



# IT-Sicherheit in kritischen energiewirtschaftlichen Infrastrukturen in Deutschland

- Stellenwert der IT-Sicherheit und Sicherheitsanforderungen
- Sicherheitskonzepte und ihre Umsetzung
- Gefährdungsmatrix mit Risikobewertung
- Normen und Standards (z.B. BSI Schutzprofil)
- Strategische Aspekte der IT-Sicherheit
- Markt und Wettbewerb
- Rechtliche und energiewirtschaftliche Rahmenbedingungen in Europa
- Marktpotenziale und -entwicklungen bis 2020
- Profile ausgewählter Wettbewerber

Moderne Informationstechnologie und digitale Vernetzung findet in zunehmendem Maße Einsatz in unserer modernen Gesellschaft. Mit der Umsetzung des Smart-Grid-Konzeptes gilt dies bspw. auch für die Infrastruktur der dezentralen Energieerzeugung, wodurch neue Angriffsflächen für potenzielle Angreifer geschaffen werden.

Während die Energieversorger sich durch die (Verbrauchs-)Datenerfassung, deren Übermittlung und Auswertung (Smart Metering) sowie durch die Fernwartung und -steuerung von netzrelevanten Komponenten (Remote Access) Optimierungen hinsichtlich der Netzinfrastruktur erhoffen, stellen Angriffe aus dem "Cyberspace" auf IT-Infrastrukturen von Kraftwerken eine reale Bedrohung dar. Das Stuxnet-Sabotageprojekt im Jahr 2010, bei dem Industrie- und kerntechnische Anlagen im Iran angegriffen wurden, ließ diese Bedrohung offenbar werden.

Aber auch auf Seiten der Endverbraucher-systeme wie Smart Metering und Smart Home besteht ein potenzielles Sicherheitsrisiko, insbesondere bezüglich des Datenschutzes. So müssen hochsensible Kunden- und Verbrauchsdaten vor Manipulation und Missbrauch geschützt werden. Entsprechend anspruchsvoll sind die aktuellen gesetzlichen Rahmenbedingungen.

Bereits jetzt können elementare IT-Sicherheitsmaßnahmen des IT-Grundschutzes angewandt werden, um einem Großteil der möglichen Bedrohungen effektiv entgegenzutreten. So entwickelte das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Schutzprofil für Smart-Metering-Gateways, das bereits die Problematik in intelligenten Stromnetzen adressiert.

Die trend:research-Potenzialstudie „IT-Sicherheit in kritischen energiewirtschaftlichen Infrastrukturen“ richtet sich an Anlagen- sowie Netzbetreiber, beschreibt und bewertet die potenziellen Gefahren, liefert strategische Lösungsansätze und zeigt ihre Umsetzung in IT-Sicherheitsgesamtkonzepten. Somit ist es möglich, gezielt eigene strategische Pläne auf unterschiedlichen Ebenen (Hardware, Software, Personal etc.) zu entwickeln und in konkrete Maßnahmen zu überführen.

Des Weiteren beantwortet die Studie in diesem Zusammenhang u. a. folgende wichtige Fragestellungen:

- Welche Gefahren bergen die neuen Informations-, Kommunikations- und Datenverarbeitungs-Technologien?
- Wo liegen Bedrohungspotenziale für Energieversorger, wie lassen sich diese bewerten?
- Wie ist der Stellenwert der IT-Sicherheit innerhalb der Energiewirtschaft und bei Energieversorgern anzusehen?
- Wer ist für IT-Sicherheit verantwortlich?
- Welche Anforderungen werden heute an die IT-Sicherheit gestellt?
- Was ist bei der Entwicklung eines Datenschutzkonzeptes zu beachten und wie lässt sich dieses in die bestehende IT-Infrastruktur implementieren?
- Wie lässt sich der Schutzbedarf ermitteln?
- Wie lassen sich kritische Infrastrukturen schützen?
- Welche Rolle spielt der Anwender im Sicherheitskonzept?
- Wie entwickelt sich der Markt, von welchen Faktoren hängt dieser ab?

