Prüfung der Sicherheit der Datenbank INFOSTAR

Bundesamt für Justiz und Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements

Das Wesentliche in Kürze

Infostar ist das zentrale Register für die elektronische Erfassung von Zivilstandsereignissen (Geburt, Ehe, Tod usw.), das der Bund den Kantonen seit 2005 bereitstellt. Rund 1200 Benutzer in 142 Zivilstandsämtern sind daran angeschlossen. Betrieben wird die Anwendung vom Fachbereich Infostar des Bundesamts für Justiz (BJ) und dem Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD). Derzeit läuft ein Modernisierungsprojekt im Umfang von rund 23,7 Millionen Franken, dessen Abschluss ursprünglich für 2023 geplant war.

In der vorliegenden Prüfung untersucht die Eidgenössische Finanzkontrolle (EFK), ob die Informationssicherheit beim Betrieb der aktuellen Anwendung gewährleistet ist. Des Weiteren prüft sie, ob die Sicherheitslücken mit dem Modernisierungsprojekt behoben sind und ob die Zusammenarbeit im Prozess zur Behandlung von Cybervorfällen funktioniert.

Die Grundlagen für die Informationssicherheit im Rahmen des Betriebs der aktuellen Anwendung und des Modernisierungsprojekts sind insgesamt gelegt, u. a. durch ihre Integration in die Standardinfrastruktur des ISC-EJPD. Allerdings sind Lücken festzustellen: Die Sicherheitsdokumentation und die Risikoanalyse der Anwendung müssen aktualisiert werden. Das Projekt «Infostar New Generation» befindet sich in einer schwierigen Phase, Anpassungen in der Organisation und Planung sind vorzunehmen und der Testansatz muss verbessert werden. Schliesslich sind die Grundlagen für den Prozess zur Behandlung von Cybervorfällen gelegt, aber eine stärkere Operationalisierung und eine bessere Kommunikation sind erforderlich.

Aktuelle Anwendung: stabiler Betrieb, aber veraltete Sicherheitsdokumentation

Durch die Integration in die Standardinfrastruktur des ISC-EJPD profitiert die aktuelle Anwendung von einer bewährten Sicherheitsarchitektur. Die Benutzerauthentifizierung, Zugriffsrechte, ein verschlüsselter Informationsverkehr und Redundanzen sind unter anderem implementiert. Architekturboards verfolgen die Entwicklung fortlaufend.

Die Aktivitäten im Anwendungs- und technischen Betrieb werden zweckmässig beschrieben und umgesetzt. Die Benutzerverwaltung, der Schadsoftwareschutz, Sicherheitsbackups, die Infrastrukturüberwachung und periodische Stabilitätstests werden durch Fachpersonen sichergestellt. Der Betrieb der aktuellen Lösung ist stabil, ihre Wartung wird jedoch durch die Komplexität der Programme erschwert.

Eine Security-Governance ist vorhanden, die Rollen sind definiert, besetzt und unter den Beteiligten klar abgegrenzt. Obwohl Infostar einen erhöhten Bedarf an Informationsschutz aufweist, ist die Sicherheitsdokumentation weitgehend veraltet. Dies kann dazu führen, dass die Verantwortlichen die Risiken, denen die Lösung ausgesetzt ist, unterschätzen. Die Sicherheitsdokumente müssen aktualisiert und eine Restrisikoanalyse muss durchgeführt und validiert werden.

Die Modernisierung sieht sich mit Schwierigkeiten konfrontiert, die Projekt- und Testorganisation müssen verbessert werden

Das 2018 lancierte Projekt zur Modernisierung von Infostar ist im Gang. Die Arbeiten sollen technische Entwicklungen nutzen und Antworten auf die Schwierigkeiten finden, die bei den Wartungstätigkeiten auftreten. Das Projekt wird nach einer agilen Methode unter der Leitung des BJ geführt, das insbesondere die Fachbedürfnisse definiert. Das ISC-EJPD ist für die Umsetzung verantwortlich.

Das Projekt ist seit mehreren Monaten mit Schwierigkeiten konfrontiert, die Personalfluktuation ist hoch und die Projektleitungsstelle ist ad interim besetzt. Die Verantwortlichen sind sich der heiklen Situation bewusst und haben Sofortmassnahmen festgelegt. Eine neue Organisation wurde eingeführt, Profile werden auf dem Arbeitsmarkt gesucht. Verzögerungen und Kostenüberschreitungen sind somit absehbar. Die EFK verzichtet auf eine Empfehlung, fordert aber eine verstärkte Integration von Fachpersonen für Sicherheit und Betrieb in die neue Organisation.

Die neue Anwendung wird im Rahmen der Standardarchitektur des ISC-EJPD realisiert. Damit profitiert sie von deren soliden Sicherheitskomponenten. Die EFK stellt aber fest, dass der Testansatz des Projekts noch nicht ausgereift ist. Sie fordert insbesondere, dass die Tiefe der Tests, ihre Automatisierung, die Nichtregression und die Fehlerbehandlung neu überdacht werden.

Behandlung von Cybervorfällen und Kontinuitätsmanagement: Die Integration muss gestärkt werden

Die Grundlagen für die Behandlung von Cybervorfällen sind angemessen definiert. Die Rollen und Zuständigkeiten werden im ISC-EJPD aktiv wahrgenommen. Die Prozesse sind beschrieben, die Leistungsbezüger sind aber nicht genügend in deren Umsetzung eingebunden. Diesen Punkt muss das ISC verbessern. Es sollte auch prüfen, ob es sinnvoll ist, Reaktionsmodelle für verschiedene Arten von Vorfällen zu entwickeln. Zum Prüfungszeitpunkt wurden die Modalitäten des Krisenmanagements aktualisiert, die EFK verzichtet deshalb auf eine Empfehlung.

Die Vorfallsmanagement- und Eskalationssysteme sind implementiert, ebenso die Kontaktstellen und die Meldewege. Bei der Abwicklung eines Vorfalls werden die Handlungen und Entscheide dokumentiert. Die Überwachungsinstrumente sind vorhanden, die Ereignisse werden protokolliert und können mit Hilfsmitteln analysiert werden.

Die Modalitäten des Business Continuity Management werden in den einzelnen Verwaltungseinheiten festgelegt, die EFK sieht jedoch die Gefahr, dass sie nicht ausreichend integriert werden. Die EFK rät dem BJ, Übungen zum Infostar-Continuity-Management mit Einbezug der Leistungsbezüger und -erbringer durchzuführen. Dies mit dem Ziel, die Koordination unter den Beteiligten zu verbessern und allfällige Schwachstellen im Prozess zu erkennen.

Originaltext auf Französisch