Governikus KG
… so innovativ ist Sicherheit

ÖFFENTLICHE STELLUNGNAHME UND KUNDENINFORMATION

Bremen, 23.11.2018

Stellungnahme zur Berichterstattung einer Schwachstelle im Governikus Autent SDK

Diese Information dient der Klarstellung der aktuellen (November 2018) Berichterstattung zu einer Schwachstelle im Governikus Autent Software Development Kit (SDK) in der Version 3.8.1 und der daraus resultierenden und von der Presse aufgegriffenen Rückschlüsse zu unsicheren Implementierungen der eID-Funktion des deutschen Personalausweises:

Im vergangenen Jahr wurde im Rahmen eines Anwenderforums zur AusweisApp2 von Governikus ein **Demobeispiel** auf Basis des Governikus Autent SDK vorgestellt, um die unkomplizierte und schnelle Implementierung der eID-Funktion des Personalausweises bei Diensteanbietern zu verdeutlichen. Dieses Demobeispiel wurde auch öffentlich zum Download zur Verfügung gestellt, ohne das vollständige Governikus Autent SDK zu beinhalten.

Das Unternehmen SEC Consult hat anhand dieses Demoszenarios, das ausdrücklich zu keinem Zeitpunkt den Anspruch hatte, eine vollumfängliche Implementierung im Realbetrieb vorzunehmen, eine Prüfung auf Schwachstellen vorgenommen und im Juli d.J. dem CERT-Bund eine Schwachstelle gemeldet.

Das von SEC Consult beschriebene Angriffsszenario bedient sich des Umstandes, dass im Demoszenario des Autent SDKs die Prüfung einer „SAMLResponse“ zwar korrekt durchgeführt, anschließend aber ein weiterer angehängter Parameter mit dem Namen „SAMLResponse“ verarbeitet wird. Während die Prüfroutine aus dem Autent SDK kommt, handelt es sich bei der Verarbeitung der SAMLResponse um einen Standardaufruf auf der Servlet API (`getParameter`) und ist somit Teil der **Beispiel**-Implementierung und hat **nichts mit dem Autent SDK** zu tun.

Die im Autent SDK enthaltenen Demoszenarien sind, wie aus dem Namen ersichtlich, zur Demonstration der Bibliotheken gedacht. Sie hatten und haben allerdings nicht den Anspruch, weitere Sicherheitsmaßnahmen, die im Realbetrieb erforderlich sind, zu erwähnen oder gar zu implementieren.

Governikus GmbH & Co. KG
Am Fallturm 9
28359 Bremen, Germany
Telefon: +49 421 204 95-0
Geschäftsführer: Dr. Stephan Klein
www.governikus.de

Pressekontakt:
Governikus, Petra Waldmüller-Schantz
Director Communications
Tel.: +49 421 204 95-54
E-Mail: petra.waldmueller@governikus.de

Diese müssen durch die jeweiligen Diensteanbieter bzw. Betreiber solcher Dienste ergriffen werden, zum Beispiel zum Schutz vor XSS-Angriffen, SQL-Injection, Replay-Angriffen usw. Diese URL-Prüfungen sind die Maßnahme, die den Angriff verhindert. Das von der OASIS spezifizierte und offene Protokoll „SAML Web Browser SSO Profil“ (Redirect Binding) findet hier Anwendung. Das SAML Protokoll ist bewusst so offen, dass weitere Parameter übermittelt werden können, wenn das von der entsprechenden Anwendung benötigt wird. Die Prüfungsregeln für den Diensteanbieter ergeben sich u.a. aus dem Standard selbst (https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf, Abschnitt 3.4.4.1 „(…) the relying party MUST ensure that the parameter values to be verified are ordered as required by the signing rules above“).

Die zu ergreifenden Maßnahmen ergeben sich aus OASIS- und OWASP-Empfehlungen, welche von unseren Kunden im Rahmen der Integration beachtet und als Voraussetzung bei der Implementierung genannt werden. In diesem Fall sind besonders die Empfehlungen von OWASP (https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet) zu beachten. Aber selbstverständlich müssen anwendungsbezogen weitere Maßnahmen umgesetzt werden.

