PRESSEMITTEILUNG

Mehr IT-Sicherheit für Maschinenbau-KMU

Projekt IUNO Insec entwickelt einfach einsetzbare Lösungen

Bonn, 14. Juli 2022 – Die IT-Systeme von KMU sind in besonderem Maße gefährdet, Opfer von Cyberattacken zu werden. Die fortschreitende Digitalisierung sowie fehlende finanzielle Ressourcen und fehlendes fachliches Know-how machen die Unternehmen zum vergleichsweise einfachen Ziel für Angreifer. Um KMU dabei zu helfen, sich wirksam gegen Cyberangriffe zu schützen, haben im BMBF-geförderten Projekt IUNO Insec Partner aus Wissenschaft und Wirtschaft einfach einsetzbare Lösungen entwickelt. Dazu gehören u.a.:

- **einfach anzuwendende Werkzeuge zur Bedrohungsmodellierung und zur automatisierten Anomalie-Erkennung**
- **Lösungen für mehr Sicherheit bei der Nutzung von Industrial-Clouds**
- **der sichere Fernzugriff auf Maschinen, u.a. für eine sichere Fernwartung**
- **ein kontrollierbares, vertrauenswürdiges Nutzungsmanagement in verteilten digitalen Wertschöpfungsnetzen**

Laut IT-Verband Bitkom haben Cyberkriminelle 2020 bei deutschen Unternehmen Verluste in Höhe von 223 Milliarden Euro verursacht. Das ist mehr als doppelt so viel wie zwei Jahre zuvor. Viele Großunternehmen haben ihre Sicherheitsvorkehrungen seitdem verstärkt, aber kleinen und mittleren Unternehmen (KMU) fehlen oft die finanziellen Ressourcen und das fachliche Know-how dazu. Dadurch werden sie immer öfter zum Angriffsziel böswilliger Hacker.

Das Forschungsprojekt IUNO hatte zwischen 2015 und 2018 eine tragfähige Basis an Sicherheitskonzepten und -lösungsbausteinen für KMU erforscht, prototypisch umgesetzt und deren Mehrwert anhand von Demonstratoren aufgezeigt. Im vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Nachfolge-Projekt IUNO Insec haben Partner aus Wissenschaft und Wirtschaft diese Basis-Konzepte ausgebaut und zu einfach einsetzbaren Lösungen weiterentwickelt, die speziell KMU aus dem industriellen Umfeld in die Lage versetzen, das eigene IT-Sicherheitsniveau anzuheben. Partner von IUNO Insec sind das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC (Verbundkoordinator), die accessec GmbH, die axxessio GmbH, das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI), das Fraunhofer-Institut für Sichere Informationstechnologie SIT und die Technische Universität Darmstadt, Fachgebiet Datenverarbeitung in der Konstruktion (DiK).

Im Projekt IUNO Insec sind Werkzeuge entstanden, mit deren Hilfe KMU ihr eigenes Sicherheitsniveau bestimmen, Zielgrößen für den gewünschten Schutz festsetzen und geeignete Maßnahmen zum Erreichen dieser Zielgrößen umsetzen können. Das versetzt KMU in die Lage, den eigenen Stand der IT-Sicherheit kontinuierlich zu evaluieren und frühzeitig anzupassen, z. B. wenn neue Gefahren bzw. neue Anforderungen des Gesetzgebers oder der Kunden es erfordern:

Testbed zur Evaluation von IIoT-Security
(Leitung: Fraunhofer AISEC)

Das entwickelte Testbed erlaubt eine dynamische Konfiguration von industriellen Netzwerkkomponenten, die auch Dritte nutzen können. Es kann verwendet werden, um das Verhalten der Produktionsumgebung mit und ohne Sicherheitslösungen im Angriffsfall zu simulieren. Für das Testbed wird nur ein Webserver benötigt, was seinen Einsatz in KMU vereinfacht. Die Bibliothek der unterstützten IIoT-Komponenten ist vorkonfiguriert und dynamisch durch Drag-and-Drop nutzbar. Auch eine Konfiguration eigener Geräte durch den Endanwender ist möglich.

Datenbasierte Anomalie-Erkennung
(Leitung: Fraunhofer AISEC)

Mit der Methodik lassen sich Abweichungen in verschiedenen Daten-Szenarien aufdecken, z. B. in Bilddateien, Netzwerkdatenströmen und Finanzdaten. Unerwünschte Zustände, die z. B. durch einen IT-Angriff auf Produktionskomponenten verursacht wurden, können frühzeitig erkannt und Gegenmaßnahmen eingeleitet werden. Die Methode ist besonders für den Einsatz in heterogenen Produktionslandschaften geeignet und kann ohne Vorwissen über mögliche Anomalien eingerichtet und ausgeführt werden.

Kontinuierliche Bedrohungsmodellierung
(Leitung: Fraunhofer SIT)

Bedrohungs- und Risikomodellierungen sind dokumentenlastig und komplex. Eine browsergestützte graphische Benutzeroberfläche vereinfacht es, Architekturmodelle als Basis einer Bedrohungsmodellierung zu erstellen. Mithilfe einer Modellierungssprache und einem graphischen Werkzeug zur Erstellung von Bedrohungsmustern lassen sich bereits existierende Architekturmodelle einfach und nutzungsfreundlich kontinuierlich analysieren.

