Das Industrie-4.0-Dilemma

Messbare IT-Sicherheit in Industrieumgebungen

Kai-Oliver Detken

Produktionsanlagen und dort verwendete Betriebssysteme entsprechen nicht unbedingt den heutigen Sicherheitsstandards, da sie für wesentlich größere Nutzungszyklen ausgelegt sind. Das war ohne Vernetzung bisher auch kein Problem. Durch Industrie 4.0 und dem notwendigen Fernwartungszugang für Hersteller ändert sich dies aber. Hinzu kommt, dass Standardprotokolle wie TCP/IP zur Anwendung kommen. Daher müssen, ähnlich wie in der sogenannten Office-IT, Sicherheitskonzepte und -implementierungen eingeplant werden. Wie ist dazu der aktuelle Stand? Wie können unbekannte Anomalien erkannt werden? Und welche Lösungen existieren bereits?

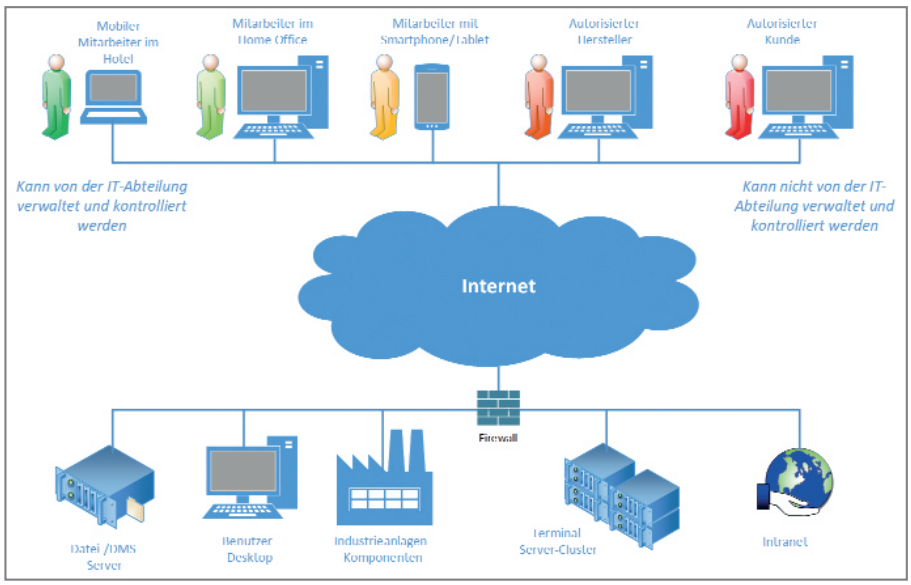

Bild 1: Mannigfaltige Remote-Zugriffe müssen verwaltet werden

Industrieanlagen wurden bisher immer autonom und abgeschottet betrieben. Um allerdings immer mehr Technikerkosten einsparen zu können, die Wartungsverträge vor Ort erfüllen müssen, haben auch Hersteller von Industriesystemen das Internet für sich entdeckt. Über Remote-Wartungszugänge können Anlagen bequem zentralisiert auf dem neuesten Stand gehalten werden (*Bild 1*). Das spart Kosten und Personal, beinhaltet aber auch neue Angriffspotenziale, da ebenfalls Angreifer versuchen könnten, diese Zugänge auszunutzen.

Daher muss man sich mittlerweile auch in Industrienetzen mit dem Thema IT-Sicherheit gezwungenermaßen auseinandersetzen, was für viele Hersteller und Unternehmen anscheinend Neuland darstellt. Denn laut einer ICS-Studie von Kaspersky Lab aus dem letzten Jahr sollen alleine 26.000 unsichere ICS-Komponenten in Deutschland problemlos über das Internet erreichbar sein (ICS – Industrial Control System, industrielles Steuerungssystem). Hinzu kommt, dass es spezielle Suchmaschinen wie Shodan (https://www.shodan.io) gibt, die gezielt nach offenen Internetverbindungen in produktionsspezifischen Protokollen suchen.

Durch das IT-Sicherheitsgesetz (ITSiG) für kritische Infrastrukturen (Kritis) ist immerhin Bewegung in den Markt gekommen. Dieses setzt einen gewissen Stand der Technik in den betroffenen Unternehmen voraus, damit ein ausreichender Schutz sichergestellt ist. Dabei reicht es nicht mehr aus, die jeweiligen Netze voneinander zu trennen.

Was ist der Stand der Technik?