An dieser Stelle nochmals der Hinweis: Das Demo-Szenario enthält nicht das vollständige Autent SDK und **kann so nicht für eine vollständige Implementierung einer im realen Betrieb durchgeführten Personalausweisintegration verwendet werden** und sollte lediglich verdeutlichen, wie einfach eine Implementierung vorgenommen werden kann! Dass allerdings im Realbetrieb weitere Maßnahmen im Rechenzentrum durchgeführt werden müssen, war nicht Bestandteil des Demoszenarios.

Wir stimmen insofern mit der Einschätzung überein, dass ein Beispiel häufig ungewollt übernommen wird, auch wenn die beigelegte Readme-Datei darauf hinweist, dass es eine Demo ist, welche zudem nur auf localhost läuft. Deswegen haben wir bereits im August 2018 einen Quick-Fix in die entsprechende Routine aufgenommen, die einen Fehler zurückmeldet, wenn relevante URL-Parameter (SigAlg, SAMLResponse, RelayState) tatsächlich mehr als einmal vorkommen. Diese Aktualisierung haben wir unseren Kunden umgehend zur Verfügung gestellt. Diese inhaltliche Prüfung wird in Realszenarien durch die o.g. Umsetzung der OASIS- und OWASP-Empfehlungen allerdings auch vor der Verarbeitung im SDK bereits durchgeführt.

Selbstverständlich läuft das SDK nur in Java-Umgebungen und die Online-Ausweisfunktion ist auch nur eine Anwendungsmöglichkeit.

Darüber hinaus ist das SDK ein Produkt der Governikus. Daher kann es nicht stellvertretend für die Online-Ausweisfunktion stehen.

Der sowohl von SEC Consult als auch von einigen Berichterstattern aufgegriffene Rückschluss, sämtliche mit Autent realisierten Integrationen der eID-Funktion des Personalausweises wären unsicher, ist damit schlicht und ergreifend falsch.

Governikus GmbH & Co. KG
Am Fallturm 9
28359 Bremen, Germany
Telefon: +49 421 204 95-0
Geschäftsführer: Dr. Stephan Klein
www.governikus.de

Pressekontakt:
Governikus, Petra Waldmüller-Schantz
Director Communications
Tel.: +49 421 204 95-54
E-Mail: petra.waldmueller@governikus.de

Über die Governikus GmbH & Co. KG (Governikus KG)

Die Governikus KG ist ein seit 1999 etablierter IT-Lösungsanbieter für Sicherheit und Rechtsverbindlichkeit elektronischer Kommunikation und elektronischer Dokumente, vor allem im Hinblick auf den Schutz personenbezogener Daten. Als Pionier im E-Government- und E-Justice liegt der Fokus des Portfolios auf der Unterstützung zur Digitalisierung von Verwaltungsprozessen. Das Governikus-Portfolio untergliedert sich in die Themenfelder sichere Identitäten, sichere Kommunikation und sichere Daten.

U.a. durch die Entwicklung und Pflege von 3 Anwendungen des IT-Planungsrates – die Anwendung Governikus, die Anwendung Governikus MultiMessenger (GMM) sowie die Anwendung DVDV (Deutsches Verwaltungsdiensteverzeichnis) – liefert das Governikus-Portfolio wichtige Lösungsbausteine zur Umsetzung gesetzlicher Vorgaben, politischer Strategien und technischer Standards, die sowohl auf nationaler als auch internationaler Ebene Bedeutung für die Digitalisierung entfalten. Governikus unterstützt dies durch Lösungen, die für gemeinsam nutzbare Basisinfrastrukturen zum Einsatz kommen. Die AusweisApp2 des Bundes zur Nutzung der Online-Ausweisfunktion wird ebenfalls von Governikus entwickelt und gepflegt.

Governikus GmbH & Co. KG
Am Fallturm 9
28359 Bremen, Germany
Telefon: +49 421 204 95-0
Geschäftsführer: Dr. Stephan Klein
www.governikus.de

Pressekontakt:
Governikus, Petra Waldmüller-Schantz
Director Communications
Tel.: +49 421 204 95-54
E-Mail: petra.waldmueller@governikus.de