Die Zukunft an Ihrer Seite.

DStGB

VITAKO
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V.

krz
Kommunales Rechenzentrum Minden-Ravensberg/Lippe

# Wie sicher sind die Rechenzentren?

Reinhold Harnisch

Geschäftsführer
stellv. Vorstandsvorsitzender der VITAKO
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V.

12. DStGB-Fachkonferenz
„Bürgernahe Sicherheitskommunikation für Städte und Gemeinden“

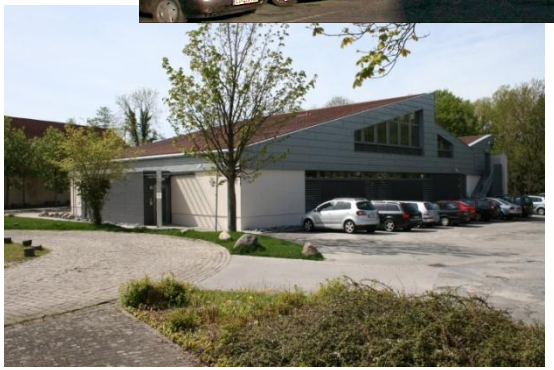
13. Juni 2012

# Agenda

- **Kurzvorstellung „krz – Der zertifizierte Service-Provider in Ostwestfalen-Lippe “**
  - Wer wir sind
  - Was wir tun
  - Wie wir es tun
- **Wie sicher sind die Rechenzentren heute?**
  - Viren, Würmer, Spammer: Bedrohungen der IT-Sicherheit
- **Wie viel IT-Sicherheit braucht ein Rechenzentrum morgen?**
- **Fazit**

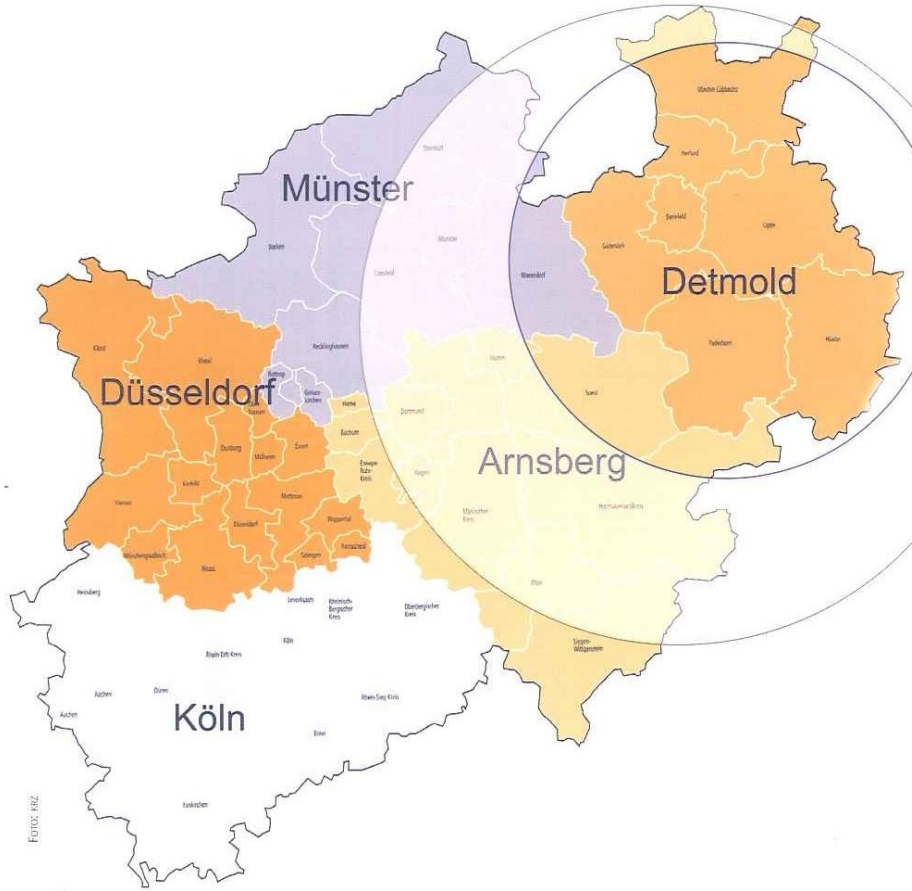
# Der kommunale Service-Provider

- 1971 Gründung
- 1972 Betriebsaufnahme
- Kommunaler Zweckverband (seit 1977)
- IT-Dienstleister für Kommunalverwaltungen und kommunale Einrichtungen
- ca. 7.500 IT-Arbeitsplätze im Verbandsgebiet
- Umsatz 2011: rd. 26 Mio. €
- über 195 Mitarbeiterinnen und Mitarbeiter



# Kunden und Anwender

- 3 Kreise, 34 Städte und Gemeinden
  (ca. 900.000 Einwohner im Zweckverband)
- Eigenbetriebe, Werke
- Gemeinnützige Vereine und Gesellschaften
- Kooperationen (OWL, Siegen, Rhein-Erft-Rur)
- Ca. 600 Kommunale Anwender in
  dreizehn Bundesländern



