Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrusT, bevh und BISG

Berlin, 29.11.2016

Umsetzung des IT-Sicherheitsgesetzes in der Praxis am Beispiel eines Energieversorgers

Rolf-Dieter Kasper, innogy SE

innogy

1

Implementierung eines ISMS nach dem BNetzA SiKat (für Energienetzbetreiber; Ausgabe August 2015)

2

Umsetzung der Sicherheitsmaßnahmen aus dem ISMS

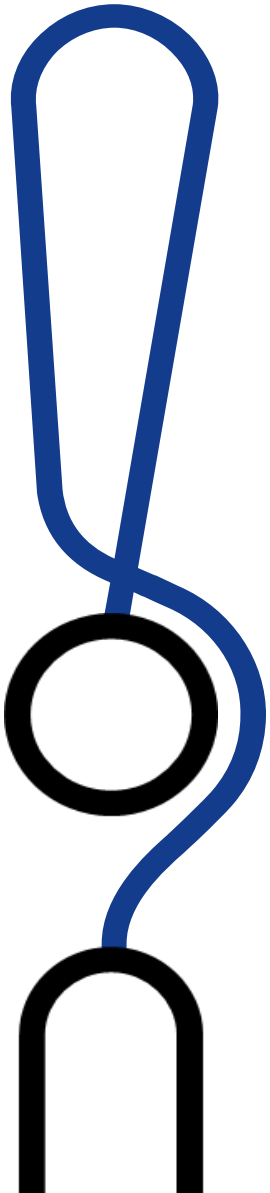
3

Zertifizierung des ISMS für Energienetzbetreiber

4

Ausblick: IT-SIG 2.0 ?

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG)



- Das am 25.7.2015 im Bundestag verabschiedete Gesetz richtet sich an alle KRITIS-Branchen in Deutschland (u.a. Energie, Verkehr, Telekommunikation)
- Zwei Jahre Umsetzungsfrist und alle zwei Jahre Nachweis der Erfüllung (z. B. durch Audits/Zertifikate z. B. nach ISO/IEC 27001).
- Der Sicherheitskatalog [§11, 1a EnWG] der Bundesnetzagentur wurde im August 2015 veröffentlicht
- Ausgestaltung der VO zur Bestimmung Kritischer Infrastrukturen in Q2/2016 mit sofortiger Wirksamkeit bzgl. der Meldepflicht für Kritische Energieanlagen- und Netzbetreiber [§11, 1c EnWG]

1 IMPLEMENTIERUNG EINES ISMS NACH DEM BNETZA SIKAT

Scoping

EnWG §11 Abs 1.a: … auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind.

BNetzA SiKat 08/2015: … Enthalten sind demnach zumindest alle TK- und EDV-Systeme des Netzbetreibers, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Daneben sind auch TK- und EDV-Systeme im Netz betroffen, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte…

Relativ einfach zu bestimmen

Je nach Größe der Organisation kann das beliebig komplex werden

Anforderungen an das Risikomanagement nach BNetzA SiKat (08/2015)

innogy

- Die allgemeinen Anforderungen an den Prozess zur Risikoeinschätzung sind in Kapitel 6.1.2. der DIN ISO/IEC 27001:2015-3 geregelt.
- Für die Komponenten, Systeme und Anwendungen, die für einen sicheren Netzbetrieb notwendig sind, ist grundsätzlich von einer Einstufung in die Kategorie „hoch“ auszugehen. Im Einzelnen ist zu prüfen, ob ggf. eine Einstufung als „kritisch“ notwendig ist…

Die meisten Beispiele betreffen einen Grundschutz der Kategorie „normal“

- Zusätzlich zu berücksichtigende Schadenskategorien u.a.
  - Beeinträchtigung der Versorgungssicherheit,
  - Einschränkung des Energieflusses,
  - Betroffener Bevölkerungsanteil,
  - Auswirkungen auf weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung),

Ein normales ISMS betrachtet Einflüsse , die keine direkten Rückwirkungen auf die eigene Organisation haben nicht weiter. Hier sind Methoden der Umsetzung zu entwickeln

- Erkannte Risiken sind i. d. Regel durch Maßnahmen nach dem allgemein anerkannten „Stand der Technik“ zu behandeln

Da ist eine hohe Anforderung für eine Flächeninfrastruktur mit einen Life-Cycle größer 25 Jahren

ISMS Regelwerk: Die wichtigsten Regelungen…

innogy

ISMS-Basisdokumente:

- ISMS Rahmenrichtlinie
- ISMS Geltungsbereich
- ISMS Policy Gesetze+Verordnungen.pdf
- ISMS Dokumentenlenkung
- Operative ISMS-Policy
  - Anhang 1 Gen. Risiken
- ISMS PBC Process Baseline Controls
  - Anhang 1 Klassifizierung vertr. Inf.
  - Anhang 2 Krypto-Verfahren
  - Anhang 3 Standortklassifizierung
  - Anhang 4 Aufbewahrungsfristen
  - Anhang 5 Erstellung Netzstrukturplan
- Lieferanten Management
  - OE_BDEW Whitepaper Secure Systems (DE/EN)
  - OE_BDEW_WP-Ausführungshinweise
  - ISMS DLR der Gruppe (DE /EN)
- ISMS Statement of Applicability

