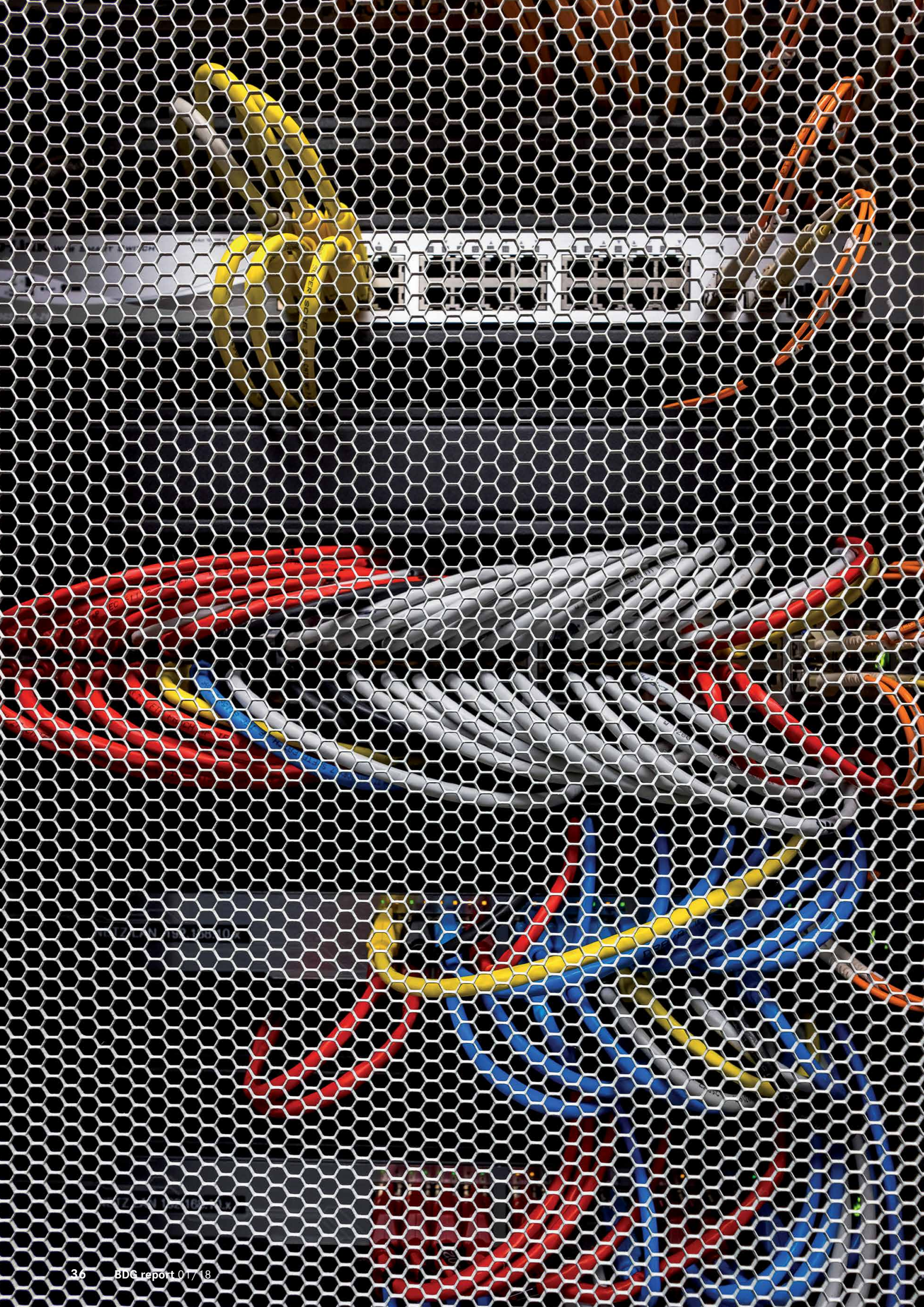


Die heile Welt der allseits gepriesenen Industrie 4.0 hat einen Haken. Mit der rasanten Entwicklung des Internet, auf das Industrie 4.0 aufbaut, ist auch die Cyberkriminalität gestiegen.

