Drei Tipps für Cybersicherheit

Immer mehr Hersteller machen sich Sorgen um ihre Cybersicherheit, da jede Woche neue Ransomware und andere Schadprogramme entwickelt werden.

Jedes Unternehmen kann Ziel eines Cyberangriffs werden. Am besten lässt sich solchen Angriffen vorbeugen, indem man vorausplant und sich auf das Unerwartete vorbereitet.

1

Vernetzte Geräte

Die Vorteile mobiler Geräte kommen in den Bereichen Zustandsüberwachung sowie prädiktiver Instandhaltung und Analytik zum Tragen. Hersteller, die vernetzte Geräte nutzen, sollten regelmäßigen Sicherheitsupdates und Softwareprüfungen durchführen, um Systemfehler zu erkennen und zu beheben.

2

Bestandssysteme

In der Regel werden industrielle Computersysteme nicht so häufig aktualisiert oder ersetzt wie Verbrauchertechnologie. Dies kann dazu führen, dass Hersteller länger anfällig für ältere Schadprogramme wie Heartbleed oder Shellshock bleiben.

Bei älteren Systemen kann es sein, dass immer noch OpenSSL-Software installiert ist. In dieser Software enthaltene Schwachstellen ermöglichen es Angreifern, Daten abzufangen oder zu stehlen.

Um diese Schwachstellen zu beseitigen, stellen viele Softwareunternehmen kostenlos kritische Updates zur Verfügung. Hersteller müssen nichts weiter tun, als ihre Software zu aktualisieren.

3

Automatisierte Produktion-ssysteme

Doch Netzwerke und Systeme sind nicht die einzigen gefährdeten Elemente. Industrielle Kontrollsysteme können ebenfalls ins Zielvisier von Ransomware geraten. Falls Computer von Fertigungsanlagen lahmgelegt werden, kann dies zu kostspieligen Ausfallzeiten führen. Hersteller sollten automatisierte Fertigungssysteme durch Zellschutz schützen. Hierbei handelt es sich um eine effiziente Abwehr gegen Man-in-the-Middle-Angriffe.

Im Zeitalter von Industrie 4.0 können vernetzte Geräte und automatisierte Systeme zusätzlichen Bedrohungen ausgesetzt sein. Angriffen beugt man am besten vor, indem man vorausplant und sich auf das Unerwartete vorbereitet.