Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Neues aus dem IT-Grundschutz

Florian Göhler - Referat BSI-Standards und IT-Grundschutz

22.04.2024, KITS

IT-Grundschutz++

- Überarbeitung des Kompendiums
- Vorstellung bei Anwendenden und Pilotierung
- Pflege aktueller Grundschutz
- Neue Produkte

In einer mehrjährigen Übergangszeit werden aktueller und künftiger IT-Grundschutz nebeneinander bestehen und anwendbar bleiben.

Satzschablonen

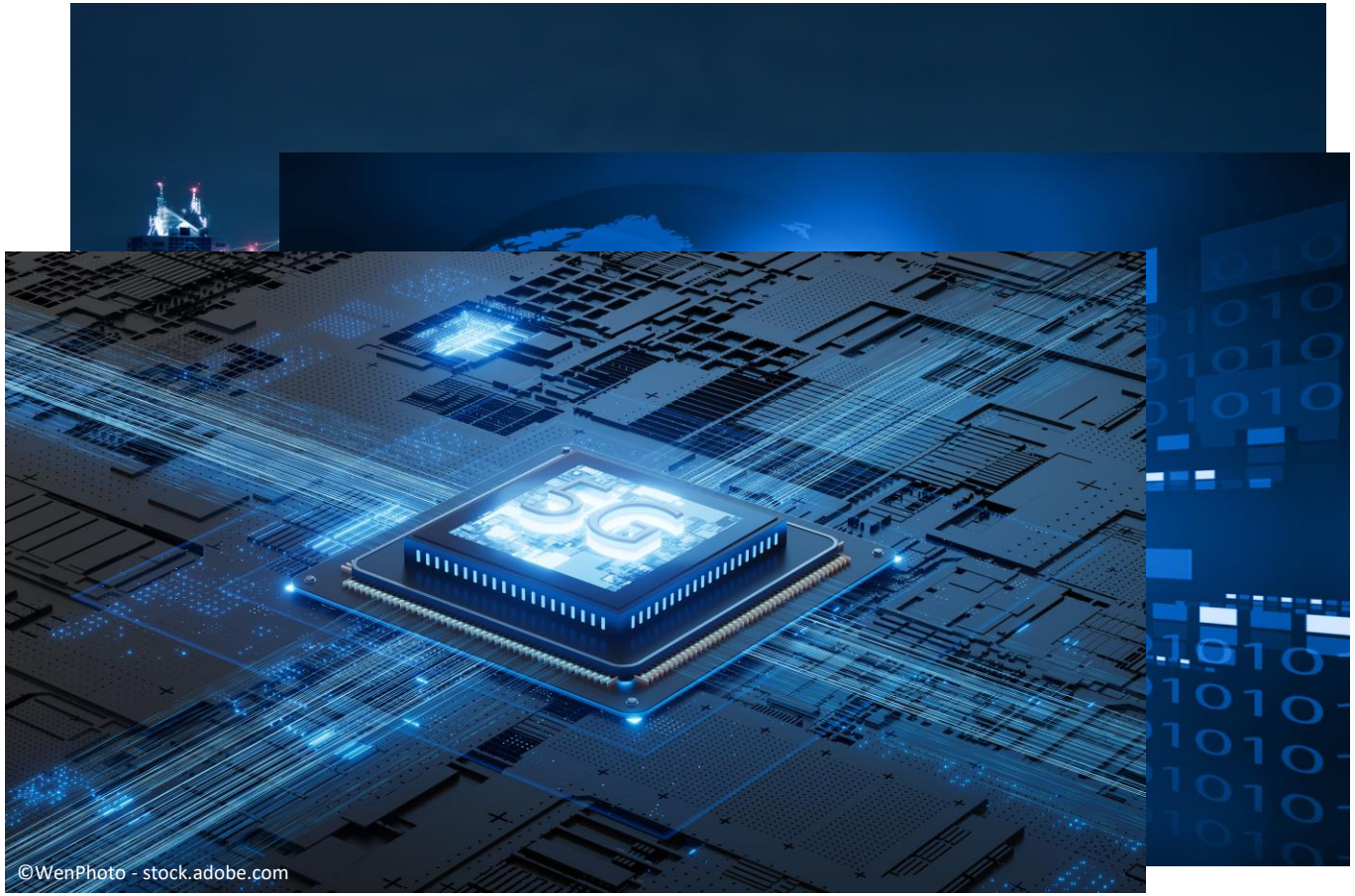
Strukturierte Anforderungen für den IT-Grundschutz

Strukturierte Anforderungen

Strukturierte Anforderungen

- Fokus Informationssicherheit

Strukturierte Anforderungen



©WenPhoto - stock.adobe.com

- Fokus Informationssicherheit
- (Fast) Keine „Umsetzungsanforderungen“

Strukturierte Anforderungen

- Fokus Informationssicherheit
- (Fast) Keine „Umsetzungsanforderungen“
- Prüfbarkeit
- Eindeutigkeit

Strukturierte Anforderungen

- Fokus Informationssicherheit
- (Fast) Keine „Umsetzungsanforderungen“
- Prüfbarkeit
- Eindeutigkeit
- Schärfung Dokumentationsanforderungen

Struktur durch Satzschablonen

{Zielobjekt} [Präzisierung ZO] {MODALVERB} <Ergebnis> [Präzisierung Prozess] {Prozesswort}

Beispiel

Struktur durch Satzschablonen

- Der Konfigurationsprozess für E-Mail-Clients SOLLTE die automatische Interpretation von HTML-Code und aktiven Inhalten verhindern.
- Der Konfigurationsprozess für E-Mail-Clients SOLLTE eine sichere Transportverschlüsselung für E-Mail-Clients aktivieren.
- E-Mail-Clients SOLLTEN E-Mails Ende-zu-Ende verschlüsseln
- Der Sensibilisierungsprozess SOLLTE Benutzende zur Überprüfung aktiver Inhalte vor der Aktivierung in Office-Anwendungen sensibilisieren.

Geschäftsprozesse im IT-Grundschutz

Motivation

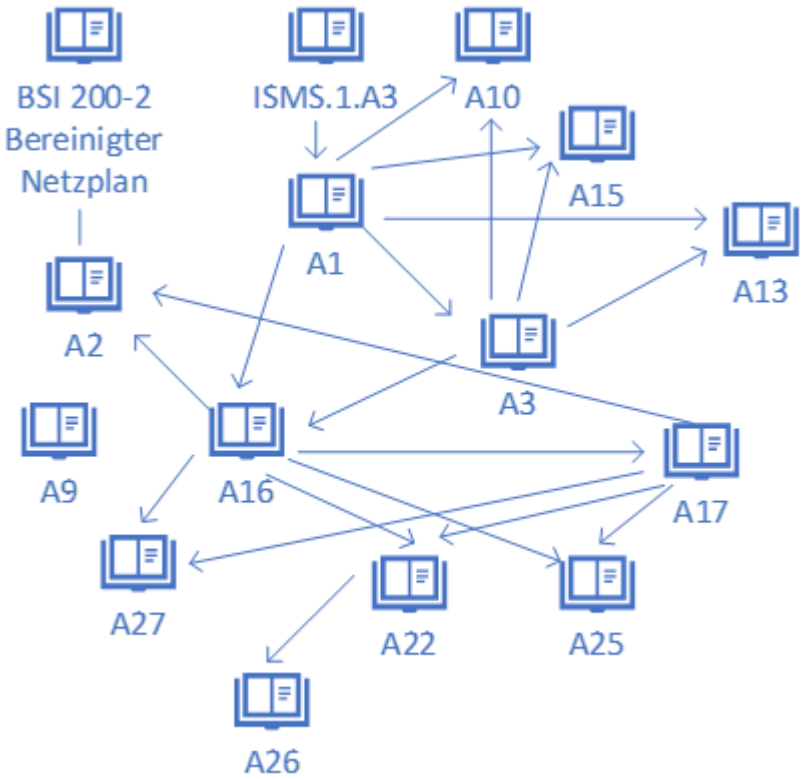
Hintergrund / Motivation

- Prozesse stellen den Kern eines ISMS dar
- Wie können Prozesse im IT-Grundschutz stärker in den Fokus gesetzt werden?
- Integration eines ISMS-Prozessmodells in den IT-Grundschutz

Dokumentation im IT-Grundschutz

Sachstand zur Optimierung der Dokumentationsaufwände im IT-Grundschutz

Beispiel Konsolidierung DA NET.1.1. für max. Transparenz und min. Aufwände



Beispiel, Ist-Situation Dokumentationsaufwände NET.1.1

Der Baustein NET.1.1 „Netzarchitektur und -design“ beinhaltet im IT-Grundschutz-Kompendium der Edition 2022 mindestens 13 Anforderungen, die Dokumentationsanforderungen explizit motivieren. Dies erschließt sich zum Teil direkt aus dem Titel der Anforderung, zum Teil aber auch erst aus deren Inhalt und den enthaltenen *Indikatoren* (so fordert A9 die *Festlegung* der als vertrauenswürdig geltenden Netze, A10 ein *Konzept* zur DMZ-Segmentierung, A15 die *Festlegung* von Personen, Prüfkriterien und Vorgaben).

1. NET.1.1.A1 Sicherheitsrichtlinie für das Netz [IT-Betrieb] (B)
   a. Setzt voraus: ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit [Institutionsleitung] (B)
2. NET.1.1.A2 Dokumentation des Netzes [IT-Betrieb] (B)
   a. Steht in Beziehung zu: Bereinigter Netzplan aus BSI 200-2
3. NET.1.1.A3 Anforderungsspezifikation für das Netz (B)
4. NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen (B)
5. NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet (B)
6. NET.1.1.A13 Netzplanung (B)
7. NET.1.1.A15 Regelmäßiger Soll-Ist-Vergleich (B)
8. NET.1.1.A16 Spezifikation der Netzarchitektur (S)
9. NET.1.1.A17 Spezifikation des Netzdesigns (S)
10. NET.1.1.A22 Spezifikation des Segmentierungskonzepts (S)
11. NET.1.1.A25 Fein- und Umsetzungsplanung von Netzarchitektur und -design (S)
12. NET.1.1.A26 Spezifikation von Betriebsprozessen für das Netz (S)
13. NET.1.1.A27 Einbindung der Netzarchitektur in die Notfallplanung [IT-Betrieb] (S)

Dokumentenpyramide der DA eines IV

Strategische(r) DA
- Aussagen zu Zielen, Umfeld, Leitgedanken & Rahmenwerken der Institution und ihres IV
- Z. B. in: Sicherheitsleitlinie, Cloud-Strategie, Notfall-Strategie, Dienstleister-Strategie

Taktische DA
- Konkretisierung strategischer DA in (Vorgabe-)Richtlinien für den IV (xy MUSS, SOLLTE, DARF NICHT …)
- Pro Thema: Geforderte primäre Eigenschaften auf Abstraktionsniveau der Bausteine, der ISO 27001/2
- Ideal: die IT-GS-Bausteine (nach Update!) sowie optionale IV-spezifische Anpassungen & Ergänzungen

Operative DA – Gestaltung (Thema)
- IV-spezifische Gestaltung der Themen taktischer DA in Konzepten und Umsetzungsr~~ichtlinien~~vorgaben
- Bsp.: Kryptokonzept, Notfallkonzept, Passwort~~richtlinie~~vorgaben, …

Operative DA – Vermittlung (Adressaten)
- IV-spezifische Vermittlung an die Adressaten der operativen DA (der Konzepte & Umsetzungsvorgaben)
- Bsp.: Arbeitsanweisungen, Prozessabläufe, Checklisten, Schulungsinhalte, KVP-Aktivitäten,…

Operative DA – Ergebnis
- (Notwendige) Ergebnisse gelebter strategischer, taktischer und operativer DA im IV
- Bsp.: Liste Zutrittsbefugter, Netzplan, FW-Konfiguration, Protokoll Revision (KVP), Bericht Korrekturmaßnahmen (KVP), Klimaprotokoll Serverraum, …

Hinweise
DA = Dokumentationsaufwand
IV = Informationsverbund
KVP = Kontinuierlicher Verbesserungsprozess

(1) Ein DA kann Inhalte enthalten, die sich mehr als einem Typ zuordnen lassen. Dies gilt insbesondere für operative DA, die sowohl Inhalte zu Gestaltung als auch zu Vermittlung und ggf. Ergebnissen enthalten können.

(2) Nur aus formalen Gründen werden keine DAs gefordert. Ein „Operativ-Ergebnis“ DA setzt z.B. nicht zwingend einen „Operativ-Vermittlung“ oder „Operativ-Gestaltung“ DA voraus.

Beispiel 1 Konsolidierung DA NET.1.1

<u>Statt 10+ nur 1 Operativ-Gestaltung DA zu NET.1.1</u>

Thematische Konsolidierung technischer DA-Anteile

- Segmentierung (A1, A5, A6, A10, A16, A19, A22, A23)
- Zonierung (A1, A4, A16)
- Kommunikationsbeziehungen (A1, A16)
- Protokolle (A1, A7, A16)
- Organisationsinterne und -übergreifende Vernetzung & Absicherung (Verschlüsselung) (A1, A7, A16, A17)
- Anbindung an nicht vertrauenswürdige Netze (A8, A9, A10, A11, A12, A16, A18)
- Administration (A17, A21)
- Netzkomponenten (A17)
- Anbindung von Endgeräten (A17, A20)

Thematische Konsolidierung organisatorischer DA-Anteile

- Erstellung, Bekanntgabe, Aktualisierung, Überprüfung des Anforderungsdokuments, sofern nicht bereits durch die Festlegungen zur Lenkung und dem Einsatz von Dokumenten abgedeckt (A1)
- Planung, Aufbau, Betrieb, Not-Betrieb, Aktualisierung, Außerbetriebnahme & Überprüfung von Netzanteilen (A13, A14, A15)

WiBA 2.0

Update zur neuen Version

Update zur Version 2.0

- Anpassung an **neue Version** des Profils „Basis-Absicherung Kommunalverwaltung“
- **67** relevante Bausteine in **19** Checklisten
  - Liste „Webserver und Webanwendungen“ jetzt „offiziell“
- **257** Prüffragen
  - Vorher **231**
  - Primär neue Fragen zu Serversystemen
    - Verzeichnisdienste, DNS-Server, ...
- Redaktionelle und inhaltliche Überarbeitung
- Liste zu weiterführenden Dokumenten
- Excel-Tool, Änderungsübersicht

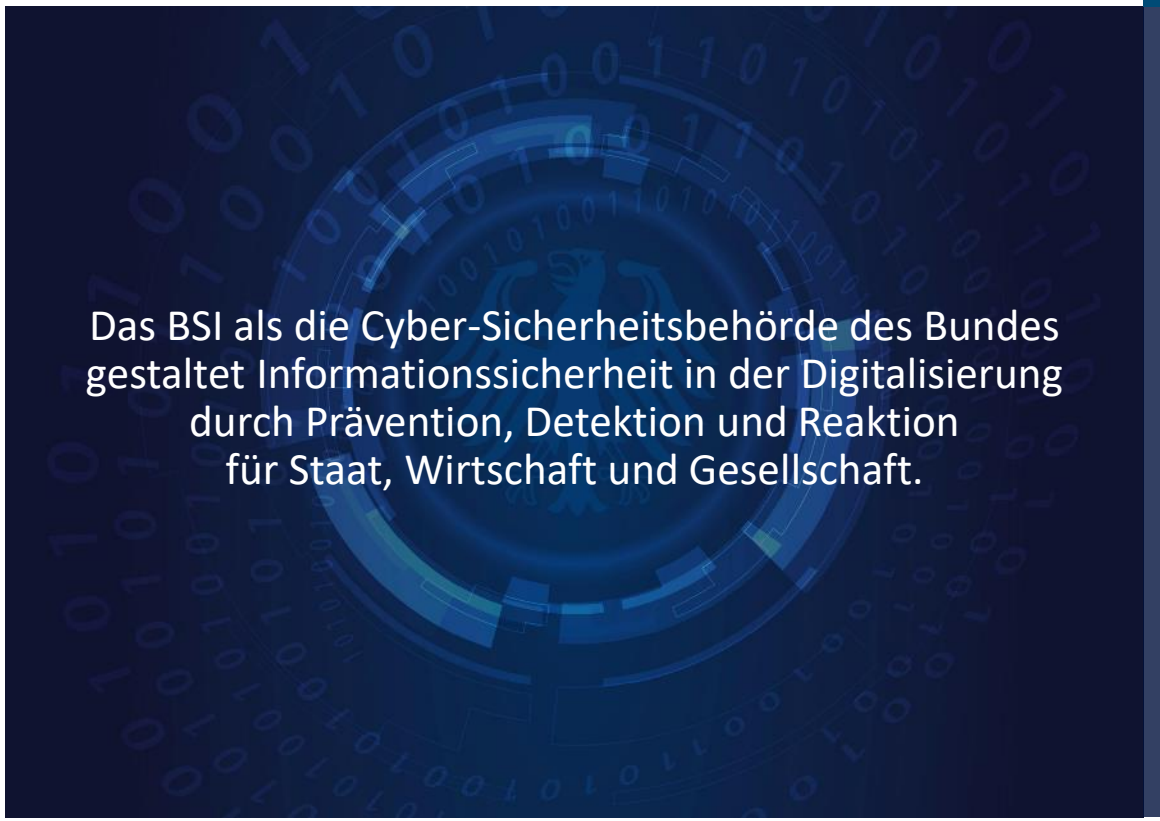
Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Florian Göhler
Referat „BSI-Standards und IT-Grundschutz“

it-grundschutz@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik