Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 106 (2015)
Heft: 10

Artikel: IT-Sicherheit in der industriellen Produktion
Autor: Krägelin, Birger
DOI: https://doi.org/10.5169/seals-856727

IT-Sicherheit in der industriellen Produktion

Herausforderungen durch Industrie 4.0 und Internet of Things

In der vernetzten Welt endet der Schutz von Produktionsanlagen nicht mehr am Gebäude oder am Fabrikgelände. Über Netzwerkverbindungen können Angreifer in Systeme eindringen und diese manipulieren. Schadcode-Infektionen können weite Bereiche lahmlegen und dabei immense physische Schäden sowie Gefahren für Leib und Leben verursachen. Nicht erst seit Meldungen über Stuxnet, Duqu, Flame und Havex ist klar, dass Produktionsanlagen Ziele von Cyber-Angriffen sind.

Birger Krägelin

Moderne Produktionsanlagen sind hochgradig vernetzt: Eingebettete Systeme kommunizieren selbstständig miteinander, Planungssysteme in der Cloud berechnen Auftragsschritte und Maschinenbelegungen, Anlagenführer überwachen und steuern aus der Ferne, Wartungspersonal greift weltweit zu und führt Konfigurationsänderungen aus.

IT-Sicherheit in der industriellen Produktion muss dabei spezifische Randbedingungen berücksichtigen, die im Büro-Umfeld, bei PC-Arbeitsplätzen und Internet-Servern so nicht zu finden sind. Die Steuerung von Produktionsanlagen stellt Echtzeit-Anforderungen, die Veränderungen auf den Systemen schwierig bis unmöglich machen. So können Software-Patches, Installation von Überwachungs-Software, Malware-Scanner und Antivirus-Programme die Funktion beeinträchtigen. Firewalls im Netzwerk und verschlüsselte Verbindungen können die Echtzeitfähigkeit gefährden. Auch der vergleichsweise lange Nutzungszeitraum von Hard- und Software in der Produktion unterscheidet sich erheblich von anderen IT-Einsatzgebieten.

Für Produktionsumgebungen müssen daher neue Strategien und Verfahrensweisen gefunden werden, um IT-Sicherheit in der Praxis umzusetzen, und das nicht nur in neuen Systemen, sondern vor allem in Altanlagen.

Anatomie von Angriffen

Angriffe gegen Produktionsanlagen können vielfältig sein und unterschiedliche Ziele haben. Von Störungen im Produktionsablauf (Denial of Service) über Diebstahl von Firmengeheimnissen bis zur Beschädigung von Maschinen und Anlagen oder der grossflächigen Zerstörung ganzer Fabriken reicht dabei die Bandbreite. Um sich gegen solche Angriffe wirksam schützen zu können, müssen daher die möglichen Angriffswege genauer betrachtet werden.

Erste Anlaufstelle für Angreifer sind dabei spezialisierte Suchmaschinen wie Shodan (www.shodan.io, **Bild 1**), die an das Internet angeschlossene Geräte suchen. Mit Suchanfragen wie «Scada», «Default Password» oder Gerätebezeichnungen namhafter Hersteller lassen sich lohnende Ziele für Angriffe finden.

Netzwerke in der Fabrik

Typische Produktionsanlagen sind heute noch in dem Verständnis aufgebaut, dass ein physischer Schutz von Gebäude und Gelände gegeben ist und keine unautorisierten Personen zugreifen können. Jedoch schon mit der Einrichtung von Fernwartungszugängen für eigenes Bedienpersonal oder für Techniker von Wartungsfirmen ist diese physische Trennung nicht mehr gegeben. Und spätestens mit der Umstellung von Modem-Verbindungen auf DSL-Anschlüsse ist die Fabrik direkt mit dem Internet verbunden.

Im Zuge der Ersetzung von Zweidrahtleitungen und Feldbussen durch billige Ethernet-Technik wandelt sich das Fabriknetz zu einem klassischen Local Area Network (LAN), das mit den gleichen Techniken strukturiert und abgesichert werden muss, die in der Office-IT seit Jahren üblich sind. Sicherheitsmassnahmen sind auf verschiedenen Ebenen anzuwenden (Defense in Depth).

Häufig kommen diese Veränderungen jedoch schleichend, der Umbau bzw. die Netzwerk-Implementierung wird von Automatisierungsspezialisten ohne vertiefte IT-Sicherheitskenntnisse durchgeführt. Planungs- und Konfigurationsfehler sowie das Fehlen von Standard-Sicherheitsmechanismen sind die Folge. Ein Netzwerk-Auditing sowie einfache Penetration-Tests können Schwachstel-

Shodan

Bild 1 Suchmaschine Shodan.