Integration

ISMS-Umsetzungsdokumente:

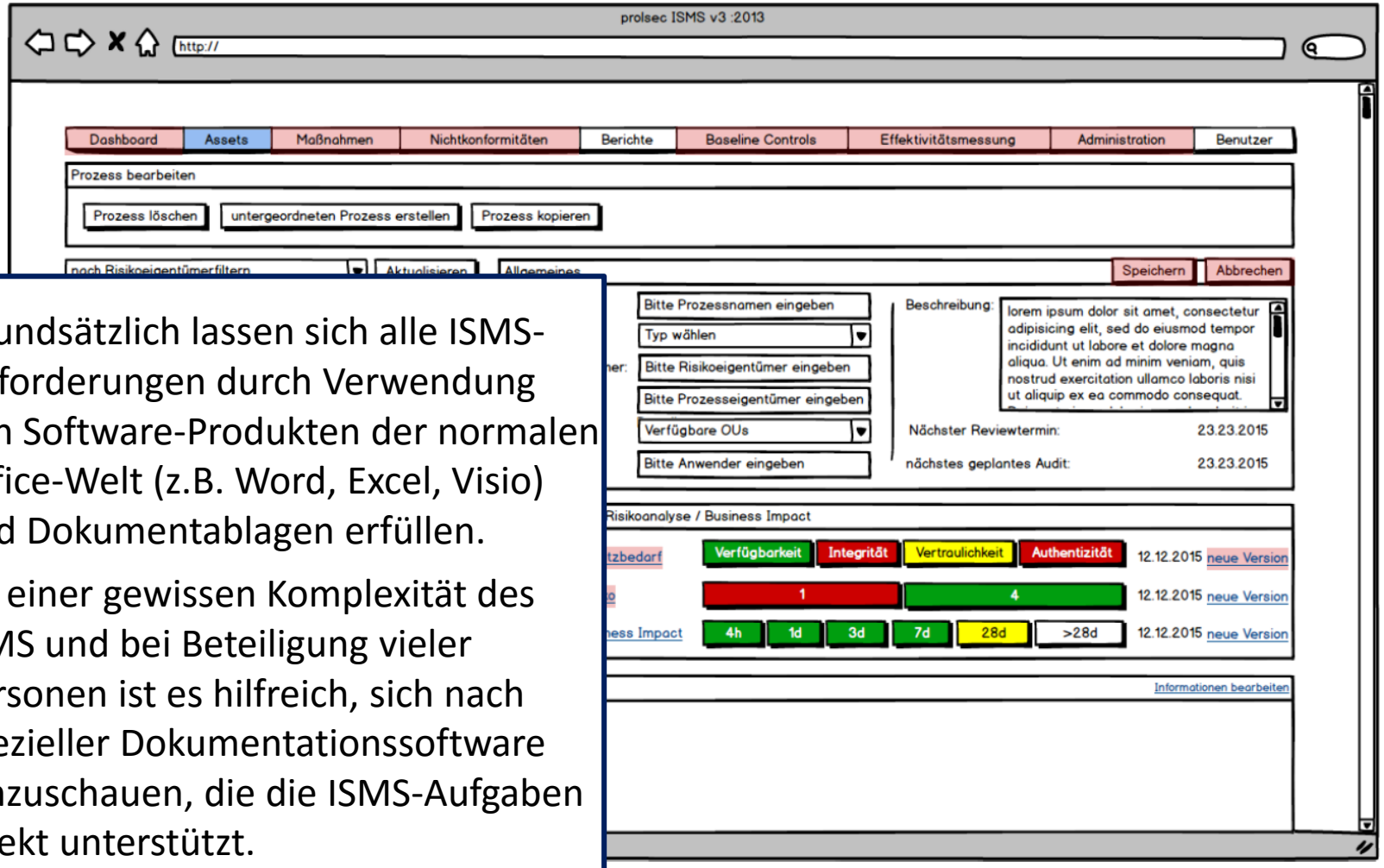
- ISMS-Assetverzeichnis
- Schutzbedarfsfeststellungen und Risikoanalysen des ISMS-Assets
- Risikobehandlungsplan/Maßnahmenliste
- Auditplanung /Auditdokumente
- Dokumentation der Behandlung der Security-Incidents
- Reporting an das Management inkl. Darstellung der Restrisiken
- Ziele des ISMS Prozesses, Dokumentation der Verbesserungen und Schulungen

Fachregelwerke

- Planungs- und Betriebsgrundsätze bzw. -richtlinie (z.B. Change- und Incident-Management)
- Betriebskonzepte für Systeme oder Dienste
- Betriebshandbücher

