Sicherheitslücken schließen – Kaspersky Lab bietet industrielle Cybersecurity Assessments für Pilsner Urquell

https://www.pilsner-urquell.de/

Pilsner Urquell

Brauerei

- Gegründet im Jahr 1842
- Pilsen, Tschechische Republik
- Über 2000 Mitarbeiter in 3 Brauereien und 13 Vertriebszentren
- 8 Verpackungsanlagen im Werk Pilsen

Plzeňský Prazdroj a.s. ist eine tschechische Brauerei, die 1842 gegründet wurde und ihren Hauptsitz in Pilsen, Tschechische Republik, hat.

Plzeňský Prazdroj hat als erste Brauerei das helle Pilsner Lagerbier der Marke „Pilsner Urquell" hergestellt und damit über zwei Drittel der produzierten Biere mit der Bezeichnung „Pils", „Pilsner" oder „Pilsener" weltweit geprägt. Plzeňský Prazdroj bedeutet so viel wie „Ursprung in Pilsen" oder „die ursprüngliche Quelle des Pilsner".

Plzeňský Prazdroj ist die führende Brauerei in Mitteleuropa. Über seine Marken verkauft Plzeňský Prazdroj mehr Bier auf dem tschechischen Markt als jedes andere Unternehmen. Seit 1999 ist die Brauerei Teil des SABMiller Konzerns (vorher „South African Breweries"). Im Rahmen der mit den Aufsichtsbehörden getroffenen Vereinbarungen, wurde Pilsner Urquell – mit Ausnahme bestimmter geographischer Gebiete – am 31. März 2017 an Asahi Breweries in Japan verkauft, bevor Anheuser-Busch InBev im Oktober 2016 SABMiller erwarb.

„Wir wollten gegen jeden unvorhersehbaren Vorfall gerüstet sein, unsere OT-Infrastruktur untersuchen und einen Bereitstellungsplan erstellen, um unser industrielles Netzwerk mithilfe von weltweit führenden Experten zu sichern."

Jan Šik, Chefingenieur Pilsner Urquell

Herausforderung

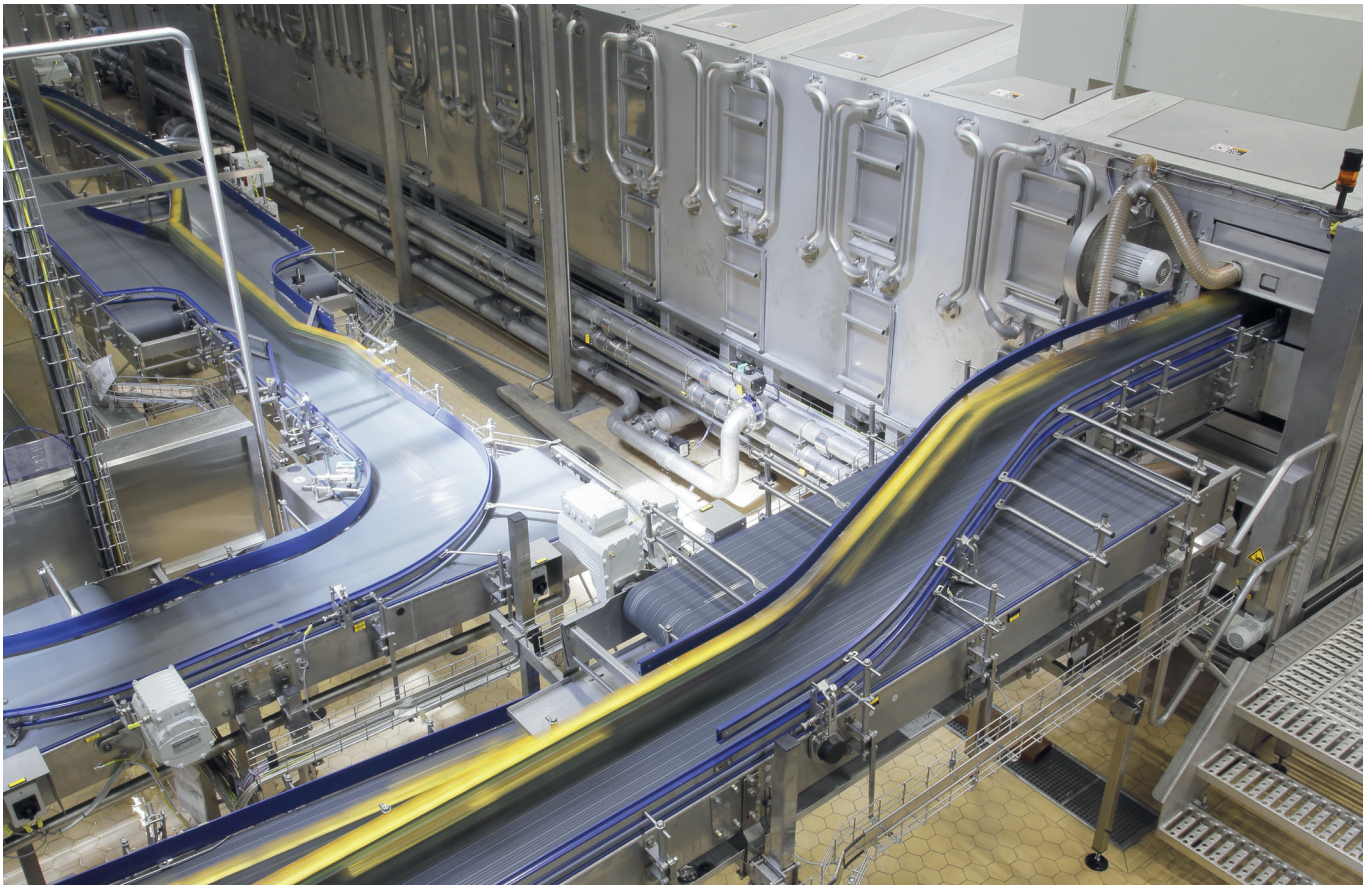
Als Großunternehmen in der Produktion nimmt Pilsner Urquell die Cybersicherheit von IT und OT sehr ernst. In den letzten Jahren wurden im Unternehmen einige unabhängige Sicherheitsprüfungen mit interessanten Ergebnissen durchgeführt. Sobald die Technologieentwicklung bei Pilsner Urquell ein kontinuierlicher Prozess wurde, entstand die Notwendigkeit eines neuen unabhängigen Assessments.

