

# DUAL USE OF DATA ALS OPTIMIERUNGSSTRATEGIE

Investitionen in Cybersecurity-Lösungen werden oftmals als „notwendiges Übel“ gesehen. Als Kehrseite der Digitalisierung, die keinen Return on Investment bringen. Aber das stimmt so nicht. Denn laut T&G bzw. TG Alpha können sogenannte Intrusion Detection Systeme durchaus auch zur Optimierung von Produktionsprozessen beitragen und die Maschinenverfügbarkeit erhöhen. Man müsse die erfassten Daten lediglich aus einem zusätzlichen anderen Blickwinkel betrachten und dementsprechend deuten. **Von Sandra Winter, x-technik**

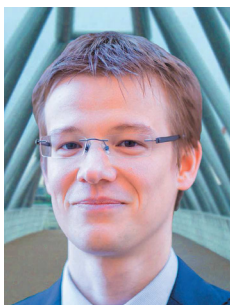
**D**aten gelten als Öl des 21. Jahrhunderts. Sie seien der Rohstoff, aus dem innovative neue Geschäftsmodelle sowie exzellente operative Leistungen entstehen. Demzufolge gewinnt die Erfassung betriebsrelevanter Kennzahlen zunehmend an Bedeutung. Aber was zahlt es sich wirklich aus zu detektieren und in weiterer Folge zu analysieren? Eine Frage, auf die es, je nachdem wer diese stellt – ob ein produzierendes Unternehmen, ein Maschinenbauer oder ein Spezialist für Cybersecurity – mitunter erst einmal unterschiedliche Antworten gibt. Die einen wollen vorwiegend die Produktivität ihrer Anlagen und Abläufe im Auge behalten und zielgerichtet optimieren können, die anderen etwaige Ungereimtheiten in den eigenen Netzwerken aufdecken. Aber trotz dieser divergierenden Schwerpunktsetzungen gäbe es laut Laurin Dörr, Leiter Business Development beim T&G Tochterunternehmen TG Alpha, auch zahlreiche Überschneidungen, die für einen „Dual Use of Data“ sprächen.

„Derzeit wird die Herstellung von Cybersicherheit oftmals als reiner Kostenfaktor gesehen, der als Kehrseite der Digitalisierung halt in Kauf zu nehmen ist. Es ginge aber auch anders. Man könnte die Anomalien, auf die Intrusion Detection Systeme (IDS) aufmerksam machen, als Optimierungshebel nutzen“, erklärt er. So könnten beispielsweise plötzlich auftretende Kom-

munikationslücken eventuell auf einen Maschinenstillstand oder überproportionale Aktivitäten bei den Sensoren, die für das Ausschleusen von Schlechteilen verantwortlich zeichnen, auf eine verdächtig hohe Produktion von Ausschuss hinweisen, die dringend zu hinterfragen wäre.

## Ein gemeinsamer Datenpool für alles als Vision

„Im klassischen Sinn wird ein IDS für die Erkennung eines ungewöhnlichen Kommunikationsaufkommens in Firmennetzwerken eingesetzt, um etwaige Angriffe zu melden. Im Grunde genommen lässt sich damit aber auch der Output eines fertigenden Unternehmens bis zu einem gewissen Grad mitmessen, weil die für beide Themen notwendigen Daten stark korrelieren“, spricht sich Laurin Dörr für eine besser aufeinander abgestimmte Vorgehensweise bei der Suche nach perfekten Lösungen aus. Seiner Einschätzung nach gehe der Trend eindeutig in die Richtung, die in der Nähe von Netzwerkgeräten oder Maschinen installierten Sensoren gleich für mehrere Zwecke einzusetzen. Schließlich sei das eigene IDS-System alphaWatch aus Digitalisierungssicht nichts anderes als ein speziell gehärteter Edge Controller, auf dem neben dem Betriebssystem auch noch eine IDS-Software läuft, die dank innovativer Machine-Learning-Algorithmen permanent mitlernt. Dadurch ist sie in der Lage, selbst unbekannte Anomalien, die nicht durch



„Derzeit wird die Herstellung von Cybersicherheit oftmals als reiner Kostenfaktor gesehen, der als Kehrseite der Digitalisierung halt in Kauf zu nehmen ist. Es ginge aber auch anders. Man könnte beispielsweise die Fähigkeiten eines Intrusion Detection Systems (IDS) zusätzlich auch noch als Optimierungshebel für die Fertigung nutzen.“

**Laurin Dörr, Leiter Business Development beim T&G Tochterunternehmen TG Alpha**



Regeln erfasst werden, aufzuzeigen. Diese Fähigkeit ließe sich auch auf zusätzliche Datenanalysen übertragen. „Die Vision wäre es, alle Daten in einem Pool zu sammeln und dann unter Zuhilfenahme von KI der geplanten Weiterverwendung entsprechend zu filtern bzw. zu clustern, bevor sie dann an die für Cybersecurity, für Lean Management, für die Leitung der Produktion oder für Digitalisierung im Allgemeinen zuständigen Personen weitergeleitet werden“, beschreibt er.