ISMS Werkzeuge

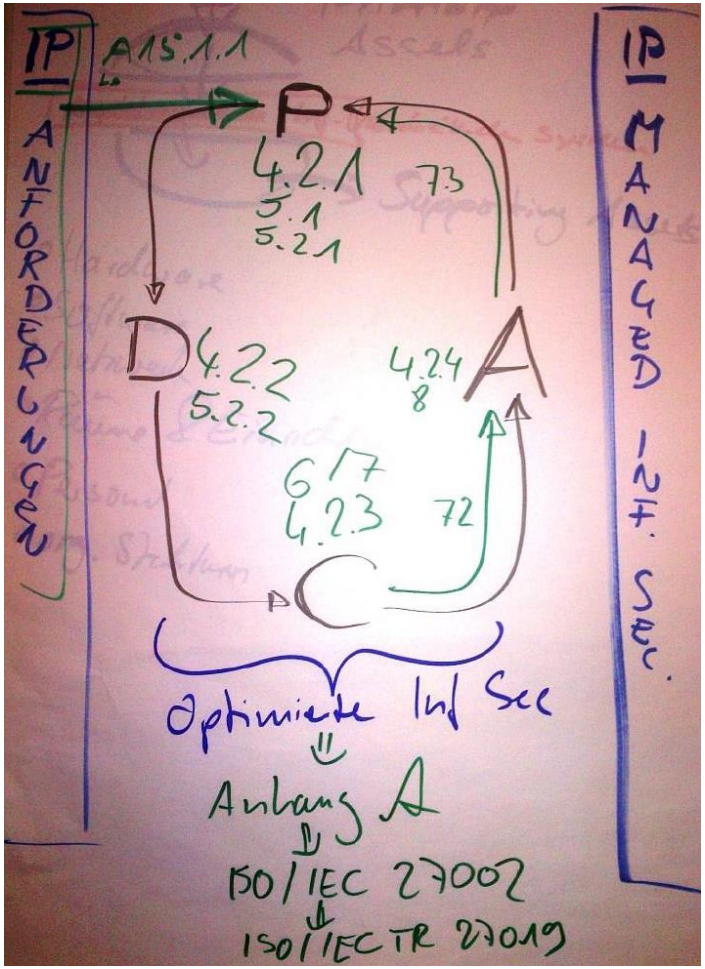
innogy



- Grundsätzlich lassen sich alle ISMS-Anforderungen durch Verwendung von Software-Produkten der normalen Office-Welt (z.B. Word, Excel, Visio) und Dokumentablagen erfüllen.
- Ab einer gewissen Komplexität des ISMS und bei Beteiligung vieler Personen ist es hilfreich, sich nach spezieller Dokumentationssoftware umzuschauen, die die ISMS-Aufgaben direkt unterstützt.

Schulungen

- Schulungen für Sicherheitsexperten
  - ISMS Lead Auditor: ISO27001:2013
  - ISMS Implementierung: ISO 27001:2013
  - Technisches Know-How für ISMS-Beauftragte und Auditoren
  - Hacking & Penetration Testing
- Schulungen Mitarbeiter im Scope des ISMS
  - Interne Schulungstage und Workshops mit eigenen und externen Experten
  - Z.B: Social Engineering und Security Awareness
- Schulungen für alle Mitarbeiter
  - Schulung „über die Line“
  - Aktuelle Cybersicherheitskampagne: “The Human Firewall“



Cybersicherheitskampagne: “The Human Firewall“

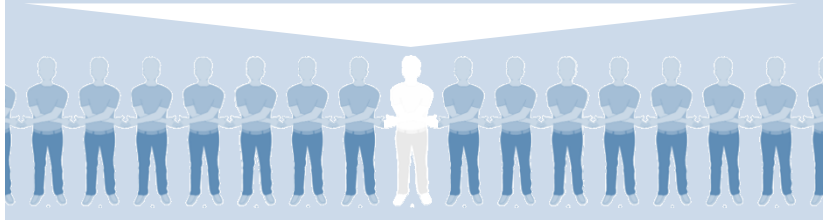
5 + 1 Schwerpunkte

Cybersicherheitskampagne: “The Human Firewall“
10 konkrete Maßnahmen

innogy

Mitarbeiterengagement ….	
1. Online Quiz	Messen des Sicherheits-bewusstseinsgrades
2. Simulierte Phishing Aktion	Phishing-Aktion, um die Mitarbeiter zu sensibilisieren und ihnen Tipps zu geben
3. E-Learning	Webbasiertes Tool zur Schulung der Mitarbeiter
4. Lunch & Learn	Interaktives Ereignis mit praktischen Tipps für die Cyber-sicherheit
5. Foto-Aktion	Mitarbeiter motivieren, ein visueller Teil der Firewall zu werden

…begleitet durch Kommunikationsmaßnahmen	
6. Online Video	Betonung der Bedeutung von Cybersicherheit
7. Promotion Artikel	Verschiedene Kommunikationsmaßnahmen
8. Gestaltungs-möglichkeiten	Posters, Flyers und Give-aways
9. Website	Intranet-Auftritt als Plattform zur Präsentation der Kampagne
10. Angriffs-statistik	Intranet-Dashboard zur Darstellung der aktuellen Intensität von Cyberattacken



Mehr Wissen und Bewusstsein resultiert in einer höheren Cybersicherheit!