Damals wandelte sich der technologische Hintergrund von separaten Systemen auf Standard-PCs zu einem virtualisierten, serverbasierten Mastersystem, das alle Systeme und Geräte miteinander verband.

Grundlegende Motivation für das Unternehmen ein Cybersecurity Assessment (CSA) durchzuführen, war die Überprüfung der Infrastruktur in der finalen Phase des Projekts, das eine Virtualisierung der Produktionssysteme und ein Upgrade der primären OT-Netzwerkkomponenten umfasste. Sekundäre Faktoren waren die Vorbereitung von wichtigen Themen und Anforderungen für das zukünftige Projekt, das sich auf eine Endpoint-Sicherheitslösung konzentrierte sowie die Sicherstellung, dass alle Produktionsstätten von Pilsner Urquell im Falle eines gezielten Cyberangriffs oder als „Opfer" eines Angriffs auf andere nahestehende Unternehmen nicht betroffen sind.

Ziel des industriellen CSA-Projekts war die Gewährleistung der Widerstandsfähigkeit von Produktionslinien und der gesamten OT-bezogenen Soft- und Hardware gegen Cyberangriffe sowie die Umsetzung einer ganzheitlichen industriellen Cybersicherheitsstrategie.

Die größten Herausforderungen für die industrielle Cybersicherheitspolitik vor CSA waren die Komplexität der OT-Infrastruktur (zwei Segmente: Brauen und Abfüllen mit völlig unterschiedlicher Infrastruktur), ihre Anbindung an externe Geschäftssysteme und die kürzlich erfolgte Inbetriebnahme einer neuen Produktionsanlage.



Nicht-invasive Lösung
Kaspersky Industrial CyberSecurity Assessment beeinträchtigt nicht die Betriebskontinuität oder Konsistenz der Industrieprozesse.

Umfassende Expertise
Erfahrungen aus der Praxis mit einem umfangreichen Spektrum an verschiedenen Branchen und OT-Ausstattungen ermöglichen den Experten von Kaspersky Lab effektiv industrielle Cybersecurity Services bereitzustellen.

Kaspersky Industrial CyberSecurity besteht aus einem Portfolio von Technologien und Services, die in jeder Phase des OT-Sicherheitsprozesses des Kunden einen Mehrwert bieten – von der Schulung und Assessment bis hin zur Vorfallsreaktion.

