Informationssicherheitsmanagementsysteme

ISMS bei Energieversorgern

Vor dem Hintergrund der Digitalisierung nimmt das Thema Informationssicherheit für Energieversorger einen immer größeren Stellenwert ein. Um auch im Netzbereich mit der Entwicklung des Energiemarkts Schritt zu halten, wurden und werden in den nächsten Jahren die IT-Systeme der Leitstellen schrittweise mit modernen Leitstellensystemen ausgerüstet. Die damit einhergehende immer stärkere Vernetzung der Netzseite mit dem Rest des Unternehmens ist jedoch auch mit Risiken verbunden.

Mit der Verabschiedung des IT-Sicherheitsgesetzes und der Veröffentlichung des IT-Sicherheitskatalogs 2015 wurden im Kontext der Informationssicherheit zumindest für den Betrieb von Strom- und Gasnetzen die Anforderungen gesetzlich festgeschrieben. Um den aktuellen Wissens- und Umsetzungsstand zum Thema Einführung eines Informationssicherheitsmanagementsystems (ISMS) bei Energieversorgern zu evaluieren, haben die Energieforen Leipzig in Zusammenarbeit mit der Seven Principles AG und der Universität Bayreuth die Studie »Informationssicherheitsmanagementsysteme bei Energieversorgern« durchgeführt (*Bild 1*).

Nur wenige EVU haben aktuell ein ISMS

Das IT-Sicherheitsgesetz sowie der IT-Sicherheitskatalog sind seit Mitte 2015 für Energieversorger Pflicht. In *Bild 2* ist jedoch ersichtlich, dass Anfang 2016 mit 66 % der größte Teil der befragten Energieversorger noch kein funktionierendes ISMS hatten.

Die Gründe, warum noch kein ISMS eingeführt wurde, sind vielfältig. Laut Studie hängt dies damit zusammen, dass sich die Unternehmen in den meisten Fällen noch in der internen Planung und Diskussion befinden oder es als noch nicht notwendig erachten, ein ISMS einzuführen. Meist haben Energieversorger in der Vergangenheit eigene Strukturen und Prozesse für die Informationssicherheit aufgebaut. Diese sind jedoch bei jedem Versorger unterschiedlich, was mit den unterschiedlichen Organisationsstrukturen im Unternehmen zusammenhängt. Demzufolge wurde in der Vergangenheit nach keinem einheitlichen Standard vorgegangen. Daraus resultierend, wird Informationssicherheit aktuell noch in unterschiedlicher qualitativer Ausprägung gelebt.

Einführung eines ISMS mit Einbindung der Mitarbeiter

Die Einführung eines ISMS ist von vielen verschiedenen Faktoren abhängig. Bei Unternehmen, die noch nicht mit der Einführung begonnen haben, gibt es Diskussion in der Geschäftsführung und im oberen Management nach Sinnhaftigkeit und Wirtschaftlichkeit. Die Rückendeckung der Geschäftsführung und des oberen Managements wird jedoch durchgehend als Voraussetzung für ein effek-

