5 FRAGEN AN...

Sven Uthe, Geschäftsführer und CTO von Devity in Paderborn

Digitale Identitäten für Sensoren, Maschinen und Roboter – was nach Science-Fiction klingt, ist der Treiber für hyperautomatisierte Infrastrukturen. Sven Uthe vom Paderborner Startup Devity erklärt, was sich dahinter verbirgt, welche Chancen sich dadurch ergeben und warum Handeln gefragt ist.

01 WAS IST UNTER DIGITALEN IDENTITÄTEN ZU VERSTEHEN?

Ein Datenaustausch im Industrial Internet of Things (IIoT) ist nur dann sicher, wenn sich die Kommunikationspartner kennen und vertrauen. Digitale Identitäten verifizieren, dass eine Information von einem bestimmten Gerät stammt, und gewährleisten die Integrität der Information. Dafür wird ein digitales Zertifikat verwendet, welches die Identitätsinformationen des Geräts kryptographisch belegt. Richtig geschützt, kann eine Identität nicht manipuliert, gefälscht oder missbraucht werden. So können sich Geräte gegenüber anderen Entitäten wie Datenplattformen ausweisen.

02 WELCHE CHANCEN ERGEBEN SICH DURCH DIGITALE IDENTITÄTEN?

Derzeit erweitern Hersteller ihr Wertversprechen, indem nicht nur ausschließlich Geräte, sondern auch Serviceleistungen verkauft werden. Abgeleitete Aktionen sind jedoch nur dann werthaltig, wenn die Daten authentisch sind. Mit digitalen Identitäten werden komplexe, sichere Prozesse möglich, die Hersteller, Zulieferer und Betreiber weltweit miteinander verbinden. So lassen sich Ursprung und Authentizität von Geräten stets eindeutig nachweisen und Plagiate identifizieren. Auch sind neue Geschäftsmodelle denkbar, etwa ein nutzungsbasiertes Pay-per-Use Modell für Roboter oder das Freischalten von lizenzbasierten Features für einzelne Komponenten.

03 WARUM SOLLTEN HERSTELLER IM JAHR 2023 HANDELN?

Mit gestohlenen Anmeldedaten oder Standardpasswörtern kann sich ein Angreifer als Benutzer ausgeben, den Datenverkehr entschlüsseln und Befehle ändern. Diese Angriffe sind einfach auszuführen, wenn der Verkehr zwischen den Endpunkten nicht authentifiziert und verschlüsselt ist. Weil IT-Sicherheit für Betreiber eine immer größere Rolle spielt, sind die Zulieferer in der Pflicht. Themen wie sichere Lieferketten und starke Authentifizierung gewinnen durch die internationale Normenreihe IEC 62443 an Bedeutung. Um ein sicheres Automatisierungsumfeld zu schaffen, fordern Standards den Einsatz digitaler Zertifikate. So unterstützen Protokolle wie zum Beispiel HTTPS oder OPC UA die sichere Identifikation des Kommunikationspartners mittels digitaler Zertifikate.

04 WAS SOLLTEN GERÄTEHERSTELLER BEACHTEN?

Um ein hohes Maß an IT-Sicherheit für Geräte und Dienste zu gewährleisten, muss bereits in der Geräteproduktion eine Identität ausgestellt werden, die dann beim Einrichten der Geräte aktualisiert wird. Um dies skalierbar durchzuführen, ist eine Public Key Infrastructure (PKI) notwendig. Die PKI liefert kryptografisch sichere, verlässliche und diebstahlsichere Identitäten. Die Identität eines Geräts muss anschließend sicher aufbewahrt werden. Es ist empfehlenswert, dafür einen Sicherheitschip (TPM) zu verwenden. Anschließend muss eine Vertrauenskette entlang der Lieferkette erstellt werden, damit Integratoren und Betreiber das Gerät sicher verwenden können. Dazu muss die Identität des Geräts angefragt, überprüft und bestätigt werden können. Schließlich gilt es, die Geräteidentität vertrauenswürdig im Betreibernetzwerk einzubetten und zu verwalten.

05 WIE KÖNNEN DADURCH KONFIGURATIONSPROZESSE ERLEICHTERT WERDEN?

Bislang erfolgt die Inbetriebnahme eines Gerätes in der Regel manuell durch einen Facharbeiter, was jedoch langsam, teuer und unsicher ist. Dadurch übersteigen die Installationskosten oftmals sogar die Kosten für die Hardware. Mithilfe von digitalen Identitäten können nun Geräte automatisch eindeutig identifiziert werden und zentral mit individuellen Konfigurationen versorgt werden. Die Geräteidentiäten werden digital über den Lieferweg übertragen. So können ganze Geräteflotten mit den gleichen Eigenschaften gleichzeitig für den Betrieb vorbereitet und ausgerollt werden. Dieses Konzept für einen effizienten Bereitstellungsprozess ist das Resultat jahrelanger Forschungsarbeit an der Universität Paderborn. Als Hochschulausgründung haben wir als Devity das Softwareprodukt Keynoa entwickelt und in Zusammenarbeit mit der Janz Tec AG in eine Ende-zu-Ende Lösung für ein industrielles Gateway umgesetzt.

Bilder: *Porträt Devity, Schmuckbild George Prentzas – Unsplash*

www.devity.eu

Kurz erklärt

Vielen Unternehmen fällt es schwer, die Möglichkeit des Internet of Things (IoT) und der Digitalisierung in vollem Umfang zu nutzen. Die Umsetzung ist bereits seit einigen Jahren technisch möglich, scheitert jedoch an der Interoperabilität der Einzelsysteme und einer nachhaltig geplanten IT-Sicherheit. Diesen Status quo fordert das Unternehmen heraus.