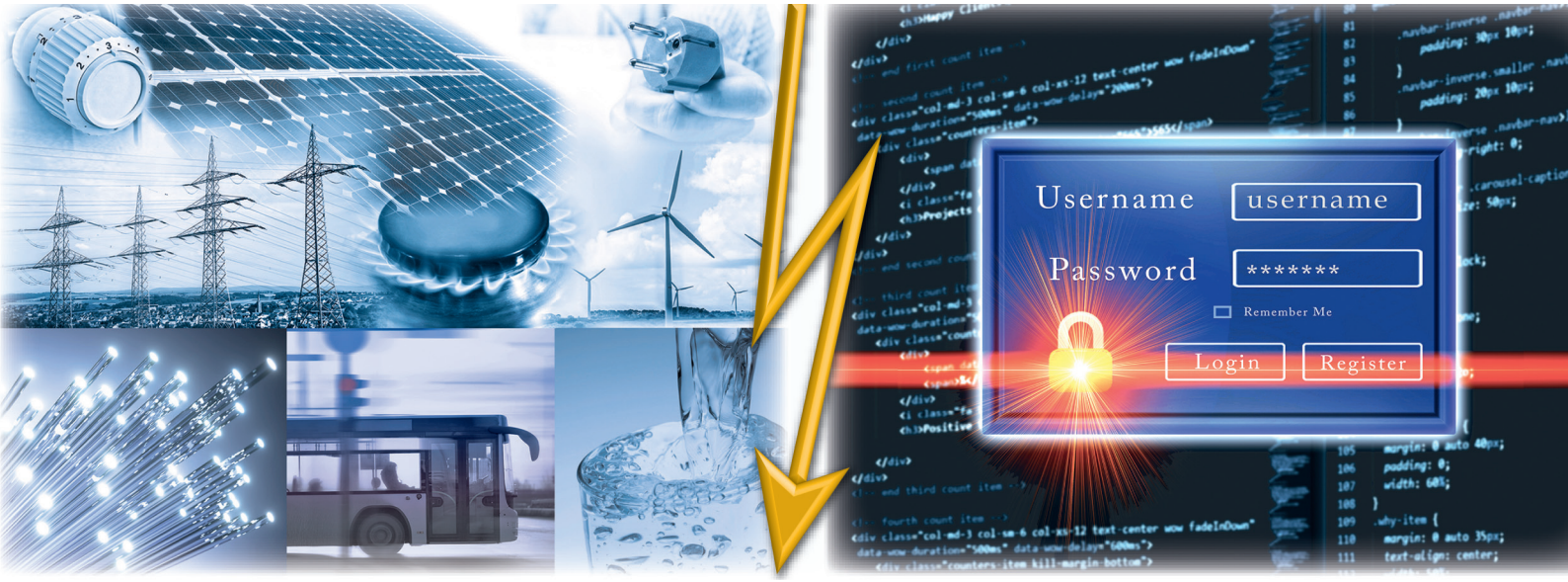


Quelle: Consist Software Solutions

Einerseits Kritis, andererseits Profit Center

Versorgungsunternehmen im Spannungsfeld Datensicherheit

Das Bild des klassischen Energieversorgers hat sich gewandelt. Immer mehr kundenfreundliche Angebote ergänzen das Portfolio vieler Stadtwerke. Einerseits werden so geänderte Marktbedingungen integriert, andererseits müssen dadurch auch gestiegene Anforderungen an die Datensicherheit beachtet werden.

Die Bundesregierung legte mit ihrer Cyber-Sicherheitsstrategie von 2016 den Grundstein für mehr Sicherheit im deutschen Cyber-Raum. Im Fokus dieser Strategie lag die erhöhte Sicherheit und der Schutz von IT-Systemen und -Diensten. Dieser Gedanke galt vor allem den kritischen Infrastrukturen (Kritis) wie Strom- und Wasserversorgung, Gesundheitswesen, Finanzdienstleistungen oder Telekommunikation.

