstelle Ostthüringen im Hinblick auf Rückfallebenen und Redundanzen. Dieses Konzept ermöglicht die Sicherstellung des Alarmierungsprozesses vom Absetzen eines Notrufs bis zur Alarmierung der Rettungskräfte – auch wenn eine oder mehrere IT-Komponenten ausfallen sollten. Die vollständige Fallstudie ist in der Quelle [LDR+18] veröffentlicht sowie unter www.itskritis.de kostenfrei verfügbar.

1 Organisation

Die Stadt Gera betreibt im Auftrag des Rettungsdienstzweckverbands Ostthüringen die Zentrale Leitstelle Ostthüringen für Rettungsdienst, Feuerwehr und Katastrophenschutz in Form einer integrierten Regionalleitstelle. Diese ist nach den Leitstellen Erfurt und Jena die drittgrößte Leitstelle im Bundesland Thüringen.

Die Leitstelle ist das ganze Jahr rund um die Uhr besetzt und beschäftigt insgesamt 22 Disponenten zuzüglich drei Mitarbeitern für Führungs- und Verwaltungsaufgaben. Dabei werden jährlich über 90.000 Einsätze disponiert, darunter Einsätze von Rettungsdienst, Krankentransport, kassenärztlichem Notfalldienst und der Feuerwehr. Vorgabe ist, dass ein Anruf unter der Notrufnummer 112 innerhalb von 10 Sekunden angenommen sein muss und innerhalb von 60 Sekunden die Rettungskräfte alarmiert worden sein müssen.

Die Ausgestaltung der IT-Systeme findet dabei im Spannungsfeld zwischen bestmöglicher Anrufvermittlung, gesetzlichen Vorgaben und neuen technischen Entwicklungen statt.

2 Kritische Infrastruktur

Gemäß der Definition des IT-Sicherheitsgesetzes [Bund15] sind Leitstellen, die von Behörden und Organisationen mit Sicherheitsaufgaben betrieben werden, Kritische Infrastrukturen. Die Leitstellen können dabei sowohl dem Sektor Gesundheit als auch dem Sektor Staat und Verwaltung zugeordnet werden. Letzterer unterliegt allerdings nicht dem IT-Sicherheitsgesetz.

Ungeachtet der Gesetzeslage sehen die Mitarbeiter der Leitstelle Ostthüringen die Leitstelle als Kritische Infrastruktur.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 236-239.

3 IT-Sicherheit

Die IT-Infrastruktur der Zentralen Leitstelle Ostthüringen ist historisch gewachsen und stellt eine von der IT der Stadtverwaltung losgelöste Insellösung dar, in der IT-Sicherheit ein priorisiertes Thema darstellt. Die IT-Infrastruktur der Leitstelle ist in sich geschlossen und hat nur wenige Schnittstellen nach außen, da die meisten Kernfunktionalitäten der Leitstelle nur das geschlossene Netzwerk erfordern (siehe Abbildung 1). Dazu zählen bspw. das Einsatzleitsystem COBRA, das die Disponenten bei der Abwicklung der Notrufannahme bis hin zum Einsatzende unterstützt aber auch andere IT-Systeme wie bspw. Datenbanken zum Verwalten der Einsatzmittel, zur Dokumentation von Einsätzen, für Recherchen oder Unterstützung der Einsatzplanung mit Hilfe von Kartendiensten.