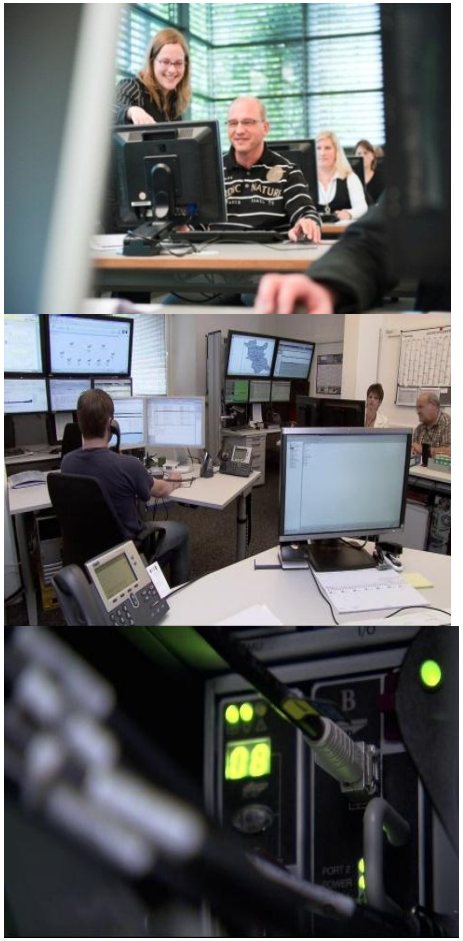

- Direkt oder indirekt werden über 9 Mio. Einwohner
  in NRW mit Services des krz betreut

# Die Aufgabenbereiche

- **Finanzwesen**
  (Finanzwesen, Gebühren, Steuern, Workflow  Zahlungseingang, …)
- **Sicherheit und Ordnung**
  (Meldewesen, Ausländerwesen, Wahlen, Verkehr, Personenstandswesen Verwarn-/Bußgeld…)
- **Schulen und Bildung**
  (Schulverwaltung Schild-Zentral, Schüler Online, Bibliotheken …)
- **Soziales und Jugend**
  (Sozialleistungen, Jugendfürsorge …)
- **Bau und Vermessung**
  (Bauverwaltung, Liegenschaftskataster, Kanal- und Straßenkataster, Geodaten-Server …)
- **Innere Verwaltung**
  (Personalwirtschaft, Zeitwirtschaft, Ratsinformationssysteme, Beihilfe …)
- **Querschnittsaufgaben**
  (DMS, Archivierung, CMS, Internethosting, E-Mail, Virtuelle Poststelle)

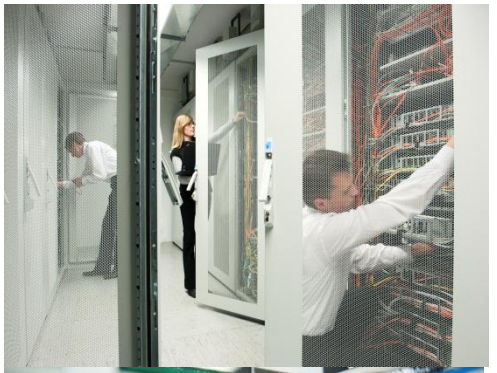
# Wichtige weitere Leistungsbereiche

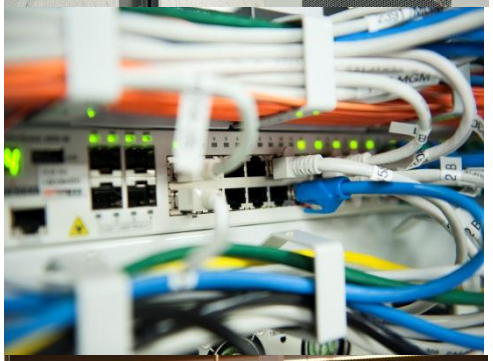
- **Schulungen**
  (Präsenzschulungen, WBT)
- **Consulting/Projektberatung**
- **Outsourcing und „Service vor Ort“**
- **Technische Dienste**
  (RZ-Betrieb, Netzwerk, Druck und Versand, ASP-Lösungen „aus der Steckdose“: z.Zt. 190 veröffentlichte Anwendungen)
- **Software-Entwicklung** (z.B. Übergangsmanagement Schüler Online, GISMA, EU-DLR)
- **Datenschutz / Programmprüfung / Informationssicherheit**
- **Handelsprodukte**
  (Hardware, Standardsoftware, Zubehör, Finanzierung)



