Deutscher IT-Sicherheitskongress

Schutz der KI im Fokus

[09.02.2021] Beim 17. Deutschen IT-Sicherheitskongress des BSI stand neben Themen wie 5G, Post-Quanten-Kryptografie oder Smart Home/Smart Factory vor allem die künstliche Intelligenz (KI) im Mittelpunkt. Das BSI veröffentlichte in diesem Kontext einen neuen Kriterienkatalog für KI-basierte Cloud-Dienste (AIC4).

In der ersten Februarwoche 2021 fand der 17. Deutsche IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik (BSI) statt. Etwa 7.000 Personen nahmen laut BSI an der erstmals vollständig digitalen Veranstaltung teil, die neben zahlreichen Fachvorträgen und einer Podiumsdiskussion auch Keynotes von Bundeskanzlerin Angela Merkel, dem saarländischen Ministerpräsidenten Tobias Hans, und dem CIO des Bundes Markus Richter und anderen umfasste. BSI-Präsident Arne Schönbohm verwies in diesem Rahmen auf die bedeutende Rolle der Informationssicherheit als „Voraussetzung einer erfolgreichen Digitalisierung“ und betonte, trotz jüngster Erfolge – etwa bei der Zerschlagung der Emotet-Infrastruktur – seien weiterhin alle Bereiche von Staat, Wirtschaft und Gesellschaft ebenso wie Privatpersonen durch Cyber-Angriffe gefährdet, zuletzt etwa auch Schul-Clouds und Bildungsserver.
Zu den thematischen Schwerpunkten der Veranstaltung gehörten 5G, die Post-Quanten-Kryptografie, Smart Home/Smart Factory und insbesondere die künstliche Intelligenz (KI). Der KI-Einsatz beeinflusst bereits jetzt viele kritische Prozesse und Entscheidungen, etwa in der Wirtschaft oder im Gesundheitsbereich, teilt das BSI mit. Gleichzeitig seien auf KI basierende Systeme neuen Sicherheitsbedrohungen ausgesetzt, die von etablierten IT-Sicherheitsstandards nicht abgedeckt würden.

Schutz KI-basierter Dienste

Im Rahmen des Kongresses veröffentlichte das BSI deshalb den neuen Kriterienkatalog für KI-basierte Cloud-Dienste (Artificial Intelligence Cloud Services Compliance Criteria Catalogue, AIC4). Der Katalog sei eine wichtige Grundlage, um die Sicherheit von KI-Systemen zu bewerten. Der AIC4 definiere erstmals ein Basisniveau an Sicherheit für KI-basierte Dienste, die in Cloud-Infrastrukturen entwickelt und betrieben werden. Ein vergleichbarer einsetzbarer Prüfstandard für sichere KI-Systeme existiere derzeit nicht. Der AIC4 umfasst laut BSI KI-spezifische Kriterien, die eine unabhängige Prüfung der Sicherheit eines KI-Services über dessen gesamten Lebenszyklus hinweg ermöglichen. Dieser Ansatz habe sich schon beim C5-Kriterienkatalog bewährt, mit dem das BSI einen weltweit anerkannten Standard der Cloud-Sicherheit gestaltet und etabliert habe. Mit dem AIC4 wolle das BSI nun eine führende Rolle bei der Absicherung von KI-Anwendungen einnehmen und einen wesentlichen Beitrag zur Gestaltung einer sicheren Digitalisierung „Made in Germany“ leisten.
Zudem will das BSI noch im Jahr 2021 einen Stützpunkt mit dem fachlichen Schwerpunkt KI im Saarland ansiedeln. Die bereits begonnene Arbeit, Kooperationen mit nationalen und internationalen Partnern zu schließen, will das Amt weiter forcieren, erklärte BSI-Präsident Arne Schönbohm.
Bereits im November 2020 war das BSI im Rahmen der vom Land Nordrhein-Westfalen geförderten Kompetenzplattform KI.NRW eine strategische Kooperation mit dem Fraunhofer IAIS eingegangen, um die Entwicklung einer KI-Zertifizierung „Made in Germany“ voranzubringen. Ziel der Zusammenarbeit sei es, Prüfverfahren für die Zertifizierung von KI-Systemen zu entwickeln, die als Basis für technische Standards dienen können. Bei der Weiterentwicklung der Prüfverfahren sollen Praxistauglichkeit und Marktfähigkeit in enger Abstimmung mit der Wirtschaft verbessert werden.

(sib)

Rückblick auf den 17. Deutschen IT-Sicherheitskongress
Informationen des BSI zu KI

Stichwörter: IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Sicherheitskongress, KI