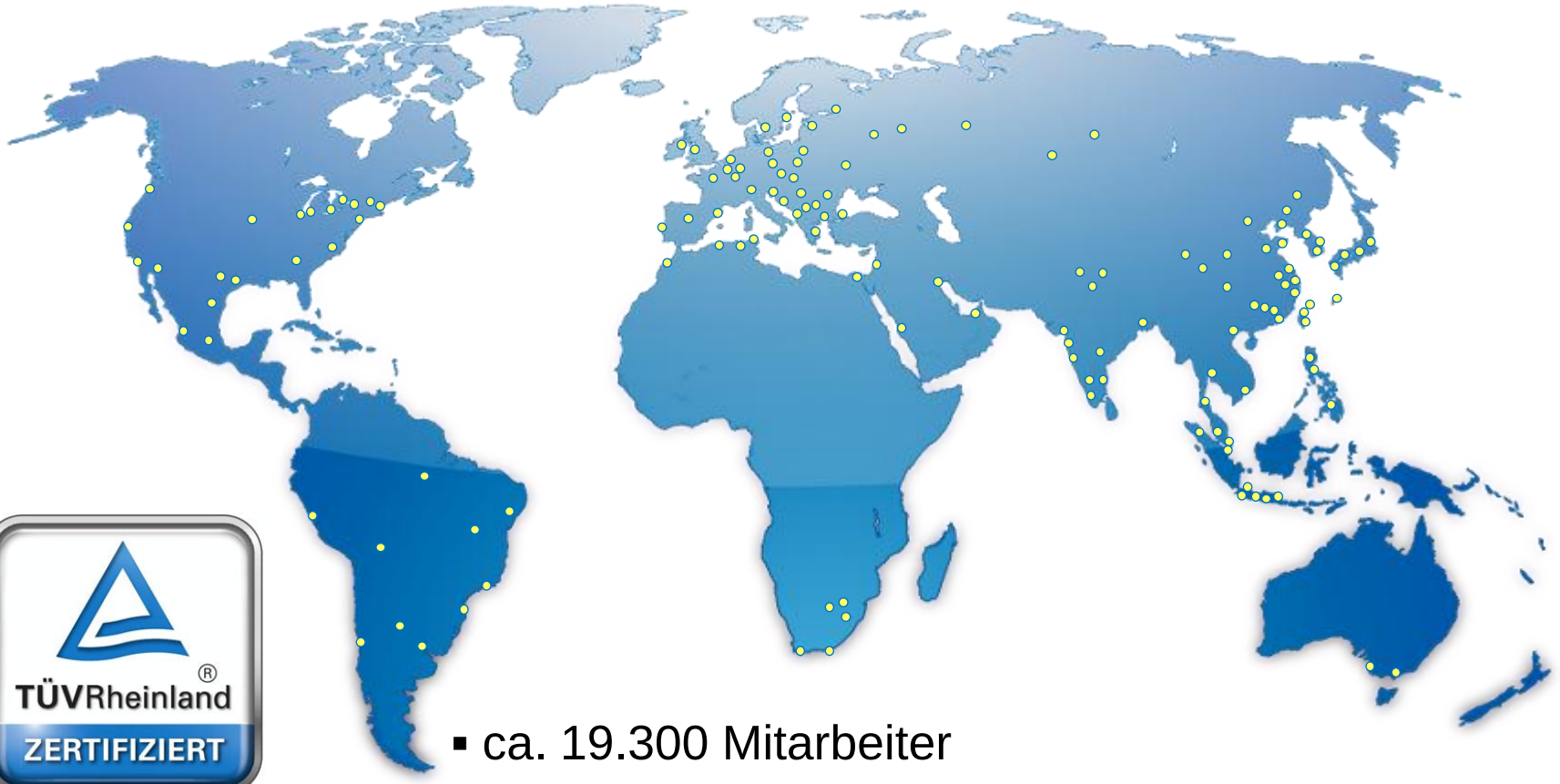
Aus Liebe zu Sicherheit und Qualität.

TÜVRheinland®
Genau. Richtig.

2015 - Auf allen Kontinenten zuhause.

- Ca. 600 Standorte in 69 Ländern
- ca. 1,7 Mrd. € Umsatz



- ca. 19.300 Mitarbeiter

TÜV Rheinland – Historie.

Meilensteine für eine sichere Zukunft.

1872

1900

1960

1970

1997

2005

TÜVRheinland®
Genau. Richtig.

TÜV Rheinland Cert - Leistungen im Überblick.

Internationale Normen und Standards

Qualitätsmanagement

- ISO 9001
- ISO/TS 16949
- VDA 6.1 ff.
- EN/AS 9100ff
- IRIS
- KBA

Energie und Umwelt

- ISO 14001
- EMAS
- DIN EN 16001
- ISO 50001
- Biomasse
- Ökoeffizienz
- § 41 EEG 2009
- EfbV
- CDM

Arbeitssicherheit

- OHSAS 18001
- SCC
- SCP
- MAAS-BGW

Nachhaltigkeit und CSR

- Nachhaltigkeits Check
- ISO 26000
- SA 8000
- BSCI/EICC
- Compliance Care
- TÜV Rheinland STAR
- GRI R3
- FSC, PEFC (Forstwirtschaft)

Informationssicherheit, IT und Qualität

- GAP Analyse
- ISO 27001
- ISO 20000
- ISO 22301
- BSI Grundschutz
- Rechenzentrum
- Prozess / ITIL
- IRCA Training
- Check your app
- Black/Whilte Listing

Gesundheitswesen

- KTQ
- DEGEMED
- deQus
- IQMP-Reha
- dPV-Standard
- ISO 13485
- Schmerzfreie Klinik
- u.v.m.

Food

- ISO 22000
- HACCP
- GMP
- IFS
- BRC
- IFIS
- Global GAP

Weitere Standards

- Bildungsträger (AZWV, ISO 29990)
- Sicherheitsdienste (DIN 77200)
- Logistik (IFS-Logistic, SQAS)
- Facility Management (GEFMA 710-730)
- u.v.m.