Bei TG Alpha stehe es bereits auf der Roadmap, zunehmend Lösungen zu schaffen, die von Anfang an beide Blickwinkel – jenen von Produktionsseite und jenen aus Sicht der OT-Security Experten – berücksichtigen und clever kombinieren. Demzufolge versuchen die Deggendorfer Spezialisten für eine „sichere Digitalisierung“ bei den von ihnen angebotenen Risikoanalysen-Workshops möglichst viele Unternehmensbereiche einzubeziehen. „Während nämlich die Entwickler beim Einsatz eines Produkts meist vom Optimalfall ausgehen, weiß der Vertrieb um die tatsächlichen Verhältnisse Bescheid und kann somit den Security-Verantwortlichen unter Umständen einen wertvollen Hinweis liefern, wie Produkte bei Kunden eingesetzt werden und ob sich

dadurch etwaige Sicherheitslücken auftun“, empfiehlt Laurin Dörr eine holistische Betrachtung des Ganzen.

### Große Datenmengen benötigen eine Struktur

Eine gut abgesicherte Konnektivität ist eine zentrale Voraussetzung für eine erfolgreiche Digitalisierung, die Verwandlung von Rohdaten in verwertbare Informationen allerdings eine ebenso essenzielle. Man müsse die in Prozesskennzahlen verborgenen Schätze nicht nur heben, anstatt sie in vielleicht sogar schon in Vergessenheit geratenen Datensilos verkommen zu lassen, sondern auch noch entsprechend aufbereiten, um sich die wahren „Gold-Nuggets“, die Richtung Operational Excellence führen, herauspicken zu können, wie es Harald Taschek ausdrückt. Das beginne mit einer „vernünftigen“, einem vorgegebenen Muster folgenden Benennung von Daten. Denn mit von „Nicht-Insidern“ nur sehr schwer oder gar nicht dechiffrierbaren Bezeichnungen für einzelne Prozesswerte fange kein Digitalisierer oder Datenanalytiker etwas an. „Bei einer Maschine mag die Logik so einer frei gewählten Namensgebung vielleicht noch nachvollziehbar sein, aber wenn es darum geht, die Werte mehrerer Anlagen zusammenzuführen, >>

**An sich ist alphaWatch** eine Angriffserkennungslösung, die Künstliche Intelligenz nutzt, um über die gesamte Kommunikation im Netzwerk zu wachen. Man könnte die Fähigkeiten dieses Intrusion Detection Systems (IDS) zusätzlich aber auch noch als Optimierungshebel für die Fertigung nutzen.



Es geht gar nicht so sehr darum, eine Fertigungslandschaft zu realisieren, die komplett durchdigitalisiert oder auf höchstem Level automatisiert ist. Eine vernünftige Transparenz zu schaffen, die gesammelten Daten in einen Kontext zu bringen, für Analysen zu verwenden und davon ableitend dann die nächsten Optimierungsschritte einzuleiten – das sind die Themen, die uns in Zukunft vermehrt beschäftigen werden.

**Harald Taschek, Geschäftsführer bei T&C**



um beispielsweise die Prozesswärmenutzung im gesamten Werk zu optimieren, stößt man mit einem unstrukturierten Datenmaterial schnell einmal an seine Grenzen“, weist der T&G-Geschäftsführer darauf hin, wie wichtig es ist, auf eine entsprechende Modellierung der ausgetauschten Informationen zu achten. In diesem Zusammenhang könnten u. a. die ANSI/ISA 95, die eine standardisierte Terminologie für einen geregelten Datenfluss zwischen verschiedenen Produktionssystemen vorgibt, oder die ANSI/ISA 88 – eine Norm für eine chargenorientierte Fahrweise bei Batch-Prozessen – als Leitfaden dienen.