Fraunhofer IOSB

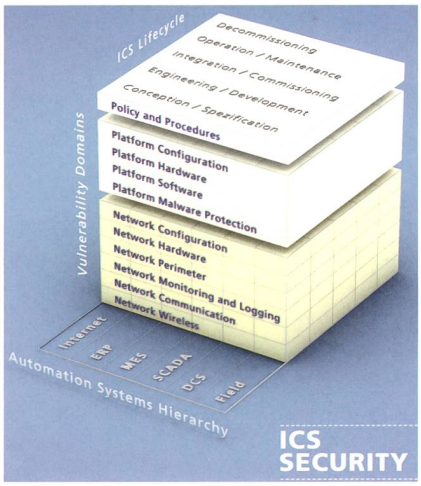


Bild 2 Sicherheitsmodell für Produktionsanlagen.

len ans Licht bringen. Oft können diese mit vorhandenen Mitteln beseitigt werden, da moderne Netzwerk-Komponenten bereits über umfangreiche Sicherheitsmechanismen wie Paketfilter oder Überwachungs- und Logging-Möglichkeiten verfügen.

Scada-Ebene

Die Ebene der Produktions-Leit- und Überwachungssysteme besteht meist aus Systemen, die auch in der Office-IT eingesetzt werden. Häufig werden hier als Betriebssystem Microsoft Windows oder Unix/Linux eingesetzt. Diese Systeme sind auf gleiche Weise verwundbar und angreifbar. Ohne Internet-Verbindung sind auf diesen Systemen Antivirus-Programme und Malware-Scanner nicht installiert, da diese ohne Online-Verbindung auch keine Updates ihrer Datenbanken durchführen können.

Wie in der Office-IT müssen jedoch auch hier entsprechende Sicherheitsmechanismen implementiert werden. Dazu gehören insbesondere eine sichere Authentifikation und ein umfassendes Rechtemanagement, je nach Einsatzumgebung auch eine Zwei-Faktor-Authentifizierung zum Zugriff auf kritische Systeme oder auf Funktionen mit weitreichenden Berechtigungen. Eine Segmentierung des Netzwerkes durch Einsatz von Firewalls anstelle der vielfach noch üblichen zweiten Ethernet-Karte im PC muss selbstverständlich sein. Neben der Installation eines Viren-/Malware-Schutzes sind auch ein Patch-Management zur zeitnahen Beseitigung von Software-Verwundbarkeiten und ein Auditing und Logging notwendig. Durch den Einsatz kryptographischer Verfahren müssen mindestens Authentifizierungsdaten, Maschinenparameter und Steuerungsprogramme, die über Netze übertragen werden, gegen Abhören und Verfälschen geschützt werden.

Da die Angriffspunkte und -techniken vielfältig sind und Schadprogramme auch unbemerkt in Systeme eingeschleust werden können, die nicht mit dem Internet verbunden sind (Air Gap), müssen diese Massnahmen durchgehend umgesetzt werden.

Steuerungsebene

Erfolgreiche Angriffe gegen Steuerungen erfordern detaillierte Prozesskenntnisse, wenn der Angreifer einen grossen, lang anhaltenden Schaden verursachen will. Entsprechend aufwendig (und teuer) sind die Vorbereitungsmassnahmen. Dies ist auch einer der wesentlichen Gründe, wieso über erfolgreiche Angriffe gegen Produktionsanlagen bisher wenig bekannt wurde.

Mittlerweile sind jedoch bereits erste Angriffsprogramme (Exploits) verfügbar, die Standardkomponenten adressieren und dort Schäden verursachen. Je nach Produktionsprozess können mit ihnen Produktionsstörungen und -ausfälle herbeigeführt werden, die einen hohen wirtschaftlichen Schaden verursachen.

Auch bei Steuerungen finden sich heute bereits viele Sicherheitsmechanismen wie Authentifikation und Verschlüsselung von Netzwerkverbindungen, die jedoch bisher nicht regelmässig aktiviert werden. So ist es häufig noch üblich, vom Hersteller gesetzte Standardpasswörter beizubehalten oder für einen Benutzerzugang keinen Passwortschutz zu aktivieren. Auch die Aktivierung von https- anstelle von http-Verbindungen wird oft nicht durchgeführt.

Maschinensteuerungen und speicherprogrammierbare Steuerungen sind keine Universalcomputer. Sie haben eine eingeschränkte Aufgabe, müssen stromsparend, robust und billig sein. Dementsprechend ist die Rechenleistung begrenzt und reicht oft für umfangreiche kryptographische Funktionen oder Zusatzaufgaben wie Logging nicht aus.