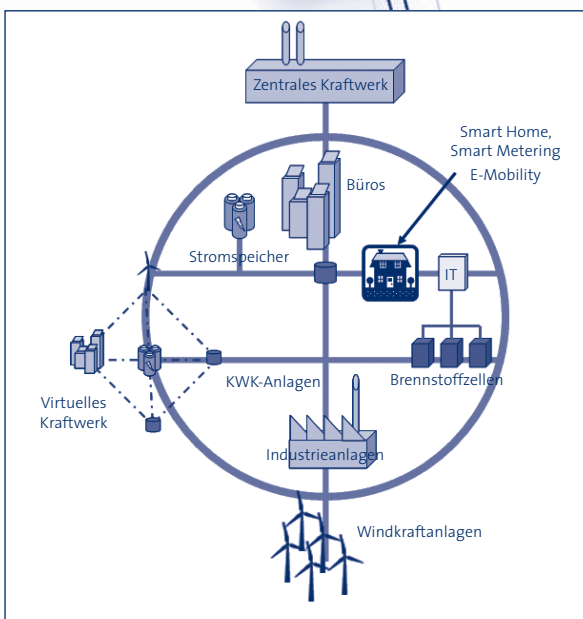


Abbildung 1: Rolle der Informations- und Kommunikationstechnologie im Smart Grid (Quelle: trend:research, 2014; überarbeitete Darstellung, basierend auf Wuppertal Institut, 2012)

## Ziel und Nutzen der Studie

Im Rahmen der Studie werden Antworten auf wichtige Fragen, die im Zusammenhang mit IT-Sicherheit in kritischen energiewirtschaftlichen Infrastrukturen stehen, gegeben. Ausgehend von der Darstellung wichtiger Rahmenbedingungen sowie dem Status quo werden Bedrohungspotenziale und Sicherheitsanforderungen an moderne IT-Konzepte in der Energiewirtschaft aufgeführt.

Es werden die Gefahrenpotenziale auf den Ebenen Hardware, Software, Prozesse und Personal bewertet und der Schutzbedarf analysiert. Dabei werden strategische Aspekte zur Absicherung der IT erläutert und operative Maßnahmen zu ihrer Umsetzung beschrieben (einschließlich Checklisten).

Nach einem Überblick über den Wettbewerb im Markt und einer Darstellung von aktuellen Trends, Chancen und Risiken für unterschiedliche Marktakteure werden hieraus ableitbare mögliche Strategien für die Marktakteure innerhalb der IT-Sicherheit in kritischen energiewirtschaftlichen Infrastrukturen aufgezeigt. Abschließend wird ein Ausblick auf die zukünftig zu erwartenden Entwicklungen gegeben.

## Methodik

trend:research setzt verschiedene Field- und Desk-Research-Methoden ein. Neben umfangreichen Intra- und Internet-Datenbank-Analysen (inkl. Zeitschriften, Publikationen, Konferenzen, Geschäftsberichte usw.) fließen in die Potenzialstudie rund 60 strukturierte Interviews mit folgenden Zielgruppen ein:

- Energieversorgungsunternehmen
- Anlagenbetreiber
- Netzbetreiber
- IT-Dienstleister, IT-Berater
- IT-Hersteller

## An wen sich die Studie richtet

Die Potenzialstudie hilft insbesondere Energieversorgern sowie Anlagen- und Netzbetreibern, aktuelle und zukünftige Risikofaktoren für die IT zu analysieren und die eigene Strategie bzw. die eigenen Maßnahmen vor diesem Hintergrund gezielt auf- und auszubauen. Der Nutzen ergibt sich für Vorstände, Geschäftsführung, Strategie-, Unternehmens- und Konzernplanung sowie IT-Abteilungen, IT-Strategieentwicklung, Risiko-management und Controlling. Für Anbieter von IT-Sicherheitssystemen und IT-Dienstleister ermöglicht die Studie die Einschätzung des Marktpotenzials und der Anforderungen und Bedarfe der Endkunden und unterstützt dadurch den gezielten Marktauftritt. Der Nutzen ergibt sich daher hier insbesondere für Vorstände, Geschäftsführung, Marketing und Vertrieb.

