Eingereichte Informationen der Gewinner:innen des InfoSec Impact Award

1. Platz: Heartbeat Emergency Server

Kurzbeschreibung :
Das Notfallkommunikationssystem HeartBeat, erlaubt es innerhalb kürzester Zeit alternative Kommunikationswege und ein grundlegendes Identity & Access Management (IAM) für eine Institution bereitzustellen und mittels Notfallkontaktadressen die potentielle Nutzerschaft über Existenz und Zugangsmöglichkeiten von HeartBeat zu informieren. Ein abgesicherter, hierarchisch organisierter und somit dezentral durchführbarer Verifikationsprozess erlaubt es, die Nutzenden entsprechend vorab festgelegter Priorisierung persönlich zu identifizieren und im System freizugeben – sodass ein Unterwandern des Kommunikationssystems durch Angreifende verhindert wird.
Das System basiert auf Open-Source Komponenten: Linux-Betriebssystem, IAM KeyCloak, Mailserver mit Webmail-Client sowie Matrix-Server für sichere Direkt-Nachrichten- und Videokommunikation.
Das System ist für eine automatisierte Inbetriebnahme bspw. bei einem Cloudanbieter vorbereitet. Nach der dortigen Bereitstellung des benötigten Servers, erfolgt die Installation aller Komponenten und Konfigurationen vollautomatisiert mittels Ansible-Playbook. Der gesamte Prozess des Aufsetzens erfordert damit nur wenige Minuten und keine tiefen Systemkenntnisse der einzelnen Systeme. Die Nutzerdatenbank des IAM wird mittels Uploads eines separat vorgehaltenen Notfall-Nutzerverzeichnisses befüllt, welches neben Identitätsinformationen die Notfallkontaktadressen der Nutzenden enthält.
Der Zugang zu den Kommunikationsressourcen wird durch ein gestaffeltes Verifizierungsverfahren geschützt. Nutzende setzen ein Passwort über ein E-Mail-basiertes Verfahren und werden anschließend persönlich per Einmal-Code verifiziert. Dieser Code wird über ein bereitgestelltes Verifikationsinterface generiert und im Rahmen einer Videotelefonie-Sitzung zwischen den Nutzenden und dem Verifizierungspersonal abgeglichen.
Erst nach erfolgreicher Verifizierung erhalten Nutzende vollen Zugriff auf E-Mail-, Nachrichten- und Videokommunikationsmöglichkeiten.

Welchen Mehrwert zur Informationssicherheit konnte das Projekt leisten (Wirkung)?
HeartBeat dient der Vorbereitung auf IT-Notfälle (IT-Notfallvorsorge) und stärkt die Resilienz der Organisation. In akuten IT-Notfallsituationen, die beispielsweise mit einer vollständigen Netztrennung einer Organisation und dem Abschalten sämtlicher eigener Systeme einhergehen, kommen alle internen Kommunikationsmöglichkeiten zum Erliegen. Die Wiederherstellung einer stabilen und vertrauenswürdigen Kommunikationsmöglichkeit, die nicht von Angreifern unterwandert werden kann, ist essenziell für die Bewältigung eines solchen Notfallszenarios. Trifft ein IT-Notfall eine unvorbereitete Organisation, ist die Wiederherstellung der Kommunikationsfähigkeit mit erheblichen Aufwänden verbunden, die zu einer mehrtägigen Verzögerung der eigentlichen Notfallbewältigung führen können.
HeartBeat ermöglicht es, die Kommunikationsfähigkeit in einer IT-Notfallsituation nahezu sofort wiederherzustellen – ohne die Notwendigkeit, dauerhaft eine externe, möglicherweise kostenintensive Parallelinfrastruktur vorzuhalten. Da moderne Kommunikation auf E-Mail, Chat und Videotelefonie basiert, wurden diese Verfahren in HeartBeat integriert.
Dadurch wird das Fachpersonal entlastet, das sich im IT-Notfall mit den ausgefallenen Systemen beschäftigen muss, und erhält gleichzeitig eine interne Kommunikationsmöglichkeit für 1:1- sowie 1:n-Kommunikation.

HeartBeat kann den Nutzenden in deutlich weniger als einer Stunde bereitgestellt werden. Die Nutzbarkeit hängt dabei ebenso von der Verifikationsgeschwindigkeit ab, die jedoch durch ein hierarchisches Prinzip und entsprechende Priorisierung so optimiert werden kann, dass IT-Fachpersonal und Führungsebene unmittelbar nach Bereitstellung freigeschaltet werden können.
Durch vorbereitende Maßnahmen und Automatisierung wird die Fehleranfälligkeit in der ersten Chaosphase einer solchen Situation auf ein Minimum reduziert. Durch entsprechende Praxistests sowie die Nutzung bekannter Anwendungen ist ein schneller und unkomplizierter Rollout für die Betroffenen möglich. Da es sich um Standard-Kommunikationswerkzeuge handelt, ermöglicht HeartBeat neben der internen auch eine zuverlässige externe Kommunikation.
Zusätzlich ist die Lösung so konzipiert, dass in einem nachgelagerten Schritt, durch entsprechende Konfiguration, die bekannten regulären E-Mail-Adressen angenommen, geprüft und an die Notfallpostfächer zugestellt werden können. Dadurch wird die Erreichbarkeit über diese Kommunikationswege wieder hergestellt, und wichtige Nachrichten gehen nicht verloren.

