Kundeninformation

Schutzmaßnahmen beim autonomen Einsatz von Client-Server-Verfahren

Sehr geehrte Damen und Herren,

mit dieser Kundeninformation möchten wir Sie auf den sicheren Betrieb von Fachverfahren besonders aufmerksam machen. Anlass hierfür ist die kontinuierlich ansteigende Zahl von Angriffen auf die Informationssicherheit von Infrastrukturen und Softwaresystemen.

Softwaresysteme in der öffentlichen Verwaltung verfügen in der Regel über einen langen Lebenszyklus, da die Einführung neuer Softwaresysteme mit einem hohen finanziellen und organisatorischen Aufwand für Behörden verbunden ist. Daher können sich auch Softwarekomponenten und -architekturen in Betrieb befinden, die gegenüber neuartigen Angriffsszenarien strukturelle Sicherheitsdefizite aufweisen.

Software, die noch auf einer sogenannten 2-Schichten-Architektur (klassisch Client-Server-Architektur) basiert, ist hierbei besonders zu betrachten. Bei dieser Architektur übernimmt der Client sowohl die Darstellung der Benutzerschnittstelle als auch die gesamte Steuerung der Anwendung, insbesondere erfolgen dabei vom Client direkte Datenbankzugriffe. Hierdurch entstehen Risiken, etwa wenn das Berechtigungskonzept auf den Clients umgangen wird oder über Seitenkanäle angegriffen wird. Dies sind potenzielle Risiken für die entsprechenden Fachdaten, denen begegnet werden muss.

In den nächsten Jahren werden die noch eingesetzten 2-Schichten-Produkte der AKDB schrittweise durch die neuen SYNERGO®-Produkte in einer modernen und der IT-Sicherheit dienlichen 3-Schichten-Architektur ersetzt. Die SYNERGO®-Produkte wie OK.VERKEHR oder OK.JUS sind im Einsatz und erfüllen die sicherheitstechnischen Anforderungen bereits vollständig. Gleiches gilt etwa für OK.EWO, das seit Ende 2020 ebenfalls technisch komplett in die SYNERGO®-Produktfamilie integriert ist.

Die AKDB minimiert das Risiko für ihre Fachanwendungen kontinuierlich durch programmtechnische Anpassungen. Darüber hinaus ist zusätzlich auch eine kundenseitige Prüfung hinsichtlich der strukturell bedingten Sicherheitsrisiken beim autonomen Betrieb von Software unverzichtbar.

Eine hierfür von der AKDB beim Fraunhofer-Institut für sichere Informationstechnologie beauftragte Studie zu typischen Angriffsszenarien und Sicherheitsmaßnahmen unterschiedlicher Ausprägung soll Sie in Ihren Bemühungen, den Betriebsrisiken zu begegnen, unterstützen.

Die dieser Kundeninformation beiliegende Studie
SICHERER KOMMUNALER IT-ARBEITSPLATZ – IT-Sicherheitsempfehlungen zum Betrieb von Fachverfahren
behandelt mit Fokus auf Client-Server-Verfahren sehr umfangreiche technische und auch organisatorische IT-Sicherheitsthemen, die für den sicheren Betrieb von Fachsoftware in einer Behörde von hohem Wert sind. Die Maßnahmen dienen dem Kernziel der IT-Sicherheit, die sensiblen Daten nachhaltig vor Diebstahl, Verfälschung und jeglichem Missbrauch zu schützen.

Wir empfehlen unseren Kunden, die Software autonom und nicht im Rechenzentrum der AKDB betreiben, diese Handlungsempfehlungen dringend zu beachten.

Die in der Studie vorgestellten Maßnahmen sind in der Regel mit zusätzlichen Kosten verbunden. Diesen Kosten sind die erheblichen Schäden gegenüberzustellen, die sich aus dem Verlust, der Veränderung oder der Offenlegung von sensiblen Daten ergeben können. Als weitere Hilfestellung beinhaltet die Studie daher auch Aussagen zur Priorisierung bestimmter Maßnahmen.

Besonders wirkungsvoll erhöht werden kann IT-Sicherheit beim Betrieb der Client-Server-Verfahren, indem die Fachprodukte mit einem besonderen Benutzer-/Rechtekonzept im Zugriff eingeschränkt werden oder indem sie vom eigentlichen Arbeitsplatz-PC auf entsprechende Terminalserver verlagert werden.

Der höchstmögliche Schutz für die sensiblen Daten kann alternativ und mit geringem Aufwand durch den Wechsel vom autonomen Betrieb der Software in das BSI-zertifizierte Rechenzentrum der AKDB erreicht werden.

Bei Fragen wenden Sie sich bitte an den für Sie zuständigen Kundenservice des Fachverfahrens.

Mit freundlichen Grüßen

Ihre AKDB