Security

PILZ
THE SPIRIT OF SAFETY

Whitepaper

Haftungsausschluss

Wir haben unser Whitepaper sehr sorgfältig zusammengestellt. Es enthält Informationen über unser Unternehmen sowie über unsere Produkte. Alle Angaben haben wir nach dem heutigen Stand der Technik und bestem Wissen und Gewissen gemacht. Dennoch können wir für die Richtigkeit und Vollständigkeit der Angaben, sofern uns nicht der Vorwurf grober Fahrlässigkeit trifft, keine Haftung übernehmen, da sich trotz aller Sorgfalt Fehler nicht vollständig vermeiden lassen. Insbesondere haben die Angaben nicht die rechtliche Qualität von Zusicherungen oder zugesicherten Eigenschaften. Für Hinweise auf Unstimmigkeiten sind wir dankbar.

Urheberrecht

Alle Rechte an dieser Publikation sind der Pilz GmbH & Co. KG vorbehalten. Technische Änderungen behalten wir uns vor. Kopien für den innerbetrieblichen Bedarf des Benutzers dürfen angefertigt werden. Die verwendeten Produkt-, Waren- und Technologiebezeichnungen sind Warenzeichen der jeweiligen Firmen.

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Deutschland

© 2018 by Pilz GmbH & Co. KG, Ostfildern,
1. Auflage

Auf einen Blick

Durch die Digitalisierung der Fabrik werden Anlagen zunehmend vernetzt. Damit steigt auch das Risiko, dass wichtige Daten ausspioniert oder manipuliert werden. Früher wurde in der Automatisierung vorwiegend über Feldbusse wie CAN und proprietäre, das heißt herstellerspezifische Protokolle kommuniziert. Um Schaden anzurichten, musste ein Angreifer schon in die Werkshalle gelangen oder via Telefonleitung mit einem Modem auf eine Maschine zugreifen. Da diese Protokolle mittlerweile zunehmend durch Ethernet und IP-Protokolle ersetzt werden, lassen sich Angriffe jetzt jedoch auch über das Internet durchführen.
Die Motive reichen von terroristischen Absichten über Industriespionage und Sabotage von Anlagen bis hin zur Erpressung von Geldzahlungen. Erleichtert wird das Geschäft der Angreifer dadurch, dass in der Automatisierung immer häufiger Open Source-Software und Softwarekomponenten aus dem Consumer-Bereich eingesetzt werden, die möglicherweise Schwachpunkte haben, die den Angreifern bekannt sind. Auch deshalb bekommt Security, also die Datensicherheit, einen immer höheren Stellenwert.
Die Erfahrung zeigt jedoch, dass diese Botschaft noch längst nicht von allen richtig verstanden worden ist. Deshalb werden in diesem Whitepaper die zentralen Aspekte von Security erläutert und Lösungsansätze vorgestellt, die sich in der Praxis bewährt haben. Dadurch können beispielsweise Maschinenbauer, Anlagenplaner, Installateure und Instandhalter erkennen, welche Rolle ihre Produkte bzw. Dienstleistungen für die Security-Strategien ihrer Kunden spielen und worauf sie achten müssen. Zudem wird auch der Aspekt der funktionalen Sicherheit (Safety) einbezogen. Denn Security und Safety sind zwei Seiten derselben Medaille, sprich sicherer Fertigungsprozesse.

Inhalt

1. Security und Safety 5
1.1. Definition 5
1.2. Wechselwirkungen 5

2. Bedeutung von Security in der Automatisierung 6
2.1. Zielsetzung 6
2.2. Mehr als IT- Sicherheit 6
2.3. Auswirkungen auf den Lebenszyklus von Anlagen 7

3. Formen der Bedrohung 7
3.1. Externe Angriffe 7
3.2. Interne Angriffe 8
3.3. Unbeabsichtigte Security-Verletzungen 8

4. Beurteilung von Security 9
4.1. Normative Grundlagen 9
4.2. Risikoanalyse 10
4.3. Gegenmaßnahmen 11

5. Umsetzung von Security-Strategien 12
5.1. Firewalls 12
5.2. Segmentierung des Netzwerks 12
5.3. Defense-in-Depth 14
5.4. Organisatorische Maßnahmen 14
5.5. Schulungen 15

6. Zusammenfassung und Ausblick 15

Glossar 17

Abbildungsverzeichnis 19

1. Security und Safety

1.1. Definition

Früher war Security fast ausschließlich ein Thema der klassischen Informationstechnologie (IT). Heute wachsen die IT- und die Automatisierungswelt jedoch immer enger zusammen. Dadurch nimmt der Grad der Vernetzung von Fertigungsanlagen und der Einsatz von Standard-Protokollen wie Ethernet für die physikalische Übertragung der Daten deutlich zu. Außerdem erlauben standardisierte Protokolle wie OPC UA, dass über IT-Systeme auf Steuerungen zugegriffen werden kann, wodurch die Datenkommunikation noch offener wird.
In der Automatisierung bedeutet der Begriff Security vor allem Schutz von Maschinen und Anlagen vor unbefugten Zugriffen von außen sowie den Schutz sensibler Daten vor Verfälschung, Verlust und unbefugtem Zugriff im Innenverhältnis. Die Bedrohungen kommen aus der Cyberwelt, zu der das Internet wie auch die gesamte moderne Informations- und Kommunikationstechnologie gehören. Das beginnt bei der Zutrittskontrolle am Werkstor und reicht bis zur Abwehr von Angriffen durch Hacker. Allerdings, so der deutsche IT-Sicherheitsexperte Ralph Langner, sind es nicht immer die „Bösen“, die Schaden anrichten. Denn viele Security-Verletzungen passieren ohne Absicht, etwa durch Bedienfehler von Kollegen und Mitarbeitern.
Der Begriff Safety bezeichnet die funktionale Sicherheit von Anlagen, also den Schutz von Mensch und Umwelt gegen vorhersehbare Bedrohungen, die von Maschinen ausgehen können. Hierzu dürfen Restrisiken, die mehr oder weniger immer vorhanden sind, vertretbare Werte nicht übersteigen. Um das zu gewährleisten, werden u. a. Komponenten wie Sicherheitsrelais und Schutzschalter eingesetzt, die dafür sorgen, dass bei einem Problem die Maschine in einen sicheren Zustand gebracht wird, von dem keine Gefahr für Mensch, Maschine und Umwelt ausgeht.
Nachdem die funktionale Sicherheit einer Maschine nach den Vorgaben der Maschinenrichtlinie abgenommen worden war, mussten sich Anlagenbetreiber über Safety keine Gedanken mehr machen, solange an der Maschine danach keine wesentlichen Änderungen mehr vorgenommen wurden. Diese Zeiten sind jedoch vorbei. Denn durch die Bedrohungen aus der Cyberwelt wird Security zu einem unverzichtbaren Element für Safety.