Inwiefern ist die Lösung für andere Behörden nachnutzbar (Nachnutzbarkeit)?
Unsere Lösung HeartBeat ist für jede Einrichtung nachnutzbar und erfordert nur wenige Anpassungen und Vorbereitungen. Für den Betrieb ist eine Vereinbarung mit einem Betreiber für ein entsprechendes Linux-System als Platform-as-a-Service erforderlich. Dabei kann es sich um einen gängigen Cloudanbieter oder eine Partnereinrichtung handeln. Eine entsprechende 2nd-Level-Notfalldomain sollte bereits im Vorfeld eingerichtet und registriert sein. Zudem muss sichergestellt sein, dass ein Zugriff auf die DNS-Konfiguration möglich ist.
Zusätzlich ist ein aktueller Personendatensatz mit den notwendigen Angaben für den Import in das IAM-System bereitzuhalten. Dieser Datensatz sollte für einen priorisierten Import von IT-Fachpersonal und Führungsebene vorbereitet und entsprechend unterteilt sein. Das Importformat ist so gewählt, dass es transparent macht, welche Daten eingelesen werden.
Das Installationsskript zur vollautomatisierten Installation von HeartBeat benötigt die Zugangsdaten zum bereitgestellten Linux-Server, den Personendatensatz und den Zugriff auf das DNS-System.
Das System ist so konzipiert, dass eine Skalierung sowohl zur Lastverteilung als auch zur Leistungssteigerung möglich ist – sowohl während der Initialisierung (durch Verteilung auf mehrere virtuelle Maschinen) als auch im laufenden Betrieb (durch Zuweisung zusätzlicher Ressourcen zu einzelnen virtuellen Maschinen). Hierbei können einzelne Systemfunktionsgruppen auf separate Maschinen ausgelagert werden.
Damit ist es sowohl für kleine als auch für sehr große Einrichtungen möglich, HeartBeat zu nutzen um die konkrete Anforderung des BSI-Standards 200-4 zum Business Continuity Management zu erfüllen:
„Für den Alarmierungs- und Eskalationsprozess MUSS technisch sichergestellt sein, dass die Kommunikations- und Alarmierungstechnik auch in einem Not- oder Krisenfall zur Verfügung steht.“
Dies kann mit HeartBeat kosteneffizient und zuverlässig gewährleistet werden.

Wie wird die fortlaufende Verbesserung der Lösung sichergestellt (PDCA-Zyklus)?
Bereits im Rahmen des Proof-of-Concepts der ersten Entwurfsidee wurde die Lösung mithilfe eines Automatisierungsskripts erstellt. Dadurch kann jederzeit eine identische Konfiguration automatisch erzeugt werden. Dieser Ansatz ermöglicht eine kontinuierliche Verbesserung der Umgebung von Beginn an. Änderungen, die durch Softwareupdates der verwendeten Produkte erforderlich wurden oder als Rückmeldungen aus dem laufenden Betrieb resultierten, flossen direkt in die Weiterentwicklung ein. Begleitend zum Entwicklungsprozess konnte stets überprüft werden, ob die entsprechende Umgebung korrekt erzeugt werden kann. Auf diese Weise wurde HeartBeat kontinuierlich verbessert und weiterentwickelt, um den aktuellen Funktions- und Leistungsumfang zu erreichen.
Dieser Prozess lässt sich nahtlos fortsetzen und in einen PDCA-Zyklus überführen. Durch das wiederholte Aufsetzen sowie die schrittweise Integration von Feedback im Rahmen der agilen Entwicklung wurde der PDCA-Zyklus von Beginn an etabliert.
Derzeit muss das Deployment noch manuell gestartet werden. Zudem erfordert die Aktualisierung von HeartBeat auf neue Softwarestände der einzelnen Komponenten derzeit noch eine manuelle Durchführung, da automatisierte Tests bislang nicht implementiert sind. Die weitere Automatisierung ist jedoch als nächster Schritt geplant. Dabei wird geprüft, ob zusätzliche Optimierungen mithilfe von Standardwerkzeugen wie GitLab CI/CD realisierbar sind. Ziel ist es, stets die aktuellen Softwareversionen zu nutzen sowie potenzielle Störungen durch Konfigurationsänderungen frühzeitig durch automatisierte Tests zu erkennen und direkt zu beheben.
Darüber hinaus sind mindestens jährliche Praxistests und Übungen mit HeartBeat für verschiedene Nutzergruppen geplant. Für diese Tests sind grundsätzlich Nachbesprechungen vorgesehen, in denen Feedback gesammelt und ausgewertet wird. Identifizierte Verbesserungen und erkannte technische Defizite werden anschließend in HeartBeat integriert bzw. behoben.
Da HeartBeat vollständig auf Open-Source-Komponenten basiert, besteht die Möglichkeit, die Lösung selbst als Open Source bereitzustellen. Dadurch kann die Weiterentwicklung und kontinuierliche Verbesserung gemeinsam mit der Open-Source-Community vorangetrieben werden.

Verwendete Technologien, Softwarelösungen oder Prozesse/ Verfahrensweise:
Die hier verwendeten Technologien stammen vollständig aus der Open Source Welt und stehen unter freien Lizenzen. Es kommt Debian GNU/Linux als Basis zum Einsatz und darauf aufbauend Standard-Software aus dem Repository für E-Mail. Als IAM Lösung wird über Docker Keycloak eingebunden und ebenso Roundcube als Webmailkomponente. Auf dem System ist Matrix Synapse als Chat-System und zusammen mit Jitsi als Videokonferenzsystem installiert. Diese Softwarekomponenten werden mittels Ansible in dem entsprechenden Ansible-Playbook zusammengeführt.