<b>1</b>	<b>Summaries</b>	5.3.2	Verbindlichkeit der IT-Verfahren
1.1	Executive Summary	5.3.3	Verfügbarkeit der IT-Verfahren
1.2	Management Summary	5.3.3.1	Hardware
		5.3.3.2	Software
		5.3.3.3	Informationen
<b>2</b>	<b>Einführung, Methodik und Definitionen</b>	5.3.4	Vertraulichkeit der IT-Verfahren
2.1	Allgemeine Grundlagen	5.4	Anforderungen an die IT-Sicherheit in Leitstellen
2.2	Einleitung	5.4.1	Leistellenmerkmale und -funktionen
2.3	Ziele und Nutzen der Studie	5.4.2	Wesentliche Bedrohungen
2.4	Aufbau der Studie	5.4.3	Sicherheitsanforderungen
2.5	Methodik und Studiendesign	5.4.4	Sicherheitsziele
2.6	Begriffsdefinitionen	5.5	Anforderungen an die IT-Sicherheit aus Sicht der Energieerzeuger und ÜNB
<b>3</b>	<b>Rahmenbedingungen</b>	5.5.1	Peripherie Sicherheitskonzepte
3.1	Energiewirtschaftliche Rahmenbedingungen	5.5.2	Übertragungskanäle (Physikalisch und mit TLS)
3.2	Energiewirtschaftliche IT-Rahmenbedingungen	5.5.3	Umgebung
3.2.1	Bedeutung und Anforderungen innerhalb der IT	5.5.4	Gesicherter Zugang
3.2.2	Status quo bei ERP und Billing	5.5.5	Office Security
3.2.3	Energiedatenmanagement (EDM)	5.5.5.1	Firewalls
3.2.4	Customer Relationship Management (CRM)	5.5.5.2	Patch Management
3.3	Rechtliche Rahmenbedingungen	5.5.5.3	Intrusion Detection Systeme
3.3.1	BDEW Whitepaper	5.5.5.4	Virenschutz
3.3.2	Bundesdatenschutzgesetz (BDSG)	5.5.6	Zertifizierung (nach ISO 27002(-9))
3.3.3	COBIT	5.6	Anforderungen an die IT-Sicherheit aus Sicht der VNB und Lieferanten
3.3.4	Common Criteria (ISO/IEC 15408-1/2/3)	5.6.1	Datenschutz
3.3.5	ISO/IEC 27002	5.6.1.1	Neue Datenschutzanforderungen für EVU in Deutschland
3.3.6	IEC 62351	5.6.1.2	Datenschutzbeauftragte
3.3.7	IT-Grundschutz-Kataloge	5.6.1.3	Beschäftigten- und Kundendatenschutz
3.3.8	IT Infrastructure Library (ITIL)	5.6.1.4	Datenschutz und Smart Metering
3.3.9	NIST SP 800-82	5.6.2	Sicherheit
3.3.10	Signaturgesetz (SigG)	5.6.2.1	Integrität zwecks Netzsteuerung
3.3.11	Telekommunikationsgesetz (TKG)	5.6.2.2	Verfügbarkeit zwecks Netzsteuerung und Abrechnung
3.3.12	Geplantes IT-Sicherheitsgesetz der Bundesregierung	5.6.2.3	Sicherer Schlüsselaustausch
3.3.13	BSI Schutzprofil	5.6.2.4	Reaktionsfähigkeit im Falle von kompromittierten Netzen
3.3.13.1	Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (Smart-Meter-Gateway)	5.6.2.5	Sichere Übertragungskanäle
