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

von: Christof Thim, David Kotarski (Universität Potsdam)

Der Schutz der IT kritischer Infrastrukturen gerät durch diverse Vorfälle und nicht zuletzt durch das IT-Sicherheitsgesetz zunehmend in den Fokus. Kleine und mittlere Betreiber benötigen Orientierung bei der Analyse ihrer Gefährdungslage und bei der Auswahl geeigneter Maßnahmen. In diesem Artikel wird ein Vorgehen skizziert, dass sich an gängigen Normen (BSI Grundschutz, ISO2700x) orientiert, aber eine leichte und schnelle Anwendung ermöglichen soll, um die IT-Sicherheit der Betreiber nachhaltig zu steigern.

Die IT-Infrastruktur bildet das Rückgrat des Unternehmens, sei es in der Verwaltung oder beim Betrieb der Infrastruktur. Die Wasserver- und Abwasserentsorgung ist durch viele kleine und mittlere Unternehmen geprägt. Diese haben selten die finanziellen und personellen Ressourcen für eine umfangreiche Analyse ihrer IT-Sicherheit. Die sich verschärfende Gefährdungslage [1], [2] potenziert die Risiken, die von der IT ausgehen. Nicht nur das Abgreifen von Kunden- oder Versorgungsdaten stellt hierbei eine Gefahr dar, sondern auch das Kompromittieren der Versorgung ist denkbar. Im Rahmen des BMBF geförderten Forschungsprojektes „AquaIT-Lab“ [3] untersuchen die Autoren diese Fragestellungen und entwickeln angepasste IT-Sicherheitsmaßnahmen.
Dieser Beitrag stellt die Herausforderungen dar, vor denen kleine und mittlere Versorger beim Schutz ihrer IT-Infrastruktur stehen und schlägt ein Vorgehen, dass die Versorger sukzessive auf ein höheres Schutzniveau hebt.

Herausforderungen für die IT-Sicherheit

Eine Reihe von Rahmenwerken geben Hinweise zur Analyse der IT. In Deutschland sind der BSI-Grundschutz sowie die international etablierte ISO2700x-Familie zu nennen. Beide geben wenig versorgerspezifische Hinweise sondern schlagen ein allgemeines Vorgehen zur Analyse vor. Dabei wird zunächst festgelegt, welche Informationen und Datenverarbeitungsprozesse als kritisch eingestuft werden. Die daran beteiligten Informationssysteme, ihre Hardware, Software, Datenhaltung, Räume, Netzwerk und Nutzer, werden bewertet. Der **Aufwand hierfür ist bei heterogen gewachsenen Infrastrukturen kleiner und mittlerer Versorger recht hoch**, da die notwendige, aktuelle Dokumentation der Infrastruktur nur unstrukturiert vorliegt. Daher scheuen die meisten Betreiber die umfassenden Analysen.
Die zweite Herausforderung stellt die **Kopplung unterschiedlicher Infrastrukturteile** dar. Neben den Anwendungssystemen der Büro-IT ist Fernwirktechnik im Einsatz, die über SCADA-

Systeme gesteuert wird. Die oben beschriebenen Analyseverfahren berücksichtigen fast ausschließlich Büro-IT. Sicherheitsmaßnahmen zur Aktualisierung von Systemen, der Installation von Firewalls und Virenscannern sind gut in der Bürowelt anwendbar. Für die Fernwirk-IT sind anderen Maßnahmen notwendig. Hier bietet die ISA/IEC 62443 einen ersten Ansatzpunkt. Auch das ICS-Kompendium [4] und Tools wie LARS ICS [5] geben Aufschluss über die Analyse und Maßnahmengestaltung für IT im industriellen Umfeld.
Das Vorgehen zur Sicherung der Büro-IT und der Steuerung-IT stehen jedoch nebeneinander, obwohl bei den jüngsten Hackerangriffen gerade die Büro-IT als Einfallstor zur Steuerungs-IT genutzt wurde (Sony-Hack, Stahlwerk-Hack). Die sukzessive gewachsene Verbindung beider IT-Welten über eine gemeinsame Vernetzung und dem Wunsch nach orts- und zeitunabhängigen Zugriff ist problematisch geworden. IT-Risiken werden dadurch zu Versorgungsrisiken und müssen in der Risikobewertung ähnlich wie Naturereignisse, Organisations- und menschliches Versagen eine Rolle spielen. Eine gemeinsame Analyse und die Bewertung der Folgen eines Angriffs auf die IT findet selten statt.
Die Ergebnissen der Sicherheitsanalysen führen zumeist zu **umfangreichen Maßnahmenlisten, die mit den bestehenden Ressourcen nicht umgesetzt werden können**. Daher muss eine Priorisierung erfolgen. In den bestehenden Sicherheitskatalogen überwiegen zudem die technischen Maßnahmen, daher gerät schnell aus dem Blick, dass eine Sensibilisierung der Mitarbeiter ähnliche Erfolge aufweisen kann.