TÜV Rheinland-Innovationen

TÜV Rheinland-Standards

- Servicequalität
- Beratungsqualität
- Kunden-zufriedenheit

Management

- Risikomanagement (ONR 49000ff)
- Zertifizierung Credit Management
- Compliance Care
- Zertifizierung Compliance Management

Tourismus

- Wellness & Spa
- Medical Wellness
- Serviced Apartment
- ECOHotel
- Mystery Checks

Customized Services

- 2nd Party Audit
- Lieferanten-Audit
- Mystery Check
- Verifizierungen
- Validierungen

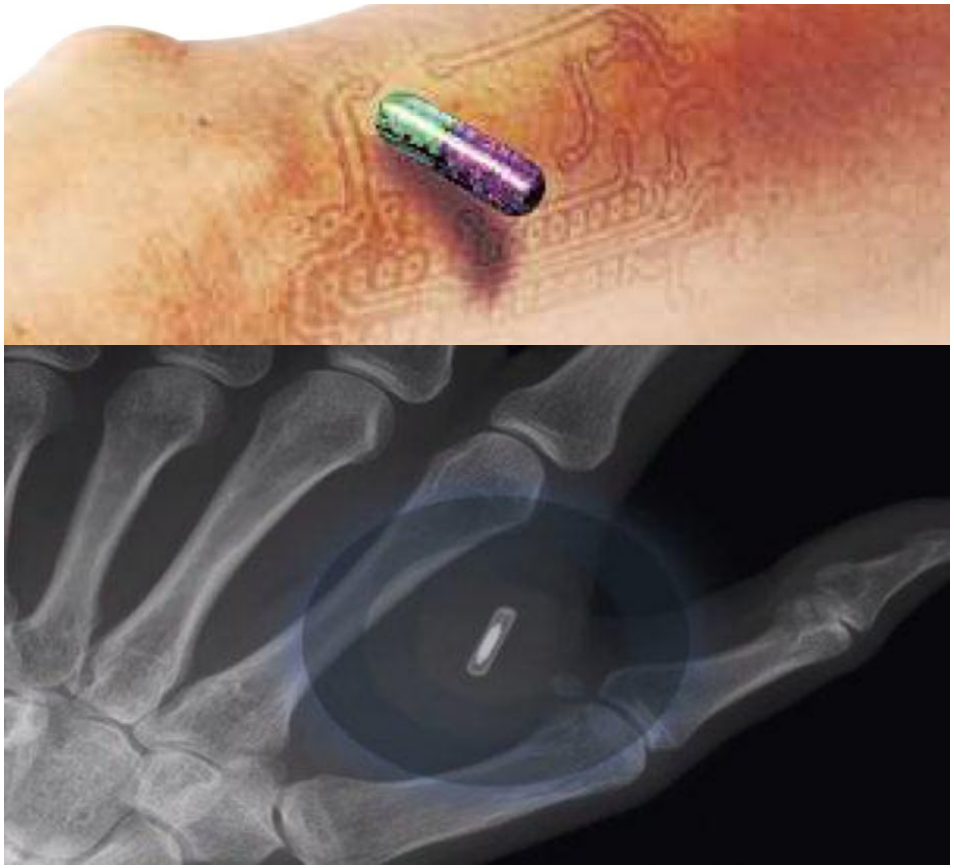
Die wichtigsten IT Trends 2015 & 2016

Nach dem Thema Digitalisierung ist das Thema Informationssicherheit das wichtigste Thema der CEO‘s

- Der Schutz vor Cyberangriffen wird nun auch Thema auf CEO-Ebene.
- Spätestens 2016 zählt IT-Sicherheit für 70 Prozent der CEOs zu den Top 3 Themen. Dieser Umstand stellt den CIO zusätzlich ins Rampenlicht.
- Das macht es zwingend erforderlich, jedes neue IT-Projekt von Anfang an maßgeblich immer unter dem Aspekt Sicherheit zu betrachten.
- Neue IT-Projekte können nur dann sicherer und besser werden, wenn sich die klassische Schere zwischen Anforderungsbeschreibung, Entwicklung, Testing, Einführung und Betrieb schließt.

Quelle:
IDC 01/2015

Raten Sie mal was das ist!



- In einem Büro-Komplex in Schweden können sich Mitarbeiter einen Chip unter die Haut pflanzen lassen, der anschließend als Schlüssel und Verifizierung dient.
- Was in Science-Fiction-Filmen als wilde Zukunfts-Phantasie erscheint, wird damit nun Realität.
- Der RFID-Chip hat eine Größe von einem Reiskorn.
- Rund 700 Menschen machen schon mit
- Dank der geringen Größe kann der Chip einfach eingespritzt werden, ein großer Eingriff ist nicht nötig.
- Aktuell lassen sich mit dem Chips Türen öffnen und Drucker bedienen
- Weitere Features sind geplant, wie beispielsweise im Café als Bezahlfunktion

Quelle:

Chip 10.02.2015

Täterprofile und die betroffenen Branchen

Deutsche Mittelständler gehören in vielen Branchen zu den innovativsten Unternehmen weltweit. Das weckt Begehrlichkeiten!!

Informationssicherheit / Datenschutz ist sinnvoll, kann Geld sparen und für den Joberhalt sorgen

VODAFONE

Strafanzeige eingereicht

Die Empörung über den Datenskandal beim Mobilfunkriesen Vodafone ist so groß, dass Kunden jetzt Strafanzeige gegen Deutschland-Chef **Jens Schulte-Bockum** stellen. Wie viele genau bisher eingegangen sind, kann die Staatsanwaltschaft Düsseldorf zwar erst in zwei Wochen sagen, aber sie bestätigt, dass schon mehrere vorliegen.

„Der Fehler liegt eindeutig bei Vodafone", sagt etwa der langjährige Vodafone-Kunde Siegfried Kurtz aus Hellenthal in der Eifel. Darum habe er den Chef wegen „Beihilfe zum Datendiebstahl" angezeigt.

