Herausforderungen der IT-Sicherheit bei kleinen und mittleren Betreibern kritischer Infrastrukturen

Der Schutz der IT kritischer Infrastrukturen gerät durch verschiedene Vorfälle und nicht zuletzt durch das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz zunehmend in den Fokus. Kleine und mittlere Betreiber benötigen Orientierung bei der Analyse ihrer Gefährdungslage und bei der Auswahl geeigneter Maßnahmen. Im Rahmen dieses Beitrags wird ein Vorgehen skizziert, das sich an gängigen Normen (BSI-Grundschatz, ISO 2700x) orientiert, aber eine leichte und schnelle Anwendung ermöglicht, um die IT-Sicherheit der Betreiber nachhaltig zu steigern.

von: Christof Thim & David Kotarski (Universität Potsdam)


Herausforderungen für die IT-Sicherheit


Obwohl bei den jüngsten Hackerangriffen gerade die Büro-IT als Einfalls- tor zur Steuerungs-IT genutzt wurde (Sony-Hack, Stahlwerk-Hack), konzentrieren sich Analysen und Maßnah-
men auf nur jeweils einen der beiden IT-Bereiche und betrachten sie nicht als integriertes Ganzes. Die sukzessive gewachsene Verbindung beider IT-Welten über eine gemeinsame Vernetzung und der Wunsch nach orts- und zeitungabhängigem Zugriff sind problematisch geworden. IT-Risiken werden dadurch zu Versorgungsrisiken und müssen in die Risikobewertung ähnlich wie Naturereignisse, Organisationss- und menschliches Versagen einbezogen werden.

Die Ergebnisse der Sicherheitsanalysen führen zumeist zu umfangreichen Maßnahmenlisten, die mit den bestehenden Ressourcen nicht umgesetzt werden können. Daher ist eine Priorisierung notwendig. In den bestehenden Sicherheitskatalogen überwiegen zudem die technischen Maßnahmen, weshalb schnell aus dem Blick gerät, dass eine Sensibilisierung der Mitarbeiter ähnliche Erfolge aufweisen kann.

**Umgang mit IT-Herausforderungen**

oder der Zugriff auf die Steuerung erfolgt direkt aus dem Büronetz. Diese Zugriffsweges gilt es gesondert zu schützen.


Insgesamt ist festzuhalten, dass die Versorgungs-IT bereits mit einfachen Mitteln auf ein höheres Niveau zu bringen ist. Insbesondere die prozessbezogene Analyse und die Sensibilisierung der Mitarbeiter eignen sich gut als erste Ansatzpunkte. Langfristig sollte IT-Sicherheit auch Thema einer informierten Unternehmensleitung sein und entsprechend in Entscheidungsprozessen berücksichtigt werden.

Literatur:

Die Autoren

Christof Thim leitet das Forschungsprojekt Aqua-IT-Lab als Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik und Electronic Government an der Universität Potsdam.

David Kotarski ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik und Electronic Government an der Universität Potsdam, spezialisiert auf IT-Sicherheit und entwickelt Methoden zur ganzheitlichen Sicherheitsschutzanalyse.

Kontakt:
Christof Thim
Universität Potsdam
August-Bebel-Str. 89, 14482 Potsdam
Tel.: 0331 977-3423
E-Mail: christof.thim@wl.uni-potsdam.de
Internet: www.lswi.de/aquitalab