WHITEPAPER

SECURITY IS OUR PROMISE

INDUSTRIAL SECURITY VON ANFANG AN

Die Komplexität von automatisierten Maschinen und Anlagen steigt stetig. Immer mehr Komponenten werden untereinander vernetzt und tauschen Informationen aus – auch über Unternehmensgrenzen hinweg. Je größer das Netzwerk ist, desto höher ist das Risiko, dass eingeschleppte Schadsoftware unbemerkt bleibt und ihr Ziel verfolgen kann. Industrial Security muss deshalb die Basis für die industriellen Netzwerke sein und nicht nur ein Add-on. Mit diesem Whitepaper möchten wir über die Risiken der digitalisierten Produktionswelten aufklären und gleichzeitig Lösungsansätze bieten, wie den Gefahren begegnet und die Risiken minimiert werden können.

WAS SIND DIE GEFAHREN UND RISIKEN?

- Diebstahl von persönlichen Daten, Betriebsdaten und geheimen Rezepturen
- Sabotage, um die Anlagen zu beschädigen oder die Umwelt zu gefährden
- Manipulation, um die Produktqualität herabzusetzen oder komplett Ausschuss zu produzieren
- Verschlüsselung von Daten, um Lösegeld zu erpressen

Es ist für jedes Unternehmen zu empfehlen, anhand einer eingehenden Risikoanalyse zu ermitteln, welche Risiken und Angriffsflächen konkret bestehen, und welche Schutzmaßnahmen dafür geeignet sind.
Nach dem Stand der Technik ist ein 100%iger Schutz nicht möglich. Ziel der Risikoanalyse ist vielmehr, die möglichen Gefahren zu erkennen und zu bewerten, welche Auswirkungen auf das eigene Unternehmen im Zweifelsfall zu erwarten sind. Sinnvollerweise werden einzelne Maschinen und Anlagen spezifisch betrachtet.

DIE ÜBLICHEN HERAUSFORDERUNGEN

- In Produktionsanlagen sind Komponenten verbaut, die keine eigenen Schutzmechanismen (beispielsweise Nutzer-Authentifizierung) haben
- Teilweise extrem heterogene und komplexe Systeme
- Netzwerk-Zugänge von außen sind für Lieferanten, Servicepartner und eigene Mitarbeiter erforderlich
- Der Mensch als Fehlerquelle: macht Konfigurationsfehler, steckt gefundene USB-Sticks in den Firmenrechner, öffnet kompromittierte E-Mail-Anhänge oder surft auf verseuchten Internetseiten.
- Externe Inbetriebnehmer oder Servicekräfte verbinden ihren Rechner mit dem Firmennetzwerk
- Unzufriedene Mitarbeiter wollen der Firma schaden

Ein vollständiger Schutz ist technisch nicht machbar. Daher gehören zu einer Security-Strategie auch Überlegungen, wie im Schadensfall zu reagieren ist. Das betrifft einerseits die Forensik, um Ursache und Schaden eines erfolgreichen Angriffs festzustellen – und andererseits die Festlegung der Maßnahmen, die zu einer schnellen Wiederherstellung des Betriebs notwendig sind.

INDUSTRIAL SECURITY IST EIN STÄNDIGER PROZESS

Industrial Security oder Cybersecurity ist kein einmaliges Projekt, dass man erledigt und abhakt – sondern ein kontinuierlicher Prozess, der entsprechend der ständig wechselnden Bedrohungslage fortlaufend überprüft und weiterentwickelt werden muss.

SAFETY ALS VORBILD

Ein Vergleich mit Safety bzw. der funktionalen Sicherheit zeigt, wie sich das Vorgehen in Sachen Industrial Security entwickeln wird. Heute ist Safety Standard und die Maschinenbauer und Automatisierer können damit umgehen. Eine Maschine ohne Risikoanalyse der Sicherheitstechnik zu entwickeln – oder dass die darin verbauten Sicherheitselemente keine entsprechende Zertifizierung haben – ist heutzutage gar nicht mehr vorstellbar. Vielmehr geben Standards und Normen vor, wie Sicherheitskomponenten entwickelt und angewendet werden müssen. Für die Sicherheit der Informationstechnik in der Industrie gibt es diese rechtlich verbindlichen Vorgaben zwar noch nicht, aber mit „Security-by-Design" sind die Methoden bekannt. Man muss sie jedoch anwenden. Eines der Schlüsselelemente hierbei ist, bereits im Entwicklungsprozess und beim Design der Automatisierungsanlage mögliche Bedrohungen zu berücksichtigen. *„Bei Safety kommt ja auch niemand auf die Idee, zuerst eine Maschine zu bauen, um sie in einem zweiten Schritt sicher zu machen",* bringt es Siegfried Müller, CEO von MB connect line, auf den Punkt.