3.3.13.2	Schutzprofil für das Sicherheitsmodul eines intelligenten Messsystems für Stoff- und Energiemengen	5.6.2.6	Sicherer Datenaustausch in der Marktkommunikation
3.3.14	Weitere	5.6.2.7	Zertifizierte Hersteller
3.4	Behörden und Verbände	5.6.2.8	Zertifizierte Anwender
3.4.1	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM)	5.7	IT-Sicherheit im Bereich Elektromobilität
3.4.2	Bundesamt für Sicherheit in der Informationstechnik (BSI)	5.7.1	Datenschutz in der Elektromobilität
3.4.3	TeleTrusT – Bundesverband IT-Sicherheit e.V.	5.7.2	IT-Sicherheitstechnologien in der Elektromobilität
3.4.4	Weitere	5.7.2.1	Ladesäule
		5.7.2.2	Fahrzeuge
		5.7.2.3	Infrastruktur
<b>4</b>	<b>Status quo</b>	<b>6</b>	<b>Aufbau- und ablauforientierte Betrachtung der IT-Sicherheit</b>
4.1	Stromnetze	6.1	IT-Sicherheit bei Energieversorgern/Netzbetreibern
4.1.1	Netzlänge und -verteilung	6.1.1	Aufbau und Implementierung eines IT-Sicherheitskonzeptes
4.1.2	Ausbau des Stromnetzes	6.1.2	KRITIS – Aufbau eines Sicherheitsmanagementsystems bei EVU
4.1.3	Fluktuierende Einspeisung und Versorgungsqualität	6.1.3	Datensicherheit im Smart Metering und Smart Grid
4.1.4	Versorgungszuverlässigkeit	6.1.4	Sicherheitsstandards und Gefahrenquellen
4.1.5	Netzüberwachung	6.1.5	Cyber-Sicherheit, Wirtschaftsspionage und IT-Sicherheit im Digital Office
4.1.6	Spannungsregelung	6.2	Aufbauorganisation
4.2	Smart Metering	6.2.1	Risikofaktoren und Symptome zum Handlungsbedarf
4.2.1	Einsatz von Smart Metering	6.2.2	Befragungsergebnisse
4.2.2	Aktueller Einsatz	6.2.3	Umsetzungsansätze
4.2.3	Entwicklung des Smart-Metering-Einsatzes seit 2007	6.3	Ablauforganisation: Kernprozesse der Energieversorger und die individuelle Bedeutung im Zusammenhang mit IT-Sicherheit
4.2.4	Einfluss EnWG-Novelle/Schutzprofil	6.3.1	Überblick
4.2.5	Allgemeine Auswirkungen durch verstärkten Smart-Metering-Einsatz	6.3.2	Erzeugung, Beschaffung, Handel
4.3	IT-gestützte Leitstellen-Systeme	6.3.3	Verteilung, Netze, Zählerwesen
		6.3.4	Vertrieb, Abrechnung, Kundenservice
<b>5</b>	<b>Anforderungen an die IT- und Datensicherheit</b>	6.4	Personal
5.1	Aufgabenbereiche der IT-Sicherheit	6.4.1	Risikofaktoren auf Personalebene
5.2	Einschätzung des Sicherheitsbedarfs	6.4.1.1	Unbewusste Verhaltensweisen
5.3	Allgemeine Anforderungen an die IT- und Datensicherheit		
5.3.1	Integrität der IT-Verfahren		

