Medieninformation

# asvin entwickelt Lösung zur Sicherung von KI-Datenlieferketten

**Stuttgart, 03.02.2021. Durch den Solarwinds-Hack sind Angriffe auf IT-Lieferketten zur größten realen Bedrohung geworden. Attacken auf Supply-Chains sind vor allem für Künstliche Intelligenz (KI) eine massive neue Gefährdung. Um den nächsten Supergau eines Angriffs auf die KI-Datenlieferketten, insbesondere auf das Machine Learning, zu verhindern, entwickelt das Stuttgarter Start-up asvin zusammen mit Spitzenforschern des Karlsruher Institut für Technologie (KIT) neue Ansätze, um Datenlieferketten gegen Angriffe abzusichern.**

Das Szenario ist aus Krimis bekannt: Attentäter kapern einen Partyservice, betreten als Lieferanten getarnt unbemerkt von der Security ein Gebäude und richten unter den Partygästen ein Massaker an. Nach einem vergleichbaren Muster haben Cyberkriminelle kürzlich im Rahmen des Solarwinds-Hacks weltweit die Kunden des Software-Unternehmens angegriffen: In ein Update der Solarwinds-Netzwerksoftware „Orion" bauten Angreifer unbemerkt eine „Hintertür" ein, durch die sie sich Zugriff auf rund 18.000 Netzwerke von Unternehmen und Behörden verschafften.

## Bedrohung für Datenlieferketten

„Da hier die Software-Lieferkette auf der Ebene der Cybersicherheit-Lieferanten kompromittiert wurde, können herkömmliche Cybersecurity-Maßnahmen wie Anti-Virus-Schutz oder das Zero-Trust-Prinzip durch Angreifer überwunden werden", erklärt asvin-CEO Mirko Ross. „Vielmehr sollten sich Unternehmen dringend um das Risikomangement von Software-Drittanbietern kümmern. Das bedeutet, Entwicklungs-, Herstellungs-, Support- und Wartungsprozesse von Software-Lieferanten müssen vertrauenswürdig und sicher sein. Um eine in diesem Sinne sichere digitale Infrastruktur zu realisieren, sollten alle Beteiligten eine kooperative Haltung entwickeln und global zusammenarbeiten."

Eine lückenlose Absicherung der Technologie- und Datenlieferketten ist vor allem unumgänglich, um Künstliche Intelligenz vor Attacken zu schützen. Denn wenn es Angreifern gelingt, in die Datenlieferkette einzugreifen und Datensätze zu korrumpieren, lässt sich KI gezielt zu falschen Aussagen lenken. Das kann fatale Folgen haben. So ist z.B. zu befürchten, dass ein KI-basiertes medizinisches Diagnoseverfahren aufgrund manipulierter Trainingsdaten unbemerkt falsche Diagnosen liefert. Manipulierte Daten in der Produktion können zu Qualitätseinbußen oder Stillstandzeiten führen. Denkbar ist außerdem, dass Angreifer die KI in einem „smarten" Fahrzeug trainieren, um das Verhalten des Fahrzeuges negativ zu beeinflussen.

## Innovative Chain-of-Trust

asvin hat eine sichere, robuste Lösung entwickelt, um Sicherheitslücken von IoT-Geräten über Updates zu schließen und langfristig funktionsfähig zu halten. Die von asvin bereitgestellte Software-Plattform und die dezentrale Infrastruktur verteilen Updates und Patches für IoT-Endgeräte. Der Vorgang wird dokumentiert und sichert die Auslieferung der Updates durch die Verwendung von smart contracts vor Manipulationen. Mit dem vom Wirtschaftsministerium Baden-Württemberg geförderten Forschungsprojekt „Poison Ivy" entwickelt asvin zusammen mit Spitzenforschern des KIT und der tsenso GmbH ein System zur Absicherung von Datenlieferket-

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

ten. Dabei werden Daten mit einem nachvollziehbaren „Vertrauenszertifikat“ von der Datenquelle bis zur Verarbeitung in der Cloud verknüpft und unveränderlich über ein Blockchain-System nachvollziehbar gesichert. Ziel der innovativen asvin Chain-of-Trust ist es, Hintertüren für datenbasierte Angriffe in KI-Anwendungen zu erkennen und zu schließen. Die Lösung soll die Lücke zwischen den herkömmlichen Angeboten und den High-end-Verfahren füllen und will dazu beitragen, Vertrauensketten in komplexen verteilten Architekturen des IoT bei moderaten Kosten zu ermöglichen. Die Ergebnisse des Forschungsprojektes werden Ende 2021 erwartet.

*Abdruck honorarfrei, Beleg (Print, Scan, Link) erbeten.*

**Über die asvin GmbH**

Im September 2018 gegründet, entwickelt das Stuttgarter Start-up-Unternehmen asvin eine sichere Open-Source-Lösung für den Software-Lebenszyklus im Internet der Dinge. Die Applikation ermöglicht, Sicherheitslücken im IoT und IIoT zu schließen und so Geschäftsprozesse ohne Risiko zu bewältigen. asvin wurde 2020 anlässlich der it-sa zum Besten Cybersecurity-Start-up Deutschlands ausgezeichnet.
Weitere Informationen: www.asvin.io

**Bildmaterial**

Das nachfolgende Bildmaterial kann im Rahmen der Berichterstattung über die asvin GmbH unter Angabe des Quellenhinweises kostenfrei verwendet werden. Hochaufgelöste Dateien erhalten Sie auf Anfrage an medien@seidel-kommunikation.de. Das Bildmaterial darf ausschließlich für redaktionelle Berichterstattungen über die asvin GmbH eingesetzt werden.


Das Führungsteam der asvin GmbH (von links nach rechts): Mirko Ross (CEO), Sven Rahlfs (COO), Rohit Bohara (CTO) / © asvin GmbH

**Kontakt**

seidel kommunikation
Brunnengasse 3
73650 Winterbach (bei Stuttgart)
T: 07181 / 26 29 376
E: medien@seidel-kommunikation.de