Wie sollten nun Versorger mit den Herausforderungen umgehen? Entsprechend der Herausforderungen sollte zunächst die Analyse der IT-Infrastruktur handhabbar gemacht werden. Hierzu bietet sich eine **prozessorientierte Analyse** an. Anstatt die gesamte Infrastruktur einmalig und vollständig zu überprüfen und abzusichern, sollten zunächst die wichtigsten Versorgungs- und Verwaltungsprozesse identifiziert werden.
Ein solches Vorgehen schlägt die amerikanische AWWA vor [6]. Der Versorgungsprozess wird anhand von Szenarien (UseCases) aus Nutzerperspektive beschrieben. Solche Szenarien können u.a. Dateitransfers oder auch PLC-Programmierungen sein. Daraus werden kritische Elemente identifiziert und abgesichert. Mögliche Verbindungen zwischen Büro- und Steuerungs-IT sollten dabei beachtet werden. Abbildung 1 zeigt, wo mögliche prozessbezogene und planungsbezogene Verbindungen vorliegen. Häufig werden aus den SCADA-Systemen Daten direkt in die Abrechnungs- oder Arbeitsplanungssysteme gespielt oder Der Zugriff auf die Steuerung erfolgt direkt aus dem Büronetz. Diese Zugriffswege gilt es gesondert zu schützen.

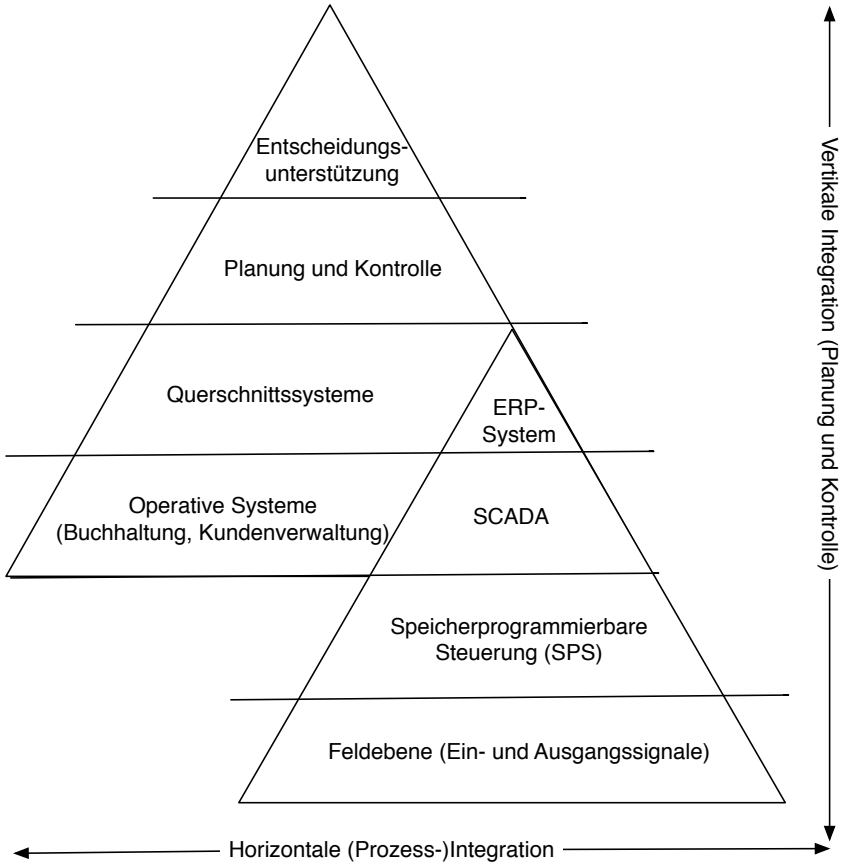

Abbildung 1: Integrierte Informationssysteme in der Versorgung

Die Auswahl schränkt somit den Analyseumfang ein und lässt die strukturierte, sukzessive Abarbeitung einzelner Szenarien zu. Somit kann der Aufwand der Analyse und die Umsetzung der Maßnahmen über kleine Projekte und über mehrere Jahre gestreut werden. Nach und nach erhöht sich die IT-Sicherheit.

Zur Analyse lassen sich die häufig verteilten **bestehenden Dokumente** wie z.B. Netzpläne, Überblick über die installierte Software, Nutzer- und Rollenkonzepte, aber auch allgemeine Risikoanalysen der Versorgungsinfrastruktur nutzen. Diese sollten zentral gesammelt werden. Die Verantwortung zur Aktualisierung kann auf mehrere Schultern verteilt werden. Nutzen sie die Qualitätsmanagement-Zertifizierungen oder anderen Branchenaudits dazu auch ihre IT-Dokumentation zu aktualisieren.