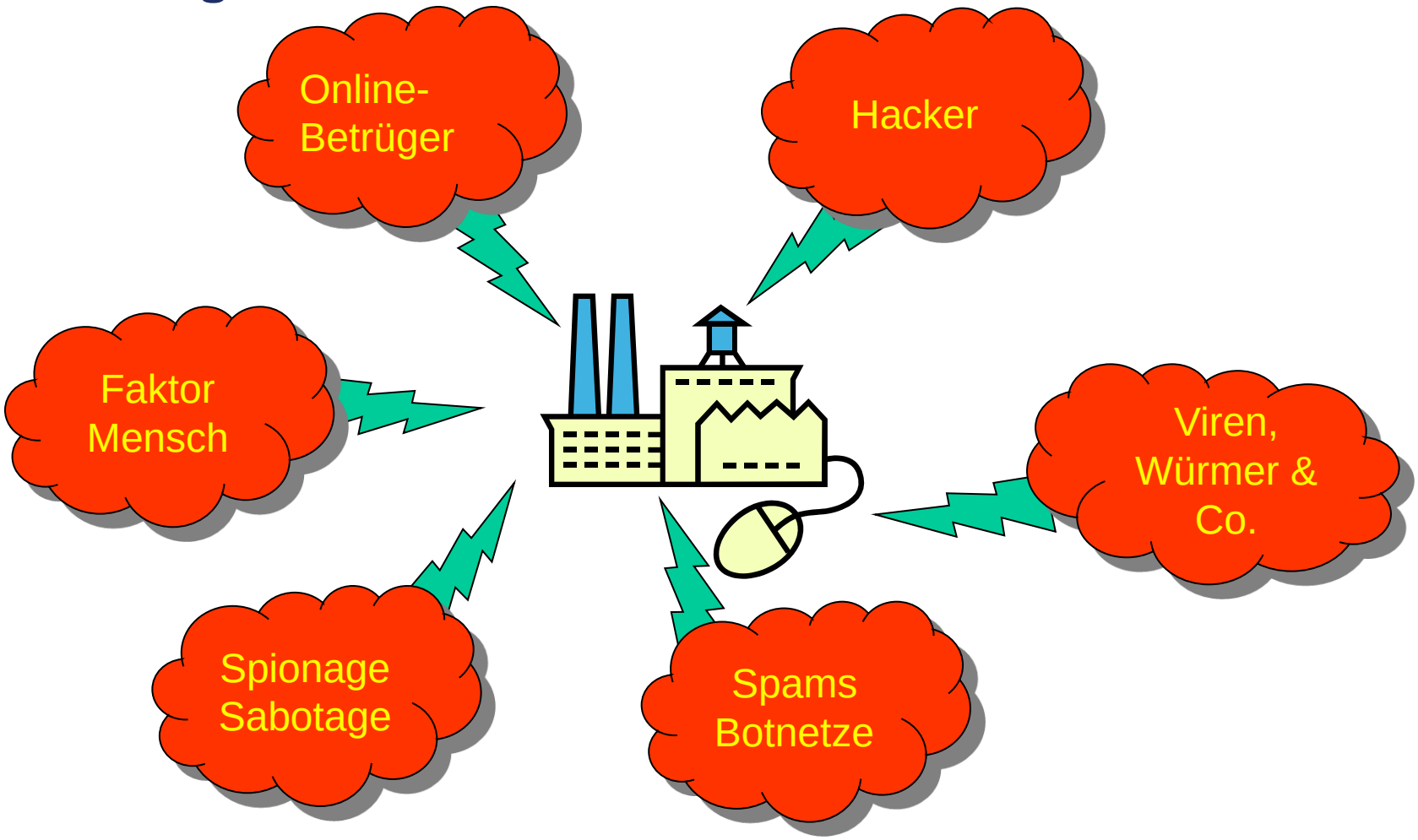
# Die Technik

- **Server**
  (homogene, energieeffiziente Serverfarm, Konsolidierung, Virtualisierung)
- **Speichersysteme**
  (gespiegelte Datenbestände an zwei Standorten, Datensicherungen an zwei Standorten)
- **Netzwerk**
  (Festverbindungen (krz-Netz), regionale Richtfunkstrecken (OWL-Netz), VPN-Technik (Internet), DOI (Behördennetz)), getrennte Netzwerkstrecken
- **Druck- und Versandzentrum**
  (Hochleistungsausstattung)

