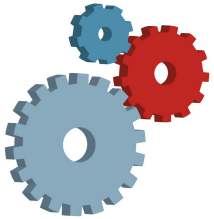
Bundesamt
für Sicherheit in der
Informationstechnik



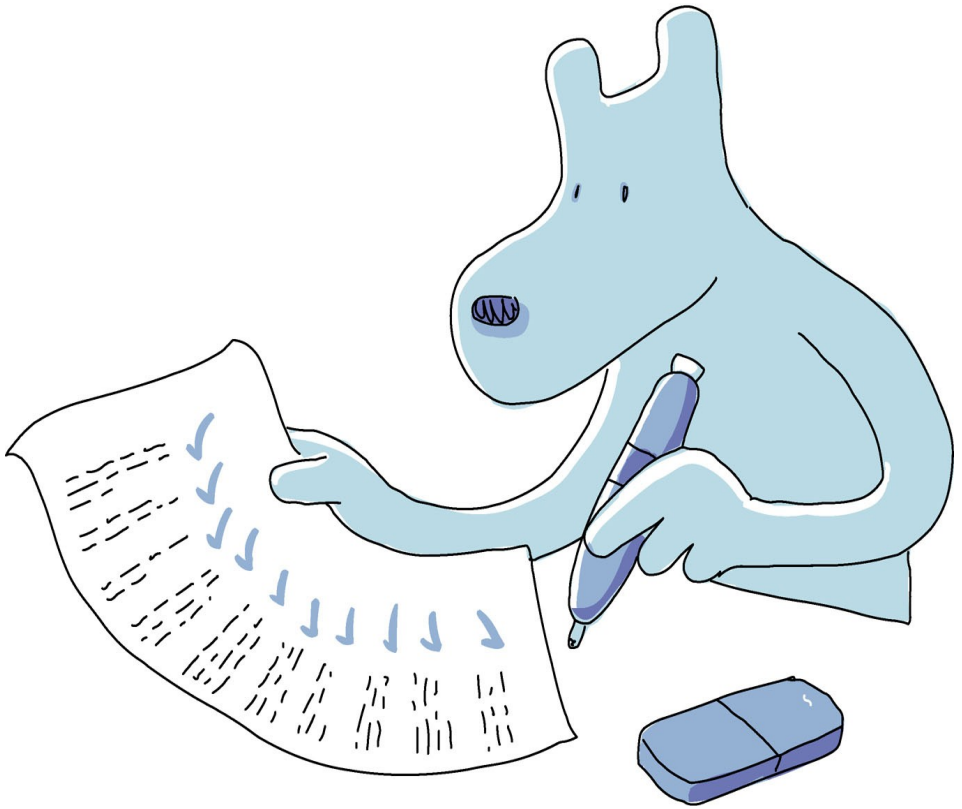
Modernisierung des IT-Grundschutzes

Isabel Münch
Referatsleiterin Allianz für Cyber-Sicherheit,
Penetrationszentrum und IS-Revision
Bundesamt für Sicherheit in der Informationstechnik

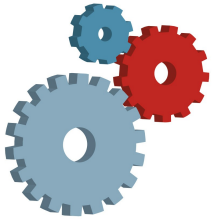
ViS!T
28./29.10.2014
Wien

Agenda

- IT-Grundschutz: Status Quo
- Modernisierungs-Fahrplan
- Situationsanalyse
- Modernisierungsansätze
- IT-Grundschutz-Tools
- Ausblick



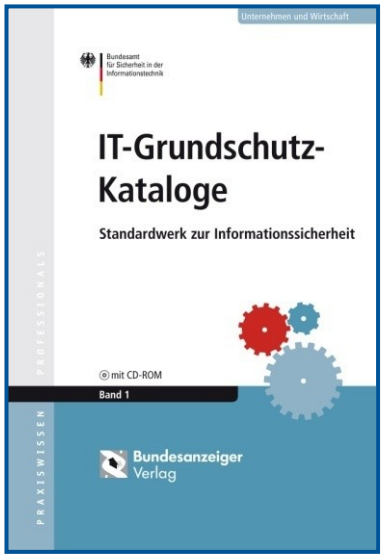
IT-Grundschutz: Status Quo



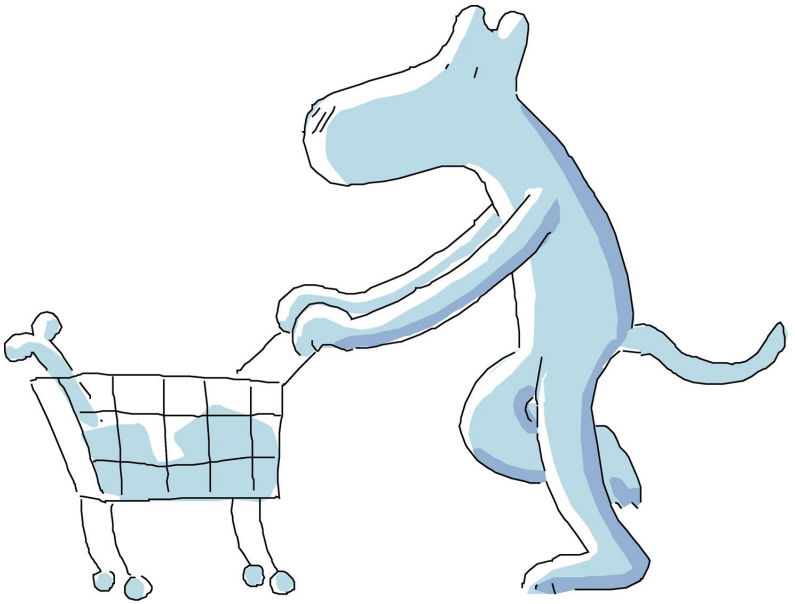
- IT-Grundschutz-Kataloge:
  - 2013: 13. Ergänzungslieferung
  - 2014: 14. Ergänzungslieferung
  - Danach ggf. 15. Ergänzungslieferung (oder neue Fassung)

    Windows 8, Netzarchitektur, Netz-Management, Identitäts- und Berechtigungsmanagement, etc.
- Veröffentlichung der englischen Übersetzung
- Zertifizierung:
  2014: 20 Zertifikate erteilt, 17 in Planung
- GSTOOL 4.x:
  Vertrieb bis Ende 2014, zuzüglich 2 Jahre Support

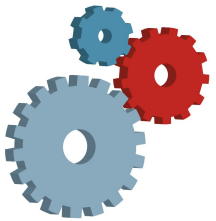
IT-Grundschutz-Kataloge
14. Ergänzungslieferung



- **Neue Bausteine:**
  - Cloud-Management
  - Cloud-Storage
  - Web-Services
  - Cloud-Nutzung
  - Allgemeine Anwendung
  - Sensibilisierung und Schulung zur Informationssicherheit
  - B 3.404 Mobiltelefon
  - B 3.405 Smartphones, Tablets und PDAs
- **Ziel: Veröffentlichung 2014**



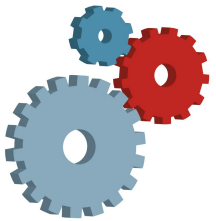
Neuausrichtung
20 Jahre IT-Grundschutz – und nun?



- Neue Anforderungen nach 20 Jahren
- Optimierung und Aktualisierung der Vorgehensweise und IT-Grundschutz-Kataloge
- Gewährleistung der Kontinuität:
  - Weiterentwicklung der "alten" IT-Grundschutz-Welt incl. 2015
  - Modernisierung zum „neuen“ IT-Grundschutz in 2015
  - Fließender Übergang und Migration ab 2016
- Ziel:

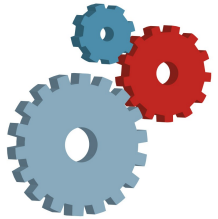
  Erhöhung der Attraktivität, Flexibilität und Skalierbarkeit sowie Schaffung der Basis für die nächsten 20 Jahre

Fahrplan Modernisierung

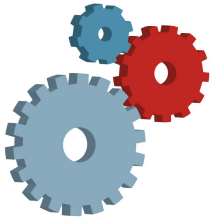


- IT-Grundschutz Neu
  - Konzeption: 2014
  - Realisierung: 2015
  - Migration: 2016
- IT-Grundschutz Classic
  - Ergänzungslieferungen bis inkl. 2015
  - GSTOOL-Pflege:
    - Metadaten-Updates für die Ergänzungslieferungen
    - Support bis Ende 2016

Fahrplan Modernisierung



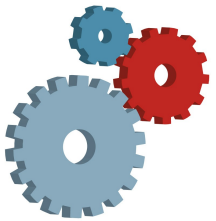
- Modernisierungs-Workshops
  - 10.09.2013: IT-SiBe-Treffen
  - 12.02.2014: BSI-interner Workshop
  - 25.02.2014: GS-Auditorentag
  - 11.03.2014: CeBIT-Diskussion
  - 30.04.2014: Workshop mit Auditoren
  - 07.05.2014: Workshop mit Auditoren
  - 13.05.2014: Workshop mit Tool-Herstellern
  - 22.05.2014: Workshop mit Ressort-IT-SiBes des Bundes
  - 27.05.2014: Workshop mit Power-Usern
  - 06.10.2014: Workshop IT-SiBe der Länder und Kommunen
  - ...



Situationsanalyse

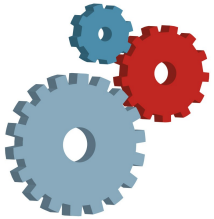
IT-Grundschutz

Situationsanalyse



- **Ausreichende Orientierung an mittleren Institutionen?**
  - Adressaten und Nutzer hauptsächlich mittlere Größe!
  - Ressourcen dort für IT-Sicherheit knapp
  - Ausreichende Berücksichtigung der Management- und Umsetzungs-Aufwände gegenüber vorhandenen Ressourcen?
- **Bedarf bei Groß-Unternehmen?**
  - Internationale Ausrichtung mit ISO 27001 zum IT-Sicherheitsmanagement, IT-Grundschutz als Hilfsmittel zur Umsetzung der IT-Sicherheit
  - Eigene Vorgehensweisen für Risikomanagement und Maßnahmenumsetzung
  - Eigenes Personal in großem Umfang

Situationsanalyse

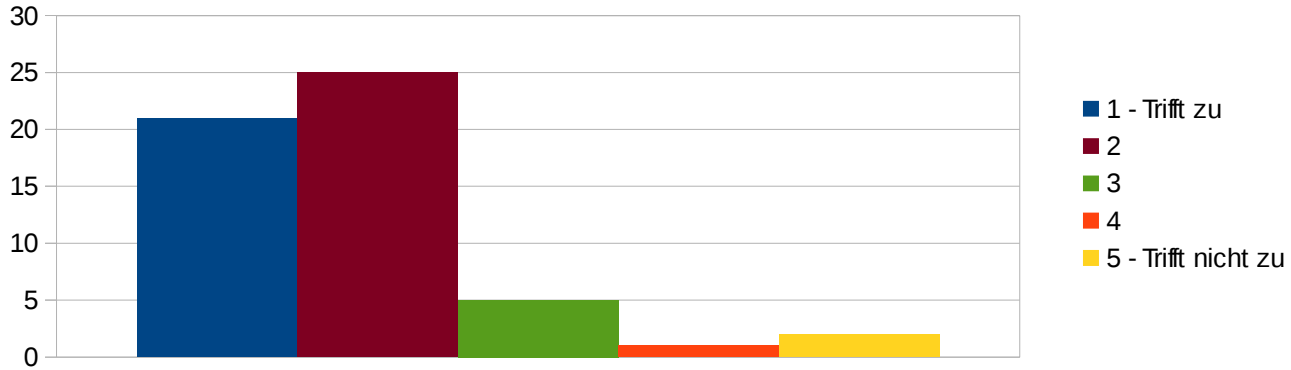


- **Priorisierte Vorgehensweisen fehlen?**
  - Ein vollständiges IS-Management mit der Umsetzung notwendiger Maßnahmen überfordert viele und gerade kleine und mittlere Institutionen
  - Gerade kleine und mittlere Institutionen (10-1000 MA) suchen oft zunächst nach den wichtigsten Sicherheitsmaßnahmen und nicht nach einem vollständigen Sicherheitsprozess
  - Oft sollte es primär vor allem um den „Schutz der Kronjuwelen“ gehen
  - Diese Bedürfnisse deckt der IT-Grundschutz „alt“ nicht ausreichend ab

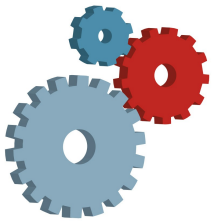
Situationsanalyse

- **Hoher Aufwand in der Initialisierung von IT-Grundschutz**
  - Vollständige Strukturanalyse
  - Schutzbedarfsfeststellung
  - Erstellung von Sicherheitskonzepten
  - Risikoanalyse
  - Dokumentation
- **Gefahr:** Erstellung von Sicherheit nur auf dem Papier. Wegen fehlender Ressourcen zur Umsetzung von Maßnahmen ist Institution trotz Dokumentation weiterhin gefährdet

Arbeitsschritte GS erfordern oft erhöhten Arbeits- und Verwaltungsaufwand?

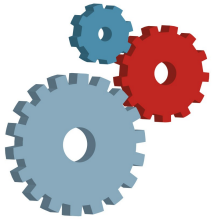


Situationsanalyse



- **Möglichkeit der Risikoakzeptanz oft nicht bekannt?**
- Risikoakzeptanz ist im IT-Grundschutz vorgesehen, z. B.:
  - BSI-Standard 100-2, 5.3. Kosten und Aufwandsschätzung
    - Maßnahmen müssen wirtschaftlich umsetzbar sein
    - Restrisiko kann getragen werden
    - Entscheidung ist zu dokumentieren
  - BSI-Standard 100-3, 6.1. Umgang mit Risiken
    - Handlungsalternative "Risikoübernahme"
    - Gefährdung tritt nur unter speziellen Voraussetzungen ein
    - Keine praxisnahe Gegenmaßnahme bekannt
    - Unwirtschaftlich
  - Bislang kein eigener Risikomanagement- und Risikoakzeptanzprozess

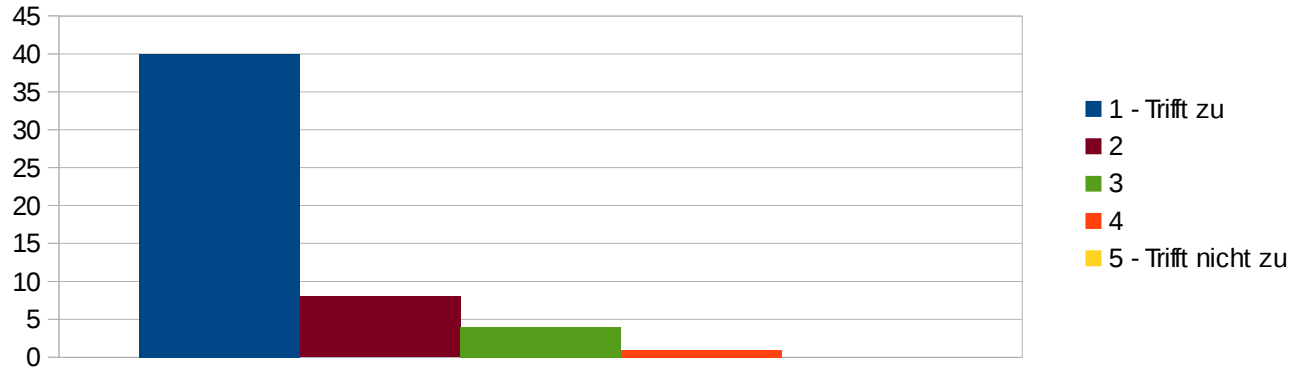
Situationsanalyse



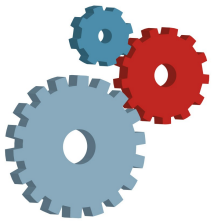
- **Passender Umfang des IT-Grundschutzes?**
  - Fehlende Aufbereitung des Gesamtwerks für Zielgruppen
    - Management
    - IT-SiBe
    - Umsetzer (Administratoren, Organisatoren, Infrastruktur...)
  - 4500 Seiten adressieren IT-SiBe und Umsetzer
  - Hohe Seitenzahl ist negativ besetzt
  - dennoch hohe Nachfrage nach aktuellen Themen (führt zu noch höherem Umfang)

Situationsanalyse

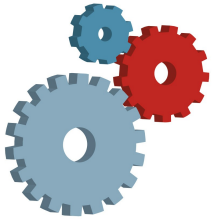
- **Mehrere parallele Empfehlungswerke des BSI?**
  - BSI-Standards 100-1, 100-2, 100-3, 100-4
  - IT-Grundschutz-Kataloge
  - Übersichtspapiere
  - ISi-Schriftenreihe
  - HV-Kompendium
  - Empfehlungen der Allianz für Cyber-Sicherheit
  - Studien
  - …



Situationsanalyse



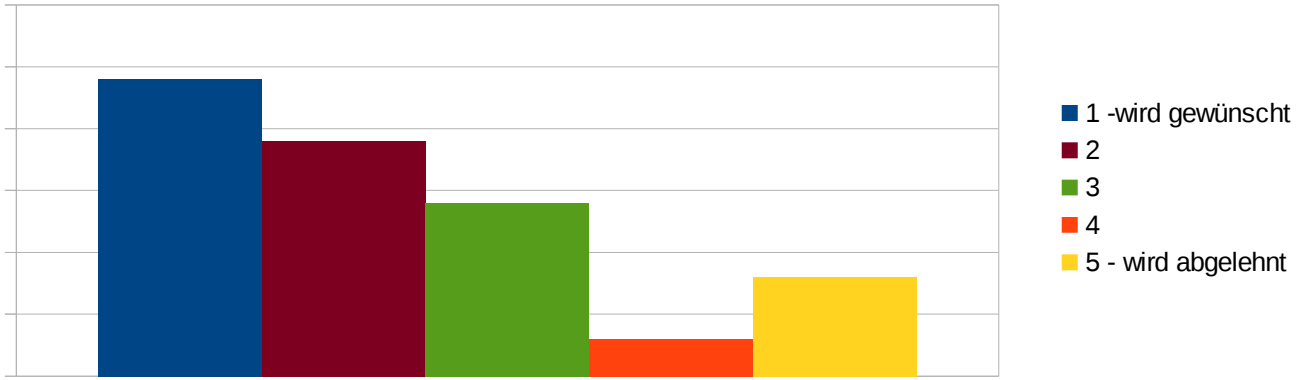
- **Zu hohes Sicherheitsniveau IT-Grundschutz für den normalen Schutzbedarf?**
- IT-Grundschutz „alt“ adressiert normalen Schutzbedarf
- Auch bei hohem Schutzbedarf werden in der Praxis oft nur vorhandene IT-Grundschutz-Maßnahmen herangezogen
- Differenzierung fehlt: Stand der Technik vs. Hochsicherheit
- Sicherheitsziel:
  - Je mehr Sicherheit, umso besser?
  - Wieviel Sicherheit ist ausreichend?



Modernisierungsansätze IT-Grundschutz Neu

Modernisierungsansätze

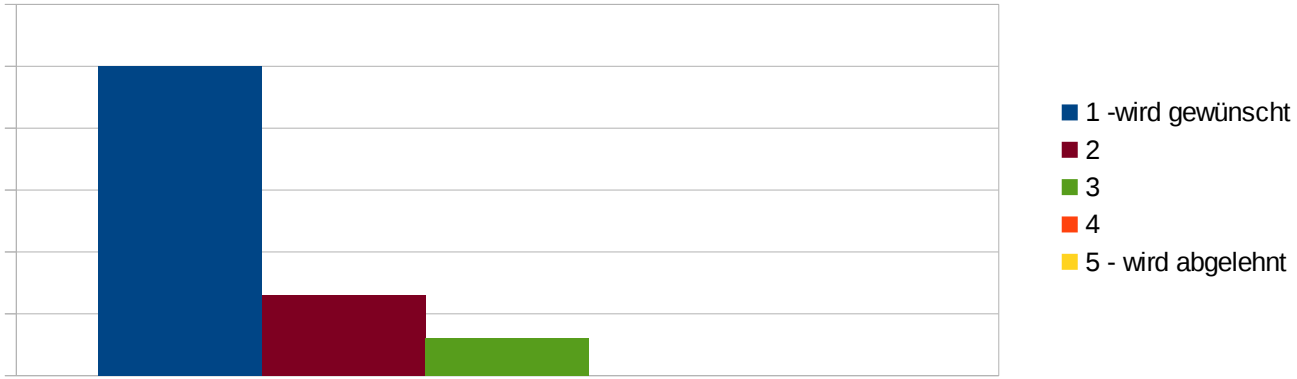
- **Stärkere Berücksichtigung der Zielgruppe kleine und mittlere Institutionen**
  - Typische Größe: 50 - 5000 Mitarbeiter/innen
  - Vorgehensweise, Aufwand und Maßnahmenauswahl berücksichtigen stärker die realen Möglichkeiten von kleinen und mittleren Institutionen
  - Bleibt auch für große Institutionen nützlich, diese nutzen IT-Grundschutz jedoch meist als ein Hilfsmittel neben anderen



Modernisierungsansätze

Skalierung der Maßnahmen

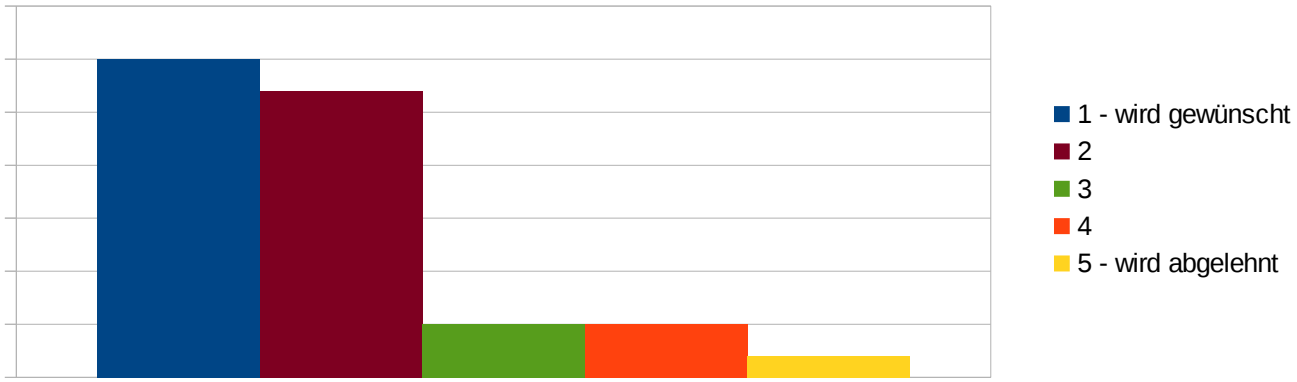
- Erst-Maßnahmen (wenige, wichtig, dringlich)
- Basis-Maßnahmen (Stand der Technik) für den normalen Schutzbedarf
- Hochsicherheits-Maßnahmen für Vertraulichkeit und Verfügbarkeit (als Beispiele, keine Vorgaben)



Modernisierungsansätze

Angebot verschiedener Vorgehensweisen

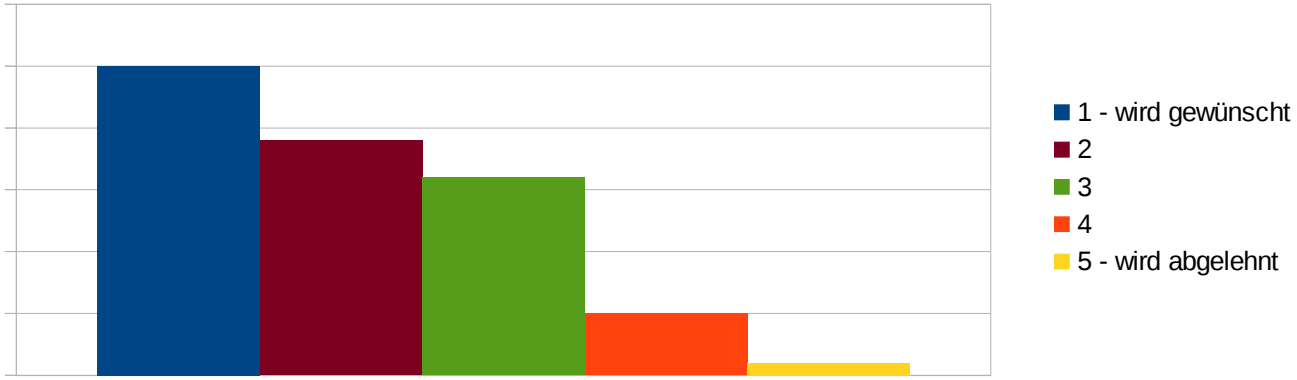
- Bottom-Up: 80:20 Umsetzung der Erst- und Basismaßnahmen mit Modellierung, ohne Schutzbedarfsfeststellung, ohne Risikoanalyse
- Erstellung eines Sicherheitskonzept (wie heute: Prozesse, Schutzbedarf, Modellierung, Risikoanalyse, ...)
- „Kronjuwelen-Ansatz“: Primär Cyber-Sicherheit für die wichtigsten Schutzobjekte



Modernisierungsansätze

Neufassung der Risikoanalyse

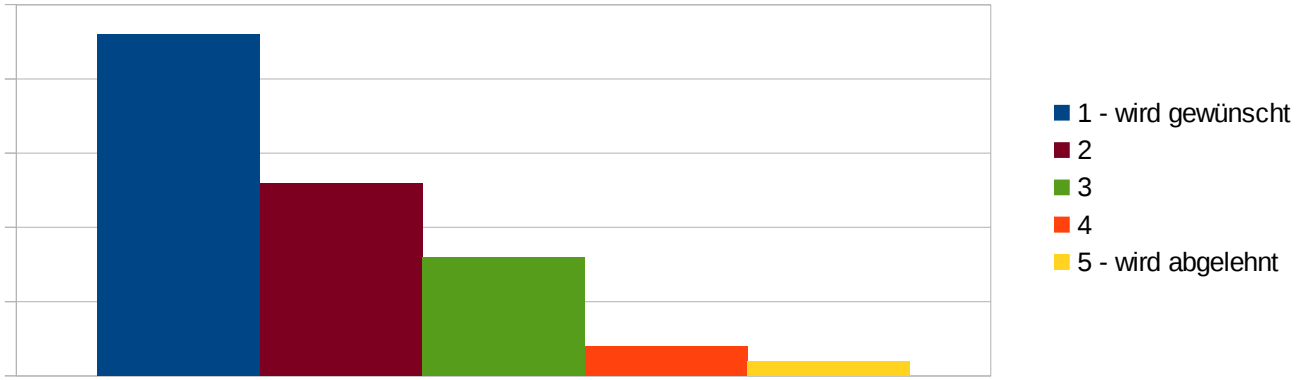
- bislang: IT-Grundschutz-spezifisches Verfahren auf der Basis der Gefährdungskataloge
- Festlegung: Bündelung aller risikobezogenen Arbeitsschritte im BSI-Standard 100-3, einschließlich Schutzbedarfsfeststellung
- BSI priorisiert die Bedrohungen/Schwachstellen des IT-Grundschutzes anhand der aktuellen Lage
- BSI gibt Maßnahmenbeispiele für Hochschutz heraus



Modernisierungsansätze

Grundsätzliche Adaption von ISO 2700X

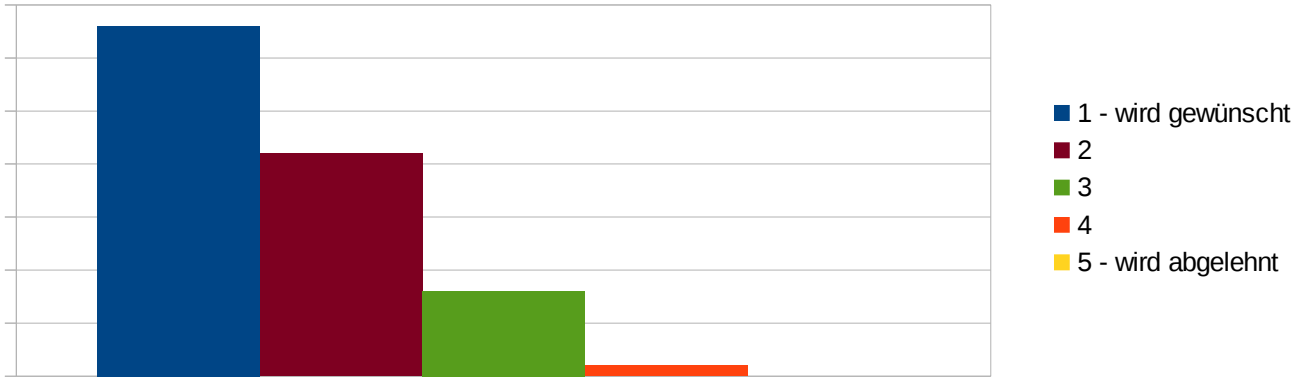
- Baustein für IT-Sicherheitsmanagement
  - Erst-Maßnahmen = wichtigste Maßnahmen des ISMS
  - Basis-Maßnahmen = ggf. unterhalb ISO 27001
  - Hoch-Maßnahmen = Verweis auf ISO 27001 oder oberhalb ISO 27001
- Ggf. Baustein „ISO 2700X-Konformität“ (Maßnahmen-Differenz zwischen ISO 27001 und Erst-/ Basis-Maßnahmen)



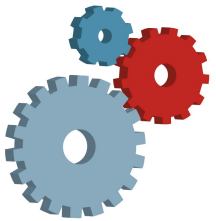
Modernisierungsansätze

Risikoorientierte Anwendung

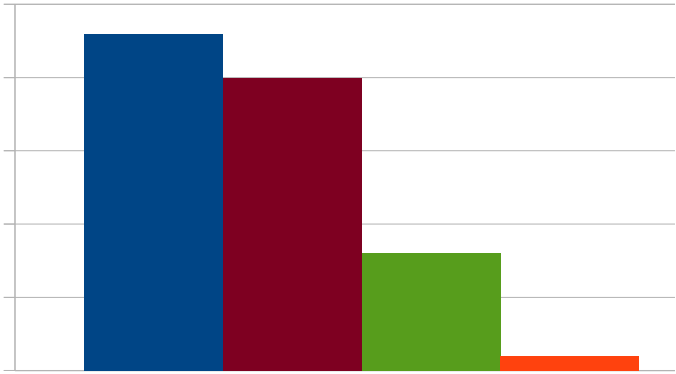
- Implementation des Risikoentscheidungsprozesses
- Inhärente Nutzung des Lagebildes
- Keine Risikoakzeptanz für Erst-Maßnahmen
- Explizite Möglichkeit der Risikoakzeptanz im Basis-Maßnahmen und Hochschutz-Maßnahmen



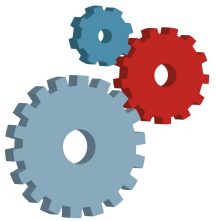
Modernisierungsansätze



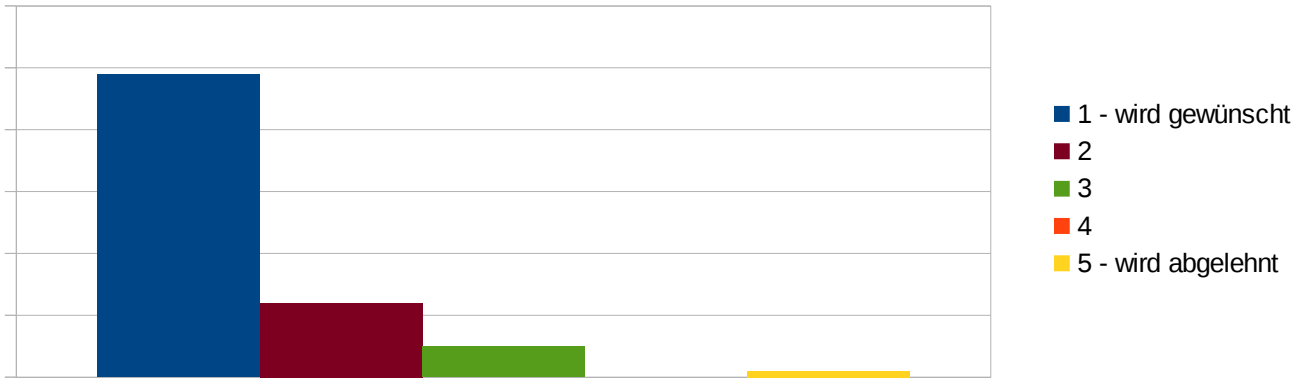
- **Tatsächliche Gefährdungslage als Grundlage**
- Quellen der Gefährdungslage:
  - BSIG §4: Meldungen der Bundesverwaltung als Quelle für Lageeinschätzungen
  - Meldepflicht KRITIS (IT-Sicherheitsgesetz)
  - Meldungen über Allianz für Cyber-Sicherheit
  - Befragungen von Branchen
- Konsolidierte Gefährdungslage
  - Trennung in Bedrohungen und Schwachstellen?
  - „TOP 10“ Bedrohungen je Themengebiet
  - „TOP 10“ Schwachstellen je Themengebiet
- Basis für Risikoanalyse und Risikoentscheidung



Modernisierungsansätze

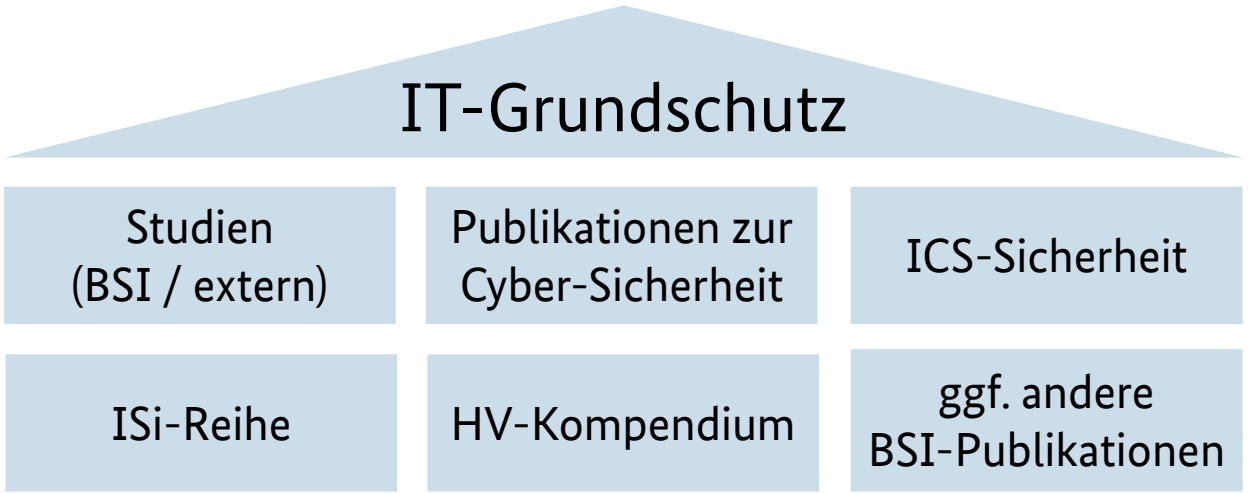


- **Verschlankung der Bausteine**
  - Rund 10 Seiten für einen Baustein (für den CISO)
  - Kürzere Erstellungszeiten, einfachere Aktualisierung
  - Verbesserte Lesbarkeit der Bausteine
  - Ergänzt um Umsetzungshinweise (für Admins)
    - Studien
    - Alte Bausteine
    - Hersteller-Dok.
    - Tools

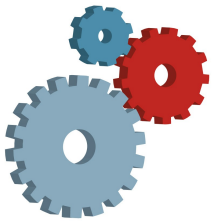


Modernisierungsansätze

- **Integration aller BSI-Empfehlungen unter einem Dach**
  - IT-Grundschutz
  - ISi-Schriftenreihe
  - ACS-Empfehlungen
  - ICS-Empfehlungen
  - Studien
  - 100-4, UMRA
  - HV-Kompendium



Modernisierungsansätze

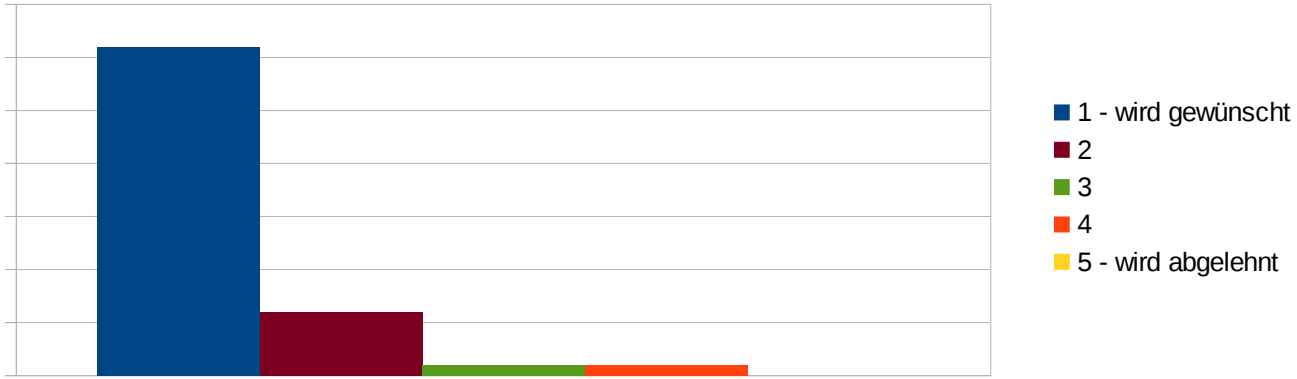


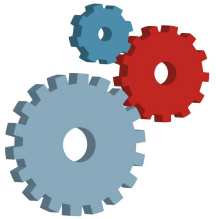
- **Entwicklung von GS-Profilen**
  - GS-Profil = Auswahl anzuwendender Bausteine und Maßnahmen für typische Institution, berücksichtigt Möglichkeiten und Risiken der Institution
  - Beispiel:
    - GS-Profil: Kommunalverwaltung in Bundesland XY
    - GS-Profil: Krankenhaus
    - GS-Profil: Wasserwerk als kritische Infrastruktur
  - Anwendbar als "Schablone"
  - Erstellung durch / mit Stakeholder
  - Zertifizierung nach GS-Profilen wird diskutiert

Modernisierungsansätze

Unterstützung der Migration

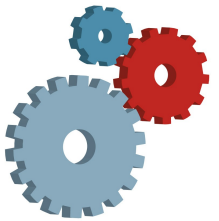
- Abbildung „alt auf neu“
- Einbindung der Tool-Hersteller
- Tool-Anforderung
  - Migration Sicherheitskonzept aus GSTOOL 4.x in neues Tool
  - Migration des Sicherheitskonzepts vom alten IT-Grundschutz auf den neuen IT-Grundschutz





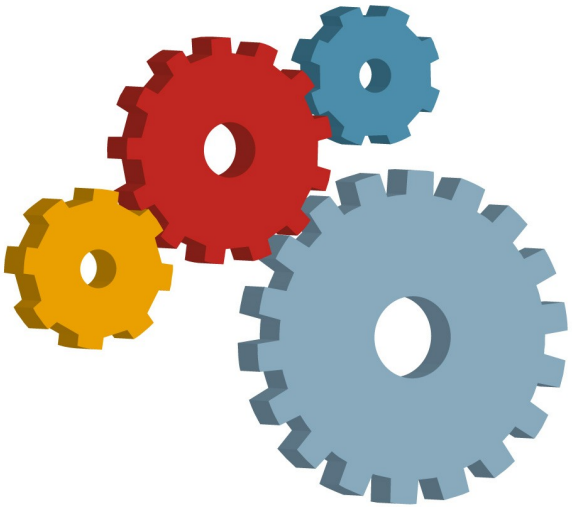
IT-Grundschutz Tools

GSTOOL
Wie geht es weiter?

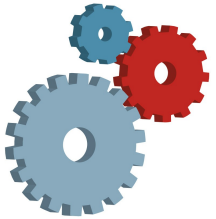


- Zukünftig keine Tool-Entwicklung durch das BSI
- Weiterhin Vertrieb des GSTOOL 4.x bis Ende 2014
- Support für mindestens zwei weitere Jahre

- Marktverfügbare IT-Grundschutz-Tools
  - Müssen Modernisierung des IT-Grundschutz unterstützen
  - Diskussion mit Herstellern
    - Import von Sicherheitskonzepten
    - Zukünftige Strukturelemente
  - Ziel: Vielfältiges Tool- und Hilfsmittel-Angebot

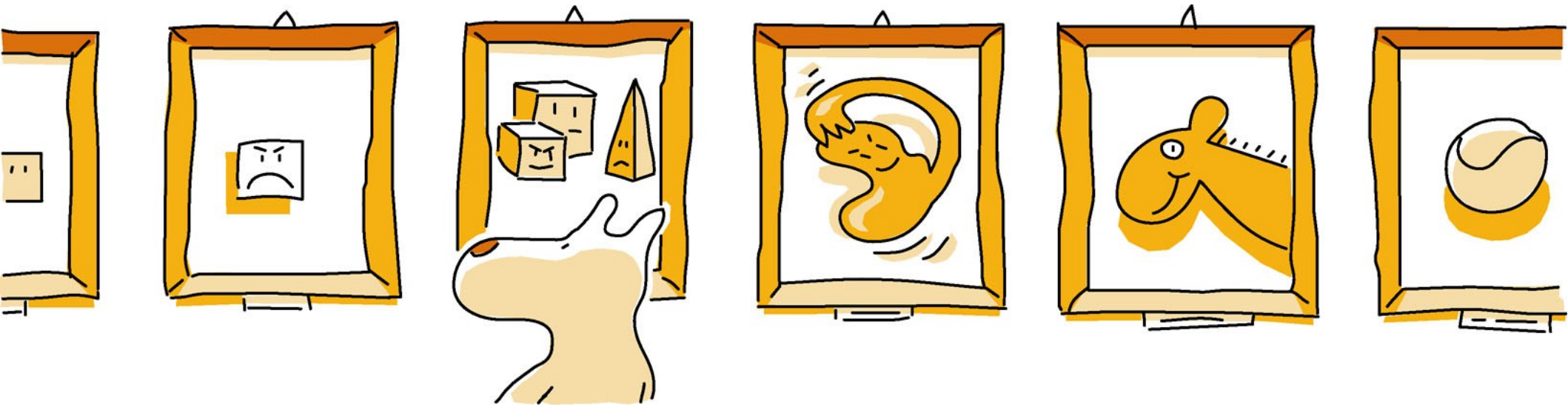


Modernisierung
Wie geht es weiter?



- Suche nach einem prägnantem Namen
  (Bisher Arbeitstitel: IT-Grundschutz Neu)
- Auswertung der Workshops und der aktuellen Umfrage
- Weitere Gespräche mit Nutzern
- Erstellung der ersten Konzepte bis Ende 2014
  - Diese werden zur Diskussion gestellt!
- Realisierung und Migration: 2015

Fragen und Diskussion



Kontakt

XING: Gruppe "Allianz für Cyber-Sicherheit"
Twitter: @CyberAllianz

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Isabel Münch
Referat C 23
Postfach 20 03 63
53133 Bonn

Telefon: +49 (0)228 99 9582 5367
Telefax: +49 (0)228 99 10 9582 5367

isabel.muench@bsi.bund.de

www.allianz-fuer-cybersicherheit.de
www.bsi.bund.de
www.bsi-fuer-buerger.de