Pilsner Urquell vor Cyberangriffen schützen

In Zeiten von Industrie 4.0 ist das Thema Cybersicherheit für Produzenten aus der Lebensmittelindustrie von elementarer Bedeutung. Das Beispiel der Brauerei Pilsner Urquell zeigt, wie über eine Sicherheitsprüfung (Audit) durch Kaspersky Lab der erste Schritt in eine weiterführende Cyberabsicherung industrieller Anlagen gemacht werden kann, ohne den laufenden Produktionsbetrieb zu stören.

Die renommierte tschechische Brauerei Pilsner Urquell mit Gründungsdatum 1842 ist das führende Brauereiunternehmen in Zentraleuropa. Das Unternehmen beschäftigt rund 2.000 Mitarbeiter in drei Brauereien, acht Verpackungslinien und 13 Vertriebszentren. Pilsen, der Sitz der Brauerei-Gesellschaft, ist als „Geburtsort“ des Pilsner Bieres weltberühmt. Mehr als Zweidrittel des weltweit hergestellten Bieres sind durch diese Biersorte inspiriert und werden unter den Namen „Pils“, „Pilsner“ oder „Pilsener“ verkauft. Pilsner Urquell ist sozusagen die Urquelle des Pils.

Seit 1999 gehört die Brauerei zur Unternehmensgruppe SABMiller (damals South African Breweries). In Abstimmung mit den Regulierungsbehörden (bevor Anheuser-Busch InBev SABMiller im Oktober 2016 übernehmen durfte) wurde Pilsner Urquell – ohne bestimmte geografische Gebiete – am 31. März 2017 an den japanischen Brauereikonzern Asahi verkauft.

Technologieentwicklung bedeutet bei Pilsner Urquell einen kontinuierlichen Prozess. In den vergangenen Jahren wurden bereits mehrere unabhängige Audits im Unternehmen durchgeführt. Als die IT von PC-Einzelplatzlösungen auf ein virtualisiertes, serverbasiertes Master-System, das alle Systeme und Geräte verbindet, umstellen wollte, sah das Unternehmen konkreten Handlungsbedarf zur Überprüfung relevanter IT-Sicherheitsaspekte.

Systemumstellung stellt neue Herausforderungen in puncto Sicherheit

Die Hauptmotivation für die Durchführung einer Cybersicherheitsprüfung – auch Cybersecurity Assessment (CSA) genannt – bestand darin, die Infrastruktur in der Endphase des Umstellungsprojekts hinsichtlich IT-Sicherheitsaspekten zu prüfen. Zudem beinhaltet das Projekt auch die Virtualisierung der Produktionssysteme sowie das Upgraden der Hauptnetzwerkkomponenten der Betriebstechnologie (OT, Operational Technology). Eine weitere Herausforderung: die Kernthemen und Anforderungen des zukünftigen Projektes hinsichtlich einer Endpoint-Sicherheitslösung zu eruieren und zu definieren. Das Ziel war klar gesetzt: Es sollten sämtliche Produktionsanlagen von Pilsner Urquell vor möglichen gezielten Cyberattacken oder Angriffen auf eng mit der Firma verbundene Unternehmen geschützt sein. „Uns ging es darum, auf sämtliche unerwartete Vorfälle vorbereitet zu sein, unsere OT-Infrastruktur auf den Prüfstand zu bringen und mit den Experten von Kaspersky Lab einen Plan zur Sicherung des industriellen Netzwerks aufzustellen“, erläutert Jan Šik, Chefingenieur bei Pilsner Urquell.

Ziel des industriellen CSA-Projektes war es, die Produktionslinien und jegliche OT-bezogene Software und Hardware gegen Cyberangriffe immun zu machen sowie das Unternehmen so aufzustellen, dass eine ganzheitliche industrielle Cybersicherheitsstrategie implementiert werden kann. Die größten Herausforderungen in Sachen industrieller Cybersicherheit vor Durchführung der Sicherheitsprüfung (CSA) waren die Komplexität der OT-Infrastruktur (zwei Bereiche: Brauerei und Abfüllung mit jeweils gänzlich verschiedener Infrastruktur), die Anbindung an externe Business-Systeme sowie der Launch der neuen Produktionslinie, der kurz zuvor stattfand.

Wer seine Schwächen kennt, kann sich schützen

Pilsner Urquell entschied sich für das industrielle CSA von Kaspersky Lab, das aus einem minimal-invasiven Remote sowie Vor-Ort-Cybersecurity-Assessment besteht. Der Vorteil: Kaspersky Industrial CyberSecurity Assessment hat keine Auswirkungen auf den laufenden Betrieb, die industriellen Prozesse laufen weiter.

Die Experten von Kaspersky Lab begannen den industriellen CSA-Prozess mit einem Infrastruktur-Audit und der Entwicklung eines Bedrohungsmodells. Die industriellen Prozesse bei Pilsner Urquell teilen sich vor allem in die Bereiche Brauerei und Abfüllung. Dazu gehören zwei Brauhäuser und Getränketank-Bereiche (Cylindrically-conical fermentation tanks, CCT) sowie acht Verpackungslinien innerhalb der Produktionsanlage in Pilsen.

Kaspersky Lab untersuchte die kritischsten Bereiche der Infrastruktur. Hierzu wurden spezifische Angriffsvektoren nachgestellt, um Sicherheitslücken aufzudecken und anschließend die Systeme auf bösartige Aktivitäten und Anomalien hin zu untersuchen.

Bei der Untersuchung des Firmennetzwerks und der verbundenen industriellen Bereiche entdeckten die Experten extern entwickelte Unternehmenssoftware, die gefährliche Sicherheitslücken aufwies – Sicherheitslücken, durch die OT-Anlagen sehr einfach angegriffen werden können. Im industriellen Bereich der Brauerei entdeckten die IT-Security-Experten sogar eine Zero-Day-Schwachstelle für SCADA-Software.

Weiter wurden Maßnahmen durchgeführt, um unkontrollierte externe Verbindungen in die sowie aus der Shop-Floor-Ebene ausfindig zu machen.

Am Ende des Infrastruktur-Audits stellte Kaspersky Lab Pilsner Urquell eine Übersicht aller entdeckten Schwachstellen und Sicherheitslücken, wie schwache Authentifizierungen, SQL-Injektionen und ähnliches, zur Verfügung; dazu gehörte auch eine detaillierte Analyse, wie diese ausgenutzt werden könnten. Darüber hinaus erhielt Pilsner Urquell eine Beschreibung der entdeckten und bestätigten Angriffsvektoren, die der Betriebskontinuität und Integrität der industriellen Prozesse des Unternehmens zum Verhängnis werden könnten.

Richtig schützen: Analyse zeigt Handlungsempfehlungen auf

Basierend auf den Ergebnissen des Audits entwickelten die Experten von Kaspersky Lab im nächsten Schritt ein Bedrohungsmodell, um daraus für das Unternehmen umsetzbare Handlungsempfehlungen abzuleiten. Ein derartiger Abschlussbericht spielt eine entscheidende Rolle: Er beinhaltet Empfehlungen für künftige Maßnahmen in punkto Cybersicherheit für spezifische industrielle Komponenten und Techniken zur Schwachstellenbeseitigung. Empfehlungen für Pilsner Urquell waren beispielsweise Update- und Passwort-Richtlinien sicherzustellen, sowie die Netzwerk- und Web-Application-Security zu verstärken.

„Durch die Analyse verfügen wir über wichtige Empfehlungen für den Sicherheits-Lebenszyklus und haben wesentliche Erkenntnisse über die Schwachstellen im Sicherheitsprozess gewonnen. Der Abschlussbericht von Kaspersky Lab hat uns viele Verbesserungsmöglichkeiten aufgezeigt“, resümiert Miroslav Zajíc, IT Analyst bei Pilsner Urquell.

Dieser strategische Ansatz für die industrielle Cybersicherheit eröffnet dem Unternehmen in Zukunft weitere Schritte hinsichtlich der eigenen IT-Sicherheit zu gehen. „Auf Basis der CSA-Ergebnisse wollen wir nun zusammen mit Kaspersky Lab die Lösung Kaspersky Industrial CyberSecurity für Netzknoten und Server implementieren“, so Miroslav Zajíc abschließend.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity ist ein Portfolio aus Technologien und Services, das umfassenden Schutz für jede einzelne Ebene von Industriesystemen bietet. Darunter auch SCADA-Server, HMI, Engineering-Workstations, SPS, Netzwerkverbindungen und Mitarbeiter. Die Lösung erhöht die industrielle Sicherheit schrittweise in allen Bereichen, von Mitarbeitern, über Prozesse bis hin zu Technologien. Die Kontinuität und Konsistenz industrieller Prozesse werden nicht beeinträchtigt: https://www.kaspersky.de/enterprise-security/industrial-solution

Autor: Denise Pflock, Corporate Communications Manager Europe bei Kaspersky Lab

Weitere Informationen und Kontakt

Kaspersky Lab GmbH
Ingolstadt
Denise Pflock
+49 (0) 841 98 18 90
kaspersky_de@berkeleypr.com
www.kaspersky.de