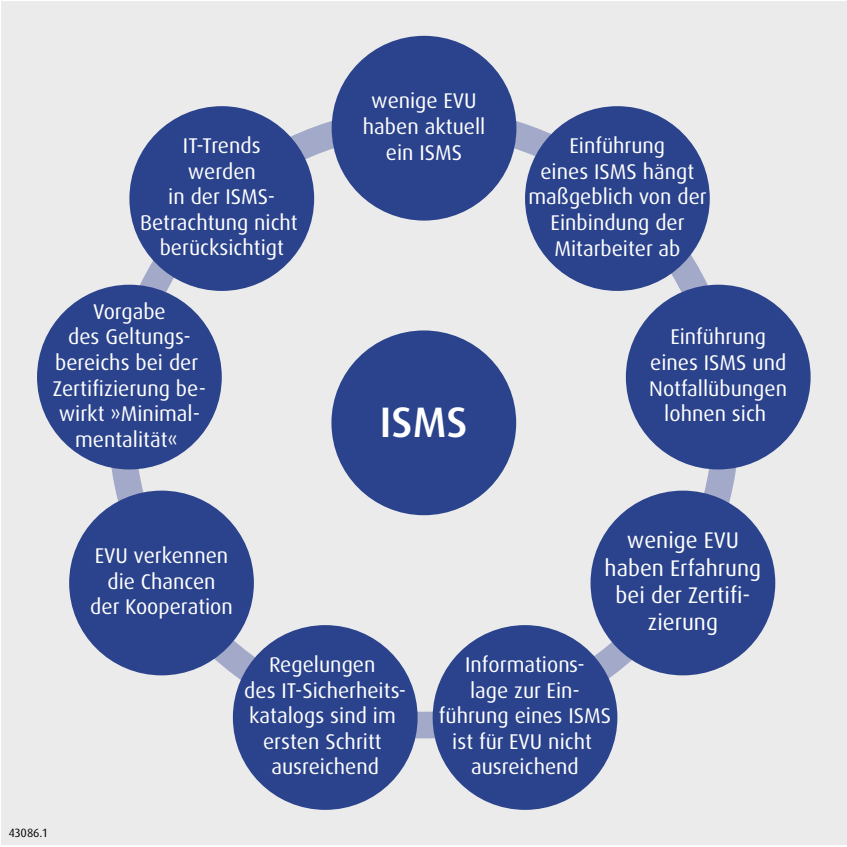

Bild 1. Die wichtigsten neun Erkenntnisse aus der Studie

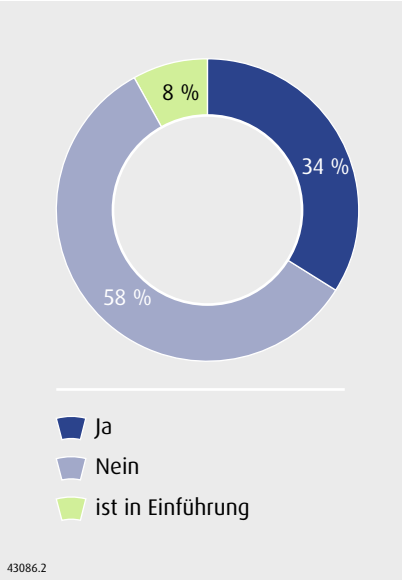

Bild 2. Wurde ein ISMS eingeführt?

tives ISMS angesehen (*Bild 3*). Außerdem werden Aspekte wie Personal und Ressourcen, Definition des Geltungsbereichs des ISMS sowie Aufbau aktueller Dokumentenstände und Erstellung praxisnaher Richtlinien und Arbeitsweisungen als sehr wichtig empfunden. Eine erhöhte Sensibilisierung der Mitarbeiter zum Thema Informationssicherheit ist essentiell. Die meisten Mitarbeiter hatten bislang mit dem Thema Informationssicherheit nur wenig Berührungspunkte. Die neuen organisatorischen Vorgaben im Zuge des ISMS wirken im ersten Moment abstrakt und führen zu Mehraufwand bei den involvierten Mitarbeitern. Daher müssen sie vor der Einführung des ISMS geschult und auf die neuen Prozesse vorbereitet werden. Außerdem muss erläutert werden, warum der höhere Aufwand in der täglichen Arbeit so wichtig ist. Ohne die Sensibilisierung der Mitarbeiter wird die Wirksamkeit eines ISMS im Unternehmen geringer sein.