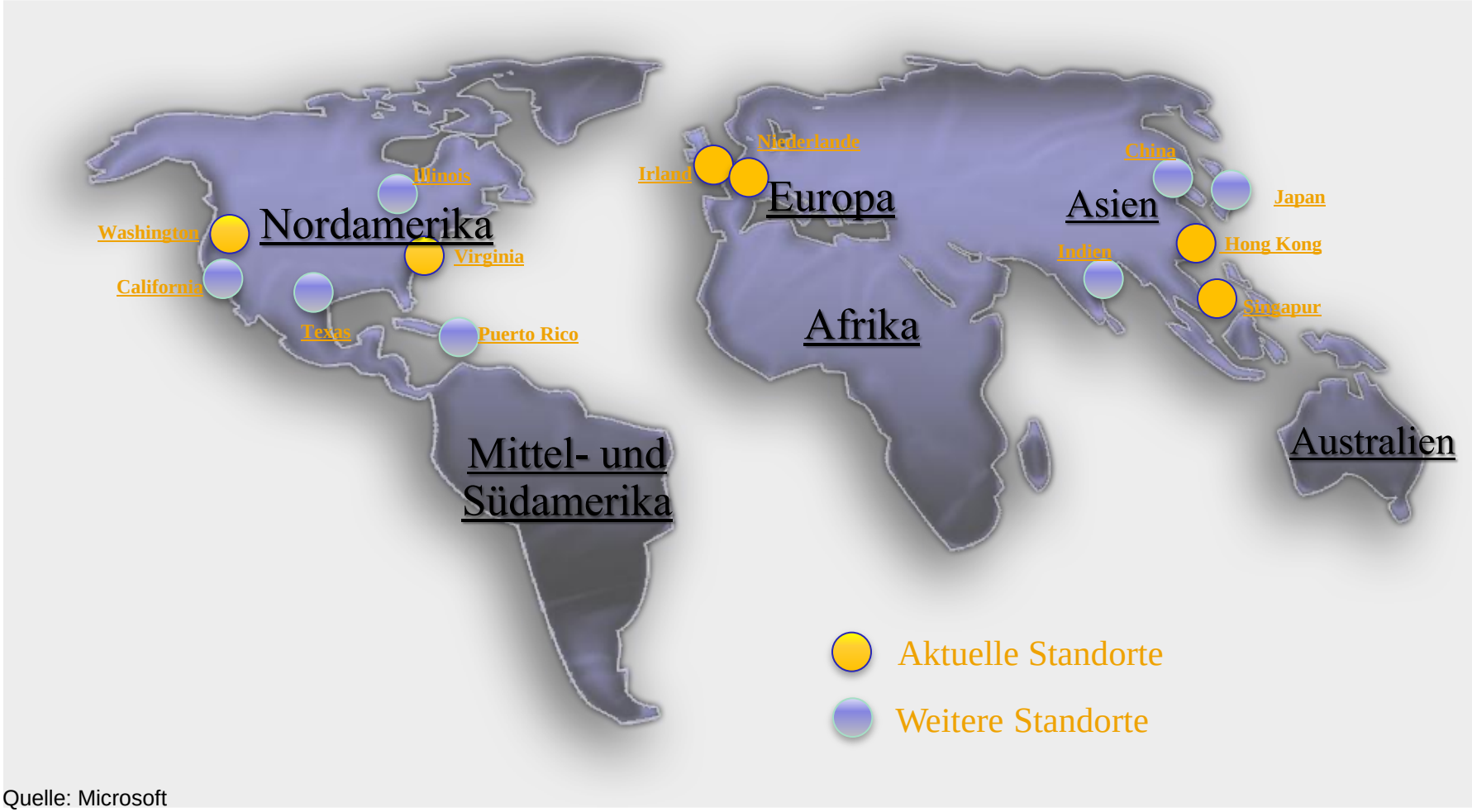




# Wie sicher sind die Rechenzentren?
# Bedrohungen der IT-Sicherheit



# Am sichtbarsten werden die Probleme beim Megathema Cloud-Computing (Amazon, Google, IBM, Microsoft)




Quelle: Microsoft

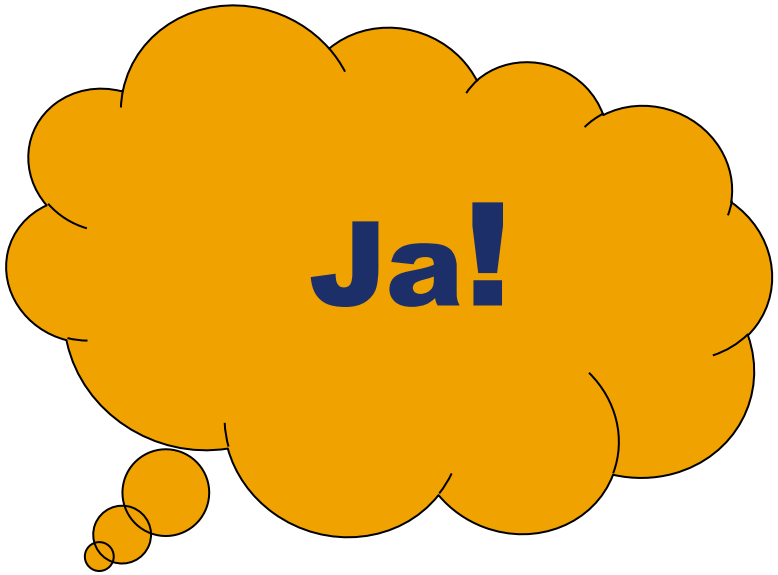
# Cloud-Computing / Datenschutz und Datensicherheit (DuD)

- Für den Betrieb von (Public)Clouds fehlt es bisher an tragfähigen Konzepten zu DuD
- Es gibt gefühlte Sicherheitsbedenken insbesondere bei Schnittstellen
- „Cloud-Datenschutz“ ist vor allen Dingen wegen globalisierungsbedingter Durchsetzungsdefizite grundsätzlich problematisch
- BSI im Lagebericht 2011: International anerkannte Standards sind zu erarbeiten und zu etablieren, auf deren Grundlage Cloud Computing-Plattformen sicherer genutzt und betrieben sowie überprüft und zertifiziert werden können.
- *„Wer heute in einer Public Cloud Personendaten verarbeitet, handelt regelmäßig unverantwortlich und rechtswidrig “*

  *(Thilo Weichert, Leiter des ULD Schleswig-Holstein)*

**Trotzdem Cloud Computing ?**

# Trotzdem Cloud-Computing?




- zur Private Cloud eines öffentlich-rechtlichen IT-Dienstleistungszentrums wie z. B. dem krz
- Denn: Die kommunalen Rechenzentren gehören zu den Vorreitern des Cloud-Computing

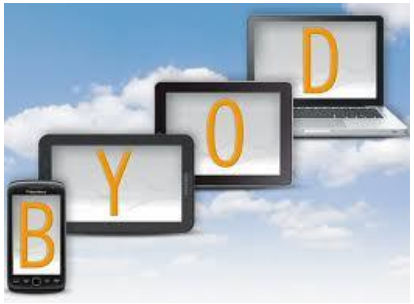
# krz-Cloud: Sicherheit und Wirtschaftlichkeit auf höchstmöglichem Niveau


- Öffentlich-rechtlich (gesetzeskonform)
- Rechtssicher (Datenschutz, Datensicherheit)
- Wirtschaftlich (über 600 öffentliche Kunden)
- Integriert (alles aus einer Hand – Single Point of Contact)
- Standardisiertes IT Service Management (konsequente Ausrichtung des ITSM am Rahmenwerk ITIL (IT Infrastructure Library) V3
- Sicher (BSI Grundschutz-Zertifikat)

# krz: Sicher? Technisch ganz sicher!

- **2-Häuser-Konzept**
- **Notstromversorgung**

- **Verschlüsselung**
- **Virenschutz** (TrendMicro)
- **Spamfilter** (NoSpamProxy)
- **URL-Filter**
- **Firewalls und Applikation-Firewalls**
- **Mobile Device Management**

# Spamvolumen 2010 im krz

noSpam proxy

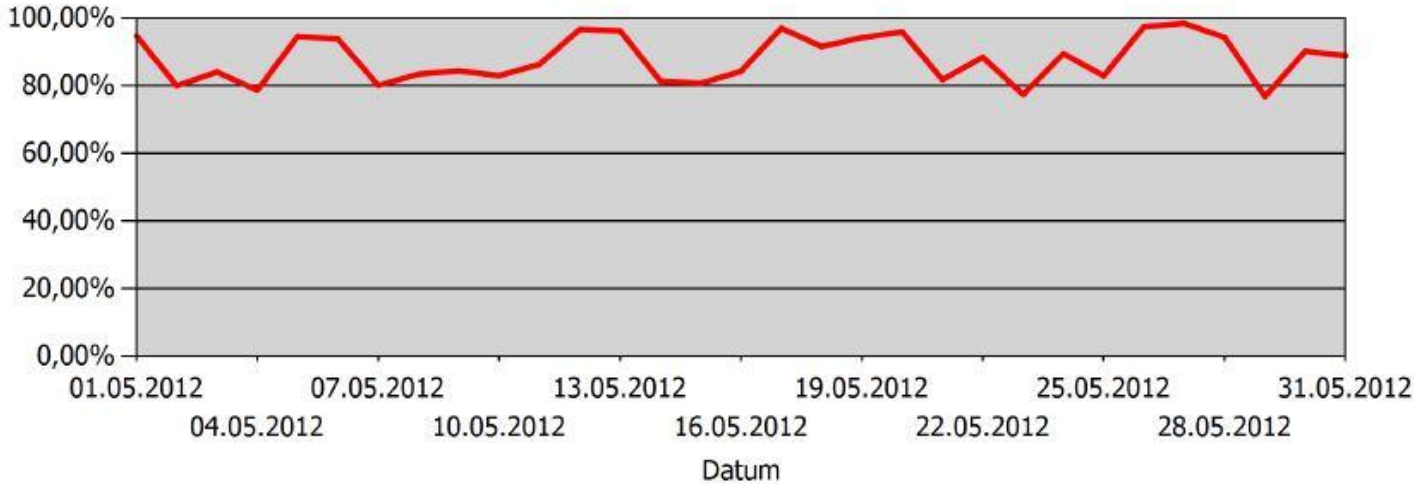
## krz wehrt täglich über 160.000 Spam-Mails ab