IT-Sicherheit für die Fabrik der Zukunft

Die zunehmende Vernetzung und Digitalisierung der Industrie geht mit steigenden IT-Sicherheitsrisiken einher. Der Grund: In einer technischen Umgebung, die vernetzt wird, nimmt der Einsatz von Geräten zu, die mit dem Internet kommunizieren. Unternehmen sollten parallel zur Einführung neuer Technologien daher immer ein Sicherheitskonzept verfolgen, um sich vor Gefahren zu schützen, die von Cyberkriminellen etwa durch Trojaner, Hacks oder Überlastungsangriffe drohen. Der BDG report besuchte die Eisengießerei Karl Casper Guss in Remchingen, einem Pionier in Sachen Industrie 4.0.

Von Robert Piterek, Düsseldorf

Karl Casper, Guss
Gründungsjahr:

1877

ca 100 Beschäftigte
Gussgewichte: 100 Kg bis 6 Tonnen

Karl Casper Guss betreibt eine hochwertige Firewall, die in Millisekunden auf Attacken reagieren und Netze sperren kann.

Fotos: Andreas Bednareck

Die Vorteile einer vernetzten Produktion sind verlockend. Bei Karl Casper Guss in Remchingen nahe Karlsruhe ist schon vieles Realität, von dem andere Gießereien noch träumen: Der Kunde kann sich im Minutentakt über den Stand aktueller Aufträge informieren. Sendet er regelmäßig Liefervorschauen, erhält er schon einen Tag nach der Bestellung seine Lieferung. Bei Karl Casper Guss selbst sind durch die technologische Aufrüstung zugleich Ausfallzeiten und Störfälle massiv gesunken, während die Verbrauchsermittlung, z. B. von Harz und Sand, mit Hilfe von Sonden schon zu einer weitgehenden Automatisierung der Bestellungen von Hilfs- und Betriebsstoffen geführt hat. „Ich kann mit einem Dashboard auf meinem Computerbildschirm in Echtzeit alle relevanten Daten abrufen, wenn der Kunde anruft“, schwärmt Malte Lüking, Technischer Geschäftsleiter bei Karl Casper Guss. „Wir wissen exakt, welcher Kasten wann gefüllt wurde, mit welchen Harzen und Härtern und bei welcher Außen- und Innentemperatur“, ergänzt der Mann, der einen beeindruckenden Wandel vom großen Skeptiker zum glühenden Anhänger der Digitalisierung in der Gießerei-Industrie durchgemacht hat. Lüking redet schnell, man kann sich gut vorstellen, dass ihn Echtzeit-Informationen wie diese bei seiner täglichen Arbeit ungeheuer unterstützen.

Karl Casper Guss-Datenschutzkoordinator Jens Trentini im Serverraum der Eisengießerei. Der IT-Fachmann ist in alle Planungsrunden für neue Anlagen und Software eingeweiht.

Der Visionär hinter den Kulissen

Lüking hat Gießereitechnik in Duisburg studiert und kennt Karl Casper Guss in- und auswendig. Schon sein Vater war hier Geschäftsleiter. Er ist der Visionär hinter den Kulissen, der das Unternehmen zu einem Vorreiter bei der Digitalisie-

Die Geschäftsleiter Felix Casper und Malte Lüking mit BDG-Redakteur Robert Piterek und IT-Koordinator Jens Trentini (v. l. n. r.).

