

A photograph of two men in a factory setting. The man in the foreground is wearing a dark jacket and is looking at a tablet held by the man behind him. The man behind him is wearing a suit and glasses. The background shows a large industrial facility with blue structural elements and various pieces of equipment.

AGC :
自動車業界の
サプライチェーンを保護

KASPERSKY 

自動車業界へのサプライヤである AGCにとって、ビジネスプロセスの 継続性は重要です。これが、AGCの 製造ラインが KASPERSKY INDUSTRIAL CYBERSECURITY によって保護されて いる理由です。



自動車

- 設立:2003年
- 市場占有率:約23%
- 2016年から Kaspersky Industrial CyberSecurity を使用

AGC Glass Germany GmbH は、2003 年から BMW、フォルクスワーゲン、メルセデス、ボルボ、オペルなどの主要メーカー向けに自動車用ガラスを製造しています。ドイツ、メンヒェングラートバッハ近郊のヴェークベルクのオフィスに 150 人のスタッフが従事するこの会社は、世界中 20 か国に 50,000 人以上の従業員を有する世界有数の日本のガラスメーカーグループである旭硝子の一部です。

AGC Glass Germany GmbH では、グループ内のどこか別の場所で製造された自動車用ガラスパネルを加工し、顧客特有のニーズに合わせてカスタマイズします。この工程には、ガラスパネルへの熱センサーや雨センサーの取り付けや、それらの密閉などが含まれます。その後、ガラス部品は自動車業界内の製造ラインへ送られます。

安定したプロセスの実現が最優先

AGC Glass Germany のような標準化された大量製造においては、製造プロセスが安定していることが非常に重要です。製造の遅れや、さらには製造ラインの停止などが起きた場合、キャンセル料のみならず、多くの場合は高額な違約金も発生する可能性があります。これに対抗するため、AGC はインダストリー 4.0 プラットフォームの Tomorrow Connect と eApps を使用して、製造プロセスが安定しているか、製造データやレシピとの整合性に関するリアルタイムの情報を収集しています。

「当社が Kaspersky Lab とパートナーを組むことにしたのは、業務を継続しながら Kaspersky Industrial CyberSecurity を実装することができることに加え、このソリューションは当社が使用している産業用制御システムと Tomorrow Connect の両方と互換性があるためです。」

AGC Glass Germany GmbH の工場長、Jan Houben 氏

Kaspersky Lab パートナーの Tomorrow Labs によって、Fraunhofer IPA およびマシンメーカーと共同で開発されましたこのソリューションは、さまざまなメーカーのマシンデータおよび ERP データを収集、リンク付け、および仮想化することで、部門間や企業間で情報をまとめることができ、透明性の高い自律生産を容易にします。

産業用制御システム向けの IT セキュリティ

ただし、このように大量の製造設備がネットワーク化されることにより、サイバー攻撃に対する弱点の数も急激に増加します。これらは、財務上の大きな損失や企業のイメージへの長期的な被害につながる可能性があります。

そのような攻撃の対象となるのはオフィスコンピューターでしたが、現在では攻撃によって製造システム全体が停止したり、最悪の場合は製品がエンドユーザーに届くまで品質が低下したことに気づかない可能性があります。これらのリスクを減らすため、AGC は Kaspersky Industrial CyberSecurity (KICS) を用いて製造設備を保護することに決めました。

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity は、重要なインフラストラクチャおよび産業用制御システム専用が開発されました。

このソリューションは、マルウェアからの保護、ホワイトリスト、ぜい弱性管理などの従来の広範なセキュリティ技術と、産業用制御システム特有の機器やプロトコルの監視技術とネットワークアクセス制御技術を組み合わせたものです。これには、USB メモリーなどのポータブルメディアおよび周辺デバイスへの接続を細かく管理できるようにするデバイスアクセスコントロールも含まれます。



セキュリティ

従来のサイバーセキュリティ技術と産業環境専用が開発された技術を併用



リスク管理

契約上の違約金からの保護



管理

産業ネットワーク上に最大の管理機能を提供することにより、許可されていないデバイスを検知

150人

従業員

10

保護されている製造ライン

Jan Houben 氏は次のように述べています。「Kaspersky Lab のソリューションは、従業員がいつ USB スティックを保護対象の機器に接続したかを認識します。そして、承認済みの USB スティックのリストを検索して、そのユーザーがデバイスの使用を許可されるべきか否かを判断します。」

これらの標準的な機能は、整合性チェックやプロセス管理コマンドのセマンティック監視などの産業用制御システム専用に設計された技術によってさらに補完されます。Kaspersky Industrial CyberSecurity は、サイバー攻撃、従業員の操作エラー、および産業ネットワーク内のアノマリを検知するために開発された特別監視モードも備えています。

10の製造ラインを保護

AGC では、各生産ラインが Kaspersky Industrial CyberSecurity を用いて保護されています。このソリューションにより、すべてのネットワークレベルが監視され、あらゆる種類のアクティビティがスキャンされます。Kaspersky Industrial CyberSecurity は、製造中の様々な異常に対しても直ちに企業にアラートを発します。

Jan Houben 氏は次のように続けます。「Kaspersky Industrial CyberSecurity はモジュール型システムであるため、当社の個々の要件や特有のインフラストラクチャに適応することが容易です。このソリューションによって、当社の技術プロセスと事業継続性に影響が及ぶことなく、あらゆるネットワークレベルでのサイバーセキュリティが実現します。」



KASPERSKY

カスペルスキーの製品とサービスについて、詳しくは担当の営業にお問い合わせいただくか、www.kaspersky.co.jpをご覧ください。

株式会社カスペルスキー
〒101-0021 東京都千代田区外神田3-12-8
住友不動産秋葉原ビル 7F
jp-sis@kaspersky.com
www.kaspersky.co.jp/industrial-security-cip

© 2017 AO Kaspersky Lab. All rights reserved. 登録商標およびサービスマークは、それぞれの所有者に属しています。Mac および Mac OS は、Apple Inc. の登録商標です。Cisco は、Cisco Systems, Inc. とその関連会社の米国およびその他の国における登録商標または商標です。IBM、Lotus、Notes および Domino は、世界各地の多数の法域で登録された International Business Machines Corporation の商標です。Linux は、Linus Torvalds の米国およびその他の国における登録商標です。Microsoft、Windows、Windows Server および Forefront は、Microsoft Corporation の米国およびその他の国における登録商標です。Android™ は Google, Inc. の商標です。Blackberry の商標は、Research In Motion Limited の所有物であり、米国およびその他の国において登録または使用されています。