Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

ISO 27001 und IT Compliance

Das Internet...

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

13.11.1990, Tim Berners-Lee

...ist 23 Jahre nach seiner Erfindung immer noch Neuland!

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

heise online > News > 2013 > KW 25 > Merkel: "Das Internet ist für uns alle Neuland"

19.06.2013 15:45 « Vorige | Nächste »

Merkel: "Das Internet ist für uns alle Neuland"

vorlesen / MP3-Download

Nach der internationalen Kritik an amerikanischen Internet-Spähprogrammen hat US-Präsident Barack Obama mehr Transparenz versprochen. Im Anschluss an ein Treffen mit Bundeskanzlerin Angela Merkel (CDU) in Berlin versicherte er, dass sich die US-Geheimdienste künftig eng mit ihren deutschen Partnern abstimmen würden und auch die Öffentlichkeit mehr Informationen bekommen solle. Obama verteidigte die Datensammlung durch den amerikanischen Geheimdienst NSA aber als unverzichtbar für die Terrorabwehr: "Die Folge davon ist, dass wir Leben retten."

Obama und Merkel im Kanzleramt

Bild: bundeskanzlerin.de

Merkel sagte, die Menschen hätten Sorge, dass es eine "pauschale Sammlung aller Daten" gebe. "Die Fragen, die noch nicht ausgeräumt sind – und solche gibt es natürlich – die werden wir weiter diskutieren." Deutschland schätze die Zusammenarbeit mit den USA in Fragen der Sicherheit. Der US-Geheimdienst habe in der Vergangenheit wichtige Informationen geliefert – etwa über die sogenannte Sauerland-Gruppe, deren geplante Anschläge in Deutschland

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

WARUM SOLLTE MAN EIN INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM HABEN…

LANGES WORT, ODER..?

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Warum ein ISMS?

- Bei uns ist noch nie etwas passiert…
- Unsere Mitarbeiter sind schon sensibel genug…
- Wir haben gar keine (wichtigen) Daten…
- Wer soll uns denn kontrollieren…
- Dafür haben wir keine Zeit…
- Dafür gibt’s kein Budget…

„Projekt Datenschutz“

Datenschutzvorfälle in Unternehmen, Organisationen und Behörden und Datenschutz-Aktivitäten der Politik

Suche nach:

- **Home**
- Das Projekt
- News
- Blog „Datenschutz“
- Links
- Twitter
- Kontakt/Impressum

Datenschutzvorfälle

Datum	Ort	Datenherkunft	Organisation	Betroffene	Anz. Betroffene	Kurzbeschreibung
09.03.2013	Burscheid	Avadas GmbH	Unternehmen	Kunden	16.000	Deutscher Avast-Distributor wurde Opfer eines Hacker-Angriffs
01.02.2013	Berlin	JT Touristik	Unternehmen	Kunden	5.000	Ryanair-Kundendaten einsehbar: Wieder Datenpanne bei Unister
14.01.2013	Niedersachsen	Rathaus Göttingen	Öffentliche Verwaltung	Bürger	einige	Rathaustoilette als Aktenlager
14.12.2012	Berlin	DaWanda	Unternehmen	Onlinenutzer	einige	Sicherheitsprobleme bei DaWanda
07.12.2012	Bremen	Jobcenter Bremen-Mitte	Behörde	Antragsteller	mehrere	Arbeitsamt achtet nicht auf Datenschutz
08.11.2012	Baden-Württemberg	Fürst-Stirum-Klinik Bruchsal	Unternehmen	ehemalige Patienten	einige	Baden-Württemberg: Patientenakten gestohlen
07.11.2012	Beringhausen	Veramed-Klinik	Unternehmen	ehemalige Patienten	einige	Dritter Datenskandal um insolvente Klinik-Ruine
04.11.2012	Leipzig	Urlaubstours.de	Unternehmen	Flugreisende	4700	Datenleck bei der Online-Gruppe Unister
12.10.2012	Baden-Württemberg	Kreiskrankenhaus Rastatt und medizinisches Versorgungszentrum Mittelbaden	Unternehmen	Aktuelle und ehemalige Patienten	Hundertausende	Baden-Württemberg: Patientendaten verschwunden
03.10.2012	Nordrhein-Westfalen	Piratenpartei	Deutsche Politik	Parteimitglieder	Mehrere	Datenschutzpanne in der Piratenpartei
21.08.2012	Deutschlandweit	Allianz	Unternehmen	Allianz-Kunden	Mehrere	Schwere Datenpanne bei der Allianz
02.08.2012	Deutschlandweit	Mister Spex	Unternehmen	Mister Spex-Kunden	Unbekannt	Hacker-Angriff auf Internetoptiker Mister Spex - Kundendaten geklaut
12.07.2012	Deutschlandweit	Credit Suisse Bank	Unternehmen	Bankkunden	2.000	Steuerhinterziehung: Credit-Suisse-Kunden fliegen durch Datenpanne auf
16.06.2012	Korschenbroich	Email-Postfach	Bildungseinrichtung	Lehrerin	1	Hacker knacken Schulpostfach
06.06.2012	Berlin	Egmont Ehapa Verlag	Unternehmen	Registrierte User des Portals lustiges-taschenbuch.de	24.000	Hacker knacken Lustiges-Taschenbuch-Datenbank
05.06.2012	Kassel	Klinikum Kassel	Unternehmen	Patienten	Rund zwanzig	Datenpanne in Kasseler Krankenhaus
31.05.2012	Tübingen	ttg team training GmbH	Unternehmen	Bürger	Mehrere	Personendaten von Tübinger Weiterbildungsfirma auf der Straße

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Warum ein ISMS?

Rechtliche Rahmenbedingungen
- Basel II
- Sarbanes-Oxley Act SOX
- KontrAG
- Datenschutz

- Konkurrenz
- Spionage
- Terrorismus

Physikalische Bedrohung
- Einbrecher & Diebe
- Vandalismus

Katastrophen
- Unwetter
- Blitzeinschlag
- Hochwasser
- Brand

Internet
- Viren & Würmer
- Hackerangriffe
- Unvorsichtiges Surfen

- Mitarbeiter
- Unwissenheit
- Leichtsinnigkeit
- Demotivation

Gesetzliche Rahmenbedingungen

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

- Telemediengesetz (TMG)
- Telekommunikationsgesetz (TKG)
- Bundesdatenschutzgesetz (BDSG)
- Gesetz gegen den unlauteren Wettbewerb (UWG)
- Über 70 weitere Gesetze zur „IT Compliance“!