rung in der deutschen Gießereibranche gemacht hat und nun immer weiter vorantreibt. Kurz nach seinem Eintritt ins Unternehmen 1997 stellte er einen ersten PC in der Produktion auf. Anfangs belächelt, setzte sich der Einsatz von IT in der Produktion immer weiter durch. Erste Projekte mit anderen Gießereien wie Dossmann aus Walldürn verschafften dem IT-interessierten Gießerei-Ingenieur erste Erfahrungen mit ERP-Systemen. Nach einem fehlgeschlagenen Versuch im Jahr 2000, arbeitsgangbezogene Rückmeldungen der Fertigungsschritte im Unternehmen einzuführen, startete Lüking 2005/2006 einen weiteren Versuch mit erfolgreichem Ausgang, der Karl Casper Guss zu einem der Pioniere in diesem Bereich machte. Mit Partnern wie SSSoft aus Aalen ging er in der Folge die Themen Vernetzung und Industrie 4.0 an, noch bevor der Trend-Begriff in aller Munde war. Die Skepsis überwog aber weiterhin – eine vergleichsweise günstige Vernetzungslösung für 30 000 Euro trug er aber testweise mit. Von da an wuchs seine Begeisterung im Zusammenspiel mit den Partnern von Tag zu Tag: „Wir haben uns im Bereich Vernetzung von Daten gegenseitig hochgepuscht und uns ausgemalt, dass wir Verbräuche ermitteln und Überwachungen in Echtzeit abgreifen können. Dann haben wir die Anlagen Stück für Stück ans Netz angeschlossen“, erinnert er sich. Lüking brachte sich jetzt verstärkt bei der Integration der Fertigungssteuerung Struktura Form des Softwareherstellers RGU im Unternehmen ein und beschäftigte sich parallel mit der Vernetzung der Anlagen. In der Folge standen immer mehr Daten zur Verfügung, was nahezu zwangsläufig zum nächsten Schritt führte: der Einführung eines Extranets mit dem Softwarepartner JKDV, um Kunden den Datenschatz zugänglich zu machen. Ein Intranet mit einer eigenen Fertigungssteuerung für die Arbeitsvorbereitung und die Anbindung der Qualitätssicherung ans Netz folgten, sodass nun Daten aus beiden Bereichen ausgewertet werden können. Aus dem einsamen PC in der Produktion, den Lüking vor über 20 Jahren aufstellte, sind inzwischen allein in der Elektroofen-Warte sechs geworden.

40 Server für Industrie 4.0

Im Werk selber wurden an allen Anlagen – vom Sandmischer über die Sandregenerierung bis zur Strahlanlage – digitale Arbeitsanzeigen angebracht, die über sogenannte virtualisierte Systeme mit den Servern verbunden sind und so effizienter und schneller funktionieren als mit einer direkten Serververbindung. Der Datenschatz, der mittlerweile auf 40 Servern schlummert, ist beachtlich: 16 Terabyte umfassen die Betriebsysteme, Programme und laufenden Daten auf dem Netzwerk-Speicher. Verglichen mit dem durchschnittlichen Datenvolumen je Haushalt in

Casper Guss-Mitarbeiter Sacher Kast erfasst Daten eines Hermle-Gussteils an der Rückmeldestation in der Geißereihalle. Ist die Rückmeldung per Bar-Code-Lesegerät erfolgt, können am Monitor zugleich Informationen über die Stückzahl, das Modell und die Bezeichnung abgelesen werden.

Deutschland, das 2017 nach Angaben der Bundesnetzagentur rund 60 Gigabyte pro Monat betrug, ist für den Betrieb der Software für Fertigungssteuerung, Vernetzung und Rückmeldung also so viel Datenvolumen erforderlich wie knapp 300 Haushalte im Monat verbrauchen. Historisch betrachtet nimmt die Datenflut (oder Big Data) auf der Erde übrigens exponenziell zu: Die bis 2003 gesammelte Datenmenge von fünf Milliarden Gigabyte wurde 2011 in 48 Stunden und 2013 bereits in zehn Minuten erreicht.