Kritis-Betreiber, zu denen u.a. Stadtwerke, Energieversorgungsunternehmen und Abwasserfirmen gehören, haben ein dem Stand der Technik entsprechendes Mindestniveau an IT-Sicherheit einzuhalten. Zudem besteht die Verpflichtung, erfolgreiche und nicht erfolgreiche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Nur, wie der Stand der Technik aussieht, wird leider nicht genau festgelegt. Das ist praktisch für das BSI, da solche Empfehlungen auch künftig nicht angepasst werden müssen, birgt aber eine gewisse Unsicherheit,

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

ob alle Maßnahmen ausreichend umgesetzt wurden. Immerhin kann man sich anhand der Schutzziele orientieren, die in dem IT-Sicherheitsgesetz gefordert werden, da sie allgemeingültig sind (s.a. Altrhein, Barchnicki, Karsten, Bartels u.a.: Handreichung zum „Stand der Technik" im Sinne des IT-Sicherheitsgesetzes (ITSiG). TeleTrusT – Bundesverband IT-Sicherheit e.V., Berlin 2016):

- Die *Verfügbarkeit* von IT-Systemen und -Komponenten ist vorhanden, wenn diese stets gemäß ihrem Zweck und Funktionsumfangs genutzt werden können.
- Die *Integrität* bezieht sich insbesondere auf die Daten. Sie ist vorhanden, wenn sichergestellt ist, dass die gesendeten Daten den Empfänger unverändert und vollständig erreichen.
- Die *Vertraulichkeit* ist gegeben, wenn die schützenswerten Daten nur in der zulässigen Art und Weise ausschließlich an die Befugten verfügbar gemacht werden.
- Die *Authentizität* ist vorhanden, wenn die eindeutige Identität der Kommunikationspartner (aber auch der kommunizierenden Komponenten) sichergestellt ist.

Auf technische Verfahren bezogen sollten daher fortschrittliche Techniken wie 2-Faktor-Authentifizierung, Datenverschlüsselung, Einsatz von sicheren Boot-Prozessen, Patch-Management, sichere Backup-Systeme, Hochverfügbarkeit und Malware-Schutz eingesetzt werden. Aber auch dem Monitoring und Reporting fällt eine wichtige Rolle zu. Durch die älteren Strukturen in Industrie- gegenüber Büroumgebungen sind aber teilweise nicht alle Anforderungen umsetzbar. So lässt sich z.B. ein Patch-Management bei älteren Betriebssystemen (z.B. Windows XP) nicht mehr durchführen, weil keine Patches mehr vom Hersteller herausgegeben werden. Ein weiteres Problem beim Monitoring: Es dürfen keine aktiven Scans auf die Industriekomponenten erfolgen, weil das die Verfügbarkeit beeinträchtigen kann. Daher müssen Industrienetze teilweise anders behandelt werden. Grundsätzlich hinken sie der IT-Sicherheit herkömmlicher Netze hinterher, weil die verwendeten Komponenten nicht dafür vorgesehen waren oder nicht entsprechend erweitert werden können.

Anomalieerkennung

Unternehmen müssen, unabhängig vom ITSiG, zum Schutz des eigenen Wissens und der Informationen, ihre eigene IT-Infrastruktur ausreichend absichern. Dieser Schutz muss der aktuellen Bedrohungslage, die geprägt ist von einer großen Vielfalt verschiedener Endgeräte und Anwendungen sowie einer stetigen Tendenz hin zur dynamischen Vernetzung von mobilen Endgeräten, Rechnung tragen. Dabei wird es immer wichtiger, Anomalien rechtzeitig zu erkennen und einem Angriff entgegenzuwirken, bevor dieser einen Schaden anrichten kann. Laut BSI vergehen bis zu 227 Tage im Schnitt, bis eine gezielte Attacke auf ein Unternehmen bemerkt wird. Ein viel zu langer Zeitraum, um schadensfrei davonzukommen.