(din) Wohl jeder kennt sie: Spams - unerwünschte und omnipräsente E-Mails mit werbenden, sexistischen oder betrügerischen Inhalten. Auch das **krz** muss sich dieser Flut von Datenmüll Tag für Tag erwehren und seine Mitgliedskommunen davor ebenso schützen wie sich selbst. Nach einer aktuellen Statistik des **krz** wurden allein im Mai 2010 etwa 5,2 Mio. E-Mails an die Mitarbeiter der krz-Verbandsmitglieder adressiert. Nur etwa 320.000 dieser E-Mails waren seriösen Ursprungs. Die übrigen knapp 4.9 Mio. E-Mails, also rund 94%, waren Spam-Nachrichten! Damit wehrt das **krz** umgerechnet 160.000 Spam-Mails im Durchschnitt pro Tag ab und schützt so die rund 9.000 Postfächer der Mitgliedsverwaltungen und des **krz**.

Stand: Mai 2010

# Spamvolumen 2012 im krz

## krz wehrt täglich über 105.000 Spam-Mails ab!




Details

| Datum | Datenvolumen | | E-Mails | | |
|---|---|---|---|---|---|
| | Empfangen | Gesendet | Angenommen | Abgelehnt | Gesendet |
| Mai 2012 | 120.131,01 MB | 75.525,91 MB | 425.274 | 3.130.919 | 319.245 |
| Total | 120.131,01 MB | 75.525,91 MB | 425.274 | 3.130.919 | 319.245 |

Stand: Mai 2012

# krz: Sicher? Ganz sicher!

- **BSI-Zertifizierung 2007 nach ISO-27001 auf Basis von IT-Grundschutz**
  Erstes kommunales Service-Rechenzentrum in Deutschland
- **BSI-Re-Zertifizierung 2009 (gültig bis 31.3.2012)**
  Weiterhin erstes kommunales Service-Rechenzentrum
- **BSI-Re-Zertifizierung 2012 (gültig bis 05.03.2015)**
  Zum dritten Mal in Folge: Erstes kommunales Service-Rechenzentrum
- **Überprüfung der Geschäftsprozesse/Qualitätsmanagement**
- **Ohne Datensicherheit kein Datenschutz**
- **Aufgabenwahrnehmung als behördliche Datenschutzbeauftragte für Kunden**
- **Wichtigste Sicherungsmaßnahme: Gut ausgebildete und motivierte Mitarbeiter in Sicherheitsfragen**


Bundesamt für Sicherheit in der Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-IGZ-0102-2012

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Informationsverbund des Kommunalen Rechenzentrums Minden-Ravensberg/Lippe

gültig bis: 5. März 2015*

Der Untersuchungsgegenstand ist der Informationsverbund des Kommunalen Rechenzentrums Minden-Ravensberg/Lippe (KRZ) in Lemgo. Dieses System besteht sich auf den vollständigen Betrieb des Rechenzentrums, alle selbst genutzten oder für Kunden zur Verfügung gestellten Anwendungen oder IT-Systeme einschließlich der dafür erforderlichen RZ-Infrastruktur.

Der oben aufgeführte Untersuchungsgegenstand wurde von Frank-Stefan Stumm, zertifizierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz, in Übereinstimmung mit dem Zertifizierungsschema des Bundesamtes für Sicherheit in der Informationstechnik geprüft. Die im Auditbericht enthaltenen Schlussfolgerungen des Auditors sind im Einklang mit den erbrachten Nachweisen.

Die durch dieses Zertifikat bestätigte Anwendung von ISO 27001 auf der Basis von IT-Grundschutz umfasst die Maßnahmenziele und Maßnahmen aus Annex A von ISO/IEC 27001:2005 und die damit verbundenen Ratschläge zur Umsetzung und Anleitungen für allgemein anerkannte Verfahren aus ISO/IEC 27002:2005. Dieses Zertifikat ist keine Empfehlung des Untersuchungsgegenstandes durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den Untersuchungsgegenstand durch das Bundesamt für Sicherheit in der Informationstechnik ist weder enthalten noch zum Ausdruck gebracht.

Dieses Zertifikat gilt nur für den angegebenen Untersuchungsgegenstand und nur in Zusammenhang mit dem vollständigen Zertifizierungsreport.