Und die Nutzung der zahlreichen ermittelten Daten in der Remchinger Eisengießerei lohnt sich. Felix Casper, kaufmännischer Geschäftsführer des Familienunternehmens, bringt es auf eine kurze Faustregel: „Die Systematik Industrie 4.0 geht in die Beschaffung, in die Produktion und in den Vertrieb. So können wir in all diesen Bereichen optimierter arbeiten."

Volkswagen wehrt 6000 Angriffe täglich ab

Doch die heile Welt der allseits gepriesenen Industrie 4.0 hat einen Haken. Mit der rasanten Fortentwicklung des Internet, auf das Industrie 4.0 aufbaut, ist auch die Cyberkriminalität kontinuierlich gestiegen. Laut dem Handelsblatt muss sich etwa Volkswagen 6000 Mal am Tag gegen Angriffe auf sein IT-Netz wehren, das Regierungsnetz erfährt 20 hochspezialisierte Angriffe täglich. Wegen der steigenden Zahl gehackter und geplünderter Privatkonten haben Banken Entschädigungsfonds eingerichtet, die Glaubwürdigkeit demokratischer Wahlen steht wegen möglicher Manipulationen durch sogenannte Internet-Trolle fremder Nationen auf dem Spiel. Der jährliche Schaden durch Cyberkriminalität soll bundesweit bei 51 Mrd. Euro liegen, was dem Staatshaushalt eines kleinen Landes entspricht.

Cornelius Kopke, Senior Consultant Cyber Security bei Capgemini, bringt in seinem Meinungsbeitrag ab S. 22 auf den Punkt, was die Reaktion auf diese Entwicklung sein muss: „Die Digitalisierung gelingt nur, wenn Sicherheit mitgedacht wird und von Anfang an den notwendigen Stellenwert in den Entwicklungen neuer Produkte, Services und Technologien erhält. Kurz: Sicherheit ist nicht alles, aber ohne Sicherheit ist alles nichts!"