Zur Anomalieerkennung lassen sich folgende Systeme grundlegend unterscheiden:

- Intrusion Detection and Prevention System (IDS/IPS): Man kann hier zwischen signatur- und anomaliebasierten Verfahren unterscheiden. Signaturen sind dabei auf vorab bekannte und erfasste Angriffsszenarien beschränkt, während anomaliebasierte Verfahren das Normalverhalten analysieren und Abweichungen und damit auch bisher unbekannte Angriffe erkennen können. Anomaliebasierte Verfahren haben allerdings meist den Nachteil, eine hohe Zahl von Falschmeldungen zu produzieren.
- Security Information and Event Management (SIEM): Um eine umfassende Betrachtung aller sicherheitsrelevanten Daten zu ermöglichen, damit komplexe Bedrohungsszenarien erkannt werden können, sind SIEM-Systeme entwickelt worden. Damit lassen sich Datenintegration und -auswertung vornehmen. Auch auf dieser Ebene kann mit statischen Regeln oder mit Anomalieerkennung gearbeitet werden. Im Gegensatz zu IDS/IPS müssen SIEM-Systeme generell mit wesentlich heterogeneren Daten und größeren Datenmengen umgehen können.

Beide Systeme gehören heute noch nicht zur Standardausrüstung in Unternehmensnetzen. Das liegt bei den IDS/IPS-Lösungen daran, dass eine hohe Zahl von Meldungen sinnvoll bearbeitet und eingeschätzt werden müssen, dafür aber oftmals die Mitarbeiterressourcen nicht zur Verfügung stehen. Zwar kann ein IPS-System auch automatisiert Gegenmaßnahmen ergreifen, was aber aufgrund der hohen Anzahl von Falschmeldungen nicht empfohlen werden kann.

SIEM-Systeme versprechen eher Abhilfe, da sie kontextbezogen verschiedene Sensordaten auswerten und lesbare Handlungsempfehlungen zur Verfügung stellen. Sie ermöglichen es, IT-Sicherheit messbar zu machen, indem beispielsweise die Effektivität von Antivirensystemen ausgewertet wird. Allerdings sind solche Systeme bisher nicht für Industrieumgebungen entwickelt worden und müssen sich grundsätzlich noch etablieren.

Kommerzielle Produkte und Forschungsprojekte

Der Markt für kommerzielle Produkte bietet eine Vielzahl von Optionen im SIEM-Bereich. Da auch die Hersteller kommerzieller Systeme erkannt haben, dass Systeme mit festen Regelwerken (SIEM der 1. Generation) zu unflexibel und in der Pflege und Entwicklung aus Kundensicht zu personalintensiv sind, wurde nach „intelligenteren" Lösungen gesucht:

- Vom Anbieter gepflegte, statische Regelwerke, die gegen dynamische Listen für verdächtige Objekte (z.B. IP-Adressen, URLs, Hashes von Binärcode) vergleichen, z.B. IBM QRadar SIEM, Tenable LCE, McAfee Enterprise Security SIEM. Die Regelwerke werden dann im Zuge von Updates z.B. monatlich erneuert, die dynamischen Listen deutlich häufiger.
- Statistische Zeitreihenanalyse von einzelnen Metriken (z.B. Nutzerzahlen, Netzbandbreite), um die Entwicklung über die Zeit als „Normalzustand" zu ermitteln, diesen dynamisch fortzuschreiben und dann

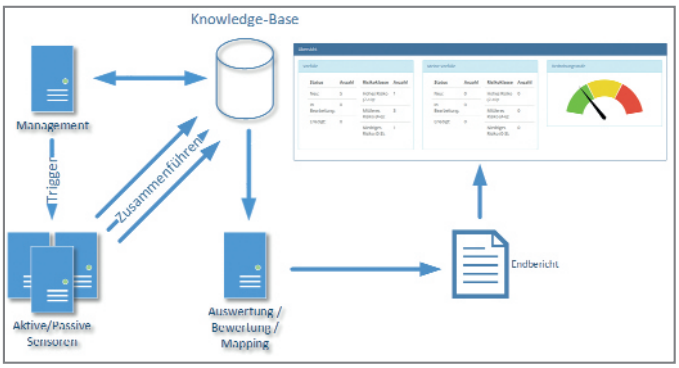

Bild 2: Ablauf eines ScanBox-Prozesses

Bild 3: Visualisierung der Vorfälle und messbare Aussage der IT-Sicherheit

signifikante Abweichungen zu detektieren. Die überwachten Metriken (nummerische Werte) und Schwellwerte für Abweichungen müssen vom Anwender definiert werden. Diese Fähigkeit ist in vielen kommerziellen Produkten zu finden.

- User and Entity Behavior Analysis (UEBA): Hierbei werden für einzelne Nutzer oder Komponenten wie IP-Adressen, Server und Anwendungen Modelle des Normalverhaltens mithilfe statistischer Analysen oder von Lernverfahren erstellt, um dann Abweichungen erkennen zu können. Hier werden neben regelbasierten und statistischen Ansätzen zunehmend auch Machine-Learning-Verfahren eingesetzt. Diese Techniken werden in mehreren Produkten genutzt (z.B. IBM QRadar, Logrhythm UEBA, Arcsight UBA, Darktrace Enterprise).