# Infrastrukturen in Deutschland

6.4.1.2	Bewusste Verhaltensweisen	<b>9</b>	<b>Der Markt für IT-Sicherheit</b>	<b>11</b>	<b>Trends, Chancen und Risiken</b>
6.4.1.3	Benutzeridentitäten	9.1	Grundannahmen und Prämissen	11.1	Trends
6.4.1.4	Weiteres	9.1.1	Grundannahmen für alle Szenarien	11.1.1	IT in der Energiewirtschaft
6.4.2	Befragungsergebnisse	9.1.2	Überblick über szenariospezifische Annahmen	11.1.1.1	IT- und Datensicherheit
6.4.3	Zusammenfassung	9.1.2.1	Energiewirtschaftliche Rahmenbedingungen	11.1.1.2	Hardware
<b>7</b>	<b>Hardwareorientierte Betrachtung der IT-Sicherheit</b>	9.1.2.2	Rahmenbedingungen in Hardware, Software und Services	11.1.1.3	Software
7.1	Leittechnik im Netzbetrieb	9.1.2.3	Rahmenbedingungen und Entwicklung in der IT der Energiewirtschaft	11.1.1.4	Organisation und Personal
7.1.1	Netzleitsysteme	9.1.2.4	Entwicklung des subjektiven und objektiven Schutzbedarfs und der Anforderungen an die IT-Sicherheit	11.1.1.5	Markt
7.1.1.1	Netzüberwachungssysteme	9.1.3	Annahmen für Szenario 1: Geringe Marktdynamik und stagnierender Schutzbedarf	11.1.1.6	Wettbewerb
7.1.1.2	Netzstationen	9.1.4	Annahmen für Szenario 2: Beschleunigende Marktdynamik und steigender Schutzbedarf	11.1.2	Trends bei den Marktakteuren
7.1.1.3	Fernwirktechnik	9.1.5	Annahmen für Szenario 3: Beschleunigende Marktdynamik und hochdynamischer Schutzbedarf	11.1.2.1	Trends bei Energieversorgern/Netzbetreibern
7.1.1.4	Schnittstellen zur Energieerzeugung	9.2	Markt und Marktentwicklung in der IT- und Datensicherheit	11.1.2.2	Trends bei IT-Systemanbietern
7.1.2	Datenübertragungssysteme im Netzbetrieb	9.2.1	Markttreiber	11.1.3	Wettbewerbstrends
7.1.2.1	Kabelbasierte Breitband-Übertragungssysteme	9.2.2	Marktbarrieren	11.1.4	Strategietrends
7.1.2.2	DSL	9.2.3	IT-Gesamtmarkt in der Energiewirtschaft	11.1.5	Befragungsergebnisse zu Trends
7.1.2.3	Powerline	9.2.4	Markt für IT-Sicherheit	11.2	Chancen und Risiken
7.1.2.4	Netzwerke (Lokale Netzwerke und Weitbereichsnetz)	9.2.4.1	Branchenneutrale Einschätzungen zur IT-Sicherheit	11.2.1	... für Energieversorger/Netzbetreiber
7.1.3	Drahtlose Übertragungssysteme	9.2.4.2	Gesamtmarkt für IT-Sicherheit in der Energiewirtschaft	11.2.2	... für IT-Systemanbieter
7.1.3.1	Mobilfunknetz	9.2.4.3	Teilmärkte	<b>12</b>	<b>Strategien</b>
7.1.3.1.1	GSM	9.2.4.4	Der Markt für IT-Sicherheit bei Energieversorgern bis 2020	12.1	Strategische Ausrichtung
7.1.3.1.2	GPRS	9.2.4.5	Befragungsergebnisse	12.1.1	Grundlegende Ausführungen
7.1.3.1.3	UMTS	9.2.5	Qualitative Marktentwicklung für IT-Sicherheit in der Energiewirtschaft	12.1.1.1	Strategiedefinition
7.1.3.1.4	LTE	<b>10</b>	<b>Wettbewerb</b>	12.1.1.2	Strategische Ziele
7.1.3.2	Weitere	10.1	Wettbewerb in der Energiewirtschaft	12.1.1.3	Einfluss auf die Rahmenbedingungen
7.1.3.2.1	Bluetooth	10.2	Wettbewerb im Bereich IT-Sicherheit	12.1.1.4	Strategieentwicklung und -formulierung
7.1.3.2.2	DECT	10.2.1	Wettbewerbsstruktur	12.1.1.5	Strategiereview/-aktualisierung
7.1.3.2.3	IrDA	10.2.2	Wettbewerbsintensität	12.1.1.6	Strategieumsetzung
7.1.3.2.4	W-LAN	10.3	Profile ausgewählter Wettbewerber im Bereich IT-Sicherheit	12.1.2	Befragungsergebnisse
7.1.3.2.5	ZigBee	10.3.1	A/V/E GmbH	12.1.3	Prinzipielle Strategieoptionen
7.2	Hardwaresysteme und Kommunikationsstandards	10.3.2	adesso AG	12.1.4	Darstellung der Extrempositionen