- https://www.debian.org/
- https://www.keycloak.org/
- https://roundcube.net/
- https://github.com/matrix-org/synapse
- https://jitsi.github.io/handbook/docs/intro/
- https://docs.ansible.com/

Weitere Informationen zur Interoperabilität:
Als Grundlage für HeartBeat wird eine virtuelle Umgebung mit Debian Linux benötigt, welche durch verschiedene Partner bereitgestellt werden kann und kurzfristig auf dem Markt bei praktisch jedem Cloudanbieter verfügbar ist. Im aktuellen Fall wurde die Implementierung auf der Umgebung des Cloudhosters Hetzner GmbH umgesetzt und spezifisch angepasst. Dies ist durch Parametrisierung beliebig adaptierbar.
Die Lösung ist mit IAM Keycloak so ausgelegt, dass weitere Webanwendungen über die Standardschnittstellen SAML und OpenID-Connect zur Authentisierung von Personen angebunden werden können. Das ist besonders von Vorteil, wenn ein IT-Notfall für längere Zeit besteht und der Notbetrieb über diese Zeitspanne hinweg aufrechterhalten werden, aber um weitere Tools und Funktionalitäten ergänzt werden muss, um Alternativen für die ausgefallen IT-Systeme zu schaffen.

Weitere Informationen zur Skalierbarkeit:
Die hier eingesetzte Lösung ist so gestaltet, dass sie für kleine Einrichtungen auf einem einzelnen System betrieben werden kann und für größer Einrichtungen durch reine Parametrisierung auf mehrere Systeme und somit die Systemlast aufgeteilt werden kann.
Darüber hinaus wurde ein von dedizierter Hardware unabhängiger Ansatz gewählt, der rein als virtualisierte Lösung innerhalb von kürzeste Zeit und mit nur sehr kurzen Unterbrechungen bereit gestellt werden kann. Etwaige notwendigen Ressourcen (z.B. CPU Leistung, Speicherkapazität) kann so bedarfsgerecht hinzugebucht werden. Da HeartBeat in kürzester Zeit und automatisiert neu aufgesetzt werden kann, kann es beliebig oft für unterschiedliche Organisationen repliziert werden, ohne dass an zentraler Stelle Aufwände entstehen. Die Nutzung ist damit beliebig skalierbar.
Darüber hinaus ist durch die dezentrale Verifikationsmöglichkeit auch eine Skalierung im Enrollment erreichbar. Entlang einer Hierarchie oder auf Grundlage bestimmter Daten können viele Personen diesen Prozess innerhalb kürzester Zeit unterstützen.

Genutzte Sicherheitsstandards:
Die hier vorgestellte Lösung ist im Rahmen des BSI Standards 200-4 ein Aspekt des Geschäftsfortführungsplans für die Business-Continuity-Strategie.
Die Bausteine des BSI Kompendiums wurden bei der Entwicklung berücksichtigt, sofern diese zur gewählten Anwendungslandschaft passen. Hier sind die Bausteine aus OPS, APPS, SYS und NET für den Betrieb entsprechend herangezogen worden, sowie ORP für die Handhabung des IAM und CON für die Vorgehensweise.
Eine explizite Analyse und Dokumentation entlang dieser Bausteine erfolgte jedoch bisher nicht.

Link für weitere Informationen / Livebetrieb etc.:
https://www.tu-darmstadt.de/it-sicherheit/itsecurity_ueberuns/index.de.jsp

2. Platz: ISM-Bot

Kurzbeschreibung:
Bei dem ISM Bot handelt es sich um eine KI Lösung, welche das Wissen innerhalb der Informationssicherheitsorganisation bündelt, zusammenfasst und schnell verfügbar macht. Der Lösung stellen wir die umfangreichen Dokumente zur Informationssicherheit als Datenbasis bereit (bspw. das BSI Grundschutzkompendium, die internen Richtlinien zur Informationssicherheit, sowie allgemeingültige übergreifende Sicherheitsanforderungen innerhalb der BA bereit. Das KI Modell welches mit OpenSource Komponenten entwickelt wurde, gibt nunmehr die relevanten Informationen welche im täglichen Handeln benötigte zusammenfassend aus. Dies unterstützt beispielweise den Second Level support im PKI Umfeld oder bei Anfragen zur Informationssicherheit, welche uns tagtäglich erreichen. Die Anwendung ermöglicht auch entsprechende E-Mails als Antwort vorzubereiten, nachdem eine Anfrage in den BOT kopiert wurde. Die Unterstützung bringt eine signifikante Zeitersparnis mit sich, da neben der Antwort auch die Quelle mit ausgegeben wird. Weiterhin ist es möglich auf übergreifendes Wissen aus der gesamten Sicherheitsorganisation zuzugreifen, ohne das hier verschiedene Systeme oder Ablagen durchsucht werden müssen. Die Bündelung aller Sicherheitsrelevanten Informationen an einem Ort macht das auffinden effizienter. In einer weiteren Ausbaustufe soll die dezentrale Sicherheitsorganisation als erster Ansprechpartner vor Ort ebenfalls Zugriff erhalten um die Anliegen vor Ort direkt mit KI Unterstützung bearbeiten zu können.

Welchen Mehrwert zur Informationssicherheit konnte das Projekt leisten (Wirkung)?
Der „ISM-Bot“ ist eine LLM-gestützte App zum Wissensmanagement und 2nd-Level-Support für die Fachbereiche der Informations- und IT-Sicherheit.
Ein Retrieval-Augmented Generation (RAG) System wie das vorliegende bietet einen erheblichen Mehrwert für die effektive Verwaltung von internen Dokumenten und spezifischem Wissen für den Fachbereich, insbesondere wenn es darum geht, auf Informationen in einer Vielzahl von Dokumenten und Richtlinien zuzugreifen. Das System ermöglicht darüber hinaus weitere Arbeitserleichterungen wie beispielsweise die Formulierung von E-Mails anhand der generierten Antworten und weitere Möglichkeiten, die generierten Antworten mittels des Sprachmodells weiter zu verarbeiten.
Mit dem „ISM-Bot“ ersparen wir uns die zunehmende zeitliche Belastung durch das händische Durchsuchen unzähliger verteilter Dokumente sowie eine weitere Zerfaserung der zunehmend unübersichtlicher werdenden Sammlung an die.

Der Mehrwert bemisst sich daher an den folgenden Punkten:

1. Schneller Zugriff auf Informationen
Die Informationssicherheitsorganisation erfordert den Zugang zu einer Vielzahl von Dokumentationen, Richtlinien und Best Practices. Ein RAG-System ermöglicht es Fachkräften, schnell und effizient auf relevante Informationen zuzugreifen, ohne auf komplizierte Abfragemethoden, unscharfe Keywords oder händisches Durchsuchen angewiesen zu sein. Dies reduziert die Zeit, die für die Suche nach Informationen aufgewendet wird, erheblich und ermöglicht es den Fachkräften, sich stärker auf ihre Kernaufgaben zu konzentrieren.

2. Verbesserte Entscheidungsfindung und Entlastung

Durch den schnellen Zugriff auf aktuelle und relevante Informationen können Fachkräfte fundierte Entscheidungen treffen. Dies ist besonders wichtig in einem Bereich, der sich ständig weiterentwickelt und schnelle Reaktionen auf Sicherheitsvorfälle erfordert. Ein Wissensmanagement-System mit LLM-Unterstützung stellt sicher, dass die neuesten Richtlinien und Best Practices immer zur Hand und niedrigschwellig zu finden sind, was die Qualität der Entscheidungen erhöht. Häufig auftretende Fragen und Probleme kann der Bot schnell beantworten und lösen, wodurch die Fachkräfte entlastet werden.

3. Schulung und Sensibilisierung
Der Bot kann als interaktives Schulungswerkzeug dienen, das Mitarbeitende über aktuelle Bedrohungen, Sicherheitspraktiken und -richtlinien informiert. Dadurch kann der Bot das Sicherheitsbewusstsein und die Kompetenz der Mitarbeiter stärken.

4. Unterstützung bei der Einhaltung von Richtlinien und Vorgaben
Durch die Nutzung des ISM-Bots wird die Einhaltung von Sicherheitsrichtlinien und -vorgaben unterstützt, es werden menschliche Fehler reduziert und sichergestellt, dass alle Mitarbeitenden die geltenden Standards befolgen.

5. Assistenz-Fähigkeiten
Die Möglichkeit, Fragen in Alltagssprache zu stellen und präzise Antworten zu erhalten, macht das System besonders zugänglich und benutzerfreundlich. Dies fördert die Akzeptanz und Nutzung des Systems durch die Mitarbeitenden und trägt zur Effizienzsteigerung bei. Ebenso beherrscht die Applikation hilfreiche Features wie E-Mail-Formulierung.

6. Benutzerfreundlichkeit und Mehrwert von generativer KI
Indem die App in vollständiger Compliance mit den hohen Sicherheitsanforderungen innerhalb der BA und vollkommen on-premise entwickelt und betrieben wird, kann der Fachbereich generative KI dem Fachbereich für die Erleichterung ihrer täglichen Arbeit nutzen, ohne dass sich Sicherheitsbedenken durch den Betrieb von externen Cloud-Lösungen, bei Hyperscalern oder anderweitigen Sicherheitsrisiken ergeben. Somit erhalten die Mitarbeitenden eine sicher nutzbare Alternative. Durch den iterativen Entwicklungsprozess in enger Abstimmung mit dem Fachbereich und die kontinuierliche Berücksichtigung von Nutzerfeedback wurde gleichzeitig sichergestellt, dass die Anwendung möglichst stark auf die Bedürfnisse der User zugeschnitten ist.

Inwiefern ist die Lösung für andere Behörden nachnutzbar (Nachnutzbarkeit)?
Die Anwendung externalisiert, wie bei RAGs üblich, die eigentliche Wissensbasis von den Modellen. Somit lässt sie sich durch diesen modularen Aufbau sehr einfach auf andere Themenbereiche oder andere Nutzergruppen anpassen, indem das sowieso schon betriebene System entweder mit anderen Dokumenten erweitert oder je nach Nutzerbasis an eine alternative Dokumentenbasis mit anderen Inhalten angebunden wird. Diese können dann dieselben Modelle innerhalb derselben Infrastruktur nutzen und benötigen lediglich eine alternative Zugriffsmöglichkeit, z.B. in Form eines einfach zu implementierenden Frontends. Je nach Auslastung des zugrundliegenden Sprachmodells ist auch eine Verteilung der Ressourcen auf andere Use Cases denkbar, welche ebenfalls ein Sprachmodell nutzen. Somit können selbst innerhalb der Organisation gehostete Modelle optimal genutzt werden. Die Anwendung kann durch die intensiven

Qualitätssicherungsmaßnahmen weiterhin mit einem möglichst kompakten Modell genutzt werden, so dass Kosten und Energieverbrauch optimiert werden.

Es laufen bereits mit mehreren interessierten Fachbereichen Abstimmungen, um die technische Grundlage des Bots für andere Bereiche wiederzuverwenden. Auch sind die Erfahrungen sicher auf andere Behörden mit ähnlichen Anliegen übertragbar.

Die Lösung wurde mit einem klaren Fokus auf Nachnutzbarkeit und Integration entwickelt:

1. Open-Source-Basis: Der ISM Wissensbot basiert auf Open-Source-Technologien, was eine kosteneffiziente Implementierung und Anpassung ermöglicht.
2. Flexible Integration: Die Architektur erlaubt eine einfache Einbindung in bestehende Systeme und den Upload spezifischer Dokumente je nach Bedarf. So können andere Behörden den Wissensbot problemlos an ihre eigenen Anforderungen anpassen.
3. Skalierbarkeit: Der Wissensbot kann je nach Bedarf um zusätzliche Module oder Datenquellen erweitert werden, was seine langfristige Einsatzfähigkeit sicherstellt.

Wie wird die fortlaufende Verbesserung der Lösung sichergestellt (PDCA-Zyklus)?
Der Wissensmanagement-Bot ist skalierbar und anpassungsfähig, was bedeutet, dass es mit den Anforderungen der Organisation wachsen kann. Die modulare Architektur ermöglicht es, verschiedene Modelle und Embeddings auszutauschen und das System an neue Anforderungen anzupassen. Dies stellt sicher, dass das System auch in Zukunft aktuell bleibt, flexibel an neue Entwicklung innerhalb der Technologie angepasst werden kann und neue Features nach Bedarf und anhand des Feedbacks der Nutzenden hinzugefügt werden können.
Den Kern der fortlaufenden Optimierung bildet dabei die Feedback-Funktion mit integriertem Dashboard, bei der anonymisierte Statistiken über Nutzung und Performance des Bots erfasst und in einem Dashboard visualisiert werden. Somit kann die Performance der Anwendung dauerhaft sichtbar gemacht werden und Optimierungspotenziale in der Qualität frühzeitig erkannt werden.

Plan
Regelmäßige Auswertungen des Nutzerfeedbacks und der Wünsche der User stellen sicher, dass neue Features dann hinzugefügt werden, sofern sie sinnvoll und gewünscht sind. Dafür werden entsprechende Zeit- und Realisierungsplanungen erstellt und regelmäßige Refinements angesetzt. Ebenso werden die verwendeten Modelle regelmäßig auf ihre Performance überprüft.

Do
Nach Umsetzung neuer Features werden diese transparent dokumentiert und in einem ersten Schritt durch eine Backend-Evaluationspipeline überprüft. Ebenso werden die Goldstandard-Daten, welche als Vorlage für die ersten nutzerunabhängigen Qualitätstests mittels Metriken dienen, regelmäßig angepasst und anhand optimal bewerteter Anfragen aus dem freiwilligen Userfeedback erweitert.

Check

Nach Umsetzung neuer Features wird ihre Effektivität und Akzeptanz bei den Usern durch das Feedback sowie entsprechende Nutzerbefragungen überprüft. Ebenso stehen Qualitätssicherungs- und Evaluationskonzepte zur Verfügung, um entstehende Probleme möglichst schnell zu lokalisieren, beispielsweise bei Datenbasis, Retrieval, Modell oder an anderer Stelle, um möglichst schnell reagieren zu können.

Act
Das System bietet die Möglichkeit, die enthaltenen Daten kontinuierlich zu aktualisieren und anzupassen, auch seitens entsprechend berechtigter Nutzer aus dem Fachbereich durch eine entsprechende Benutzeroberfläche. Darin unterscheidet sich die Lösung auch von einem Standalone-Chatmodell wie ChatGPT, dessen enthaltene Informationen nicht extern kontrollier- oder änderbar sind. Durch die Externalisierung der Datenbasis können bei der vorliegenden Anwendung neue Dokumente einfach über das Front- oder Backend hinzugefügt und veraltete entfernt werden. Dies stellt sicher, dass das Wissensmanagement-System stets auf dem neuesten Stand ist und die aktuellsten Informationen bereitstellt. Diese Flexibilität ist entscheidend, um mit den sich schnell ändernden Anforderungen und Bedrohungen im Bereich der Informationssicherheit Schritt zu halten.
Ebenso lassen sich einzelne Komponenten des Gesamtsystems, welche sich als nicht mehr performant erweisen, unabhängig voneinander austauschen oder aktualisieren, so dass flexibel auf neue Herausforderungen reagiert werden kann.

Verwendete Technologien, Softwarelösungen oder Prozesse/ Verfahrensweise:
Die Anwendung wurde vollständig on-premise mit Open-Source-Modellen und Embeddings realisiert. Für die Implementation wurde das Python-Framework llama-index verwendet.
Kern der Anwendung sind die Komponenten Vektor-Database/Wissensbasis, das eigentliche Sprachmodell sowie das Frontend. Herzstück ist das kompakte Open-Source-LLM von Mistral AI, Mistral-Nemo-Instruct-2407 (12b). Hierbei handelt es sich um ein speziell für RAG-Anwendungen angepasstes Sprachmodell, was sich aufgrund seiner Kompaktheit (über hundertmal kleiner als GPT-4) sehr gut für den on-premise-Betrieb eignet und auf einer einzigen H100-GPU im BA-eigenen Rechenzentrum für bis zu 150 gleichzeitige Nutzerinnen und Nutzer verwendet werden kann. Das Serving der Modelle erfolgt mit einer separaten Instanz von vLLM.
Die Dokumente werden in einer separaten Pipeline vorverarbeitet, in entsprechende Abschnitte unterteilt und mit dem Open-Source-Embeddingsmodell deepset-mxbai-embed-de-large-v1 (Mixedbread AI) vektorisiert, ebenso wie an das System gesendete Anfragen. Die Retrieval-Komponente, welche die Anfragen mit den am besten passenden Dokumentenauszügen abgleicht, verwendet eine Hybridsuche (vektorbasiert und keywordbasiert mit dem probabilistischen Retrieval-Modell BM25).
Das Frontend wurde in Streamlit umgesetzt und beinhaltet eine Benutzeroberfläche, in der Fragen eingegeben und die Antworten sowie die extrahierten Auszüge aus den Dokumenten eingesehen werden können.

