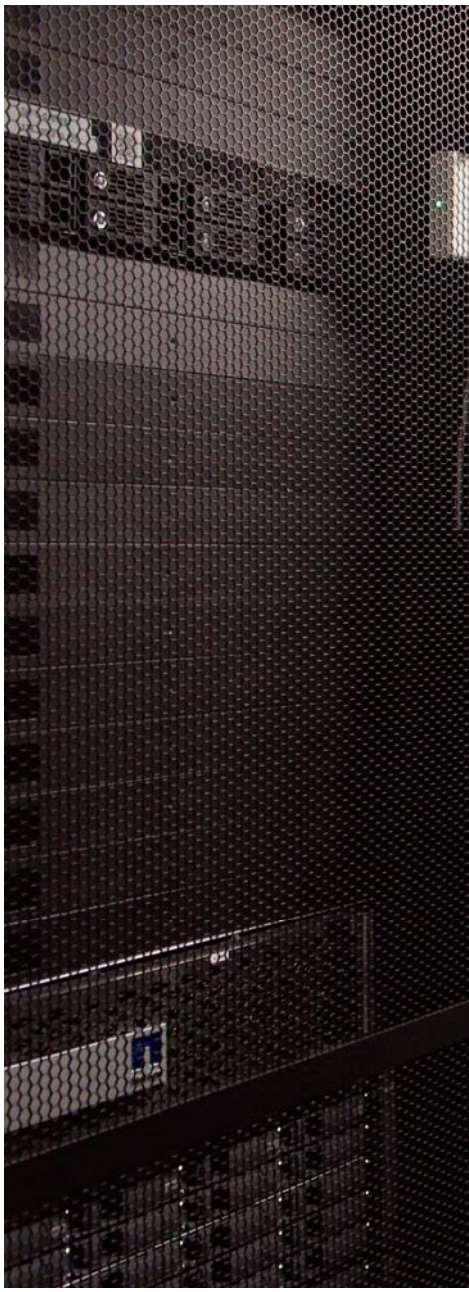
Die Abwehr steht



Die Betreiber kritischer Infrastrukturen müssen besondere Vorkehrungen treffen, um die Automatisierungstechnik vor unbefugtem Zugriff durch Hacker zu schützen. Mit den Automation-Security-Dienstleistungen unterstützt ABB die Betreiber auf dem Weg zu den gesetzlich geforderten Zertifizierungen.

Die Auswirkungen eines Cyberangriffs auf die Prozessleittechnik von Energieerzeugungsanlagen, virtuellen Kraftwerken oder Wasserver- und -entsorgungsanlagen können schwerwiegend sein. Die denkbaren Szenarien reichen von Personen- und Sachschäden über Umweltbeeinträchtigungen bis hin zu wirtschaftlichen Ausfällen. Aus diesem Grund wurden im IT-Sicherheitsgesetz für die Betreiber kritischer Infrastrukturen – also von Einrichtungen, deren Ausfall Versorgungsengpässe, Störungen der öffentlichen Sicherheit oder sonstige dramatische Folgen nach sich ziehen würde – besondere Pflichten im Hinblick auf den Schutz ihrer IT-Infrastruktur definiert. Über rein technische Maßnahmen hinaus sind sie verpflichtet, ein Information Security Management System (ISMS) gemäß DIN ISO/IEC 27001 einzuführen und regelmäßig zertifizieren zu lassen.

Risiken effektiv steuern

Wirksame Sicherheitskonzepte für Prozessleitsysteme schützen bestmöglich vor Cyberangriffen, ohne die Verfügbarkeit, Zuverlässigkeit und Stabilität der Anlagen einzuschränken. Als führender Leitsystemanbieter hilft ABB Unternehmen dabei, die eingesetzten Systeme sicher zu betreiben. Das Ziel ist es, das vom IT-Sicherheitsgesetz geforderte Schutzniveau zu erreichen und über den gesamten Lebenszyklus der Anlage aufrechtzuerhalten.