2 UMSETZUNG DER SICHERHEITSMASS-NAHMEN AUS DEM ISMS

Implementierung der ISMS-Controls im Regelwerk der technischen Fachbereiche

innogy

Umsetzung der Forderung ISO/IEC 27001 Kap 5.1 b („Die oberste Leitung muss sicherstellen, dass die Anforderungen des ISMS in die Geschäftsprozesse der Organisation integriert werden“)

- Planungs- und Betriebsgrundsätze bzw. -richtlinie (z.B. Change- und Incident-Management)
  - Inhalt: Verstehen der Organisation und ihres Kontextes; Verstehen der Erfordernisse und Erwartungen interessierter Parteien; Maßnahmen zum Umgang mit Risiken und Chancen
- Betriebskonzepte für Systeme oder Dienste
  - Inhalt: Die Betriebskonzepte der ISMS Assets enthalten die spezifischen Dienstausprägungen und Sicherheitsmaßnahmen, die für den Betrieb relevant sind.
- Betriebshandbücher
  - Inhalt: Die Betriebshandbücher setzen die Anforderungen der Betriebskonzepte praktisch um und enthalten die geltenden Regelung für den Betrieb und die dazugehörigen Betriebsaufzeichnungen als Anlagen oder Verweise

Interne Audits

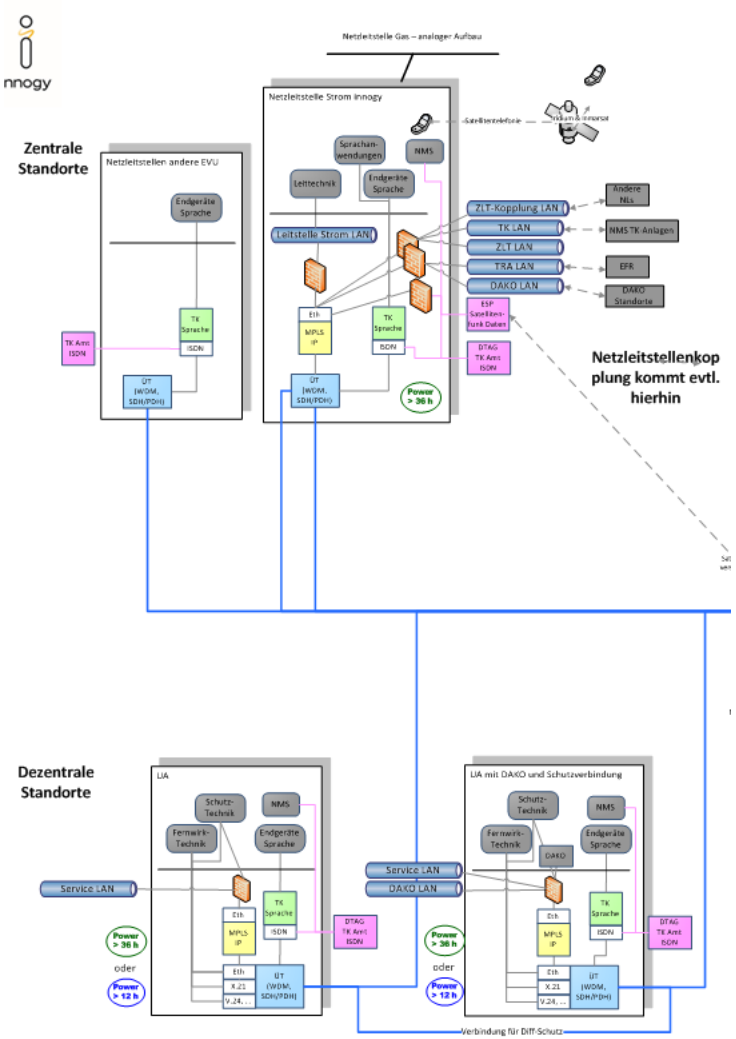
- ISO/IEC 27001 Kap 9.2 Internes Audit:
  - Die Organisation muss in geplanten Abständen interne Audits durchführen, um Informationen darüber zu erhalten, ob das ISMS:
  - a) die Anforderungen
    - 1) der Organisation an ihr ISMS und
    - 2) dieser Internationalen Norm erfüllt;
  - b) wirksam verwirklicht und aufrechterhalten wird.
- Bei einem zertifizierten ISMS sind alle ISMS-Assets mindestens einmal im Drei-Jahres-Zyklus auch intern zu auditieren.
- Auditoren sind so auszuwählen und Audits so durchzuführen, dass die Objektivität und Unparteilichkeit des Auditprozesses sichergestellt ist.
- Die Ergebnisse der Audits werden gegenüber der zuständigen Leitung berichtet.
- Dokumentierte Informationen und Ergebnisse des Audits sind aufzubewahren.

Organisatorische und technische Maßnahmen

- BNetzA SiKat (08/2015): Risiken sind durch geeignete Maßnahmen auf Basis des allgemein anerkannten „Stand der Technik“ zu behandeln
- Wichtig sind häufig die ergänzenden Regelungen nach DIN ISO IEC TR 27019 2015 für die Besonderheiten der Energieversorgung als Flächeninfrastruktur (z.B: 10.11.1 Behandlung von Altsystemen, 9.3.1 Betriebseinrichtung in Bereichen anderer Energieversorger usw.)
- Bei den Branchenbesonderheiten sucht man sonst die „allgemeine Anerkenntnis“ vergebens.