AM ANFANG STEHT DIE RISIKOBETRACHTUNG

Eine Risikobetrachtung ist nur anhand einer konkreten Anwendung durchführbar. Sie ist daher auch bei jeder Anlage von Neuem erforderlich. Dazu werden die verschiedenen möglichen Angriffsvektoren innerhalb der Anlage betrachtet. Im Wesentlichen sind das interne und externe Schnittstellen. Nach außen ist das beispielsweise der Netzwerkanschluss. Das kann das Firmennetzwerk des Betreibers sein oder ein direkter Internetanschluss per LAN, WLAN oder Mobilfunk. Im Inneren ist das unter anderem ein USB-Anschluss an einem HMI-Gerät oder an einer SPS, ein Netzwerkanschluss innerhalb der Anlage oder eine andere mögliche steckbare Schnittstelle wie ein Profibusstecker. Alle diese Schnittstellen sind potentielle Einfallstore für Schadsoftware oder Angriffe. Abgesehen von den physischen Schnittstellen geht es auch um die Benutzerschnittstellen, wie beispielsweise ein Visualisierungssystem mit verschiedenen Zugangsebenen. Hier kann jemand Schwachstellen bei der Benutzeranmeldung ausnutzen.

> *„Das Risiko ist nicht nur der böse Hacker von außen. Auch eigene Mitarbeiter können aus Spieltrieb oder absichtlich dem Unternehmen schaden",*

berichtet Siegfried Müller aus seiner langjährigen Erfahrung. Nachdem alle möglichen Schnittstellen identifiziert sind, geht es darum, mögliche Schäden zu definieren. Das kann ein Schaden bei Fehlfunktionen sein, beispielsweise werden falsche Rezepturen für Lebensmittel gemixt, oder ein Ausfall und Stillstand der Anlage. Alle Schnittstellen und Risiken sollten entsprechend aufgelistet und jeweils eine Maßnahme geplant werden.

SICHERHEIT AUF MEHREREN EBENEN

Eingangs wurde erwähnt, dass sich umfassende Netzwerke nur schwer beherrschen lassen. Die Lösung dazu ist die Segmentierung der Netzwerke und die Bildung sicherer Zonen, indem der Datenaustausch zwischen den Netzwerksegmenten streng reglementiert wird. Das Konzept der Segmentierung basiert auf dem „Defense-in-depth"-Ansatz. Sinngemäß bedeutet das eine Verteidigung gegen Cyberangriffe über mehrere Linien. *„Wenn ein Angreifer die erste Hürde überwunden hat, soll er nur auf ein begrenztes Segment Zugriff haben und bald auf die nächste Hürde treffen"*, erläutert Siegfried Müller und ergänzt: *„Damit wird wirksam verhindert, dass sich eine Fehlfunktion oder eine Schadsoftware sofort über das gesamte Netzwerk ausbreitet"*. Die „Defense-in-depth"-Methode ist auch die Basis der im Moment entstehenden Norm IEC 62443.

Die Kommunikationszonen werden idealerweise dadurch gebildet, dass man Systeme oder Anlagenteile zusammenfasst, die funktional zusammengehören und kontinuierlich miteinander Daten austauschen. Netzwerkteilnehmer, die nur selten oder wenig Daten austauschen, werden mit Firewalls voneinander abgetrennt. Anhand einer sogenannten Whitelist wird in den Firewalls festgelegt, welche Kommunikationspartner bestimmte Daten austauschen und Dienste nutzen dürfen. Alles, was nicht explizit erlaubt ist, wird gesperrt.

Eine richtige und lückenlose Konfiguration einer IT-Firewall ist natürlich erforderlich und setzt IT-Erfahrung und Netzwerkkenntnisse beim Automatisierer voraus. Konfigurationsfehler führen hier häufig zu Sicherheitslücken.