War ein Versorgungsunternehmen bei seiner Gründung ein reiner Produzent von Stromerzeugnissen, ausschließlich Wasserlieferant oder Abfallentsorger, so erstreckt sich die Dienstleistungspalette einiger Versorgungsunternehmen heute auch auf den Betrieb eines Nahverkehrs- und Telekommunikationsnetzes oder öffentlicher Schwimmhallen. Einher gehen Verkauf und Vermarktung dieser Dienstleistungen an den Endkunden. Damit fällt ein Versorgungsunternehmen nicht nur in die Kritis-Kategorisierung Strom- und Wasserversorger, sondern auch in mindestens zwei weitere Bereiche.

Strom- und Wasserversorgung

Die Strom- und Wasserversorgung ist die klassische Dienstleistung eines Versorgungsunternehmens und damit dessen Kerntätigkeit mit gewachsenem, großen Know-how im Unternehmen.

Telekommunikationsdienstleister

Im Zuge der Digitalisierung und Vernetzung der heutigen privaten und wirtschaftlichen Systeme treten verschiedene Versorgungsunternehmen allein oder in Kooperation mit Partnerunternehmen als Telekommunikationsdienstleister auf und versorgen tausende Haushalte mit Internetverbindungen wie Glasfaseranschluss oder herkömmlichen DSL-Leitungen. Üblicherweise gehört auch die Bereitstellung von Telefonie zum Portfolio eines Versorgungsdienstleisters mit Telekommunikationsprodukten. Für Telekommunikationsdienstleister gelten die entsprechenden Telekommunikationsgesetze und -regularien.

Vermarktung und Verkauf an Endkunden

Zur Gewinnmaximierung vermarkten und verkaufen eine große Anzahl von Versorgungsunternehmen ihre Dienstleistung selbst. Im Zuge dieser Tätigkeiten fallen größere kritische Datenmengen aus dem Finanzsektor – wie Bankverbindungen, persönliche Adressen, Liquidation – an. Diese Datenmengen gelten als besonders schützenswert und ihr Verlust ist ein erhebliches Risiko für das Unternehmen.

Die Erweiterung und Veränderung der Dienstleistungen einschließlich der damit verbundenen Geschäftsmodelle ist jedoch bei weitem noch nicht abge-

schlossen. Rund 41 % der Versorgungsunternehmen haben 2016 in einer Studie angegeben, dass sich ihr Geschäftsmodell weiterhin stark verändert. Als Treiber dieser Entwicklung zählt Wirtschaftlichkeit, Klimaschutz, Akzeptanz und Versorgungssicherheit. Vor allem die Digitalisierung wird als größte Herausforderung gesehen, was nicht zuletzt an neuen Gesetzesinitiativen in diesem Bereich liegen dürfte (*Bild 1*) [1].

