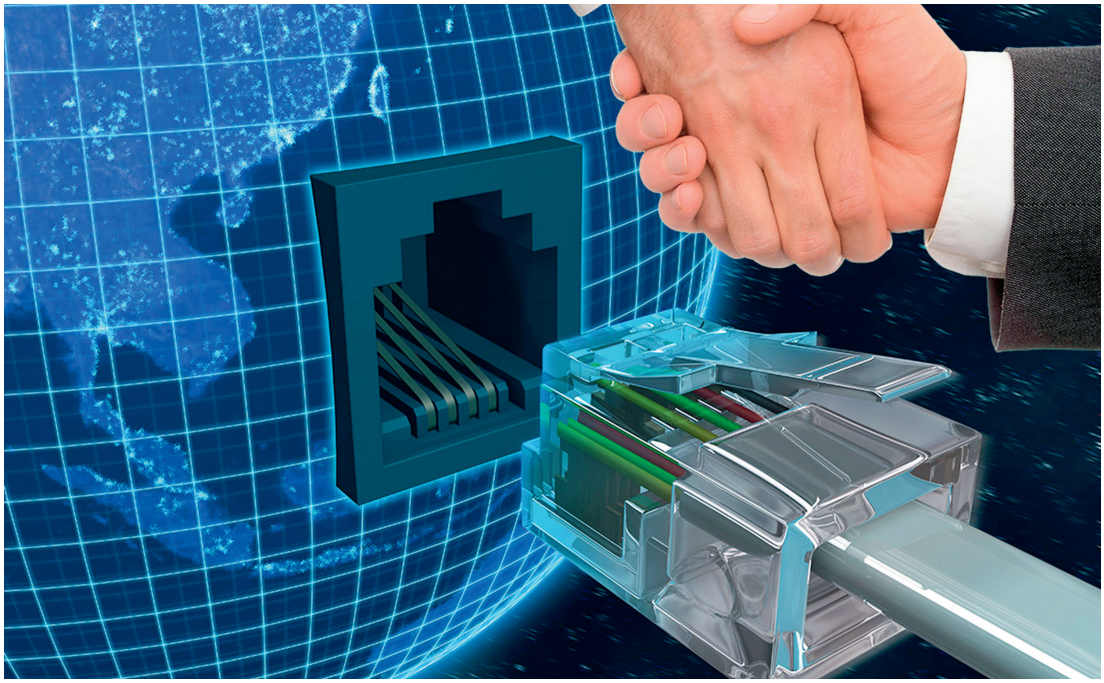

Digitalisierung bedeutet auch immer einhergehend Security-maßnahmen zu beachten, auch im Maschinenbau. (Bild: T&G/TG alpha)

SECURITY BY DESIGN IM RECYCLINGPROZESS

Gezielter Schutz vor Cyberangriffen: Die Themen Nachhaltigkeit und Sicherheit fordern die Produktionswelt täglich aufs Neue. Demgemäß hat sich das oberösterreichische Unternehmen Erema seit seiner Gründung mit beeindruckenden Maschinen für das Kunststoffrecycling zum Weltmarktführer entwickelt. Ihrem Motto entsprechend „We close the loop!" strebt Erema stets danach, den neuesten technologischen Entwicklungen einige Schritte voraus zu sein. So auch, wenn es um das Security by Design seiner Kunststoffrecyclingmaschinen geht. Auf ihrer dazu noch lange nicht endenden Cybersecurity-Route steht Erema die TG alpha GmbH, ein Tochterunternehmen der T&G Automation GmbH, zukunftsorientiert zur Seite. **Von Luzia Haunschmidt, freie Redakteurin**

