Cybersecurity: Risiko-Bewusstsein reicht nicht aus

„Wo viel Licht ist, ist starker Schatten“. Dieses bekannte Goethe-Zitat trifft auch auf die digitale Transformation zu: Die Datenkommunikation nutzt nicht nur dem Unternehmen, sondern lockt auch den Datendieb. Die Risiken der „digitalen Schattenwelt“ beleuchten VDMA-Sicherheitsexperte Steffen Zimmermann , der auch den Besuch des Themenparks Industrie 4.0 auf der Metav 2018 empfiehlt, und Bernd Zapf, Leiter Development New Business & Technology bei der Gebr. Heller Maschinenfabrik GmbH in Nürtingen. Von Nikolaus Fecht

VDMA-Sicherheitsexperte Steffen Zimmermann sieht den Themenpark Industrie 4.0 auf der Metav 2018 als gute Informationsquelle für alle Themen rund um Cybersecurity. „Cybersecurity spielt für Anbieter eine wichtige Rolle, denn es ermöglicht neue, innovative Geschäftsmodelle“, erklärt Zimmermann. Wer beispielsweise Condition Monitoring oder Predictive Maintenance anbiete, müsse sich langfristig nicht nur Gedanken über die technische Realisierung, sondern auch über die sichere Gestaltung des Datenverkehrs machen. Seine Empfehlung für Unternehmen: „Fragen Sie in Düsseldorf die Anbieter ganz gezielt, ob und wie sie das Thema Cybersecurity bei ihren Lösungen berücksichtigen. Dabei geht es zuallererst um die Risikobetrachtung. Ist an die Absicherung vertraulicher Daten gedacht? Wer hat Zugang zu diesen Daten? Wie funktioniert die Datenabfrage aus dem Ausland – also zum Beispiel aus China?

Das Risikobewusstsein in Sachen Cybersecurity habe in den Unternehmen deutlich zugenommen. „Bedrohungen durch den Menschen wie Fehlverhalten und Sabotage, das Einschleusen von Schadsoftware sowie Social Engineering und Phishing stehen dabei nach wie vor an oberster Stelle“, sagt Zimmermann. „Leicht durchzuführende technische Schutzmaßnahmen werden jedoch immer noch nicht ernst genommen.“ Als ein aktuelles Topthema bezeichnet er die mit dem Internet verbundenen Steuerungskomponenten, die sich mit einfachen technischen Mitteln leicht vor Hackern schützen ließen.

Einsatz eines gesicherten Kommunikations-Computers

Wie es funktioniert, zeigt die Gebr. Heller Maschinenfabrik GmbH aus Nürtingen im Themenpark industrie 4.0 in Düsseldorf. „Heller hat gemeinsam mit Siemens in den vergangenen zwei Jahren insbesondere an dieser Frage gearbeitet, um eine sichere Lösung für die Anbindung von Werkzeugmaschinen an das Internet darstellen zu können", erklärt Bernd Zapf, Leiter Development New Business & Technology bei Heller. „Hierzu werden wir unsere Maschinen ausschließlich über einen gesicherten Kommunikations-Computer ins Internet bringen, das heißt zwischen Maschinensteuerung und Kundennetzwerk wird für Verbindungen ins Internet der Industrie-PC Sinumerik Edge von Siemens dazwischengeschaltet."

Sinumerik Edge übernimmt das Auslesen von Daten aus der Maschinensteuerung und speichert diese in einem Ringpuffer zwischen. Die Daten werden entweder weiter verarbeitet oder direkt für die Weiterleitung ins Internet vorbereitet. Auf diese Weise ist gewährleistet, dass keine Direktverbindung vom Internet zur Maschine möglich ist und dass die Daten mit den höchsten Sicherheitszertifikaten verschlüsselt werden. Dieser Kommunikationsweg erfüllt die gesetzlichen Anforderungen an den Cloud-basierten Datenverkehr gemäß der internationalen Normenreihe „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme" (IEC 62443) und entspricht den von Siemens vorgegebenen Sicherheitszertifikaten.

Auf der Metav 2018 demonstrieren die Nürtinger an der Ausbildungsmaschine Profitrainer mit Heller4Industry verschiedene Industrie-4.0-Technologien, beispielsweise beim Datenverkehr mit MindSphere: Dieses offene Internet-of-Things-System von Siemens hilft beim Aufbereiten von Daten. Es handelt sich dabei um eine Cloud-Technologie, die mit unterschiedlichen Cloud-Infrastrukturen (AtoS oder Microsoft Azure) zusammenarbeitet.

Sichere digitale Identitäten: Basis für Datenaustausch

Als Basis für den automatisierten und autonomen Datenaustausch setzt sich der VDMA für die „sichere digitale Identität (SDI" ein. Zimmermann: „Der Anwender sollte die Entscheidungen der beteiligten Systeme anhand von sicheren digitalen Identitäten eindeutig nachvollziehen und zuordnen können." Die Anforderungen an diese Identitäten sind hoch. Sie dürfen sich nur sehr schwer kopieren lassen, müssen fälschungssicher sein und sich auch widerrufen oder weitergeben lassen. Maschinenbauer sollten sich daher jetzt Gedanken machen, wie sie das Thema SDI in die Tat umsetzen können.

Heller zählt auf diesem Gebiet zu den Pionieren. Zapf: „Unter dem Begriff Heller4Industry bieten wir seit der EMO Hannover 2017 für die Nutzung von bestimmten Heller-Bearbeitungszentren ein Betreibermodell mit einer pay-per-use-Bezahlmethode für die Nutzlaufzeit der Maschinen an. Dieses digitale Geschäftsmodell nennen wir Heller4Use. Das digitale Bezahlen geschieht per SEPA-Lasteinzugsverfahren." Das Erfassen der Nutzlaufzeit findet auf einem sicheren Weg im Inneren der Maschinensteuerung mit anschließender Übertragung über Sinumerik Edge zu MindSphere statt, wo die Nutzlaufzeit ausgewertet und Heller-intern über SAP abgerechnet wird.

Definition: Sichere digitale Identität (SDI))

SDI ist eine eindeutige Identität mit zusätzlichen Sicherheits-eigenschaften für eine belastbar vertrauenswürdige Authentifizierung eines Objekts (Entität). Sie verhindert die Vortäuschung einer falschen Identität. Jedes vernetzte Gerät, das über offene Netze kommuniziert, benötigt eine sichere Identität. Hauptziel ist die Identifikation und Authentifikation von individuellen Entitäten. Sechs Merkmale definieren eine SDI: Identifikation, Integrität, Fälschungsresistenz, Offline-Identifikation, Authentifikation und Offline-Authentifikation. (Quelle: Wibu Systems)

Autor: Nikolaus Fecht ist Fachjournalist in Gelsenkirchen.