OpenR@thaus

Serviceportal nicht erreichbar

[02.07.2024] Wegen einer Sicherheitslücke wurde das Serviceportal OpenR@thaus zum zweiten Mal in kurzer Zeit vom Netz genommen. Davon betroffen sind rund 300 Kommunen. Die Wartungsarbeiten dauern derzeit an. Offenbar besteht ein Zusammenhang zu einer Schwachstelle der BundID, die es erlaubt, relativ einfach auf einer eigenen Website ein BundID-Log-in umzusetzen.

„Die Online-Dienstleistungen in unserem Serviceportal können für voraussichtlich eine Woche nicht in Anspruch genommen werden. Hintergrund ist eine potenzielle Sicherheitslücke, wegen der das Serviceportal vorsichtshalber vom Netz genommen wurde. Es sind kurzfristige Wartungsarbeiten notwendig“ – diesen Text postete die Stadt Braunschweig kürzlich auf Facebook. Die Stadt nutzt die Lösung OpenR@thaus des IT-Dienstleisters ITEBO. Verschiedene weitere Kommunen, die OpenR@thaus als Bürgerportal im Einsatz haben, haben vergleichbare Meldungen veröffentlicht. Insgesamt sollen laut der IT-Newsseite Golem und der Website Security Incidents etwa 300 Kommunen betroffen sein und die Dienste abgeschaltet haben.

Kein Datenabfluss

Auch ITEBO spricht von einer „potenziellen Beeinträchtigung“, wegen derer das Serviceportal OpenR@thaus vorsichtshalber vom Netz genommen worden sei. Die Dauer der Arbeiten, die das System härten und wieder sicher ans Netz bringen sollen, wurden zunächst auf etwa eine Woche geschätzt, inzwischen spricht das Unternehmen von zusätzliche Aufgabenstellungen, die aufgetreten seien und die eine Anpassung des internen Zeitplans erforderlich machten. Für Nutzerinnen und Nutzer der Anwendung bestehe jedoch kein Grund zur Beunruhigung: Personenbezogene und auch sonstige Daten seien nicht abgegriffen worden, so ITEBO.
Trotz der Unterbrechung des Dienstes sind in vielen Kommunen die Online-Services wenigstens teilweise noch nutzbar. „Lediglich einige Komponenten, wie zum Beispiel das Bürgerpostfach stehen aktuell nicht zur Verfügung“, heißt es beispielsweise aus Braunschweig.

Lücken bei der BundID

Weitere Informationen zu der Sicherheitslücke gibt es derzeit von ITEBO nicht. Allerdings liegt die Vermutung nahe, dass ein Zusammenhang zu Sicherheitslücken in der BundID besteht. Die BundID ist essenziell für den Zugang zum Bürgerkonto und damit zu online angebotenen Verwaltungsdienstleistungen. Über diese Schwachstelle berichtete die IT-Sicherheitsforscherin Lilith Wittmann ausführlich in einem Beitrag auf der Online-Publishing-Plattform Medium. Die von Wittmann entdeckte Schwachstelle ermöglicht es jedem, einen BundID-Log-in auf der eigenen Web-Seite anzubieten. Dadurch können zwar keine Daten erlangt werden, jedoch ist es möglich, Nutzer dazu zu bringen, sensible Daten freiwillig anzugeben.
Der Fehler basiert auf einer Fehlkonfiguration in OpenR@thaus. Wittmann führt diese auf die Verwendung des grundsätzlich sicheren, aber kompliziert zu implementierenden SAML-Verfahrens zurück, welches bei der BundID für die Authentifizierung benutzt wird. Kurz nachdem dieser Fehler bekannt wurde, wurden zahlreiche Verwaltungsdienste vorübergehend abgeschaltet und die Sicherheitslücke behoben. Allerdings entdeckte die Forscherin anschließend eine weitere Schwachstelle in der Software Liferay, auf der

OpenR@thaus basiert. Ihr gelang es daraufhin erneut, einen BundID-Log-in auf einer von ihr erstellten Web-Seite anzubieten. Daher wurden am 18. Juni 2024 erneut zahlreiche digitale Verwaltungsdienste abgeschaltet.

(sib)

Information bei ITEBO
Detaillierter Bericht über beide Sicherheitslücken bei Medium

Stichwörter: IT-Sicherheit, OpenR@thaus, Digitale Identität, BundID