Gegenwärtig hat sich die Kunststoffindustrie zwei Herausforderungen zu stellen: der Kreislaufwirtschaft und Digitalisierung. Mit diesen Themen beschäftigt sich auch Erema. Dem zugrunde liegt, dass die Ansprüche an das Regranulat beim Kunststoffrecycling stetig steigen, während gleichzeitig stärker verschmutzte Inputströme und neue Materialzusammensetzungen im Recyclingprozess verarbeitet werden müssen. Mithilfe der Digitalisierung eröffneten sich neue Möglichkeiten für die Planung, Steuerung und Organisation dieser Prozesse, um geforderte Mengen an hoher und stabiler Regranulatqualität bereitstellen zu können. Dieser Möglichkeiten sich mehr als bewusst, entwickelte Erema schon früh smarte Technologien zu seinen Recyclingmaschinen wie das „Smart Start-Paket" für einen hohen Automatisierungsgrad. Auch die „QualityOn-Pakete" für die kontinuierliche Messung von Qualitätsdaten wie Farbe, MVR und Zusammensetzung des Inputmaterials während des laufenden Verarbeitungsprozesses sind eine dieser Entwicklungen Eremas bzw. auch das Smart Factory re360, ein MES-System, das Produktions- und Maschinendaten des gesamten bestehenden Maschinenparks erfassen kann. Weitere Assistenzsysteme und Informationstools stehen seit 2019 den Erema-Kunden über deren Kundenplattform BluPort – wo bestehende und neue digitale Assistenzsysteme stets auf dem neuesten Stand gebündelt sind – zur Verfügung.

„Auf dieser Onlineplattform bündeln wir übersichtlich und benutzerfreundlich praktische Dienstleistungs- und Datenaufbereitungs-Apps, die unsere Kunden bei der Qualitätskontrolle unterstützen und so die Maschinenperformance steigern. Mit Fokus auf Datensicherheit und Kundennutzen ergänzen und erweitern wir laufend unser Angebot auf BluePort", so Erema Managing Director Markus Huber-Lindinger.

Cybersecurity auf der Maschinenebene

Bei allen Digitalisierungsanstrengungen sind stets die damit einhergehenden internationalen Normen und Verordnungen zu berücksichtigen – so, wie dies als Maschinenhersteller sowie -betreiber seitens der Safety-Vorschriften

> Die Themen Security und Safety sind fortlaufende Prozesse, die immer wieder Abstimmungen bedürfen. Sämtliche Schwachstellenanalysen werden von T&G/TG alpha stets für Erema dokumentiert. So entsteht ein Konzept für dringlich zu erledigende Handlungen und Verbesserungen, die langfristig umzusetzen sind.
>
> **Laurin Dörr, Businessdevelopment-Leiter der T&G-Tochterfirma TG alpha GmbH**

der Maschinenrichtlinien zu beachten ist. So haben seitens nach IEC 62443 Hersteller wie Betreiber von Maschinen einen risikobasierten Ansatz zur Vermeidung und Behandlung von Sicherheitsrisiken zu beachten. Auch die neuen Regelungen der Cybersicherheits-Richtlinien NIS 2 zu Netz- und Informationssystemen, die seit 16. Jänner 2023 in Kraft getreten und bis spätestens Oktober 2024 in Österreich umzusetzen sind, betreffen sämtliche Unternehmen kritischer Infrastrukturen und Anbieter digitaler Dienste und stellen auch Maschinen- und Anlagenbauer vor Herausforderungen.

Damit war für Erema bereits vor zwei Jahren klar, sich mit den dazu neuen Gegebenheiten zu befassen und Vorkehrungen rechtzeitig in Angriff zu nehmen. Dazu prüfte der Kunststoffrecyclingspezialist vorab gemeinsam mit Unterstützung von TG alpha GmbH, welche Cybersecurity-Bedrohungen und damit einhergehenden Schutzmaßnahmen bei seinen aktuellen Maschinenkonzepten und deren Architektur in Frage kommen. „Unser Ziel ist es, ein Plug-&-play-fertiges Security-Konzept für unsere Maschinen übergeben zu können, damit Kunden das eigene Maschinen-Netzwerk sicher und systemfrei andocken können“, erklärt Markus Steininger-Arbeithuber, Software Engineer bei Erema.

