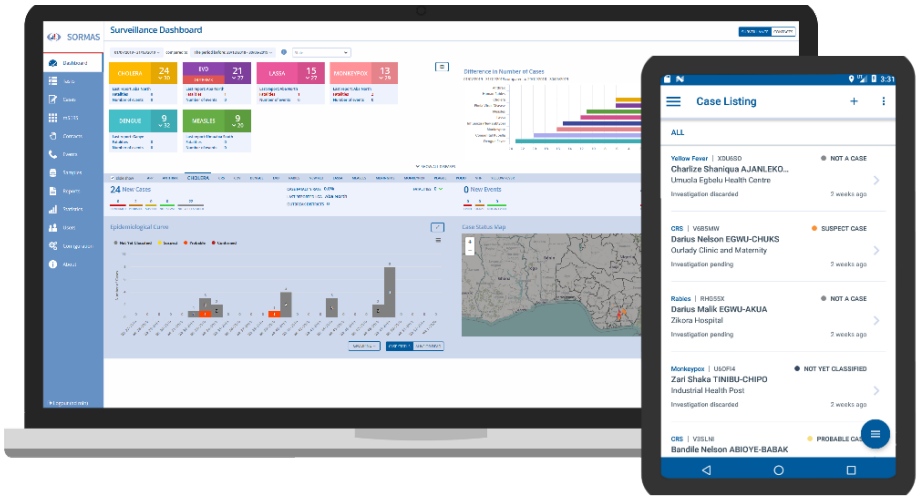


Bild: HZI

Offene Kontaktverfolgung

Sicherheitslücken im Pandemie-Management-System SORMAS

Deutsche Gesundheitsämter setzen bei der Kontaktverfolgung und Quarantäneverhängung von Corona-Infizierten zunehmend auf die Open-Source-Software SORMAS. Das System ist weltweit zum Management von Epidemien im Einsatz. Bis vor Kurzem hätten sich Angreifer allerdings einfach von außen in SORMAS einklinken können.

Von Dr. Andreas Kurtz

SORMAS steht für: Surveillance, Outbreak Response Management and Analysis System. Das federführend vom Helmholtz-Zentrum für Infektionsforschung (HZI) entwickelte System dient der Verwaltung von Kontaktpersonen und zur Nachverfolgung von Infektionsketten. Ursprünglich zur Eindämmung der westafrikanischen Ebola-Epidemie im Jahr 2014 konzipiert, wird SORMAS mittlerweile auch von deutschen Behörden bei der Corona-Pandemie eingesetzt.

Das Managementsystem ist seit 2016 ein Open-Source-Projekt, der Quellcode auf GitHub verfügbar. So kann das System weltweit sehr einfach und unbürokratisch eingesetzt werden. Bei einem Scan fand c't Dutzende aktive SORMAS-Installationen rund um den Globus verteilt. Sie sammeln für gewöhnlich Namen, Adressen und Telefonnummern, Testergebnisse sowie Quarantäne-Anordnungen von Infizierten und ihren potenziellen Kontakten. Wenn diese brisanten Informationen in falsche Hände geraten oder gar manipuliert oder gelöscht würden, hätte das nicht nur für die Betroffenen, sondern für die gesamte Pandemiebekämpfung fatale Folgen.

Gefährliche Standard-Accounts

Bis Mitte März wurden bei jeder Installation von SORMAS zu Demo- und Testzwecken ungesicherte Standard-Accounts angelegt und standardmäßig aktiviert, bis hin zum Administrator. Die simplen zugehörigen Passwörter standen festverdrahtet im Quellcode. Wer ihn studierte, konnte sich mit diesen Zugängen von außen über das Internet in die Systeme einklinken und nach Belieben Personendaten auslesen, verändern oder löschen.

Solche Standard-Accounts mit statischen Passwörtern sind ein Verstoß gegen das „Security by Default"-Paradigma. Es bedeutet, dass eine Software schon im Auslieferungszustand die sicherst mögliche Konfiguration aufweisen sollte. In der Praxis führen solche Default-Logins immer wieder zu ernsten Problemen.

