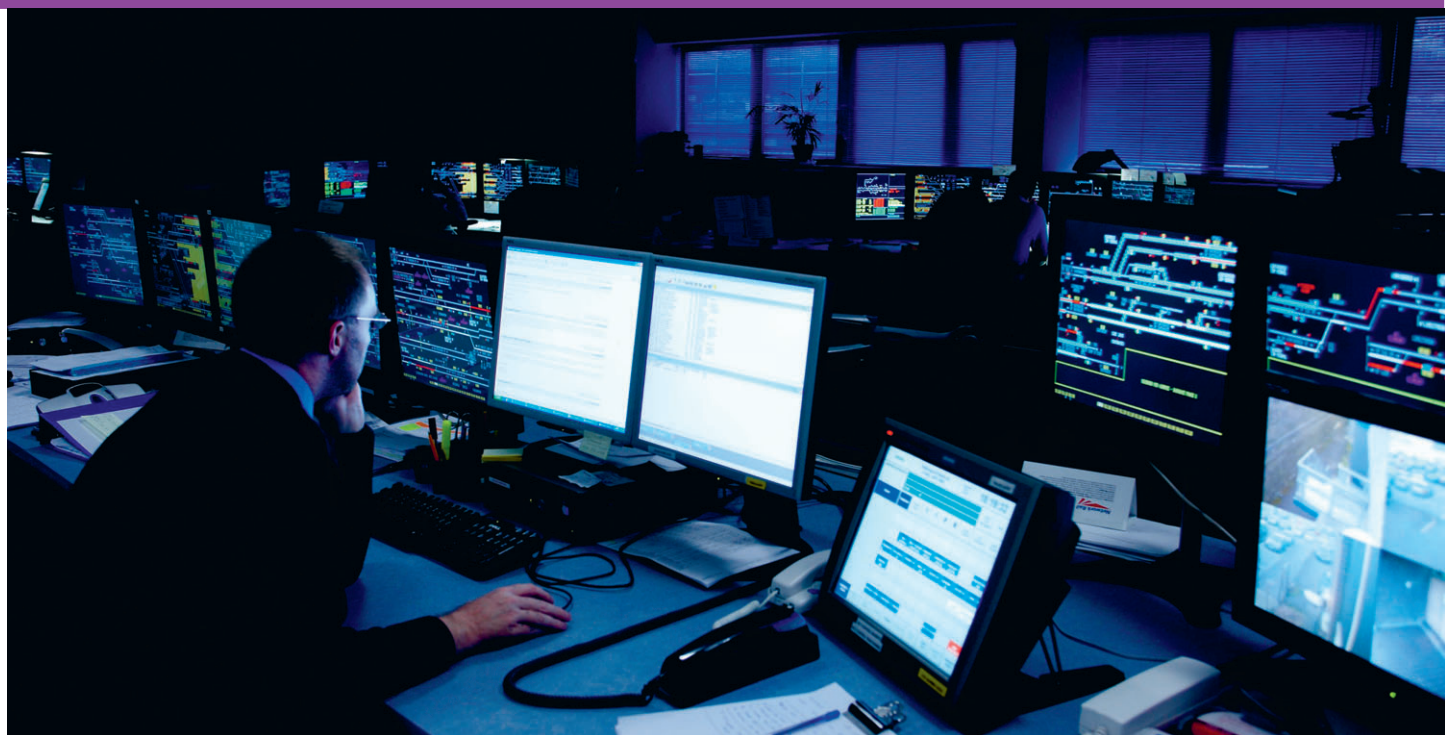

Bild: Siemens

ICT-Sicherheit auslagern?

Chancen, Risiken und Handlungsoptionen | Bei der Migration in die Cloud müssen wir gegen unser Bauchgefühl kämpfen: Der Verlust der Anlage in den eigenen Mauern wird als Kontrollverlust empfunden. Das EU-Projekt «Critical Infrastructure to Cloud Computing» zeigt aber auf, dass die Cloud bezüglich Sicherheit wesentliche Vorteile hat – nicht nur in einem normalen Umfeld, sondern auch bei Leitsystemen.

