Penetrationstest: Die Remote-Service-Verbindung auf die Probe gestellt.

Bosch Packaging Technology beschäftigt weltweit rund 6200 Mitarbeiter, die unterschiedlichste Füll-, Prozess- und Verpackungstechnik entwickeln, fertigen und installieren. Um den weltweiten Kunden noch schnelleren Anlagenservice zu bieten, kann das Unternehmen eine Remote-Service-Verbindung zu den Maschinen nutzen. Sensible Daten und Know-How müssen dabei gegenüber möglichen Cyber-Angreifern geschützt werden. Der Verpackungsspezialist beauftragte deshalb TÜV Rheinland mit einem Penetrationstest. Damit hat Bosch Packaging Technology eine belastbare und objektive Einschätzung, dass die gegenwärtige IT-Sicherheitsstrategie greift.

www.tuv.com/
informationssicherheit

BOSCH
Technik fürs Leben

TÜVRheinland®
Genau. Richtig.

Ob Kaffee, Gemüse oder Süßwaren: Für die Nahrungsmittelbranche bietet Bosch Packaging Technology eine Vielzahl an Verpackungslösungen. Im Bereich Pharma reicht das Portfolio von Maschinen zur Abfüllung steriler, flüssiger und pulverförmiger Pharmazeutika über Inspektionstechnologie bis hin zu Tablettenpressen und Track & Trace-Systemen.

ATTRAKTIVES ZIEL FÜR ANGREIFER

Mit ihrem Angebot und umfassendem Know-How sind sowohl Bosch Packaging Technology als auch viele der Kunden etablierte Größen in den Zielmärkten. Entsprechend attraktiv wäre es für Cyber-Angreifer, über mögliche Sicherheitslücken in Netzwerk, IT-Systemen, Anwendungen oder mobilen Geräten sensible Geschäfts- und Kundendaten zu manipulieren, zu stehlen oder gar einen Produktionsausfall zu verursachen. Viele Betriebe sind heutzutage bereits kompromittiert, ohne es zu ahnen. Soweit wollte es die Bosch-Tochter aus dem Geschäftsbereich Industrietechnik nicht kommen lassen. Um dieses Risiko proaktiv zu vermindern und Sicherheitslücken in der Verbindung für den Remote Service aufzuspüren, beauftragte die Bosch Packaging Technology die Experten von TÜV Rheinland mit der Durchführung eines Penetrationstests.

HACKERN ZUVORKOMMEN – MIT EINEM SIMULIERTEN CYBER-ANGRIFF

In einem Penetrationstest betrachten die Security Analysts die IT-Infrastruktur aus der Sicht eines Hackers und simulieren eine realistische Cyber-Attacke. Mithilfe einer Worst-Case-Betrachtung untersuchen die Experten für Cybersecurity, was der größtmögliche durch einen Angreifer verursachte Schaden ist. Nachdem die Security Analysts erste Sicherheitsmaßnahmen umgehen können, suchen sie gezielt nach Informationen auf bereits kompromittierten Systemen:

- Dateien oder Datenbanken mit Zugangsinformationen,
- Log-Dateien und Backups,
- Konfigurations- oder Quellcode-Dateien, die über die Funktionsweise dieser oder anderer Anwendungen Aufschluss geben.

So werden möglichst viele und detaillierte Informationen ermittelt, die einem Angreifer helfen könnten, die Angriffsfläche besser einzuschätzen und anschließend möglichst effizient angreifen zu können. Der Schadensfall wird nicht final getestet, sondern es wird lediglich nachgewiesen, dass ein solcher möglich wäre.

VERRINGERTE KRITIKALITÄT

Im Falle von Bosch Packaging Technology waren die Ergebnisse erfreulich: Die aufgedeckten Schwachstellen erwiesen sich in punkto Klassifizierung lediglich von geringer Kritikalität – ein gutes Zeichen für die Wirksamkeit der implementierten Sicherheitsstrategie beim Verpackungsspezialisten.

Dennoch kein Grund, die Hände in den Schoß zu legen, denn auch weniger kritische Sicherheitslücken können sich in Verbindung mit neuen Schwachstellen unter Umständen zu einem größeren Problem verdichten. Deshalb folgt Bosch Packaging Technology den Empfehlungen von TÜV Rheinland, wie sich diese potenziellen Einfallstore eliminieren bzw. auf ein akzeptables Maß reduzieren lassen: mittels praktikabler Gegenmaßnahmen, die den Anforderungen gemäß ISO 27001 und IT-Grundschutz nach BSI entsprechen.

DETAILLIERTE DOKUMENTATION

Abschließend wurde die Untersuchung in einem detaillierten übersichtlichen Prüfbericht dokumentiert. Er beinhaltet eine Klassifizierung der identifizierten Schwachstellen, bezogen auf die IT-Sicherheit der Systeme im Untersuchungsbereich anhand einer dreistufigen Risikoskala. Ergänzend listet er die Empfehlungen für adäquate Schutzmaßnahmen auf. Der Prüfbericht enthält eine Beschreibung der bei der Analyse gewählten Vorgehensweisen sowie Informationen zur Reproduktion der Ergebnisse.

PROFESSIONELLE ZUSAMMENARBEIT

„Die Ergebnisse des Penetrationstests und die Empfehlung von TÜV Rheinland sind für uns sehr wertvoll“, so Sandro Gisler, Remote Service Portal Owner von Bosch Packaging Technology. „Die Zusammenarbeit verlief in Vorbereitung und Durchführung reibungslos und professionell. Sicherlich werden wir solche wichtigen Präventivmaßnahmen im Bereich Cybersecurity künftig regelmäßig durchführen. Nur so können wir sicher sein, dass wir Cyber-Kriminellen keine unnötigen Angriffsflächen bieten und unsere Daten und Know-How so gut wie möglich geschützt sind. Das gibt unseren Kunden Sicherheit.“

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung. DE19_D01_1900131

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
service@i-sec.tuv.com

www.tuv.com/pentest

TÜVRheinland®
Genau. Richtig.