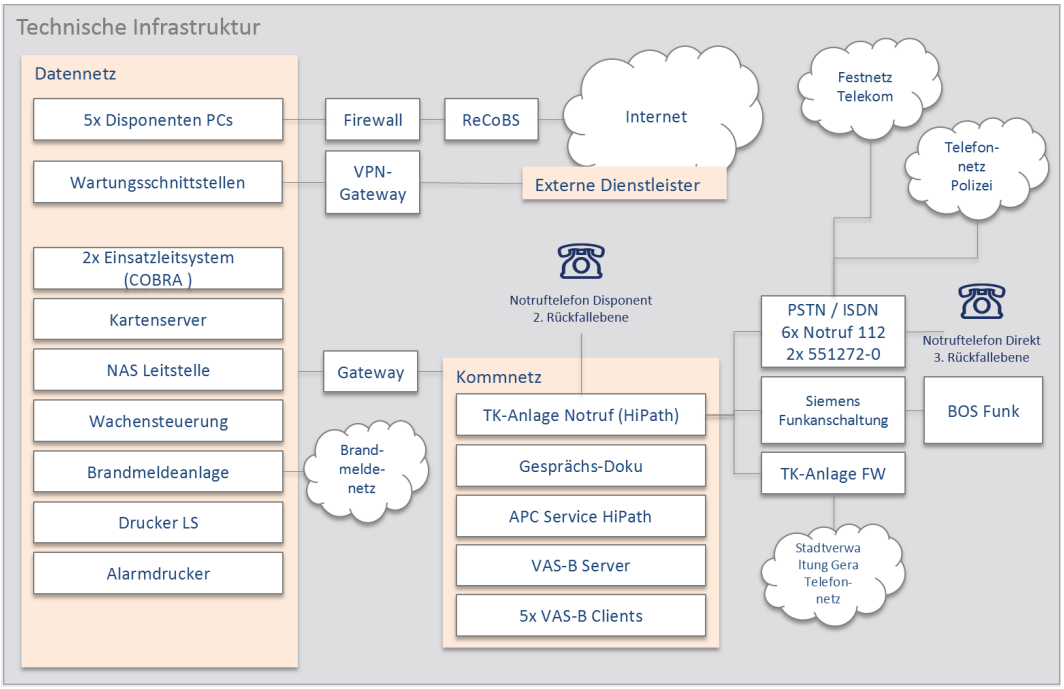

Abb. 1: IT-Infrastruktur der Zentralen Leitstelle Ostthüringen [LDR+18]

Da Ausfälle von IT-Systemen durch technisches Versagen, höhere Gewalt oder durch andere Gründe gemäß [BSI11] zum Ausfall einzelner Kernprozesse oder gar des gesamten Betriebs führen können, steht die IT-Sicherheit in der Leitstelle im Spannungsfeld mit den gesetzlichen Anforderungen, dass in nur 10 Sekunden ein Notruf spätestens entgegengenommen werden und in maximal 60 Sekunden ein Einsatzbefehl erteilt werden muss.

Diese Anforderungen stellen sowohl für den Disponenten als auch für die IT-Infrastruktur besondere Herausforderungen dar, die es einerseits mit geschulten Mitarbeitern und andererseits mit einem ausgeklügelten Konzept an Rückfallebenen und Redundanzen zu bewältigen gilt (siehe Abbildung 2).

Im Regelbetrieb stehen dem Disponenten alle Funktionen, Dienste und Geräte zur Verfügung, um dem Hilfesuchenden die bestmögliche Hilfe zu bieten. Ein eingehender Notruf per Telefon wird zu Beginn von der PSTN / ISDN-Anlage entgegengenommen und an das Kommunikationssystem HiPath weitergeleitet. Unmittelbar im Anschluss erfolgt die Gesprächsaufzeichnung, zu der Leitstellen gesetzlich verpflichtet sind. Das Kommunikationssystem HiPath stellt dann den Notruf an den VAS-B Server zur Vermittlung und Abfrage durch. Der Disponent

kann daraufhin über seinen Disponenten Arbeitsplatz-PC auf den eingehenden Notruf zugreifen, diesen annehmen und bearbeiten.