									VERANTWORTLICH:				
Nr.:	Risikobezeichnung	Einstufung:	Risiken:	Betroffene Objekte:	Empfohlene Maßnahmen, gemäß RA Smartpool I V1.3.1		durchgeführte Maßnahmen: Stand: 24.06.2016	Status-Phase	Gesamt-betreiber	RWE Z	RWE I	RWE NT	Siemens
7	Fehlendes Patchmanagem	untragbar	• Manipulation von Software • Ausfall von Geräten • Fehlfunktion von Geräten • Softwarefehlfunktion • Verfälschung von Daten	Alle Komponenten	7.1	Erstellung von Dokumentationen, Systembeschreibungen und Betriebskonzeption nach Konzernvorgaben inkl. Definition einer Patchmanagementrichtlinie und regelmäßige Updates aller Systeme.	PDN-Komponenten sind größtenteils bereits in vorhandens Patch-Mgt. eingebunden; (Betriebsssystem RedHat wird über Update-Server bearbeitet) Wartungsvertrag mit Siemens vorhanden Betriebsabläufe werden im Rahmen der Task-Force definiert	in Arbeit	x				
					7.2	Berücksichtigung in der Betriebskonzeption (SLA mit den Fachabteilungen, die die Systeme warten – z.B. RWE IT und Prüfung, ob die Richtlinien den Anforderungen entsprechen)	Betriebsabläufe werden im Rahmen der Task-Force definiert	offen	x				
8	Fehlendes Changemanage	untragbar	• Ausfall von Geräten • Fehlfunktion von Geräten • Softwarefehlfunktion	Alle Komponenten	8.1	Erstellung von Dokumentationen, Systembeschreibungen und Betriebskonzeption nach Konzernvorgaben mit Aufbau eines Changemangement-Systems inkl. eines Entscheidungsgremiums	Betriebsabläufe werden im Rahmen der Task-Force definiert	offen	x				
9	Firewall Fehlkonfiguration	tragbar	• Manipulation von Software • Ausfall von Geräten • Fehlfunktion von Geräten • Softwarefehlfunktion Verfälschung von Daten	le Komponent	9.1	Berücksichtigung von Regelungen zu Firewall-Änderungen in der Betriebskonzeption (inkl. Prüfung des Regelsatzes bei Änderungen nach 4-Augenprinzip entsprechend der Konzernvorgaben)	Regelbetrieb der RWE NT	erledigt				x	
					9.2	Einführung einer redundanten Firewall und Definition der Kommunikationsbeziehungen	restritive Firewallregeln in Absprache mit dem Hersteller eingerichtet; redundante Firewall vorhanden	erledigt		x		x	x

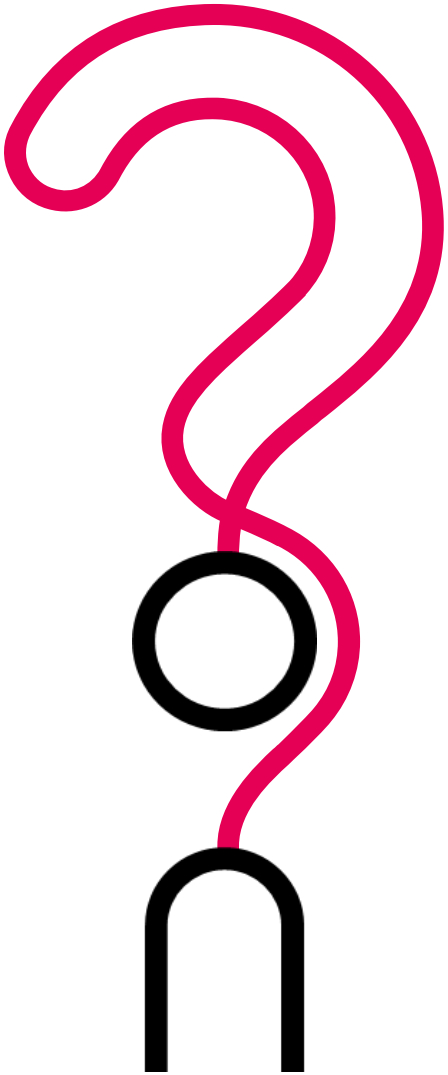
Der Netzstrukturplan



- Der Netzbetreiber hat eine Übersicht über die vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten mit den anzutreffenden Haupttechnologien und deren Verbindungen zu erstellen.
  - Leitsysteme und Systembetrieb
  - Übertragungstechnik/Kommunikation
  - Sekundär-, Automatisierungs- und Fernwirktechnik
- Folgende Netzstrukturen sind grundsätzlich zu trennen:
  - Büronetz (DIN ISO/IEC 27002)
  - Prozessnetz (DIN SPEC 27019)
- Schnittstellen zu Dritten sind darzustellen