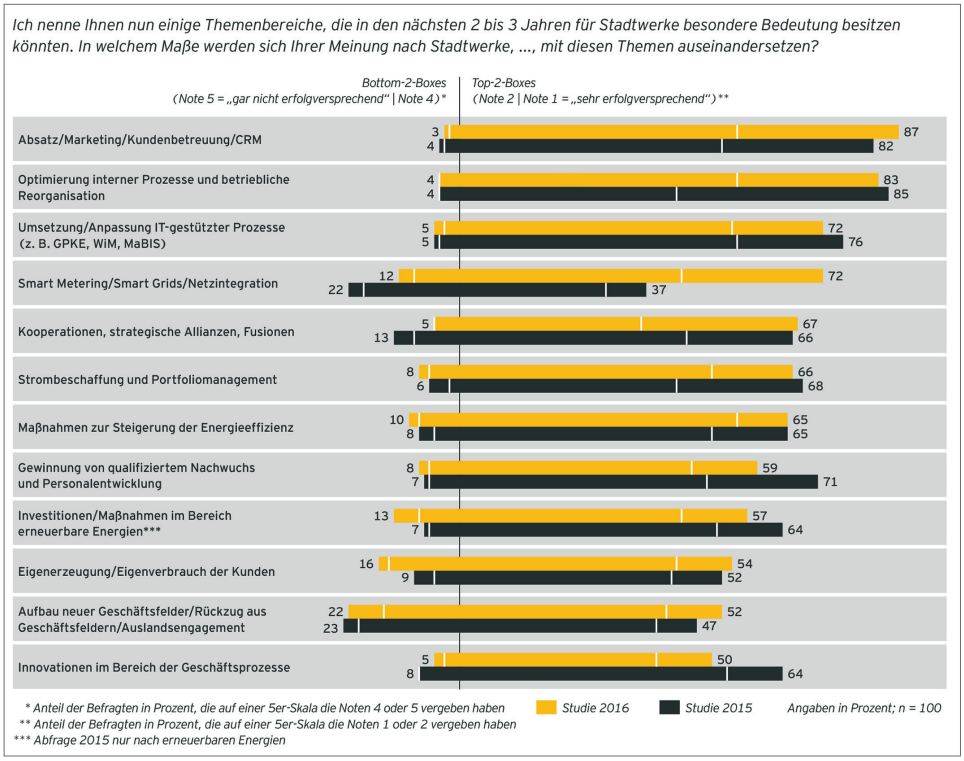


Bild 1. Die wichtigsten Themen für Stadtwerke in den nächsten zwei bis drei Jahren

Gesetz zur Digitalisierung der Energiewende

Bundesregierung und Europäische Union treiben in ihrer Funktion als Gesetzgeber die Versorgungssicherheit vor allem durch neue Regularien und Vorschriften voran. Am 29. August 2016 hat die Bundesregierung beispielsweise ein Gesetz zur Digitalisierung der Energiewende erlassen. Dieses Gesetz ist die wichtigste Grundlage für den Aufbau einer Kommunikationsinfrastruktur in Energieversorgungsnetzen. Die Einführung intelligenter und vernetzter Messsysteme hat das Zähl- und Messwesen grundlegend verändert. Allerdings bringt dieses neue vernetzte Messsystem Herausforderungen bei der Daten- und Netzwerksicherheit mit sich. Bereits in § 2 des Gesetzes weist der Gesetzgeber auf die Anforderungen zur Gewährleistung des Datenschutzes, der Datensicherheit und Interoperabilität in Schutzprofilen hin.

Den geänderten Anforderungen gerecht werden

Wie kann ein Unternehmen, dessen klassische Kernaufgaben nicht in der Erfüllung von IT-Regularien oder Datenschutzaspekten liegen, dem geänderten Gesamtbild des Versorgungsunternehmens als Kritis-Unternehmen gerecht werden? Den Verantwortlichen droht bei Nichteinhaltung der gängigen Standards im IT-Security und Datenschutzbereich enormer finanzieller Schaden. Ab Mai 2018 kann es durch das Inkrafttreten der EU-DSGVO im schlimmsten Fall zu einer Geldstrafe in Höhe von 4 % des weltweiten Umsatzes kommen. Diese angedrohten Ordnungsmaßnahmen sollten jeden Verantwortlichen zum Umdenken bewegen. Zur Bewältigung dieser Aufgaben und Erwartungen gibt es zwei Lösungsvarianten:

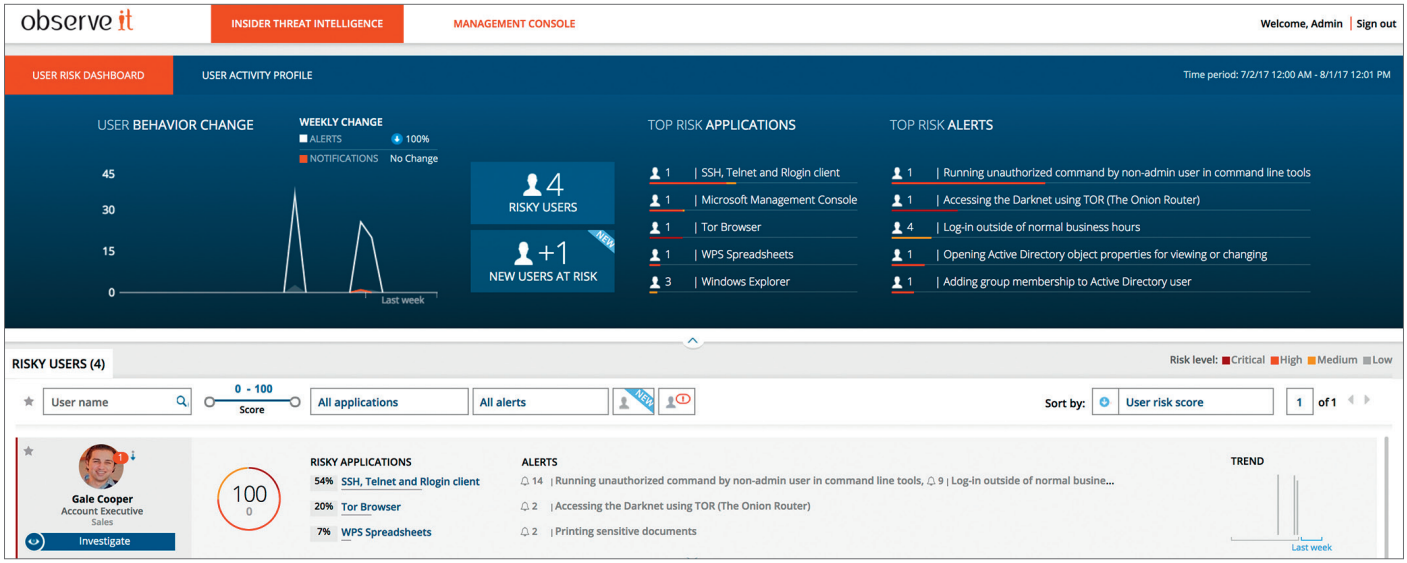
- Auslagerung von Produktverantwortung (White-Label) und Dienstleistungen an einen Partner oder externen Dienstleister
- Aufbau des Security-Know-hows und Implementierung von Sicherheitslösungen sowie Festlegung von Security-Prozessen mit externen Dienstleistern.

Eine Auslagerung von Dienstleistungen und Produkten ist für Versorger nie vollständig möglich. Selbst als ausschließlich klassischer Produzent von Energie fällt ein Versorgungsdienstleister unweigerlich ab einer bestimmten Leistungsschwelle in die Kritis-Kategorie, für die verschärfte IT-Sicherheitsanforderungen gelten. Grundsätzlich gelten für ihn die Bestimmungen des Bundesdatenschutzgesetzes (BDSG). Eine Auslagerung von Dienstleistungen oder Produkten kann aus diesem Grund die Security-Herausforderung im Umfang nur verringern, aber nicht abstellen.

Aufgrund des sehr oft fehlenden IT-Security-Expertenwissens muss in der Regel ein externer Dienstleister bei Aufbau und Betreuung der Security-Prozesse hinzugezogen werden. Vor allem beim Installieren der nötigen Infrastruktur, wie Security Operations Center (SOC) oder dem Sicherheitsinformations- und Ereignismanagement (Siem), wird dieser zur Unterstützung beauftragt. Nach Meinung und Erfahrung von 52 % der deutschen Unternehmen birgt solch eine Beratung und Wartung durch externe Experten ein gewisses Risiko [2, S. 21]. Das Vertrauen in die eigenen Mitarbeiter ist hier deutlich höher. Aus diesem Grund wird eher versucht, das Security-Bewusstsein der Mitarbeiter im Unternehmen zu schärfen, beziehungsweise deren Security-Wissen zu erweitern.

Bedrohung von innen heraus ist größtes Problem

Dieser Aufbau von Security-Wissen ist auch generell zwingend notwendig, denn 71 % aller gemeldeten Datenpannen im Jahr 2016 standen im Zusammenhang mit vertrauenswürdigen Anwendern [2, S. 13]. Hierunter fallen sowohl die externen als auch die internen Mitarbeiter. Diese Innentäter können in jedem Unternehmen mehr Schaden verursachen, als es ein externer Hacker-Angriff oder eine DDoS-Attacke (Distributed Denial of Service/Dienstblockade) jemals könnten. Die Gründe liegen darin, dass oft sowohl der interne als auch externe Mitarbeiter umfassende Rechte für seine Tätigkeiten im Unternehmen benötigt. Beispiele für Personengruppen mit gefährlichen Rechten sind der Datenbankadministrator, der Server-Admin-(SA-)Rechte auf der Kundendatenbank zum Update und Wartung besitzt, oder der Active-Directory-(AD-) Administrator, der zum Anlegen und Verwalten neuer Anwender-Accounts im Unternehmen benötigt wird. Bei einer falschen Verwendung können diese beiden Personengruppen dem Unternehmen enormen Schaden zufügen.



