# TeleTrusT

## IT-Sicherheitsstrategie für Deutschland

## Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe

→ **Ein Aspekt der IT-Sicherheitsstrategie für DE**

**TeleTrusT** - Bundesverband IT-Sicherheit e.V.

**Gemeinsam für Sicherheit und Vertrauenswürdigkeit in der vernetzten Informations- und Wissensgesellschaft**

Version: 01.09.2014

# Vorwort
## → Management Summary

Die heutige IT-Sicherheitssituation ist für eine Informations- und Wissensgesellschaft wie Deutschland nicht angemessen sicher und vertrauenswürdig genug.

Der Bundesverband IT-Sicherheit – TeleTrusT hat im Rahmen der Ideen zu einer IT-Sicherheitsstrategie für Deutschland einen ersten Schritt gemacht, und daraus Ergebnisse dargestellt und eine weitere Vorgehensweise vorgeschlagen.

In dieser TeleTrusT-Präsentation werden:

- Die Stärken der IT-Sicherheit in Deutschland aufgezeigt
- Die Ergebnisse einer Analyse der wichtigsten und verfügbaren IT-Sicherheitstechnologien dargestellt. Dabei wurden Bewertungen der Lage bezüglich der eigentlichen IT-Sicherheitstechnologie, der Bedeutung für die Zukunft sowie die Marktstärke der deutschen IT-Sicherheitsunternehmen in den entsprechenden IT-Sicherheitsbereichen vorgenommen.
- Zur Gestaltung der IT-Sicherheitsstrategie für Deutschland werden pragmatische Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe definiert und für die zukünftige Nutzung aller Stakeholder in Deutschland vorgeschlagen.

Die Wirkungsklassen erlauben so eine strukturierte Analyse und zweckorientierte Umsetzung der erforderlichen Maßnahmen.

Sie reflektieren die unterschiedlichen und immer wichtiger werdenden Wirkungsaspekte, die ein Zusammenspiel von internationalen IT-Marktführen und IT-Sicherheitsunternehmen aus Deutschland modulierbar machen und ein angemessenes Optimum der nationalen IT-Sicherheitssouveränität gestaltbar macht

Zum Schluss werden die nächsten anstehenden Aufgaben und Schritte vorgeschlagen.

# Inhaltsverzeichnis

# Inhaltsverzeichnis

TeleTrusT
Pioneers in IT security.

## IT-Sicherheitssituation und der Weg zu einem angemessenen IT-Sicherheitsniveau

# IT-Sicherheitssituation
## → Bewertung

- Es gibt in Deutschland eine **massive Abhängigkeit** von der **IT**
- Zwiespalt: **Zurzeit keine angemessene Vertrauenswürdigkeit**

  ► Steigende Zahl von IT-Sicherheitsvorfällen zeigt, dass das allgemeine Sicherheitsniveau zurzeit nicht ausreicht (siehe auch BSI Lagebilder)

  ► Die Wirkung von IT-Sicherheitslösungen ist an vielen Stellen heute nicht mehr ausreichend

  ► Die Vertrauenswürdigkeit von IT-Systemen ist eine wichtige und notwendige Eigenschaft

- **Beurteilung der eigenen IT-Sicherheitslage ist für Anwender/Entscheidungsträger nicht einfach**
  Konsequenzen können eigentlich nicht eingeschätzt werden
- **Ableiten notwendiger IT-Sicherheitsmaßnahmen**
  Wieviel Schutz wird für ein bestimmtes IT-System benötigt?
  Angemessenheit der IT-Sicherheitsmaßnahmen ist schwer zu beurteilen

# Inhaltsverzeichnis

# IT-Sicherheitsherausforderungen
## → Erforderlicher Nachholbedarf

**Die aktuelle Situation der IT-Sicherheit in Deutschland bietet Raum für notwendige Verbesserungen:**

- Existenz **zu vieler Schwachstellen in Software**
- Nachholbedarf bei der **Schadsoftware-Erkennung und -Vermeidung**
- Nachholbedarf gibt es ebenfalls bei **Advanced Persistent Threat (APT)** (komplexe und zielgerichtete Angriffe)
- **Schutz vor Identitätsdiebstahl** bietet großen Raum für weitere Verbesserungen
- Neue Methoden für die **Messbarkeit von Gefahren- und Bedrohungspotential** notwendig
- Vermeidung der **Nutzung ineffektiver IT-Sicherheitslösungen** (absichtlich/unabsichtlich)

# IT-Sicherheit Deutschland
## → Besondere Stärken

TeleTrusT
Pioneers in IT security.

- **Sehr hohe Kompetenz im Bereich des Datenschutzes**
  - → Erfahrungen mit dem Schutz der Privatsphäre
- **Sehr hohes Vertrauen im Bereich der IT-Sicherheit**
  - → mittelstandsgeprägte Sicherheitsindustrie
  - → umfangreiche und kompetente IT-Sicherheitsforschung
  - → hohe Kompetenz bei Sicherheitsevaluierungen (BSI, „TÜVs“, …)
  - → offene Kryptopolitik
- **Kulturell gute Voraussetzungen**
  - → traditionell verlässliche IT-Sicherheit
  - → hohes Verständnis für IT-Sicherheit und Datenschutz
  - → sehr viel Erfahrung bei der Umsetzung von IT-Sicherheitslösungen
- Deutschland sollte **Verantwortung übernehmen** und ein
  - **sicheres** und
  - **vertrauenswürdiges**

  globales Internet für die Zukunft entscheidend mitgestalten

# Inhaltsverzeichnis

# Analyse der Anbieter im In- und Ausland
## → Umsetzung der Analyse

- Nachfolgend werden **die Ergebnisse einer Analyse** der wichtigsten und verfügbaren IT-Sicherheitstechnologien dargestellt.
- Dabei werden **Bewertungen der Lage** bezüglich der eigentlichen IT-Sicherheitstechnologie, der **Bedeutung für die Zukunft** sowie die **Marktstärke der deutschen IT-Sicherheitsunternehmen** in den entsprechenden IT-Sicherheitsbereichen vorgenommen.
- In der **Kategorie Bedrohungen** werden exemplarisch Fälle von möglichen Szenarien dargestellt.
- Zusätzlich werden in der **Kategorie der Anbieter** die **Standorte berücksichtigt**, um die **geografische Aufteilung im Ausland** aufzuzeigen, welche hinsichtlich **Vertrauenswürdigkeit und IT-Sicherheit eine Rolle** spielen kann.

| *Kategorie* | *Bewertung* | *erforderlich ab Wirkungsklasse* | *Bedrohungen* | *In- und Ausländische Anbieter* |
|---|---|---|---|---|

# Analyse der Anbieter im In- und Ausland
## → Wirkungsklassen

- Die **Kategorie der Wirkungsklasse** soll einen Hinweis auf die erforderliche Einstufung geben.

