4 Konzepte der IEC 62443

Die Norm IEC 62443 basiert auf einigen übergeordneten Grundkonzepten. In der ersten Edition des Teils IEC 62443-1-1 [2], der 2009 veröffentlicht wurde, sind einige dieser Konzepte beschrieben. Ein Aktualisierung des Dokuments ist in Arbeit, das die folgenden Konzepte detaillierter beschreiben wird.

4.1 Tiefgestaffelte Verteidigung (Defense-in-Depth)

Defense in Depth – dieses wichtige Konzept basiert auf der Erkenntnis, dass beim Schutz der industriellen Anlagen gegen Cyberangriffe die Beteiligung aller Stakeholder erforderlich ist: Betreiber, Integrator und Hersteller. Eine einzige Maßnahme ist im Allgemeinen nicht ausreichend, um einen angemessenen Level der Schutzmaßnahmen zu erreichen. Vielmehr müssen mehrere, untereinander abgestimmte und koordinierte Maßnahmen umgesetzt werden, die jeweils als Verteidigungslinien angesehen werden können. Die „*Defense in Depth*"-Strategie wird seit langem im militärischen Bereich angewendet. Schon im Mittelalter wurden die Burgen mit mehreren Verteidigungslinien ausgestattet: mit Festungsgraben, Zugbrücke, Außenmauer, Innenmauer, Bergfried und zuletzt der gepanzerten Tür am Zimmer des Feudalherrn. Überwindet der Angreifer eine Hürde, so steht ihm die nächste Verteidigungslinie entgegen. Die verschiedenen Bestandteile der Norm IEC 62443 unterstützen die Auslegung einer Defense-in-Depth-Strategie zum Schutz gegen Cyberangriffe.

Wenn man sich die Verteidigungslinien als Schalenmodell vorstellt, dann sind die äußeren Schichten beim Betreiber zu finden. Eine Grundvoraussetzung jedes Schutzkonzepts beginnt mit der Sensibilisierung der Mitarbeiter für die Gefahren von Cyberangriffen. Die Anlage muss physisch geschützt sein mit einer Zugangskontrolle aller autorisierten Personen. Die Norm fordert organisatorische Maßnahmen: definierte Prozesse zum Betrieb der Automatisierungslösung oder Maschine aber auch Kompetenzaufbau durch Informationsveranstaltungen oder Schulungen und klare Verantwortlichkeitsstrukturen in der Organisation. Zum Beispiel ist es sehr wichtig, die Rollen und Privilegien aller Anwender der Automatisierungslösung zu definieren und auf das minimal Notwendige einzugrenzen. Zu nennen ist auch die Festlegung der Maßnahmen im Voraus, die das Aufrechterhalten des Betriebs im Fall eines erfolgreichen Cyberangriffs sicherstellen sollen, sog. *„Business Continuity Plan"*.

Weitere Verteidigungslinien werden in der Auslegung der Automatisierungslösung gebildet, z. B. durch die Segmentierung des Kommunikationsnetzwerks in Firewall-geschützte Zellen oder den Zugriffsschutz mit Passwörtern. Zur Unterstützung der vom Betreiber festgelegten Rollen und Privilegien sollte die Automatisierungslösung so konfiguriert werden, dass die Anwender nur solche Aktionen durchführen können, die für ihre Aufgabe notwendig sind, sog. *„least privilege"*. Solche Maßnahmen werden in der Regel durch den Integrator umgesetzt.

Die inneren Verteidigungslinien werden über die Geräte und Komponenten der Automatisierungslösung bzw. der Maschine realisiert: durch dort integrierte Sicherheitsfunktionen. Zum

Beispiel werden Virenscanner oder weiße Listen (White Listing) zum Schutz gegen Malware eingesetzt. Schutz gegen Manipulation bieten Verschlüsselung, Hash-Techniken oder auch signierte Firmware-Downloads. Angriffe zum Herausfinden der Passwörter, sog. *„password guessing“*, werden durch Verzögerungen zwischen nacheinander folgenden Anmeldeversuchen abgewehrt.