1.2. Wechselwirkungen

Weil Fertigungsprozesse durch Safety-Funktionen unterbrochen werden können, wird häufig versucht, diese – rechtswidrig – zu umgehen, was bisher vor allem durch mechanische Maßnahmen verhindert wurde. Ein Beispiel dafür sind verplombte Schrauben, die verhindern, dass sich Schutzschalter einfach entfernen lassen. Heute ist es jedoch möglich, solche Manipulationen über das Netzwerk vorzunehmen. Wenn etwa eine Maschine wegen eines Lichtgitters in einen sicheren Zustand geht, lässt sich dessen Programm so verändern, dass die entsprechenden Daten nicht mehr ausgewertet werden. Dadurch ist die Schutzfunktion deaktiviert, und die Maschine läuft auch in Gefahrensituationen einfach weiter.
Anderseits könnten Safety-Mechanismen auch benutzt werden, um Maschinen über das Netzwerk gezielt lahmzulegen. Hierzu muss lediglich die Datenkommunikation unterbrochen werden. Denn die Safety-Mechanismen prüfen zyklisch, ob der Netzteilnehmer auf der anderen Seite der Verbindung noch aktiv ist. Sobald keine Antwort erfolgt, stoppt die Maschine. Eine Möglichkeit, dies zu bewerkstelligen, sind die bereits erwähnten DoS-Attacken, die eine Überlast im Netzwerk erzeugen.

Über das Netzwerk lassen sich jedoch nicht nur Fertigungsprozesse beeinträchtigen, sondern es können auch noch andere Gefahren drohen. Einen Ansatzpunkt für Angreifer bieten Safety-Mechanismen, die kontrollieren, ob der Antrieb einer Maschine an- oder abgeschaltet wird. Wenn diese Mechanismen so verändert werden, dass der Antrieb ständig läuft, kann dies dazu führen, dass eine Maschine im schlimmsten Fall zerstört wird. Deshalb werden kostenintensive Investitionsgüter wie etwa Windkraftanalgen häufig doppelt und dreifach geschützt.

2. Bedeutung von Security in der Automatisierung

2.1. Zielsetzung

Durch Ansätze wie Industrie 4.0, bei denen die Vernetzung von zentraler Bedeutung ist, stellen Bedrohungen aus der Cyberwelt ein ernsthaftes Problem für produzierende Unternehmen dar. Zwar lassen sich grundsätzlich alle IT-basierten Prozesse schützen, aber das ist aufwändig und teuer. Deshalb sollte zunächst untersucht werden, welche Risiken tatsächlich bestehen. Denn eine Security-Strategie muss letztlich immer die Kosten und den Nutzen für die Produktivität eines Unternehmens gegeneinander abwägen.
Security zielt darauf ab, die Verfügbarkeit des Netzwerks und der Geräte sowie die Integrität und Vertraulichkeit der Daten zu gewährleisten. Hierzu müssen beispielsweise verteilte Steuerungssysteme sowohl vor Angriffen wie etwa DoS-Attacken als auch vor Software-, Geräte- und Bedienfehlern geschützt werden. Eine andere Möglichkeit, Fertigungsprozesse zu unterbrechen, besteht darin, die Übertragung oder Speicherung von Daten zu manipulieren, weshalb deren Integrität eine wichtige Rolle spielt. Und auch eine Verletzung der Datenvertraulichkeit kann schwerwiegende Folgen haben, etwa wenn das Anwendungsprogramm einer Maschine ausspioniert wird und diese dann nachgebaut werden kann.

2.2. Mehr als IT- Sicherheit

Um unterschiedlichen Bedrohungsszenarien flexibel begegnen zu können, werden heute Security-Strategien umgesetzt, die aus mehrere Schutzschichten bestehen: Im Kern befinden sich die Automatisierungskomponenten. Dann folgt das Netzwerk, über das diese Komponenten mit anderen oder etwa einem ERP-System (Enterprise Ressource Planning) kommunizieren können. Die oberste Schicht bildet die Fabrik, die durch ein Firewall-Konzept nach außen abgeschirmt wird.
Solche Konzepte reichen jedoch nicht aus, um Anlagen rundum zu schützen. Denn Bedrohungen können wie erwähnt ebenso von innen ausgehen. Daher bildet der physische Schutz gegen einen unberechtigten Zugriff auf Netzwerkgeräte wie Firewalls und Switche die Grundlage jeder Security-Strategie. Nur wenn diese Geräte nicht frei zugänglich sind, lässt sich verhindern, dass sie vor Ort manipuliert werden können. Eine einfache, aber wirkungsvolle Maßnahme kann etwa darin bestehen, die Netzwerkgeräte in abschließbaren Schaltschränken oder Verteilerkästen zu installieren. Zugleich lässt sich dadurch auch das Risiko von Bedienfehlern durch nicht befugtes Personal deutlich reduzieren.

2.3. Auswirkungen auf den Lebenszyklus von Anlagen

Anlagen können einen Lebenszyklus von 20 Jahren und mehr haben. Bisher wurden sie in aller Regel nach dem Grundsatz „Never change a running system“ betrieben. Das heißt, wenn ein Safety-Mechanismus aktualisiert werden musste, wurde normalerweise die Steuerung gegen ein neues Modell des gleichen Typs ausgetauscht. Denn die funktionale Sicherheit ist solange gewährleistet, solange an der Maschine keine wesentlichen Änderungen vorgenommen werden. Sie beruht auf statistischen Fehlermodellen, die angeben, wie wahrscheinlich es ist, dass ein Schadensereignis eintritt. Und daran ändert sich über die Zeit so gut wie nichts.
Security ist dagegen ein „Moving Target“. Hier geht es nicht wie bei Safety darum, dass ein Fehler beispielsweise mit einer Wahrscheinlichkeit von 1:100.000 auftritt, sondern das Verhältnis kann auch 1:1 sein, wenn ein Angreifer erst einmal in ein Netzwerk eingedrungen ist. Außerdem werden immer ausgeklügeltere Methoden entwickelt, um Abwehrmaßnahmen zu überwinden, und bisher sichere Algorithmen erweisen sich plötzlich als unsicher. So war bis vor einigen Jahren der Data Encryption Standard (DES) ein gängiges Verfahren. Heute empfiehlt das BSI (Bundesamt für Sicherheit in der Informationstechnik), es nicht mehr einzusetzen. Gleiches gilt etwa für den Hashing-Algorithmus MD5. Und mit Quantencomputern wird es in nicht allzu ferner Zeit möglich sein, kryptografische Schlüssel in wenigen Minuten oder gar Sekunden zu errechnen, was mit heutigen Computern noch eine Ewigkeit dauern würde.
Weil Security keine physikalische Größe ist, sondern ein „Moving Target“, müssen die Maßnahmen gegen Cyberbedrohungen ständig aktualisiert werden. Die Verantwortung dafür liegt in erster Linie bei den Anlagenbetreibern, für die Datensicherheit zugleich Investitionsschutz bedeutet. Denn durch eine effektive Security-Strategie können sie ihre Anlagen ebenso lange wie bisher nutzen. Umgekehrt sind Maschinenbauer und Komponentenhersteller in der Pflicht, die Betreiber sofort über neue Sicherheitsprobleme zu informieren und Updates für die Software ihrer Geräte bereitzustellen, mit denen Schwachstellen behoben werden können. Das erfordert jedoch, dass beide Seiten über den gesamten Lebenszyklus der Produkte hinweg eng zusammenarbeiten.