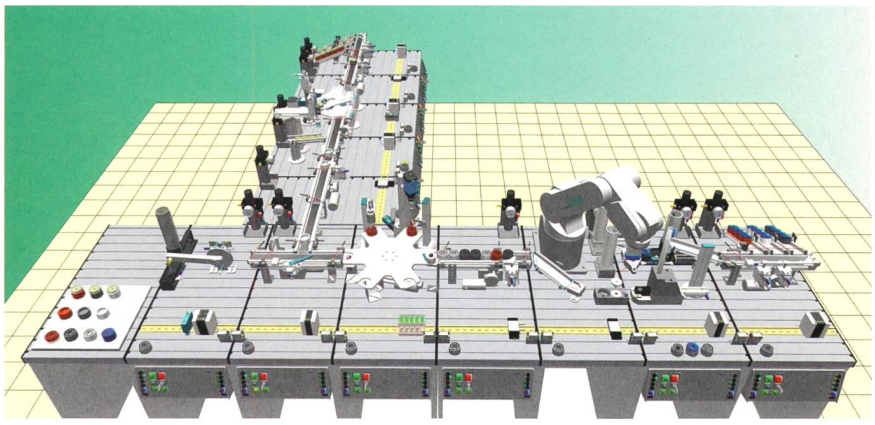
Die Programmierer bei den Herstellern dieser Geräte verfügen selten über ausreichende IT-Sicherheitskenntnisse, ein Entwicklungsprozess zur Erstellung sicherer Software (Security by Design) fehlt. Das Aufdecken fehlerhafter Schnittstellen, falsch implementierter Sicherheitsfunktionen oder Hersteller-eigener Kryptographie-Funktionen, die in kurzer Zeit gebrochen werden können, sind an der Tagesordnung.

Herausforderung Cloud

In den Szenarien von Industrie 4.0 besitzen alle Komponenten in den Produktionsanlagen und Fabrikumgebungen erweiterte Intelligenz und kommunizieren miteinander. Clouddienste ermöglichen dabei die bedarfsgerechte Bereitstellung der notwendigen Verarbeitungsleistung mit gemeinsam genutzten IT-Ressourcen. Die Komponenten selbst können dabei kleiner und kostengünstiger ausfallen, denn sie integrieren nur noch lokale Schnittstellen, Kommunikationsdienste und Notfallfunktionen. Durch Anpassung und Erweiterung in der Cloud können neue und verbesserte Funktionen schnell und einfach eingeführt werden.

Bei einer Kommunikation über das Internet besteht zusätzlich die Möglichkeit, Informationen und Visualisierungen zur Überwachung und Steuerung der Anlagen bei Bedarf überall abzurufen und z.B. Tablets oder Smartphones in die betrieblichen Abläufe zu integrieren.

Voraussetzung hierfür sind zuverlässige Kommunikationsverbindungen (Verfügbarkeit) und angepasste Sicherheits-



Fraunhofer IOSB

Bild 3 Simulierte Produktionsanlage im Fraunhofer IOSB.

massnahmen, um die eindeutige Identifikation der beteiligten Kommunikationspartner sicherzustellen (Authentizität) und den Zugriff Fremder auf Daten (Vertraulichkeit) und Verarbeitungsfunktionen (Autorisierung) zu verhindern.

Besondere Risiken entstehen dabei einerseits durch Implementierungsfehler der Sicherheitsfunktionen in den beteiligten Komponenten oder deren fehlerhafte Konfiguration beim Einsatz, andererseits entsteht durch die Zentralisierung von IT-Ressourcen ein Single Point of Attack. Insbesondere die Verlagerung von Aufgaben zu externen Dienstleistern in Public-Cloud-Systeme eröffnet Angreifern ein lohnendes Ziel. Hier können Angreifer mit überschaubarem Aufwand ganze Industriebereiche gleichzeitig treffen.

Aber auch die Inhouse-Konsolidierung in Private-Cloud-Systemen bietet den Angreifern neue Möglichkeiten. Meist sind diese Systeme in klassischer IT-Technik aufgebaut und haben bekannte Fehler und Schwachstellen. Darüber hinaus werden in Private Clouds oft mehrere Anwendungen des Unternehmens gehostet, so dass ein erfolgreicher Angriff gleich weite Teile des Unternehmens, von der Produktion über die Office-IT bis hin zu ERP-Systemen, lahmlegen kann.

Umfassender Ansatz

Ein Sicherheitsmanagement für Produktionsanlagen muss alle beteiligten Komponenten erfassen und den ganzen Lebenszyklus von Anlagen berücksichtigen. Bild 2 zeigt die verschiedenen Dimensionen, die dabei zu betrachten sind.

Schwachstellen und Verwundbarkeiten finden sich in den verschiedenen Bereichen der Netzwerk-Implementierung, bei den eingesetzten Komponenten und Geräten, aber auch in den organisatorischen Vorgaben und den Geschäftsprozessen. Um diese zu vermeiden oder zumindest effektiv behandeln zu können, sind Vorkehrungen in allen Phasen einer Produktionsanlage zu treffen, beginnend bei der Spezifikation von Neuanlagen oder Umbauten/Erweiterungen bis hin zum Abbau und der Entsorgung. Denn auch bei der Entsorgung von Komponenten müssen Firmengeheimnisse wie Rezepturen, Maschinenparameter oder Passwörter und kryptographische Schlüssel noch geschützt werden. In dieses Sicherheitsmanagement sind auch alle Ebenen im Unternehmen einzubeziehen.