7.2.1	Modem	10.3.3	arvato Systems perdata GmbH	12.1.5	Übersicht der möglichen Strategieoptionen
7.2.2	Datensammler/-konzentratoren/-logger	10.3.4	Atos IT Solutions and Services GmbH	12.1.6	Aufzeigen der Entscheidungskriterien
7.2.3	Bus-Systeme	10.3.5	BTC Business Technology Consulting AG	12.2	IT-Richtlinien-Konzept/IT-Sicherheitskonzept
7.2.3.1	M-Bus (kabelbasiert)	10.3.6	C1 CONEXUS GmbH	12.3	Schutzbedarfsfeststellung
7.2.3.2	M-Bus (funkbasiert)	10.3.7	Cisco Systems GmbH	12.3.1	IT-Anwendungen
7.3	Datenübertragung im Bereich Smart Metering und Smart Home	10.3.8	CGI Group Inc.	12.3.2	IT-Systeme
7.3.1	Powerline	10.3.9	COUNT+CARE GmbH	12.3.3	IT-Netze
7.3.2	GSM/GPRS	10.3.10	cronos Unternehmensberatung GmbH	12.3.4	IT-Infrastruktur
7.3.3	Breitband (bspw. DSL)	10.3.11	cst energy services GmbH	12.4	Strategische Sicherheitsleitlinien
7.3.4	Punkt-zu-Punkt-Übertragung	10.3.12	DMS GmbH	12.4.1	Grundlagen
7.4	IT-Systemlösungen	10.3.13	e.dat GmbH	12.4.2	Überprüfung und Anpassung der Strategie
7.5	Energiedatenmanagement und Datenspeicherung von Zählerdaten	10.3.14	Enseco GmbH	12.4.3	Automatisierung versus Individualisierung in der Gefahrenabwehr
<b>8</b>	<b>Forschungsinstitutionen und Pilotprojekte</b>	10.3.15	evu zählwerk Abrechnungs- und Servicegesellschaft mbH	12.4.4	Sicherheit versus Arbeitsfähigkeit/Usability
8.1	Forschungsinstitutionen	10.3.16	FACTUR Billing Solutions GmbH	12.4.5	Notfallkonzepte und -management: IT-Sicherheit als Bestandteil des Risikomanagements
8.1.1	Allianz für Cyber-Sicherheit	10.3.17	items GmbH	12.4.6	Datensicherungskonzept
8.1.2	Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)	10.3.18	Landis+Gyr AG	12.5	Ableitung von strategischen und operativen Maßnahmen
8.1.3	Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL)	10.3.19	LAS GmbH	12.6	Personalstrategien
8.1.4	Nationales Cyber-Abwehrzentrum	10.3.20	numetris AG	12.7	Softwarestrategien
8.1.5	Weitere	10.3.21	prego services GmbH	12.8	Hardwarestrategien
8.2	Forschungs- und Pilotprojekte	10.3.22	regio iT gesellschaft für informationstechnologie mbH	12.9	Weitere Strategieaspekte
8.2.1	IT-Sicherheit für Kritische Infrastrukturen – Bundesministerium für Bildung und Forschung	10.3.23	regiocom GmbH	<b>13</b>	<b>Ausblick</b>
8.2.2	Secure eMobility – Bundesministerium für Wirtschaft und Energie (BMWi)	10.3.24	rku.it GmbH	13.1	Energiewirtschaftliche Entwicklungen nach 2020
8.2.3	(SG) – Smart Grid Security Guidance (A)	10.3.25	RSA Security Inc.	13.1.1	Entwicklung der politischen Rahmenbedingungen
8.2.4	INTEGRA – Smart Grids Modellregion Salzburg (A)	10.3.26	SAP Deutschland AG & Co. KG	13.1.2	Entwicklung der dezentralen Energieerzeugung
8.2.5	Smart Web Grid (A)	10.3.27	secunet Security Networks AG	13.1.3	Entwicklung im Bereich „smarter“ Technologien
8.2.6	Österreichs Energie (A)	10.3.28	Soluvia Billing GmbH	13.1.4	Zukünftige energiewirtschaftliche Herausforderungen
8.2.7	“PRECYSE” – Prevention, protection and reaction to Cyber Attacks to Critical Infrastructures (europaweit)	10.3.29	Steria Mummert Consulting AG	13.2	Entwicklungen im Netzbetrieb und dem Netzmanagement
8.2.8	SPARKS – Smart Grid Protection Against Cyber Attacks	10.3.30	Symantec (Deutschland) GmbH	13.3	Entwicklung des Einsatzes von IKT und IT in der Energieversorgung
8.2.9	HyRiM – Hybrid Risk Management for Utility Providers	10.3.31	VOLTARIS GmbH		
		10.3.32	Weitere		
		10.3.33			