Schritt 1: Risikoanalyse

„Im Vorfeld starten wir mit einer Risikoanalyse anhand eines speziell dafür erstellten virtuellen Maschinenmodells. Im Anschluss bewerteten wir in einer zwei Tage dauernden Analyse die potenziellen Gefahren für die Maschine während ihres Betriebs und verknüpften diese mit den daraus folgenden möglichen Schäden. Als Ergebnis davon erhielten wir ein S-Coding, das beschreibt, wie hoch die Gefahren im Vergleich mit den bereits getroffenen Gegenmaßnahmen ausfallen und welche ungesicherten Gefahrenquellen noch teilweise oder gänzlich abzugleichen sind“, führt der Experte aus. „Wichtig dabei ist – und das betonen wir in unseren Workshops – dass mögliche Lösungsansätze zu den noch ungesicherten Gefahrenquellen unmittelbar erarbeitet werden“, so Laurin Dörr, Businessdevelopment-Leiter bei TG alpha GmbH. Dabei ist zu prüfen, welche Lösungsansätze hinsichtlich ihrer Wirtschaftlichkeit umsetzbar und im Rahmen der geltenden Normen und Verordnungen verpflichtend sind.

Schritt 2: Härtung der bestehenden Hard- und Software

„Aufgrund der Ergebnisse der Risikoanalyse erhält man den Überblick zu sämtlichen noch zu bewerkstelligenden Cyberrisiken auf der Maschinenebene. Damit wird es relativ einfach, innerhalb der Entwicklungsabteilung eine Security-Roadmap aufzustellen. Wie Laurin Dörr bereits bemerkte, gilt es dazu die softwaretechnischen Belange, aber noch häufiger die Hardware resilient zu gestalten, um die wesentlichen Systemdienstleistungen bei Gefahr in Verzug aufrecht zu erhalten“, führt Steininger-Arbeithuber aus. „Das heißt dann in die Umsetzung zu gehen, wie etwa neue Einstellungen vorzunehmen, bestimmte Prozesse durchzuführen und diese folglich einem Update zu unterziehen. Das ist ein ziemlicher Entwicklungsaufwand, jedoch ohne erhöhte Kostenaufwände für einen möglichen zusätzlichen Hardwarebedarf oder Softwareaufwand.“

Arbeitstechnisch heißt dies im Detail festzumachen, wie man die Bereitstellung der Maschinendaten organisiert bzw. welche Protokolle und Schnittstellen sich dazu eignen. Auch die Fragen des Datenhostings sind zu überdenken: Benötigt man zusätzlich zur eigenen Cloud die eines Fremdanbieters? Welche Clouds und Kommunikationsschnittstellen sind sicher? Welche Firewalls sind in hohem Maß wirksam und vor welchen Cyberattacken schützen diese auf der Maschinenebene? Ebenso nicht zu vergessen ist die Klärung der Administration und Funktionalitäten der Zugriffsrechte, etwa für die Fernwartungsservice-Mitarbeiter des Maschinenherstellers, wie auch für die Maschinenbediener im Produktionsprozess. „In dieser Phase schafft man die Rahmenbedingungen für die Systeme, damit diese genau detektieren können, woher welche Angriffe >>

Shortcut

Aufgabenstellung: Security by Design der Erema-Kunststoffrecyclingmaschinen umsetzen; Digitalisierungsstrategie fokussieren; Kreislaufwirtschaft und entsprechende Maschinenansprüche umsetzen; Normen und neue Richtlinien einhalten

Lösung: Ausführliche Beratung und Lösungsansätze vonseiten TG alpha GmbH zu den erforderlichen Maßnahmen.

Nutzen: Aktuelle Gesetztes- und Normenentwürfe sowie neue Richtlinien werden dem aktuellen Anforderungsstand nach für die entsprechenden Maschinen umgesetzt.

Die INTAREMATVEplus DuaFil Compact von Erema erzielt feinste, doppelt gefilterte Regranulat-Qualität auf eine extrem energiesparende Art.

kommen. Entsprechend reagierende Abwehrmaßnahmen sind zu setzen", so Dörr.