Vodafone hatte vor einer Woche den Diebstahl von zwei Millionen Kundendaten bekannt gegeben. Der Verdächtige, ein Mitarbeiter eines externen Dienstleisters, soll heimlich Namen, Adressen und Geburtsdaten sowie Kontonummern kopiert haben.

juergen.berke@wiwo.de

- Nach dem **massivsten Diebstahl von Kreditkarten-Daten** in der US-Geschichte **verliert** der Chef der Warenhauskette Target **seinen Job!**.
- Gregg Steinhafel war **35 Jahre** im Unternehmen.
- **Hacker** waren in die Systeme von Target eingedrungen und erbeuteten dabei Daten von Kredit- und Bankkarten sowie Postadressen, Telefonnummern und E-Mail-Adressen von bis zu **70 Millionen Kunden.**

Die Schäden durch Internet-Straftaten werden auf 50 Milliarden Euro geschätzt

Quelle: Wirtschaftswoche & Aachener Nachrichten - Stadt / Wirtschaft / Seite 7

Die Frage nach dem Businesscase - Verbindung zwischen IT-Risiken und wichtigen Reputationsfaktoren

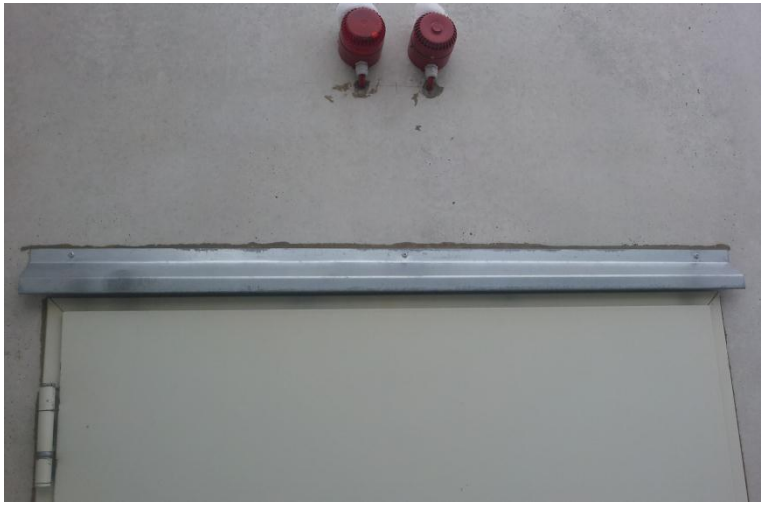
- <u>Entwicklung an den Börsen:</u>
  Erfolgreiche Unternehmen erkennen besser die Verbindungen zwischen IT-Risiken und wichtigen Reputationsfaktoren

- Die Korrelation ist besonders ausgeprägt zwischen der IT und der Kundenzufriedenheit sowie dem Markenimage

- Etwa 84 der Unternehmen mit einem hervorragenden Ruf sagen, ihr Potenzial für IT-Risikomanagement sei stark oder sehr stark ausgeprägt

Quelle: IBM Studie

Im Audit gibt es auch Best Practice Hinweise – Dreingabe von Unterlagen unserer zertifizierten Kunden



Best Practice Hinweise – es kann so einfach sein

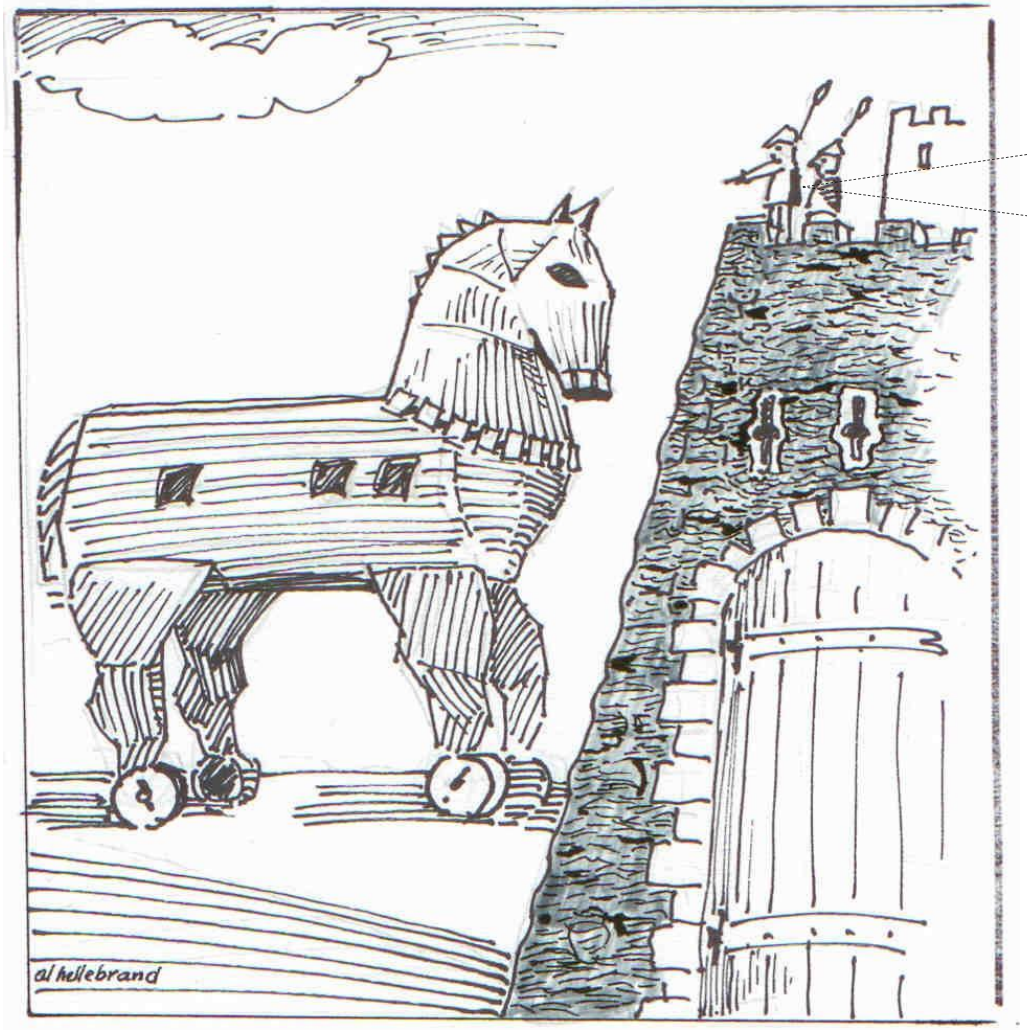
- Computer & Bildschirme strahlen elektromagnetische Wellen ab
- Mit geeigneter Technik selbst aus einer Entfernung von bis zu 50 Metern und durch Wände hindurch werden sensible Informationen gewonnen
- Diese Daten lassen sich leicht rekonstruieren
- Experten ist diese Methode schon lange bekannt unter dem Schlagwort "Tempest"