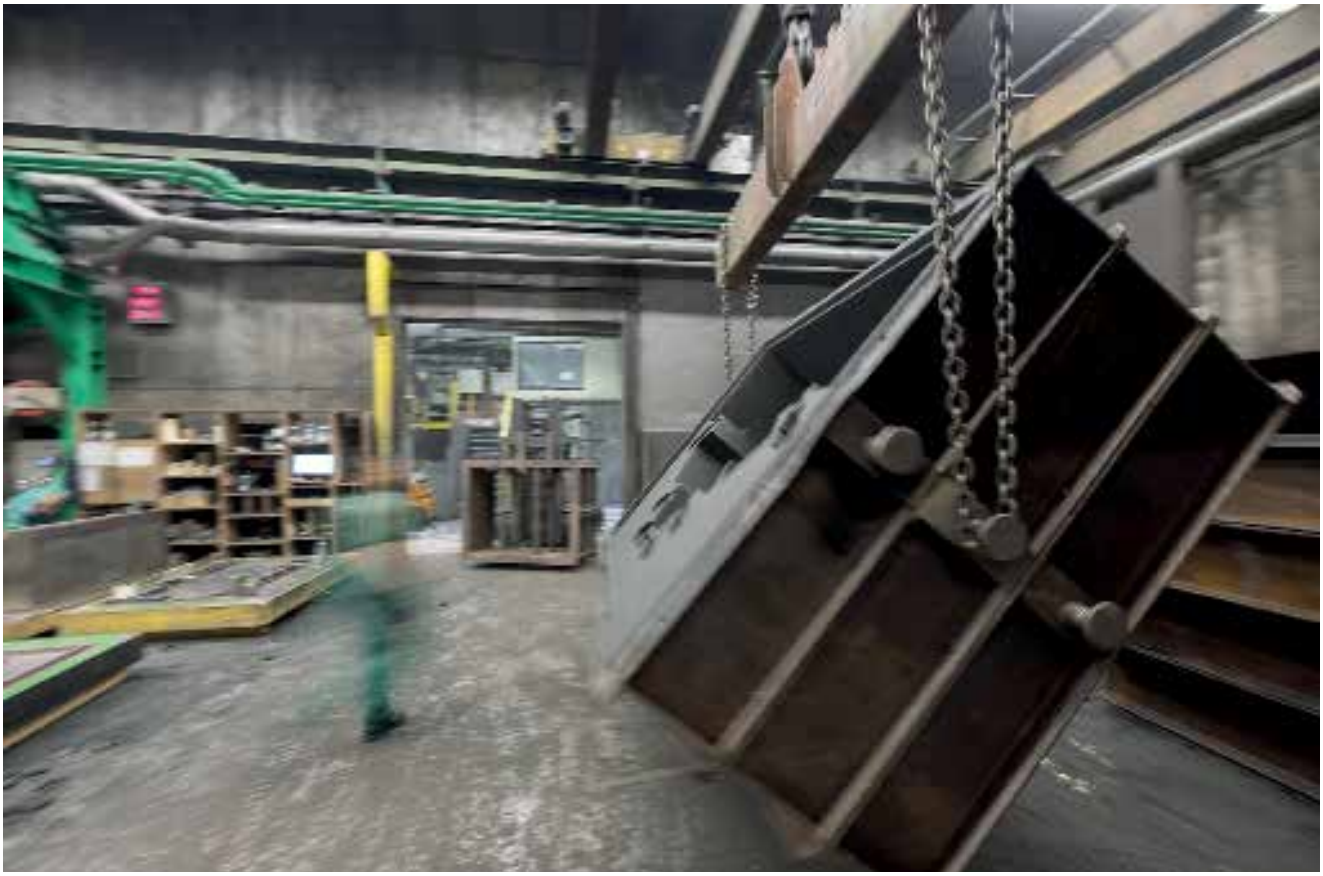
Cybersicherheit im Blick

Langjähriger Dienstleistungspartner bei Karl Casper Guss ist die Remchinger Trentini GmbH. Ihr Geschäftsführer Jens Trentini ist bei Casper zugleich IT-Beauftragter und Datenschutzkoordinator und begleitet den Aufbau der IT-Infrastruktur in der Eisengießerei aufmerksam und kritisch. Der IT-Fachmann ist in die Planungsrunde jeder neuen Anlage und die Anschaffung jeder neuen Software eingebunden und hat seit 2010/2011 neben der Funktionalität der Anlagen immer auch das Thema Cybersicherheit im Blick gehabt. Doch wie können Attacken, die so große Player wie Volkswagen oder die Bundesregierung in Bedrängnis bringen, erfolgreich abgewehrt werden?

Abguss von Eisenschmelze in eine mit Gewichten beschwerte Form. Die Gießerei fertigt Bauteile für große Werkzeugmaschinenbauer.

„Wir haben die Verschiedenen Netze, wie Verwaltungs-, Produktions-, Telefon- und WLAN-Netz konsequent voneinander getrennt", erklärt Trentini die Sicherheitsstrategie von Karl Casper Guss. Im Rahmen von VISU werden mit intelligenten Produktionsüberwachungssystemen alle Anlagen, Schmelzöfen und Produktionsprozesse in Echtzeit überwacht und gesteuert, um die Produktions- und Verbrauchsdaten zur Optimierung und Störungsbehebung auswerten zu können. „So können die Berührungspunkte mit dem Internet minimiert werden", ergänzt er. „Darüber hinaus haben wir im ERP-System Strukturen geschaffen, um Wildwuchs zu vermeiden, der Schwachstellen schaffen und das Risiko erhöhen kann."