Aktivitäten der Fraunhofer-Gesellschaft

Die Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. arbeitet mit ihren 66 Forschungsinstituten in Deutschland an Zukunftsszenarien auch für die vernetzte Produktion. Insbesondere die Herausforderungen der Internet-Anbindung und der Nutzung von Cloud-Diensten sind dabei ein wichtiges Thema.

Das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB in Karlsruhe hat zu diesem Zweck ein besonderes IT-Sicherheitslabor für Produktionsanlagen eingerichtet, in dem die Wissenschaftler Schwachstellen und Verwundbarkeiten von Geräten und Komponenten sowie Design-Schwächen von Netzwerk-Protokollen untersuchen und Massnahmen zur Abwehr sowie neue Sicherheitslösungen entwickeln. Schwerpunkte liegen dabei in der Analyse von Angriffsszenarien und in Verfahren zur Angriffserkennung sowie im Einsatz und in der Weiterentwicklung von OPC-UA als Kommunikations-Framework für die Szenarien der Industrie 4.0. Zudem arbeiten die Forscher an der Übertragung von selbstlernenden Verfahren zum Condition Monitoring komplexer Prozesse auf eine Anomalie-Erkennung in Netzwerken auf der Ebene von Steuerungen.

Dazu können sie im Labor unterschiedliche Fabrikumgebungen mit virtuellen und realen Komponenten nachstellen und Angriffe simulieren. So können Komponenten im Einsatz untersucht und kundenspezifische Abwehrstrategien entwickelt werden. Bild 3 zeigt eine simulierte Produktionsanlage, die von physischen speicherprogrammierbaren Steuerungen gesteuert wird. Angriffe durch Malware werden hier untersucht, ohne dass die Gefahr physischer Schäden an realen Maschinen besteht.

Autor

Dipl.-Inform. **Birger Krägelin** ist IT-Sicherheitsbeauftragter im Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB in Karlsruhe. Dort leitete er 2014 den Aufbau eines IT-Sicherheitslabors für Produktionsanlagen, das er auch weiterhin beratend begleitet. Als Spezialist für Netzwerksicherheit und Cloud-Computing berät er interne und externe Kunden.

Fraunhofer IOSB, DE-76131 Karlsruhe
birger.kraegelin@iosb.fraunhofer.de

Résumé

Sécurité informatique dans la production industrielle

Défis liés à l'industrie 4.0 et à l'Internet des objets

Dans le monde interconnecté, la protection d'installations de production ne s'arrête plus au bâtiment de l'entreprise ou sur le terrain de l'usine. Par l'intermédiaire de connexions réseau, des pirates peuvent s'infiltrer dans les systèmes et les manipuler. Des codes malveillants peuvent paralyser de vastes domaines et ainsi provoquer d'importants dommages physiques, voire mettre la vie de personnes en danger.

La gestion de la sécurité des installations de production doit comprendre tous les composants impliqués et prendre en considération tout le cycle de vie des installations, en commençant par la spécification des nouvelles installations ou des transformations/extensions et allant jusqu'au démantèlement et à l'élimination. Car lors de l'élimination de composants, les secrets professionnels tels que les recettes, paramètres machine ou mots de passe et clés cryptographiques doivent également être protégés. No

Electrosuisse / ITG-Kommentar

Kontrollverlust durch die Vernetzung?

Die Vereinheitlichung der in der Wirtschafts- und Prozessinformatik eingesetzten Technologien ist heute aus wirtschaftlichen Gründen Realität. Gleichzeitig werden die Systeme zunehmend vernetzt, um die Automatisierung zu erhöhen, den Betrieb zu optimieren und neue Geschäftsmodelle zu unterstützen. Der Trend zu weiteren Sensoren im Internet of Things (IoT) beschleunigt die Vereinheitlichung und Vernetzung.

Eine Standardisierung in der Vernetzung der beiden Welten ist noch nicht etabliert und die eingebauten Sicherheitsfunktionen nicht aufeinander abgestimmt. Um industrielle Steuerungs- und Informationssysteme sowie ihre Schnittstellen abzusichern, ist die ganzheitliche Sicherheitsbetrachtung besonders wichtig, denn sie bildet die Voraussetzung zur Nutzung der neuen Möglichkeiten ohne Kontrollverlust.

Dr. **Thomas Wettstein,** CEO Avectris AG, und Vorstandsmitglied der Informationstechnischen Gesellschaft (ITG) von Electrosuisse