Blick-Fänger

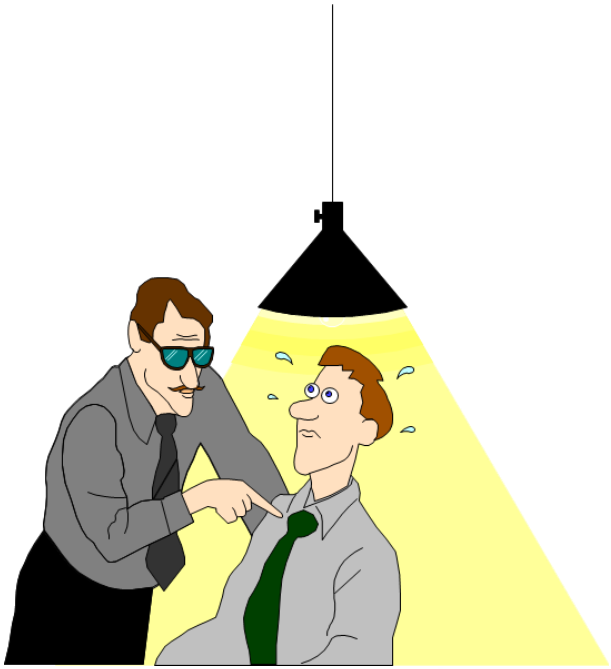
Längst nicht immer kommen Spione übers Netz. Oft genug – etwa im Zug oder am Flughafen – lesen sie einfach von der Seite mit, was Geschäftsleute auf dem Laptop-Display anschauen. Abhilfe schafft der **Vikuiti** Blickschutzfilter von 3M, der nur direkt von vorne freie Sicht aufs Display von Smartphone, Tablet oder PC ermöglicht. Neugierige Späher von der Seite sehen dagegen Schwarz.

Preis: ab 30 Euro

Es werden keine reinen Checklistenprüfer gesucht



Woher sollen wir wissen, dass da keine TÜV Prüfer drin sind ?!



TÜVRheinland®
Genau. Richtig.

Folgende Unternehmen sind dort wegen Datenschutzvorfällen gelistet:

Deutsche Bank, Allianz, Credit Suisse, Klinikum Kassel, BKK, Neckermann, Sony, Jobcenter und Bildungsbehörde Bremen, Amtsgericht Düsseldorf, Immobilienscout24, Kabel Deutschland, Zeit-Verlag, PWC, Piratenpartei, Unicef und Unesco

Folgende Unternehmen haben uns u.a. beauftragt:

- ***Artegic AG***
- ***Vodafone***
- ***Postbank Systems***
- ***Borussia VfL 1900 Mönchengladbach***

Ungewöhnlicher Fund

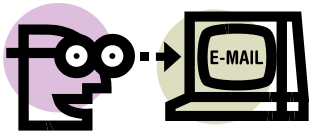
Piraten finden Akten auf Toilette im Rathaus Göttingen

14.01.2013 16:17 Uhr

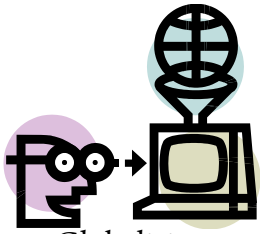
Brisanter Fund auf der Rathaustoilette: Rund 2000 Seiten mit „hochsensiblen, personenbezogenen Daten", inklusive Namen und Adressen, hat Martin Rieth, Vorsitzender der Piraten-Ratsfraktion, in einem Karton im ersten Stock des Rathauses gefunden.

Brisantes auf der Toilette: Pirat Martin Rieth am Fundort. Der Vorfall sei „alarmierend".
© Heller

Bedrohungen für Informationen

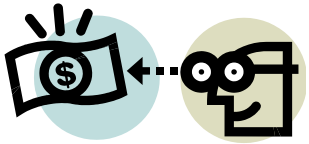


Internetnutzung/IT

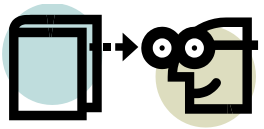


Globalisierung

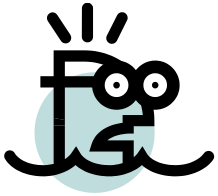
Internet



Diebstahl & Betrug



(Über)-Regulierung

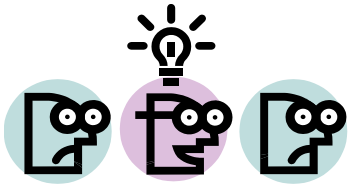


Wie kann man damit umgehen?