Die Entscheidung, die Netze zu trennen und eine hochwertige Firewall zu installieren, die in Millisekunden auf Attacken reagieren und Netze sperren kann, fiel bereits vor sieben Jahren. Neuralgische Punkte bleiben aber alle Verbindungen nach draußen – das betrifft Mitarbeiter und Kunden gleichermaßen. „Jeder neue Kunde ist zunächst einmal gesperrt – wir müssen seinen Port erst freigeben", verrät Trentini und fügt erklärend hinzu: „Ein Verschlüsselungstrojaner zum Beispiel braucht immer eine Verbindung nach draußen, sonst funktioniert er nicht." Ist der Kunde dann erst im System, steht ihm eine Datenbank zur Verfügung, die aber nicht etwa direkt an die internen Systeme angedockt



Ein gewaltiger Formkasten wird mit einem Hallenkran bewegt. In der Eisengießerei im badischen Remchingen arbeiten rund 100 Mitarbeiter im 3-Schicht-Betrieb.

ist, sondern von einem ausgelagerten Bereich gespeist wird, der Daten von einem gesicherten Port abruft. „Wird der Port dennoch geknackt, können so nur Daten abgegriffen werden, die dem Kunden ohnehin zur Verfügung gestellt werden – eine Gefahr für die interne Produktion gibt es nicht", betont er.

Die wichtigsten Sicherheitslecks

Beim Kauf oder der Entwicklung neuer Software hat der IT-Techniker insbesondere zwei Dinge im Blick: ob sie kompatibel mit anderer Software ist und in einer zentralen Datenbasis bereitgestellt werden kann.

Um die Daten zu schützen, ist besonders ein durchdachtes Backup-System, das Daten automatisch und mehrstufig speichert, unverzichtbar bei der Sicherheitsplanung einer digitalsierten Produktion. Bei Karl Casper Guss speichert das System Daten in einem nachgelagerten Bereich, um ausgefeilten Computerviren den Zugriff zu erschweren. 100prozentige Sicherheit vor der Kreativität von Cyberkriminellen gibt es aber nicht: „Wenn alles schiefgeht, müssen wir auf maximal eine Woche alte Daten zugreifen", gesteht Trentini ein. Sichert ein Unternehmen seine Daten nicht oder zu selten, kann es im Falle eines Datenraubs zum Erpressungsopfer werden. Zahlreiche Fälle, in denen hohe Bitcoin-Summen erpresst wurden, sind dokumentiert.

Die größten Sicherheitslecks bei der Digitalisierung von Unternehmen sind jedoch die berüchtigten Standardpasswörter und der Mensch. Bei allen IT-Systemen, z. B. Siemens-SPS-Steuerungen, sind im Werkszustand entweder keine oder Standardpasswörter, wie z. B. die Zahlenfolge 1234, eingespeichert. Werden sie nicht geändert, sind sie eine Einladung für Hacker. Leicht zu knackende Standardpasswörter sind auch die Ursache für Überlastungs- oder DDOS-Angriffe, bei der internetfähige Geräte wie Smart-Fernseher oder Handys von Hackern

Felix Casper und Malte Lüking in der Elektroofen-Warte. Der Schmelzbetrieb hat eine Kapazität von zwei Tonnen und eine Anschlussleistung von 1,3 Megawatt. Lüking plant u. a. noch eine Pfannenvorheizstation auf Sauerstoffbasis mit RFID-Tags. So sollen die verschiedenen Aufheizprogramme und Pfannen koordiniert und Mitarbeiterfehler eliminiert werden.

AAGM-Geschäftsführer Peter Wagner mit Bernd Nieß, SPS-Programmierer der Firma ROM aus Stuttgart (v. l. n. r.). Derzeit wird bei Karl Casper Guss eine neue Sandregenerierungsanlage installiert. AAGM baut die Anlage, ROM die Steuerungen. Wagner hat mit Lüking schon vor Langem bei der Vernetzung von Anlagen zusammengearbeitet.

zu Tausenden gekapert und für den Angriff auf ein System genutzt werden können.

