**Entwickler-Fehler**

# Magazin findet Sicherheitslücken bei Rettungsdienst-Infrastruktur IVENA

**Über die Plattform IVENA koordinieren Rettungsleitstellen und Krankenhäuser die Versorgung von Patienten. Das IT- und Tech-Magazin „c't" hat das System unter die Lupe genommen – mit erschreckenden Ergebnissen.**

Nicht nur aus technischer, auch aus organisatorischer und rechtlicher Sicht weist das eHealth-Projekt dem Bericht zufolge Mängel auf.
(c) k_rahn/Fotolia.com

Die Redaktion fand demnach nicht nur leicht behebbare technische Probleme, sondern stieß vor allem auf einen organisatorischen und juristischen Flickenteppich bei dieser kritischen Infrastruktur. „Durch mehrere leicht vermeidbare Fehler beim Entwicklerteam landete ein Admin-Kennwort im Klartext im Netz, Angreifer hätten vollen Zugriff auf das System bekommen können", heißt es in dem Bericht.

Viele Rettungsleitstellen und Krankenhäuser verlassen sich bei der Koordination von Notfällen mittlerweile auf Software und vernetzte Systeme. Eines der verbreitetsten Systeme ist IVENA, kurz für „Interdisziplinärer Versorgungsnachweis". Seit Frühjahr 2020 gibt es in IVENA zudem ein Modul mit dem Namen „Sonderlage" für die Corona-Pandemie, das freie Kapazitäten für Covid-Patienten verwaltet und das in der Hälfte der Bundesländer im Einsatzist. „IVENA läuft im Browser und jeder Kunde, also eine Kommune oder ein ganzes Bundesland, muss seine Instanz selbst betreiben – meist in Rechenzentren der öffentlichen Hand", schildern die c't-Autoren.

Bei einer NDR-TV-Reportage über den Rettungsdienst in Hannover sei einem c't-Leser ein verdächtiges Detail auf, das in einem Browserfenster eines Leitstellen-Computers zu sehen war: An die Adresse ivena-niedersachsen.de war eine kryptische Zeichenkette angehängt, offenbar eine sogenannte Session-ID. „Unseren Hinweisgeber erinnerte das daran, wie Webseiten früher häufig programmiert wurden und er wurde neugierig", erklärt c't-Redakteur Jan Mahn, der die Hinweise des Lesers nachrecherchierte. „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", schildert er das Problem.

Auf dem Server der Entwickler fand er dann noch mehr Sicherheitsprobleme: unter anderem eine Datei mit Benutzernamen und Kennwort für das IVENA-System. „Mit den gefundenen Zugangsdaten konnte man Benutzeraccounts verwalten, Krankenhäuser abmelden und hätte somit viel Schaden anrichten können", berichtet Mahn. Das Kennwort funktionierte, wie die Entwickler später bestätigten, nicht nur in Niedersachsen, sondern auf allen IVENA-Instanzen, unter anderem auch in Hessen, Berlin und München.

Mit diesen Beobachtungen kontaktierte c’t sofort die Entwicklerfirma und wies darauf hin, dass auch die Nutzerkennwörter potenziell in Gefahr waren. Das Unternehmen reagierte zügig. Fünf Stunden nach dem Hinweis erhielt c’t die Information, dass das Admin-Kennwort geändert und der Fehler auf dem Webserver beseitigt sei. Alle Nutzer wurden per E-Mail aufgefordert, ihre Kennwörter zu ändern.

„Damit ist zwar die akute Gefahr gebannt, doch auch aus organisatorischer und rechtlicher Sicht weist das eHealth-Projekt Mängel auf“, sagt Mahn. Es fehle es an klaren Verantwortlichkeiten. Wer die Infrastruktur genau betreibt und vor allem verantwortlich ist, sei auch auf Nachfragen bei Kliniken und Behörden nicht klar. „Wir waren überrascht, wie hemdsärmelig Krankenhäuser und Rettungsleitstellen eine solche kritische Infrastruktur betreiben.“

06.11.2020, 08:42, Autor: ks