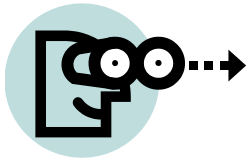
Social Engineering

Unwissenheit von

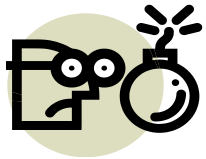
Mitarbeitern



Mitteilungsbedürfnis



Spion vs. Spion

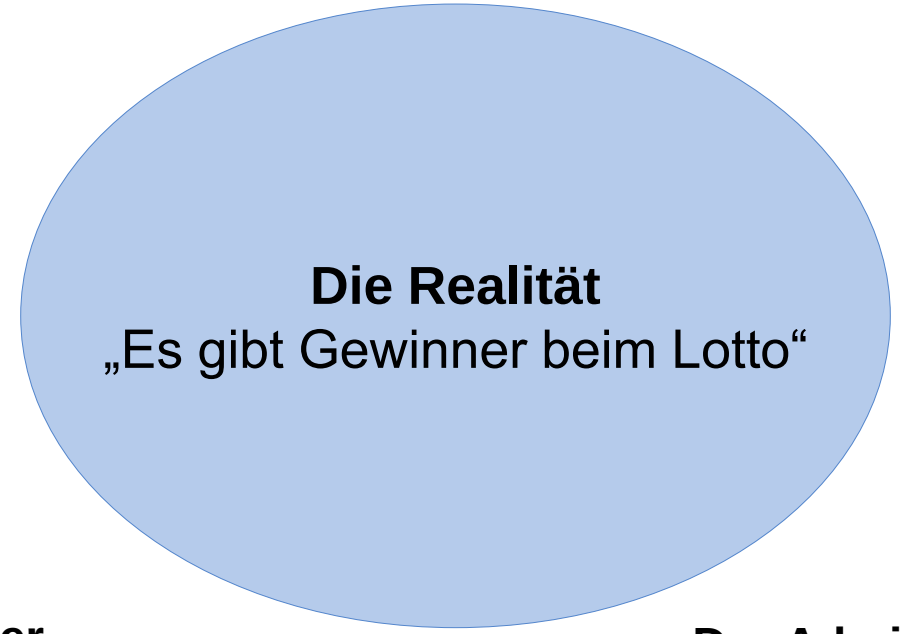


Terror/Unruhe

Risikobetrachtungen
Klassischer Umgang mit Risiken

Der Rheinländer
„Et hät noch evve jot jejange!“

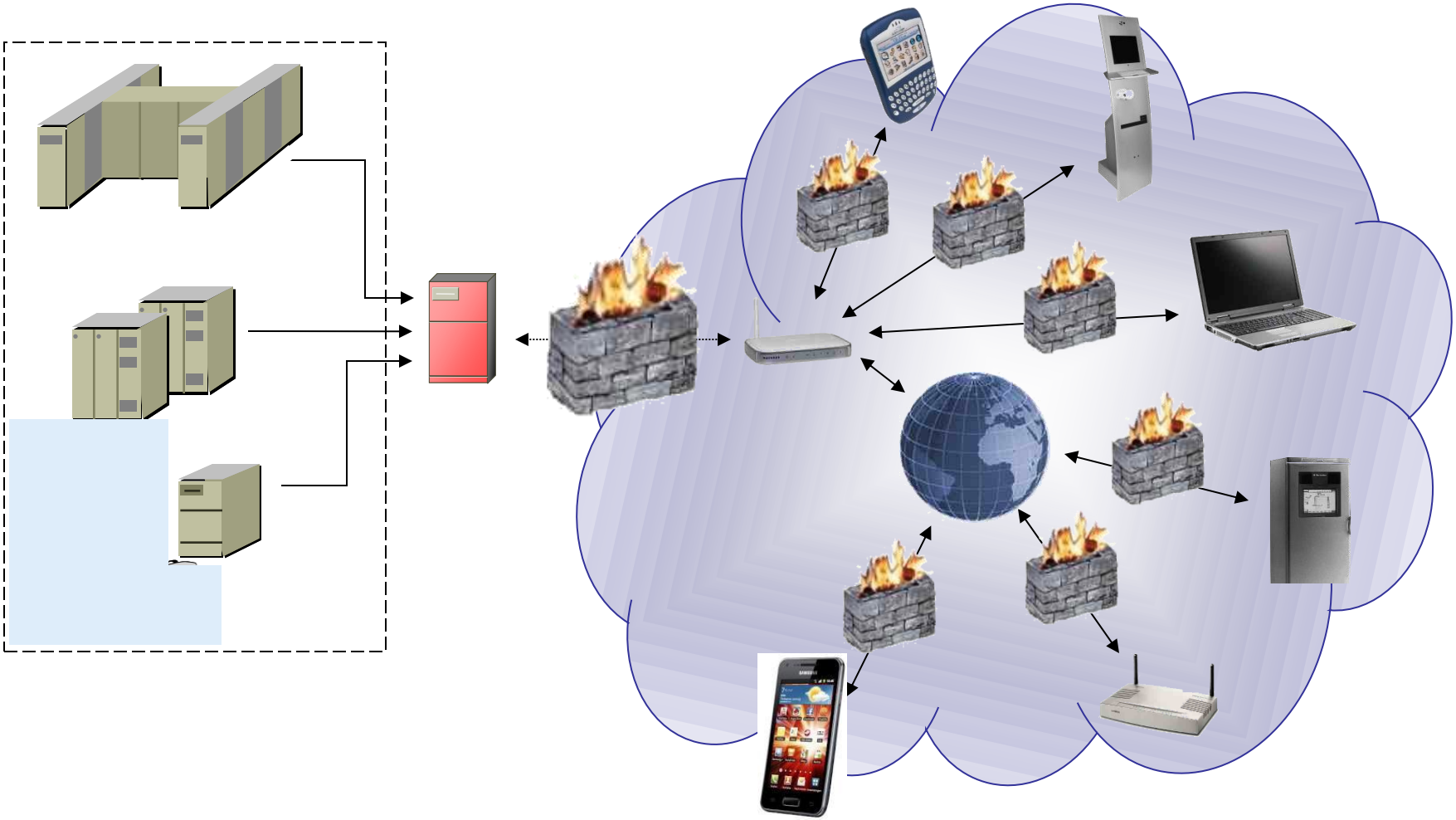
Der Strauß
…einfach mal den Kopf in den Sand stecken