Die Lösung von Kaspersky Lab

Pilsner Urquell entschied sich für das industrielle CSA von Kaspersky Lab, welches ein minimal invasives Cybersecurity Assessment extern oder lokal bietet. Die Experten bei Kaspersky Lab begannen den industriellen CSA-Prozess mit einer Infrastrukturprüfung und der Entwicklung von Bedrohungsmodellen. Die industriellen Prozesse bei Pilsner Urquell sind hauptsächlich unterteilt in die Bereiche Brauen und Flaschenabfüllung. Dazu gehören zwei Brauhäuser und CCT-Bereiche mit acht Verpackungsanlagen im Werk Pilsen. Die Experten untersuchten die wichtigsten Bereiche der Infrastruktur und bildeten dabei bestimmte Angriffsvektoren nach. Dabei erkannten sie Schwachstellen und scannten nach schädlichen Aktivitäten und Anomalien.

Ausgangspunkt des Assessments war das Unternehmensnetzwerk, das mit einer industriellen Zone verknüpft war. Die Experten von Kaspersky Lab stellten extern entwickelte Unternehmenssoftware fest, die gefährliche Schwachstellen aufwies und durch die der Zugriff auf einige der OT-Geräte über ein anderes IT-System vereinfacht werden kann. Beim industriellen Teil des Bierbrauens entdeckten die Experten von Kaspersky Lab eine Zero-Day-Schwachstelle in einer SCADA-Software.

In dieser Phase wurden weitere Aktivitäten durchgeführt, um alle unkontrollierten externen Verbindungen vom/zur Industrieanlage aufzudecken und darzulegen.

Am Ende dieser Phase erhielt Pilsner Urquell von den Experten von Kaspersky Lab eine vollständige Liste mit entdeckten Schwachstellen und Sicherheitslücken, einschließlich schwacher Authentifizierung, SQL-Injections usw. sowie eine detaillierte Analyse, wie man sich diese zunutze machen könnte. Darüber hinaus erhielt Pilsner Urquell eine Beschreibung der erkannten und bestätigten Angriffsvektoren, die die Kontinuität oder Integrität der industriellen Prozesse des Unternehmens beeinträchtigen könnten.

Basierend auf den Forschungsdaten der ersten Phasen entwickelten die Experten von Kaspersky Lab ein Bedrohungsmodell, das als Grundlage für die Entwicklung umsetzungsfähiger Empfehlungen dient. Dieser Abschlussbericht ist essentiell für Kunden, da er Empfehlungen für fortlaufende Cybersicherheitsmaßnahmen für spezifische industrielle Komponenten sowie Techniken zur Risikominimierung von Schwachstellen umfasst. Zu einer Empfehlung für Pilsner Urquell gehörten Updates und Passwortrichtlinien sowie die Stärkung der Netzwerk- und Webanwendungssicherheit.

„Die Analyse zeigte uns wichtige Empfehlungen für den Sicherheitslebenszyklus sowie bedeutende Schwachstellen in den Sicherheitsprozessen. Mehrere verbesserungswürdige Bereiche wurden identifiziert und alle Ergebnisse wurden in einem Abschlussbericht zusammengefasst“, so Miroslav Zajíc, IT-Analyst bei Pilsner Urquell.

„Die Entscheidung mit Kaspersky Lab zusammenzuarbeiten, ist uns aus vielerlei Gründen leicht gefallen. Ihre Erfahrung im Bereich der Cybersicherheit, ihre Professionalität und die Vielschichtigkeit ihrer Lösung im Vergleich zu anderen Anbietern sind für uns von enormen Wert und gewährleisten eine erfolgreiche Zukunft für die Sicherheitsstrategie unseres Unternehmens."

Ondřej Sýkora,
C&A Manager,
Pilsner Urquell

Perspektive

Pilsner Urquell bekräftigt, dass die Experten von Kaspersky Lab das industrielle CSA gut organisiert und professionell durchgeführt haben und die Grundlage für ein sicheres strategisches Konzept für die industrielle Cybersicherheit innerhalb des Unternehmens geschaffen haben.

„Mit Kaspersky Lab wollen wir die Ergebnisse und Empfehlungen von CSA weiterverfolgen und möchten die Verhandlungen bezüglich der Bereitstellung von Kaspersky Industrial CyberSecurity-Lösungen für Nodes und Server fortsetzen“, sagt Ondřej Sýkora, C&A Manager bei Pilsner Urquell.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity ist ein Portfolio bestehend aus Technologien und Services, das umfassenden Schutz für jede einzelne Ebene der Betriebstechnologie 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 zu Kaspersky Lab finden Sie unter https://ics.kaspersky.de/

Informationen über ICS-Cybersicherheit:
https://ics-cert.kaspersky.com
Neues über Cyberbedrohungen:
de.securelist.com

#truecybersecurity

www.kaspersky.de

© 2018 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* Auszeichnung für weltweit führende Leistungen in den Bereichen Internetwissenschaft und Internettechnologie auf der 3. Weltinternetkonferenz (Wuzhen-Gipfel)

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