TEXT BERNHARD M. HÄMMERLI

Die Auslagerung der ICT-Sicherheit wird in der Studie CI2C «Critical Infrastructure to Cloud Computing», in fünf Schritten analysiert: Kann die Sicherheit im eigenen Unternehmen erzeugt werden und was würde das bedeuten? Wie wird die Verfügbarkeit der diversen Optionen von CI2C (intern und Cloud) bewertet? Welchen Einfluss hat die Betriebsgrösse auf die Produktion von ICT-Sicherheit? Was bedeutet heute ICT-Besitztum und weshalb sind auf der ICT-Sicherheitsbühne starke Trends zur De-Globalisierung festzustellen?

ICT-Security selbst erzeugen?

ICT-Sicherheit ist ein Geschäft, das stark von der Expertise abhängt: Je besser die Expertise, umso höher ist auch die Sicherheit. Meist ist das Gebiet der Sicherheit so breit, dass ein Experte alleine nicht alles abdecken kann. Es braucht dazu mindestens drei Profile (Malware-Schutz, Intrusion Management und BCM/DRP). Führende Anbieter von Security aus der Cloud haben jedoch wesentlich mehr Profile verfügbar. Bei einer Sicherheit 24h/7 Tage pro Woche resultiert daraus eine Organisation mit 25 bis 30 Mitarbeitern im Sicherheitsbereich. Es gibt Organisationen, die sich mit Sicherheit von 8–17 h/5 Tage pro Woche begnügen. Aber reicht dies wirklich aus?

Die ICT-Sicherheit während den Ferien und bei Veränderungen (Reorganisation, Umzug, Joint Venture, Akquisition) ist auch zu berücksichtigen. Können die Daten in dieser Zeit richtig geschützt werden?

ICT-Sicherheitsexperten sind grundsätzlich gut, stossen aber immer wieder an spezifische Grenzen. Zudem stellt sich die Frage, wie gut der Zugriff auf 2nd und 3rd Level Support ist. Welche Alternativen bestehen, um Unterstützung zu erhalten, zum Beispiel in einem Information Sharing Network wie Cert, Frist, Melani oder indirekt via Provider?

Es ist klar, dass eine betriebseigene Sicherheitsfunktion mit 1 bis 2 Personen die Anforderungen bei Weitem nicht abdecken kann. Alternativen sind Verträge mit einem Security Operation Center (SOC) für grössere Firmen oder ein «Total Protection»-Angebot eines Produkteanbieters, das im Wesentlichen Cloud-gesteuert ist (Sicherheits-Updates aus der Cloud, Vorfalls-Analysen in der Cloud).

Beispiel Verfügbarkeit

Zur Beurteilung der Verfügbarkeit werden die Resultate der Untersuchung verschiedener Architekturoptionen des CI2C-Projekts verwendet, wie sie von Wissenschaftlern an der Critical Infrastructure Security Conference (10.–12. 10.2016) in Paris vorgestellt wurden. Dabei wurden vier Architekturoptio-

nen des italienischen Energietransportsystems untersucht **(Bild 1)**.

In diesem System werden Remote Units (RU) oder Terminals für Echtzeit-Interventionen bezüglich Spannung zum Regeln der Last und Unterbrechungen eingesetzt. Die Regional Control Centers (RCC) gruppieren und überwachen die RUs in grösseren geografischen Zonen und die zwei National Centers (NC) sammeln Daten und versenden sie nicht zeitkritisch zu den RCCs. Die NCs sind zuständig für die Befehlsplanung sowie die Analyse und Statistik von kritischen Ereignissen.

Vier Architekturoptionen wurden untersucht **(Bild 2)**:

- RU, RCC und NC werden nur mit eigenen und gemieteten Leitungen verbunden (keine Cloud).
- RU, RCC und NC werden alle direkt durch die Cloud verbunden.
- Nur RCCs werden durch die Cloud verbunden, RUs und NCs werden mit eigenen und gemieteten Leitungen verbunden.
- RU und RCC werden mit eigenen und gemieteten Leitungen verbunden, RCC zu NC wird durch die Cloud verbunden.