Quelle: ObserveIT

Bild 2. Analyse-Dashboard eines Sicherheitstools

IT-Sicherheit im Einklang mit Mitarbeiterrechten

Jedem diversifizierten Versorgungsunternehmen und Kritis-Unternehmen ist ein Insider-Threat-Programm anzuraten, das beispielsweise auch von der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) innerhalb der Finanzbranche als zwingend notwendig angesehen wird. Die Einführung solcher Insider-Threat-Applikationen, wie der des Marktführers ObserveIT, gestaltet sich jedoch in Unternehmen mit Betriebsräten meist schwierig. Die Gründe liegen in der großen Angst der permanenten Dauerüberwachung der Mitarbeiter. Dies ist jedoch bei einem korrekt konfigurierten Insider-Threat-Programm nicht der Fall. Eine permanente Überwachung würde auch nicht dem BDSG, vor allem der darin geforderten Datensparsamkeit, entsprechen (*Bild 2*).

Neben dem Erkennen von Cyber-Angriffen aufgrund unregelmäßiger, beziehungsweise anormaler Tätigkeiten hoch privilegierter Mitarbeiter, unterstützt ein funktionsfähiges Insider Threat Management Tool bei verschiedenen Schutzzielen, die ab Mai 2018 durch die EU-DSGVO vorgegeben werden. Beispiele hierfür sind die umgekehrte Beweislast, die Verantwortung für Daten und die Verarbeitung durch Fachpersonal.

Umkehr der Beweislast

Künftig muss jedes Unternehmen die Security- und Datenschutzvorgaben nicht nur befolgen, sondern auch belegen, dass seine Mitarbeiter diese einhalten und dies auch in der Vergangenheit getan haben. Der Nachweis der Einhaltung einer Prozesskette mit unterschiedlichen Tools ist kaum möglich. Die Erfassung verschiedenster Tätigkeiten und deren Verknüpfung zur Prozesskette kann nur durch ein Insider Threat Tool datensparsam umgesetzt werden.

Verantwortung für Daten und Verarbeitung durch Fachpersonal

Es muss sichergestellt sein, dass Daten nur auf Anweisung des Verantwortlichen und personenbezogene Daten nur vom Fachpersonal verarbeitet werden. Diese Verarbeitungs- und Zugriffsbeschränkungen werden durch Insider Threat Tools kontrolliert und durchgesetzt.

Anwender in den Mittelpunkt stellen

Um Konformität mit den gängigen IT-Security- und Datenschutzstandards sowie Compliance-Anforderungen zu erreichen, sollten Versorgungsdienstleister deutlich mehr als die einfache Installation von Hardware und Applikationen, wie SIEM, SOC, PIM, Firewalls oder ähnlichen vorsehen. Der Anwender oder Mitarbeiter muss im Fokus der IT-Security-, Datenschutz- und Compliance-Aktivitäten stehen, umgesetzt durch Schulungen und ein Insider-Threat-Programm. Leider wird dies meist vergessen. Dies zeigt die hohe Zahl an Schäden, die durch Innentäter verursacht werden. In Deutschland liegen diese im Durchschnitt bei 3,5 Mio. € [3].

Literatur

[1] Bundesverband der Energie- und Wasserwirtschaft e. V.; Ernst & Young GmbH: Digitalisierung in der Energiewirtschaft. Stadtwerkestudie, Juni 2016.
[2] Bundesamt für Informationstechnik (BSI): Ergebnisse der Cyber-Sicherheits-Umfrage 2016.
[3] Ponemon Institute: Ponemon Institute Research Report 2016 Cost of Data Breach Study: Global Analysis, Benchmark Research Sponsored by IBM. Independently Conducted by Ponemon Institute LLC. June 2016.

Dipl.-Inf. **Dennis Buroh**, Senior Consultant Security, Consist Software Solutions GmbH, Kiel

>> office@consist.de

>> www.consist.de

43424