AGC

TOMORROW LABS

Kaspersky schützt das AGC-Werk in Deutschland

kaspersky BRING ON THE FUTURE

Kaspersky Industrial CyberSecurity

AGC Glass Germany

agc-automotive.com

tomorrow-connect.com

Fertigungsindustrie

- Gegründet im Jahr 2003
- Kunden: BMW, Volkswagen, Mercedes, Volvo, Opel
- Nutzt Kaspersky Industrial CyberSecurity seit 2016

AGC Glass Germany produziert seit 2003 Glas für führende Automobilhersteller wie BMW, Volkswagen, Mercedes, Volvo und Opel. Im Werk Wegberg nahe Mönchengladbach sind 150 Mitarbeiter beschäftigt. AGC gehört zur Asahi Glass Company, einem weltweit führenden japanischen Glashersteller mit mehr als 54.000 Mitarbeitern in mehr als 30 Ländern auf der ganzen Welt.

AGC Glass Germany GmbH veredelt die innerhalb des Konzerns gefertigten Glasscheiben für den Automobilbereich, um sie auf die spezifischen Anforderungen ihrer Kunden anzupassen. Dazu gehört der Einbau zusätzlicher Heizdrähte oder Regensensoren in die Front- oder Heckscheiben oder das Abdichten. Anschließend werden die Glaselemente an die einzelnen Produktionsstandorte in der Automobilindustrie geliefert.

Hintergrund und Prioritäten

„In den zwei Jahren seit der Einführung von KICS konnten wir uns von Kasperskys kundenorientiertem Ansatz und der dynamischen Entwicklung des Produkts überzeugen. Außerdem läuft die Zusammenarbeit mit Kaspersky auch auf menschlicher Ebene sehr gut – wir schätzen die effektive Teamarbeit und die prompten Rückmeldungen."

Jan Houben, Betriebsleiter bei AGC Glass Germany GmbH

Stabile Prozesse sind für einen Produktionsstandort von standardisierten Großserien wie AGC Glass Germany von größter Bedeutung. Eine Lieferverzögerung oder gar ein vollständiger Stillstand der Produktionslinien kann nicht nur hohe Stornierungskosten, sondern in vielen Fällen auch teure Vertragsstrafen nach sich ziehen. Um das zu verhindern, nutzt AGC die Industrie 4.0-Plattform Tomorrow Connect und eApps, um die Prozessstabilität und Abweichungen von den Vorgaben in Echtzeit überwachen zu können.

Dabei handelt es sich um eine Lösung, die vom Kaspersky-Partner Tomorrow Labs in Zusammenarbeit mit dem Fraunhofer Institut und Maschinenbauern entwickelt wurde. Im Rahmen dieser Lösung werden Maschinen und ERP-Daten von unterschiedlichen Herstellern gesammelt, verknüpft und visualisiert, um die Informationen im Sinne einer transparenten, autonomen Produktion abteilungsübergreifend und unternehmensweit zusammenzuführen.

Die große Zahl an vernetzten Produktionsanlagen erhöht aber in erheblichem Maße auch die der Schwachpunkte für Cyberangriffe. Und auch das kann zu erheblichen finanziellen Verlusten und einem anhaltenden Reputationsschaden für das Unternehmen führen.

Deshalb ist man sich bei AGC der Bedeutung einer entsprechend ausgelegten Cybersicherheitslösung bewusst. Eine solche Lösung hat für Unternehmen viele Vorteile. Es geht darum, das Risiko einer Geschäftsunterbrechung einzudämmen, die Lieferkette abzusichern, Vorschriften einzuhalten und vieles andere mehr.

„Mit Kaspersky haben wir uns für einen anerkannten Anbieter von industrieller Cybersicherheit als Technologiepartner entschieden. Kaspersky verfügt über eine weitreichende Expertise und Forschungskapazitäten und bietet damit nicht nur Software, sondern auch Threat Intelligence und Vulnerability Assessments", erklärt Jan Houben, Betriebsleiter bei AGC Glass Germany GmbH.