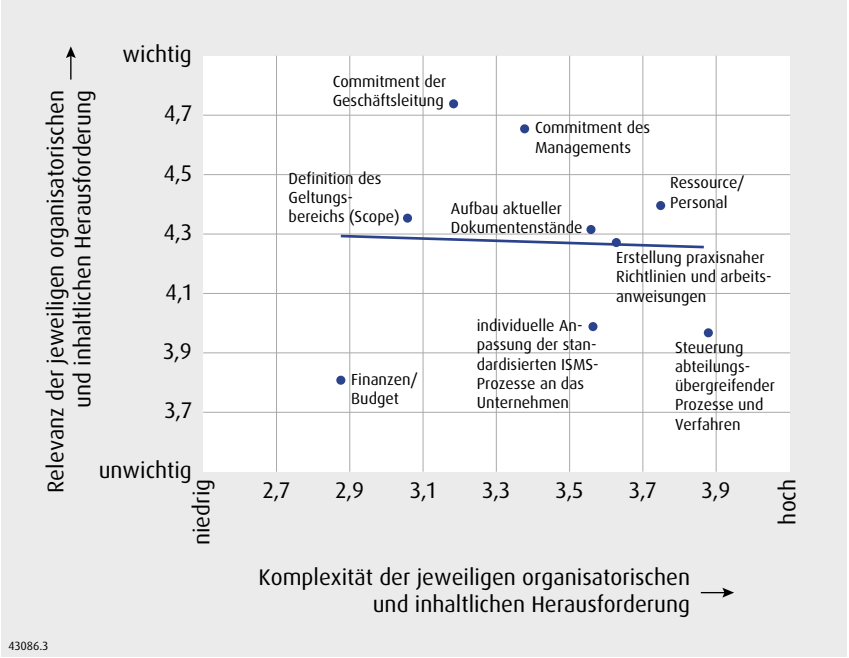

Bild 3. Relevanz der aufgeführten organisatorischen und inhaltlichen Voraussetzungen bei der Einführung eines ISMS

Ein Drittel der befragten Unternehmen hat keine personellen Ressourcen, um Informationssicherheit intensiver voranzutreiben.

Es zeigte sich in der Studie jedoch auch, dass bei einem Drittel der befragten Unternehmen keine personellen Ressourcen vorhanden sind, um dieses Thema intensiver voranzutreiben. Hier liegt der Fokus hauptsächlich auf der Suche nach einem geeigneten Beratungsunternehmen zur Unterstützung bei der Einführung des ISMS. Vielfältige Beratungsangebote machen es für Energieversorger schwierig, den passenden Dienstleister zu wählen. Deswegen vertrauen viele Versorger auf Berater, mit denen schon Projekte in der Vergangenheit im Kontext Informationssicherheit durchgeführt wurden.

Erfahrungen bei der Zertifizierung

Ein weiterer Grund, warum aktuell bei 66 % der Unternehmen noch kein ISMS eingeführt wurde, ist die fehlende Erfahrung beim Thema Zertifizierung. Denn zusätzlich zur Einführung des ISMS muss dieses den Anforderungen der aktuellen Norm ISO 27001 genügen. Selbst bei den Energieversorgern, die ein ISMS eingeführt haben, ließen aktuell nur 30 % der befragten Unternehmen mit ISMS eine Zertifizierung durchführen (*Bild 4*). Verwendete Normen sind hierbei ISO/IEC TR 2019:2013 – sowie die deutsche Vorgängerversion DIN 27009 –, die Vorgängerversion der ISO/IEC 27001:2005 und die ISO/IEC 27001:2013 (DIN ISO/IEC 27001:2015). Insgesamt 85 % der befragten Energieversorger gaben an, dass sie keine für die ISO 27001 ausgebildeten Auditoren in ihrem Unternehmen beschäftigen. Dies hat zur Folge, dass in den meisten Fällen das fachliche Know-how eingekauft werden muss.

Die Unsicherheiten im Zuge der Zertifizierung zeigen sich auch in *Bild 5*. Hier ist die Wichtigkeit der aufgeführten Anforderungen bei der Wahl des Zertifizierungsstandards dargestellt. Für die befragten Unternehmen ist es vor allem wichtig, dass die gewählte Norm den gesetzlichen und regulatorischen Anforderungen entspricht. Als zweiter wichtiger Punkt wird genannt, dass Berater und Dienstleister mit der Norm vertraut sind. Dies ist den Unternehmen wichtiger, als dass eigene Mitarbeiter mit der Norm vertraut sind. Hierbei sind sich Unternehmen, die ein ISMS eingeführt haben, und solche, die es noch müssen, einig.

Chancen durch Kooperation

Die finanziellen Mehrbelastungen durch die verpflichtende ISMS-Einführung sind vor allem für kleine EVU und Netzbetreiber eine große Herausforderung. Durch die fehlende Klarheit der Kostenanerkennung im Rahmen der Anreizregulierung durch die Bundesnetzagentur und die gleichzeitig enorm schwankenden Aufwandseinschätzungen ergeben sich hohe finanzielle Risiken. Darüber hinaus setzt durch die gesetzliche Vorgabe ein Wettrennen um die knapper werdenden Ressourcen an Beratungs- und Zertifizierungsleistung ein. Kooperationen mit anderen EVU bieten sich in dieser Konstellation geradezu an. Dennoch sind 60 % der befragten Unternehmen bei der Einführung eines ISMS nicht zu einer Kooperation bereit (*Bild 6*).