3. Formen der Bedrohung

3.1. Externe Angriffe

Ethernet-basierte Automatisierungsnetzwerke sind vielfältigen Bedrohungsszenarien ausgesetzt, die sich jedoch anhand des Ausgangspunkts kategorisieren lassen. Denn im Grunde gibt es nur externe und interne Angriffe sowie unbeabsichtigte Security-Verletzungen, wobei die Motive variieren.
Wenn Netzwerke von außen angegriffen werden, geschieht dies in aller Regel in böswilliger Absicht. Dazu gehört etwa die Sabotage von Anlagen. Welche Folgen das haben kann, verdeutlicht ein Beispiel, das zwar veröffentlicht wurde, aber ohne „Ross und Reiter“ zu nennen: Nach einem erfolgreichen Angriff auf einen Hochofen in Deutschland musste dieser am Ende abgerissen werden, weil die Schmelze hart geworden war.
Ein anderes Bedrohungsszenario, das negative Auswirkungen haben kann, ist die Industriespionage. Wenn etwa Informationen zu Produkten oder Fertigungs-Know-how ausgespäht werden, ist möglicherweise die Wettbewerbsfähigkeit eines Unternehmens

gefährdet. Das gilt ebenso, wenn vertrauliche Finanzdaten oder Informationen über Kunden, Ausschreibungen und Aufträge entwendet werden.
Um an Passwörter und Zugangsdaten zu gelangen, setzen Angreifer teilweise perfekt gefälschte Internetseiten und E-Mails ein, sogenanntes Phishing. Wenn die Empfänger nicht auf der Hut sind, haben die Angreifer leichtes Spiel. Deshalb ist es wichtig, dass Unternehmen ihre Mitarbeiter für das Thema Security sensibilisieren und Richtlinien aufstellen, die für alle verbindlich sind.
Schließlich gibt es in jüngster Zeit immer häufiger Angriffe, die schlicht in krimineller Absicht durchgeführt werden. Das Mittel der Wahl ist derzeit sogenannte Ransomware, die etwa in Word-, PowerPoint- oder Excel-Dateien versteckt sein kann, die via E-Mail verschickt wird. Wenn ein Empfänger sie öffnet, werden alle Dateien auf seinem Rechner verschlüsselt. Außerdem kann sich die Malware auf weitere Geräte im Netzwerk ausbreiten. Die einzige Möglichkeit, um wieder an die Daten heranzukommen, besteht in der Zahlung eines Lösegelds.

3.2. Interne Angriffe

Obwohl Angriffe von außen immer wieder Schlagzeilen machen, sind Angriffe von innen ebenso gefährlich. Denn so können Security-Strategien im wahrsten Sinne des Wortes umgangen werden. Die Absichten der Angreifer sind mehr oder weniger die gleichen wie bei den Angriffen von außen, nur die Vorgehensweise unterscheidet sich.
Die eine Möglichkeit besteht darin, dass Angreifer in das Unternehmen hineingelangen und dort etwa einen freien Ethernet-Anschluss suchen, um Malware in das Netzwerk einzuschleusen. Hierzu reicht ein kleiner USB-Stick aus, der bei der Kontrolle am Werkstor nicht auffällt.
Weitaus häufiger dürften Angreifer jedoch den Umstand ausnutzen, dass auch bei Security der Mensch das schwächste Glied in der Kette ist. Eine wirksame Methode um Personal zu manipulieren, ist beispielsweise das sogenannte Social-Engineering.
Hierbei geht es darum, sich das Vertrauen von Mitarbeitern zu erschleichen und diese sozusagen als williges Werkzeug zu benutzen. Das A und O dafür ist eine gründliche Recherche im Vorfeld, etwa auf Unternehmensseiten im Internet, wo häufig Namen und Funktionsbezeichnungen von Angestellten zu finden sind. Mitunter reicht es dann schon aus, wenn ein Angreifer einem Mitarbeiter gegenüber erwähnt, er habe mit Kollege X gesprochen und der habe gesagt, er solle sich an ihn wenden, um als betriebszugehörig durchzugehen.

3.3. Unbeabsichtigte Security-Verletzungen

Die weitaus meisten Cybervorfälle resultieren jedoch weder aus externen noch internen Angriffen, sondern geschehen unbeabsichtigt. Die Folgen können ebenso schwerwiegend sein wie bei den beiden anderen Bedrohungsszenarien, also etwa zum Ausfall von Netzwerken oder zur Verbreitung sensibler Informationen führen. Gründe sind vor allem falsch konfigurierte Geräte und Bedienfehler.
Deshalb müssen die Mitarbeiter in der Fertigung, die normalerweise keine IT-Experten sind, entsprechend geschult werden. Darüber hinaus lassen sich Netzwerke auch so umsetzen, dass die Auswirkungen, die von falsch konfigurierten oder falsch bedienten Geräten ausgehen können, durch eine Segmentierung, also eine Aufteilung in Subnetze, und den Einsatz unterschiedlicher Security-Mechanismen begrenzt werden.

4. Beurteilung von Security

4.1. Normative Grundlagen

Security spielt in der klassischen IT schon seit langem eine zentrale Rolle, weshalb es eine Reihe von Normen gibt wie etwa die Reihe der „ISO/IEC 27000 „Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016); German version EN ISO/IEC 27000:2017“. Die Anforderungen lassen sich jedoch nicht ohne Weiteres auf die Automatisierung übertragen. Denn dort steht die Verfügbarkeit der Daten an erster Stelle, was eine wesentliche Voraussetzung für reibungslose Fertigungsprozesse ist, während in der IT die Vertraulichkeit der Daten oberste Priorität hat.
Um effektive Security-Lösungen für die Automatisierung zu ermöglichen, haben verschiedene Organisationen begonnen, entsprechende Normen zu erarbeiten. Darin werden jedoch nur Teilaspekte wie etwa die Abgrenzung von Security und Safety beschrieben. Außerdem liegen sie weder als Entwurf noch als offizielle Norm vor, sind also eher technische Referenzen.
Mit der IEC 62443 „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“ gibt es dagegen eine internationale Normenreihe, die in Teilen schon verabschiedet wurde und die IT-Sicherheit in der Automatisierung umfassend behandelt. Das Themenspektrum reicht von