Die Analyse kam zum Schluss, dass die erste Lösung 2 Tage, die zweite 6 Minuten, die dritte 3 Minuten und die letzte 13 Stunden pro Jahr nicht verfügbar wären. Die Cloud bietet also bezüglich Sicherheit bessere Kommunikationsverbindungen an.

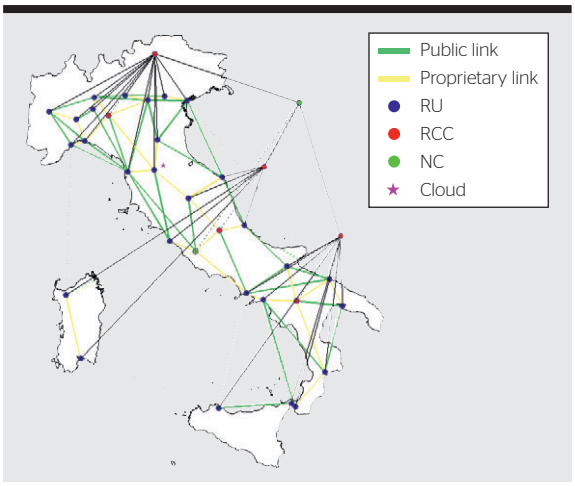

Bild 1 Das italienische Energietransportsystem.

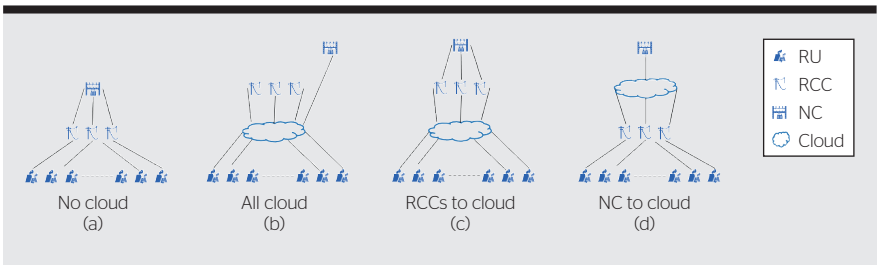

Bild 2 Die vier untersuchten Architekturoptionen. a) keine Cloud, b) direkte Verbindung durch die Cloud, c) nur RCCs werden durch die Cloud verbunden, sowie d) RCC zu NC wird durch die Cloud verbunden.

