Hochschule Zittau/Görlitz
UNIVERSITY OF APPLIED SCIENCES

Fakultät Elektrotechnik und Informatik

Informationssicherheit – aktuelle Bedrohungen und Herausforderungen

Marietta Spangenberg
Admin-Tag des HRZ
26.4.2016

Kenne Dich selbst …

wir müssen immer und überall

- auf dem aktuellen Stand sein
- auf die Informationen des Unternehmens zugreifen können
- erreichbar sein
- im Internet präsent sein
- und sofort auf eingehende Nachrichten reagieren
- …
- → Kein Problem

Welche Daten verarbeiten wir?

Wer klassifiziert die Daten?

Was sind personenbezogene Daten?

Wer ist verantwortlich?

Wie ist das mit Forschungsdaten?

Verträge mit Dritten?

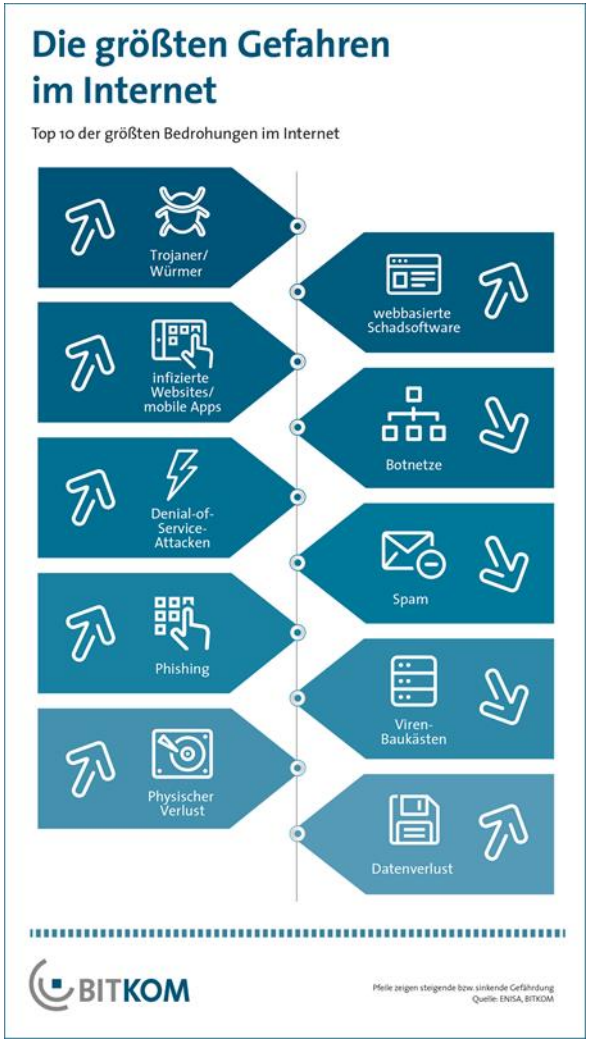
Welche Werte haben wir?

…

Hochschule – Freiheit von Forschung und Lehre = interessantes Ziel für Angreifer?

… und Deinen Feind

- Malware
- Phishing
- Spam
- Identitätsdiebstahl
- Datenverlust
- Hackerangriffe
- Erpressung
- DoS-Attacken
- Betrug
- Spionage
- Social Engineering
- Diebstahl des Systems oder der Medien
- Irrtum und Nachlässigkeit der Mitarbeiter
- Systemausfälle
- …



Aktuelle (Un)Sicherheitslage

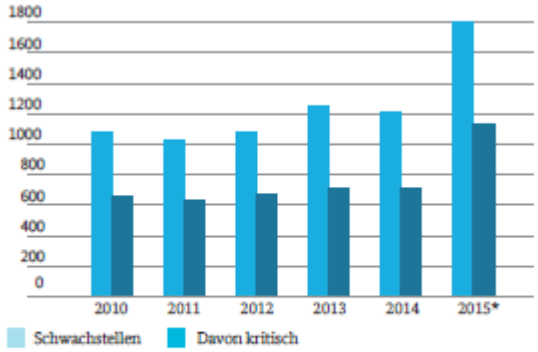
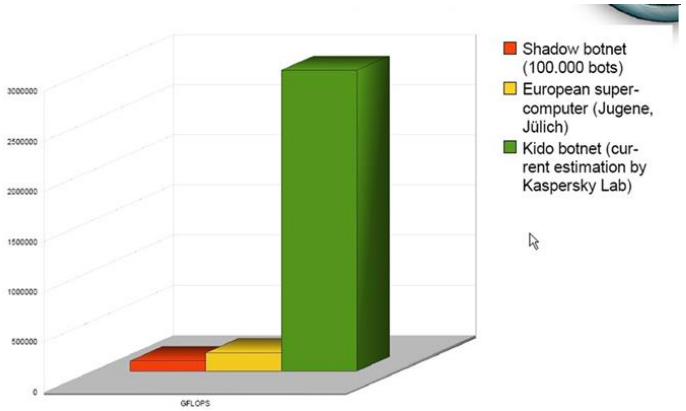


Abbildung 1: Anzahl aller Schwachstellen der in der BSI-Schwachstellen-ampel erfassten Softwareprodukte. * Zahlen für 2015 sind aus den bis Ende September 2015 entdeckten Schwachstellen hochgerechnet



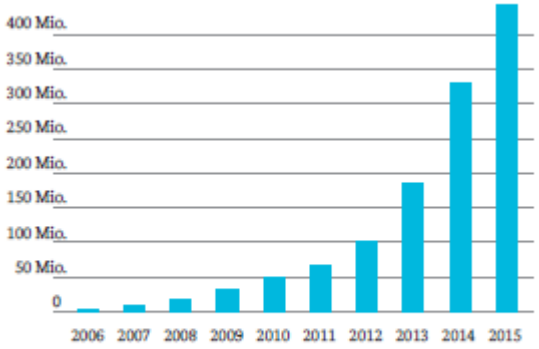


Abbildung 4: Anzahl bekannter Windows-Schadprogrammvarianten

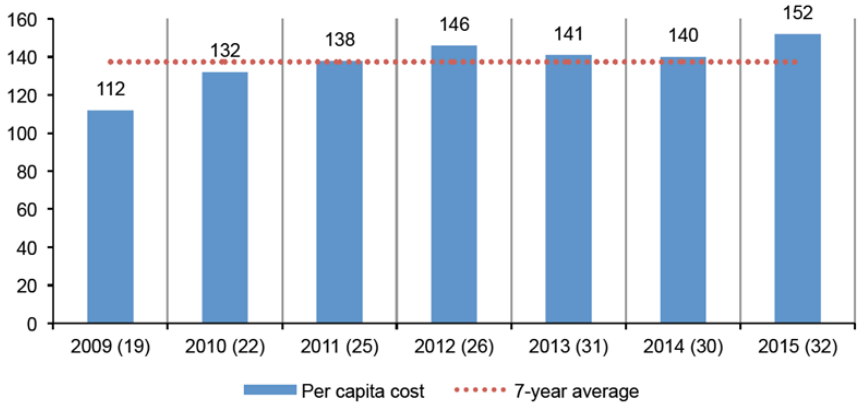
- Die Bedrohung durch Cyber-Crime ist insbesondere für den Sektor Finanz- und Versicherungswesen relevant. Die verübten Verbrechen reichen von Identitätsdiebstahl über Cyber-Angriffe auf die Infrastrukturen von Bankinstitutionen bis hin zur Erpressung.
- Angriffe politisch motivierter Hacktivisten sind bei Unternehmen der KRITIS-Sektoren Medien (De-facements oder Platzierung von Falschinformati-onen auf gekaperten Medienwebseiten), Energie und Kreditwirtschaft zu beobachten.

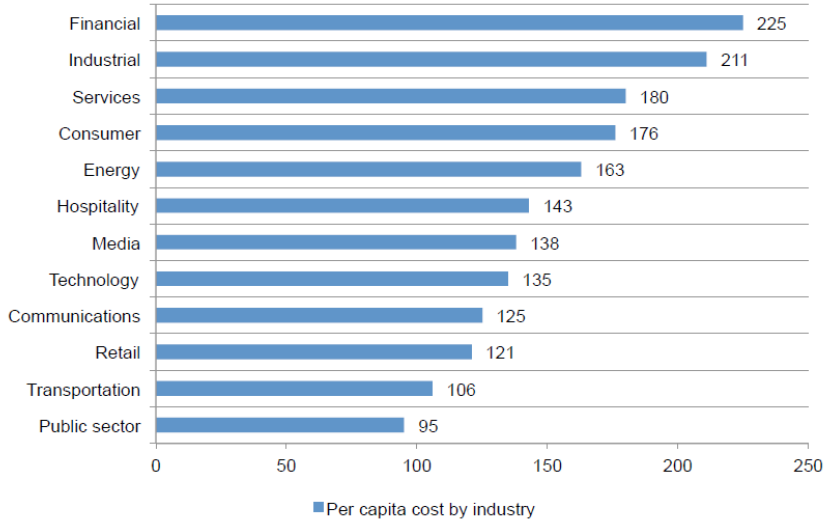
Quelle: Lagebericht BSI 2015

Aktuelle (Un)Sicherheitslage

German study at a glance

- 32 companies participated
- €3.52 million is the average total cost of data breach
- 2.9% increase in total cost of data breach
- €152 is the average cost per lost or stolen record
- 8.2% increase in cost per lost or stolen record





Quelle: Ponemon-Studie 2015

Aktuelle (Un)Sicherheitslage

Die Gefährdungslage der IT-Sicherheit in Deutschland 2015 wird in vielen Bereichen als hoch bewertet:

Gefährdung	2014	2015
Cloud Computing		→
Software-Schwachstellen	→	↑
Hardware-Schwachstellen		→
Nutzerverhalten und Herstellerverantwortung		↑
Kryptografie		→
Internet-Protokolle		↑
Mobilkommunikation		↑
Sicherheit von Apps		↑
Sicherheit von Industriellen Steuerungsanlagen		↑
Schadsoftware	↑	↑
Social Engineering	↑	→
Gezielte Angriffe - APT	→	↑
Spam	↑	↑
Botnetze	→	↑
Distributed Denial-of-Service (DDoS)-Angriffe	→	→
Drive-by-Exploits und Exploit-Kits	→	↑
Identitätsdiebstahl	↑	↑

Legende
Gefährdung 2015 (niedrig, durchschnittlich, hoch) ↓ → ↑

Beispiele:

Im Landschaftsverband Rheinland (LVR) infizierte TeslaCrypt 12.000 Arbeitsplätze (Dezember 2015)

Jigsaw verschlüsselt und löscht pro Stunde eine, bei Neustart 1000 Dateien, nach 72 Stunden ist alles gelöscht, aber Rettung ist möglich

Aktuelle (Un)Sicherheitslage

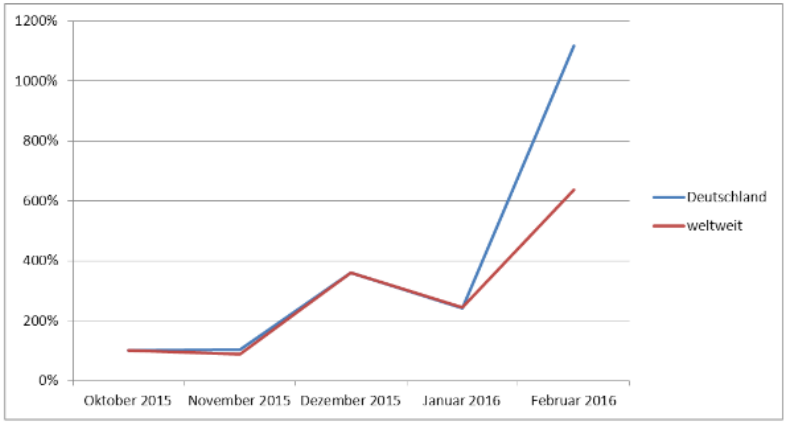
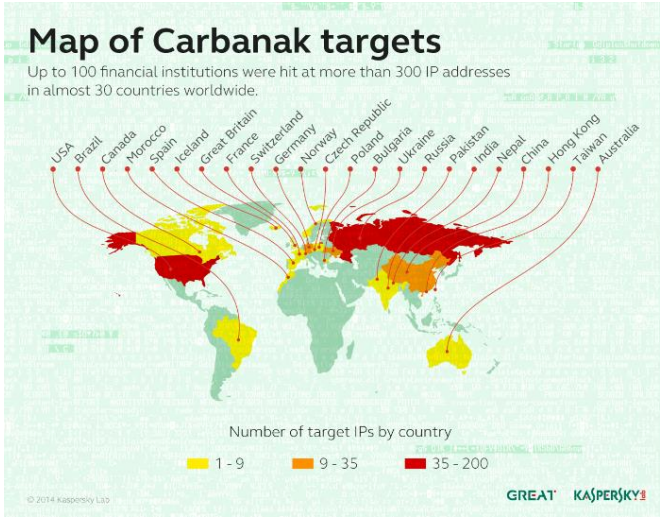


Abbildung 1: Trend der Ransomware-Detektionen in Deutschland Oktober 2015 – Februar 2016, Quelle: BSI

mehr als 5000 Neuinfektionen pro Stunde in Deutschland durch Locky

- Trixibad
- Baufirma
- Hochschule
- Fraunhofer Institut Bayreuth
- Krankenhaus in Hollywood
- …

- DDoS Angriff auf mobiles und später Festnetz von A1 (Austria Telekom)
- Carbanak – 1 Milliarde US$



- Datenrisiko durch Steganographie → Datenabfluss, Malware

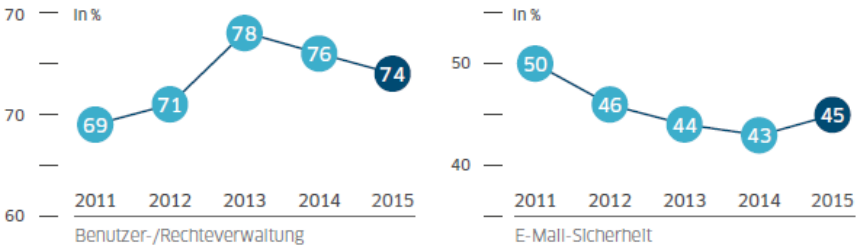
Car Hacking → Rückruf von 1,4 Millionen Autos

Wie gut sind wir gewappnet?

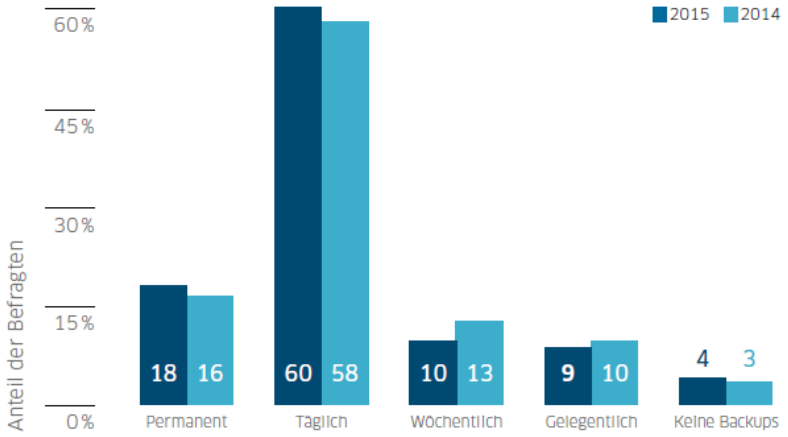
Stagnierender IT-Schutz trotz gewachsener Verunsicherung

Bei einer insgesamt starken Digitalisierung und steigenden Verunsicherung sind die tatsächlich getroffenen Sicherheitsvorkehrungen unzureichend. Deuteten die Zwischen-

- Einzelbausteine überwiegen
- Punktueller Einsatz
- Keine ganzheitlichen Konzepte
- …
- Resignation?



↑ Abb. 5: Fünf-Jahres-Vergleich technischer und organisatorischer IT-Schutzmaßnahmen

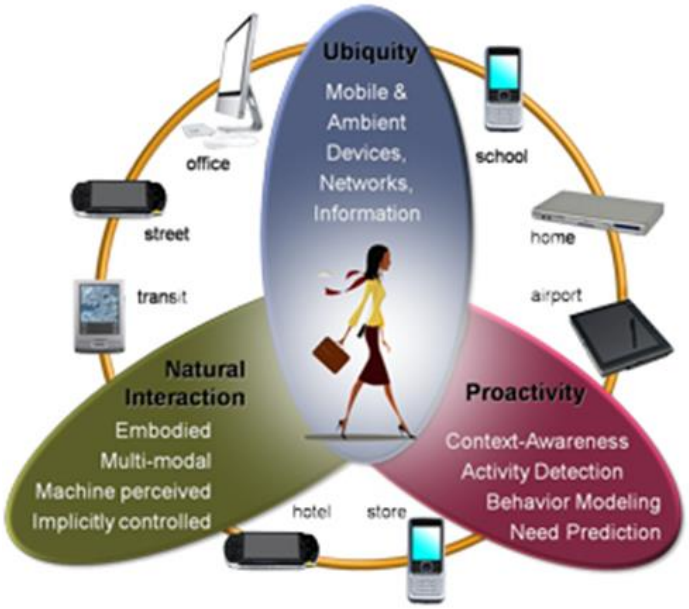


↑ Abb. 7: Häufigkeit der Datensicherung in Unternehmen

Quelle: DsiN Sicherheitsmonitor Mittelstand 2015

Neue Herausforderungen

- Cloud
- Ubiquitous Computing
- BYOD
- Smart Home
- IoT
- Industrie 4.0
- …



- Spear Phishing
- Advanced Persistant Threats: Stuxnet, Duqu, Flame, …

Cloud – Dropbox & Co.?

- viele Vorteile, sparen Ressourcen, Rechenleistung, …
- Wer hat Zugriff auf die Daten? Wie sind sie geschützt?
- Dropbox, Google Drive und iCloud → Standort in USA → US-Gesetze gelten: Regierung, Regierungsorganisationen oder Dritte können ohne die Angabe von Gründen über die Daten verfügen, sie auswerten oder nutzen
- Privat – eigene Entscheidung, aber für Nutzung in Unternehmen und Hochschulen ungeeignet, für personenbezogene Daten tabu!!
- Ggf. deutsche/EU Anbieter
  - Sicherungsmaßnahmen gegen Datenverlust?
  - Notfallkonzept?
  - Schutz der Daten und Dienste gegen den Zugriff von Dritten?
  - Welche Verfügbarkeit wird garantiert?
  - Rückübertragung der Daten und Dienste von einem Anbieter?
  - Rechtliche Rahmenbedingungen für die Erbringung der Dienstleistung ?
  - Was passiert bei Insolvenz eines Anbieters?
- →Nutzung eigener Ressourcen der Hochschule – ownCloud??

Cloud – Dropbox & Co.?

Schatten – IT ???

- Unkontrollierter Wildwuchs der genutzten IT-Lösungen
- An IT-Abteilungen bzw. Rechenzentren vorbei
- … untergräbt Informationssicherheit und Compliance
- Vorwurf: IT kann gewünschte Lösung nicht oder nicht schnell genug anbieten
- → Unternehmensdaten auf privaten Dropbox-Accounts gespeichert, wo sie nichts zu suchen haben
- Anbieter verschlüsselt die Daten? - z.B. Dropbox verschlüsselt Daten, dann kann Dropbox diese jederzeit wieder entschlüsseln

Doodle?

- Schnell und unkompliziert Termine vereinbaren → Doodle

- Doodle und der Datenschutz?
- Positiv: Nutzung ohne Registrierung möglich
- Kein wirksamer Zugriffsschutz
- Nutzung von Google Analytics → Weitergabe von Daten in USA
- Alternativen??
  - Alternative1
  - Alternative2

BYOD - Smartphone?

- Verwendung privater Endgeräte für berufliche Zwecke
- E-Mails abrufen, Dateien bearbeiten, Telefonate führen, …
- Privates Gerät: kein oder wenig Einfluss auf Sicherheitseinstellungen, großer Aufwand, da große Gerätevielfalt
- Trennung privater und dienstlicher Nutzung
- für einen Mitarbeiter tatsächlich wichtig E-Mails unterwegs abzurufen oder telefonisch erreichbar zu sein → Anschaffung von Firmengeräten (Get a Business Device – GABD)
- → Mobile Device Management
  - Verschlüsselungslösungen für Gerät und Anwendungen (z.B. Mail)
  - Antivirensoftware
  - Möglichkeit eines Fernzugriffs im Falle eines Verlusts oder Diebstahls
  - Sicherheitsschulung für die Mitarbeiter, Richtlinien für Nutzung des Gerätes

Social Media?

- Bitkom 2015: 75 Prozent der deutschen Unternehmen setzen Social Media für interne oder externe Kommunikation ein
- Firmenauftritt – was gibt man preis?
- Nutzung privater Accounts durch Beschäftigte am Arbeitsplatz → Einfallstor für Malware
- Social Engineering → Mitarbeiter als Informant (unfreiwillig)
- Produktivitätsverlust
- Netz vergisst nichts (z.B. archive.org)
- Datenschutzrecht, insbesondere BDSG, setzt Unternehmen enge Grenzen → gilt auch für Social Media
- Verstöße - gerichtliche oder außergerichtliche Verfahren mit Datenschutzbehörden oder juristische Streitigkeiten mit betroffenen Mitarbeitern vorprogrammiert
- Bei Datenschutzverstößen drohen Bußgelder bis zu 300.000 Euro

Social Media?

- Unabhängig davon, ob Mitarbeiter Social Media-Anwendungen privat oder beruflich nutzen
- ob sie Inhalte für das Unternehmen bei Twitter, Facebook o. ä. verbreiten,
- oder ob das Unternehmen interaktive Dienste wie Blogs, Foren oder Communitys anbietet:
- → Mitarbeiter müssen hinsichtlich des Themas Sicherheit sensibilisiert werden

- → Social Media Richtlinien
- Bitkom: Die Richtlinien sollten definieren, welche Ziele damit verfolgt werden, in welchen Kanälen welche Inhalte kommuniziert werden sollen bzw. dürfen und welche Zielgruppen adressiert werden. Auch ist es wichtig, Verantwortlichkeiten festzulegen und Ansprechpartner zu benennen.

Datenklassifikation?

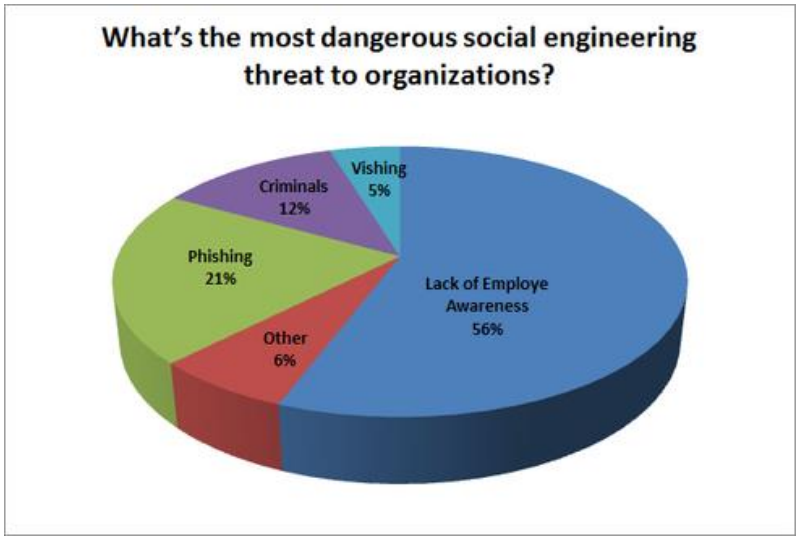
- Welche Daten verarbeiten wir überhaupt?
- Wer ist der Eigentümer?
- Wer ist verantwortlich?
- Wo werden sensible Daten verarbeitet und gespeichert?
- Welche Daten haben welchen Schutzbedarf?
- Wie erfolgt der Datenaustausch?
- Mehr als offene Briefe

Datenklassifikation durch Verantwortliche + ggf. Kunden

- Bearbeitende Personen/Gruppen/Prozesse
- Speicherort
- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Personenbezogene Daten
- Compliance

Schwachstelle „Mitarbeiter“ und „Studierende“

Ursache menschliches Fehlverhalten zwischen 25 und 84%



Mit wenig Aufwand viel erreichen

→ Security Awareness

Quelle: InformationWeek

Gesetze gelten auch an der Hochschule

- KonTraG
- HGB
- GDPdU, GoBS
- Basel II
- Solvency II
- …
- BDSG
- Datenschutzgesetze der Länder
- Sozialgesetzbuch
- …
- Urheberrechtsgesetz
- Telekommunikationsgesetz
- Telemediengesetz
- …
- NEU: IT-Sicherheitsgesetz

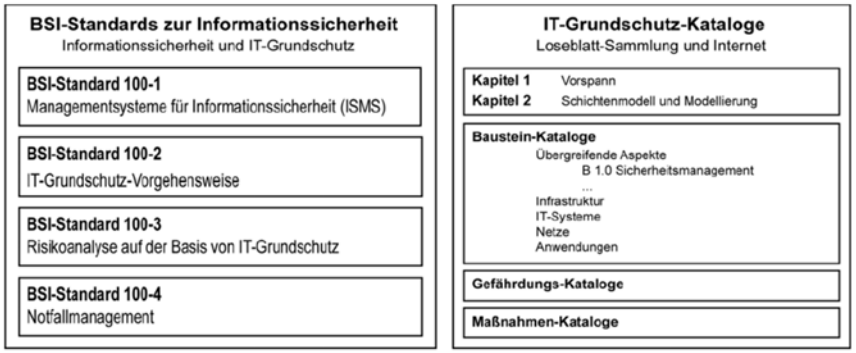
- BSI-Kritisverordnung (Referentenentwurf 13.1.2016)

- Gefährdung der Aufgabenerfüllung
- Verstoß gegen Verträge (Geheimhaltung)
- Finanzielle Schäden bzw. Auswirkungen
- Vernichtung von Arbeitsplätzen
- Fortbestand der Einrichtung
- Imageschäden
- Sanktionen, Strafen
- Haftung (auch für Mitarbeiter)
- …
- Strafgesetzbuch
- Schadensersatz
- …

Entwicklung ISMS

→ STRATEGIE

- Organisatorische Maßnahmen
  - Informationssicherheitskonzept, Informationssicherheitsbeauftragter
  - Mitarbeiter sensibilisieren und einbinden
  - Richtiges Maß an Sicherheit finden
  - …
- Technische Maßnahmen
  - Perimeterschutz
  - Antivirenschutz
  - Sicherheitslücken schließen
  - Nach Schwachstellen suchen auch innerhalb
  - Forensische Analysen → frühzeitige Erkennung von Angriffen
  - Backup
  - …

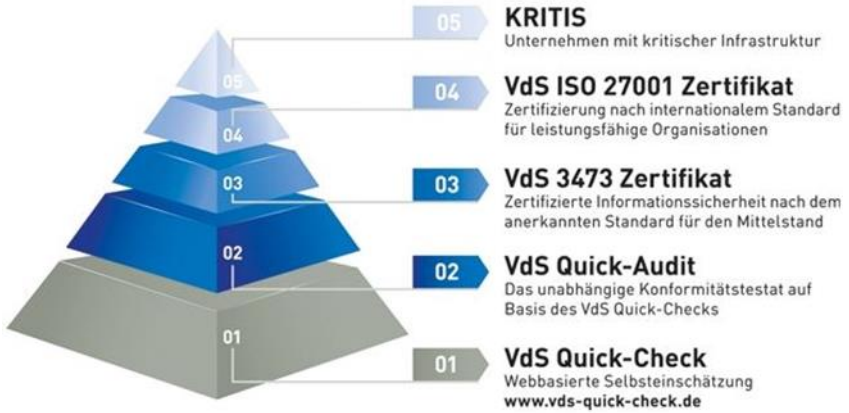


- ISO 27000 (series) ISMS Family of Standards
- IT-Grundschutz des BSI
- BSI-Standards
  - BSI-Standard 100-1, -2, -3, -4
- COBIT ITIL (IT Infrastructure Library)
- ISIS12
- VdS 3473

Speziell für KMU – und Hochschulen?

VdS 3473

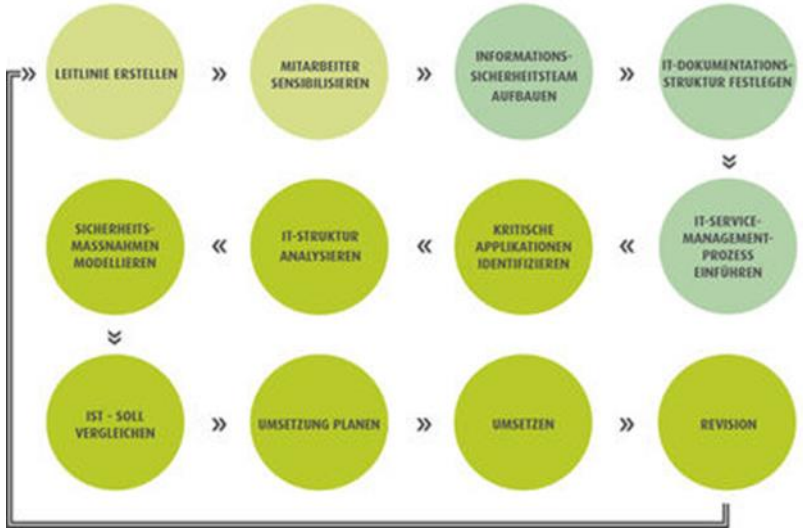
Leitlinie ISMS für KMU
Cyber-Security



Quelle:
http://vds.de/de/vds-cyber-security/cyber-security-fuer-kmu/

ISIS12

Für KMU, Dienstleister, Kommunen als Vorstufe zu ISO 27001 bzw. IT-Grundschutz



Quelle: http://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html

IT- Sicherheit ist ein Ziel …