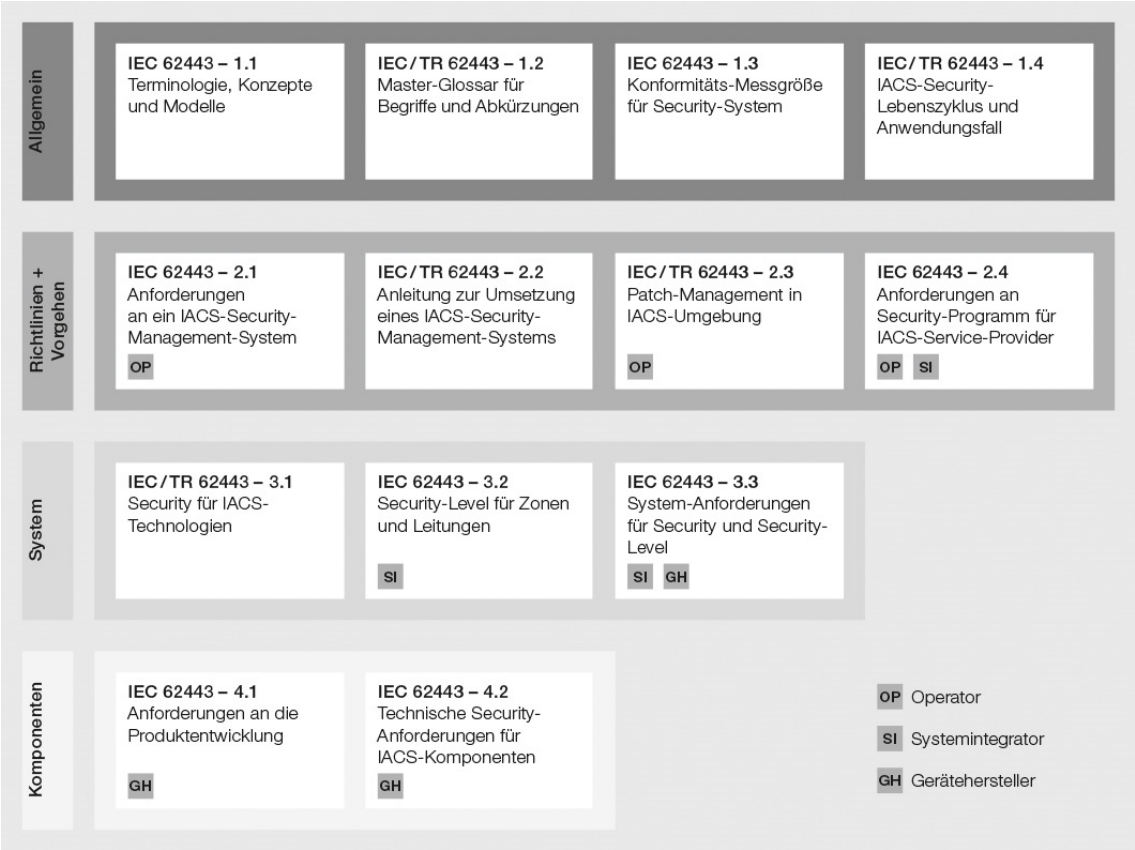


Abbildung 1: Norm IEC 62443

der Risikoanalyse über Best Practices (bewährte Verfahren) bis hin zur sicheren Entwicklung von Produkten (Security by Design). Dadurch bietet die IEC 62443 die derzeit beste Orientierungshilfe für Anlagenbetreiber und Gerätehersteller, um Security effektiv umzusetzen.

Das „ICS Security Kompendium“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) wendet sich insbesondere an die Betreiber industrieller Steuerungssysteme. Erläutert werden sowohl allgemeine Grundlagen als auch besondere Anforderungen und relevante Standards. Außerdem werden geeignete Maßnahmen vorgestellt und Wege aufgezeigt, wie sie durchgeführt werden können.
Während die IEC 62443 und das „ICS Security Kompendium“ eher etwas für Experten sind, ermöglicht die VDI-Richtlinie VDI/VDE 2182 einen vergleichsweise einfachen Einstieg in die Thematik. Außerdem haben auch verschiedene Unternehmen aus der Automatisierungsbranche Schriften herausgegeben, die mitunter jedoch den Umfang eines Buchs haben. Aufgrund der Komplexität der industriellen Security ist es sicherlich ratsam – spätestens wenn es an die Umsetzung geht – externe Spezialisten hinzuzuziehen.

4.2. Risikoanalyse

Eine Security-Strategie beginnt ebenso wie jede anderen Strategie mit einer Bestandsaufnahme, oder anders formuliert: Die Anlagenbetreiber müssen sich zunächst ein

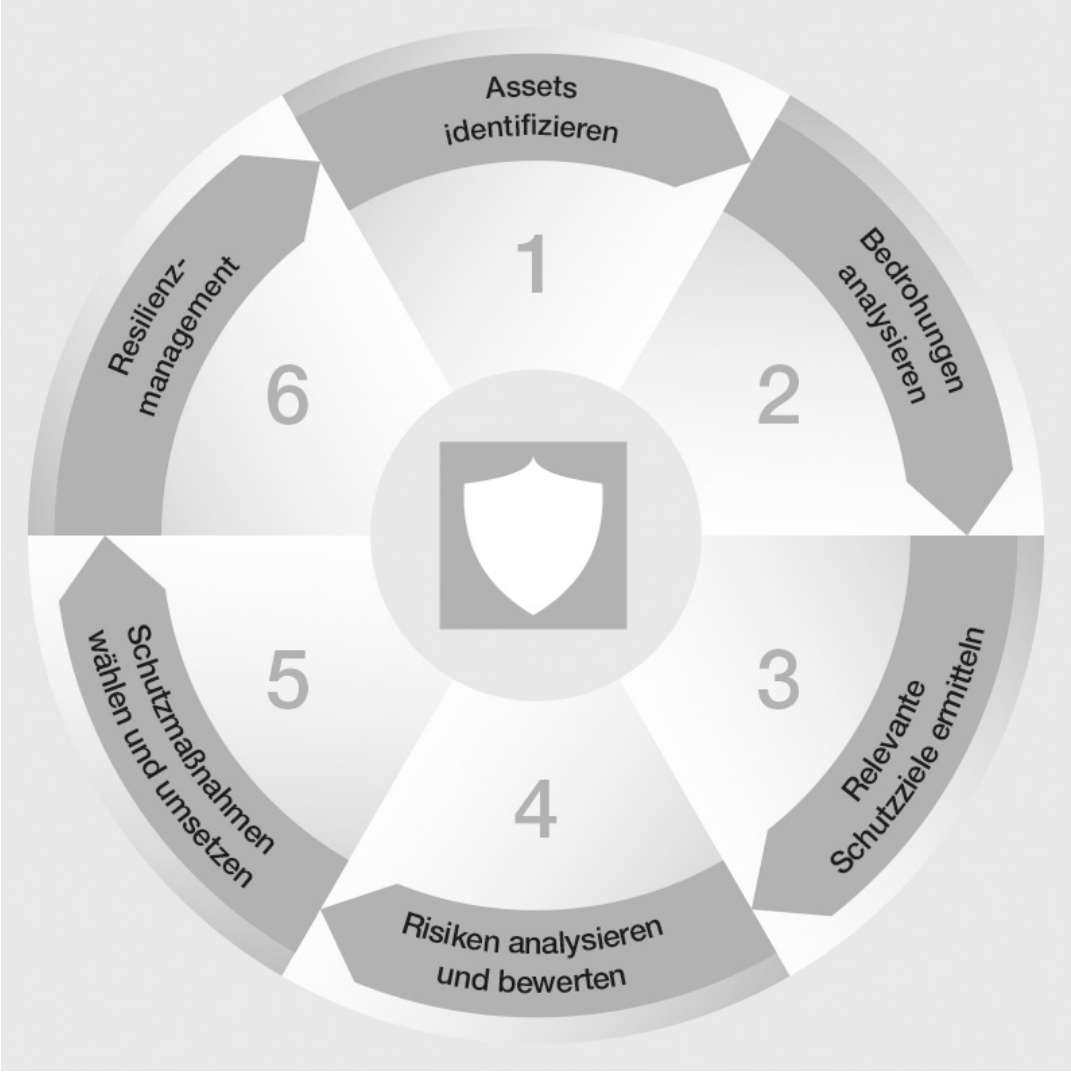
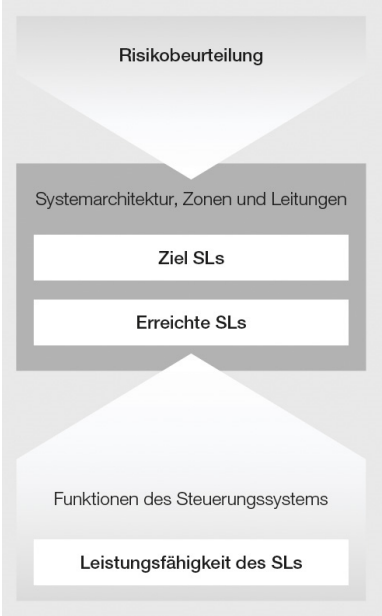