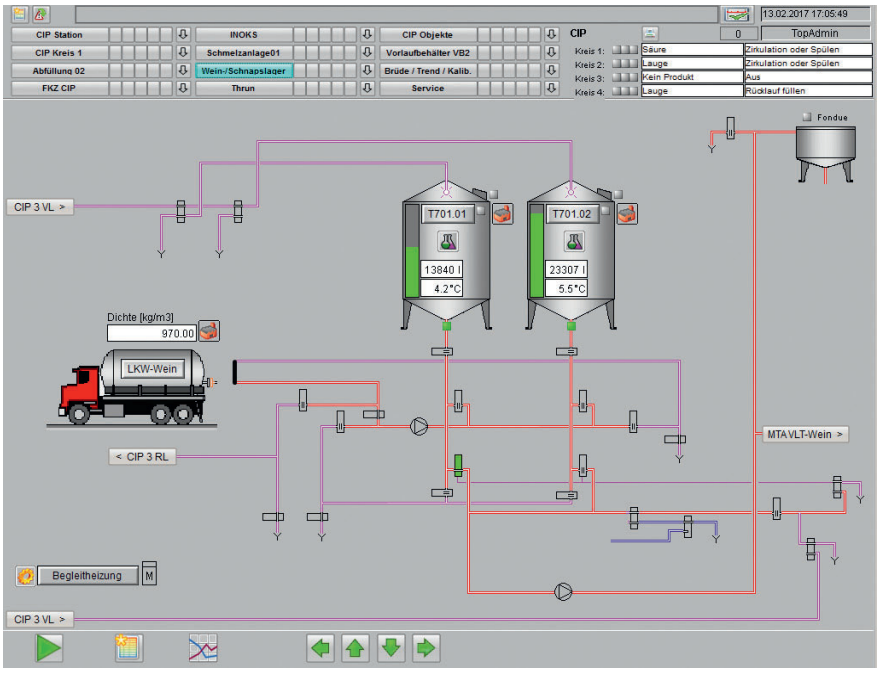

Bild 3 Scada-Leitsysteme kommen in unterschiedlichsten Bereichen zum Einsatz. Beispiel: Lebensmittelbereich (Wein-/Schnapslager).

Security und Betriebsgrösse

Eine spannende Frage ist, ob die Betriebsgrösse einen Einfluss auf den Aufwand zur Sicherung der ICT hat. Muss ein Kleinstunternehmen nur Micro-Security machen und ein Global Player Giga-Security, um das Unternehmen gleich gut zu sichern? Auch Kleinstunternehmen werden von Hackern angegriffen und haben für eine gleich hohe Sicherheit wie ein Global Player ähnlich grosse Aufwendungen. Die ICT-Security skaliert nicht mit der Grösse des Unternehmens. Der einzige Ausweg ist, die Ökonomie der Grösse zu nutzen und die Sicherheitsaufgabe auszulagern.

Was heisst Besitzen in der ICT?

Bei der jungen Generation (unter 25 Jahren) gibt es viele Vertreter, die die Kurzlebigkeit vieler Dinge erkannt haben: Sie wollen nicht mehr besitzen (CD, DVD, Songs, Programme etc.), sondern wollen diese als Service – wenn sie gebraucht werden – mieten. Den Service ohne Ballast geniessen. Die ältere Generation hat noch erlebt, was es hiess, die Hard- und Software zu besitzen. Sie hatte dabei gemischte Gefühle: «gute», weil sie dachte, sie hätte die Kontrolle, «ungute», weil der Service nicht immer den Erwartungen entsprach.

Bilder: Hämmerli

Wie sind heutige Geräte wie Laptops zusammengesetzt, bzw. woher kommen ihre Komponenten? Eine Studie zeigte auf, dass in einem Dell-Laptop Komponenten aus 31 Nationen vorhanden waren. Programme wie Bios, Driver, Betriebssystem und Analysewerkzeuge sind auch potenzielle Quellen für Hintertüren, die bestimmten Dritten Zugriff auf Systeme erlauben. Die möglichen Löcher sind so zahlreich, dass wir davon ausgehen können, dass die eine oder andere Möglichkeit auch ausgeschöpft wird. In der Security-Gemeinschaft wird davon ausgegangen, dass jede Zugriffsmöglichkeit auf fremde Systeme eines Tages auch genutzt wird. Veröffentlichungen, wie die von Snowden, bestätigen bis zu einem gewissen Grad diese Einschätzung. Zusätzlich zu den erwähnten potenziellen Angriffspunkten kommen noch Schwachstellen von Apps, Updates, Sicherheitssoftware und Skriptfiles hinzu. All diese Möglichkeiten lassen sich nicht mit handelsüblichen Produkten absichern. Deshalb haben einige Staaten (u.a. die EU) nun begonnen, eine eigene ICT-Sicherheitsindustrie aufzubauen, um wieder mehr Kontrolle zu erhalten.

Das erwähnte Bauchgefühl, das uns Richtung Besitztum lenkt, kann nach objektiven Kriterien nochmals relativiert werden: Professionelle Services sind besser, 24 h verfügbar und haben mehr Möglichkeiten, um auf 2nd und 3rd Level Support sowie auf Information Sharing Netzwerke zuzugreifen.