FUNKTIONALITÄT UND VERFÜGBARKEIT STEHEN AN ERSTER STELLE

Im Gegensatz zur klassischen IT steht an einer Produktionsanlage die Verfügbarkeit über allem anderen. Das lässt sich mit einem einfachen Vergleich erklären: Die Steuerung eines Bearbeitungszentrums oder einer Abfüllanlage muss innerhalb von Millisekunden reagieren. Dagegen spielt es bei einem Büro-PC keine Rolle, wenn der Benutzer einmal fünf Sekunden auf einen Virenscanner wartet. Zudem sind in den Produktionsanlagen vielfältige Systeme wie beispielsweise Industrie-Steuerungen, Bedienpanels und Antriebe verbaut, die keine eigenen Sicherheitsmerkmale haben. Sie bieten einen offenen Zugriff auf Daten und Anwenderprogramme, ohne dass eine Authentifizierung erforderlich ist. Dazu kommt „never touch a running system“. Wenn sich beispielsweise ein XP-Rechner im Netzwerk befindet, dessen Software-SPS genau für ein bestimmtes Servicepack freigegeben ist, sind Updates aus funktionalen Gründen tabu. In der Norm IEC 62443 ist das Thema Absicherung von Altsystemen unter dem Begriff „Zones & Conduits“ zu finden. „Conduit“ bezeichnet den Zonenübergang zwischen zwei Sicherheitszonen.

Abschließend ein paar Grundsätze und allgemeine Maßnahmen, mit denen sich ein Mindestschutz erreichen lässt:

- Komplexe, sichere Passwörter statt „1234“ oder „Passwort“
- Standardpasswörter der Hersteller (Auslieferungszustand) ersetzen
- Geheime Passwörter statt Post-It am Rechner
- Verfügbare Patches und Updates sofort installieren
- Benutzern entsprechende Rollen zuweisen (Admin nur für Admins!)
- Netzwerke in logische Einheiten segmentieren
- 2-Faktor Authentifizierung verwenden

DIE SECURITY-KOMPETENZ VON MB CONNECT LINE

WIR STEHEN FÜR SICHERE VERBINDUNGEN

Wir als Hersteller von Hard- und Software für Fernwartungssysteme und Industrial IoT-Anwendungen verpflichten uns gegenüber unseren Kunden zur Entwicklung sicherer Produkte und Dienstleistungen. Wir garantieren eine zuverlässige und schnelle Reaktion auf bekannt werdende Sicherheitslücken. Dass uns das Thema Industrial Security besonders am Herzen liegt, zeigen auch unsere Verbandsarbeit und unsere Mitgliedschaften – beispielsweise beim Cluster Mechatronik & Automation Bayern e.V., beim TeleTrusT – Bundesverband IT-Sicherheit e.V. und in der European Cyber Security Organisation (ECSO). Um unseren Ansprüchen in diesem sehr sensiblen Bereich gerecht zu werden, arbeiten wir stetig daran, unseren Kunden und Anwendern „state of the art“-Sicherheitstechnologie anbieten zu können.

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

Allianz für Cyber-Sicherheit

Wir sind Mitglied im Bundesverband IT-Sicherheit e.V. (TeleTrusT). Unsere Produkte entsprechend den Richtlinien dieser Organisation, was uns erlaubt das „Security Made in Germany“ Label zu tragen. TeleTrusT ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst.

Weiterhin ist MB connect line Mitglied in der Allianz für Cybersicherheit und wir arbeiten aktiv mit dem Bundesamt für Sicherheit und Informationstechnik zusammen. Dies ermöglicht unseren Entwicklungsingenieuren schnellstmöglich, Sicherheitsbedrohungen nicht nur reaktiv, sondern vor allem präventiv entgegen zu wirken.

100% Sicherheit kann niemand garantieren. Aber man kann das Mögliche dafür tun. Keine ausnutzbaren Schwachstellen - so lautet das Ergebnis eines toolgeschützen und manuellen Penetrationstests von mbCONNECT24 - durchgeführt von dem IT-Sicherheitsdienstleister NIXU.

Durch Nutzung von Open Source Technologien steht MB connect line nicht nur für höchste Sicherheit bei der Nutzung des mbCONNECT24 Portals, sondern auch für Flexibilität bei der Integration externer Hardware. Unser Fernwartungssystem arbeitet mit X.509 Zertifikaten, OpenSSL und TLS-Verschlüsselung. Gehostet werden unsere Server in Hochsicherheits-Rechenzentren weltweit.

SECURITY BY DESIGN

Die Security-Betrachtung ist nicht nur für den Entwicklungsprozess eines Automatisierungsprojekts wichtig, sondern auch für die eingesetzten Produkte und Komponenten. Die MB connect line Lösungen werden streng nach dem Prinzip „Security by Design“ entwickelt. Basis sind für uns die in der IEC62443 festgelegten Normen.
„Zu Beginn haben wir den gesamten Entwicklungsprozess auf den Prüfstand gestellt“, so Siegfried Müller und erläutert weiter: *„Eine unserer Anforderungen war hierbei die Gewährleistung eines sicheren Boot-Prozesses des Betriebssystems, so dass es nicht möglich ist, eine manipulierte Firmware auf dem System einzuschleusen“*. Der sogenannte Secure-Boot Prozess stellt sicher, dass nur vom Hersteller signierte Firmware akzeptiert wird. Dafür sind unter Umständen auch Anpassungen des Hardware-Designs notwendig, welche nur am Anfang einer Entwicklung realisierbar sind.

SECURITY BY DEFAULT

Das heißt, dass bereits im Auslieferungszustand ein hohes Maß an Sicherheit besteht. Konkret bedeutet das, dass alle relevanten Sicherheitsmerkmale eines Systems aktiviert sind und der Anwender – je nach Anwendungsfall – bei Bedarf Sicherheitsfunktionen deaktivieren kann, sie jedoch in keinem Fall erst aktivieren muss. Bei MB connect line bedeutet das beispielsweise, dass wir auf einheitliche Standardpasswörter verzichten und stattdessen jedes System mit einem individuellen Passwort ausliefern – oder die Firewall zu Beginn alles sperrt und der Anwender einzelne Teilnehmer im Rahmen der konkreten Anwendung frei gibt.

INDUSTRIE-ROUTER

Die Industrie-Router mbNET und mbNET.rokey sind mit einem sicheren Hardware-Element (Kryptochip) und einem Secure Boot-Konzept ausgestattet, so dass Geräte nur mit signierter und vertrauenswürdiger Firmware booten können. Die Daten im Speicher sind verschlüsselt – und ohne den im Kryptochip gespeicherten Schlüssel nicht lesbar.

AUTOMATION FIREWALL

Auch bei der Entwicklung der Firewall mbNETFIX war das erste Ziel die Minimierung von Angriffsvektoren. Gerade bei Embedded Systemen wird zur Konfiguration oft eine Benutzer-Schnittstelle via Webserver implementiert. Diese Webserver-Implementierungen zeigen meist viele Verwundbarkeiten und sind eine potentielle Schwachstelle. Beim mbNETFIX wurde auf das Interface via Webserver verzichtet. Die Konfiguration erfolgt per eigener Software, welche dann mittels eines sicheren Protokolls (SSH) mit der Firewall kommuniziert. Per Default erfolgt die Kommunikation nur über den geschützten USB Port. An den Ethernet-Schnittstellen ist hier kein Konfigurationsdienst vorhanden und damit auch nicht angreifbar.

ZERTIFIZIERTER ENTWICKLUNGSPROZESS

Sichere Systeme und Geräte setzen einen sicheren Entwicklungsprozess voraus. Selbstverständlich sind die Entwicklungs-Ingenieure von MB connect line entsprechend zertifiziert. Dafür setzen wir auf ein TÜV Experten-Zertifizierungsprogramm im Bereich der sicheren Softwareentwicklung und auf Expertenwissen auf dem Gebiet der IT-Sicherheit (Teletrust T.P.S.S.E.). „

> *„IT-Sicherheit ist bei uns eine Management-Entscheidung und ganz klar die Basis für unseren zukünftigen Erfolg. Das Verständnis von IT und OT zusammen ist die Herausforderung, die wir gerne annehmen“,*

bringt es Siegfried Müller auf den Punkt.

© 2019 MB connect line GmbH. mbCONNECTLINE_DE_whitepaper_11_19