Abbildung 2: Projektschritte der Risikoanalyse

Bild davon machen, welchen Bedrohungen sie ausgesetzt sind und welche Unternehmenswerte sie vorrangig schützen wollen. Im zweiten Schritt lassen sich dann gemäß IEC 62443 fünf Security Level definieren, die von 0 (nicht gefährdet) bis5 (extrem gefährdet) reichen, und für die jeweils unterschiedlichen Anforderungen gelten. Wie diese konkret erfüllt werden können, wird jedoch nicht gesagt.



Security Level	Schutz
SL 0	Kein Schutz
SL 1	Schutz gegen einfachen oder zufälligen Missbrauch
SL 2	Schutz gegen absichtlichen Missbrauch mit einfachen Mitteln
SL 3	Schutz gegen absichtlichen Missbrauch mit fortgeschrittenen Mitteln
SL 4	Schutz gegen absichtlichen Missbrauch mit fortgeschrittenen Mitteln und umfangreichen Ressourcen

SL = Security Level

Abbildung 3: Risikobeurteilung mit Hilfe der Security Level

Als Faustformel gilt, dass grundsätzlich alle Geräte, die einen Ethernet-Anschluss haben, gefährdet sind. Denn sie können sozusagen als Einfallstor für Angriffe von außen und innen dienen oder der Ausgangspunkt unbeabsichtigter Security-Verletzungen sein. Wenn auf diesen Geräten zudem gängige Betriebssysteme installiert sind, nimmt das Risiko zu. Vor allem dann, wenn für diese keine Sicherheits-Updates mehr angeboten werden. Um herauszufinden, wie sich solche Systeme erfolgreich angreifen lassen und welche Malware es hierfür gibt, genügt häufig eine Recherche in Suchmaschinen.
Eine Risikoanalyse ist jedoch stets nur eine Momentaufnahme. Denn jederzeit können neue Bedrohungen entstehen, die einbezogen werden müssen. Galten etwa Prozessoren bisher als unkritisch, wurden dort jüngst Sicherheitslücken entdeckt, die unter den Namen „Meltdown“ und „Spectre“ zusammengefasst werden und viele PCs angreifbar machen. Dadurch geraten u. a. auch Soft-SPSen (Software-basierte speicherprogrammierbare Steuerungen) in das Visier von Angreifern. Kurzum: Security ist ein permanenter Prozess, der einen langen Atem erfordert.

4.3. Gegenmaßnahmen

Nachdem die zu schützenden Unternehmenswerte identifiziert und priorisiert worden sind – ein erfolgreicher Angriff auf eine Steuerung hat normalerweise schwerwiegendere Folgen als der auf ein Visualisierungstool –, muss entschieden werden, wie den Bedrohungen begegnet werden soll.
Der Königsweg besteht darin, Angriffe und unbeabsichtigte Security-Verletzungen von vornherein zu verhindern. Aufgrund der Komplexität und Dynamik der Materie lässt sich das jedoch nicht immer bewerkstelligen. Denn selbst wenn Spezialisten beauftragt werden, ständig

nach möglichen Schwachstellen im Netzwerk zu suchen, gibt es letztlich keine Rundumversicherung gegen alle Eventualitäten.
Deshalb kommt es darauf an, Security-Probleme sofort zu erkennen und unverzüglich zu handeln. Hierzu können u. a. alle Ereignisse im Netzwerk protokolliert (Event Logging) und dann ausgewertet werden. So lässt sich etwa feststellen, wann auf ein bestimmtes Gerät zugegriffen wurde. Wenn beispielsweise Wartungsarbeiten zu einer Zeit stattgefunden haben, in der das sonst nie geschieht, sollten alle Alarmglocken läuten.
Wenn ein Angriff erfolgreich war oder die Datensicherheit schon unbeabsichtigt verletzt wurde, muss das Problem so schnell es geht behoben und die Ursache gründlich analysiert werden, damit es künftig nicht erneut auftreten kann.

5. Umsetzung von Security-Strategien

5.1. Firewalls

Eine Maßnahme, um Security-Strategien umzusetzen, ist der Schutz des Netzwerks durch spezielle Geräte. Obwohl auch Router und Switche Sicherheitsmechanismen unterstützen können, spielen Firewalls nach wie vor eine zentrale Rolle. Dabei handelt es sich entweder um Softwarelösungen oder Appliances (Kombination aus Hard- und Software), die anhand individuell definierter Regeln und mit Funktionen wie Deep Packet Inspection oder Intrusion Detection den gesamten Datenverkehr überwachen.
Weil Firewalls normalerweise aufwändig konfiguriert werden müssen, sind umfassende IT-Kenntnisse erforderlich, die im Fertigungsbereich häufig fehlen. Deshalb hat Pilz mit der SecurityBridge eine industriegerechte Firewall entwickelt, die sich durch anwendungsspezifische Voreinstellungen nach dem Plug-and-play-Prinzip leicht in Betrieb nehmen lässt. Mit ihr können nicht nur Steuerungssysteme von Pilz vor Angriffen und unberechtigten Zugriffen geschützt, sondern auch Prozessdaten mit geringer Latenz übertragen werden.
Die effektivsten Security-Geräte nützen jedoch nur wenig, wenn sie nicht von Grund auf sicher entwickelt wurden und dieser Aspekt auch über den gesamten Lebenszyklus beachtet wird – Stichwort Secure by Design. Denn Prozessoren können, wie das Beispiel Meltdown und Spectre zeigt, auf einmal nicht mehr sicher sein. Außerdem ist es durchaus möglich, dass Malware in einen Fertigungsprozess eingeschleust und dann in den Produkten installiert wird, um später als Hintertür für Angriffe zu dienen. Um solchen Szenarien einen Riegel vorzuschieben, müssen die Hersteller die Cyberwelt ständig nach neuen Bedrohungen durchsuchen und – falls erforderlich – so schnell wie möglich zusätzliche Sicherheitsmechanismen in ihre Geräte integrieren und Patches (Sicherheits-Updates) zur Verfügung stellen.