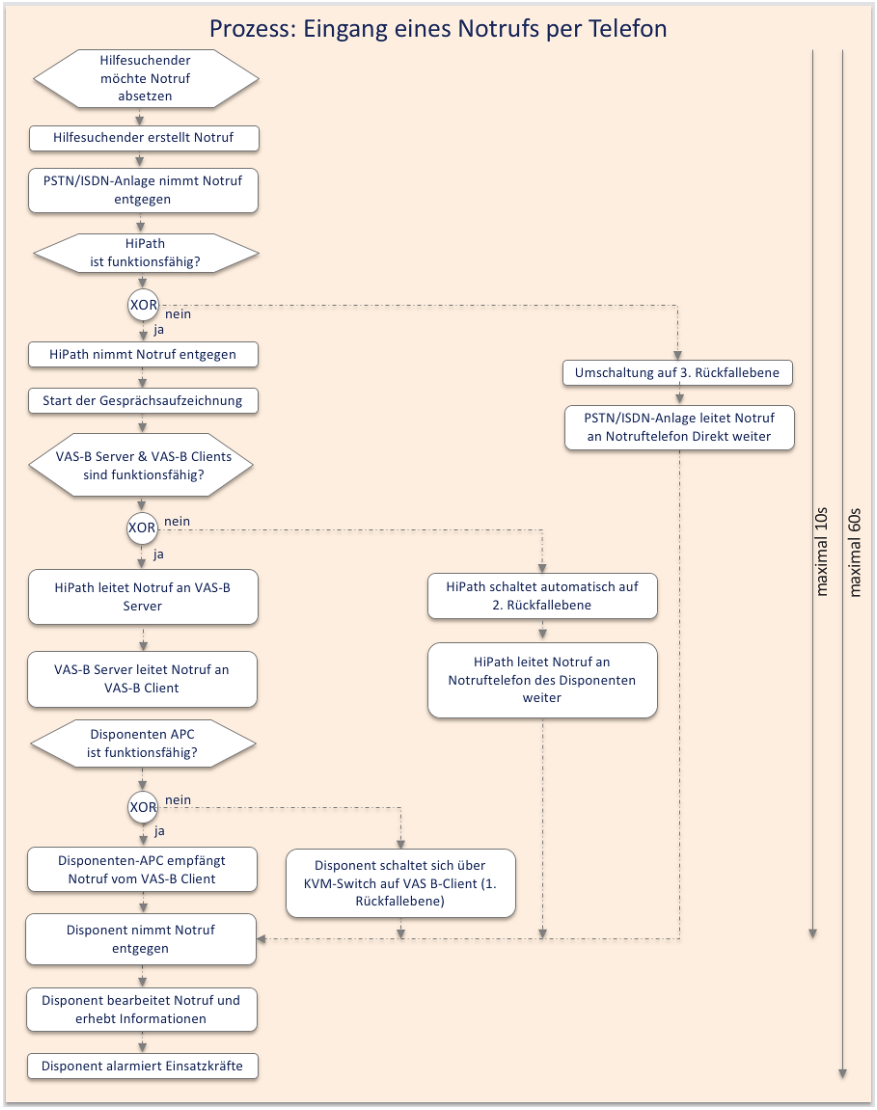

Abb. 2: Prozess zum Eingang eines Notrufs per Telefon [LDR+18]

In diesem Prozess sind mehrere IT-Systeme unterschiedlicher Hersteller beteiligt und unterliegen zudem dem Risiko, dass einzelne Komponenten oder gar ganze Systeme zeitweise oder langfristig ausfallen können. Aus diesem Grund identifizierte die Zentrale Leitstelle Ostthüringen Worst-Case Szenarien und entwickelte daraufhin ein IT-Infrastrukturkonzept, das mehrere Rückfallebenen und Redundanzen vorsieht:

- Rückfallebene 1: Für den Fall, dass ein Arbeitsplatz-PC ausfällt, kann sich der Disponent direkt auf den VAS-B Client aufschalten und den Notruf wie gewohnt entgegennehmen.
- Rückfallebene 2: Die zweite Rückfallebene sieht vor, dass im Falle eines Ausfalls des VAS-B Servers oder Clients ein Notruf per Telefon an den Disponenten zugestellt werden kann. Für diesen Fall hat jeder Disponent an seinem Arbeitsplatz ein zusätzliches Telefon, das mit der HiPath verbunden ist und im Falle des o.g. Ausfalls aktiviert wird.
- Rückfallebene 3: Die dritte Rückfallebene geht im Schadensszenario davon aus, dass die HiPath-Anlage nicht einsatzbereit ist. In diesem Fall leitet die PSTN / ISDN-Anlage den

Notruf nicht an die HiPath-Anlage weiter, sondern an ein einzelnes Notruftelefon, das für alle Disponenten in der Leitstelle bereitsteht. In diesem Szenario stehen den Disponenten die gewohnten Services, wie etwa Datenbanken, nicht zur Verfügung. Um jedoch eine funktionierende Betriebsvariante gewährleisten zu können, hält die Zentrale Leitstelle Ostthüringen eine papiergebundene Lösung bereit. Damit die Disponenten im Ernstfall eine solche Betriebsvariante reibungslos aufrechterhalten können, sind intensive Schulungen, fortwährende Weiterbildungen und praktische Übungen notwendig.

Die Gewährleistung eines reibungslosen Betriebs in unterschiedlichen Betriebsvarianten erfordert von den Disponenten eine hohe Flexibilität und Einsatzbereitschaft. Damit es jedoch (wenn möglich) gar nicht erst so weit kommt, dass die Disponenten auf eine papiergebundene Variante zurückgreifen müssen, sind die IT-Mitarbeiter stets bemüht, die Anlagen und IT-Komponenten regelmäßig zu überprüfen, zu testen und zu warten. Zudem finden in der Zentralen Leitstelle Ostthüringen regelmäßig Notfallübungen statt, in der die Rückfallebenen getestet werden, um die Funktionsfähigkeit der IT-Infrastruktur sicherzustellen.

4 Erfolgsfaktoren

Die Mitarbeiter der Zentralen Leitstelle Ostthüringen sehen sich der besonderen Herausforderung gegenüber, dass mit limitierten Ressourcen die Hochverfügbarkeit des Alarmierungsprozesses gewährleistet sein muss. Hinzu kommt, dass neue und moderne Herstellerlösungen die Komplexität der Systeme und Prozesse erhöhen.

Dass das trotz der Herausforderung gemeistert werden kann, hat mehrere Gründe. So ist es hilfreich, dass ein Einsatzleitsystem ausgewählt wurde, das Insellösungen von anderen Herstellern modular integrieren kann.

Hinzu kommen gute Strukturen und festgelegte Prozesse, die einerseits formal niedergeschrieben sind, andererseits im täglichen Ablauf gelebt werden. So kann dem Wandel in der technischen Entwicklung gut begegnet werden.

Ein wesentlicher Faktor für den sicheren Betrieb der Zentralen Leitstelle Ostthüringen ist die Bereitschaft der Mitarbeiter, über ihren Aufgabenbereich hinaus Probleme zu erkennen und Lösungen zu entwickeln. Dabei wird versucht, Probleme nicht nur zu lösen, sondern auch den zugrundeliegenden Ursachen auf den Grund zu gehen. Im Zusammenhang damit möchten die Mitarbeiter der Leitstelle ihre IT-Infrastruktur kennen und verstehen, was maßgeblich dazu beiträgt, dass die Belegschaft Probleme selbst lösen kann.

Literatur

[LDR+18] U. Lechner, S. Dännart, A. Rieb, S. Rudel: CASE KRITIS – Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen, Logos (2018).

[Bund15] Bundesgesetzblatt (2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31.

[BSI11] Bundesamt für Sicherheit in der Informationstechnik (2011): IT-Grundschutz - G 0.25 Ausfall von Geräten oder Systemen. https://www.bsi.bund. de/ DE/ Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g00/g00025.html