Bonn, 6. März 2012

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Bernd Kowalski
Abteilungspräsident

* Unter der Bedingung, dass die ab 6. März 2012 jährlich durchzuführenden Überwachungsaudits mit positivem Ergebnis abgeschlossen werden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon +49 (0)228 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 9582-111

# Wer will mich angreifen?

# Die Evolution der Angreifer

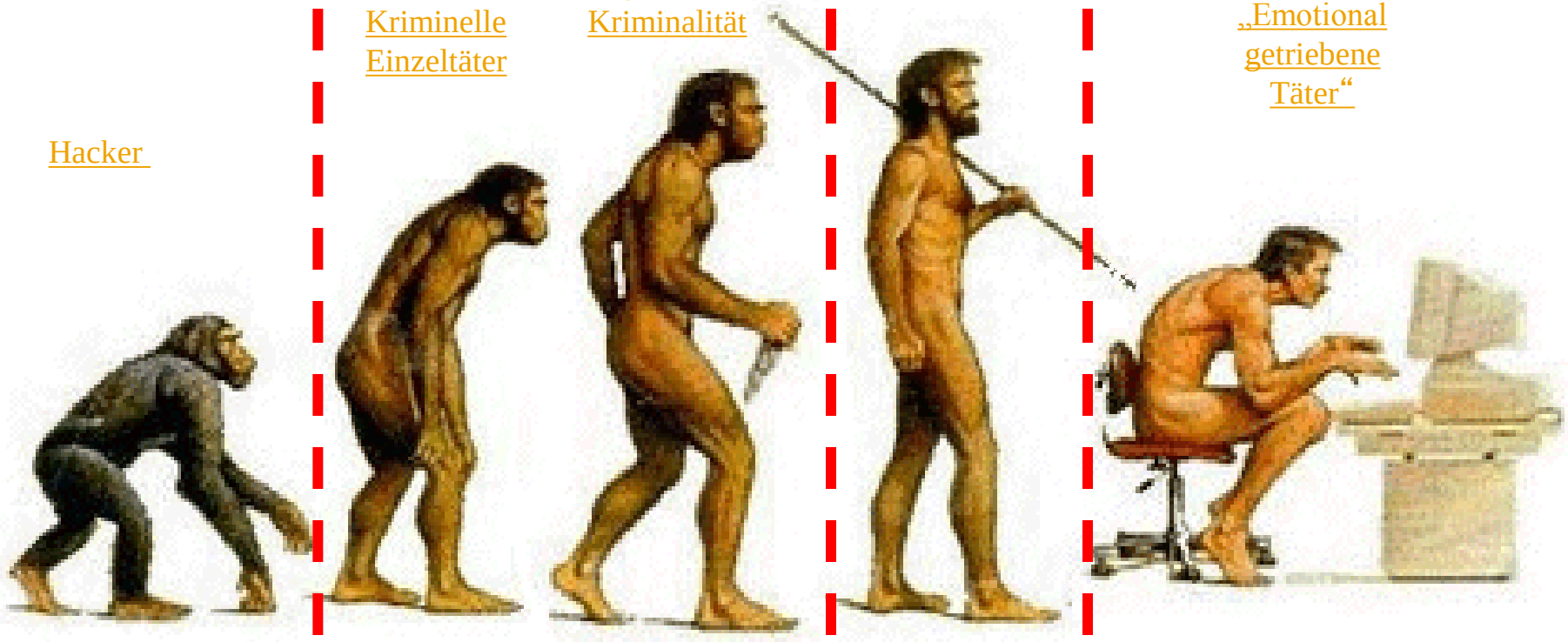
Hacker

Kriminelle Einzeltäter

Organisierte Kriminalität

Staatl. Institutionen

„Emotional getriebene Täter“



Geltungsdrang, Spieltrieb

Wirtschaftliche Interessen

Politisch-wirtschaftl. Interessen

Frust & Rache

Quelle: HiSolution AG

# Was ist IT-Sicherheit?

Das ist der **Zustand eines IT-Systems**, in dem Risiken, die beim Einsatz dieses IT-Systems vorhanden sind, **durch angemessene Maßnahmen auf ein tragbares Maß beschränkt werden.**

- IT-Sicherheit betrifft aber nicht nur IT-Komponenten, sondern auch
  - Organisation
  - Personal
  - Räumliche Infrastruktur
  - Arbeitsplätze
  - Betriebsabläufe

# Was ist das?

# Evonik schützt sich mit Keksdosen vor Lauschangriffen

Vor allem wegen seiner Lithium-Ionen-Batterien für Elektroautos fürchtet Evonik Spionageangriffe und schützt sich mit unkonventionellen Mitteln.

# Gründe für Angriffe auf die IT-Sicherheit

- Wirtschaftsspionage (China, USA, Russland, Nordkorea….)
- Staatliche Ermittlungen (China, USA……)
- Militärische Interessen (Iran, Stuxnet, Duqu, Flame)
- Kriminelle Internetkonzerne in Kolumbien, Rumänien, Tallin
- Neugier, spielerische Herausforderung (Hackergruppen LulzSec, Anonymus)
- Langeweile, Frust

- „Die meisten Schadprogramme sprechen Chinesisch!“
(Eugene Kaspersky)

# Konsequenzen

**Entnetzung** - Rückschritt als Fortschritt - Realisierbar ?
(Sandro Gaycken in seinem Buch Cyberwar)

- Sensible und kritische Systeme maximal reduzieren
- Verbindungen an große, externe Netze restlos kappen
- Bietet Sicherheit und ist verträglich mit allen Freiheitsrechten
- Trend zur Entnetzung

**China hat die Entnetzung schon weitgehend umgesetzt. Der gesamte internationale Traffic läuft über vier zentrale Gateways; regionale Netzcluster können schnell und zentral vom Netz getrennt werden. Sensible Systeme dürfen schon seit 2000 nicht an größere, externe Netze angeschlossen werden und ausländische Software darf überhaupt nur begrenzt eingesetzt werden.**

# Konsequenzen / Cyberabwehr in Deutschland

- Wichtige IT-Komponenten werden im Ausland hergestellt
  - Betriebssystem
  - Internet-Router von Cisco (Bundeswehr)
  - Computerchips (Produktion in Asien)
  - Netzausrüster Huawei (chinesische Vermittlungstechnik bei British Telecom und dem DFN)

