www.sps-magazin.de

29. Jahrgang | **Ausgabe 9** | September 2016 | EUR 9,-

SPS MAGAZIN

Zeitschrift für Automatisierungstechnik

RFID-Lösungen direkt in ERP-, MES- und andere Datensysteme einbinden

Integrator für Industrie 4.0

PILZ

Highlights

Marktübersichten

Produktübersichten

Bild: Bosch Rexroth AG

Produktneuheiten ab Seite 18

Bild: Pilz GmbH & Co. KG

Cyber-Sicherheit für Kritische Infrastrukturen

Bild: geralt / pixabay.com

Kritis-Betreiber sind in der Pflicht, ihre IT-Sicherheitsvorkehrungen anzupassen.

Seit rund einem Jahr ist in Deutschland das neue IT-Sicherheitsgesetz in Kraft. Besonders Betreiber sogenannter Kritischer Infrastrukturen sind nun in der Pflicht, ihre IT-Sicherheitsvorkehrungen anzupassen. Um bei der Erarbeitung eines ganzheitlichen Konzepts bis hin zur Auditierung alle wichtigen Aspekte im Blick zu behalten, empfiehlt es sich, auch auf die Unterstützung erfahrener Spezialisten zurückzugreifen.

Kaum eine Woche vergeht, in der nicht von Cyber-Angriffen auf öffentliche Institutionen, Behörden oder privatwirtschaftliche Unternehmen in Deutschland berichtet wird. Diese erfolgen zielgerichtet und werden technisch immer ausgereifter und komplexer. Der jährliche Schaden durch Cyber-Angriffe und deren Auswirkungen wird vom Cyber-Sicherheitsrat auf jährlich bis zu 50Mrd.€ geschätzt.

Ziel: signifikante Verbesserung der Sicherheit

Mit dem Mitte 2015 vom Deutschen Bundestag verabschiedeten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme soll eine signifikante Verbesserung der Sicherheit von IT-Systemen in Deutschland erreicht werden. Insbesondere Betreiber sogenannter kritischer Infrastrukturen (KRITIS) sind aufgrund ihrer besonderen Verantwortung für das Gemeinwohl verpflichtet, ein Mindestniveau an IT-Sicherheit einzuhalten und IT-Sicherheitsvorfälle zu melden, denn ein Ausfall oder eine Beeinträchtigung ihrer Infrastrukturen kann weitreichende gesellschaftliche Folgen haben. Im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik sind solche Infrastrukturen als Einrichtungen, Anlagen oder Teile davon definiert, die den folgenden Sektoren angehören:

- Energie,
- Informationstechnik und Telekommunikation,
- Transport und Verkehr,
- Gesundheit/Pharma,
- Wasser,
- Ernährung
- sowie Finanz- und Versicherungswesen

Diese sind von hoher Bedeutung für das Funktionieren des Gemeinwesens, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Anforderungen des neuen IT-Sicherheitsgesetzes

Kritis-Betreiber müssen nun also bestimmte Mindest-Sicherheitsstandards für ihre IT-Infrastrukturen einhalten. Der durch