3 ZERTIFIZIERUNG DES ISMS

Pflicht zur Zertifizierung des ISMS für Netzbetreiber



- Der Netzbetreiber ist verpflichtet, die Konformität seines ISMS mit den Anforderungen dieses IT-Sicherheitskatalogs durch ein Zertifikat zu belegen
- Die Bundesnetzagentur erarbeitet hierzu gemeinsam mit der Deutschen Akkreditierungs-stelle (DAkkS) ein entsprechendes Zertifikat auf der Basis von DIN ISO/IEC 27001
- Die Zertifizierung muss durch eine unabhängige und für die Zertifizierung akkreditierte Stelle durchgeführt werden
- Der Netzbetreiber hat der Bundesnetzagentur bis zum 31.01.2018 den Abschluss des Zertifizierungsverfahrens mitzuteilen

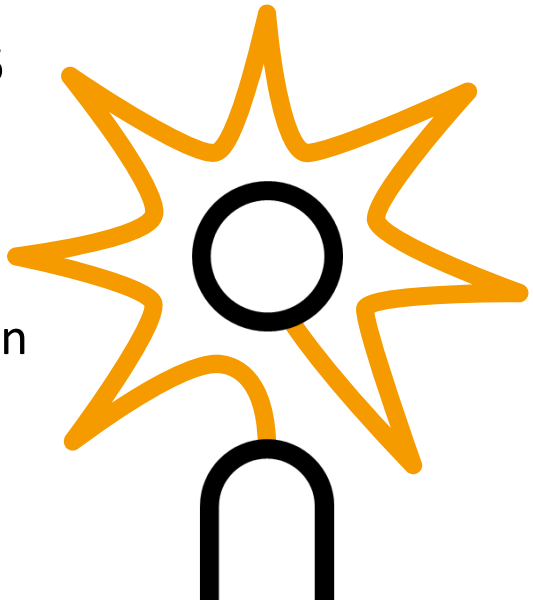
Abgestimmte Vorgehensweise zwischen den Beteiligten im Konzern

- Im 1 Q. 2016 wurde folgende Vorgehensweise zwischen der RWE DAG und unseren deutschen VNB abgestimmt:
  - Der Konzerneinkauf soll mit Unterstützung von DS Rahmenverträge (RV) mit einer Auswahl von Zertifizierungs-Dienstleistern schließen, die das benötigte Zertifikat ausstellen können
  - Die deutschen VNBs der RWE DAG sollen bei ihrem Zertifizierungs-Dienstleister zu den vereinbarten Konditionen des RV die benötigten Dienstleistungen abrufen können
  - Der RV umfasst jeweils einen ganzen Zyklus mit dem Zertifizierungsaudit und zwei Überwachungsaudits und einem zusätzlichen (vom DAkkS genehmigten) Pre-Audit. Weiterhin enthält der RV eine Regelung für zusätzliche Leistungen und Reisekosten

Meinungen, Fragen und die Eindeutigkeit von Normen

innogy

- Alle Zertifizierer gehen streng nach den Vorgaben der DAkkS, den Standards ISO/IEC 27006 und ISO/IEC 17021-1 vor.
- Je nach Hintergrund des Unternehmens und Kenntnis der Energiebranche hat daraus jeder sein eigenes Rezept für den „Aufwand“ entwickelt (Erstaunlich divergente Positionen und Vorgehensweisen bei der Angebotslegung erkennbar).
- Bei der Höhe des Preises pro Audit-Tag waren die geringsten Unterschiede feststellbar.
- Das Beschaffungsprojekt wurde Mitte November 2016 abgeschlossen.
- Hinweis: Das Akkreditierungsverfahren für „unseren“ Zertifikattyp läuft zur Zeit und wird voraussichtlich bis 1 Q 2017 abgeschlossen sein. Einige Zertifizierer haben ihr Audit dazu bereits durchlaufen und können ab Anfang 2017 Energienetzbetreiber zertifizieren.