Über eine Auswertung der von SORMAS genutzten digitalen Zertifikate (Certificate Transparency Logs) und einschlägige Suchmaschinen entdeckte c't Anfang Februar eine Vielzahl potenziell anfälliger SORMAS-Installationen im Internet – von Indien bis Afrika und von Australien bis Europa. Da unsichere Standardeinstellungen erfahrungsgemäß häufig nicht angepasst werden, ist die Gefahr groß, dass sich darunter auch zahlreiche Installationen mit Default- Logins und Standardpasswörtern befinden.

Situation in Deutschland

Auf Nachfrage von c't erklärte das HZI Ende Februar, dass es die Probleme nicht als Sicherheitslücke einstufe. So erklärten die Update-Hinweise, dass die automatisch angelegten Konten lediglich Demo- oder Testzwecken dienen. Administratoren würden dazu angehalten, die Konten auf Produktivsystemen selbstständig zu entfernen oder die Passwörter zu ändern.

Wenn die Admins das jedoch vergaßen oder die Aufforderung nicht lasen, blieben die Konten weiterhin aktiv. Das

System selbst warnte Betreiber nicht vor aktiven Standard- oder Administrator-Konten mit unveränderten Passwörtern.

Laut HZI seien deutsche Gesundheitsämter in der Regel nicht betroffen. Insgesamt 336 Ämter würden ihre SORMAS-Instanzen über das gemeinsam mit dem RKI konzipierte Projekt SORMAS@DEMIS beantragen, die dann von einem IT-Dienstleister installiert und zentral betrieben würden. Diese Instanzen würden grundsätzlich ohne Standard-Accounts aufgesetzt und für jede würde ein neues, individuelles Administrator-Passwort vergeben. Die Konfiguration und weitere Nutzung obliege dann dem jeweiligen Gesundheitsamt. Unklar blieb jedoch, wieviele der 39 weiteren an das RKI angeschlossenen Gesundheitsämter diesen Service nicht nutzen und SORMAS auf eigene Faust betreiben.

Hilfe aus Heilbronn

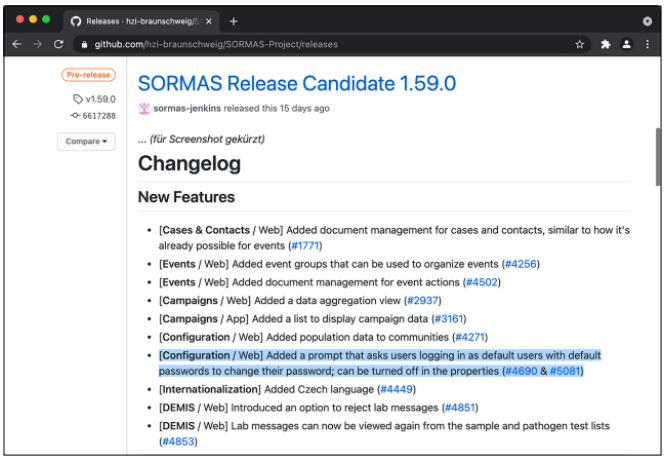
Die HZI-Entwickler reagierten auf die Hinweise von c't und änderten die SORMAS-Konfiguration so ab, dass bei zukünftigen Neuinstallationen keine Default-Logins mehr angelegt werden. Die Änderungen wurden mit Release 1.58 im März veröffentlicht.

Durch diesen offiziellen Fix änderte sich aber nichts an bestehenden Installationen: Wurde SORMAS bereits mit Default Logins installiert, waren diese auch nach dem manuell einzuspielenden Update weiterhin gültig. Zudem warnte SORMAS auch nicht vor dem Admin-Konto, das weiterhin bei jeder Neuinstallation immer mit dem gleichen, fest im Code der Anwendung hinterlegten Standardpasswort angelegt wird.

Diese verbliebenen Probleme wurden erst in der SORMAS-Version 1.59 angegangen, die bis zum 14. Mai bei den vom HZI betreuten Gesundheitsämtern aufgespielt werden sollte. c't hatte eine Forschungsgruppe der Hochschule Heilbronn kontaktiert, die sich mit Cybersicherheit an der Schnittstelle zu medizinischen Anwendungen beschäftigt. Die Forscher um Prof. Dr.-Ing. Andreas Mayer erkannten das Problem und steuerten dem HZI kurzfristig Code bei.