Security
Verbindet industrielles Netzwerk-Monitoring mit Endpoint-Schutz und wurde speziell für Industrieumgebungen entwickelt

Risikomanagement
Schützt vor Vertragsstrafen wegen Produktionsunterbrechungen oder Nichteinhaltung der Qualitätsvorgaben

Integrität
Überwacht die Integrität der Daten, die an das Bediener-Dashboard übertragen werden, schützt vor besonders hochentwickelten Angriffen

Stärkere Integration

Zur Stärkung der eigenen Sicherheitsstellung, hat sich AGC für Kaspersky Industrial CyberSecurity, kurz KICS, entschieden. Dabei handelt es sich um ein spezielles Portfolio an Softwareprodukten für den Schutz von industriellen Steuersystemen (ICS)

KICS for Nodes schützt ICS/SCADA-Server, HMIs und Engineering-Workstations vor den unterschiedlichen Cyberbedrohungen, die durch menschliche Faktoren, generische Malware, zielgerichtete Angriffe oder Sabotage entstehen können. KICS for Networks arbeitet auf der Ebene des industriellen Kommunikationsprotokolls (Modbus, IEC-Stack, ISO usw.) und untersucht den Datenverkehr von Industrieunternehmen mithilfe fortschrittlicher DPI-Technologie (Deep Packet Inspection) auf Anomalien. Darüber hinaus bietet es Ressourcenerkennung und eine visualisierte Netzwerkübersicht.

Zwei Jahre nach der ersten Implementieren von KICS beschloss AGC, das Projekt im Sinne eines noch effektiveren Funktionsumfangs zu erweitern. Dazu aktualisierte AGC die vorhandenen Installationen von KICS for Nodes und KICS for Networks auf die neuesten Versionen. Außerdem integrierte Kaspersky KICS in Tomorrow Connect, das von Tomorrow Labs bereitgestellt wird. Das brachte weitere Vorteile:

- Echtzeit-Produktionstelemetrie und Cybersicherheitsstatus auf dem Dashboard des Werkleiters,
- KICS garantiert die Sicherheit der Telemetrie und sorgt für eine Überwachung auf Endpoint Security-Vorfälle und anormales Verhalten,
- KICS erkennt mithilfe von DPI technologische Fehler, so dass Fehler im Produktionsablauf vermieden werden und die Produktqualität gewährleistet werden kann.

Ergebnisse

„Mit dieser Lösung erhalten wir Cybersicherheit auf allen Ebenen des Netzwerks, ohne dass unsere technologischen Prozessabläufe beeinträchtigt werden."

Jan Houben, Betriebsleiter
bei AGC Glass Germany GmbH

Zusammen mit Tomorrow Labs ist es Kaspersky gelungen, die Kaspersky Industrial CyberSecurity-Produkte erfolgreich zu aktualisieren und an die Bedürfnisse von AGC anpassen. Mit diesem Projekt ist AGC vollständig geschützt und reaktionssicher aufgestellt. Außerdem konnte dank KICS die Integrität bei der Datenübertragung an Tomorrow Connect gewährleistet werden. Für das Unternehmen ist damit seine Geschäftskontinuität und Sicherheit, aber auch die Zuverlässigkeit seiner Lieferkette gegenüber den Partnern gewährleistet.

„Kaspersky Industrial Cybersecurity ist modular aufgebaut, daher lässt es sich an unsere speziellen Anforderungen und Infrastrukturen anpassen", fährt Jan Houben fort. „Mit dieser Lösung erhalten wir Cybersicherheit auf allen Ebenen des Netzwerks, ohne dass unsere technologischen Prozessabläufe beeinträchtigt werden."

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity ist ein Portfolio bestehend aus Technologien und Services, das umfassenden Schutz für jede einzelne Ebene von Betriebstechnologie (Operational Technology, OT) und sämtliche Elemente Ihres Unternehmens bietet. Darunter auch für SCADA-Server, HMIs, Engineering-Workstations, SPS, Netzwerkverbindungen und Mitarbeiter, ohne dabei die Geschäftskontinuität und Konsistenz der industriellen Prozesse zu beeinträchtigen.

Weitere Informationen finden Sie unter www.kaspersky.de/ics

Kaspersky ICS CERT:
https://ics-cert.kaspersky.com
Cyber Threats News:
https://de.securelist.com/

#Kaspersky
#BringontheFuture

www.kaspersky.de



* World Leading Internet Scientific and Technological Achievement Award auf der 3. Weltinternetkonferenz (Wuzhen-Gipfel)

** Sonderpreis der Industriemesse China International Industry Fair (CIIF) 2016