Bild: Thorsten Hübner

Dubios digitalisiert

c't deckt auf: Kritisches Sicherheitsleck bei Rettungsdienst-System IVENA

Über die Plattform IVENA koordinieren Rettungsleitstellen und Krankenhäuser die Versorgung von Notfallpatienten. Durch mehrere leicht vermeidbare Fehler beim Entwicklerteam landete ein Admin-Kennwort im Klartext im Netz. Eine Sabotage hätte Menschenleben gefährdet. Doch neben leicht behebbaren technischen Problemen offenbarte sich ein organisatorischer und juristischer Flickenteppich bei dieser kritischen Infrastruktur.

Von Jan Mahn

Wenn der Rettungsdienst kommen muss, entscheiden oft Sekunden – ist der Patient erst einmal untersucht, steht oft der zügige Transport in ein Krankenhaus an. Am besten in eines, das ihn auch aufnehmen und bestmöglich versorgen kann. Weil die Fahrt in eine überfüllte oder nicht richtig ausgestattete Notaufnahme nicht nur teuer, sondern schlimmstenfalls sogar lebensbedrohlich sein kann, verlassen sich viele Rettungsleitstellen und Krankenhäuser mittlerweile auf Software und vernetzte Systeme.

Ein solches System heißt IVENA, die Abkürzung steht für „Interdisziplinärer Versorgungsnachweis". Die Krankenhäuser tragen in das Onlinesystem ihre Ressourcen ein – also zum Beispiel Kapazitäten in der Notaufnahme, Ärzte nach Fachbereichen und Diagnosegeräte. Die Mitarbeiter im Rettungsdienst, die den Patienten vor Ort untersucht haben und einen Platz im Krankenhaus brauchen, geben der Rettungsleitstelle per Funk oder Handy einen sechsstelligen Code, den PZC-Code, durch. Die ersten drei Ziffern kodieren das Leiden des Patienten, die folgenden beiden Ziffern das Alter, die letzte Ziffer die Dringlichkeit. IVENA zeigt dann für den Einzugsbereich freie Krankenhäuser mit der für den Patienten passenden Ausstattung an. Der Disponent in der Leitstelle wählt eine Klinik aus, meldet den Patienten dort an und gibt den Namen des Krankenhauses an den Rettungsdienst durch. In der Datenbank von IVENA wird vermerkt, dass der Patient auf dem Weg ist und eine Ressource für die nächste Zeit blockieren wird.

Auch im Krankenhaus läuft IVENA, nicht nur auf PC-Arbeitsplätzen, oft auch als großer Informationsbildschirm in der Notaufnahme. Das Personal sieht dort in einer Tabelle, welche Patienten gerade auf dem Weg sind, kann sich vorbereiten und dringliche Fälle priorisieren. Über verschiedene Schnittstellen kann IVENA zusätzliche Alarme auslösen, zum Beispiel per Pager oder über die Telefonanlage des Krankenhauses.

Die ursprüngliche Idee zu IVENA stammt aus Hessen. Zusammen mit dem Frankfurter Gesundheitsamt entwickelt die Firma mainis IT-Service GmbH die Software seit 2009. Vertrieben wird sie mittlerweile in ganz Deutschland. Teilweise bestellen und betreiben einzelne Kommunen eine IVENA-Instanz, in vielen Bundesländern (etwa in Niedersachsen, Berlin, Brandenburg, Sachsen-Anhalt und Hessen) laufen Plattformen flächendeckend oder fast flächendeckend.

Das Programm läuft im Browser, und jeder Kunde, also eine Kommune oder ein ganzes Bundesland, muss seine Server-Instanz selbst betreiben – meist in Rechenzentren der öffentlichen Hand. IVENA generiert aus den gemeldeten Kapazitäten und den Fällen eine tabellarische Übersicht nach Krankenhäusern und zeigt nach einem Ampelsystem an, wie ausgelastet die Einrichtungen pro Zeitabschnitt sind. Diese Übersicht kann man in vielen IVENA-Instanzen als Bürger ohne Zugangsdaten einsehen. In Niedersachsen etwa unter ivena-niedersachsen.de, in Hessen unter ivena-hessen.de. In München haben die Betreiber diesen öffentlichen Zugang 2018 sperren lassen, nachdem Datenjournalisten des Bayerischen Rundfunks anhand der frei verfügbaren Daten unbequeme Details zur Versorgungslage und zur Überlastung des Krankenhauspersonals recherchiert hatten (siehe ct.de/y7xw).

Generalschlüssel ohne Schutz

Auf IVENA aufmerksam wurden wir durch den Hinweis eines Lesers. Er hatte die

Software in einer TV-Reportage des Norddeutschen Rundfunks über den Rettungsdienst gesehen (Video siehe ct.de/y7xw). Im Browserfenster eines Leitstellencomputers aus Hannover, das im Film zu sehen war, fiel ihm ein verdächtiges Detail auf: An die Adresse ivena-niedersachsen.de war eine kryptische Zeichenkette angehängt, offensichtlich eine sogenannte Session-ID. Das erinnerte den Hinweisgeber an die Anfänge der Webentwicklung: Bis etwa Anfang der 2000er war es üblich, auf Websites, die mit einer Authentifizierung versehen sind, nach erfolgreicher Anmeldung eine solche Zeichenkette an die Adresse anzuhängen. Darüber konnte der Server die Sitzung des Nutzers wiedererkennen. Von diesem Konzept haben sich Webentwickler aber lange verabschiedet. Das Problem: Eine solche URL, also inklusive des Schlüssels für eine aktive Sitzung, landet zum Beispiel im Verlauf des Browsers oder Nutzer verschicken die URL versehentlich an andere. Wer den Link bekommt, ist automatisch angemeldet. Stattdessen speichert man die Session-ID heutzutage in Cookies.

Wer ein solch antiquiertes Sicherheitskonzept verwende, so der Gedanke des Hinweisgebers, könnte noch weitere Sicherheitsprobleme aus längst vergangenen Tagen mitschleppen. Also schaute er sich die Anwendung aus Niedersachsen, die er im Film gesehen hatte, genauer an. Außerdem sah er sich auf der Homepage des Herstellers um. In einem leicht aufspürbaren Pfad wurde er fündig: Der Betreiber hatte versäumt, auf dem Apache-Webserver das sogenannte Directory Listing abzustellen. Auch das ist ein typisches Relikt aus vergangenen Zeiten. Navigierte man auf den Pfad eines Ordners, zeigte der Server eine Übersichtsseite über dessen Inhalte. Per Links konnte man darin bequem navigieren. Auf diese Weise fand unser Leser eine INI-Datei, die außer einigen Einstellungen auch einen Benutzernamen und ein Kennwort enthielt; laut Kommentaren war der Zugang für eine Entwicklungsinstanz von IVENA gedacht. Kurzerhand probierte er die Daten auf der niedersächsischen Plattform aus – und war angemeldet. Mit dieser Erkenntnis wandte er sich besorgt an unsere Redaktion.

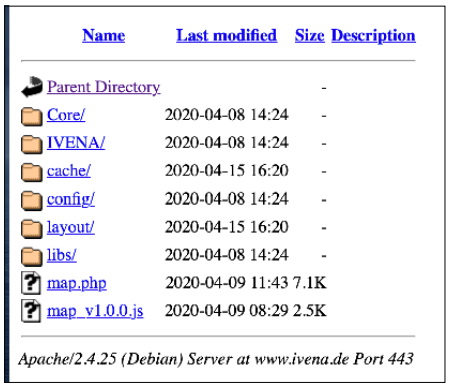
Der gefundene Account durfte so ziemlich alles auf der Plattform – er war Administrator mit vollen Rechten zur Benutzer- und Krankenhausverwaltung. Er durfte also nicht nur Patienten anmelden, wie es ein Mitarbeiter der Rettungsleitstelle darf, sondern auch ganze Krankenhäuser abmelden, anlegen und Kennwörter anderer Nutzer ändern. Der Schaden, den ein übelgesinnter Finder der Zugangsdaten hätte anrichten können, wäre gewaltig. Plötzlich wären viele Rettungsleitstellen in Niedersachsen von einem wichtigen Werkzeug abgeschnitten gewesen, die Bildschirme in unzähligen Notaufnahmen hätten nur noch Fehler oder manipulierte Daten angezeigt. Ein solcher Ausfall oder eine Sabotage hätten schlimmstenfalls Menschenleben gefährden können. Wie uns die Entwickler später bestätigten, hatte der gefundene Account auch in allen anderen IVENA-Instanzen in Deutschland volle Zugriffsrechte.

Personenbezogene Daten wie Alter, Diagnose und Geschlecht, die sich in den Datensätzen fanden, konnten keinem konkreten Patienten zugeordnet werden – Namen, Adresse oder Geburtsdaten werden in IVENA nämlich nicht erfasst. Einsehbar waren dagegen die Kontaktdaten aller Benutzer, also dienstliche Kontaktdaten von Ärzten, Mitarbeitern der Leitstellen und den Notaufnahmen. Diese Daten findet man aber überwiegend auch auf den Homepages der Krankenhäuser.

Flächendeckendes Problem

Diese Erkenntnisse waren mehr als besorgniserregend. Gespräche mit Personal aus einer Notaufnahme bestätigten unsere Einschätzung, dass ein Ausfall oder Manipulationen im Krankenhausalltag verheerend sein könnten. Großen Schaden, so das Ergebnis unseres Gesprächs, hätte der Admin-Account auch mit dem Modul „MANV“ anrichten können. Damit kann man einen „Massenanfall an Verletzten“ in einer Region anmelden – wie etwa bei einem Zugunglück oder Flugzeugabsturz.

Mit diesen Informationen kontaktierten wir sofort die Entwicklerfirma mainis IT und wiesen darauf hin, dass auch alle Nutzerkennwörter potenziell geändert werden müssten. Schließlich hatte der betroffene Account das Recht, diese zurückzusetzen oder Rechte zu bearbeiten.



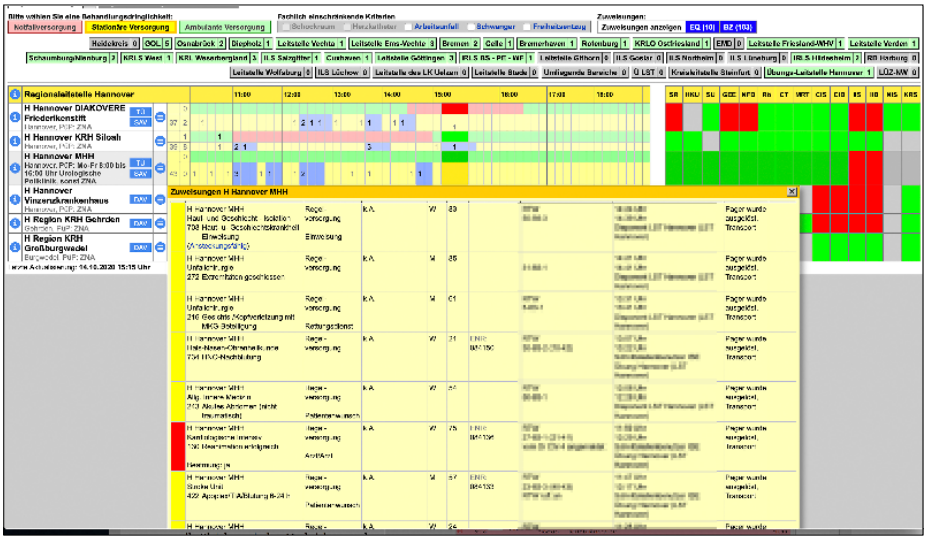
Name	Last modified	Size	Description
Parent Directory		-	
Core/	2020-04-08 14:24	-	
IVENA/	2020-04-08 14:24	-	
cache/	2020-04-15 16:20	-	
config/	2020-04-08 14:24	-	
layout/	2020-04-15 16:20	-	
libs/	2020-04-08 14:24	-	
map.php	2020-04-09 11:43	7.1K	
map_v1.0.0.js	2020-04-09 08:29	2.5K	

Apache/2.4.25 (Debian) Server at www.ivena.de Port 443

Einer der folgenschweren Fehler: Der Webserver der Entwickler lieferte eine Übersichtsseite für Ordner aus. So konnte man die Datei mit dem Kennwort leicht finden.

Technische Fehler

Das Unternehmen reagierte zügig. Am späten Abend, etwa fünf Stunden nach unserem Hinweis, bekamen wir die Information, dass das Kennwort geändert und der Fehler in Apache beseitigt sei.



IVENA stellt die Auslastung der Krankenhäuser unter anderem in Tabellen mit Ampelfarben dar. Die Zuweisung von Patienten auf Krankenhäuser soll damit effizienter werden.

In einem längeren Gespräch mit mainis IT gab ein Mitarbeiter am nächsten Tag die Fehler unumwunden zu und sprach gleich in mehreren Punkten von völligem menschlichen Versagen. Falsch sei es gewesen, einen Super-Admin-Account anzulegen, in allen Instanzen dasselbe Kennwort zu verwenden, dieses noch im Klartext irgendwo zu hinterlegen und den Apache-Server dann noch so falsch zu konfigurieren. Das Kennwort gelangte im April 2020 auf den Webserver, nachdem das Unternehmen – nach eigenen Angaben mit letzter Kraft – ein Modul für die Covid-19-Bettenauslastung fertiggestellt und auf Wunsch der niedersächsischen Landesregierung noch eine öffentliche Auslastungskarte implementiert hatte. Die Konfigurationsdatei mit dem Kennwort gehörte zu ebendieser Kartenschnittstelle.

Dieser Zeitdruck und die besonderen Umstände sollen, so der Verantwortliche, das Versagen keinesfalls entschuldigen und höchstens etwas erklären. Die zahlreichen individuellen Fehler, etwa ein Kennwort für alle Instanzen und das Directory Listing, seien unter keinen Umständen zu entschuldigen. So viel Offenheit und Ehrlichkeit nach Hinweisen auf Sicherheitslücken ist nicht alltäglich.

Auch die weiteren Maßnahmen waren vorbildlich: Mainis IT veröffentlichte eine ausführliche Stellungnahme auf der Homepage ivena.de und per Rundschreiben an alle Nutzer-Accounts mit dem Hinweis auf einen möglichen Vorfall nach Artikel 33 der DSGVO. Demnach wurde am 16. Oktober auch der hessische Landesdatenschutzbeauftragte informiert. Uns gegenüber berichtete man außerdem, eine ausführliche Analyse aller Logfiles in allen Instanzen durchgeführt zu haben. Jeder Schreibvorgang wurde protokolliert, sodass sich alle Aktionen des Admin-Accounts seit April zurückverfolgen ließen. Der Account habe nirgendwo Schaden angerichtet und keine Kennwörter anderer Nutzer geändert. Überdacht werde auch die Anmeldung – alle Benutzer-Accounts, die andere Benutzer verwalten können, sollen in Zukunft verpflichtend mit einem zweiten Faktor (TOTP oder FIDO2) gesichert werden. Arbeiten daran hätten bereits begonnen.

Organisatorisches Versagen

Die akute Gefahr war damit gebannt und wir sahen uns das IT-Projekt aus organisatorischer und rechtlicher Sicht an. Dabei fanden wir allerlei Merkwürdiges.