Automation Security von ABB umfasst Sicherheitsdienstleistungen für Automatisierungssysteme, die den Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit vollauf gerecht werden. Dabei werden zwei Kategorien unterschieden: einmalig durchzuführende Maßnahmen und regelmäßige Dienstleistungen, die Bestandteil des Servicevertrags Power Generation Care sind.

Am Anfang steht die Analyse

Risiken lassen sich kontrollieren, aber niemals vollkommen beseitigen. Es geht darum, potenzielle Gefahren, Schäden und Störungen auf ein Mindestmaß zu reduzieren. Damit dieser Ansatz der Risikosteuerung möglichst effektiv ist, sollte der erste Schritt darin bestehen, sich einen Überblick über den gegenwärtigen Sicherheitsgrad des Systems zu verschaffen.

Das Cyber Security Assessment (CSA) stellt aktuell implementierte Schutzmaßnahmen sowie empfohlene oder bereits definierte Vorgaben gegenüber und identifiziert so Sicherheitslücken. Der Penetration Test erkennt einen hohen Anteil der anlagenspezifischen Schwachstellen. Auf der Basis von CSA und Penetration Test lässt sich ein anlagenspezifisches Sicherheitskonzept erstellen, das die konkreten organisatorischen und technischen Maßnahmen festlegt. Seine Wirksamkeit steht und fällt mit der korrekten Umsetzung und der konsequenten Befolgung durch alle Beteiligten. Das Cyber Security Training sensibilisiert das Anlagenpersonal und vermittelt das notwendige Know-how.

Zugriff für Unbefugte verboten

Ein wichtiger Faktor, um Prozessautomatisierungssysteme vor unbefugter Nutzung zu schützen, ist eine sichere Authentifizierung. Sie sorgt dafür, dass ausschließlich die richtigen Personen Zugriff auf die richtigen Informationen haben. Im Zuge der Systemhärtung werden Funktionen und Programme, die für den Betrieb nicht erforderlich sind, deaktiviert oder eingeschränkt. Während Leitsys-