5.2. Segmentierung des Netzwerks

Firewalls werden klassischerweise am Übergang von einem sicheren in ein unsicheres Netzwerk platziert, also etwa zwischen einem Intranet und dem Internet. Dieser sogenannte Perimeter-Schutz stößt jedoch schnell an Grenzen, wenn es darum geht zu verhindern, dass sich Malware wie eine Epidemie über das gesamte Netzwerk ausbreitet und dieses ebenso wie die angebundenen Anlagen lahmlegt.

Deshalb sieht die Norm IEC 62443 vor, Netzwerke nach dem „Zones and Conduits“-Modell zu unterteilen.

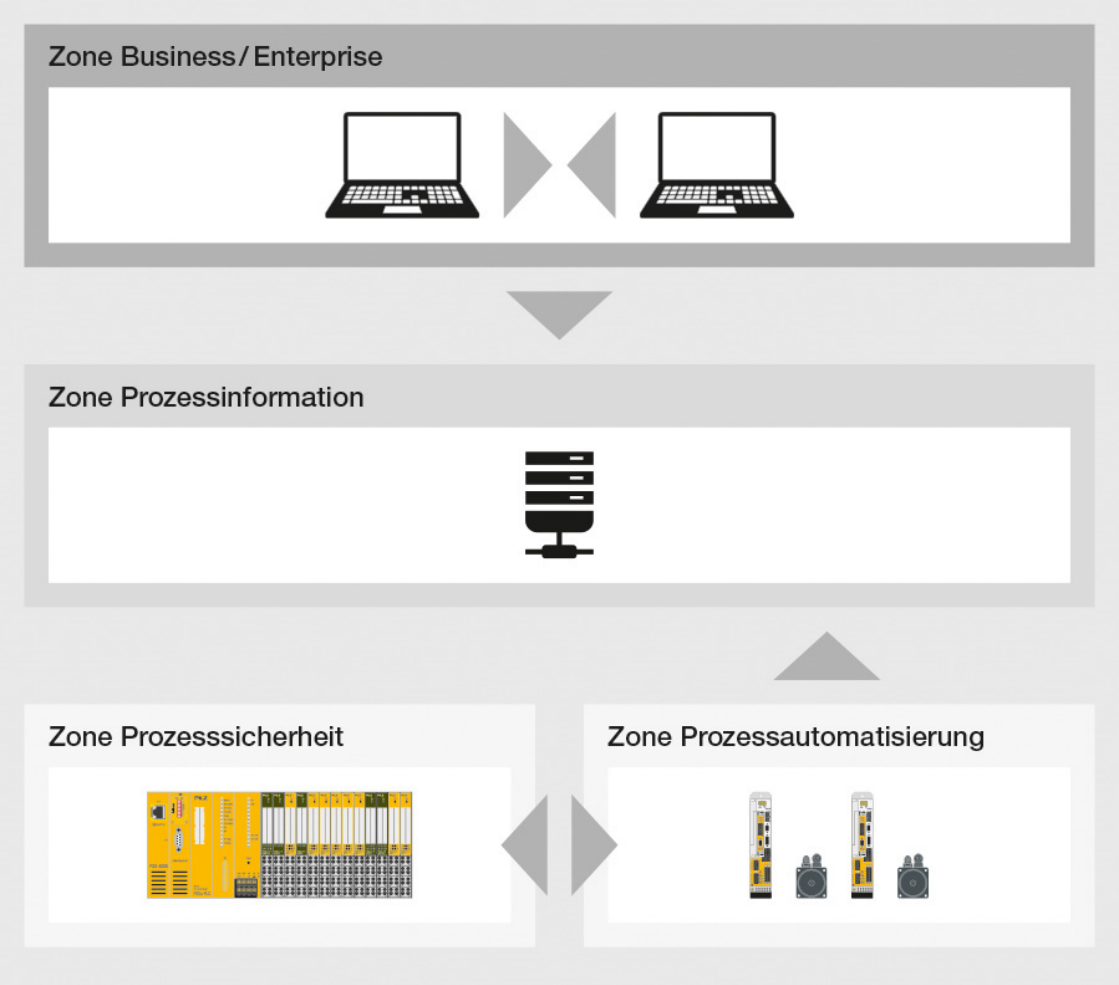


Abbildung 4: "Zones and Conduits"-Modell

Dadurch lassen sich beispielsweise das Verwaltungs- und das Produktionsnetzwerk trennen. Falls erforderlich, kann auch dieses Netzwerk segmentiert werden, und zwar bis hin zu einzelnen Fertigungszellen. Hierzu werden zunächst Zonen identifiziert, in denen Geräte ähnliche Security-Anforderungen haben, und anschließend durch Firewalls oder sichere Router gegeneinander abgeschottet. So lässt sich sicherstellen, dass über die Leitungen (Conduits) zwischen den Zonen nur die Geräte senden und empfangen können, die dazu berechtigt sind. Was das in der Praxis heißt, verdeutlicht das folgende Beispiel: Unbeabsichtigte Security-Verletzungen werden häufig durch falsch konfigurierte Geräte verursacht. Die Folgen sind etwa eine Übertragung von Daten oder sogenannte Broadcast-Stürme, die wiederum andere Geräte beeinträchtigen können. Wenn Netzwerke dagegen in geschützte Subnetze segmentiert werden, sind nur die Geräte innerhalb der Zone betroffen, in der das Problem aufgetreten ist. Das gilt ebenso für die Auswirkungen von versehentlichen oder böswilligen internen Zugriffen.