Weitere Informationen zur Interoperabilität:
Der Wissensmanagement-Bot ist in das Ökosystem der übergreifenden Plattform für Rechenintensive Methoden innerhalb der BA eingebunden und kann folglich trotz der in sich abgeschlossenen Architektur beispielsweise für die kombinierte Nutzung von Modellen (Serving mit vLLM) anderer Anwendungen zur Verfügung stehen. Ebenso wurden die

Erfahrungen und Erkenntnisse aus dieser ersten realisierten Anwendung dieser Art intensiv mit anderen Projektteams geteilt, welche an ähnlichen Anwendungen arbeiten, so dass die Entwicklung weiterer Systeme mit ähnlichen Voraussetzungen stark gefördert wurde.
Da die bestehende Plattform cloud-nativ aufgebaut wurde, ist auch eine spätere Übertragbarkeit in eine Cloud-Umgebung möglich, sofern Datenschutz und IT-Sicherheit gewährleistet werden können.

Weitere Informationen zur Skalierbarkeit:
Die Anwendung kann durch ihren modularen Aufbau und ihre containerbasierte Architektur mit der entsprechenden Hardware fast beliebig an entsprechende Nutzerzahlen angepasst werden. Handlungsbedarf bei der Skalierung lässt sich durch die entsprechenden Informationen aus dem Dashboard zu durchschnittlichen Antwortzeiten und Auslastungen erkennen. Durch die modulare Architektur und Containerisierung lässt sich der Bot durch die Freigabe weiterer Hardware schnell und unkompliziert an steigende Nutzerzahlen oder zunehmende Auslastung anpassen. Auch eine Skalierung in die Cloud ist denkbar (sieh auch Interoperabilität).

Genutzte Sicherheitsstandards:
Die Anwendung wurde ausschließlich on-premise realisiert und die Bereitstellung der Modelle erfolgt in der Form von safetensors. Nutzer:innen müssen für die Nutzung des Bots eine separate Berechtigung bestellen und werden mittels OAuth2-Proxy verwaltet. Die Bestellung wird überprüft und so sichergestellt, dass nur autorisierte Personen auf den Bot zugreifen können. Die KI-Lösung entspricht den geltenden Datenschutzgesetzen und hat erfolgreich eine datenethischen Risikoeinschätzung durchlaufen. Die Sicherheitsmaßnahmen werden in einem Sicherheitskonzept gemäß BSI IT-Grundschutz nachgehalten. Regelmäßige Code-Überprüfungen, Penetrationstests und interne Audits helfen uns, potenzielle Sicherheitslücken zu identifizieren und zu beheben.

Link für weitere Informationen / Livebetrieb etc.:
x

3. Platz: GA-Lotse

Kurzbeschreibung:
GA-Lotse ist eine neuartige Anwendungsplattform für den Öffentlichen Gesundheitsdienst. Dabei wurden für die Neuentwicklung bereits von Anfang an Prinzipien wie Security by design und Privacy by design konsequent berücksichtigt. GA-Lotse baut konsequent auf einer Zero Trust Sicherheitsarchitektur auf. Die Lösung ist modular und flexibel aufgebaut und kann auch in anderen Bereichen der Verwaltung nachgenutzt werden. Bisher integriert wurden fachliche Module für die Zwecke der Kinder- und Jugendmedizin (Einschulungsuntersuchung), der Hygieneüberwachung (Begehung von Einrichtungen) sowie des Infektionsschutzes (Impfberatung und Masernschutz). Bei der Entwicklung wurde besonders Wert auf einen sicheren Softwareentwicklungsprozess gelegt, der durch externe Partner durch Threat Modeling, Pen Testing sowie Cloud Security unterstützt wird. Die Anwendungen können Cloud-native auf Cloud Plattformen betrieben werden, sind aber auch in On-Premises Umgebungen nutzbar. GA-Lotse ist als verteilte Anwendung konzipiert und kommuniziert auf Basis eines Service Mesh-Ansatzes. Dabei gibt es eine harte Trennung nach Instanzen für einzelne Gesundheitsämter (bis zu 25 allein in Hessen), die wiederum in mehrere nach Anwendungszweck unterteilte Datenbankservices und Anwendungsservices unterteilt sind. Damit können unterschiedliche fachliche Konfigurationen der einzelnen Ämter auf einer Plattform abgedeckt werden. GA-Lotse ermöglicht neben der Unterstützung der Verwaltungstätigkeiten auch eine statistische Auswertung der individuellen Fachlichkeiten auf Basis eines Data Mesh Ansatzes. GA-Lotse ist vollständig als Open Source verfügbar und ist für die Nachnutzung in anderen Bundesländern (u. a. in Bayern) im Gespräch. Auf Basis von GA-Lotse werden zukünftig auch weitere fachliche Module (z. B. Trinkwasserüberwachung) entwickelt. Darüber hinaus ist auch die Anbindung weiterer Anwendungen wie landesspezifischen Frontends in Planung. GA-Lotse wird gefördert aus Mitteln der EU (NextGenerationEU).

Welchen Mehrwert zur Informationssicherheit konnte das Projekt leisten (Wirkung)?
GA-Lotse ist eine konsequente Neuentwicklung, die bereits in der Konzeption bestimmte Defizite vermeiden konnte. Der Mehrwert für die Informationssicherheit ergibt sich aus vielfacher Hinsicht:

- Durch die Nutzung eines konsequenten Zero Trust Paradigmas in allen Teilen der Anwendung konnten bisher eher nutzungsunfreundliche und selbst fehleranfällige Zugangswege über VPN entfallen, ohne dabei aber an Sicherheit zu verlieren
- Durch die grundlegend segmentierte Architektur mit mehreren Policy Enforcement Points konnte einerseits die Angriffsfläche minimiert werden sowie mehr generelle, kontinuierliche Überprüfung von Sicherheitseigenschaften im System genutzt werden
- Durch die konsequente Verwendung von Passkeys sind klassische Phishing-Angriffe, die auf das Abgreifen von Authentifizierungsinformationen abzielen, technisch nicht mehr möglich.
- Durch konsequente Nutzung eines IAMs mit einem übergreifenden Rechte- und Rollenkonzept konnte einerseits eine granulare Zugriffskontrolle geschaffen werden, die gleichzeitig auch verbindlich über verschiedene, bisher eigenständige Anwendungen genutzt wird

- Durch die nach Cloud native Prinzipien kann die Anwendung in unterschiedlichen Umgebungen (Cloud oder On-Premises) einfacher aufgesetzt, gewartet und aktualisiert werden
- Durch die Anwendung von signierten Container-Images kann die Integrität der laufenden Anwendungen kontinuierlich überwacht werden
- Durch die Integration von unterschiedlichen Policy-Informationen (Systemeigenschaften wie Browserversionen, Sessions, Zugriffsorte, etc.) kann ein besseres Monitoring über Ereignisse im System geschaffen werden
- Durch die Anwendung von Privacy und Security by Design Ansätzen ist es auch bei Kompromittierung von Einzelkomponenten nicht möglich, Allmacht über Datensätze im System zu erlangen. Dazu gehören etwa die Verteilung von Personenklardaten über mehrere Services mit getrennten Zugriffsentscheidungen, die Vermeidung von eindeutigen Identifiern an Personendatensätzen über unterschiedliche Verfahren sowie die Nutzung von 4-Augen-Prinzipien oder manuellen Freigaben bei Prozessen, die umfassende Datenabfragen ermöglichen (etwa Auskunftsanfrage nach DSGVO)
- Durch die Anwendung von verschlüsselten Logs, welche nur im 4-Augen-Prinzip freigegeben werden können, konnte einerseits der Umfang von Logging-Ereignissen erhöht werden, dabei aber gleichzeitig die Bedürfnisse von Personalvertretungen berücksichtigt werden
- Durch die konsequente Vermeidung von Endpunkten, welche alle Daten eines Fachmoduls gleichzeitig ausgeben können, ist ein möglicher Datenabfluss von Gesamtdatensätzen erschwert worden

Inwiefern ist die Lösung für andere Behörden nachnutzbar (Nachnutzbarkeit)?
GA-Lotse kann in allen Komponenten unter einer Open Source Lizenz nachgenutzt werden. Dabei stehen alle Komponenten, die keine tiefere Fachlichkeit enthalten, unter einer permissive Lizenz (Apache 2.0) zur Verfügung und ermöglichen so die Erstellung weiterer Fachlichkeiten auch über den Öffentlichen Gesundheitsdienst hinweg. Dazu gehören Komponenten für Kalenderdienste, verteilte Stammdatenverwaltung, Zero Trust Kommunikationskomponenten zur Integration in ein Service Mesh, aber auch abstrakte Softwarebibliotheken oder Frameworks. Die fachlichen Komponenten, die speziell für den Öffentlichen Gesundheitsdienst von Nutzen sind, stehen unter einer copyleft Lizenz (aGPLv3) zur Verfügung.
Für Hessen wir die Lösung auf Basis einer Infrastructure as a Service Cloud-Umgebung für die Gesundheitsämter in Hessen als Software as a Service Lösung betrieben. Ein eigenständiger Betrieb ist auf Basis jeder anderen Kubernetes- / Docker-kompatiblen Betriebsumgebung möglich.
Architektonisch erhalten (Gesundheits-)ämter erhalten die Möglichkeit, auf Basis eines eigenen IAMs bzw. eines gestellten IAMs auf Basis von Keycloak ihre jeweiligen Zugriffsrechte zu verwalten, sowie ihre Daten für sich isoliert beizubehalten. Damit sind auch eigenständige Konfiguration pro Amt möglich, die aber Sofware-seitig zentral gepflegt und gewartet werden können.
Auf Basis der Softwareplattform ist auch die Integration eigener Services und Module möglich.
Durch vollständiges Offenlegen von Quelltext und Dokumentation, sowie Bereitstellung aller Schnittstellen als OpenAPI sind Anpassungen und Erweiterungen, aber auch Anbindungen an Fremdsysteme vereinfacht möglich. Um ein gleichmäßig hohes

