Investitionen absichern mit Penetrationstests

Safety ist ein etabliertes Thema im Industriealltag. Ohne Sicherheitsschuhe oder Helm dürfen viele Werkshallen gar nicht erst betreten werden. Das Vermeiden von Unfällen ist heute zum Glück Standard. Wie aber sieht es mit der IT-Security aus?

Bild: ©kentoh / Fotolia.com

Unter dem Schlagwort Industrie 4.0 werden unterschiedliche Aspekte einer allumfassenden Digitalisierung industrieller Fertigungsprozesse diskutiert. Ein Werkzeug, dessen Standzeitende erreicht ist, signalisiert dies nicht nur dem Maschinenbediener, sondern fordert aus dem Lager gleich selbst Ersatz an. Darüber hinaus löst es auch eine Nachbestellung im ERP-System aus. Solche Szenarien mögen noch nicht die ganze Branche durchdrungen haben, doch weit entfernt von der Realisierbarkeit sind sie nicht mehr. Dafür sollten zunächst einmal jedoch alle beteiligten Systeme möglichst nahtlos miteinander vernetzt werden und untereinander kommunizieren dürfen.

Neue Risiken

Wo jedoch neue Kommunikationsmöglichkeiten geschaffen und zuvor getrennte IT-Systeme miteinander vernetzt werden, da entstehen Risiken, denen vorgebeugt werden muss. Das Unfallrisiko in der industriellen IT entsteht vor allem an den Schnittstellen. Es mag dem digitalen Betriebsablauf dienen, wenn die Einkaufsabteilung mit ERP-System auf die Bestände der Werkzeugmagazine zugreifen kann, oder der Fertigungsleiter von seinem Bürorechner aus Zugang zu den Statusinformationen der Fertigungsstraße hat. Es ist aber ebenso denkbar, dass solche Verbindungen zwischen Büronetzwerk und industriellem Steuernetz missbraucht werden. Ein digitaler Angreifer, der sich über eine Malware Zugang auf den Desktop-PC eines Verwaltungsmitarbeiters im technischen Einkauf verschafft, hätte von dort aus dann auch Zugriff auf die Steuerung der Fertigungszelle – mit möglicherweise fatalen Folgen. Das Stichwort, um solche 'IT-Unfälle' zu vermeiden, heißt 'Netzwerkseparierung'. Solange der Produktionsleiter E-Mails schreibt, nutzt er seinen Officerechner. Will er die Daten der Fertigung einsehen und eventuell sogar per Fernzugriff korrigierend eingreifen, nutzt er ein Zweitgerät. Im Fall eines erfolgreichen Hackerangriffs auf das Verwaltungsnetzwerk bleibt der Angreifer außen vor, da zwischen den beiden Netzen kein Übergang besteht.

Bewusstsein schaffen

Auch wenn in vielen produzierenden Unternehmen bereits IT-Sicherheitsrichtlinien existieren und Netzwerkseparierung kein Fremdwort ist, liegt der Schwerpunkt häufig genug auf der technischen Umsetzbarkeit gewünschter 'Industrie 4.0'-Funktionalitäten auf Produktionsebene. IT-Security ist dabei häufig ein Nebenaspekt. Umso wichtiger ist es, ein Bewusstsein dafür zu schaffen und digitale Sicherheitsmaßnahmen nach ihrer Integration auf ihre Wirksamkeit zu prüfen. Ein geeignetes Instrument, die eigene IT-Sicherheit auf den Prüfstand zu stellen, ist ein sogenannter Penetrationstest. Ein Penetrationstest ist eine Hackerattacke unter kontrollierten Bedingungen und deckt auf diese Weise eventuell vorhandene Sicherheitslücken auf, noch bevor diese missbraucht werden können. Dabei sollte es jedoch nicht bei einer einmaligen Prüfung bleiben: Täglich werden neue Sicherheitslücken in Softwareprodukten gefunden. Penetrationstests sollten deshalb fest in Prüfpläne integriert und entsprechend häufig und regelmäßig durchgeführt werden. Der einzelne Test untersucht dabei ein oder mehrere Angriffsszenarien, die Auftraggeber und Tester in Hinblick auf das Unternehmen und dessen Eigenarten definieren: Angriffsursprung, Angriffsziel, Testtiefe , Testmittel, Wissensstand und die Motivation des Angreifers. Speziell bei Industrieunternehmen kommen noch weitere Fragen hinzu, die sich aus einer Besonderheit der Branche ergeben, denn auch im Zeitalter der Industrie 4.0 hat Infrastruk-

Auszug aus IT&Production, Fachzeitschrift für erfolgreiche Produktion, Ausgabe 9/2016.
Digitales Belegexemplar mit freundlicher Genehmigung des Fachmagazins IT&Production. Dieses Dokument ist ausschließlich zur elektronischen Speicherung durch den Autor sowie zur Weitergabe per E-Mail bestimmt. Abweichende Verwendung nur mit Zustimmung des Verlages.

tur eine längere Lebensdauer. Die Smartphones der Mitarbeiter mag man alle drei Jahre austauschen, eine Maschine – auch eine digital vernetzte – hat weiterhin Standzeiten von 15 bis 20 Jahren. Aus Sicht der IT-Security muss hier berücksichtigt werden:

- Wie ist der Sicherheitsstatus der an der Produktion beteiligten Komponenten? Gibt es Maschinen und Systeme, die aufgrund einer Abnahme/Zulassung nicht gepatcht werden können?
- Gibt es 'schwache Glieder' in der Kette, zum Beispiel Windows XP-Systeme, auf die aus Gründen der Kompatibilität nicht verzichtet werden kann? Wie sind diese separiert?
- Wie sieht es mit dem WLAN in der Produktionshalle aus? Sind noch Geräte wie Handscanner mit dem nicht mehr sicheren Kryptostandard WEP im Einsatz? Können sich Angreifer auf diesem Weg drahtlos mit dem Steuerungsnetz verbinden?
- Inwieweit sind die IT-Schnittstellen der Maschine für die Bediener direkt zugänglich? Können beispielsweise USB-Anschlüsse erreicht und hierüber potenziell Schadsoftware eingebracht werden?
- Gibt es Servicezugänge? Sind diese vom restlichen Netz getrennt? Oder lässt sich über den Fernwartungszugang für eine bestimmte Maschine auch auf andere Bereiche des Steuerungsnetzes zugreifen?

Wer als Penetrationstester erfolgreich sein will, der sollte seine IT-Spezialkenntnisse immer auf dem neuesten Stand halten. Doch nicht nur aus diesem Grund empfiehlt es sich, entsprechende Untersuchungen extern durchführen zu lassen: Denn eine hauseigene Fachabteilung unterliegt auf Dauer auch dem Risiko, 'betriebsblind' zu werden. Der regelmäßige Blick von außen durch unabhängige Penetrationstester hilft dabei, blinde Flecken aufzudecken und Sicherheitsprobleme zu beheben, bevor es zu einem realen Anriff kommt.

Zugriff von außen

Die Digitalisierung in der Industrie unter dem Schlagwort 'Industrie 4.0' wird das bestimmende Thema der Branche bleiben. Ob man dabei auch 'IT-Security 4.0' im Blick hat, bleibt abzuwarten. Schon heute sind viele Maschinen in der Produktion schlicht Computersysteme, die Zugriff von außen über verschiedene Protokolle erlauben. Zur Steuerung werden Webapplikationen ebenso eingesetzt wie domänenspezifische Software. Durch Visualisierung von Produktionsprozessen über Clouddienste lässt sich Effizienz steigern, per Fernwartung oder Remote-Support via VNC oder RDP unterstützen externe Dienstleister Maschinenbediener vor Ort. Je mehr Zugriffsmöglichkeiten geschaffen werden, desto mehr muss auch mit potenziellen digitalen Angreifern gerechnet werden. ■

Die Autoren Dr. Oliver Grasmück und Marcel Mangold arbeiten bei der Syss GmbH.

www.syss.de