Safety first!

Die Vermeidung von Unfällen haben Unternehmen fest im Blick. Ohne Sicherheitsschuhe oder Helm dürfen viele Werkshallen gar nicht erst betreten werden. Das ist heute glücklicherweise selbstverständlich. „Security 1.0" ist – so könnte man sagen – praktisch Industriestandard. Wie aber sieht es mit Security 4.0 aus?

Unter dem Schlagwort „Industrie 4.0" werden schon länger unterschiedliche und häufig divergierende Aspekte einer möglichst allumfassenden Digitalisierung industrieller Fertigungsprozesse diskutiert – von der Planungsebene des ERP, über die Konstruktion im CAD bis hin zur einzelnen Maschine auf Shopfloor-Ebene. Solche Szenarien mögen noch nicht die ganze Branche durchdrungen haben, doch weit entfernt von der Realisierbarkeit sind sie nicht mehr. Dafür sollten zunächst einmal alle beteiligten Systeme möglichst nahtlos miteinander vernetzt werden und untereinander kommunizieren dürfen. Wo jedoch neue Kommunikationsmöglichkeiten geschaffen und zuvor getrennte IT-Systeme miteinander vernetzt werden, da entstehen Risiken – digitale Unfallrisiken, denen ebenso vorgebeugt werden muss, wie Verletzungen durch herunterfallende Werkstücke.

Das Unfallrisiko in der industriellen IT, um im Bild zu bleiben, entsteht vor allem an den Schnittstellen. Es mag sinnvoll sein und dem digitalen Betriebsablauf dienen, wenn die Einkaufsabteilung direkt aus dem ERP heraus auf die Bestände der in den Werkzeugmagazinen einer Fertigungszelle vorrätig gehaltenen Fräser und Bohrer zugreifen kann. Es ist aber ebenso denkbar, dass solche Verbindungen zwischen Büronetzwerk und industriellem Steuernetz missbraucht werden. Ein digitaler Angreifer, der sich über eine per E-Mail-Anhang verschickte Malware Zugang auf den Desktop-PC eines Verwaltungsmitarbeiters im technischen Einkauf verschafft, hätte von dort aus auch Zugriff auf die Steuerung der Fertigungszelle – mit möglicherweise fatalen Folgen.

Separation der Netze

Das Stichwort, um solche „IT-Unfälle" zu vermeiden, heißt „Netzwerkseparierung", bezogen auf das oben genannte Beispiel also zunächst einmal eine vollständige Trennung von Officenetz und Produktionsnetz, im Idealfall sogar physisch, sprich mit je eigener, getrennter Verkabelung und der Nutzung eigener Geräte für den Zugriff auf Industriesteuerungen. Solange der Produktionsleiter also E-Mails schreibt, nutzt er seinen Officerechner. Will er die Daten der Fertigung einsehen und eventuell sogar 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. In vielen Unternehmen liegt der Schwerpunkt aber noch auf der technischen Umsetzbarkeit gewünschter „Industrie 4.0"-Funktionalitäten auf Produktionsebene. IT-Security ist dabei häufig noch ein Nebenaspekt.

Ein geeignetes Instrument, die eigene IT-Sicherheit auf den Prüfstand zu stellen, ist ein sogenannter „Penetrationstest". Also eine Hackerattacke unter kontrollierten Bedingungen. Auf diese Weise deckt man eventuell vorhandene Sicherheitslücken auf, noch bevor diese missbraucht werden können. Dabei sollte es jedoch nicht bei einer einmaligen Prüfung bleiben: Täglich werden neuen Sicherheitslücken in Softwareprodukten gefunden. Penetrationstests sollten deshalb fest in Prüfpläne integriert und regelmäßig durchgeführt werden. Der einzelne Test untersucht dabei ein oder mehrere individuell definierte Angriffsszenarien.

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 Infrastruktur eine längere „Lebensdauer". Wer als Penetrationstester erfolgreich sein will, sollte daher 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 Angriff kommen kann und im schlimmsten Fall Produktionsanlagen stillstehen. So berichtete etwa das BSI in „Die Lage der IT-Sicherheit in Deutschland 2014" von einem gezielten Hackingangriff auf ein deutsches Stahlwerk, bei dem die Steuerung eines Hochofens so manipuliert werden konnte, dass die Anlage beschädigt wurde.

Security 4.0

Die Digitalisierung in der produzierenden 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. 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 – auch direkt über das Internet – geschaffen werden, desto mehr muss auch mit potenziellen digitalen Angreifern gerechnet werden.

Szenarien Penetrationstest

1. Der Angriffsursprung (Von wo?)
2. Das Angriffsziel/der Scope (Was?)
3. Die Testtiefe (Wie detailliert?)
4. Die Testmittel (Wie?)
5. Der Wissensstand und die Motivation des Angreifers (Wer?)

Dr. Oliver Grasmück,
Leiter der Öffentlichkeitsarbeit SySS GmbH

Marcel Mangold,
Senior IT-Security Consultant SySS GmbH

SySS GmbH
www.syss.de