5.3. Defense-in-Depth

Um Angreifern das Handwerk so schwer wie möglich zu machen, kann das „Zones and Conduits“-Modell auch als zentrales Element für eine tief gestaffelte Verteidigung (Defense-in-Depth) des Netzwerks dienen. Dieses Prinzip, das beim Bau von Befestigungsanlagen angewendet wird, beruht darauf, Eindringlingen immer neue und andere Hindernisse in den Weg zu legen. So konnten im Mittelalter Burgen etwa durch einen Wassergraben, Fallgruben, Zugbrücken, Türme und mehrere Mauern geschützt sein.
Die Zonen und Leitungen eines Netzwerks entsprechen den Toren einer Burg. Die Mauern und die anderen Hindernisse werden von den Firewalls und sicheren Routern gebildet, die unterschiedliche Security-Mechanismen unterstützen. Zu ihnen gehören beispielsweise eine Zugriffskontrolle gemäß IEEE 802.1x und Access Control Lists, die unbekannte Geräte und Protokolle blockieren. Außerdem gibt es Mechanismen, die bei verdächtigen Netzwerkaktivitäten Alarme auslösen oder erkennen, wenn IP-Pakete mit gefälschten Absender-Adressen verschickt werden (IP-Spoofing).

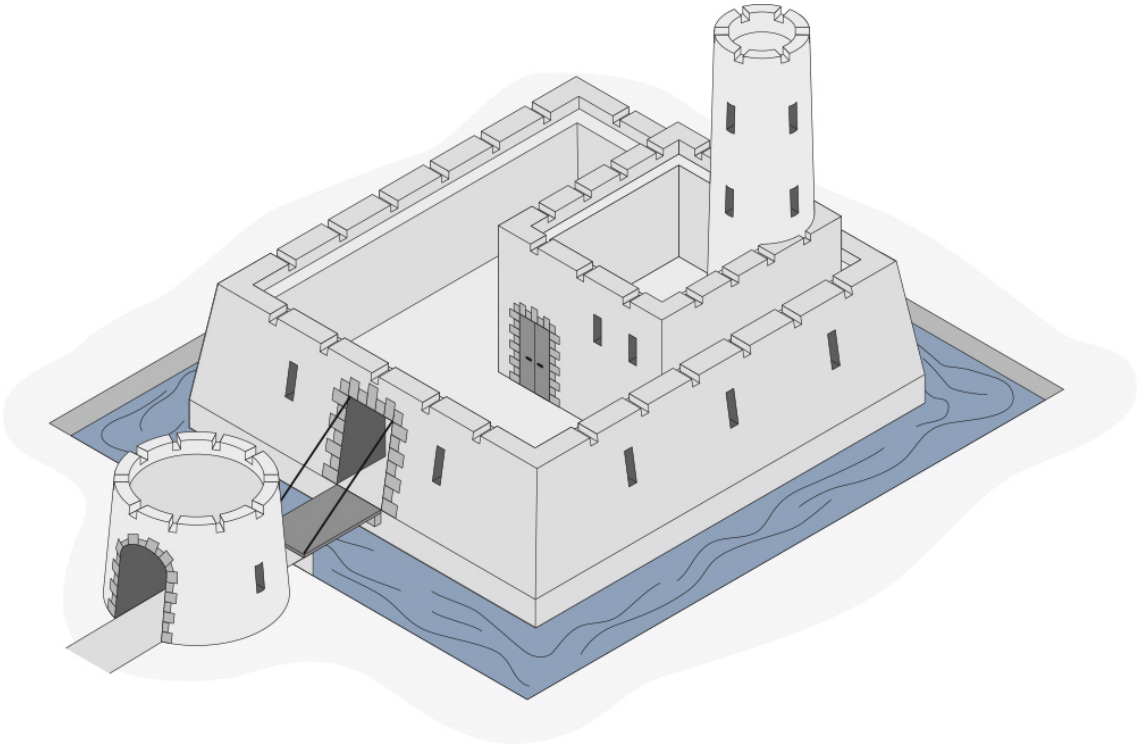


Abbildung 5: Verteidigungsebenen am Beispiel einer Burg

Dadurch ist gewährleistet, dass eine Angriffsmethode allein nicht zum „Erfolg“ führt. Um weiter in ein Netzwerk vorzudringen, muss ein Angreifer also immer wieder neue, sich überlappende Schutzschichten überwinden. Und selbst wenn es ihm gelingen sollte, in das Subnetz einer Fertigungszelle einzudringen, wäre es ihm kaum möglich, von dort aus Ziele in benachbarten Subnetzen anzugreifen.

5.4. Organisatorische Maßnahmen

Ob sich produzierende Unternehmen vor Bedrohungen aus der Cyberwelt schützen, ist, wie bereits angesprochen, immer eine Abwägung von Kosten und Nutzen. Hierzu verpflichtet sind

beispielsweise in Deutschland laut IT-Sicherheitsgesetz nur Betreiber von Infrastrukturen, die eine gesamtgesellschaftliche Bedeutung haben, wozu beispielsweise die Bereiche Energie, Verkehr und Gesundheit gehören. Auch in anderen Ländern bestehen vergleichbare gesetzliche Vorgaben, in den USA etwa für den Schutz von Stromnetzen.
Angesichts der zahlreichen Bedrohungen spricht vieles dafür, Anlagen sowohl vor beabsichtigten als auch unbeabsichtigten Security-Verletzungen zu schützen. Mit ausgeklügelten Firewall-Konzepten allein ist es jedoch nicht getan. Vielmehr muss das gesamte Unternehmen sozusagen Security verinnerlichen. Zudem sollten Richtlinien aufgestellt werden, die nicht nur für alle Mitarbeiter gelten, sondern ebenso für Partner wie etwa Gerätehersteller und Dienstleister.
Darüber hinaus ist es wichtig, dass IT- und Automatisierungsspezialisten Hand in Hand arbeiten, wozu sie sich mit den unterschiedlichen Anforderungen und Arbeitsweisen des jeweils anderen vertraut machen müssen. Schließlich sollte eine Organisation aufgebaut werden, deren Mitglieder für die Datensicherheit in der Fertigung und deren ständige Verbesserung verantwortlich sind. An der Spitze steht idealerweise ein Security-Beauftragter, der zur obersten Führungsebene gehört oder wenigstens direkt an diese berichtet.

5.5. Schulungen

„Wer aufhört, besser zu werden, hat aufgehört, gut zu sein“, lautet ein Erfolgsrezept, das Unternehmen auch bei Security beherzigen sollten. Eine Möglichkeit dazu bieten regelmäßige Schulungen, mit denen sich beispielsweise das Bewusstsein der Mitarbeiter schärfen lässt. Andere Inhalte können etwa Informationen zu aktuellen Bedrohungen sein oder Unterweisungen, wie sich bestimmte Sicherheitslücken schließen lassen. Denn nur dann, wenn die Security-Kompetenz gezielt erweitert wird, kann verhindert werden, dass Mitarbeiter aus mangelnder Qualifikation falsche Entscheidungen treffen.
Es gibt zahlreiche Anbieter, die Security-Schulungen durchführen. Die Seminare von Pilz, die sowohl am Stammsitz in Ostfildern bei Stuttgart als auch bei Kunden oder – in komprimierter Form – als Webinar veranstaltet werden, richten sich insbesondere an Maschinenkonstrukteure und Anlagenplaner. Sie geben einen grundlegenden Überblick und erläutern, wie Gefahren erkannt und minimiert werden können. Das Themenspektrum reicht von der Netzwerkarchitektur über die Authentifizierung von Netzteilnehmern und die Verschlüsselung von Daten bis hin zu einer sicheren Fernwartung.