Der Unternehmer
„bei uns passiert so was nicht!“

Der Administrator
„Wir hatten noch nie Probleme!“

IT Sicherheit: Gemanagte Kombination aus Technik und Organisation



Die Normen ISO/IEC 27002:2013 und ISO/IEC 27001:2013

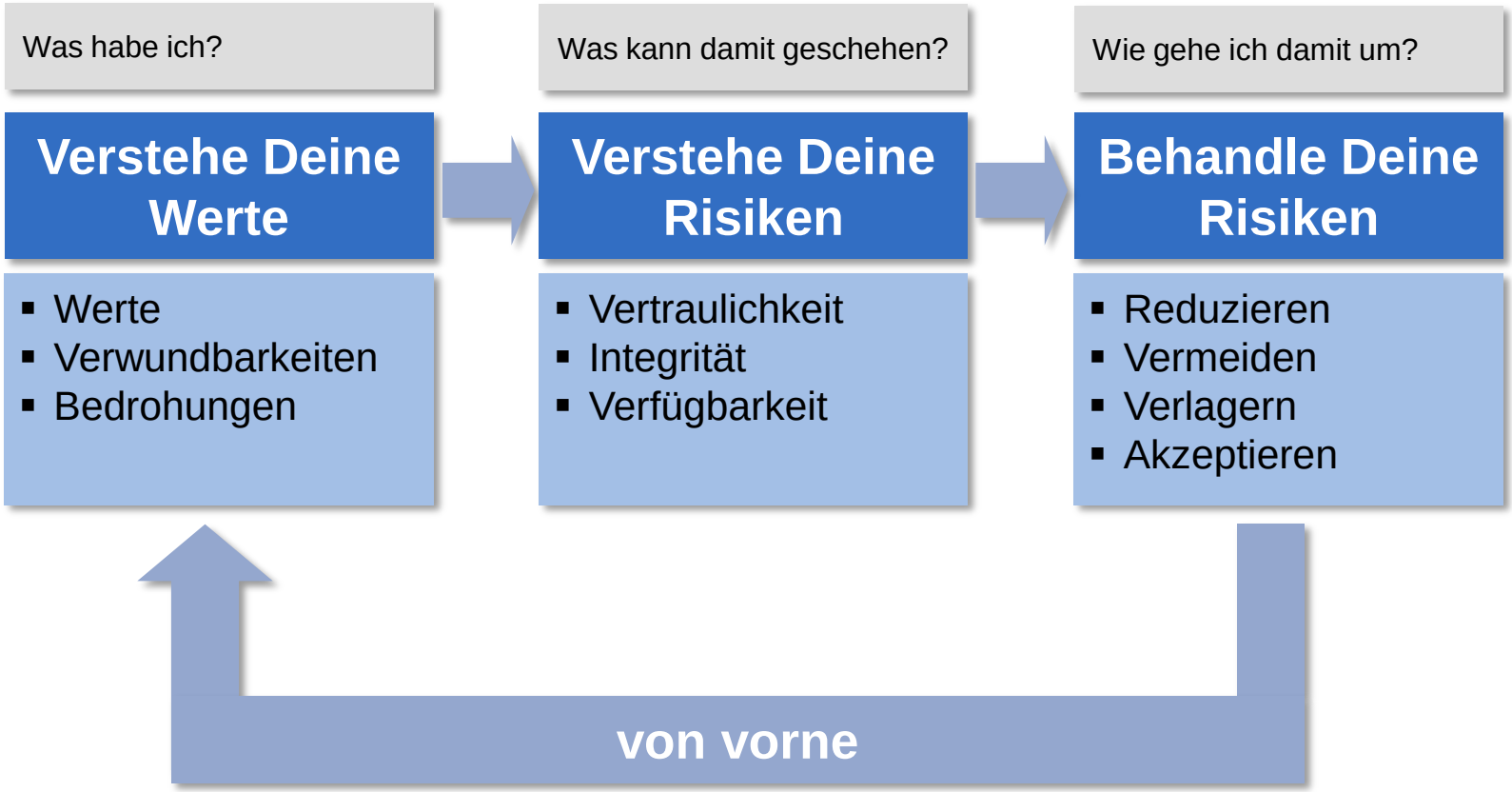
- Norm für die Bewertung der Sicherheit von IT-Umgebungen. Der Standard beinhaltet eine umfassende Sammlung optimaler Verfahren („best practices“) und besteht aus **zwei Teilen:**

  - **ISO/IEC 27002:2013** Informationssicherheits-Managementsystem (ISMS).
    Gibt Vorschläge zur Umsetzung und entspricht inhaltlich der ISO 17799. Es wurde durch die ISO-Gremien in internationaler Zusammenarbeit optimiert und ergänzt.

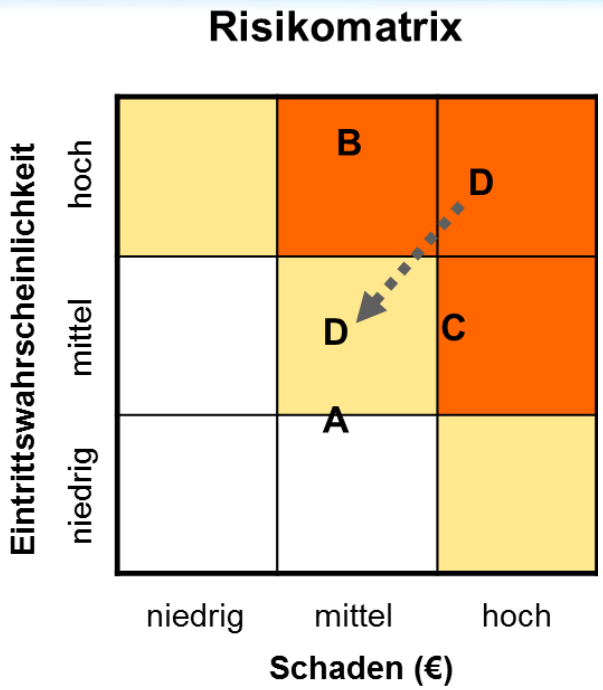
  - **ISO/IEC 27001:2013** beschreibt die Anforderungen an die Umsetzung und Dokumentation eines ISMS.
    => **Dies ist die Prüfgrundlage für Zertifizierung eines ISMS.**

ISMS nach ISO 27001

PLAN – Risikobasierte Steuerung von Sicherheitsmaßnahmen



Risikomanagement
Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe



Vorsicht an der Bahnsteigkante: Willkommen auf dem „gefährlichsten Marktplatz der Welt"

- Kritische Erfolgsfaktoren:
  - Vollständigkeit der Szenarien
  - Ermittlung realistischer Wahrscheinlichkeiten
  - Berechnung der Schadenshöhe