Durch die Ergänzungen der Hochschule Heilbronn werden SORMAS-Nutzer und Betreiber bei vorhandenen Default-Logins oder Standardpasswörtern nun gewarnt und es werden Passwortwechsel für die betroffenen Konten erzwungen – inklusive für das des Administrators.

Im Changelog von SORMAS auf GitHub führt das HZI den erzwungenen Passwortwechsel als neues „Feature" auf. Dass es sich dabei um ein wichtiges Sicherheitsupdate handelt, erfahren die Nutzer nicht.



Verfolgt man die emsige Betriebsamkeit des SORMAS-Teams auf GitHub, erkennt man schnell, wie mit Hochdruck an neuen Funktionen, Verbesserungen und Bugfixes gearbeitet wird. Im Hinblick auf die Standard-Accounts wäre trotzdem energischeres Handeln wünschenswert gewesen – ebenso wie ein transparenterer Umgang mit Sicherheitsproblemen und deren Behebung durch sicherheitsrelevante Updates.

Zwei-Faktor-Authentifizierung

Um dem hohen Schutzbedarf der in SORMAS verarbeiteten Gesundheits- und Personendaten gerecht zu werden, drängen sich noch eine ganze Reihe weiterer Verbesserungen auf. Das zeigt ein Blick in den OWASP Application Security Verification Standard, einem umfassenden Kriterienkatalog zur Absicherung von Webanwendungen. Er beschreibt beispielsweise in Abschnitt 2 detaillierte Anforderungen an eine sichere Authentifizierung, etwa eine Zwei-Faktor-Authentifizierung.

Wie die Kooperation der Heilbronner Forschungsgruppe mit dem HZI zeigt, ist das SORMAS-Team gegenüber externen Beiträgen aufgeschlossen und nimmt sie dankbar an. Wer ihm auf GitHub unter die Arme greifen und so zur erfolgreichen Pandemiebekämpfung beitragen möchte, rennt offene Türen ein.

Betreiber von SORMAS sollten in jedem Fall darauf achten, dass sie alle Standardpasswörter geändert haben und stets die neuste Version einsetzen, um mögliche Sicherheitslöcher zu schließen, bevor Angreifer sie ausnutzen. *(hag@ct.de)* c't

SORMAS und Sicherheitsregeln:
ct.de/yq4a

SORMAS-Nutzerkonten

Im Kern besteht SORMAS aus einem mit der Jakarta Enterprise Edition aufgesetzten Backend-Server mit einem Web-Frontend als Hauptzugangsweg. Ergänzend gibt es eine Android-App, die über ein REST API mit dem Backend interagiert. Für den einfachen Betrieb stehen vorgefertigte Docker-Images zur Verfügung.

Um die komplexen Abläufe des Epidemie-Managements und aller daran beteiligten Personengruppen über ein System zusammenzuführen, verfügt SORMAS über ein umfassendes Rollenkonzept mit Dutzenden Rollen und jeweils unterschiedlichen Berechtigungsstufen.

Personen der Rollengruppe „Hospital Informant" sind dafür verantwortlich, Verdachtsfälle in der Bevölkerung zu erkennen und an das System zu melden, beispielsweise aus einer Klinik. „Laboratory oder Surveillance Officer/Supervisor" analysieren und validieren die so eingespeisten Informationen anschließend. „Case/Contact Officer bzw. Supervisor" kontrollieren bestätigte Fälle sowie Eindämmungsmaßnahmen und verfolgen sie nach. Für Administratoren steht schließlich eine Rolle mit umfassenden Berechtigungen zur Verfügung, um das Gesamtsystem und seine Benutzer zu verwalten.

Problematisch ist, dass SORMAS bis zur Version 1.57 für jede dieser Rollen automatisch ein Benutzerkonto angelegt hat. Die Passwörter entsprachen dabei jeweils den Benutzernamen.