Implementierung von Angriffserkennungssystemen

Derart „einfache" Mittel zum Zweck sind beispielsweise die Anlegung individueller, benutzergeprüfter Zugriffsrechte. So wäre etwa im Fall eines gehackten Mobiltelefons eines Maschinenbedieners schnell die Ursache einer Maschinenstörung bis hin zum Angreifer eruiert. Um solchen Virenattacken entgegenzuwirken, müssen hinsichtlich der Cybersecurity entsprechende Verhaltensregeln vermittelt werden. „Dies gelingt in erster Linie durch regelmäßige Mitarbeiter-Workshops. Denn die besten technischen Vorkehrungen bringen nichts, wenn die Mitarbeiter nicht mitmachen", so Dörr. „Deshalb spricht man von der ‚Härtung der Systeme' im ersten Schritt und startet in Folge den zweiten Schritt dort, wo man noch nicht ausreichend Sicherheit geschaffen hat, nämlich bei der Resilienz der Mitarbeiter. Hierzu schränkt man den Personenkreis ein, der tatsächlich und unbedingt Zugang zur Maschine benötigt. Steininger-Arbeithuber erklärt: „Laut den Ergebnissen unserer Risikoanalyse hatten wir in der Vergangenheit bereits für die Erlangung der Cybersecurity auf unseren Maschinen recht gut vorgearbeitet. Verbesserungen konnten wir allerdings noch in den Bereichen der Datenvisualisierung ausmachen und auch auf der Organisationsebene der Zugriffsberechtigungen."

Schritt 3: Integritätsschutz

Ein weiteres Thema, das die Engineering-Abteilung bei Erema beschäftigte, ist die Regelung der Maschinenverordnung nach IEC 62443, die die umfängliche Nachweispflicht der auf der Maschine laufenden Software in Bezug auf Industrial Security verlangt. Steuerungssysteme sind zunehmend vernetzt und kommunizieren über öffentliche Netze. Mit Cyber-Physical Systems fusioniert die analoge Welt mit der physischen und die digitale Welt mit der virtuellen Realität. Dieser auch als Industrie 4.0 bezeichnete Trend bietet aber nicht nur Komfort und Mehrwert, sondern öffnet die Systeme und erhöht damit die Gefahr für Angriffe von außen. Durch Integritätsschutz-Maßnahmen werden Verfügbarkeit und Sicherheit der Systeme gewährleistet, und zwar auf der Safety- und Security-Ebene.

„Dazu haben wir die cybersicherheitstechnischen Änderungen der Maschinensoftware von Erema verifiziert und im Prozess deren Verfügbarkeit gegengeprüft bzw. validiert", ergänzt Dörr. Damit wird auch dem Integritätsschutz laut den Maschinensicherheitsrichtlinien entsprochen. Den Zeitaufwand hierfür schätzt Steininger-Arbeithuber „mit etwa zwei Monaten ein, der schlussendlich von zwei Mitarbeitern in Zusammenarbeit mit mehreren Abteilungen bei uns im Haus bewältigt wird. Wir haben dazu eigens eine Arbeitsgruppe installiert, um die aus der mit T&G/TG alpha aus der Risikoanalyse generierten und empfohlenen cybersicherheitstechnischen Neuerungen zu implementieren. Wichtig in diesem Projekt ist uns aber auch, dass diese Neueinführungen ebenso den Bedürfnissen unserer Kunden entsprechen – und dazu gilt es natürlich in Folge für manche Kundenanforderungen immer wieder adäquate Anpassungen auszuarbeiten."

Schritt 4: Penetrationstests

„Security und Safety sind fortlaufende Prozesse, die immer wieder Abstimmungen bedürfen. Sämtliche Schwachstellenanalysen werden somit von T&G/TG alpha für Erema dokumentiert", führt Dörr aus „So entsteht ein Konzept für dringlich zu erledigende Handlungen und für Verbesserungen, die langfristig umzusetzen sind." Nachdem das Erema-Engineering-Team die Optimierungen durchgeführt hat, werden von T&G/TG alpha umfassende Penetrationstests auf der Geräteebene vorgenommen. „Ein weiterer Gegencheck fällt dann noch auf der Prozessebene von uns an, der auf die Einhaltung der vorgeschriebenen Norm IEC 62443 und andererseits laut den Grundschutz-Vorgaben für angewandte industrielle sichere Systeme des BSI (Bundesamt für Sicherheit in der Informationstechnik) abzielt, da diese intensiver auf die technischen Ausstattungen an sich eingehen", so Dörr. „Das Ziel von T&G/TG alpha ist immer gemeinsam mit den Kunden Wissen aufzubauen, die Cybersicherheits-Standards effizient und wirtschaftlich umzusetzen und damit zur Vertrauenssteigerung gegenüber Kunden beizutragen. Nach erfolgreichen Auditierungen und Penetrationstests wird daher ein entsprechendes Zertifikat ausgestellt, welches Erema zum Nachweis gegenüber Kunden verwenden kann."

Schritt 5: Cyber Resilience Act

Ein weiterer Gesetzesentwurf ist der geplante Cyber Resilience Act der EU, der eigens Anforderungen an die Cybersecurity für alle Komponenten-, Maschinen- und Anlagenhersteller wie deren Betreiber stellt. So sollen Produkte mit digitalen Elementen vom Design über die Herstellung bis hin zur Nutzung höhere Sicherheitsvorgaben erfüllen. Im Klartext betrifft dies Produkte sowohl aus dem B2B-Bereich, wie Steuerungen und Sensoren, als auch reine Softwareprodukte wie Betriebssysteme. „Diese Verordnung, die voraussichtlich im Herbst 2023 umgesetzt wird, hat es

> Die Zusammenarbeit mit der T&G/TG alpha war von Beginn an sehr gut. Es wurde laufend in kleinen MS-Teams-Meetings der aktuelle Stand vonseiten TG alpha kommuniziert. Auf Fragen meinerseits wurde stets sehr schnell reagiert.

Markus Steininger-Arbeithuber, Software Engineer bei Erema

in sich. Abhängig von den möglichen Auswirkungen, müssen Hersteller vor der Inverkehrbringung von Produkten mit digitalen Elementen sicherstellen, dass diese ohne bekannte Schwachstellen ausgeliefert werden. Dazu gehören deren technische Dokumentation und auch die Bewertung von Cybersicherheitsrisiken. Nach der Inverkehrbringung haben Hersteller weiters Melde- und Korrekturmaßnahmepflichten zu erfüllen", so Dörr.

Ein weiterer Verordnungsentwurf, der bis Oktober 2024 für alle EU-Länder zum nationalen Gesetz wird, konzentriert sich auf die Herabsetzung der Grenzwerte sämtlicher Unternehmen kritischer Infrastrukturen. Hier wurde die Liste der betroffenen Unternehmen um Hersteller wie des Maschinenbaus, Fahrzeugbaus, von Elektronikkomponenten und des Recyclings ausgeweitet. „Das bedeutet, dass unsere Kunden künftig auch zu den Betreibern kritischer Infrastrukturen klassifiziert werden", resümiert Steininger-Arbeithuber. „Was uns als Maschinenhersteller wiederum fordert, jegliche Cybersicherheit-Dokumentationen an unsere Kunden verpflichtend weiterzugeben, damit sie diese in ihren eigenen Anlagenkonzepten umsetzen können. Mit steigenden Kundenanforderungen hinsichtlich Cybersecurity ist kurzfristig zu rechnen." Dörr schließt seine Ausführungen ab: „Somit macht es in jedem Fall Sinn, sich schon heute mit allen künftigen neuen Gesetzen diesbezüglich zu befassen.

Dass T&G/TG alpha auf diesem Weg eine richtungsweisende wie wertvolle Hilfe darstellt, unterstreicht Steininger-Arbeithuber: „Die Zusammenarbeit mit der T&G/TG alpha war vom ersten Tag an sehr gut. Es wurde immer wieder in kleinen MS Teams-Meetings der aktuelle Stand vonseiten TG alpha kommuniziert und auch auf Fragen von meiner Seite wurde immer sehr schnell reagiert. Ich freue mich auf die weitere Zusammenarbeit mit T&G/TG alpha."

www.tug.at

Anwender

Erema mit Sitz im oö. Ansfelden bei Linz hat sich seit seiner Gründung 1983 mit innovativen Maschinen für das Recycling von Kunststoffen zum Weltmarktführer entwickelt. Lösungsorientiert werden dazu durchdachte, zuverlässige Maschinen und Komponenten kreiert. Aktuell sind etwa 7.500 ihrer Systeme weltweit im Einsatz. Gemeinsam werden jährlich mehr als 20 Millionen Tonnen hochwertigstes Granulat produziert. Erema forscht dazu laufend nach neuen Technologien und weiteren Optimierungen.

EREMA Group GmbH
Unterfeldstraße 3, A-4052 Ansfelden, Tel. +43 732-3190-0
www.erema-group.com