Eine Kooperation bei der Einführung eines ISMS ist durchaus eine Herausforderung, da die verschiedenen Unter-

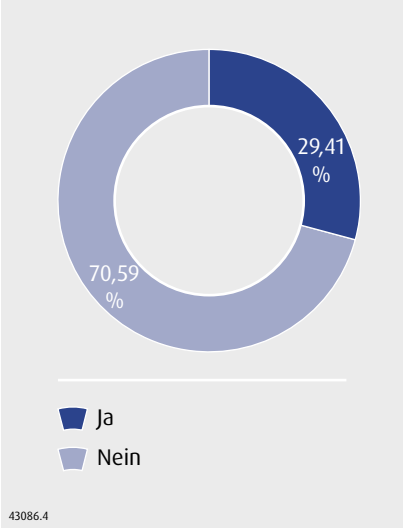

Bild 4. Ist ihr ISMS zertifiziert?

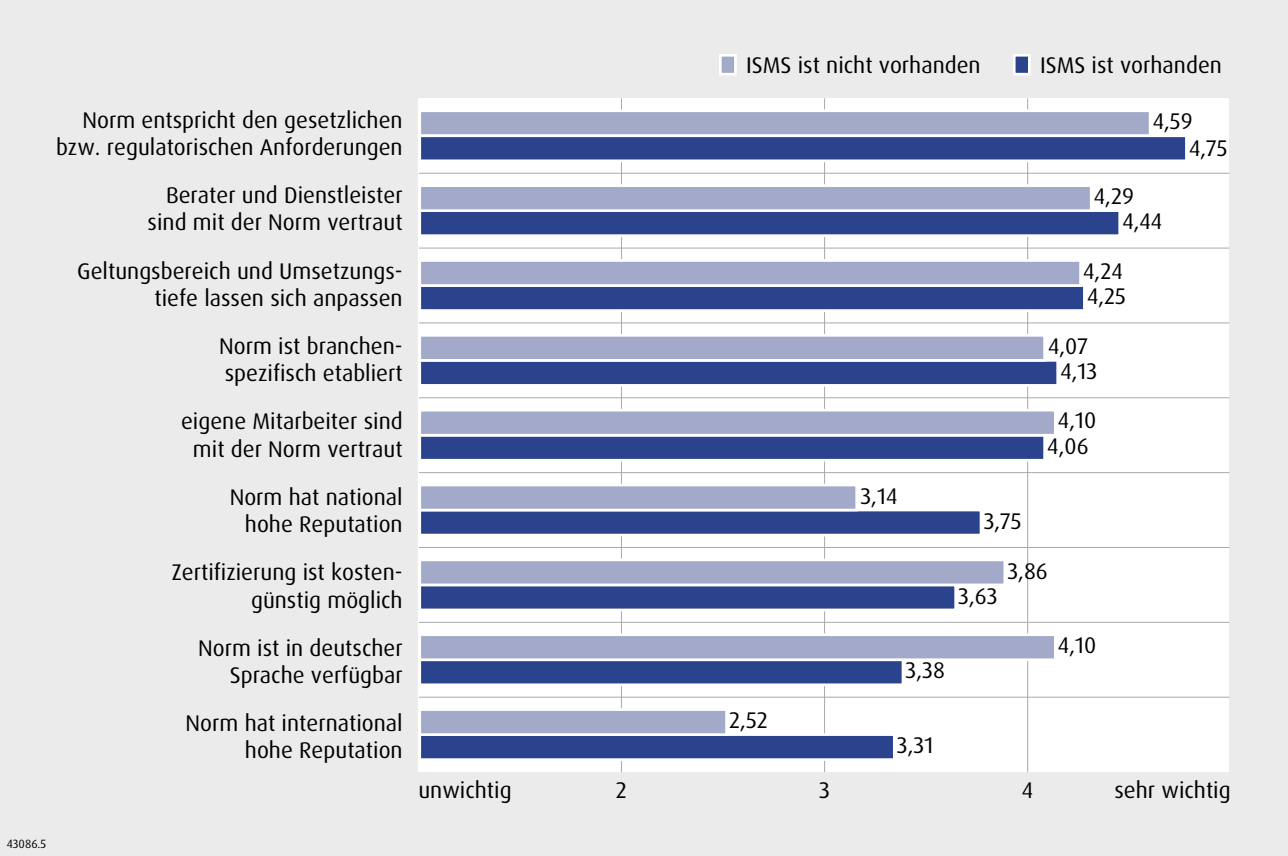

Bild 5. Wichtigkeit der aufgeführten Anforderungen zur Wahl des Zertifizierungsstandards

nehmensstrukturen und Unternehmenskulturen berücksichtigt werden müssen. Dies erfordert ein sehr hohes Maß an Koordination und Kompromissbereitschaft. Daher ist die zurückhaltende Kooperationsbereitschaft nachvollziehbar. Anders sieht es bei der Kooperation im Rahmen der Zertifizierung des ISMS aus. Diese lässt sich leichter koordinieren und bietet trotzdem erhebliches Sparpotenzial.