Die Instanz ivena-berlin.de zum Beispiel wird von ekom21 betrieben, einer öffentlich-rechtlichen Körperschaft aus Hessen. Diese Plattform nutzen, darauf deuten zumindest die Logos im Kopfbereich der Seite hin, neben Berlin auch Sachsen-Anhalt und Brandenburg mit. Das Impressum stammt aus einem Online-Impressum-Generator, die Seite mit der Datenschutzerklärung war bis Redaktionsschluss einfach leer. Als Betreiber wird im Impressum ekom21 genannt – die uns auf Anfrage aber schriftlich mitteilten, inhaltlich nicht verantwortlich zu sein und nur das Hosting zu übernehmen. Wer dann verantwortlich ist? „Nach unserem Kenntnisstand wurde die Anwendung in Berlin zentral über die Senatsverwaltung eingeführt“, so ekom21. Auch die Berliner Charité als angeschlossenes Krankenhaus ist sich keiner Verantwortung bewusst. Auf Anfrage heißt es: „Es handelt sich bei IVENA um ein Projekt der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung, weshalb wir Sie bitten möchte, sich bezüglich Ihrer Fragen dorthin zu wenden.“ Hier hat sich ganz offenkundig niemand mit den organisatorischen Fragen des Projekts beschäftigt und vorab sicher keine Rechtsabteilung konsultiert.

Wie uns mainis IT beschrieb, ging die Initiative in einigen Bundesländern oft von einzelnen Krankenhäusern aus, die im Einzugsbereich einer Rettungsleitstelle eine gemeinsame Plattform betreiben wollten und IVENA oft auch bezahlen. In Niedersachsen hat zum Beispiel das Gesundheitsministerium die Plattform als Pilotprojekt für einzelne Kreise aufgesetzt, wie aus einem Bericht auf dessen Homepage hervorgeht; an diese Instanz haben sich dann immer mehr Krankenhäuser angehängt. Die Digitalisierung verlief hier also, untypisch für staatliche Projekte, von unten nach oben und ohne Vergabe-, Prüf- und Genehmigungsverfahren recht hemdsärmelig. Das Klinikum Region Hannover schrieb uns auf unsere Fragen nach der Zuständigkeit: „Das KRH hat mit hannIT einen Auftragsdatenverarbeitungsvertrag geschlossen, in dem die Verantwortlichkeit für die Datenübertragung und -verarbeitung im Rahmen von IVENA beim KRH verbleibt.“ Einen solchen Vertrag sollte jeder mit seinem Hoster abschließen. Die Frage der Zuständigkeit beantwortet das aber nicht. Die hannIT findet sich im Impressum als Betreiber und in der Datenschutzerklärung als Verantwortlicher, bezeichnet sich auf unsere Anfrage aber lediglich als Hoster. Als Verantwortliche sieht man „die in Niedersachsen an das IVENA-System angeschlossenen Krankenhäuser und Leitstellen“.

Kern des organisatorischen Problems ist eine komplizierte Drei- oder Viereckbeziehung zwischen Krankenhäusern, Kommunen mit den Rettungsleitstellen, Rechenzentrum und teilweise dem Bundesland. Irgendwo in diesem Konstrukt fehlt es an klaren Verantwortlichkeiten, die für ein solches Projekt nötig gewesen wären. Auch Sicherheits-Audits oder Maßnahmen wie eine Zweifaktor-Anmeldung wurde von den Kunden nicht systematisch eingefordert. Anders als das technische Problem eines veröffentlichten Kennworts, das vom Entwickler zügig behoben wurde, dürfte das Entknoten dieses rechtlichen Konstruktes die Betreiber und Beteiligten in Krankenhäusern und Landkreisen deutlich länger beschäftigen. *(jam@ct.de)*

Wer hier zuständig ist, ließ sich nicht ergründen. Die Plattform nutzen Berlin, Brandenburg und Sachsen-Anhalt. Betreiber ist laut Impressum das Rechenzentrum ekom21 – die sich selbst auf Anfrage aber nur als Hoster bezeichnen.

Stellungnahme und Dokumente:
ct.de/y7xw