- **Ist der Vorsprung noch aufholbar und kann die Kontrolle über diese wichtigen Komponenten zurückgewonnen werden?**

# Konsequenzen / Cyberabwehr in Deutschland

- Geheime Arbeitskreise sollen Antworten finden
  (BMI, Siemens, Bosch, Telekom)
- Bund richtet Kompetenzzentren für IT-Sicherheit in Saarbrücken, Darmstadt und Karlsruhe ein
- Aufbau des Cyber-Abwehrzentrums beim BSI (10 MA)
- NRW-Cybercrime-Kompetenzzentrum LKA (100 MA)
- Bund stellt 30 Millionen für Forschung im Bereich IT-Sicherheit bereit
- Einrichtung einer Task-Force „IT-Sicherheit in der Wirtschaft“
  (Rund ¾ der kritischen Infrastrukturen sind in privater Hand -BITKOM-)

# Schutz der öffentlichen Verwaltung
## (Horst Flätgen, Vizepräsident des BSI):

- BSI betreibt mit seinem Computer-Emergency-Response-Team (CERT) und dem Nationalen Cyber-Abwehrzentrum in Bonn eine Art Frühwarnsystem des Bundes
- Er macht aber auch darauf aufmerksam, dass eine vergleichbare Institution auf Länderebene nicht existiert
- Einen „direkten Draht“ zu den Kommunen gibt es erst recht nicht

„Im kommunalen Bereich aber sind die Folgen von Gesetzen und Verordnungen in der Regel am stärksten spürbar. Doch werden im legislativen Prozess weder die Konsequenzen für die Arbeitsprozesse noch die hochkomplexen IT-Infrastrukturen berücksichtigt“.

Dr. Marianne Wulff, Geschäftsführerin von VITAKO

# Schutz der öffentlichen Verwaltung
## (Franz-Reinhard Habbel, Sprecher des DStGB)

- Bund ist für viele internationale „Bedroher“ interessant
- Unterschiedliche Gefährdungstatbestände
- Einheitliche Sicherheitsstandards für ebenübergreifende Fachanwendungen
- Einheitliches IT-Sicherheitsmanagement durch Etablierung von Verantwortlichen für die Umsetzung der Sicherheitsziele auf allen Ebenen
- Nicht jede kleinste Kommune wie Fort Knox sichern; deshalb verlangen die Kommunen bei der Verabschiedung von Leitlinien zur IT-Sicherheit auch ein Mitspracherecht ihrer Verbände

# Was ist in der öffentlichen Verwaltung „durchsetzbar“ ?

- **IT-Planungsrat**
  - **Schwerpunktthema : IT-Sicherheit**
    Kooperationsgruppe Leitlinie Informationssicherheit
    (Städtetag, VITAKO wurden „gehört“, aber die Anregungen zum kommunalen Bereich sind im Entwurf nicht erkennbar; zumindest BSI-Grundschutz enthalten); öffentliche Verwaltung nur Bund und Länder ?
  - **Schwerpunktthema : Nationale eGovernment-Strategie (NEGS)**
    Kooperationsgruppe für die Ausgestaltung NEGS
    (Das Umsetzungskonzept liegt vor und bezieht den kommunale Bereich explizit ein: „Entwicklung und Verabschiedung einer gemeinsamen IT-Sicherheitsstrategie von Bund, Ländern und Gemeinden“)
- **Handlungsleitfaden nPA** des BMI (Entwicklung Sicherheitskonzeptes)
  - Einführung lag in der Verantwortung durch Länder und Kommunen

# Was ist in der öffentlichen Verwaltung „durchsetzbar“ ?

- **Landesebene (NRW)**
  - **Projekt IDV (Integriertes Datenverarbeitungssystem Verbraucherschutz)**
    Das Landesamt für Natur, Umwelt und Verbraucherschutz erstellt eine IT-Sicherheitsleitlinie, die Bestandteil des Rahmenvertrages zwischen dem Land NRW und den beiden kommunalen Spitzenverbänden ist.
    Bei der Erstellung und Umsetzung des Sicherheitskonzeptes wird das IT-Grundschutzhandbuch des BSI zugrundegelegt.
  - **IT.NRW**
    Bei der technischen Administration werden grundsätzlich die empfohlenen Maßnahmen gem. Grundschutzhandbuch des BSI angewandt.
- **Die Datenschutzbeauftragten der Länder empfehlen auch die Anwendung von IT-Grundschutz**

# Was ist in der öffentlichen Verwaltung „durchsetzbar“ ?

- **Kommunale Ebene**
  - **Vertreten durch Städtetag / Städte- und Gemeindebund**
    Anhörung / Stellungnahme / Weitergabe
  - **VITAKO (Bundesgemeinschaft der kommunalen IT-Dienstleister)**
    **FAG IT-Sicherheit und Datenschutz:**
    u.a. Erarbeitung eines generellen Fahrplanes für die Einführung eines Informationsmanagementsystems (ISMS) nach BSI-Standard
  - **Kommunale IT-Dienstleister** (Beispiel krz)
    Beratungs- und Auditangebote zur Informationssicherheit
    Angebot eines Basis-Workshop-Paket IT-Grundschutz für Kommunen als Einstieg in ein rechtssicheres Informations-Sicherheits-Management-System
- **Das Vorgehen nach BSI-Grundschutz ist der richtige Weg für ein Mindestsicherheitsniveau.**

# Fazit - I

- **Entnetzung** insbesondere bei den kritischen Infrastrukturen erforderlich?
- **Mindestsicherheitsanforderungen** / Standards / Zertifikate für Cloud Computing
- Der Aufbau eines föderalen verwaltungsinternen **Warn- und Informationsdienstes** (Cert-Verbund) ist für die IT-Sicherheit von besonderer Bedeutung.
- Das Vorgehen nach **BSI-Grundschutz** ist der richtige Weg für ein Mindest-sicherheitsniveau und bietet damit die Möglichkeit auf einer ersten Stufe für unterschiedliche Ebenen einheitliche Sicherheitsstandards zu erreichen.