Angesichts solcher, leichtfertig unterschätzter Gefahren bildet die auf der Münchner Sicherheitskonferenz im Februar entwickelte „Charter of Trust" die Probleme im Mittelstand nicht ab, ist Trentini überzeugt. Auf der Konferenz hatten sich die Teilnehmer auf ein Identitätsmanagement für internetfähige Anlagen, eine sichere Verschlüsselung und kontinuierliche Hersteller-Updates geeinigt. „Wir sollten erst einmal bei den Standardpasswörtern anfangen, dann würde die Sicherheit direkt deutlich steigen", mahnt er.

Die häufigsten Sicherheitsprobleme gehen aber von den Mitarbeitern selbst aus. Kein E-Mail-System kann zu 100 Prozent gesperrt werden, deshalb setzen Trentini, Casper und Lüking auch auf die Schulung der Beschäftigten. „Wenn die Mitarbeiter etwas Verdächtiges öffnen, gibt es Gefahren, deshalb müssen sie sich des Risikos bewusst sein", weiß Trentini. Ein weiteres Risiko sind USB-Sticks, mit denen Viren und Trojaner in das System eingeschleust werden können – die sind bei Karl Casper Guss allerdings gesperrt.

Digitalisierte Produktion wird zur Selbstverständlichkeit

Die Remchinger Gießerei ist den Weg zur Fabrik der Zukunft schon ein gutes Stück vorangesprintet. Für den Unternehmer Felix Casper ist die Richtung vorgezeichnet: „Unsere Kunden – Top-High-Tech-Unternehmen aus dem Werkzeugmaschinenbau – entwickeln sich mit uns. Wer nicht mitgeht, kann solche Kunden in drei bis vier Jahren gar nicht mehr beliefern. Das Gussteil erhalten sie dann zwar noch, die Übersicht über den Prozess wird für den Kunden dann aber selbstverständlich sein." Die Branche sollte deshalb nach Caspers Überzeugung mitziehen. Er rechnet mit einer zunehmenden Erwartungshaltung der Kunden, Prozesse digital zu beobachten und nachzuvollziehen, die Gießereien ohne digitalisierte Produktion in einigen Jahren in die Knie zwingen könnte.

Nachhaltig investieren ist Trumpf

Rund eine halbe Million Euro investiert Karl Casper Guss jährlich in IT, enthalten sind hier aber auch Kosten wie Druckerpatronen und Lizenzkosten. „Die Einführung der Digitalisierung in der Produktion kann nur funktionieren, wenn nachhaltig investiert wird", betont Trentini. „Ansonsten ist das Geld verbrannt!"

Der IT-Fachmann rechnet künftig mit höheren Software-Kosten, weil Microsoft sein Lizenzsystem umstellt und die Kosten darüber hinaus wegen der neuen Europäischen Datenschutzgrundverordnung, die im Mai in Kraft tritt, steigen dürften. Sie fordert u. a., dass eine Software „Sicher per Design" sein soll.

Die Optimierung der Produktion mit neuen Technologien bei Karl Casper Guss ist nicht abgeschlossen. Lükings aktuelles Projekt, das er wieder mit der Firma Dossmann durchführt, ist die Einführung von RFID-Chips in der Produktion. Seit einem Dreivierteljahr werden sie in einer neuen Halle erfolgreich für die Formkastenverwaltung im Testbetrieb eingesetzt. Zurzeit steht das automatische Auslesen auf dem Programm. „In zwei, drei Jahren sind wir vollständig umgestellt", verspricht er. Doch auch dann wird das Engagement bei Karl Casper Guss in Sachen Industrie 4.0 wohl nicht zum Erliegen kommen. Wichtigstes Motto für das Trio ist nämlich: Dranbleiben! Und Felix Casper ergänzt: „Das was heute noch gut ist, kann morgen falsch sein!"

www.casper-guss.de

Rückmeldestationen, in denen per Bar-Code-Lesegerät Rückmeldungen über Arbeitsschritte erfolgen, gibt es im ganzen Werk.