ISMS nach ISO 27001:2013
Gliederung

- IS-Themen

Management

- Informationssicherheitspolitik (5.2, A.5)
- ISMS-Organisation (5.3, A.6)
- Information Asset Management (A.8)
- IS Incident Management (A.16)
- Compliance (A.18)
- Leadership (5)
- Beziehungen zu Lieferanten (A.15)

Personal

- Personelle Sicherheit (A.7)

Zutritt / Gebäude / Umgebung

- Physische Sicherheit (A.11)

Tagesgeschäft

- Betrieb (A.12)
- Kryptographie (A.10)
- Kommunikations-sicherheit A.13)

Planung / Projekte

- Beschaffung, Entwicklung und Wartung von Systemen (A.14)

Zugang / Zugriff

- Zugangskontrolle (A.9)

Geschäftsprozesse

- IS Risiko Management (8.2, 8.3)
- Business Continuity Management (A.17)

ISMS nach ISO 27001:2013
Mindestdokumentation

Normkapitel	Dokument
4.3	Geltungsbereich des ISMS
5.2	Informationssicherheitspolitik
6.1.2	Prozess der Einschätzung von Informationssicherheits-Risiken (Risikoanalyse)
6.1.3	Prozess der Behandlung von Informationssicherheits-Risiken (Risikobehandlungsplan)
6.1.3 d)	Erklärung zur Anwendbarkeit (Statement of Applicability, SoA)
4.3	Geltungsbereich des ISMS
6.2	Informationssicherheitsziele
7.2 d)	Nachweis der Kompetenz
7.5.1 b)	Dokumentierte, von der Organisation festgelegte Informationen, soweit für die Wirksamkeit des ISMS erforderlich
8.1	Operative Planung und Kontrolle
8.2	Ergebnisse der Risikoanalyse
8.3	Ergebnisse der Risikobehandlung
9.1	Nachweis der Ergebnisse von Überwachung und Messung der Wirksamkeit
9.2 g)	Nachweis des Auditprogramms und der Auditergebnisse (Interne Audits)
9.3	Nachweis der Ergebnisse des Management Reviews
10.1 f)	Nachweis über die Eigenschaften der Abweichungen und Folgeaktivitäten
10.1 g)	Nachweis über die Ergebnisse von Korrekturmaßnahmen

Bestandsaufnahme

Ablauf einer Bestandsaufnahme für ISO/IEC 27001

- Festlegung des Scopes, Auswahl und erste Sichtung von Dokumenten und Abläufen
- Sichtung der Prozessdokumentation
- Sichtung vorhandener Nachweise zur Anwendung des ISMS sowie Durchführung von Interviews
- Ergebnisauswertung (Berichts- und Präsentationserstellung)
- Präsentation der Ergebnisse

Vorteile einer vorgelagerten Bestandsaufnahme

Vorteil	Erläuterung
Auswirkungen erkennen	Bei einer Bestandsaufnahme werden die einzelnen Kapitel der Norm mit den Gegebenheiten im Unternehmen verglichen.
Geltungsbereich	Anhand der Bestandsaufnahme kann der Geltungsbereich für die anstehende Zertifizierung ggf. eingegrenzt werden. Somit können die Kosten für die Zertifizierung reduziert werden.
Stärken und Schwächen erkennen	Nach der Bestandsaufnahme kennt das Unternehmen seine Stärken und Schwächen. So können Ressourcen besser eingesetzt und somit Kosten reduziert und die Dauer der Vorbereitung verringert werden.
Mitarbeiter einbinden	Mitarbeiter und Führungskräfte kennen die Herausforderungen und können somit besser motiviert und eingebunden werden.
Dokumentation, Technik und Infrastruktur	Mit der Bestandsaufnahme werden Schwächen in der Dokumentation und der technischen Infrastruktur deutlich, so dass genügend Zeit bleibt, Maßnahmen zu treffen.

Ihr Weg zu Ihrem ISO/IEC 27001 Zertifikat

Implementierung (evtl. mit Berater)

Bestands-
aufnahme

Scope
festlegen

Schutz-
bedarf
feststellen
und Risiken
bewerten

SoA festlegen und
Controls auswählen
bzw. Maßnahmen
festlegen

Controls implementieren,
Management Review und
interne Audits durchführen

Zertifizierung
durchführen


Zertifikat

Standard ISO/IEC 27001:2005

Zertifikat-Registrier-Nr. xx xxx xxxx

TÜV Rheinland Cert GmbH bescheinigt:

Zertifikatsinhaber: <Logo>
<Kunde>
<Kundenanschrift
>

Geltungsbereich: Standort Musterstadt

Durch ein Audit, Bericht Nr. nnnnnnnn, wurde der Nachweis erbracht, dass die Anforderungen des Prüfkataloges für ISO/IEC 27001:2005, der TÜV Rheinland Cert GmbH bezüglich Dokumentation und wirksamer Umsetzung erfüllt sind.

Das Fälligkeitsdatum für Folgeaudits ist der dd. mmm.

Gültigkeit: Dieses Zertifikat ist gültig bis yyyy-mm-dd
vom yyyy-mm-dd bis zum yyyy-mm-dd.

yyyy-mm-dd

www.tuv.com

TÜVRheinland®

TÜVRheinland®
ZERTIFIZIERT

Management
System
ISO 27001:2013

www.tuv.com
ID 0000000001

TÜVRheinland®
Genau. Richtig.