BAScloud
(Leitung: accessec)

Die BAScloud (BAS: Building Automation System) bildet Daten der lokalen Infrastruktur in einem digitalen Zwilling in der Cloud ab. Dies erfolgt durch digitale Erfassung, Normierung, Speicherung und Bereitstellung von Messdaten. Auch Sollwerte können sicher in die Infrastruktur zurückgesendet werden. Sie verfügt über eine Schnittstelle (API), um relevante Daten für Drittsysteme und -services verfügbar zu machen. Ein Rollen- und Rechte-System erlaubt ein feingliedriges Berechtigungsmanagement. Das technische Netzwerk ist vom Internet getrennt und bleibt so vor möglichen Cyberangriffen geschützt. Die BAScloud steht als Software-as-a-Service (SaaS) zur Verfügung.

Sicherer Fernzugriff auf Assets und Maschinen im Unternehmensnetzwerk
(Leitung: axxessio)

Die Lösung ist speziell für den Einsatz von sicheren Fernwartungsdienstleistungen konzipiert. Durch die Kombination von VPN- und SDN-Technologien werden sichere Verbindungen von außerhalb zu einem bestimmten Endpunkt innerhalb des Unternehmensnetzwerks hergestellt. Die Verwaltung der notwendigen Kontrollen läuft automatisiert ab. Für eine benutzerfreundliche Prozessgestaltung erfolgt die Planung und Durchführung der Fernwartungseinsätze über eine Cloud-Plattform mit verschlüsselter und authentifizierter Verbindung. Die eingesetzten Technologien sind Open Source verfügbar. Damit sind sie unabhängig von Drittanbietern und werden kontinuierlich von der Community weiterentwickelt.

Attributbasiertes Nutzungsmanagement
(Leitung: TU Darmstadt)

Digitale Wertschöpfungsnetze sind durch die dynamische Anzahl unterschiedlichster Teilnehmender geprägt. Das attributbasierte Nutzungsmanagement ermöglicht es, feingranulare Nutzungsregeln aufzustellen, während auf Basis der SDN-Technologie die Nutzung bzw. Kommunikation überwacht und gesteuert werden kann. Die dynamische, flexible und differenzierte Autorisierung und die

Nutzungskontrolle erhöhen die Vertraulichkeit und Integrität der digitalen Kommunikation. Der Betrieb ist auf gängiger Hardware möglich, nur SDN-Switches sind zusätzlich erforderlich.

Simulationsbasierte Nutzungskontrolle
(Leitung: TU Darmstadt)

Um die attributbasierte Nutzungskontrolle optimal einzusetzen, werden genaue Kenntnisse über das zu überwachende System benötigt. Auf Grundlage von Verhaltenssimulationen, die der Produktentwicklung entstammen, kann ein digitaler Zwilling diese Informationen bereitstellen. Der Vergleich von simulierten Systemzuständen des digitalen Zwillings und zulässigen Systemzuständen dient insbesondere zur Verfeinerung der Nutzungskontrolle. Der Betrieb des Simulationsmodells ist auf gängiger Hardware möglich.

Anomalie-Erkennung und Deception Proxy
(Leitung: DFKI)

Insider Threats und Advanced Persistant Threats (APTs) werden oft erst spät, manchmal auch erst einige Monate, nachdem sie das Netzwerk infiziert haben, entdeckt. Doch sie lassen sich durch eine auf Täuschung (engl. Deception) basierende Anomalie-Erkennung frühzeitig aufspüren. Sucht ein Angreifer im Netzwerk nach verwundbaren Servern, wird ihm eine erfundene Login-Seite durch den vorgeschalteten Deception Proxy präsentiert. Sobald der Angreifer mit einem solchen Köder interagiert, macht er sich erkenntlich. Die Implementierung mittels Proxy macht es KMU sehr einfach, auf »Deception« basierende Verteidigung anzuwenden, da die Täuschungselemente, sogenannte »Honeytokens«, nicht auf den Produktivsystemen abgelegt werden müssen, sondern in den Netzverkehr eingeschleust werden können.

Das Projekt IUNO Insec lief von Oktober 2018 bis Juni 2022 und hatte ein Volumen von 4,5 Mio. EUR (davon 85% Förderanteil durch das BMBF).

Kontakt

AXXESSIO GMBH BONN

Jin-Young Lee

Pressestelle

Kurfürstenallee 5

53177 Bonn

Deutschland

Telefon: +49 228 76 36 31 0

lee@axxessio.com

ÜBER AXXESSIO

Die axxessio GmbH ist eine international tätige IT- und Managementberatung, die auf die Konzipierung und Umsetzung großer IT-Systeme und digitaler Transformationsprozesse spezialisiert ist. Zu ihren Kunden zählen führende Unternehmen aus den Bereichen Telekommunikation, Logistik, Finanzdienstleistung und Industrie. Gemeinsam mit ihnen führt die axxessio GmbH strategische und innovative IT-Projekte durch.

Weitere Informationen erhalten Sie unter www.axxessio.com
Folgen Sie uns auf Facebook: www.facebook.com/axxessioGmbH

Pressebereich axxessio GmbH: www.axxessio.com/de/presse

presse@axxessio.com