human power management ag

hpm ..Themenwelt

Cybersecurity: Herausforderungen in der digitalisierten Produktion

Algorithmen sind rücksichtlos

Die in der Presse berichteten Ereignisse, wie der versuchte Cyberangriff auf das Chemiewaffenlabor in Spiez oder der Ausfall vieler Computer durch die Ransomware Wannacry sind nur die Spitze eines Eisberges, der auch mittlere und kleinere Produktionsbetriebe gefährdet, die computergesteuerte Betriebsmittel einsetzen.

2010 wurde Stuxnet entdeckt, eine komplexe Malware, die wahrscheinlich zur Sabotage des iranischen Nuklearprogramms entwickelt wurde. Obwohl vieles darauf hindeutet, dass Stuxnet für einen gezielten Angriff konzipiert war, wurden diverse Produktionssysteme Unbeteiligter als Kollateralschaden betroffen, da der Angriff über die weitverbreiteten Produkte Microsoft Windows, Siemens WinCC und S7 Steuerungen umgesetzt wurde. Grund war die Art der Verbreitung, Nachlässigkeiten im Konzept und Fehler in der Programmierung.

Seither ist die Digitalisierung in der Produktion weiter fortgeschritten und die Vernetzung wird durch Konzepte wie Industrie 4.0 und IoT (Internet of Things) vorangetrieben. Zudem wurden auch die Angriffsmethoden verfeinert. Damit steigt die Verwundbarkeit gegenüber Malware, die industrielle Steuerungssysteme angreift. Dabei spielt es leider nur eine untergeordnete Rolle, ob der Betreiber des Steuerungssystems das eigentliche Angriffsziel ist, da die Verwundbarkeit bereits durch die Verwendung ähnlicher Hard- und Software entsteht. Damit werden Schutzmassnahmen auch für mittlere und kleinere Unternehmen relevant, die digital gesteuerte Produktionsmittel einsetzen.

Obwohl ein absoluter Schutz nur in Ausnahmefällen ein realistisches Ziel sein kann, können bereits relativ einfach umzusetzende Massnahmen Sicherheit und Resilienz markant erhöhen.

hpm human power management ag
Tuggenerstrasse 8
8008 Zürich

T: 043 443 0660
info@hpmag.ch
www.hpmag.ch

Spezialitäten der OT gegenüber der IT

Die Operational IT (OT), die in der Produktion eingesetzt wird, unterscheidet sich in wesentlichen Aspekten von der klassischen IT. Die OT Landschaft ist weniger homogen und Hard- und Software sind im Durchschnitt älter.

Hard- und Software der klassischen IT lässt sich vergleichsweise leicht standardisieren. OT Systeme werden hingegen in der Regel für einen spezifischen Zweck installiert und sind dafür optimiert.
Aufgrund dieser Diversität wird der Support für OT Systeme oft nicht von der firmeneigenen IT Abteilung sondern primär vom Lieferanten geleistet. Dieser hat dazu in vielen Fällen einen Fernzugriff Zugang für Wartungszwecke.

OT Systeme sind typischerweise auch wesentlich länger im Einsatz und werden oft bewusst nicht gepatcht, um die Verfügbarkeit im Produktionsprozess nicht zu gefährden. Damit entziehen sie sich dem standardisierten IT Security Management, was leicht dazu führt, dass die Verantwortlichkeit für die Sicherheit in eine organisatorische Grauzone abgleitet.

OT Systeme verarbeiten vielfach nicht nur Daten sondern steuern auch physische Aktoren, wie z.B. Motoren und Ventile. Unter Malwarebefall können sie damit grundsätzlich auch eine physische Beeinträchtigung des Produktionsprozesses und im Extremfall eine Gefährdung für Mensch und Maschine auslösen.

Gleichzeitig konvergieren IT und OT kommunikationstechnisch, was die Verbreitung von Malware sowohl für die Implementierung, als auch für den Transport erleichtert. Die zunehmende Standardisierung von Datenschnittstellen für industrielle Systeme zur Verbesserung der Interoperabilität trägt leider auch zur Verwundbarkeit bei. Statt produktspezifische Malware zu entwickeln, können Angreifer standardisierte Methoden verwenden. Damit steigt auch für Unbeteiligte die Gefahr, durch Kollateralschaden in Mitleidenschaft gezogen zu werden.

Bedrohungen, Akteure und deren Motivation

Die Bedrohungslage hat sich geändert. Was 1988 mit dem Morris Internet Worm als Studentenstreich begann, hat sich von der Spielwiese für aufmerksamkeitsheischende „Skript Kiddies“ und „Hacktivisten“ zum Geschäftsfeld von Klein- und Grosskriminellen gewandelt. Mittlerweile hat die Verwundbarkeit von digital kontrollierten Systemen auch die Aufmerksamkeit von staatlich gesponserten Institutionen zur Spionage und Sabotage gefunden.