Für die Chief Information Security Officers (CISO) bedeutet die Cloud «weg vom Engineering im eigenen Betrieb» und hin zum Aushandeln von Verträgen und «Terms und Conditions». Das bedingt das Zusammenarbeiten mit Juristen und Anwälten. Im eigenen Unternehmen wird sich der CISO vermehrt mit dem menschlichen Faktor und organisatorischen Aspekten befassen, denn diese stellen die Hauptrisiken dar, die nur im eigenen Unternehmen mitigiert werden können. Die Reduktion dieser Hauptrisiken ist wirksam. Mit recht einfachen Mitteln kann viel erreicht werden.

Fazit

Das Konzept «Besitztum» hat heute ausgedient. Zunehmend wird man sich mit Lizenzen und Leasing auseinandersetzen. In einem Markt, in dem die Lebensdauer der Güter nur 2 bis 5 Jahre beträgt, ist das sinnvoll.

Die ICT-Sicherheit skaliert nicht mit der Unternehmensgrösse. Für KMU ist die eigenständige Erzeugung von Sicherheit eine Illusion. Es geht nun darum, glaubwürdige Global Players als Partner auszuwählen, wenn ein abstraktes Servicemodell gewünscht wird. Für ein partnerschaftliches Verhältnis mit einem Sicherheitsprovider gibt es in der Schweiz viele Angebote, bei denen Kundenwünsche berücksichtigt werden. Wichtig ist, dass die Resilience (= Protect – Detect – Response) vom Provider voll abgedeckt wird.

Man sollte sich zudem bewusst sein, dass sich das Cloud-Zeitalter nicht aufhalten lässt: Eine Zeitströmung wie die Cloud Services kann nur verzögert, aber nicht gestoppt werden. Die Cloud ist ebenso wie gekaufte Installationen im eigenen Betrieb Angriffen ausgesetzt. Diesbezüglich sind beide Lösungen leider gleich schlecht. Cloud-Lösungen sind jedoch in allen anderen Punkten bezüglich ICT-Sicherheit überlegen.

Bei der Erpressbarkeit oder im Falle eines politischen Konfliktes liegt das Bauchgefühl richtig. Vorsorge bedeutet hier die Wahl inländischer Lösungsanbieter. Ist das nicht möglich, dann sollte zumindest eine Fallbacklösung auf inländische Anbieter berücksichtigt und vorbereitet werden.

Link
→ www.ci2c.eu

Autor
Prof. Dr. Bernhard M. Hämmerli ist Professor für ICT-Security und Networking an der Hochschule Luzern – Informatik.
→ HSLU, 6343 Rotkreuz
→ bernhard.haemmerli@hslu.ch

Weiterbildungsangebote

Im Kontext der hier behandelten Fragen bietet die Hochschule Luzern folgende Kurse an:

Fachkurs Certified Network Associate CCNA: www.hslu.ch/c125

CAS Cisco Certified Network Professional: CCNP www.hslu.ch/c126

MAS Network Manager: www.hslu.ch/m113

CAS Projektmanagement Informatik/Technik: www.hslu.ch/c185

MAS Information Security: www.hslu.ch/m111

RÉSUMÉ

Délocalisation de la sécurité des TIC

Possibilités, risques et options d'intervention

La migration dans le Cloud peut entraîner une sensation étrange : la perte de l'installation dans ses propres murs est perçue comme une perte de contrôle. Le projet de l'UE « Critical Infrastructure to Cloud Computing » indique toutefois que le Cloud présente des avantages essentiels en termes de sécurité et ce, non seulement dans un environnement normal, mais également en ce qui concerne les systèmes de supervision et de contrôle tels que Scada.

Le fait que la sécurité des TIC ne varie pas en fonction de la taille de l'entreprise représente un vrai défi. Pour les PMU la réalisation autonome de la sécurité est une illusion. Il s'agit plutôt de sélectionner des Global Players dignes de foi en tant que partenaires lorsqu'un modèle de service abstrait est souhaité. Quiconque souhaite entretenir une relation partenariale avec un fournisseur de sécurité dispose de nombreuses offres en Suisse qui permettent au client de présenter ses propres souhaits. Ce faisant, il est important que le fournisseur couvre entièrement la résilience (Protect – Detect – Response). NO