Es empfiehlt sich zur **Umsetzung von Sicherheitsmaßnahmen in kleinen Schritten** vorzugehen. Konzentrieren Sie sich zunächst auf die einfachsten Maßnahmen zur Absicherung. Neben einem funktionierenden Rechte- und Zugriffssystem sollten ein aktueller Viren- und Malwareschutz sowie ein durchdachtes Konzept für mobile Datenträger (USB-Sticks, etc) Standard der IT sein. Des Weiteren sind mobile Endgeräte nur überlegt einzusetzen und gesondert abzugesichern. Dazu zählen spezielle Zugriffswege auf die Unternehmensinfrastruktur z.B. via VPN. Die Steuerung-IT sollte in einer besonders gesicherten

Zone genutzt werden. Mit Verbindungen in die Büro-IT ist sparsam umzugehen. Auch die Einbindung von Dienstleistern sollte geregelt werden.
Technische Lösungen sind nur ein Aspekt der IT-Sicherheit. Von ebenso großer Bedeutung ist die **Sensibilisierung der Mitarbeiter** für Sicherheitsmaßnahmen. Hierzu zählt auch die ausgewogene Ausgestaltung der technischen Lösungen. Das Erzwingen komplexer Passwörter erhöht zwar aus technischer Sicht die Sicherheit, die Nutzer beginnen aber, sich Passwörter zu notieren. Auch das gezieltes Abgreifen von Zugangsdaten (Spear-Phishing-Attacken) oder das Erschleichen physischen Zugangs, z.B. als Wartungspersonal oder Bote zielen auf unbedarftes Nutzerverhalten. Die Sensibilisierung, die auch spielerisch erfolgen kann (z.B. in Awareness-Kampagne [7]), führt zu aufmerksamen Mitarbeitern, die IT-Sicherheit in ihren Arbeitsalltag integrieren.
IT-Sicherheit ist kein einmaliges Projekt, das die Versorger umsetzen. Es erfordert vielmehr eine kontinuierliche Überprüfung und Anpassung. Langfristig sollten Versorger daher ein angemessenes **Informationssicherheitsmanagement** etablieren. Hierzu zählt die Festlegung von Verantwortlichkeiten, Überprüfungszyklen aber auch die Verfügbarkeit von Ressourcen für die IT-Sicherheit. Die Umsetzung kann sukzessive vorgenommen werden und sich daraus zur gelebten Praxis entwickeln.
Damit geht auch die **Integration der Risikobetrachtung der IT in die unternehmensweite Risikoanalyse** einher. Es wird ein zweistufiges Verfahren vorgeschlagen. Die IT-Risiken können in in Risiken der Büro-IT und Risiken der Steuerungs-IT unterschieden werden. Schutzziele sind bei der Büro-IT die Integrität, Verfügbarkeit und Vertraulichkeit der Daten- und Datenverarbeitungsverfahren. Auf der Seite der Steuerungs-IT ist es die Versorgungssicherheit. Die Folgen des Verfehlens eines dieser Ziele muss in die unternehmensweite Risikobetrachtung einfließen. Folgen können qualitativ bewertet werden, wenn z.B. Kundendaten abfließen, oder es kann der wirtschaftliche Schaden eines Systemausfalls geschätzt werden. Insbesondere bei der Steuerungs-IT sind Maßnahmen zu berücksichtigen, die die Versorgungsrisiken dämpfen, z.B. der Umstieg auf manuelle Steuerung. Durch diese Integration wird die Gefährdung der Infrastruktur durch IT-Angriffe sichtbar, bewertbar und budgetierbar.

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 das Thema einer informierten Unternehmensleitung sein und entsprechend in Entscheidungsprozessen berücksichtigt werden.

Literatur/Quellen:

[1] BSI (2014): Die Lage der IT-Sicherheit in Deutschland 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf
[2] Unisys (2014): Critical Infrastructure: Security Preparedness and Maturity, https://www.hunton.com/files/upload/Unisys_Report_Critical_Infrastructure_Cybersecurity.pdf
[3] Aqua-IT-Lab. www.lswi.de/aquaitlab
[4] BSI (2013): ICS-Security-Kompendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf
[5] BSI (2014)LARS ICS. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/materialien/tools/140627_LARS_ICS_Light_and_Right.html
[6] AWWA (2014): Process Control System Security Guidance for the Water Sector. http://www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf
[7] HvS Consulting (2015): Security Awareness: Microsoft jagt das Phantom. http://www.hvs-consulting.de/files/Phantom_Whitepaper.pdf