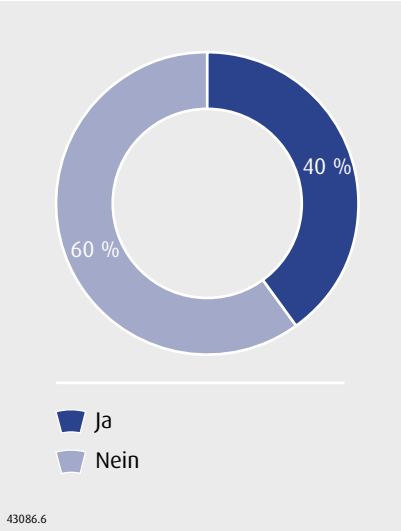

Bild 6. Anteil der geplanten Unternehmenskooperationen im Rahmen der ISMS-Einführung

Besonders wenn sich ganze Unternehmensgruppen für einen gemeinsamen Rahmenvertrag für die Zertifizierung entscheiden, lassen sich die Kosten erheblich reduzieren, ohne an Qualität einzubüßen.

IT-Trends berücksichtigen

Technische Innovationen und Trends vor allem in der Mobilfunktechnologie spielen oft keine Rolle, wenn es um die Betrachtung sicherheitsrelevanter Aspekte geht. Nach Ansicht der Mehrheit der Energieversorger – egal ob ein ISMS vorhanden ist oder nicht – wird beispielsweise die Nutzung persönlicher IT- und Kommunikationsgeräte[1] nicht als Risikoaspekt angesehen (*Bild 7*). Eine Erklärung hierfür könnte sein, dass diese Möglichkeit von vornherein für die Mitarbeiter ausgeschlossen wird, bedarf aber einer einzelfallspezifischen Betrachtung. Diese Vorgehensweise entspricht dem Trend, dass Mitarbeiter – vor allem Führungskräfte –, ihre persönlichen Geräte mit in das Unternehmen bringen, um damit zu arbeiten. Ein gutes Beispiel ist der Geschäftsführer, für den eine Ausnahme eingerichtet wird, damit er mit seinem Tablet das unternehmensinterne WLAN nutzen kann. Solche Ausnahmen sprechen sich in der Belegschaft sehr schnell herum und erodieren die Position des ISMS-Beauftragten und die aufgestellten Regeln.

Aus Sicht des ISMS sind hingegen die digitale Prozessabwicklung sowie eine grundlegende Virtualisierung wichtig. Diese Wahrnehmung deckt sich mit dem Ansatz, den ein ISMS verfolgt, in dem alle digitalen Prozesse auf dem Prüfstand stehen und dokumentiert werden: Cloud Services, mobile Apps, Enterprise Collaboration und das Internet der Dinge (IoT) werden zwar wahrgenommen, spielen in der Risikobetrachtung jedoch keine gesonderte Rolle.

Fazit und Ausblick

Die Ergebnisse der vorliegenden Studie zeigen die Wirksamkeit eines ISMS. Diese Wirksamkeit wird maßgeblich durch den systematischen Prozess zur Analyse einzelner Unternehmensbereiche positiv beeinflusst. Außerdem wird deutlich, dass die Stärkung des Sicherheitsbewusstseins der eigenen Mitarbeiter eine notwendige Voraussetzung für die Wirksamkeit eines ISMS ist. Dieses Sicherheitsbewusstsein ist zur Einführung und im Betrieb eines ISMS in den Vordergrund zu stellen. Die langfristige Sensibilisierung für das Thema IT-Sicherheit im Unternehmen

[1] Bring your own device (BYOD).