Zu erwähnen ist auch, dass die Prozesse des Integrators möglichst darauf ausgelegt werden sollten, dass während des Designs der Automatisierungslösung nicht zusätzliche Angriffsmöglichkeiten geschaffen werden. Dazu gehört zum Beispiel das gezielte Löschen aller vorübergehenden Accounts, der Schutz der System- und Default-Accounts durch strenge Passwörter oder die systematische Aktualisierung aller Schutzmaßnahmen gegen Malware. Security-Maßnahmen sollten auch Bestandteil der Entwicklungsprozesse des Herstellers sein, mit dem Ziel, möglichst Schwachstellen in den Produkten auszuschließen. Dazu gehören Risikoanalysen, Programmierrichtlinien, statische und dynamische Codeanalysen oder Penetrationstests.

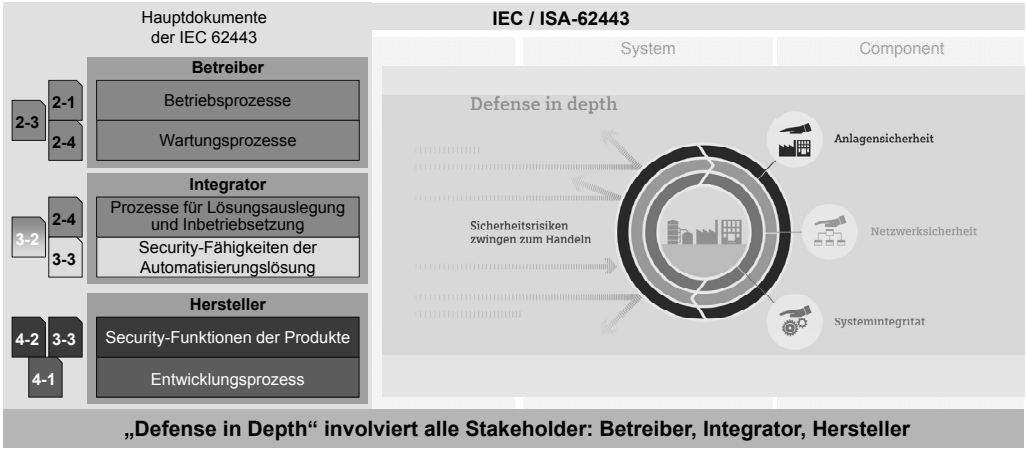

Bild 3 Tiefgestaffelte Verteidigung (Defense-in-Depth)

Dass Schwachstellen und damit Angriffsvektoren durch die jeweiligen Stakeholder erzeugt werden können, zeigt folgendes Beispiel im Thema Anwenderverwaltung und Zugriffskontrolle (*„User Management and Access Control, UMAC“*). In den Produkten findet man oft noch fest codierte Passwörter. Gelingt es einem Angreifer, den Code auszulesen und zu analysieren, wird es für ihn ein Leichtes sein, solche Passwörter ausfindig zu machen. Dafür sind im Internet zuhauf Werkzeuge verfügbar. Eine andere typische Schwachstelle ist die Möglichkeit, Privilegien zu erhöhen und sich zum Beispiel durch Überwinden der Anwenderverwaltung als Administrator anzumelden. Damit stehen dem Angreifer alle Mittel zum Missbrauch zur Verfügung. Die Hersteller können solche Schwachstellen durch klare Regeln für die Programmerstellung im Entwicklungsprozess vermeiden. In der Verantwortung des Integrators liegt wie bereits erwähnt der Schutz der bei der Werksauslieferung vorhandenen System- und Default-Accounts durch Ändern der Default-Passwörter. Während der Auslegung der Automatisierungslösung werden in der Regel temporäre Accounts angelegt, die hohe Privilegien besitzen und durch schwache Passwörter geschützt sind. Während der Designphase möchte