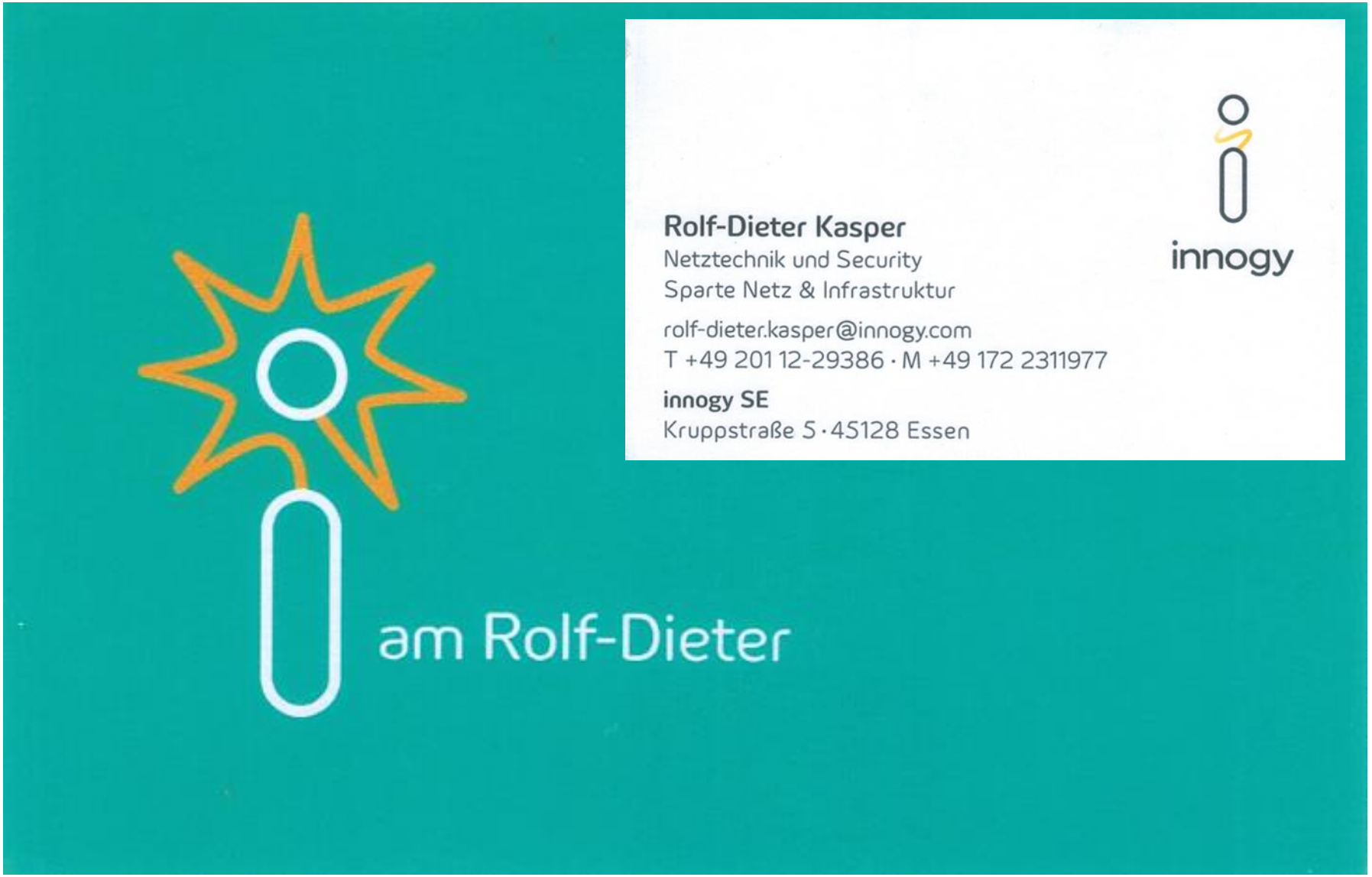
4 AUSBLICK

Ausblick

innogy

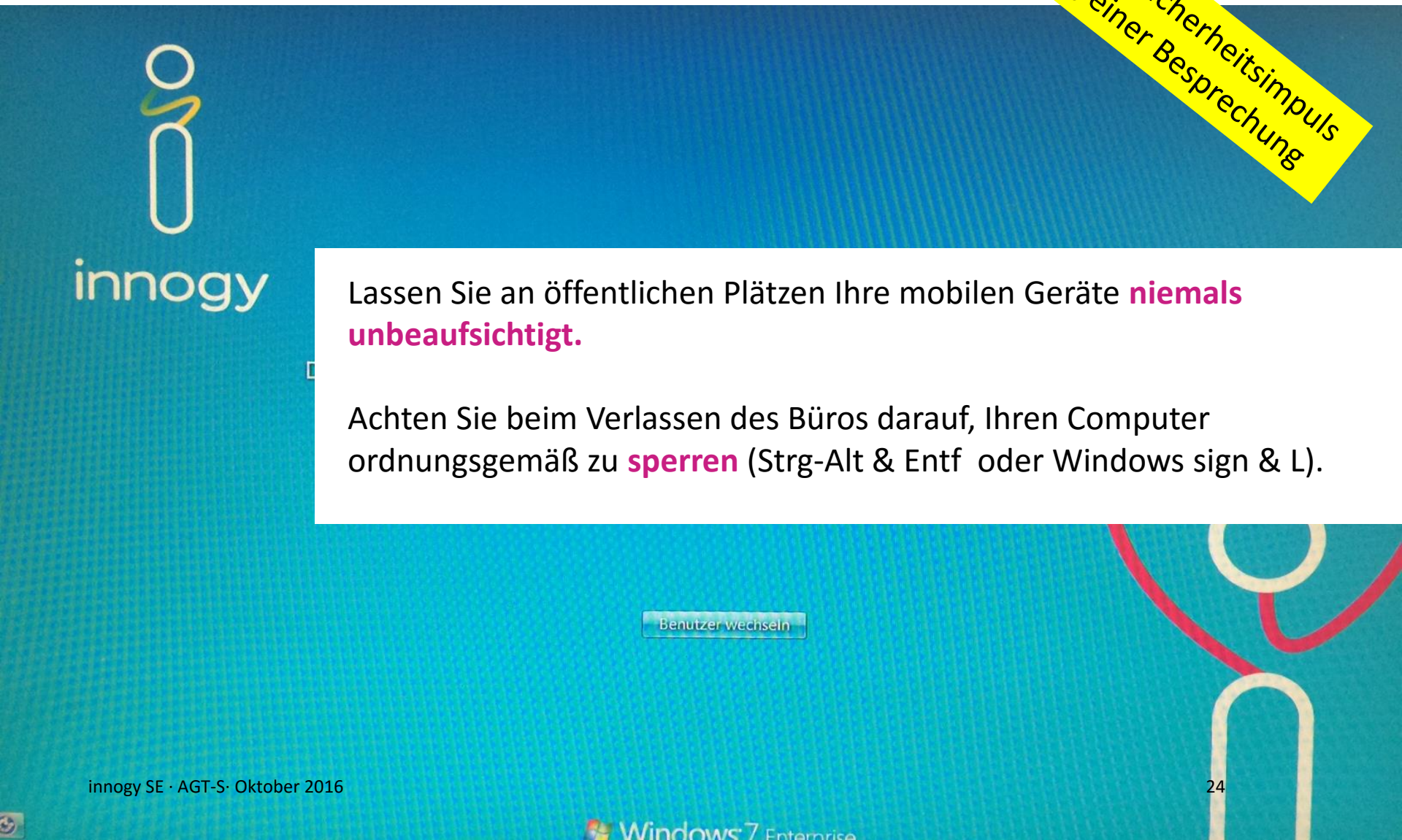
- Das laufendes Verfahren mit
  - jährlichen Kontrollaudits und
  - 3 jährige Rezertifizierung