Sicherheitsniveau der Anbindung von weiteren Schnittstellen zu ermöglichen, bietet GA-Lotse nach Zero Trust Prinzipien aufbauende Trust Clients zur Anbindung weiterer Services mit gleichem Sicherheitsniveau an das Service Mesh, um Maschinen-zu-Maschinen-Kommunikation abzusichern. Dadurch kann auch mit heterogenen Schnittstellen ein gleich hohes Sicherheitsniveau der Authentifizierung und Autorisierung aller Anwendungen erreicht werden, immer mit beidseitig authentifizierten Schnittstellen mittels mTLS.
Sofern das mit GA-Lotse bereitgestellte IAM genutzt werden, werden die Anmeldeverfahren für Benutzende konsequent auf passwortlose Authentifzierung mittels Passkeys / FIDO2 umgestellt und erhöhen damit die Phishingresistenz der Anwendung.
GA-Lotse löst damit zwei Probleme: Für die Authentifizierung werden kryptografisch sichere Verfahren zum Nachweis von Identitäten von Maschinen oder Personen verwendet (Zertifikate oder Passkeys), die ein Abgreifen von Credentials stark erschweren bzw. ein Angreifen von Verbindungen mittels Maschine in the Middle Angriffe sehr stark erschweren.
Gleichzeitig wird durch den vereinfachten Aufbau der Netzarchitektur durch den Wegfall der Notwendigkeit von VPN-Lösungen, aber auch dem Vermeiden von nicht nutzungsfreundlichen 2FA-Verfahren zur Anmeldung Frust bei Benutzenden vermieden. Durch Kontinuierliche Evaluierung von Sicherheitseigenschaften bei jedem Zugriff wird darüber hinaus auf Basis des Zero Trust Paradigmas die Sicherheit kontinuierlich erhöht.

Wie wird die fortlaufende Verbesserung der Lösung sichergestellt (PDCA-Zyklus)?
Bereits bei der initialen Konzeption und Architektur von GA-Lotse wurde ein konsequenter PDCA-Zyklus angewandt. Aufbauend von einer grundlegenden Bedrohungsanalyse der Software- und Betriebsumgebungen wurden mittels eines Threat-Models entsprechende Risiken für alle Assets bewertet und mögliche Verbesserungspotenziale evaluiert.
Dies wurde in der Risikoanalyse durch sowohl durch eine entwicklungsinterne Bedrohungsanalyse durch Unterstützung des Entwicklungsteams durch externe Experten als auch von durch die Auftraggeberin beauftragte Risikomodellierung validiert. Dabei wurden auch Bedrohungen unter Einsatz anspruchsvoller Mittel mit umfangreichen Ressourcen und hoher Motivation bewertet.
Das Threat Model und die Risikobewertung dienen auch als Grundlage für eine Bewertung der technischen Restrisiken für die Abschätzung im Rahmen einer Datenschutzfolgeabschätzung.
Die konkrete Umsetzung wird iterativ begleitend durch interne Security-Expertise (dedizierte Expert*innen im agilen Entwicklungszyklus) sowie bei dedizierten Themenbereichen wie Cloud Security durch externe Expertise sicherheitstechnisch kontinuierlich fachlich begleitet, einen sicheren Softwareentwicklungszyklus garantieren zu können.
Dazu werden in der Entwicklung bestimmte automatisiert testbare bösartige Testszenarien abgeprüft (unauthorisierte Endpunkte, Korrektheit von Logs, etc.).
Für externe Abhängigkeiten in Softwarekomponenten werden Software Bill of Materials sowie automatisierte Abhängigkeitenscanner eingesetzt, um Software kontinuierlich aktuell zu halten sowie die aktuelle Risikobetroffenheit kontinuierlich beurteilen zu können.
Gegen Ende von wichtigen Projektphasen werden Komponenten dediziert einem Pentest unterzogen. Dies geschieht auch integriert zur Validierung von erkannten Restrisiken aus der Prüfung im Threat Model. Im Laufe der Weiterentwicklung und des Betriebs werden dann in wiederkehrenden Abständen Pentests für das Gesamtsystem (Software und Betriebsumgebung) kontinuierlich alle 6 bis 12 Monate durchgeführt.

Dieses generelle Entwicklungsmodell aus Risikoanalyse, sicherem Softwareentwicklungszyklus, Pentesting sowie kontinuierlicher Überwachung von Abhängigkeiten wird auch bei Erweiterungen und Anpassungen der Software angewandt.

Verwendete Technologien, Softwarelösungen oder Prozesse/ Verfahrensweise:
Backend: Java, PostgreSQL, Spring Boot, Hibernate, liquibase
Frontend: node.js, next.js
Betrieb: Docker, Kubernetes, Sigstore
Wichtige Drittkomponenten: Keycloak, nginx
Supply-Chain: Dependency-Track

Weitere Informationen zur Interoperabilität:
GA-Lotse verwendet in allen APIs offene Schnittstellendokumentationen (openAPI)
Fachspezifisch werden im Austausch mit anderen Anwendungen Profile auf Basis von FHIR (Gesundheitsbereich) genutzt, Nutzung von FIT-Connect in Vorbereitung
Nutzung von BundID und Mein Unternehmenskonto als externe Identity Provider
Nutzung des Matrix-Protokolls für Chatanwendungen

Weitere Informationen zur Skalierbarkeit:
Anwendung komplett über Kubernetes orchestrierbar und skalierbar:

- Neue Instanzen können einfach hinzugefügt
- Ressourcen oder Module von Instanzen können einfach konfiguriert werden
- Instanzen lassen sich aber über gemeinsame zentrale Dienste vernetzen

Genutzte Sicherheitsstandards:

- Theat Model nach OVE EN IEC 62443-3-2
- DIN EN IEC 62443-3-3 (VDE 0802-3-3):2020-1
- Detail Threats nach STRIDE Systematik
- IS-Penetrationstest nach Vorgehenempfehlung des BSI
- Sicherheitskonzept auf Basis BSI-IT-Grundschutz in Umsetzung
- Datenschutzfolgeabschätzung nach Standard-Datenschutzmodell 3.0

Link für weitere Informationen / Livebetrieb etc.:
www.ga-lotse.de