Aber auch im Forschungsumfeld gibt es Bestrebungen, die Anomalieerkennung zu verbessern bzw. intelligenter umzusetzen. So fokussiert das Projekt Scanbox den Prototyp einer Security-Analyse-Hardware-Appliance (**www.scanbox-project.de**). Autark in Netzen oder Netzsegmenten platziert, soll das System ohne Eingriff von außen das aktuelle Sicherheitsniveau des Netzes erheben. Das Appliance-System wird vor dem Einsatz automatisch mit den relevanten Sicherheits-Updates versorgt und anschließend vom Nutzer im zu bewertenden Netzsegment platziert und aktiviert. Ab diesem Zeitpunkt arbeitet das Gerät dann vollautomatisch.

Nach jedem Scan-Prozess wird ein Bericht erstellt und in der Knowledge-Base hinterlegt (*Bild 2*). Ein Gesamtreport führt die Einzelberichte zusammen und erstellt eine ganzheitliche Beurteilung. Hier werden Schwachstellen nach Schweregrad sortiert und aufgelistet. Zur leicht verständlichen und übersichtlichen Darstellung kommt ein einfaches Visualisierungsschema zum Einsatz (*Bild 3*). Die geplante Lösung soll Nutzern bei detektierten Fehlern konkrete Hilfestellung bei der Behebung der erkannten Schwachstellen anbieten. Hierfür ist ein Mapping auf die Lösungsvorschläge des BSI vorgesehen.

Das Projekt Glacier verfolgt hingegen einen anderen Ansatz (**www.glacier-project.de**). Hier hat man ebenfalls erkannt, dass die zunehmende Integration von klassischer IT sowie von Produktions- und Steuersystemen ganz neue Risiken erzeugt. Neben klassischen Sicherheitsmaßnahmen wie Firewalls und Malware-Schutz gewinnen Logging und Monitoring daher zunehmend an Bedeutung. Denn jedes Unternehmen muss davon ausgehen, dass professionelle Angreifer:

- den Perimeterschutz überwinden können;
- der eingesetzte Schadcode nicht zuverlässig erkannt wird.

Das Eindringen kann dann nur durch ungewöhnliches System- oder Applikationsverhalten sowie anomale Netzkommunikation erkannt werden.

Die Erkennung setzt typischerweise aber auch voraus, dass die Daten unterschiedlicher Systeme in einem Analysesystem aggregiert und korreliert werden. Dabei ergeben sich durch die großen Datenmengen besondere Herausforderungen. Gegenstand des Vorhabens ist deshalb die Entwicklung von fortgeschrittenen Konzepten zur automatischen Aggregation und Analyse sicherheitsrelevanter Netzdaten. Durch die automatisierte Aggregation und Analyse soll nicht nur eine Anomalie erkannt, es soll auch die Sicht auf die Daten (Aggregationsebene), die das Fehlverhalten beschreibt, direkt aufgezeigt werden können.

Fazit

Der Nachweis für Sicherheits- und Qualitätsanforderungen wird komplexer und durch die starke Vernetzung steigt das Angriffsrisiko. Auch fordern immer mehr Gesetze entsprechende Sicherheitsmaßnahmen, die nicht nur den Kritis-Bereich betreffen. Unternehmen und Betreiber müssen daher ein profundes Security- und Risk-Management vorweisen und belegen, dass ihre IT-Infrastruktur über ausreichende Schutzmechanismen verfügt. Dazu muss mindestens der Stand der Technik zwingend eingehalten werden, um kein Einfallstor für Angreifer zu bieten. Zusätzlich sollte ein Monitoring auf Anomalien erfolgen, was die Überwachung der Verfügbarkeit ergänzt, um Sicherheitslücken zeitnah erkennen zu können.

Hierfür kommen SIEM-Lösungen infrage, die in der Lage sein sollten, mehr als statische Regelwerke abzudecken und die IT-Sicherheit messbar machen. Herstellerlösungen sind teilweise vorhanden, decken aber meistens nur Büronetze ab. Erste Forschungsprojekte sind hingegen angetreten, um auch zukünftig in Industrie-4.0-Umgebungen ein höheres Sicherheitsniveau zu ermöglichen. *(bk)*