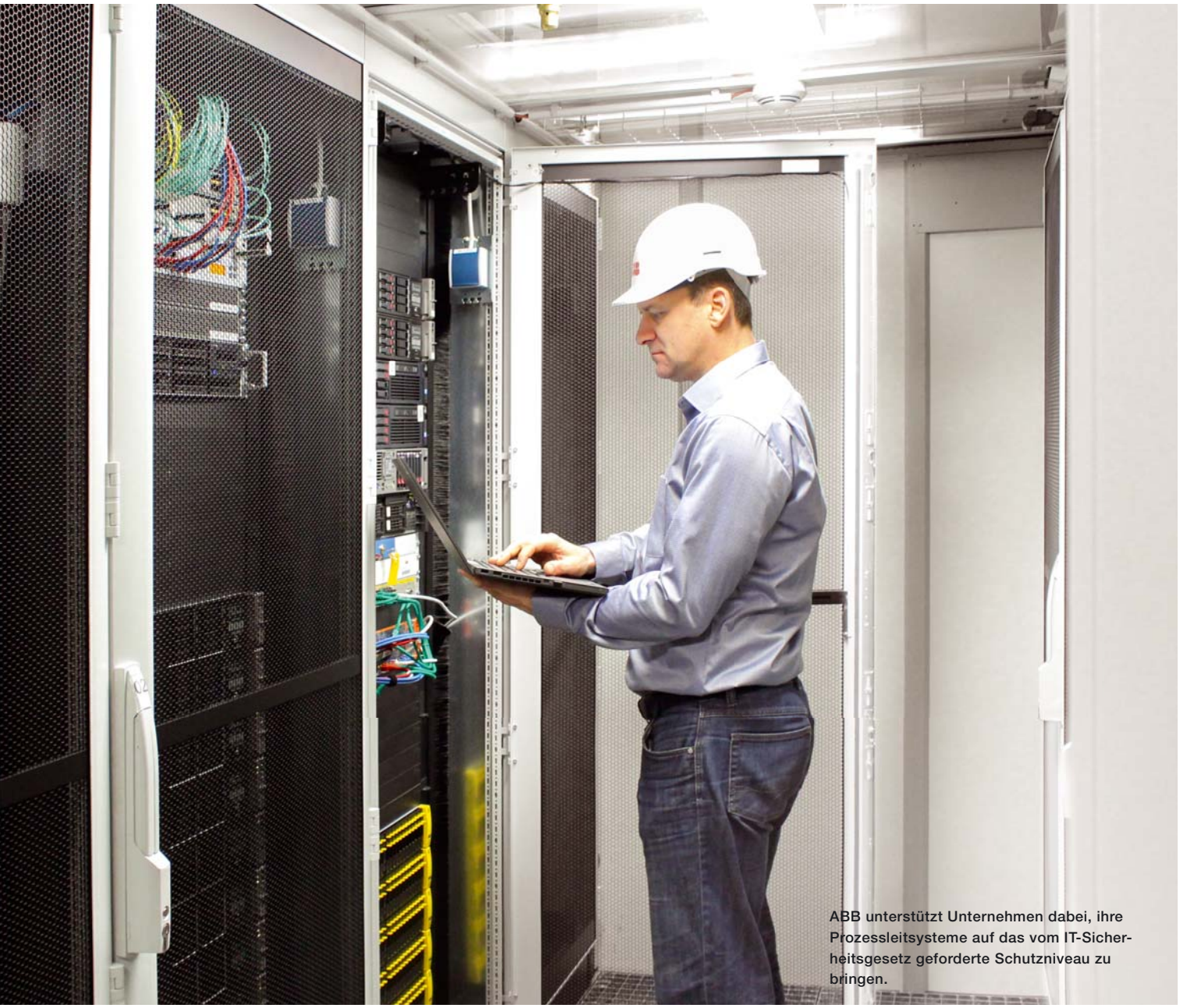


ABB unterstützt Unternehmen dabei, ihre Prozessleitsysteme auf das vom IT-Sicherheitsgesetz geforderte Schutzniveau zu bringen.

Wirksame Sicherheitskonzepte schützen vor Cyberangriffen, ohne die Verfügbarkeit, Zuverlässigkeit und Stabilität der Anlagen einzuschränken.

teme in der Vergangenheit physisch von anderen Geräten entkoppelt und damit vor äußeren Einflüssen geschützt waren, besteht heutzutage häufig die Notwendigkeit einer horizontalen und vertikalen Integration. Die Lösung bietet der Aufbau eines Zonenmodells, bei dem das Netzwerk aus mehreren Segmenten mit unterschiedlichen Sicherheitskriterien besteht.

Über solche grundlegenden Maßnahmen hinaus umfassen die Cyber-Security-Lösungen von ABB auch zusätzliche Dienstleistungen, die das Sicherheitskonzept erweitern und eine regelmäßige Überprüfung des Schutzniveaus festlegen. Dazu gehören beispielsweise das Patch Management, der Schutz vor Schadprogrammen, der Fernzugriff und die Fernwartung sowie eine geeignete Backup- und Recovery-Strategie.

Der richtige Partner

In enger Zusammenarbeit mit den Betreibern sorgt ABB für die schrittweise Umsetzung der definierten Maßnahmen, um das angestrebte Sicherheitsniveau zu erreichen und aufrechtzuerhalten. Die ABB-Experten verfügen über umfassende prozessspezifische Kenntnisse in den zu den kritischen Infrastrukturen zählenden Branchen und zeichnen sich durch vielfältige Projekterfahrungen bei der Planung und Umsetzung von Sicherheitslösungen aus. Sie beraten hersteller- sowie produktunabhängig und sind von der Systemkonzeption bis zur Realisierung von technischen Sicherheitsmaßnahmen die Wegbegleiter zu einer erfolgreichen Zertifizierung nach DIN ISO/IEC 27001.

Weitere Infos: richard.biala@de.abb.com