6. Zusammenfassung und Ausblick

Um größtmögliche Security zu erreichen, kommt es vor allem darauf an, die Architektur des Netzwerks sowie die Kommunikationsprotokolle und die Art des Datenverkehrs genau zu kennen. Denn nur so lassen sich sowohl externe als auch interne Bedrohungen abwehren, seien sie nun beabsichtigt oder unbeabsichtigt.
Früher war Security eigentlich nur in der klassischen Informationstechnologie (IT) ein Thema. Seitdem im Zuge von Industrie 4.0 in Fertigungsanlagen immer häufiger Serienprodukte aus dem Consumer-Bereich und komplexe Betriebssysteme eingesetzt werden, muss sich jedoch auch die Automatisierung damit befassen. Weil sich die Normen aus der IT nicht eins zu eins übertragen lassen, wurden neue erarbeitet, von denen die IEC 62443 die wichtigste ist. Denn

sie definiert, wie eine umfassende Security-Strategie für den industriellen Bereich Schritt für Schritt entwickelt und umgesetzt werden kann.
Zugleich müssen diese Strategien auch Safety einbeziehen, weil sich deren Funktionen letztlich nur gewährleisten lassen, wenn die entsprechenden Daten zuverlässig übertragen werden. Denn Security-Bedrohungen können sich ständig verändern und mithin auch die Gegenmaßnahmen. Das heißt, obwohl diese beiden Aspekte der Automatisierung auch weiterhin eigenständig bleiben, müssen sie eng aufeinander abgestimmt werden. Die gute Nachricht: Wer sich schon mit Safety auskennt, wird sich bei Security leichter tun, weil sich die Vorgehensweisen ähneln.

Glossar

Access Control List	Eine Access Control List (ACL; deutsch: Zugriffssteuerungsliste) legt fest, in welchem Umfang einzelne Personen, Rechner oder Netze über welche Dienste auf den Router oder Switch zugreifen dürfen. Der Zugriff kann für einzelne Rechner oder Netze und für die jeweilige Zugriffsmethode festgelegt werden.
Broadcast-Sturm	Ein Broadcast-Sturm ist eine starke Anhäufung von Broadcast-Verkehr in einem Rechnernetz, der dazu führt, dass keine Netzwerkverbindungen mehr aufgebaut werden und bestehende Verbindungen unterbrochen werden können. Ein Broadcast-Sturm kann durch einen Angriff, durch falsche Konfiguration oder auch schlechtes Netzwerkdesign entstehen.
Deep Packet Inspection	Deep Packet Inspection steht für ein Verfahren in der Netzwerktechnik, Datenpakete zu überwachen und zu filtern. Damit können Spams bekämpft werden, außerdem kann Deep Packet Inspection zur Überlastkontrolle und Reduzierung des Datenverkehrs eingesetzt werden.
DES (Data Encrption Standard)	Data Encryption Standard, kurz DES ist ein standardisiertes symmetrisches Verschlüsselungsverfahren.
Intrusion Detection System	Mit Hilfe von Intrusion-Detection können Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind, frühzeitig erkannt werden, sodass schnell Gegenmaßnahmen eingeleitet werden können.
IP-Spoofing	IP-Spoofing bezeichnet in Computernetzen das Fälschen von Absender-IP-Adressen von IP-Paketen, um dem angegriffenen IT-System eine falsche Identität vorzuspielen. Jedes IP-Paket enthält in seinen Kopfdaten seine Absenderadresse. Ein Angreifer kann diese Absenderadresse in den Kopfdaten so fälschen, dass es aussieht, als wäre das Paket von einem anderen Computer versendet worden. Viele Protokolle der TCP/IP-Familie können nur über eine IP-Adresse authentifiziert werden. Wurde diese gefälscht, können Sicherheitsmaßnahmen wie z.B. die IP-adressbasierte Authentifizierung im Netzwerk ausgetrickst werden. IP-Spoofing ist dabei nur eine Art von Spoofing. Heutzutage werden unter "Spoofing" alle Methoden verstanden, mit denen sich Authentifizierungs- und Identifikationsverfahren umgehen lassen, welche vertrauenswürdige Adressen oder Hostnamen in Netzwerkprotokollen verwenden.
Hashing-Algorithmus MD5	MD5 (Message Digest Algorithm 5) gehört zur Gruppe mathematischer Einwegfunktionen. Dies bedeutet, dass es

	keine einfache Möglichkeit gibt, aus dem Ergebnis auf die Eingangsparameter zu schließen. Bei MD5 wird eine beliebige Menge von Eingangsdaten auf einen 128 Bit langen Wert abgebildet. Bei einem Hash-Algorithmus wird davon ausgegangen, dass es extrem schwierig ist, zwei Eingangsdokumente zu finden, die den gleichen Ergebniswert (Kollision) liefern. Im Fall von MD5 sind seit einiger Zeit Schwächen bekannt, die es einem Angreifer ermöglichen, Kollisionen zu erzeugen.
Meltdown und Spectre	Meltdown und Spectre sind Sicherheitslücken, die in Mikroprozessoren entdeckt wurden und über die ein unautorisierter Zugriff auf den Speicher fremder Prozesse möglich ist.
Netzwerk-Standard IEEE 802.1x	IEEE 802.1X ist ein Netzwerk-Standard zur Authentifizierung von Anwendern in IEEE-802-Netzen. Dieser Standard fungiert als Kontrollinstanz, die den Anwender überprüft, bevor er auf das LAN- oder WLAN-Netzwerk zugreift.
Security-Ziel: Integrität	Integrität im Zusammenhang mit Daten stellt sicher, dass Daten sowie die Funktionsweise eines Systems stets korrekt sind. Ist Integrität gewährlistet, können unautorisierte oder unbemerkte Veränderungen sofort erkannt und ausgeschlossen werden.
Segmentierung von Netzwerken	Segmentierung bedeutet, dass man ein Netzwerk in kleinere Einheiten aufteilt. Diese Einheiten werden dann mit Firewalls oder anderen Geräten, mit denen sich die Kommunikation einschränken lässt, gekoppelt. Somit lassen sich sowohl die Auswirkungen von Broadcast-Stürmen oder anderen "versehentlichen" Ereignissen, als auch die Auswirkungen von Angriffen einschränken.

Abbildungsverzeichnis

Abbildung 1: Norm IEC 62443 9
Abbildung 2: Projektschritte der Risikoanalyse 10
Abbildung 3: Risikobeurteilung mit Hilfe der Security Level 11
Abbildung 4: "Zones and Conduits"-Modell 13
Abbildung 5: Verteidigungsebenen am Beispiel einer Burg 14

Wir sind international vertreten. Nähere Informationen entnehmen Sie bitte unserer Homepage
www.pilz.com oder nehmen Sie Kontakt mit unserem Stammhaus auf.

Stammhaus: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Deutschland
Telefon: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: info@pilz.de, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY