ITEBO

# OpenR@thaus-Vorfall aufgearbeitet

## [23.07.2024] Mit seinem Verwaltungsportal OpenR@thaus liefert ITEBO zahlreichen Kommunen eine Basisinfrastruktur, um Leistungen, wie vom OZG vorgesehen, digital anbieten zu können. Im Juni war die Lösung aus Sicherheitsgründen offline gestellt worden. Nun berichtet ITEBO im Detail über den Vorfall und dessen Aufarbeitung.

Im Juni 2024 wurde das Serviceportal OpenR@thaus aufgrund von Sicherheitsbedenken innerhalb kurzer Zeit zwei Mal vorsorglich vom Netz genommen (43998+wir berichteten). Nun meldet der IT-Dienstleister ITEBO, der Sicherheitsvorfall sei abgeschlossen und schildert die Vorfälle detailliert aus seiner Perspektive. Demnach wurde OpenR@thaus Ziel eines Scam-Angriffs. Durchgeführt wurde dieser von der Hacktivistin Lilith Wittmann, der es am Abend des 7. Juni 2024 gelang, potenzielle Missbrauchsmöglichkeiten eines Redirects (Weiterleitung) der BundID auf nicht legitimierte Webseiten offenzulegen. Um diese Weiterleitungen zu unterbinden, seien die Systeme des Serviceportals OpenR@thaus als Sofortmaßnahme von der BundID getrennt worden, berichtet ITEBO. Innerhalb von 24 Stunden sei am Wochenende in Zusammenarbeit mit einem Cybersecurity-Dienstleister und dem Bundesministerium des Innern und für Heimat (BMI) eine Lösung für diesen spezifischen Missbrauchsvektor geschaffen worden. Die Portale waren daher am 9. Juni wieder verfügbar. ITEBO verweist auf die bestehenden Zertifizierungen ISO/IEC 20000-1:2018 und ISO/IEC 27001:2017, die Prozesse und Verfahren vorsehen, wie in Krisenfällen zu verfahren ist. In diesem Fall sei auf das Business Continuity Management (BCM) und den dazugehörigen Notfallplan (Continuity Plan OpenR@thaus) zurückgegriffen worden.

### Kunden blieben auf dem Laufenden

Nach dieser zügigen Fehlerbehebung geriet OpenR@thaus am 17. Juni erneut in den Fokus der Angreiferin und wurde wieder vorbeugend vom Netz genommen, das Abschalten aller Serviceportale wurde veranlasst. „Aufgrund des Angriffs wurden durch die BundID alle Authentifizierungen von OpenR@thaus-Usern gesperrt. Eine Nutzung der Portale durch Bürgerinnen und Bürger war nicht mehr effektiv möglich, da die Anmeldung über das Nutzerkonto nicht mehr zur Verfügung stand. Die Sacharbeiterinstanzen waren allerdings noch verfügbar. Eine Bearbeitung der vorhandenen Anträge durch die kommunalen Verwaltungen konnte somit weitergeführt werden“, erläutert Thomas Cormann, Servicebereichsleiter bei ITEBO.
Wittmann hatte die von ihr aufgedeckte Sicherheitslücke auf die Verwendung des SAML-Verfahrens zurückgeführt, welches bei der BundID für die Authentifizierung benutzt wird. Eine weitere Sicherheitslücke sah die Informatikerin in der Software Liferay, auf der OpenR@thaus basiert. Hierzu merkt ITEBO jetzt an, dass diese Sicherheitslücke in Liferay eine Softwareversion betreffe, welche bereits seit Mitte 2021 nicht mehr in den Serviceportalen zur Verwendung kam.
Wie ITEBO angibt, wurden betroffene Kunden per E-Mail fortlaufend über aktuelle Sicherheitsmaßnahmen und ihren Umsetzungsstatus informiert. In Zusammenarbeit mit dem BMI wurden umfangreiche Maßnahmen zur Härtung des Quellcodes getroffen. Die OpenR@thaus-Portale waren am 4. Juli 2024 wieder verfügbar.

### ITEBO holt externe Berater hinzu

ITEBO will den Vorfall nun auch zum Anlass nehmen, um gemeinsam mit einem externen Cybersecurity-Unternehmen Gespräche zu den Themen Produktsicherheit, Betriebssicherheit und Möglichkeiten von Analytik und Härtung aufzunehmen. „Die daraus gewonnenen Erkenntnisse werden unsere bisherigen Maßnahmen der Cybersecurity ergänzen“, sagt Udo Wenker, Geschäftsführer der ITEBO-Unternehmensgruppe. Wenker betont, dass „über den Angriffsvektor“ zu keinem Zeitpunkt Datenabflüsse möglich gewesen seien. Auch ein unerwünschter Fremdzugriff auf die Serviceportale oder die Kommunikation zur BundID sei zu keiner Zeit möglich gewesen. „Wir bedauern die Unannehmlichkeiten und auch die entstandene Verunsicherung, die durch die Abschaltung des Serviceportals entstanden sind, sehr“, so Wenker.

(sib)

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