Auf die sehr häufig an T&G gerichtete Frage, welche Daten es sich am meisten zu sammeln lohne, antworten die Großpetersdorfer in aller Regel: Je mehr, desto besser. Verzichtbares später wieder auszusortieren und wegzulassen sei ohnehin jederzeit möglich. „Idealerweise entsteht durch die regelmäßige Befüllung eines zentralen Datenpools mit klar strukturierten Inhalten im Laufe der Zeit ein Digitaler Zwilling des gesamten Werks, der es erlaubt, über ein generelles Tool unterschiedlichste Reports über den aktuellen Status quo abzurufen“, schildert Harald Taschek einen Weg, der seiner Erfahrung nach unter Garantie zu messbaren Verbesserungen führt. „Es geht gar nicht so sehr darum, eine Fertigungslandschaft zu realisieren, die komplett durchdigitalisiert oder auf höchstem Level automatisiert ist. Eine vernünftige Transparenz zu schaffen, die gesammelten Daten in einen Kontext zu bringen, für Analysen zu verwenden und davon ableitend dann die nächsten Optimierungsschritte einzuleiten – das sind

die Themen, die uns in Zukunft vermehrt beschäftigen werden“, prophezeit er und fügt ergänzend hinzu: „Mit Proficy CSense von GE führen wir ein Advanced Analytics Software-Framework im Portfolio, das produzierende Unternehmen dabei unterstützt, Erkenntnisse aus historischen Daten zu gewinnen, die laufenden Prozesse zu analysieren, prädiktive Vorhersagen zu treffen und ein zielgerichtetes Troubleshooting zu betreiben.“

### Kundenspezifisch anpassbares Out-of-the-Box IoT-Portal

Für den Maschinen- und Anlagenbau hat T&G ebenfalls eine individuell adaptierbare Out-of-the-Box-Digitalisierungslösung parat: OEM Basic – einen secure gestalteten Cloud-Zugang. „IoT-Portale haben gemeinhin zwei Verwendungszwecke zu erfüllen: Zum einen sollen sie den Herstellern von Maschinen und Anlagen helfen, ihre weltweit installierte Basis zu monitoren, um zu neuen Einsichten zu gelangen, die sich positiv auf jedwede Weiterentwicklungs-, Service- und Wartungsaktivitäten auswirken. Zum anderen gilt es, auf Kundenseite alle Hierarchieebenen, vom Maschinenbediener bis hin zum Management, bestmöglich beim Betreiben der Anlage zu unterstützen“, erklärt Armin Taschek, der bei T&G für Vertrieb & Consulting im Bereich Automatisierung und Digitalisierung zuständig ist. Dafür müsse ein IoT-Portal so ausgelegt sein, dass es relativ einfach an neu hinzugekommene Maschinentypen, -ausführungen oder -serien anpassbar ist und gleichzeitig alles abbildet, was an Use Cases aufpoppen könnte – egal, ob bestimmte Grenzwerte zu überwachen und bei de-

**OEM Basic, eine individuell anpassbare Out-of-the-Box-Digitalisierungslösung für den Maschinen- und Anlagenbau** basiert hardwareseitig je nach geforderter Leistungskapazität auf Emerson PACSystems IPCs oder auf Exor-Geräten.



» Mit OEM Basic, einer individuell adaptierbaren Out-of-the-Box-Digitalisierungslösung für den Maschinen- und Anlagenbau, können wir sowohl Neuanlagen als auch alte Bestandsmaschinen mit Steuerungen egal welchen Herstellers anbinden, um in kürzester Zeit ein für den jeweiligen Kunden maßgeschneidertes, zukunftsfähiges IoT-Portal aufzubauen.

**Armin Taschek, Vertrieb & Consulting im Bereich Automatisierung und Digitalisierung bei T&G**

ren Über- bzw. Unterschreiten entsprechende Alarmer abzusetzen, Maschinendaten frei nach Kundenwunsch zu analysieren und auszuwerten, eine Fernwartungslösung zu realisieren, ein automatisiertes Ersatzteilbestellwesen zu integrieren oder vermarktbar digitale Serviceleistungen zu generieren sind. „Wir können sowohl Neuanlagen als auch alte Bestandsmaschinen mit Steuerungen egal welchen Herstellers anbinden, um in kürzester Zeit ein für den jeweiligen Kunden maßgeschneidertes, zukunftsfähiges IoT-Portal aufzubauen“,

beschreibt Armin Taschek mit OEM Basic ein umfassendes Lösungspaket, das hardwareseitig je nach geforderter Leistungskapazität auf Emerson PACSystems IPCs oder auf Exor-Geräten basiert. Bei Letztgenannten befinden sich u. a. ein VPN-Fernwartungsrouten sowie mehr als 200 Kommunikationsprotokolle standardmäßig mit an Bord. Damit sei mit nur einem Device für maximale Konnektivität gesorgt.

[www.tug.at](http://www.tug.at)

XXX