**Wirkungsklasse 0** ► Basis-IT-Sicherheit

- **Bürger mit privater Nutzung**

**Wirkungsklasse 1** ► Schutzbedarf: mittel

- **Unternehmen, Organisationen, Behörden**

**Wirkungsklasse 2** ► Schutzbedarf: hoch

- **Unternehmen, Organisationen, Behörden, Infrastruktur (+ Industriespionage)**

**Wirkungsklasse 3** ► Schutzbedarf: sehr hoch

- **Unternehmen, Organisationen, Behörden, Infrastruktur (+ Cyberwar, Sabotage, …)**

**Wirkungsklasse 4** ► Verschlusssachen bis streng geheim

- **Verschlusssachen**

# Analyse der Anbieter im In- und Ausland
## → Sichere Vernetzung

| Sichere Vernetzung | Bewertung | erforderlich ab Wirkungsklasse | Bedrohungen | In- und Ausländische Anbieter |
|---|---|---|---|---|
| **Sichere Anbindung mobiler User / Telearbeiter** | A ++<br>B +<br>C - | alle ab Klasse 1 | Abfangen sensibler Informationen und Abhören von Kommunikation | **Ausland:** Cisco (USA), Juniper (USA), Fortinet (USA)<br><br>**Deutschland:** secunet, genua, NCP, gateprotect, Sirrix, HOB |
| **Layer3-VPN** | A ++<br>B +<br>C 0 | alle ab Klasse 3 | Mitschneiden und Abfluß von Daten durch Hintertüren und Sicherheitslücken in Netzwerkhardware | **Ausland:** Cisco (USA), Juniper (USA), Check Point (Israel), Fortinet (USA)<br><br>**Deutschland:** secunet, genua, gateprotect, Sirrix, LANCOM, HOB |
| **Layer2-Encryption** | A ++<br>B +<br>C 0 | alle ab Klasse 3 | Mitschneiden und Abfluß von Daten durch Hintertüren und Sicherheitslücken in Netzwerkhardware | **Ausland:** SafeNet (USA), Crypto AG (Schweiz)<br><br>**Deutschland:** secunet, Rohde & Schwarz, atmedia |
| **Datendiode** | A +<br>B 0<br>C 0 | Klasse 4 | Angriff auf Übermittlung und Empfang von Daten, die in eine Richtung an einen festen Empfänger transportiert werden | **Ausland:** -<br><br>**Deutschland:** genua, secunet |

Bewertung der Lage in Deutschland:
**A Bedeutung für die Zukunft**
**B Technologischer Vorsprung in Deutschland**
**C Marktstärke der dt. Unternehmen**

Eine Fortsetzung der Analysen finden Sie in der Anlage 1.

# Deutsche Stärken der IT-Sicherheit
## → Besondere Kompetenzen in Deutschland

TeleTrusT
Pioneers in IT security.

### Zahlreiche IT-Sicherheitstechnologien aus Deutschland:

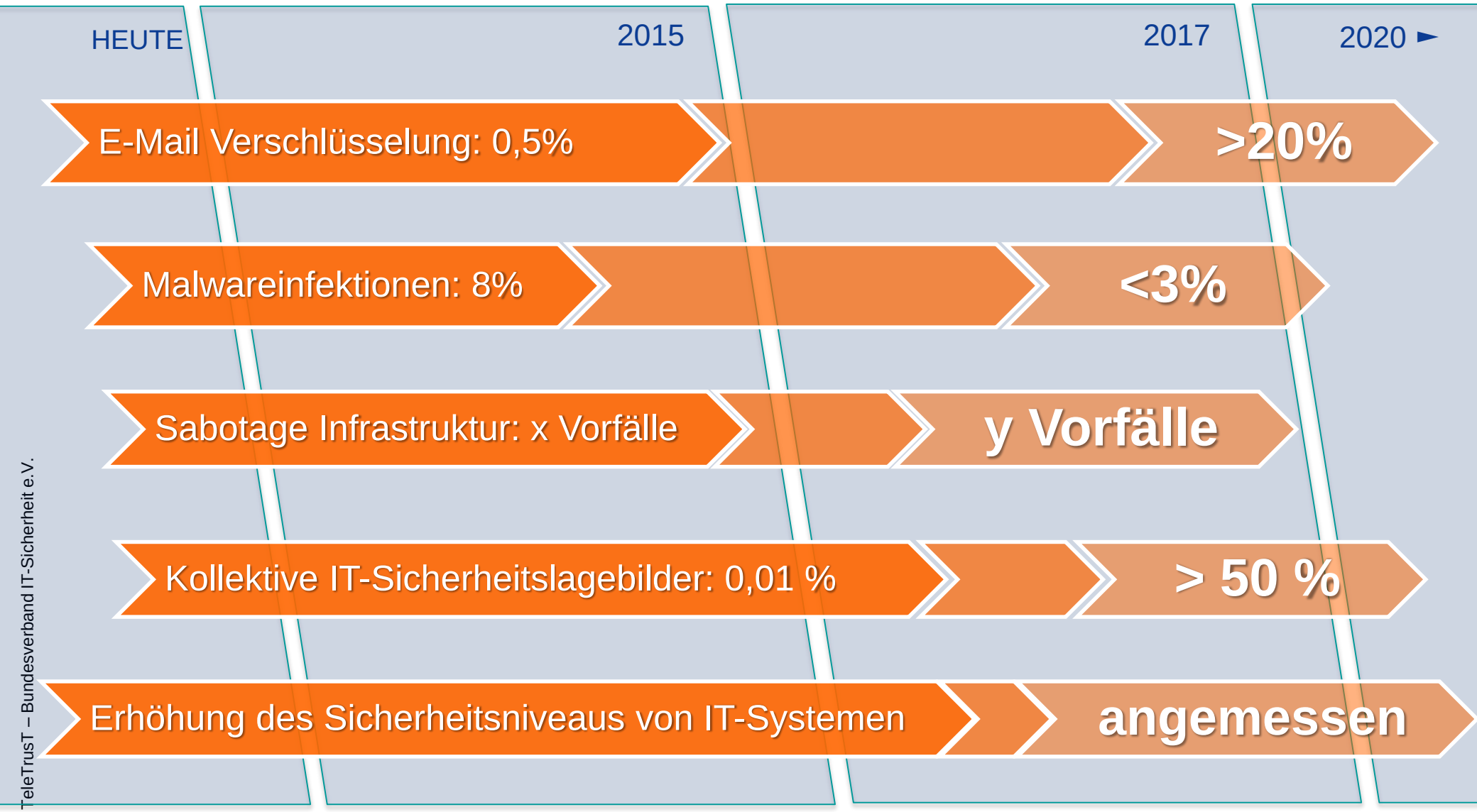
- **Sicherheitskern** *(Sicheres Booten, Separierungstechnologien, …)*
- **Security Token** *(Smartcards, Hardware-Sicherheitsmodule, …)*
- **Verschlüsselungstechnologien** *(Kommunikations- und Objektverschlüsselung, Kryptohardware)*
- **Proaktive IT-Sicherheitstechnologien** zur Exploitbekämpfung
- Technologie zur **Abwehr von Schadsoftware**
- **Firewall-Technologien**
- Technologien für **sichere Identitäten** *(PKI, TrustCenter)*
- **Frühwarnsysteme** *(Angriffe, Lagebildgenerierung, …)*

# Inhaltsverzeichnis

# Ziel: IT-Sicherheitsstrategie für Deutschland

- **Die IT-Sicherheitsstrategie** hat das **Ziel**, das Niveau der IT-Sicherheit **nachhaltig** auf einen jeweils angemessenen Stand **zu erhöhen und zu halten**.
- Es werden vorhandene IT-Sicherheitsprozesse und -technologien genutzt und im Bedarfsfall IT-Sicherheitslösungen für neue Problemstellungen erarbeitet.
- **Aus Deutschland stammende**, notwendige hochwertige und wirkungsvolle IT-Sicherheitstechnologien und -prozesse werden berücksichtigt.
- Die **etablierten** IT-Systeme und -Lösungen der jeweiligen internationalen Hersteller werden konstruktiver in die IT-Sicherheitsstrategie eingebunden.
- Die erforderlichen IT-Sicherheitsmaßnahmen der wichtigen Stakeholder (Anwender, Hersteller, Politik, Forschung) werden **identifiziert und berücksichtigt**.
- Um das Ziel **nachhaltig und erfolgreich** umzusetzen, wird die Roadmap den jeweiligen erforderlichen Anforderungen angepasst und umgesetzt.

# Strategie IT-Sicherheit Deutschland
## → Beispiele von mögliche Zielen



# Erhöhung des Sicherheitsniveaus von IT-Systemen
## → Wirkungsklassen

## Umsetzungsvorschlag:

- **Einteilung von IT-Systemen** in leicht verständliche Wirkungsklassen
- **Identifikation** und **Empfehlung** angemessener IT-Sicherheitsmaßnahmen für jede Wirkungsklasse unter Berücksichtigung herausragender nationaler, vertrauenswürdigerer Technologien und Standards

# Inhaltsverzeichnis

# Wirkung von IT-Sicherheitsmaßnahmen
## → Unterschiedliche Wirkungsaspekte

Beschreibung unterschiedlicher Wirkungsaspekte und Maßnahmen, wie die maximale Wirkung erzielt werden kann.

- **Die prinzipielle Wirkung gegen konkrete Bedrohungen**
  (z.B. Verschlüsselung gegen das Lesen von Klartext)
  - Maßnahme: Darstellung der Wirkung von Kryptoverfahren

- **Die konkrete Wirkung gegen konkrete Bedrohungen**
  (z.B. richtige Implementierung von Verschlüsselungstechnologien; Zufallszahlen, Algorithmus, Einbindung, …)
  - Maßnahme: Evaluierung von IT-Sicherheitslösungen

- **Die gewollte Wirkung gegen konkrete Bedrohungen**
  (z.B. sind Hintertüren oder gewollte Schwächen eingebaut)
  - Maßnahme: Qualitätssiegel: "IT Security made in Germany"

# Internationale Marktführer in die Pflicht nehmen

## → Stärkere Kooperation für mehr Vertrauen (Beispiel)

- Marktführende IT-Technologien kommen in vielen Bereichen aus dem Ausland, z.B. Betriebssystem mit Festplattenverschlüsselung
- Vollständige Vertrauenswürdigkeit nicht gewährleistet aber trotzdem großflächig im Einsatz mangels Alternativen

► Microsoft Windows Bitlocker Verschlüsselungssoftware (USA), Integriert ins Betriebssystem ohne die Möglichkeit einer Schnittstelle für Softwarelösungen anderer Hersteller


**Prinzipielle und konkrete Wirkung müsste nachgewiesen werden**

► Sirrix Trusted-Disk Verschlüsselungssoftware (DE), Softwarelösung als eigenständiges IT-Sicherheitsprodukt zusätzlich zu bestehenden Softwarekomponenten auf dem Rechner


**Gewollte Wirkung per Definition gegeben** *(„Made in Germany“)*

- Möglichkeit einer Schnittstelle zum Ersetzen bestehender eingebauter IT-Sicherheitstechnologien durch deutsche Lösung für eine höhere Wirkung der IT-Sicherheit.

# IT-Sicherheitsbedrohungen
## → Einteilung in Wirkungsklassen

TeleTrusT
Pioneers in IT security.

► Welcher Schutzbedarf wird in den verschiedenen Wirkungsklassen gedeckt?

| | |
|---|---|
| **Wirkungsklasse 0**<br>Basis-IT-Sicherheit | Infektionen durch Schadsoftware (Viren, PC-Geiselnahme, Keylogger, Trojaner)<br>Angriffe auf das heimische Netzwerk, Abfischen von Banking Daten |
| **Wirkungsklasse 1**<br>Schutzbedarf: mittel | Angriff auf den Datenbestand (Kunden-, Mandanten-, Patientendaten)<br>Infektionen durch Schadsoftware und Mitschneiden von Kommunikation |
| **Wirkungsklasse 2**<br>Schutzbedarf: hoch | Diebstahl von Plänen und Dokumenten mit Hilfe von Schadsoftware<br>Kopieren von sensiblen Daten auf externe Datenträger |
| **Wirkungsklasse 3**<br>Schutzbedarf: sehr hoch | Sabotage von Infrastruktur (Wasserwerke, Energieversorger, Finanzdienstleister)<br>Gezielte Attacke gegen einzelne Wissensträger in Industrie und Politik |
| **Wirkungsklasse 4**<br>Verschlusssachen bis streng geheim | Angriff auf Informationen und Kommunikation<br>Eindringen in staatliche oder wirtschaftlich extrem kritische Systeme |

# Kern-Wirkungsklassen
## → Übersicht

- Gewichtung für eine Einstufung in die Wirkungsklassen notwendig, die auch in größerem Maße monetär messbar sind:

### Wirkungsklasse 1

- IT Systeme sind relevant für Unternehmung, jedoch gibt es **keine existenzielle Abhängigkeit** (z.B. Handwerk)

### Wirkungsklasse 2

- IT Systeme sind absolut **relevant für die Organisation** und ein **Ausfall** kann neben extrem **hohen Kosten** auch die **Existenz bedrohen** (z.B. Warenproduzenten, Forschungsinstitute)

### Wirkungsklasse 3

- **Bedrohungen** nicht nur für **eigene** Sicherheit und **Existenz**, sondern auch die **von Dritten** (z.B. kritische Infrastrukturen)

# Einordnung von Wirkungsklassen
## → Gefahren, Schutzbedarf, Kosten

TeleTrusT
Pioneers in IT security.

### Wirkungsklasse 0 — Bürger mit privater Nutzung

*Prozentualer Anteil:*

- Gefahren: Privatsphäre, Cybercrime
- Kosten: Grundbetrag +5%

*100%*

### Wirkungsklasse 1 — Unternehmen, Organisationen, Behörden

- Gefahren: Privatsphäre, Cybercrime mit höherem Gefährdungsgrad, gesetzlicher Datenschutz
- Schutzbedarf: mittel
- Kosten: Grundbetrag +10%

*70%*

### Wirkungsklasse 2 — Unternehmen, Organisationen, Behörden, Infrastruktur

- Gefahren: Industriespionage, gezielte Angriffe auf Werte des Unternehmens, Cybercrime
- Schutzbedarf: hoch
- Kosten: Grundbetrag +20%

*27%*

### Wirkungsklasse 3 — Unternehmen, Organisationen, Behörden, Infrastruktur

- Gefahren: Wirtschaftsspionage (Nachrichtendienste) und Cyberattacken, Cyberwar (Sabotagen)
- Schutzbedarf: sehr hoch, inkl. VS-NfD
- Kosten: Grundbetrag +50%

*3%*
*+ Infrastrukturkosten*

Kernklassen

### Wirkungsklasse 4 — Verschlusssachen

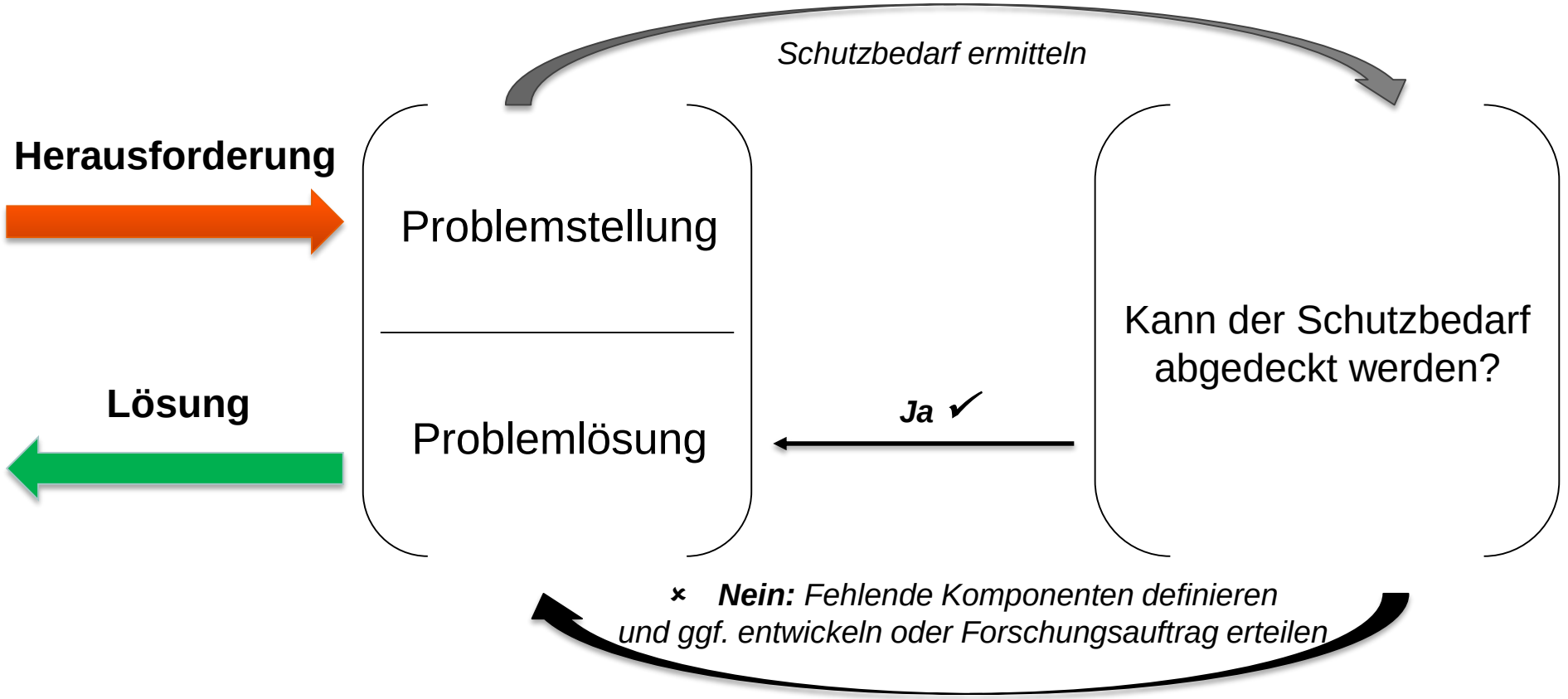
- Nationale Sicherheit
- Schutzbedarf: gemäß Geheimschutzordnung GSO, ab VS/V
- Kosten: Grundbetrag +400%

*0,01%*

Eine detaillierte Beschreibung zu den einzelnen Wirkungsklassen finden Sie in der Anlage 2.

# Kontinuierliches und angemessenes IT-Sicherheitsniveau

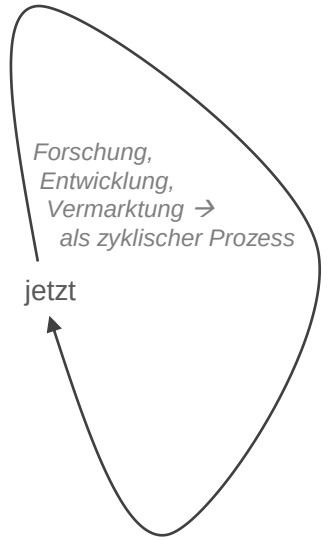
## Kontinuierliche Erhöhung eines angemessenen IT-Sicherheitsniveaus und der Vertrauenswürdigkeit mit Hilfe der deutscher IT-Sicherheitstechnologien



# IT-Sicherheitsbedrohungen und –maßnahmen → Lücken, die geschlossen werden müssen

## Problemlösungen, die existieren, sollten leicht erreichbar sein

- Beim Finden von IT-Sicherheitstechnologien und -Lösungen helfen Plattformen wie z.B.
  - **Marktplatz IT-Sicherheit** (*www.it-sicherheit.de)*
  - **TeleTrusT Bundesverband IT-Sicherheit e.V.** *(www.teletrust.de)*
- Auffinden von qualifiziertem Personal oder Dienstleistern sollte möglichst einfach sein
- **Novitäten** sollten **gefördert** werden und eine schnelle Markteinführung sollte unkompliziert möglich sein




## Forschungsinitiativen helfen bei fehlenden IT-Sicherheitstechnologien

- Fehlende IT-Sicherheitsprozesse und -komponenten müssen **ausgeschrieben** und in der Forschung **erarbeitet** werden
- Im Optimalfall zusammen mit **Partnern** aus der **Wirtschaft** für die größtmögliche Nähe zum Markt

# Umgang mit Restrisiken

- **Unabhängig von der IT-Sicherheitslösung wird es immer Restrisiken geben, die verantwortet werden müssen**
- Manche IT- und IT-Sicherheitsgebiete können nicht durch „*made in Germany*“ abgedeckt werden
- Gewählte Wirkungsklasse nimmt definiertes Restrisiko in Kauf
- Das Restrisiko kann akzeptiert oder versichert werden. Es ist auch möglich, eine höhere Wirkungsklasse zu nutzen (monetäre Minimierung)
- Restrisiken sind **nur dann akzeptabel**, wenn alle Optionen ausgeschöpft und alle verfügbaren Wirkungsklassen in Erwägung gezogen wurden
- Die **personalen Sicherheitsmaßnahmen** wurden auf angemessene Weise und im notwendigem Umfang **durchgeführt**

# Inhaltsverzeichnis

# Die nächsten Aufgabenstellungen
## → Die wichtigsten Stakeholder

Die Ergebnisse und Aufgaben müssen getragen werden durch die wichtigsten Stakeholder:

- Anwender (Verbände, Vereine, Gruppen)
- IT-Sicherheitsanbieter (Verbände, Vereine, Gruppen)
- Politik, Gesetzgeber
- Wissenschaft und Forschung

# Die nächsten Aufgabenstellungen
## → Anwender

### Anwender (Verbände, Vereine, Gruppen)

- Müssen definieren, welche Features sie in welchen Wirkungsklassen brauchen
- Welche einsatzspezifische Randbedingungen berücksichtigt werden müssen, um solche Produkte einzusetzen
- Wunsch einer Gesamtverantwortung für die IT-Sicherheitslösungen

# Die nächsten Aufgabenstellungen
## → IT-Sicherheitsanbieter

## IT-Sicherheitsanbieter (Verbände, Vereine, Gruppen)

- IT-Sicherheits-Bundles als maßgeschneiderte und vertrauenswürdige Produkte und Lösungen definieren und umsetzen, die für die einzelnen Wirkungsklassen zum Einsatz kommen sollen
- Produkte müssen unkompliziert, einheitlich, benutzbar, stabil und sicher sein
- Sicherstellung der reibungslosen Integration in vorhandene IT-Lösungen

# Die nächsten Aufgabenstellungen
## → Politik, Gesetzgeber

TeleTrusT
Pioneers in IT security.

## Politik, Gesetzgeber

- Berücksichtigung der Marktsituation und der internationalen Mitspieler
  → **Anreize schaffen** mit den zur Verfügung stehenden Mitteln:
  - **Motivation, Regulierung, Empfehlung, Gesetzgebung**
- **Verhinderung von Veräußerung** deutscher IT-Sicherheitstechnologien ins Ausland
- Motivation für **Forschung und Entwicklung** notwendiger IT-Sicherheitstechnologien
- **Hilfestellung für den deutschen Mittelstand** bei der Einführung der Wirkungsklassen

# Die nächsten Aufgabenstellungen
## → Wissenschaft und Forschung

## Wissenschaft und Forschung

- Entwicklung von modernen und notwendigen IT-Sicherheitstechnologien um den kontinuierlich steigenden Anforderungen zu genügen
- Engere Zusammenarbeit mit der IT-Sicherheitsindustrie

# Vorgehen
## → Der nächsten Schritte

- **Einführung und Umsetzung eines strukturierten Prozesses**, um die gemeinsamen Aufgaben **zielgerichtet** umsetzen zu können (z.B. runder Tisch)
- **TeleTrusT ist bereit hier eine besondere Verantwortung zu übernehmen**
- **Weitere Schritte (Vorschlag)**
  - Insbesondere Definition und Umsetzung der vorgeschlagenen Wirkungsklassen
  - Stärkere Verwendung von E-Mail-Verschlüsselung,
  - Besserer Schutz der Infrastruktur vor Sabotage,
  - Absenkung von Malwareinfektionen,
  - …

# TeleTrusT

## IT-Sicherheitsstrategie für Deutschland

### Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe

→ Ein Aspekt der IT-Sicherheitsstrategie für DE

## Ziel: Bündelung der Kräfte


**Ansprechpartner:**

**TeleTrusT-Vorsitzender Prof. Dr. (TU NN) Norbert Pohlmann**

**E-Mail: norbert.pohlmann@teletrust.de**

**Tel.: +49 (209) 95 96 515**

**Mobil: +49 (173) 30 21 838**


**TeleTrusT** - Bundesverband IT-Sicherheit e.V.

**Gemeinsam für Sicherheit und Vertrauenswürdigkeit in der vernetzten Informations- und Wissensgesellschaft**

# Autoren

**Ammar Alkassar**,
TeleTrusT Vorstand / Sirrix AG

**Sebastian Barchnicki**,
TeleTrusT / Institut für Internet-Sicherheit – if(is)

**Michael Böffel**,
TeleTrusT / secunet Security Networks AG

Dr. **Guido von der Heidt**,
TeleTrusT Vorstand / Siemens AG

Prof. Dr. (TU NN) **Norbert Pohlmann**,
TeleTrusT Vorsitzender / Institut für Internet-Sicherheit – if(is)

# Anhang 1
## → Analyse von Technologien

- **Nachfolgend finden Sie eine Fortsetzung der Analysen inklusive eine Bewertung der Lage in DE**

# Analyse der Anbieter im In- und Ausland
## → Sicherer Internetzugang

| Sicherer Internetzugang | Bewertung | erforderlich ab Wirkungsklasse | Bedrohungen | In- und Ausländische Anbieter |
|---|---|---|---|---|
| **Firewall** | A ++<br>B 0<br>C - | alle ab Klasse 1 | Angriffe von außen, Portscans, ungewollte Kommunikation von Diensten und Anwendungen nach Außen | **Ausland:** Palo Alto Networks (USA), Cisco (USA), Juniper (USA), Check Point (Israel), Sophos (Großbritannien)<br><br>**Deutschland:** genua, gateprotect |
| **IPS/IDS** | A +++<br>B -<br>C -- | alle ab Klasse 2 | Angriffe von außen, die unmittelbar auf die Infrastruktur einer Organisation durchgeführt werden | **Ausland:** Sourcefire/Cisco (USA), ISS/IBM (USA), Extreme Networks (USA), Symantec (USA)<br><br>**Deutschland:** Institut für Internet-Sicherheit |
| **Sicherer Browser/ReCoBS** | A ++<br>B +<br>C + | alle ab Klasse 3 | Einbruch in Systeme durch infizierte Webseiten | **Ausland:** FireEye (USA), Bromium (USA), Invincea (USA)<br><br>**Deutschland:** Sirrix, secunet, m-privacy |
| **Virtuelle Schleuse** | A +<br>B 0<br>C 0 | alle ab Klasse 2 | Einschleusen von Schadcode in beliebige Umgebungen mit Hilfe von Dokumenten, Dateien und anderen Trägersystemen | **Ausland:** FireEye (USA)<br><br>**Deutschland:** - |

Bewertung der Lage in Deutschland:
**A Bedeutung für die Zukunft**
**B Technologischer Vorsprung in Deutschland**
**C Marktstärke der dt. Unternehmen**

# Analyse der Anbieter im In- und Ausland
## → Digital Enterprise Security

| Digital Enterprise Security | Bewertung | erforderlich ab Wirkungsklasse | Bedrohungen | In- und Ausländische Anbieter |
|---|---|---|---|---|
| **Authentikation** | A ++<br>B +<br>C 0 | alle ab Klasse 1 | Identitätsdiebstahl, Missbrauch fremder Identitäten | **Ausland:** RSA (USA), gemalto/SafeNet (USA)<br><br>**Deutschland:** Bundesdruckerei, secunet, Giesecke & Devrient |
| **Sichere Anbindung zwischen Anbieter und Anwender** | A ++<br>B 0<br>C - | alle ab Klasse 2 | Mitlesen und Auswerten von vertraulichen Daten | **Ausland:** Cisco (USA), Juniper (USA)<br><br>**Deutschland:** secunet, genua, Sirrix, gateprotect |
| **Hardware-Sicherheitsmodul (HSM)** | A +<br>B +<br>C + | alle ab Klasse 3/4 | Angriff auf vermeintlich sichere kryptografische Programmmodule | **Ausland:** gemalto/SafeNet (USA), Thales (Frankreich)<br><br>**Deutschland:** Ultimaco (Kryptoserver, bis Kl. 3) secunet (SINA Core, Kl. 4) |
| **Public-Key-Infrastruktur (PKI)** | A ++<br>B +<br>C + | alle ab Klasse 2 | Fälschen von Identitäten, um sich als Bank oder Institution auszugeben, um das Vertrauen von Anwendern zu erschleichen | **Ausland:** Microsoft (USA), OpenTrust (Frankreich), neXus (Schweden)<br><br>**Deutschland:** secunet, Bundesdruckerei/D-TRUST, T-Systems/TeleSec, Sirrix |

Bewertung der Lage in Deutschland:
**A Bedeutung für die Zukunft**
**B Technologischer Vorsprung in Deutschland**
**C Marktstärke der dt. Unternehmen**

# Analyse der Anbieter im In- und Ausland
## → Client- und Serversicherheit (1)

| Client- und Serversicherheit | Bewertung | erforderlich ab Wirkungsklasse | Bedrohungen | In- und Ausländische Anbieter |
|---|---|---|---|---|
| **AV und personal Firewall** | A -<br>B 0<br>C 0 | alle ab Klasse 0 | Schadsoftware-Infektionen, ungewollte Verbindungen nach außen | **Ausland:** Kaspersky (Russland), AVG (Niederlande), Panda (Spanien), F-Secure (Finnland), Symantec (USA), AVAST (Tschechien), Trend Micro (Japan), McAfee/Intel (USA), BullGuard (Großbritannien), Eset (USA), Bitdefender (Rumänien), Ikarus (Österreich), Sophos (Großbritannien)<br><br>**Deutschland:** Avira, (GData) |
| **Exploit Protection / Sicherer Browser** | A +++<br>B ++<br>C -- | alle ab Klasse 1 | Angriffe durch infizierte Webseiten, Diebstahl lokaler persönlicher Daten | **Ausland:** Bromium (USA), Invincea (USA)<br><br>**Deutschland:** Sirrix, secunet |
| **Device und Portkontrolle** | A ++<br>B 0<br>C -- | alle ab Klasse 2 | Kopie vertraulicher Dokumente auf beliebige externe Datenträger | **Ausland:** Symantec (USA), Sophos (Großbritannien), McAfee/Intel (USA), DeviceLock (USA)<br><br>**Deutschland:** itWatch, (CenterTools) |
| **Full Disk Encryption** | A +++<br>B 0<br>C 0 | alle ab Klasse 1 | Einsehen von Daten auf verlorenen oder gestohlenen Geräten durch Unbefugte | **Ausland:** Microsoft (USA), McAffee/Intel (USA), Sophos (Großbritannien), Winmagic (Kanada), EgoSecure/Kaspersky (Russland)<br><br>**Deutschland:** Sirrix, secunet, (CE Infosys), (CenterTools) |
| **File & Folder Encryption** | A +++<br>B 0<br>C 0 | alle ab Klasse 1 | Diebstahl von Wechseldatenträgern und Extraktion sensibler Daten | **Ausland:** Microsoft (USA), Symantec (USA), Cryptzone (Schweden), Cypherix (Süd-Afrika), DESlock (UK)<br><br>**Deutschland:** AppSec, itWatch, Sirrix, Secomba |

Bewertung der Lage in Deutschland:
**A Bedeutung für die Zukunft**
**B Technologischer Vorsprung in Deutschland**
**C Marktstärke der dt. Unternehmen**

# Analyse der Anbieter im In- und Ausland
## → Client- und Serversicherheit (2)

| Client- und Serversicherheit | Bewertung | erforderlich ab Wirkungsklasse | Bedrohungen | In- und Ausländische Anbieter |
|---|---|---|---|---|
| **Voll-Virtualisierung / TrustedComputing, Seperation** | A ++<br>B 0<br>C 0 | alle ab Klasse 2 | Infektion oder Angriffe auf einen Rechner kompromittiert das gesamte System | **Ausland:** Sysgo/Thales (Frankreich), oklabs/General Dynamics (USA), Oracle (USA), Lynx Software Technologies (USA), BlackBerry (Kanada), Bromium (USA)<br><br>**Deutschland:** secunet, Sirrix, genua, Trust2Core |
| **Data Leakage Prevention** | A ++<br>B 0<br>C - | alle ab Klasse 2 | Abfluß hochsensibler Daten nach Außen | **Ausland:** Symantec (USA), RSA (USA), Websense (USA), Sophos (Großbritannien)<br><br>**Deutschland:** itWatch, iT-Cube Systems |
| **E-Mailverschlüsselung** | A +++<br>B -<br>C - | alle ab Klasse 0 | Abfangen, Mitlesen, Manipulieren von E-Mail-Korrespondenz | **Ausland:** Microsoft (USA), Symantec (USA)<br><br>**Deutschland:** Telekom/Telesec, Sirrix, Giegerich & Partner |
| **Sicheres Logon (Smartcard etc.)** | A +<br>B 0<br>C + | alle ab Klasse 1 | Nicht autorisierte Nutzung von Geräten | **Ausland:** RSA (USA), gemalto/SafeNet (USA), gemalto (Niederlande)<br><br>**Deutschland:** Telesec, secunet, Giesecke & Devrient, Bundesdruckerei/D-TRUST, Sirrix |
| **Remote Access / Secured VPN** | A +<br>B +<br>C - | alle ab Klasse 2 | Belauschen der Kommunikation zwischen Host und entfernter Maschine | **Ausland:** Cisco (USA), Juniper (USA)<br><br>**Deutschland:** NCP, secunet |

Bewertung der Lage in Deutschland:
**A Bedeutung für die Zukunft**
**B Technologischer Vorsprung in Deutschland**
**C Marktstärke der dt. Unternehmen**

# Analyse der Anbieter im In- und Ausland
## → Mobile Security

| Mobile Security | Bewertung | erforderlich ab Wirkungsklasse | Bedrohungen | In- und Ausländische Anbieter |
|---|---|---|---|---|
| **App Security / Secure Marketplace** | A ++<br>B -<br>C - | alle ab Klasse 2 | Einschleusen von bösartigen Apps, um Daten auf mobilen Geräten auszuspähen | **Ausland:** Bitdefender (Rumänien), Sophos (Großbritannien), Samsung (Südkorea)<br><br>**Deutschland:** Avira |
| **Sichere Plattform** | A +<br>B +<br>C 0 | alle ab Klasse 2 | Angriffe auf qualitativ mangelhafte Softwarekomponenten eines Systems | **Ausland:** Secusmart/Blackberry (Kanada), Blackphone (Schweiz), Thales (Frankreich)<br><br>**Deutschland:** Trust2Core, Sirrix |
| **Cloud Encryption** | A +++<br>B +<br>C + | alle ab Klasse 0 | Ausspähen von Daten und Diebstahl geistigen Eigentums durch Dritte (Firmen, Mitarbeiter, Geheimdienste) | **Ausland:** Spideroak (USA), Trend Micro (Japan), CipherCloud (USA)<br><br>**Deutschland:** Sirrix, Telekom, itWatch, Secomba |
| **Voice Encryption** | A ++<br>B +<br>C 0 | alle ab Klasse 3 | Ausspähen von Gesprächen | **Ausland:** BlackBerry/Secusmart (Kanada), Whisper Systems (USA), Sectra (Schweden)<br><br>**Deutschland:** GSMK, Rohde & Schwarz, Sirrix, Trust2Core |
| **Secure Messaging** | A +++<br>B -<br>C - | alle ab Klasse 0 | Mitschneiden und Auswerten aller Inhalte textueller Kommunikation | **Ausland:** BlackBerry (Kanada), Threema (Schweiz), Brosix (Bulgarien), Open Whisper Systems (USA)<br><br>**Deutschland:** GSMK, Sirrix, Chiffry, shape.ag |
| **Mobile Device Management** | A ++<br>B -<br>C - | alle ab Klasse 2 | Angriffe auf mobile Geräte aufgrund von Schwachstellen durch mangelnde Wartung oder Diebstahl | **Ausland:** Airwatch/VMWare (USA), MobileIron (USA), Good Technology (USA), Sophos (Großbritannien), Fiberlink/IBM (USA), Citrix (USA), Soti (Kanada), Symantec (USA), EgoSecure/Kaspersky (Russland)<br><br>**Deutschland:** Sirrix, SEVEN PRINCIPLES |
| **Basistechnologie (Secure Execution Environment)** | A +<br>B --<br>C -- | alle ab Klasse 3 | Angriff auf Systemebene und Ausspähen von Daten durch Unbefugte | **Ausland:** Samsung (Südkorea), Trustonic (Großbritannien)<br><br>**Deutschland:** - |

Bewertung der Lage in Deutschland:
**A Bedeutung für die Zukunft**
**B Technologischer Vorsprung in Deutschland**
**C Marktstärke der dt. Unternehmen**

# Anhang 2
## → Wirkungsklassen im Detail

- **Nachfolgend finden Sie eine detaillierte Beschreibung zu den einzelnen Wirkungsklassen 0 bis 4.**

# Wirkungsklassen

## → Wirkungsklasse 0: Basis-IT-Sicherheit

*Möglichst besonders vertrauenswürdige Technologien aus Deutschland*

### IT-Sicherheitsmaßnahmen

- **Technologien zur Abwehr von Schadsoftware**
- **Software zum Schutz der Privatsphäre**
- **Daten in der Cloud verschlüsseln**
- „BSI für Bürger“ Sicherheitstipps und Checklisten *(bsi-fuer-buerger.de)*
- Automatische Updates (Nutzung aller Möglichkeiten des Betriebssystems)
- Arbeiten mit eingeschränkten Benutzerrechten

### Personale Sicherheitsmaßnahmen

- Solides Basiswissen über Umgang mit IT und IT-Sicherheits-Gefahren notwendig, also ein Mindestmaß an Verständnis über die Wirkung und mögliche Konsequenzen von Fehlverhalten oder der notwendigen Schritte bei Problemfällen

# Wirkungsklassen
## → Wirkungsklasse 1: Erweiterte IT-Sicherheit

### IT-Sicherheitsmaßnahmen

- Basis-IT-Sicherheit, zudem zusätzlich:
  - Sichere Anwendungen/Browser *(z.B. wenn möglich kein Java, Flash)*
  - Backupsoftware und sichere Verwahrung
  - Cloud nur in Verbindung mit Verschlüsselung
    *(Zero-Knowledge, Technologie von ext. Anbietern, separat eingesetzt, Ziel: Cloud-Dienstanbieter hat keinerlei Möglichkeiten zur Einsicht der ihm anvertrauten Daten)*

### Personale Sicherheitsmaßnahmen

- Basiswissen + erweitertes Wissen über Umgang und Gefahren notwendig und umfangreiches Wissen über Datenschutzaspekte und den Umgang mit persönlichen Daten

# Wirkungsklassen

## → Wirkungsklasse 2: Höherwertige IT-Sicherheit

*Möglichst besonders vertrauenswürdige Technologien aus Deutschland*

### IT-Sicherheitsmaßnahmen

- **Erweiterte-IT-Sicherheit, zudem zusätzlich:**
  - **Sicherheitskern**
  - **Verschlüsselung**
  - **Sicheres Identitätsmanagement**
  - **Frühwarnsysteme**

### Personale Sicherheitsmaßnahmen

- Erweitertes Wissen + Wissen über intelligente Social Engineering Angriffe
- Sicherheitstraining bei dem größeren Wert auf die Verantwortung gelegt werden muss, um sich darüber klar zu werden, welche höhere Risiken eventuelle Angriffe mit sich bringen können

# Wirkungsklassen

## → Wirkungsklasse 3: Hochwertige IT-Sicherheit

### IT-Sicherheitsmaßnahmen

- Höherwertige IT-Sicherheit
- Plus
  - **Proaktive IT-Sicherheitstechnologien**

*Möglichst besonders vertrauenswürdige Technologien aus Deutschland*

### Personale Sicherheitsmaßnahmen

- Erweitertes Wissen + Sicherheitstraining und Awareness bei dem zum einen aufgezeigt werden muss, welche Verantwortung diese Sicherheitsklasse mit sich bringt und zum anderen, welche Risiken vorhanden sind und welche Konsequenzen hierbei einher gehen und die Vermeidung dieser
- Aufklärung darüber, wie man Unklarheiten beseitigt und wo externe kompetente Hilfe zu finden ist, falls die eigene Kompetenz die Grenzen erreicht hat

# Wirkungsklassen

## → Wirkungsklasse 4: Geheimschutz-IT-Sicherheit

### IT-Sicherheitsmaßnahmen

*Möglichst besonders vertrauenswürdige Technologien aus Deutschland*

- **Hochwertige-IT-Sicherheit**
- **erweiterte Sicherheitsmaßnahmen**
- **Strenge gesetzliche zu erfüllende Vorgaben gemäß Geheimschutzordnung** (VS/GSO) zur Wahrung der nationalen Sicherheit

### Personale Sicherheitsmaßnahmen

- Umfassendes Sicherheitstraining und ausführliche Awareness-Maßnahmen
- Besonderes Wissen über zielgerichtete Angriffe
- Einhaltung der notwendigen Vorschriften in höchstem Maße im Dienste der nationalen Sicherheit und der internationalen Partner