ja der Entwickler nicht aufwendig bei jedem Einloggen ein langes, komplexes Passwort eingeben müssen. Eine häufig anzutreffende Schwachstelle ist, dass diese Accounts vor der Übergabe der Lösung an den Betreiber nicht gelöscht wurden. Man kann sich vorstellen, was ein Angreifer dadurch anrichten kann. Durch entsprechende Vorgaben in den Prozessen des Integrators können solche Schwachstellen leicht vermieden werden. Schließlich liegt es am Betreiber, die Namen der Personen, die den definierten Rollen zugewiesen sind, während der Betriebsphase zu pflegen. Da diese oft viele Jahre dauert, ist die Verantwortung des Betreibers besonders groß. Wenn zum Beispiel ein Administrator die Firma verlässt, ist es von eminenter Wichtigkeit, dessen Account zu löschen. Möchte diese Person der Firma schaden, wären die Verteidigungsmöglichkeiten sehr eingeschränkt. Eine andere wichtige Aufgabe des Betreibers ist, dafür zu sorgen, dass die Passwörter vertraulich behandelt werden und regelmäßig geändert werden. Hier sind die Betriebs- und Wartungsprozesse gefragt. Aus dem genannten Beispiel wird ersichtlich, dass alle der o. g. Maßnahmen umgesetzt werden müssen, um einen gewissen Schutz zu erreichen. Eine einzelne Schwachstelle reicht aus, um die gesamte Kette zu schwächen und die Anlage anfällig zu machen.

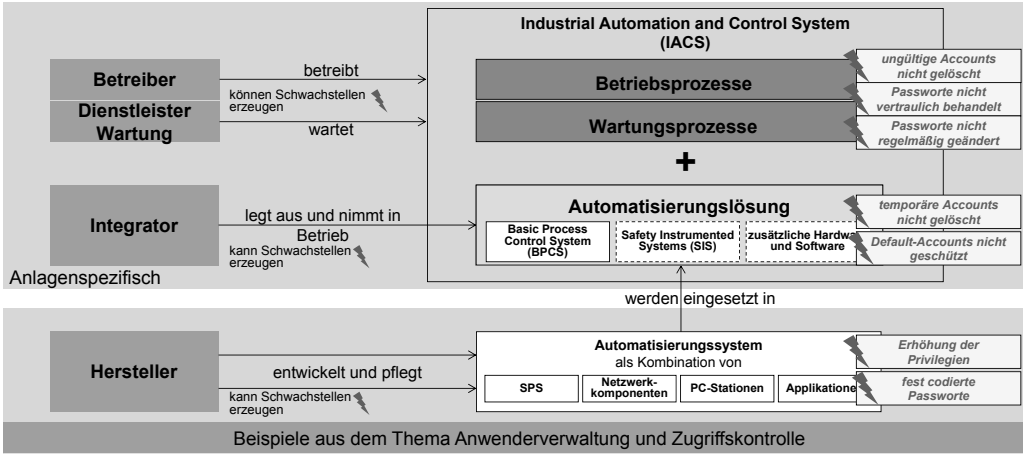

Bild 4 Beispiele von Schwachstellen bei Anwenderverwaltung und Zugriffskontrolle

4.2 Risikobewertung nach VDI/VDE 2182

Die Schutzmaßnahmen gegen Cyberangriffe ergeben sich aus der Bewertung der Bedrohungen und der Konsequenzen im Fall eines Angriffs auf die Betrachtungsgegenstände, die in der Verantwortung der jeweiligen Organisation sind. Für den Hersteller sind es seine Produkte, der Integrator wird die Automatisierungslösung betrachten und für den Betreiber steht die Produktionsanlage im Fokus.

Die prinzipielle Vorgehensweise gliedert sich in vier Phasen, die zyklisch wiederholt werden:

1. Planung / Bewertung der Risiken und der möglichen Gegenmaßnahmen
2. Festlegung der Schutzmaßnahmen