Heute sind Malware Toolkits allgemein verfügbar, die ausreichend mächtig sind, um auf einfache Weise automatisiert flächendeckende Angriffe zu ermöglichen. Das bedeutet, dass ein Unternehmen für einen Angriff gar nicht mehr unmittelbar interessant sein muss, um Opfer zu werden.

Grundsätzlich muss darüber hinaus auch angemerkt werden, dass eine Firma nur darum schon interessant sein kann, weil sie eine bestimmte Industrie mit einer essentiellen Komponente beliefert.

Die OT ist wegen allfälligen bewusst nicht mit Updates versehenen Windows Rechnern gefährdet. Der durchaus sinnvolle Grundsatz „never change a running system“ kollidiert hier mit dem Bedarf, sich Veränderungen in der Bedrohungslage anpassen zu können. Die zunehmende Verbreitung von IoT Geräten auf Linux Basis stellt ebenfalls zusätzliche Einfallstore bereit, obwohl diese durch Phishing Angriffe weniger gefährdet sind, da sie in der Regel nicht von Menschen bedient werden. Fernzugriffsmöglichkeiten für Wartungszwecke sind ebenfalls potentielle Gefahrenquellen, wenn sie nicht akribisch gesichert sind.

Unter den Akteuren suchen „Skript Kiddies“ und „Hacktivisten“primär Aufmerksamkeit, ihre Ressourcen sind begrenzt und sie verursachen vor allem Ärger. Gefährlicher sind Elemente mit kriminellem Hintergrund, hier besteht für die meisten Firmen primär die Gefahr mit Ransomware erpresst zu werden. Es gibt aber auch einen Schwarzmarkt für infizierte Rechner, über die Eindringlinge die Kontrolle mit Malware übernommen haben, sogenannte Zombies. Hat ein Hacker die Kontrolle über Rechner in einem Firmennetz erlangt, kann er versuchen, diesen illegalen Zugriff zu verkaufen.

Eine noch gefährlichere und zunehmend registrierte Kategorie sind APT (Advanced Persistent Threat) Angriffe, zu denen auch der eingangs erwähnte Stuxnet gehört. Sie zielen auf ganze Industriezweige ab und sind auf den längeren Verbleib in Unternehmen ausgelegt, über Monate, häufig über Jahre. Hinter diesen Angriffen stehen Organisationen und sehr viel Geld. Unternehmen verlieren unter Umständen bei erfolgreichen Angriffen die Hoheit über ihr Netzwerk. Hier ist die OT in allen Elementen grundsätzlich gefährdet.

Angriffsmittel und Techniken

Schwere Angriffe erfolgen durchwegs über mehrere Stufen:
- Schwachstellenerkennung
- Auswahl des Angriffsmittels
- Übertragung des Schädlings
- Installation einer Zugriffmöglichkeit von aussen durch den Schädling
- Verbindungsaufbau von aussen zum infizierten System
- Aktion zur Erreichung des Angriffsziels

Nach Erfolg hat der Angreifer die Kontrolle über einen sogenannten Zombie, der in der Regel zweistufig über „Command & Control Server“ und einem „Botmaster“ kontrolliert werden. Solche Botnetze können automatisiert aufgebaut und auf dem Schwarzmarkt verkauft werden.

Schutzmassnahmen

• Awareness
Die Problemlösung beginnt mit der Problemfeststellung

• Inventar
Um eine umfassende Sicherheitslösung zu implementieren ist eine vollständige Übersicht über die potentiell gefährdeten OT Systeme unerlässlich

• Patchen
Die identifizierten Systeme sind auf den aktuell sichersten Stand zu bringen

• Segmentierung
Eine Segmentierung des Netzwerkes erschwert den Angriff und ermöglicht als speziell gefährdet identifizierte Systeme zusätzlich zu schützen

• Backups
Für die inventarisierten Systeme ist ein auf Abwesenheit von Malware verifizierter Backup zu erstellen und ein zugehöriges Restore Prozedere zu definieren und zu testen

• Detektion
Nach Möglichkeit sollten im Netzwerk Detektionssysteme installiert werden, die Anomalien erkennen können. Auf jeden Fall sollte unerklärtes Verhalten aufgezeichnet werden.

• Reaktion
Die identifizierten Systeme müssen in einen Incidence Response Prozess eingebunden sein. Unerklärbares Verhalten muss immer auf den Grund gegangen werden, da ein Sicherheitszwischenfall nicht in jedem Fall auf den ersten Blick als solcher erkannt werden kann.

Interim Projektleiter Cyber Security

die erfolgreiche Umsetzung eines Projektes benötigt nebst vielen Aspekten immer zwei Grundvoraussetzungen:

- Kapazität
- Kompetenz

Bei uns finden Sie Beides!

Steht bei Ihnen genau ein solches oder ähnlich gelagertes Projekt an und Sie haben das Interesse, dieses mit uns abzuwickeln? Über eine Kontaktaufnahme freuen wir uns.

hpm human power management ag, Zürich