  führt zu einer ständigen Verbesserung des Sicherheitsniveaus.
- Ausbilden von Sicherheitsexperten in allen adressierten Unternehmen bringen deutliche Verbesserung beim Erkennen von Angriffen und durch eine zielgerichtete Reaktion auch eine Begrenzung der Schäden.
- Das im ISMS enthalte Lieferantenmanagement und die gesetzliche Forderung, die beim Betreiber gesetzten Sicherheitsanforderungen auch an Lieferanten und Dienstleister weiterzugeben, führen schon heute wahrnehmbar zu sicheren Produkten bzw. Systemen und zu mehr Sicherheitsbewusstsein bei den Dienstleistern.
- Die Kommunikation (u.a. Meldepflicht und Branchen- und Themenarbeitskreise usw.) mit den Behörden führt zu einem besseren Verständnis der unterschiedlichen Positionen und Randbedingungen.


Rolf-Dieter Kasper
Netztechnik und Security
Sparte Netz & Infrastruktur
rolf-dieter.kasper@innogy.com
T +49 201 12-29386 · M +49 172 2311977
innogy SE
Kruppstraße 5 · 45128 Essen
innogy
am Rolf-Dieter

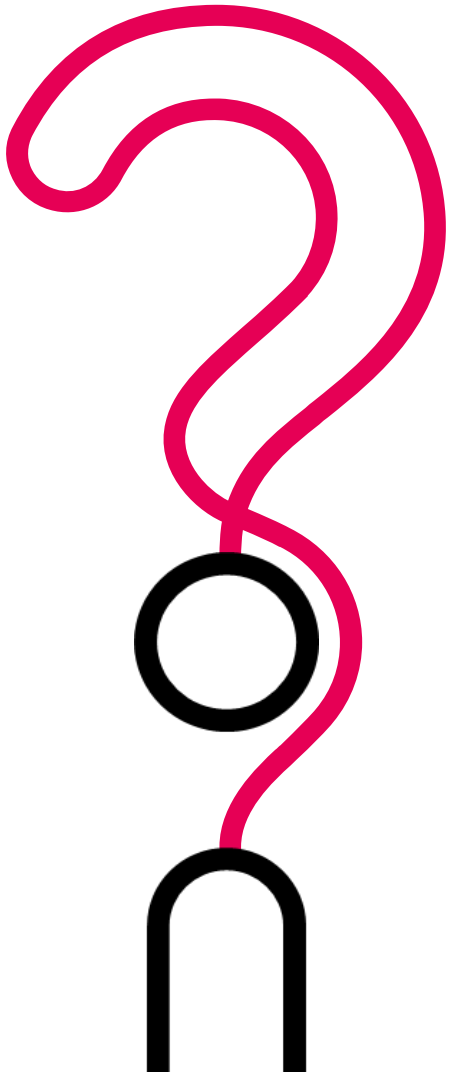
Sperren Sie ihren Rechner beim Verlassen des Arbeitsplatzes!

Beispiel eines Sicherheitsimpuls am Anfang einer Besprechung



Lassen Sie an öffentlichen Plätzen Ihre mobilen Geräte **niemals unbeaufsichtigt.**

Achten Sie beim Verlassen des Büros darauf, Ihren Computer ordnungsgemäß zu **sperren** (Strg-Alt & Entf oder Windows sign & L).



FRAGEN?