Die Studie wird ca. 600 Seiten umfassen. Aufgrund der laufenden Erarbeitung können sich die Inhalte noch leicht ändern. Inhaltliche Vorschläge können bis zum Ende des Subskriptionszeitraumes aufgenommen werden.

# Faxantwort an 0421 . 43 73 0-11

oder per Post an trend:research GmbH • Parkstraße 123 • 28209 Bremen  
sowie im Internet unter www.trendresearch.de

Hiermit bestellen wir die Potenzialstudie (Nr. 17-0258)

## »IT-Sicherheit in kritischen energiewirtschaftlichen Infrastrukturen in Deutschland«

- als Printversion zum Preis von .....EUR 4.700,00
- als PDF-Version
- mit einer Single-User-Lizenz zum Preis von .....EUR 4.700,00
  - mit einer Multi-User-Lizenz zum Preis von .....EUR 9.400,00
  - mit einer Corporate-Lizenz zum Preis von .....EUR 18.800,00
- und \_\_\_\_\_ zusätzliche Printkopien ..... (je EUR 400,00)

personalisiert auf\* \_\_\_\_\_

- Wir bestellen vor dem **20. März 2014** und erhalten 10% Subskriptionsrabatt.
- Als Besteller der Studie sind wir an der Teilnahme an einem Kick-Off-Workshop (siehe rechts) interessiert. (Bitte beachten Sie, dass nur Anmeldungen vor Ablauf des Subskriptionsrabatts berücksichtigt werden können)..... [Für Studienbesteller kostenfrei]
- Als Besteller der Studie sind wir an einer Vorstellung der Studienergebnisse im Rahmen eines persönlichen Ergebnisworkshops (siehe rechts) interessiert ..... [Preis auf Anfrage]
- Bitte senden Sie uns das **Studienverzeichnis 2014** zu.

So sind wir auf Sie aufmerksam geworden.

- Erhalt dieser Disposition
  - per Post
  - per E-Mail
- Internet
- Empfehlung durch \_\_\_\_\_
- Presseartikel in \_\_\_\_\_
- Sonstiges \_\_\_\_\_

\* Die mit einem Stern gekennzeichneten Felder müssen ausgefüllt werden.

Vorname:\* \_\_\_\_\_

Name:\* \_\_\_\_\_

Funktion: \_\_\_\_\_

Unternehmen:\* \_\_\_\_\_

Straße:\* \_\_\_\_\_

PLZ/Ort:\* \_\_\_\_\_

Tel./Fax:\* \_\_\_\_\_

E-mail:\* \_\_\_\_\_

- Wir sind **nicht** damit einverstanden, den Newsletter von trend:research zu erhalten.