# Fazit - II

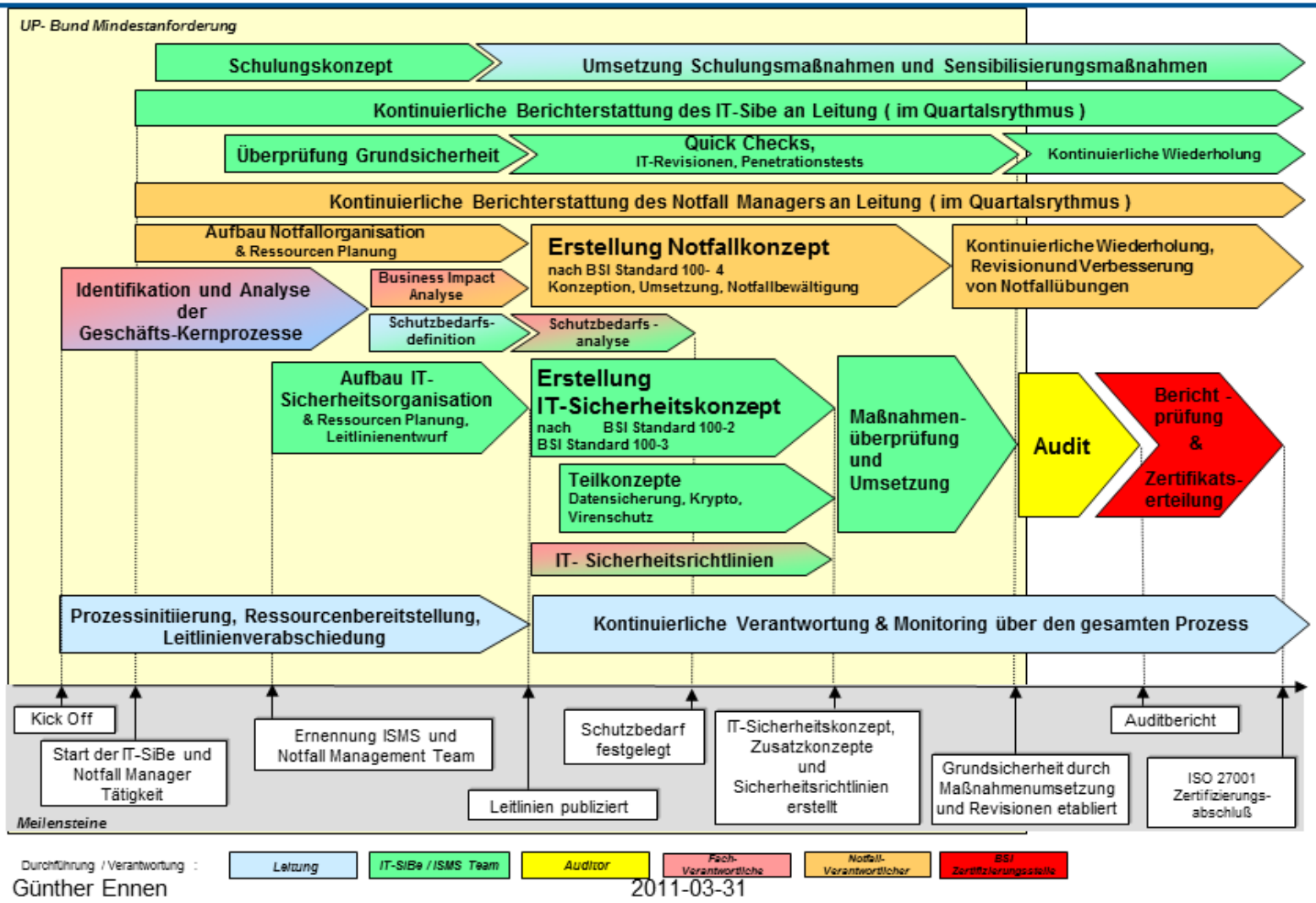
- Eine **Zertifizierung nach ISO 27001** auf der Basis von IT-Grundschutz stellt für Rechenzentren nicht nur ein wichtiges Qualitätsmerkmal dar, sondern gilt z. B. als Voraussetzung für den Betrieb eines eID-Servers. Auch die elektronischen Funktionserweiterungen des nPA werden nur von Bürgern und Unternehmen angenommen, wenn ihre Daten sicher sind.

- In der VITAKO-FAG IT-Sicherheit und Datenschutz wird u. a. durch gegenseitigem Wissens- und Erfahrungsaustausch an der Einführung von **Informationssicherheitsmanagementsystemen** (ISMS) für weitere Gebietsrechenzentren gearbeitet. Dies kommt auch den Kommunen zu Gute.

Bundesamt
für Sicherheit in der
Informationstechnik

# IT- Sicherheit gestalten

## Prozessgesamtübersicht mit Meilensteinen



**„Sicher ist, dass nichts sicher ist.**
**Selbst das nicht!“**

Joachim Ringelnatz

Die Zukunft an Ihrer Seite.

Kommunales Rechenzentrum
Minden-Ravensberg/Lippe

# Vielen Dank für Ihre Aufmerksamkeit

Reinhold Harnisch
Geschäftsführer

Kommunales Rechenzentrum
Minden-Ravensberg/Lippe
Am Lindenhaus 21
32657 Lemgo

Tel: 05261/252-100
r.harnisch@krz.de
www.krz.de

Die Zukunft an Ihrer Seite.

krz

Kommunales Rechenzentrum
Minden-Ravensberg/Lippe

# Kunden
# rundum
# zufrieden