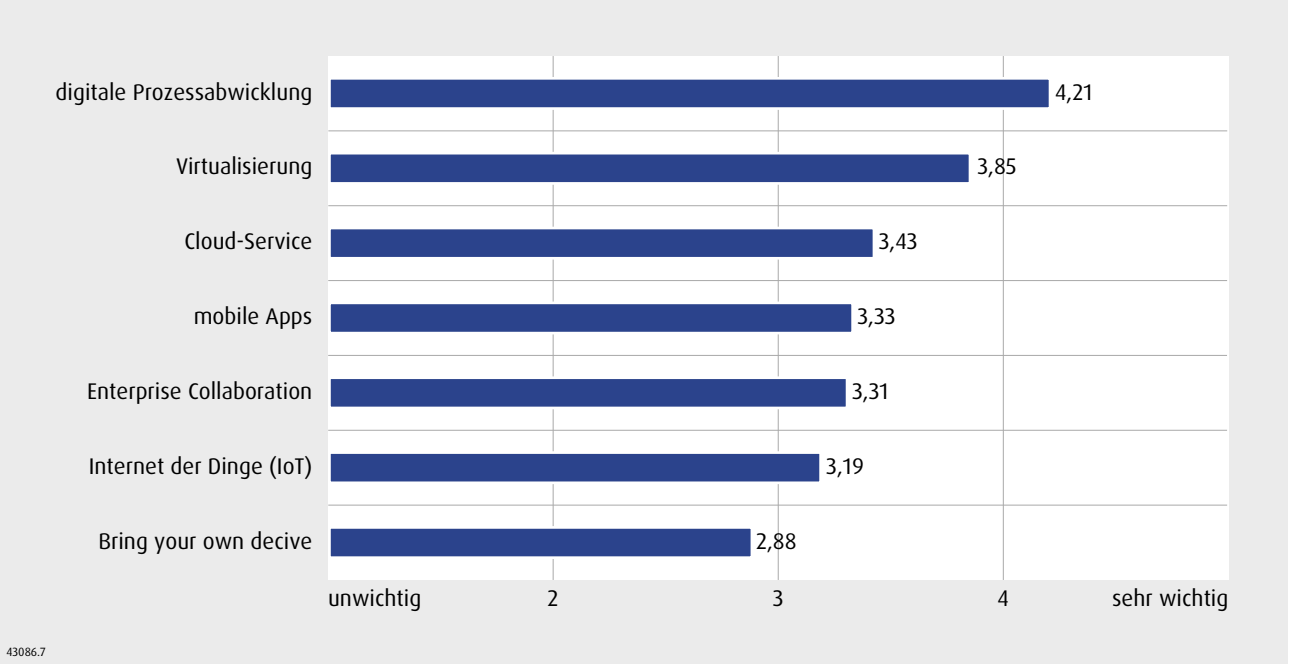

Bild 7. IT-Trends und deren Relevanz für die Informationssicherheit

ist hierbei eine besondere Herausforderung. Die Einführung eines ISMS wird für Energieversorger ein längerfristiger Prozess sein und eine Phase der Transformation in verschiedenen Unternehmensbereichen nach sich ziehen. Daher ist es wichtig, dass die Sensibilisierung zur IT-Sicherheit nicht dem Praxisalltag geopfert wird und dass die Neubewertung und die Modellierung bisheriger Prozesse im Unternehmen in Wechselwirkung stattfinden.

Außer dem Bewusstsein dienen konkrete technische Lösungen der Umsetzung des ISMS. Eine mitunter unüberschaubare Komplexität der historisch gewachsenen Infrastruktur erschwert dies jedoch. IT-Sicherheitskomponenten im Energieversorgungsnetz dienen dedizierten Aufgaben, haben eine eingeschränkte Sichtweise auf das Unternehmensnetzwerk und benötigen daher eine qualifizierte Administration.

Doch auch hier finden sich in der Praxis unterschiedliche Ansätze und ein breit gefächertes Verständnis. Eine von den Unternehmen gewünschte und von den Herstellern versprochene allumfassende Lösung gibt es nicht. Hersteller müssen umdenken und sich dem aktuellen Prozess der Industrialisierung durch geeignete und brauchbare Konzepte stellen. In diesen muss der Sicherheitsgedanke bereits konzeptionell in der Architektur der Systeme, der Software und den Applikationen verankert sein.

Andreas Hänel,
Leiter Kompetenzfeld Analytik und Informationstechnologie, Energieforen Leipzig GmbH, Leipzig

Fabian Wohlfart,
Leiter Kompetenzfeld Erzeugung & Infrastruktur, Energieforen Leipzig GmbH, Leipzig

>> andreas.haenel@energieforen.de
fabian.wohlfart@energieforen.de

>> www.energieforen.de

43086