Projekt 29

Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

NUR SO ALS BEISPIEL...

DATENSCHUTZ!

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

BDSG

- Das BDSG ist seit 1996 ein gültiges Bundesgesetz.

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

BDSG

- Dennoch kennen nur 26%
  von 1.000 angestellten Geschäftsführern
  den Inhalt dieses Gesetzes!

(Quelle: Institut Allensbach – Umfrage 2013)

???

???

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Andrea Voßhoff

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Ihre Ernennung wurde von Datenschützern kritisiert, da Voßhoff in ihrer Zeit als Bundestagsabgeordnete für mehrere datenschutzrechtlich umstrittene Gesetzesvorhaben wie die Vorratsdatenspeicherung, das Zugangserschwerungsgesetz, die Online-Durchsuchung und das ACTA-Abkommen gestimmt hatte.[4]

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

BDSG

Das BDSG ist ein „Verbotsgesetz mit Erlaubnisvorbehalt“?!?

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

BDSG

- Vorschriften zum Umgang und zum Schutz von personenbezogenen Daten.

- Was sind personenbezogene Daten?

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

BDSG

Novellierung zum 01.09.2009: Neuregelungen, etwa bzgl.

- Adresshandel
- Verbesserte Auskunftsrechte des Betroffenen
- Meldepflicht bei Verstößen durch Unternehmen
- Übergangsfrist für personalisierte Werbung bis 1. Juli 2012
- Keine Änderungen für Online-/E-Mail-Marketing

Wesentliche Grundsätze:

- Datensparsamkeit (§ 3a BDSG)
- Erhebung von Daten durch Unternehmen grds. nur mit
- Zustimmung des Berechtigten (der Person), §§ 4, 4a, 28 BDSG
- Nicht benötigte Daten müssen gelöscht/gesperrt werden, § 35 BDSG


Regierung von Mittelfranken - Windows Internet Explorer
http://www.regierung.mittelfranken.bayern.de/aufg_abt/abt1/abt1dsa10.htm
regierung mittelfranken datenschutz
Favoriten
Regierung von Mittelfranken
Regierung von Mittelfranken
Inhalt – Suche
Unsere Aufgaben
Unser Service
Mittelfranken
Wir über uns
Impressum
Start – Aktuelles
Unsere Aufgaben
Sicherheit Kommunales Soziales
Wirtschaft Landesent-wicklung und Verkehr
Planung und Bau
Schule und Bildung
Umwelt Gesundheit Verbraucher-schutz
Gewerbe-aufsicht
Pressearbeit Personal Gleichstellung Datenschutz
Öffentlichkeits-arbeit
Datenschutz
Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich
Wer sind wir?
Tätigkeitsberichte und weitere Informationen zum Datenschutz
Externe Links zu weiteren Datenschutz-Themen
Links zu anderen Datenschutzaufsichtsbehörden
Links zu Datenschutzvorschriften
Kontakt
Suche...
DATENSCHUTZ
PERSÖNLICHKEITSSCHUTZ
Zuletzt geändert am 10.01.2007.
| Seitenanfang | Inhalt/Suche | Impressum/Datenschutz/Haftungsausschluss | Kontakt | ©
2006 Regierung von Mittelfranken, Promenade 27, 91522 Ansbach |
Hier finden Sie unsere Erklärungen zum Impressum, Datenschutz und Haftungsausschluss
http://www.regierung.mittelfranken.bayern.de/allgem/impresum.htm
Internet
100%

Der Tiger hat nun endlich Zähne bekommen!!

Bayerische Datenschützer prüfen Websites auf Datenschutzverstöße

Lars Klatte | 8.05.2012 | Gesetze

Das Tracking-Tool Google Analytics stand lange Zeit in der Kritik der deutschen Datenschutzbehörden. Im September 2011 wurde dann bekannt gegeben, dass dieses Tool bei Einhaltung bestimmter Voraussetzungen rechtskonform einsetzbar sei. Nun hat das Bayerische Landesamt für Datenschutzaufsicht mehrere tausend Webseiten überprüft.

Lesen Sie mehr zum Ergebnis der Untersuchung.

Das Bayerische Landesamt für Datenschutzaufsicht hat insgesamt 13.404 Websites geprüft. Hiervon nutzten 2.449 den Analysedienst Google Analytics. Allerdings wurde dieser von nur 3% der Nutzer – also gerade einmal von 78 Betreibern – datenschutzkonform eingesetzt.

Die Datenschützer werden die übrigen Webseiten-Betreiber nun auffordern, sich an das geltende Datenschutzrecht zu halten und kündigten für Ende Mai bereits den zweiten Prüfdurchgang an.

Projekt 29

Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

ISO 27001 – EINE TOLLE NORM!

ISO 27001 – nicht noch eine Norm!

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

- ☹ **Braucht Zeit**
- ☹ **Viel Geld (Zertifizierung, Rezertifizierung)**
- ☹ **Mehr Personal**
- ☹ **Kompliziertere Arbeitsabläufe**
- ☹ **Verhindert Innovation**

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Oder vielleicht doch?

- ☺ **Methodisches Vorgehen / Soll-Ist-Vergleich**
- ☺ **Vollständige Abdeckung einer best. Menge von Gefährdungen**
- ☺ **Referenzierbare / übertragbare Konzepte oder Maßnahmen**
- ☺ **Praxiserprobte Maßnahmen (Best Practice)**
- ☺ **Optimierung interner Prozesse / klare Vorgaben**
- ☺ **Nachvollziehbare / quantifizierbare IT-Sicherheit**

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Ziele der ISO 27001

Die ISO/IEC 27001 wurde als Modell für den Aufbau, die Verwirklichung Durchführung, Überwachung, Bewertung, Aufrechterhaltung und Verbesserungen eines Informationssicherheitsmanagementsystems ISMS erarbeitet.

Die ISO/IEC 27001 ist Prozessorientiert.
Die ISO 27001 basiert auf dem PDCA – Zyklus.
Die ISO 27001 hat große Übereinstimmung mit ISO 9001.

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Informationssicherheit

Was ist Informationssicherheit?

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Werten unabhängig von ihrer Form. Dies umfasst sowohl schriftliche, bildliche als auch gesprochene Informationen.

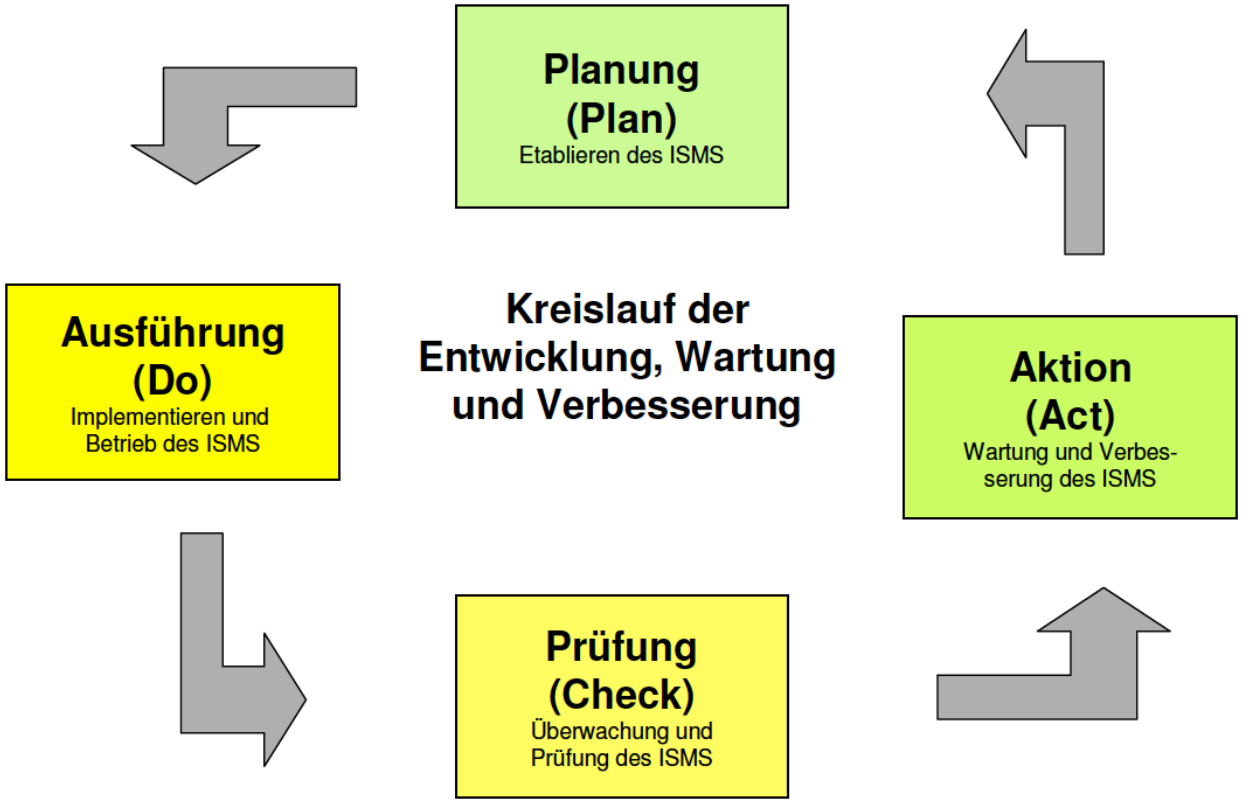
Vertraulichkeit: Eigenschaft dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.

Integrität: Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten.

Verfügbarkeit: Eigenschaft, einer berechtigten Einheit auf verlangen zugänglich und nutzbar zu sein.

PDCA Modell der ISO 27001

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity



Aufbau und Inhalte

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

- Klassifizierung der Unternehmenswerte
- Durchführung einer Risikoanalyse
- Bereitstellung der erforderlichen Mittel
- Verpflichtung der Unternehmensführung zur Sicherheit
- Implementierung des ISMS
- Dokumentation der Unternehmensregeln
- Sensibilisierung der Mitarbeiter
- Regelmäßige Bewertung des ISMS
- Korrektur- und Vorbeugemaßnahmen

Aufbau und Inhalte der ISO 27001

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Die ISO/IEC 27001 besteht aus zwei Teilen.

1. **Generelle Anforderungen an ein ISMS nach 27001**
   ➔ Kapitel 4-8

2. **Spezielle Anforderungen**
   ➔ Anhang A (normativ) Maßnahmenziele und Maßnahmen

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Aufbau und Inhalte

Kapitel 4 - 8

4. **Informationssicherheitsmanagementsystem**
   ➔ **Aufbau und Umsetzung eines ISMS**
   Risikomanagement

5. **Verantwortung der Leitung / Management**
   ➔ **Verpflichtung (Sicherheitspolitik, ISMS)**
   Ressourcenmanagement

6. **Interne ISMS Audits**
   ➔ **In geplanten Abständen durchführen**

7. **Managementbewertung**
   ➔ **Eingaben für Bewertung**

8. **Verbesserung des ISMS**
   ➔**Korrektur- und Vorbeugemaßnahmen**

Aufbau und Inhalte

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Anhang A (normativ) Maßnahmenziele und Maßnahmen

Maßnahmenziele und Maßnahmen:

A.5 Sicherheitsleitlinie / Sicherheitspolitik

A.6 Organisation der Informationssicherheit

A.7 Management von organisationseigenen Werten (Wert = Alles was für die Organisation von Wert ist.)

A.8 Personelle Sicherheit

A.9 Physische und umgebungsbezogene Sicherheit

A.10 Betriebs- und Kommunikationsmanagement

A.11 Zugangskontrolle

A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen

A.13 Umgang mit Informationssicherheitsvorfällen

A.14 Sicherstellung des Geschäftsbetriebes (Kontinuitätsmanagement)

A.15 Einhaltung von Vorgaben (Compliance)

Projekt 29

Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

UND WAS STEHT NUN WIRKLICH DRIN?

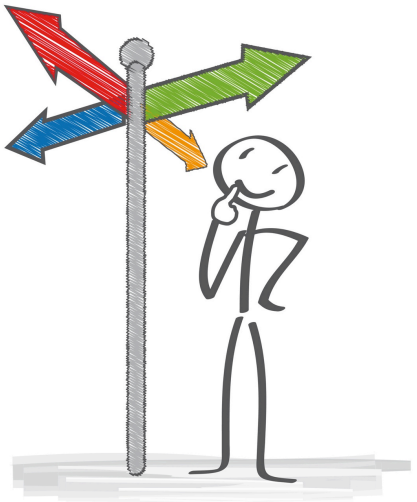
Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.5 Sicherheitsleitlinie / Sicherheitspolitik

Ziel: Richtungsvorgabe und Unterstützung des Managements bei der Informationssicherheit, in Übereinstimmung mit geschäftlichen und gesetzlichen Anforderungen.

- Definition einer Informationssicherheitspolitik
- Regelmäßige Überprüfung der Informationssicherheitspolitik



Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht…

„Die Amerikaner haben Bedarf an Telefonen, aber wir nicht. Wir haben genügend Laufburschen."

(Sir William Herny Pierce – British Postal Office CEO – 1878)

„Es gibt keinen Grund dafür, dass jemand einen Computer zu Hause haben wollte."

(Ken Olsen – Gründer Digitale Equipment – 1977)

„Niemand wird jemals mehr als 640 KB Speicher auf seinem PC benötigen."

(Bill Gates – 1981)

„Das Spam-Problem wird in 2 Jahren gelöst sein."

(Bill Gates – 2004)

Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.6 Organisation der Informationssicherheit

A.6.1 Interne Organisation

Ziel: Handhabung der Informationssicherheit innerhalb der Organisation.

- Definition der Zuständigkeiten, Verantwortlichkeiten, Genehmigungsverfahren, Vertraulichkeitsvereinbarungen etc.

A.6.2 Externe Beziehungen

Ziel: Aufrechterhaltung der Sicherheit von Informationen und informationsverarbeitenden Einrichtungen der Organisation, die mit Externen in Kontakt kommen.

- Umgang mit externen Dienstleistern und Kunden

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht...

Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.7 Management von organisationseigenen Werten (Assets)

A.7.1 Verantwortung für organisationseigene Werte Interne

Ziel: Aufbau und Aufrechterhaltung des angemessenen Schutzes von organisationseigenen Werten. (Informationen zugehörige Prozesse, Systeme und Netzwerke)

- Inventarisierung von Vermögenswerten.
- Verantwortlichkeiten und Regeln für Umgang mit Vermögenswerten

A.7.2 Klassifizierung von Informationen

Ziel: Sicherstellung des angemessenen Schutz von Informationen.

- Regelung welche Informationen wichtig bzw. unwichtig sind.
- Kennzeichnung der Informationen (z.B. Vertraulich, nur für Intern, etc.)

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht…

Täter erriet Sicherheitsfrage zu Lieblingshaustier

Hacker greift Romneys E-Mail-Account an

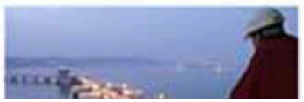
Mittwoch, 06.06.2012, 10:42

Mitt Romney während einer Wahlkampfveranstaltung. Sein privater E-Mail-Account wurde von Hackern angegriffen. Reuters

Der private E-Mail-Account des republikanischen US-Präsidentschaftskandidaten Mitt Romney ist offenbar Ziel eines Hackerangriffs geworden. Das Passwort hierfür war demnach leicht zu knacken – Romney hatte sein Lieblingshautier gewählt.

Ein anonymer Hacker habe sich Zugang zu dem Hotmail-Account Mitt Romneys verschafft, indem er die Antwort auf eine Sicherheitsfrage zum Lieblingshaustier des Politikers erraten habe, berichtete die US-Internetseite „Gawker" am Dienstag (Ortszeit). Der Online-Dienst sei direkt nach der Aktion von dem Hacker selbst informiert worden. Dieser habe sich zudem mit demselben Passwort Zugang zu Romneys Dropbox-Konto verschafft, einem Service zum Austausch von Dateien.

ZUM THEMA



Naja...


Please provide the following Login information.
E-mail
Confirm E-mail
Your Sign-In Question
What was the make of your first car?
Your Answer
Confirm Your Answer
Create Profile
What was the make of your first car?
What is the name of your favorite movie?
What is the name of your favorite TV show?
Who is your favorite actor or actress?
What is the name of your favorite band or musical group?
What is your favorite internet password?
What is the name of the street where you grew up?
What is your favorite food?
What is the name of your favorite restaurant?
What is the name of your favorite cartoon character?
What is the name of your favorite fictional character?
Where did you go on your first date?
What is your favorite pet's name?
What is your best friend's last name?
Life@UPS | About Us |
Site Guide | UPS Global |
Privacy Policy | Trademarks |

Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Ziel: Schutz vor unerlaubtem Zutritt, Beschädigung und Störung der Infrastruktur und der Informationen der Organisation.

- Sicherheitszonen, Zutrittskontrollen, Sicherung von Büros, etc.
- Schutz gegen Umwelteinflüsse (Feuer, Wasser, etc)

A.9.2 Sicherheit von Betriebsmitteln

Ziel: Verhinderung von Verlust, Beschädigung, Diebstahl oder Kompromittierung von Informationen und den zugehörigen Systemen.

- Schutz (unerlaubter Zugriff)
- Versorgungseinrichtungen (Notstrom)
- Verkabelung (Anzapfen),
- Instandhaltung (Verfügbarkeit auf Datenzugriff gewährleisten)
- Sichere Entsorgung (Festplatte)

Bei uns doch nicht...

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Behörden-Daten auf Flohmarkt verkauft

Ganz Glücksburg für 30 Euro

Steuerbescheide, Konzessionen, Gesprächsvermerke, Protokolle und Schreiben: Ein Mann kauft auf einem Flohmarkt mehrere Festplatten und findet auf ihnen sämtliche vertraulichen Dokumente der Stadtverwaltung Glücksburg.

Sämtliche vertraulichen Dokumente der Stadtverwaltung Glücksburg aus mehreren Jahren sind offenbar durch eine schwere Panne in falsche Hände geraten. Nach Recherchen des NDR fand ein Mann aus Glücksburg die Daten auf rund 15 Festplatten und mehreren Servern, die er nach eigenen Angaben auf einem Flohmarkt gekauft hatte.

"So etwas darf nicht passieren. Hier handelt es sich nicht nur um individuelle Nachlässigkeit sondern um Organisationsverschulden der Stadt", sagte der schleswig-holsteinische Datenschutzbeauftragte Thilo Weichert.

Glücksburg ist vor allem für sein Wasserschloss bekannt

Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.10 Betriebs- und Kommunikationsmanagement

A.10.1 Verfahren und Verantwortlichkeiten

Ziel: Korrekter und sicherer Betrieb der Informationsverarbeitenden Einrichtungen.

- Dokumentierte Betriebsprozesse einschl. Änderungsverwaltung, Verantwortlichkeiten
- Trennung von Test- und Produktiveinrichtungen

A.10.2 Management der Dienstleistungserbringung von Dritten.

Ziel: Aufrechterhaltung der Informationssicherheit bei gleichzeitiger Sicherstellung der Dienstleistungserbringung entsprechend der Liefervereinbarung.

- Regelmäßige Überwachung und Überprüfung der Einhaltung

A.10.3 Systemplanung und Abnahme

Ziel: Das Risiko von Systemfehlern und Systemausfällen zu minimieren.

- Kapazitätsplanung (Serverüberlastung)
- System-Abnahme (Kriterien definieren zur Abnahme / Was muss es können?)

A.10.4 Schutz vor Schadsoftware

Ziel: Schutz der Integrität von Software und Informationen.

- Maßnahmen gegen Schadsoftware, Regelung für mobilen Programmcode

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht...

Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.10 Betriebs- und Kommunikationsmanagement

A.10.5 Backup

Ziel: Erhaltung der Integrität und der Verfügbarkeit von Informationen

- Erstellung von Backup

A.10.6 Management der Netzsicherheit

Ziel: Informationen in Netzen und Infrastruktur zu schützen.

- Angemessene Verwaltung und Kontrolle von In und Externen Netzen
- Sicherheitseigenschaften und Adminanforderungen für alle Netze definieren

A.10.7 Handhabung von Speicher- und Aufzeichnungsmedien

Ziel: Unerlaubte Veröffentlichung, Veränderung, Zerstörung von Informationen und Systemen (Assets) sowie Störung des Geschäftsbetriebs verhindern.

- Verwaltung von Wechselmedien (Verfahrensanweisungen)
- Entsorgung von Medien
- Umgang mit Informationen (Verfahren für Umgang und Speicherung von Informationen festlegen)

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht...

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Die Lösung!

Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.11 Zugangskontrolle

A.11.4 Zugangskontrolle für Netze

Ziel: Verhinderung von unbefugtem Zugang zu Netzdiensten.

- Regeln zur Nutzung von Netzen
- Technische Möglichkeiten beachten und nutzen (Routingkontrolle etc.)

A.11.5 Zugriffskontrolle auf Betriebssysteme

Ziel: Verhinderung von unbefugtem Zugriff auf das Betriebssystem.

- Sichere Anmeldung, Benutzerauthentisierung, Passwortverwaltung
- Dienstprogramme einschränken kontrollieren / Session Time-out

A.11.6 Zugangskontrolle zu Anwendungen und Information

Ziel: Verhinderung des unbefugten Zugangs zu Informationen in Anwendungssystemen.

- Einschränkung von Informationszugriff (Benutzerspezifische Zugangskontrolle)
- Isolation sensibler Systeme

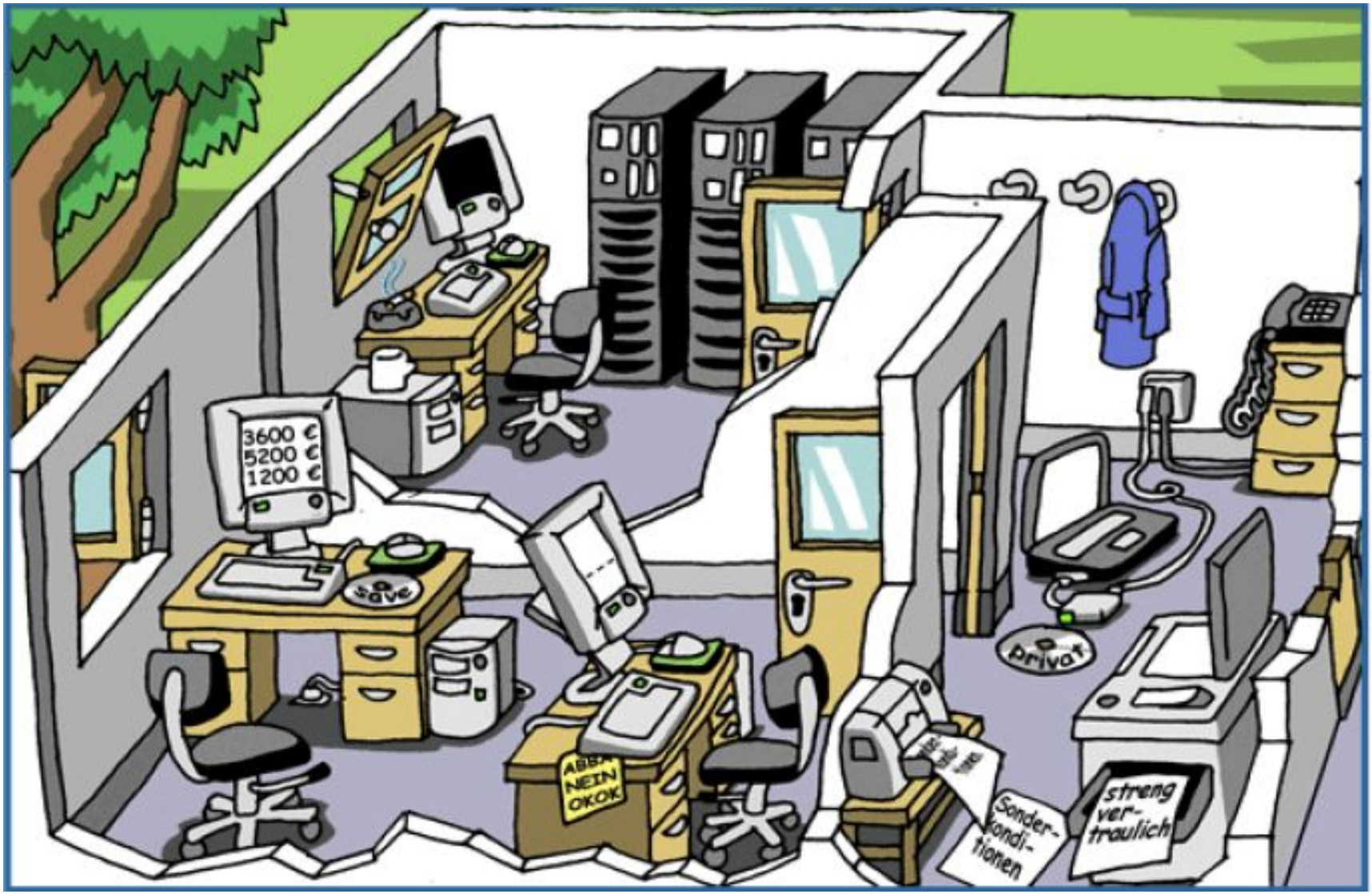
A.11.7 Mobile Computing und Telearbeit

Ziel: Sicherstellen der Informationssicherheit bei mobile Computing und Telearbeit.

- Regelungen, Leitlinien und Maßnahmen zur sicheren Nutzung.

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht...



Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.13 Umgang mit Informationssicherheitsvorfällen

A.13.1 Melden von Informationssicherheitsereignissen und Schwachstellen

Ziel: Schwachstellen in Informationssystemen müssen gemeldet werden, sodass rechtzeitig reagiert werden kann.

- Verpflichtung zur Meldung für Schwachstellen für Alle (Intern und Extern)
- Sicherstellung der geeigneten Kommunikationswege (Managementkanäle)

A.13.2 Umgang mit Informationssicherheitsvorfällen und Verbesserungen

Ziel: Einhaltung eines einheitlichen und effektiven Ansatzes zum Umgang mit Informationssicherheitsvorfällen.

- Verantwortlichkeiten für den Umgang mit Vorfällen festlegen
- Lernen aus den Vorfällen sicherstellen
- Sammeln von Beweisen

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht...

Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.14 Sicherstellung des Geschäftsbetriebes (Business Continuity Management)

A.14.1 Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs

Ziel: Schutz vor Unterbrechung von Geschäftsaktivitäten. Schutz von kritischen Geschäftsprozessen vor den Auswirkungen von Störungen von Informationssystemen sowie Katastrophen. Rechtzeitige Wiederaufnahme von Geschäftsprozessen.

- Gelenkter Prozess zur Sicherstellung des Geschäftsbetriebs
- Identifizierung und Risikobetrachtung von Ereignissen die den Geschäftsbetrieb stören können
- Notfallpläne
- Rahmenwerk für die Notfallpläne festlegen. (Widersprüche vermeiden)
- Regelmäßiges Testen, Überprüfen und Neubewerten der Notfallpläne

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht...

Anhang A

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

A.15 Einhaltung von Vorgaben (Compliance)

A.15.1 Einhaltung gesetzlicher Vorgaben

Ziel: Vermeidung von Verstößen gegen Gesetze, amtliche oder vertragliche Verpflichtungen, sowie gegen Sicherheitsanforderungen.

- Identifikation der relevanten Gesetze
- Schutz von geistigem Eigentum. Beachtung von Urheberschutz bei Software
- Datenschutz und Vertraulichkeit. Verhinderung von Missbrauch

A.15.2 Einhaltung von Sicherheitsregelungen –standards, und technischer Vorgaben

Ziel: Sicherstellung, dass Systeme die Sicherheitsregelungen und -Standards einhalten.

- Manager müssen in Ihrem Verantwortungsbereich die Einhaltung sicherstellen
- Regelmässige Prüfung der Einhaltung der Vorgaben

A.15.3 Überlegungen zu Revisionsprüfungen von Informationssytemen

Ziel: Steigerung der Effektivität und Minimierung der Störungen bei Revisionsprozessen für Informationssysteme.

- Sorgfältige Planung von Revisionsprozesen, um Störungen der Geschäftsprozesse zu vermeiden
- Missbrauch von Tools zur Untersuchung von Informationssystemen vermeiden

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

Bei uns doch nicht...

Informationssicherheit aus Sicht der ISO 27001

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

- Risiken managen und innerhalb einer wirtschaftlichen und sicheren Toleranzbreite halten.
- Spielregeln festlegen (Security Policy)
- Veränderungen wahrnehmen und berücksichtigen
- ISM-System regelmäßig prüfen
- Korrektur- und Verbesserungsprozess umsetzen

Die Enttäuschung ist vorprogrammiert

Kleine Denksportaufgabe: Man braucht es nicht und trotzdem wird es wie verrückt gekauft. Was ist das? Ganz einfach: ein Heimcomputer. Wir prüften sieben Modelle und suchten verzweifelt nach sinnvollen Einsatzmöglichkeiten. Unser Fazit: Wer auf die elektronische Aufrüstung seines Heimes verzichtet, büßt keine Lebensqualität ein.

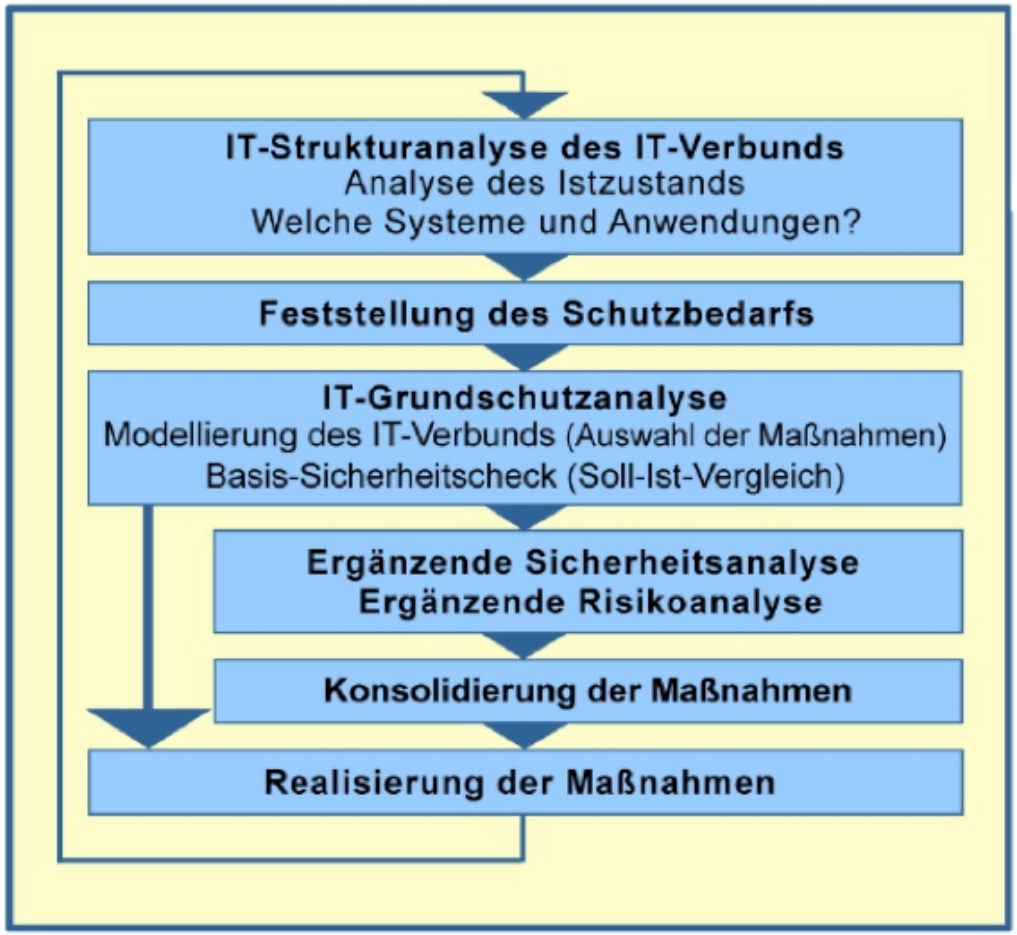
Projekt 29

Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

UND WAS WAR NOCH MAL GLEICH MIT DEM „IT-GRUNDSCHUTZ“?

Zwei Wege, ein Ziel!

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity



Bundesamt
für Sicherheit in der
Informationstechnik

Projekt 29
Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

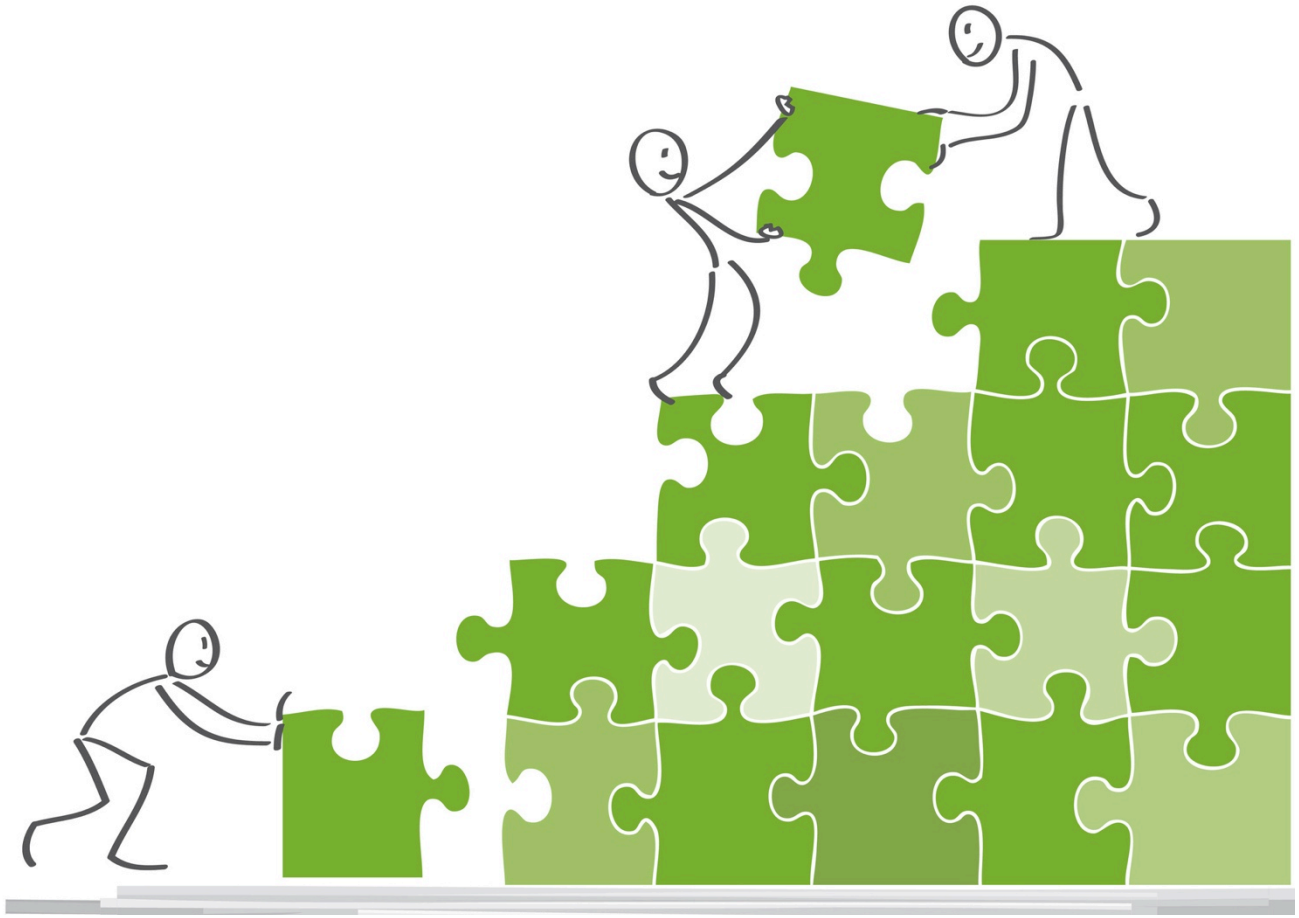
Der Standard

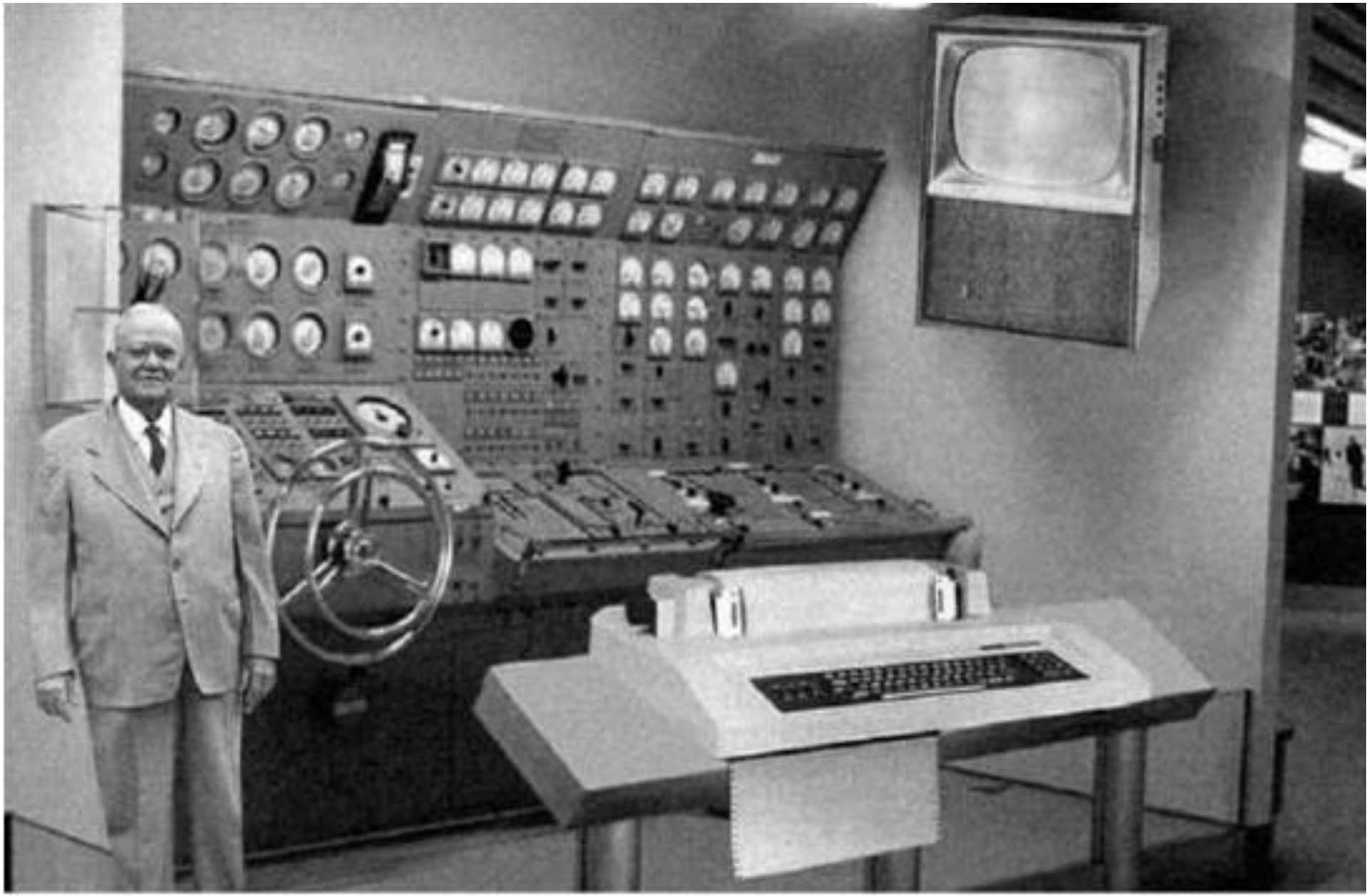
- **BSI Standards**
  - **BSI-Standard 100-1:**
    Managementsysteme für Informationssicherheit
  - **BSI-Standard 100-2:**
    Vorgehensweise nach IT-Grundschutz
  - **BSI-Standard 100-3:**
    Risikoanalyse auf der Basis von IT-Grundschutz
  - **BSI-Standard 100-4:**
    Notfall-Management
- **IT-Grundschutzkataloge**
  - **Loseblattsammlung**
  - **Themenorientierte Bausteine (z.B. Server unter Linux)**
  - **Gefährdungs- und Maßnahmenkataloge**
- **Ermöglicht Zertifizierung nach**
  ISO 27001 auf der Basis von IT-Grundschutz

Projekt 29

Datenschutz | Informationssicherheit
IT Compliance | Business Continuity

FAZIT

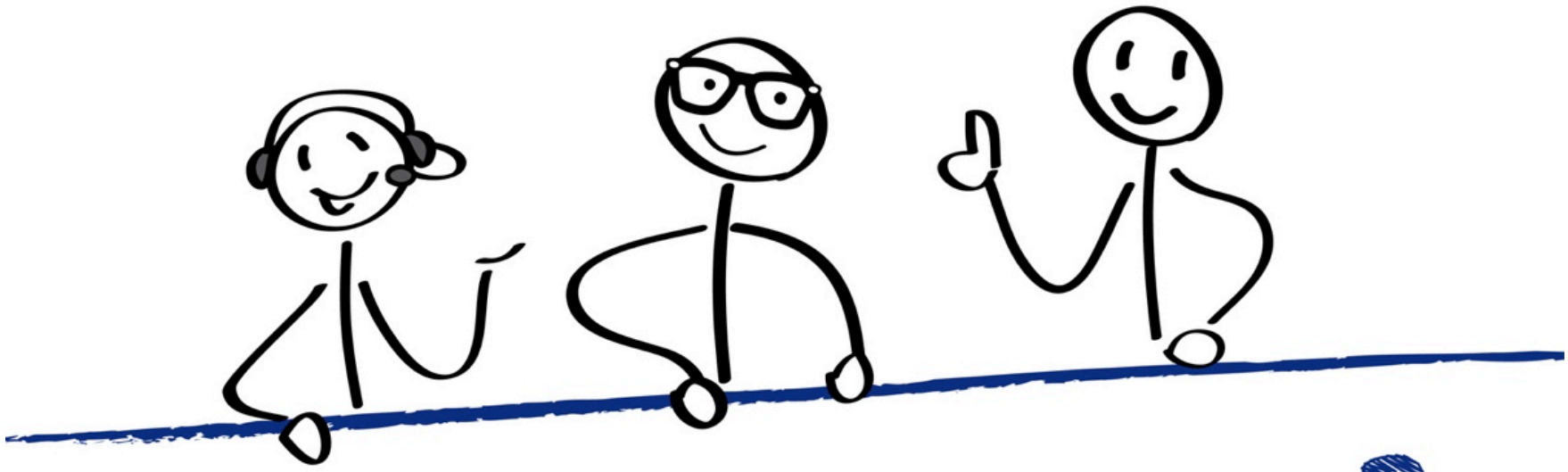




Scientists from the **RAND** *Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 30 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use.*

Projekt 29

Datenschutz | Informationssicherheit
IT Compliance | Business Continuity



Sie haben Fragen?
Wir helfen Ihnen!

Projekt 29

Datenschutz | Informationssicherheit
IT Compliance | Business Continuity