Relevanz der ISO 27001 Zertifizierung

Unter allen weltweit themenspezifischen Normen verzeichnet die Norm ISO:IEC 27001:2005 2014 mit 23 % den größten Zuwachs

Zertifizierung nach ISO 27001
Nutzen

- Nachweis der Sicherheit gegenüber Dritten (Gesetzgeber, Mitarbeitern, Lieferanten, Kunden und Partner)
- Wettbewerbsvorteil: „Dokumentierte Qualität“ durch eine unabhängige Instanz
- Kostenreduktion durch transparente und optimierte Strukturen
- Sicherheit als integraler Bestandteil der Geschäftsprozesse
- Kenntnis und Kontrolle der IT-Risiken / -Restrisiken
- Dokumentation von Strukturen und Prozessen
- Absicherung des CIO & IT-Sicherheitsverantwortlichen

Zertifizierung nach ISO 27001
weiterer Nutzen

- Gesteigertes Sicherheitsbewusstsein der Mitarbeiter
- Beurteilen der Organisationsprozesse nach Sicherheitsgesichtspunkten
- Vorrang der Sicherheit des Geschäftsbetriebes: Business Continuity Management
- Weltweit anerkannter Standard
- Mögliche Senkung von Versicherungsprämien
- Referenzierung des IT-Prozess-Management-Standards „ITIL“ auf ISO 27001
- Nahtloses Einpassen von ISO 27001 in evtl. bestehende Managementsysteme, wie z.B. ISO 9001
- 10 Spiele ohne Niederlage (Erstzertifizierung VFL B. MG)

TÜVRheinland®
ZERTIFIZIERT
Management System
ISO 27001:2013
www.tuv.com
ID 0000000001


Certificate
ISO/IEC 27001:2005

The Certification Body for Information Security Management Systems of the TÜV Rheinland Industrie Service GmbH, hereby certifies that the organisation

Computacenter AG & Co. oHG
Europaring 34 - 40
D - 50170 Kerpen

has implemented and applies a management system for information security for the scope

- Information Technology Services Germany
- Configuration Center
- Data Erasure Process in the Service Center
in Kerpen, Germany

As a result of audit, report no. 6300/076/02 dated 2006-02-15, it was established that the requirements according to the international standard

ISO/IEC 27001
Information technology – Security techniques -
Information security management systems - Requirements

have been satisfied with respect to documentation and practical implementation.

This certificate is valid until 2009-05-18

Certificate No. 01 153 02001

Cologne, 2006-05-30

Certification of Management Systems

TÜVRheinland®
Genau. Richtig.

Werbemöglichkeit: Prüfsiegel, mobil, Certipedia

TÜVRheinland®
Genau. Richtig.

Werbemöglichkeit: Zertifikatsübergabe, Pressetexte

TÜVRheinland®
Genau. Richtig.

Glaubwürdigkeit – unterstützt durch Zertifizierung

frantab / Shutterstock.com

TÜVRheinland®
Genau. Richtig.

Warum TÜV Rheinland Cert ?

- ✓Wir sind **Marktführer bei der ISO 27001** im deutschsprachigen Raum
- ✓ Wir haben eine starke Auswahl an **Referenzkunden** in fast allen Branchen
- ✓ Wir haben drei Auditoren mit dem **Ü2 Geheimstatus**
- ✓ Nachhaltigkeit / CSR wird bei uns gross geschrieben, **UN Global Compact**
- ✓ **TOP Arbeitgeber** in den letzten 4 Jahren und ein installiertes Compliance MS
- ✓ Möglichkeit auf **integrierte Managementsysteme** mit ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 22301 mit internen und externen Kostenvorteilen
- ✓ Unser Produktverantwortlicher Bruno Tenhagen ist **anerkannter IRCA Tutor**
- ✓ Wir stellen drei **Grundschutz - Auditoren** mit Doppelqualifikation ISO 27001

Zitate unserer Referenzkunden

„Die kooperative Arbeit mit den TÜV-Rheinland-Auditoren und ihr fachkundiger Blick von außen tragen zusätzlich zum kontinuierlichen Verbesserungsprozess bei.“

(Eckart Böhringer, Teamleader IS Quality Services bei Computacenter)

„Neben der Professionalität der Auditoren hat uns auch die pragmatische Art gefallen, mit der das Audit durchgeführt wurde“.

(Ingo Geisler, Head of Business Continuity, Vodafone D2 GmbH)

„Durch die strukturierte, effektive und engagierte Arbeitsweise der TÜV Rheinland-Auditoren, Mitarbeiter und Verantwortlichen der TOS gelang innerhalb eines engen Zeitrahmens eine nachweisliche Optimierung unseres Information Security Management Systems.“

(Ulrich Mühlhoff Director Technologie TOS)

Die Zertifizierung bringt conova einen Vorteil bei der Wettbewerbsfähigkeit. Aufgrund der Referenzen, der positiven Erfahrungen anderer Unternehmen, sowie der Professionalität und Freundlichkeit sämtlicher Kontaktpersonen, fiel die Entscheidung auf den TÜV Rheinland.

(Michael Geisler, Informationssicherheitsbeauftragter, conova communications GmbH

Zitate unserer Referenzkunden

„Besonders gut hat uns die Flexibilität bei der Termingestaltung und die Unterstützung im Vorfeld der Zertifizierung nach ISO 27001 durch die Auditoren des TÜV Rheinlands gefallen. Das Auditklima war stets angenehm und den Gegebenheiten unseres Unternehmens angemessen. Die Mischung aus Unterstützung und Eigenbeitrag durch den TÜV Rheinland war optimal.

(Gisela Pohlig, Informations Sicherheits Coordinator der Firma Canon Deutschland GmbH)

„Aufgrund der positiven Erfahrungen unserer Zusammenarbeit können wir jedem interessierten Unternehmen empfehlen, sich von der TÜV Rheinland Cert GmbH im Vorfeld analysieren bzw. zertifizieren zu lassen.“

(Gunther Vaßen, IT-Sicherheitsbeauftragter der ifm electronic GmbH)

„Wir entschieden uns für TÜV Rheinland, da das Unternehmen gleichermaßen in technischen, als auch organisatorischen Aspekten profundes Know-how hat.“

(Harald Weishaupt, Leiter Infrastrukturbetrieb bei ZF)

Antriebs- und Fahrwerktechnik

Ihre Ansprechpartner für Informationssicherheit

Daten sind das Gold der Zukunft!

„90% der auf der Welt heute existierenden Daten sind in den letzten zwei Jahren erzeugt worden.“ (Quelle: Bitkom Newsletter 09/2012)

Ralph Freude
Dipl.-Kfm.

Head of Business Line Information- & Telecommunicationtechnology

TÜVRheinland®
Precisely Right.

TÜV Rheinland Cert GmbH
Krefelderstr. 225
D-52070 Aachen

Tel +49 241-1825-234
Fax +49 221-806 369912
Mobil +49 172-233 1454
Mail Ralph.Freude@de.tuv.com
www.tuv.com