Datum

Unterschrift/Stempel

## trend:research

Trend- und Marktforschungsstudien werden von trend:research aktuell und exklusiv erarbeitet. Umfangreiche eigene (Primär-)Marktforschung, gemischt mit Erfahrungen und Wissen aus liberalisierten Märkten, aufbereitet mit eigener Methodik, führen zu nachvollziehbaren Aussagen mit hohem Wert. Die Schwerpunkte sind Untersuchungen in sich stark wandelnden Märkten, z. B. in den liberalisierten Energie- und Entsorgungsmärkten.

trend:research liefert Studien, Informationen und Untersuchungen an über 90 % der größeren EVU und unterstützt damit existenzielle Entscheidungen – die Referenzliste erhalten Sie auf Anfrage.

## Kick-Off-Workshop

Im telefonischen Kick-Off-Workshop werden Methodik und Ziele der Studie vorgestellt und eine inhaltliche Fokussierung mit dem teilnehmenden Unternehmen diskutiert.

## Ergebnisworkshop

Im Ergebnisworkshop werden die Kernergebnisse der Studie vorgestellt und diskutiert. Eine inhaltliche Fokussierung der Vorstellung für das teilnehmende Unternehmen ist möglich. Der Ergebnisworkshop ermöglicht darüber hinaus durch gezielten und engen Erfahrungsaustausch die Ausgestaltung und Konkretisierung von Lösungsansätzen im eigenen Unternehmen.

## Konditionen

Die Potenzialstudie »IT-Sicherheit in kritischen energiewirtschaftlichen Infrastrukturen in Deutschland« kostet je nach Wahl als Printversion (persönliches Exemplar) EUR 4.700,00. Die **Single-User-Lizenz** (personalisierte, passwortgeschützte CD-Rom mit geschütztem PDF) kostet EUR 4.700,00. Die **Multi-User-Lizenz** (bis zu 10 personalisierte, passwortgeschützte CD-Roms mit geschütztem PDF) kostet EUR 9.400,00. Die **Corporate-Lizenz** (CD-Rom mit freigegebenem PDF) kostet EUR 18.800,00. Zusätzliche Printkopien (Verwendung nur innerhalb des Unternehmens) stellen wir Ihnen für EUR 400,00 zur Verfügung. Alle Preise verstehen sich zzgl. der gesetzlichen Mehrwertsteuer. Zahlungsweise ist per Überweisung oder Scheck innerhalb von 14 Tagen nach Rechnungsstellung. Bei Bestellung bis zum **20. März 2014** gewähren wir Ihnen einen Subskriptionsrabatt von 10%. Bei gleichzeitiger Bestellung anderer Studien (s. u.) bieten wir Ihnen 10% Mengenrabatt. Die Studie ist ab **Juni 2014** verfügbar.

## Weitere Studien

trend:research gibt weitere Studien heraus, z. B.:

- IT-Strategien in der Energiewirtschaft**  
geplant, ca. 600 Seiten, EUR 4.700,00
- Smart Home 2.0 (2. Auflage)**  
August 2013, 983 Seiten, EUR 4.900,00
- Stromspeicher: Chancen und Risiken für Stadtwerke, Hersteller und Verbraucher – in Kooperation mit ZfK –**  
Mai 2013, 1.126 Seiten, EUR 7.500,00
- Smart Grids (3. Auflage): Netzintegration Erneuerbarer Energien – in Kooperation mit ENERGIE&MANAGEMENT –**  
Dezember 2009, ca. 800 Seiten, EUR 4.200,00
- Dezentrale Energieerzeugung in Deutschland bis 2030**  
Juli 2012, 620 Seiten, EUR 7.900,00
- Straßenbeleuchtung 2020 (2. Auflage)**  
Dezember 2009, ca. 800 Seiten, EUR 4.200,00

Weitere Informationen können Sie mit diesem Formular anfordern oder im Internet unter [www.trendresearch.de](http://www.trendresearch.de) abrufen.

© trend:research, 2014

**trend:research**  
Institut für Trend- und Marktforschung

- Bremen
- Bremerhaven
- Köln
- Stuttgart