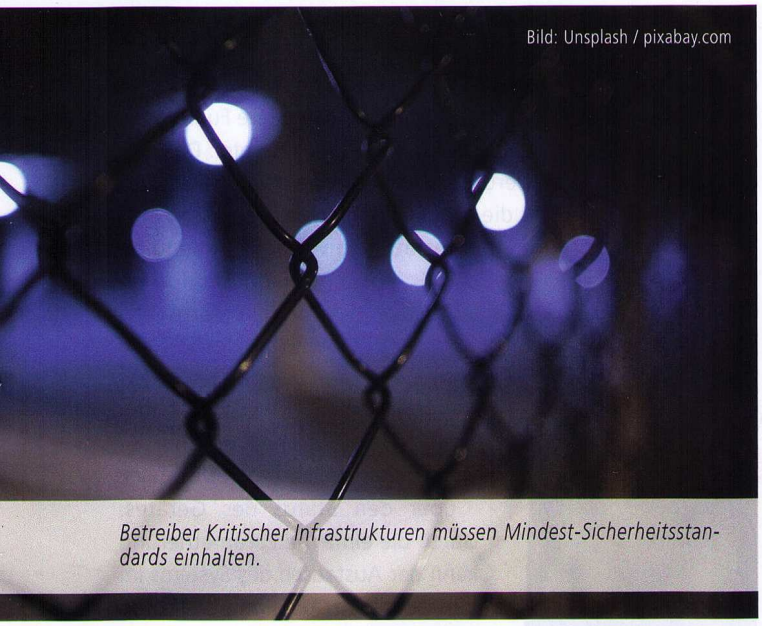

Bild: Unsplash / pixabay.com

Betreiber Kritischer Infrastrukturen müssen Mindest-Sicherheitsstandards einhalten.

Bild: TBIT / pixaby.com

Bei der Umsetzung der Anforderungen empfiehlt es sich, einen Experten zu Rate zu ziehen.

das IT-Sicherheitsgesetz im BSI-Gesetz neu hinzu gekommene Paragraph 8a legt fest, dass diese Unternehmen verpflichtet sind, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Infrastrukturen maßgeblich sind. Darüber hinaus haben die Betreiber mindestens alle zwei Jahre die Erfüllung der Anforderungen, wie oben dargestellt, auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Des Weiteren ist nunmehr gesetzlich festgelegt, dass IT-Sicherheitsvorfälle meldepflichtig sind. Das Bundesamt für Sicherheit in der Informationstechnik ist die zentrale Meldestelle für Betreiber kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik. KRITIS-Betreiber haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, unverzüglich an das BSI zu melden.

Umsetzung der Anforderungen – was ist zu tun?

Wichtige Maßnahmen mit hoher Komplexität zur Umsetzung der Anforderungen aus dem IT-Sicherheitsgesetz sind der Aufbau eines Risiko- und Krisenmanagements sowie die Planung, Etablierung, Aufrechterhaltung und ständige Verbesserung eines Information Security Management Systems (ISMS) nach dem internationalen Informationssicherheits-Standard ISO27001. Für den Aufbau des Risiko- und Security-Management-System empfiehlt es sich, bereits in der Planungsphase die Hilfe spezialisierter Berater in Anspruch zu nehmen. Soll das bestehende System im Unternehmen überprüft und angepasst werden, so bieten sich ein von extern durchgeführter Sicherheitscheck oder eine GAP Analyse an, um die wesentlichen Bausteine des ISMS zu testen. Technische, organisatorische, personelle und bauliche Maßnahmen werden dabei auf ihren Umsetzungsstatus hin geprüft. Ein abschließender Ergebnisreport gibt Aufschluss über den Status des ISMS im jeweiligen Unternehmen und zeigt den Handlungsbedarf auf. Nach der Umsetzung der dafür erforderlichen technischen und organisatorischen Maßnahmen, wie der Etablierung von Notfallmanagement- und Security-Incident-Prozessen oder der Besetzung der Rollen des Information Security Managers sowie Notfall- und Krisenmanagers, kann nach Erreichen des geforderten Umsetzungsgrads der Maßnahmen die Zertifizierung nach ISO27001 in Angriff genommen werden.

BSI-zertifizierte Revisoren

Der Einsatz BSI-zertifizierter Informationssicherheits-Revisions- und Beratungsexperten (IS-Revisor) gewährleistet die notwendige Qualität und stellt sicher, dass die Ergebnisse bei Behörden und externen Stellen anerkannt werden. Die erfolgreiche Zertifizierung ist der entscheidende Meilenstein bei der Umsetzung der Anforderungen des IT-Sicherheitsgesetzes und ein wirksamer Beitrag zur Abwehr von Cyber-Angriffen gegen die kritischen Infrastrukturen. ■

Autor: ***Dr.-Ing. Christian Scharff,***
CISSP, zertifizierter Informationssicherheits-Revisions- und Beratungsexperte (BSI),
zertifizierter Datenschutzauditor (TÜV)
Accuris AG
www.accuris.de