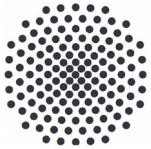


Universität Stuttgart
Stabsstelle Informationssicherheit

Der Schmerz bei der Beschaffung von Cloud-Dienstleistungen: Die Prüfung der technischen und organisatorischen Maßnahmen (TOM)

Standardisiertes Verfahren für die TOM-Prüfung bei der Beschaffung am Beispiel Cloud-Dienstleistungen

33. DFN-CERT Sicherheitskonferenz , 28.1.2026

Oliver Göbel

Universität Stuttgart
RUS-CERT
Stabsstelle Informationssicherheit

Um was geht es?

- Cloud-Dienste?
  - ➔ Nicht nur: Datenverarbeitung bei Dritten.
- Datenschutz (Stichwort “TOM”)?

  ➔ TOM für die Vearbeitung unserer Daten, egal ob mit oder ohne personenbezogene Daten.

  ➔ “TOM” Datenschutzsprech – passt aber auch auf Informationssicherheit.
- Überschneidung Informationssicherheit und Datenschutz groß

  ➔ Die meisten TOM für den Datenschutz sind TOM für die Informationssicherheit.

⇒ Es geht um Informationssicherheit, erweitert um exklusive Datenschutzanforderungen, sofern erforderlich.

UNIVERSITÄT STUTTGART
RUS-CERT
STABSSTELLE INFORMATIONSSICHERHEIT

- RUS-CERT wurde 1998 am **R**echenzentrum der **U**niversität **S**tuttgart gegründet.
- Seit 2001 Stabsstelle des Kanzlers/der Kanzlerin → Vermeidung von Interessenskonflikten mit CIO und IuK-Betreibern → Normkonformität
- Klassische CERT-Aufgaben: IR, VR, Threatmonitoring,...
- Zentrale Sicherheitsdienste: Firewall, Detektion, Scans...
- Technische Beratung von IuK-Betreibern der Constituency
- ISMS
- Beratung und Unterstützung bei Zertifizierungen – i.W. ISO/IEC 27001 und TISAX aber auch Vorgaben der EU usw.
- Gutachten

Gutachten...
Die Sache mit den TOM

- TOM-Prüfung für die Informationssicherheit, spätestens seit der ISMS-Pflicht (2017)
- TOM-Prüfung für AVV und VVT schon sehr viel länger Pflicht.
- Enge Zusammenarbeit mit DSB und DPO, TOM-Prüfungen gemeinsam durchgeführt.
- Allerdings: Es gab keinen standardisierten Prozess!
  ➔ Begleitung von Projekten mal schlecht, mal recht
- Seit 2024 hat unser DPO keine eigene technische Kompetenz
  ➔ Die TOM-Prüfung ist komplett zu uns gewandert.
- Immer mehr AVVs, weil jeder in die Cloud will oder seine Daten durch Dienstleister verarbeiten lassen will
  ➔ immer mehr TOM-Prüfungen

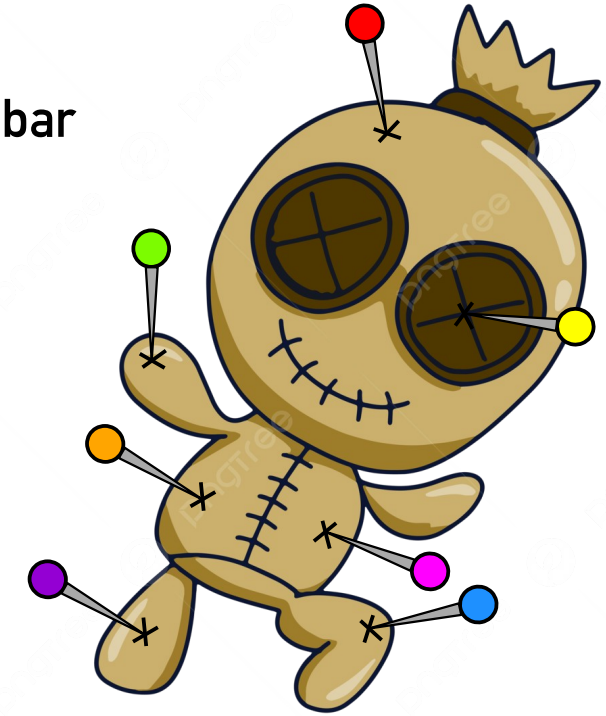
Ein Plan

- Da waren wir nun also: machtloser Spielball der Umstände und quälten uns durch die Gutachten.
- Was tun?

  ⇒ Probleme analysieren und Gegenmittel entwerfen

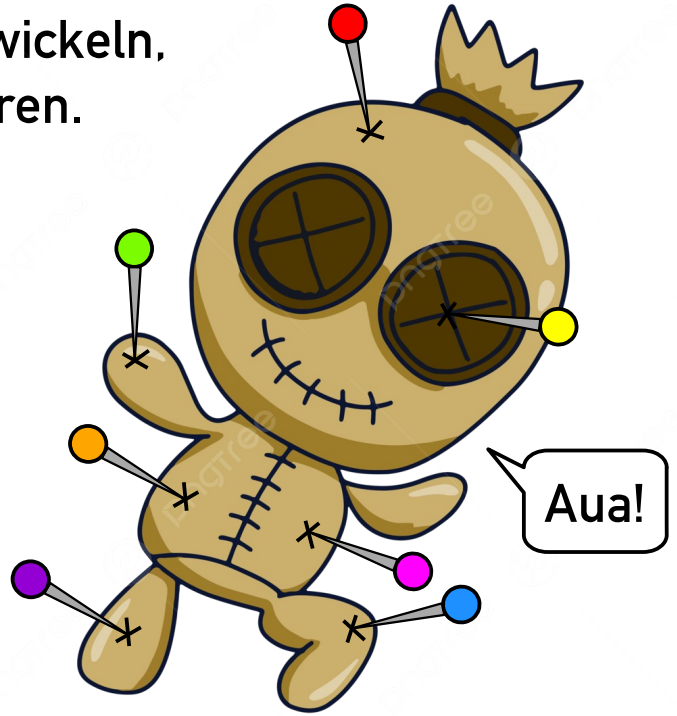
7 Schmerzen der TOM-Prüfung

1. Schmerz: Zu späte Einbindung
2. Schmerz: Dokumentation nicht vergleichbar
3. Schmerz: Prüfung der Umsetzung
4. Schmerz: Kein anerkanntes Verfahren
5. Schmerz: Alles zwei Mal prüfen?
6. Schmerz: Mangelnde Kooperation
7. Schmerz: Ängste und Bedenken



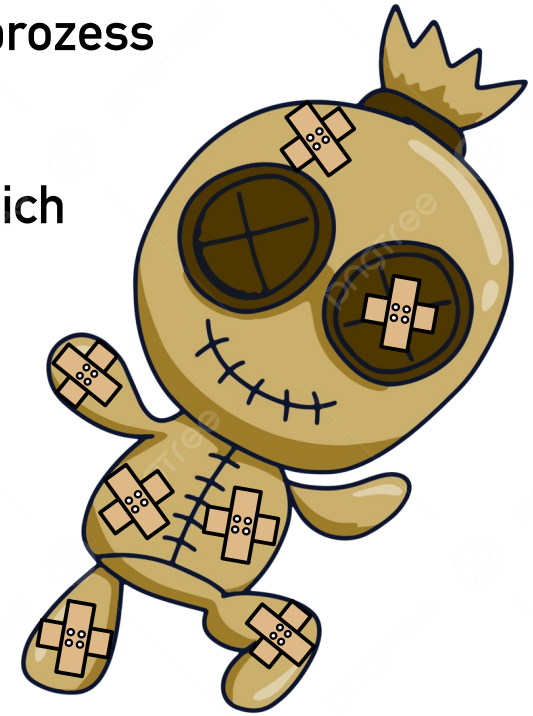
Gegenmittel

- Idee: ein standardisiertes Verfahren entwickeln, und in die Prozesse der Uni fest integrieren.
- Anforderungen an das Verfahren formulieren
- Das Verfahren anwenden und so seine Validität und Nützlichkeit nachweisen
- Das Verfahren dauernd verbessern und anpassen



7 Wünsche an ein Verfahren

1. Prüfung ausreichend früh im Beschaffungsprozess
2. Standardisierte Doku von allen Anbietern
3. Spieß umdrehen: Statt Umsetzung prüfen, sich die Erfüllung von Anforderungen rechtlich verbindlich vertraglich garantieren lassen
4. Orientierung an den Normen (ISO, BSI)
5. Ein Verfahren für Informationssicherheit und Datenschutz
6. Aufwand für Anbieter minimieren
7. Logik, Erfahrung, (positive) Rückmeldung durch Auftragnehmer



Weitere Wünsche

- Verfahren geeignet sowohl für Beschaffungen als auch Ausschreibungen
- Resultierende Dokumentation verwendbar als Vertragsanhang und im ISMS
- (An-)Bieter muss keine internen/geheimen Dokumente beilegen.
- Auswertung muss schnell gehen
- Ausschluss von für einen AVV nicht geeigneter Anbieter muss nachvollziehbar und gut begründet sein
- Mogeln durch Anbieter muss riskant sein!
- Zwei Teile: Dokumentation und Prozess
- Verfahren und Ergebnis muss verbindlich sein!

Umsetzung

- Entwicklung in Zusammenarbeit mit ZENDAS ➔ Datenschutzaspekte
- Implementiert als **Fragebogen**
- Satz **generischer**, **atomarer Anforderungen**, deren Erfüllung abgefragt wird
- **Attribuierung**: Festlegung von MUSS- und SOLLTE-Anforderungen
- **Ankreuzbar** ☒: „erfüllt“, „erfüllt ab“, „nicht erfüllt“, „nicht anwendbar“
- Jeweils ein **Freitextfeld** für die Begründung bei Nichtanwendbarkeit

  ➔ **Spieß umgedreht!**
- Jederzeitige **Audits** vorbehalten
- Teil der zentralen/dezentralen **Beschaffungsprozesse**
- Erste **Anwendungen**: TOM-Prüfung für die Beschaffung von Cloud- und Fernwartungs-Dienstleistungen
- **Derivate** - bislang: Checklisten für Backup- und Loggingkonzepte

Prozess

1) Fragebogen ist Teil der **Ausschreibungs- bzw. Beschaffungsunterlagen**

   → Gilt auch für **Direktvergaben** unter 20.000€!

   → Dient als Prüfung der **grundsätzlichen Geeignetheit** eines Anbieters

2) **Prüfung** des/der ausgefüllten Fragebogens/Fragebögen

   → Notwendige Voraussetzung zur Teilnahme des Anbieters an Auswahl: Alle MUSS-Anforderungen müssen *"erfüllt"*, begründet und akzeptabel *"erfüllt ab"* oder *"nicht anwendbar"* angekreuzt sein
   ⇒ **Identifikation geeigneter Anbieter**

   → **Rangfolge** nach Erfüllungsgrad der SOLLTE-Anforderungen möglich

   → Prüfung und entsprechende Auswahl **vor Zuschlagserteilung!**

3) Ausgefülltes Formular bei Zuschlagserteilung **verbindlich**!

   → Entsprechender Eintrag, z. B. im EVB-IT Cloudvertrag, Ziffer 9 „Sonstige Vereinbarungen"

Themengebiete

- Die Anforderungen sind derzeit in folgenden Themengebieten gruppiert:
  - → Allgemeine Anforderungen
  - → Personal
  - → Dokumentation
  - → Schutz der Verfügbarkeit
  - → Zutritt zur Infrastruktur
  - → Zugang zur Infrastruktur
  - → Authentifizierung
  - → Zugriff auf die Infrastruktur
  - → Mobile Geräte
  - → Verschlüsselung
  - → Datenträger
  - → Vorfallsbehandlung
  - → Protokollierung (Logging)
  - → Datensicherung (Backup)
  - → Risiken der Lieferkette
  - → Risiken durch Unterauftragnehmer
  - → Datenschutz expizit

UNIVERSITÄT STUTTGART RUS CERT STABSSTELLE INFORMATIONSSICHERHEIT

ZENDAS
Zentrale Datenschutzstelle der baden-württembergischen Universitäten

Anforderungen an die Informationssicherheit und den Datenschutz

bei der Erbringung von Clouddienstleistungen für die ausschreibende/auftraggebende Stelle

Ausschreibende/auftraggebende Stelle (AG):

Universität Stuttgart, Institut für Wolkiges (IfW)

Anbietende/auftragnehmende Stelle (AN):

Firma Superfluffy Cloud-Dienste GmbH&Co KG

Bezeichnung der Ausschreibung/des Dienstes:

Clouddienst für Wolkenverwaltung

Version der Vorlage: CT-20240805

Dokumentstatus: ENTWURF

TLP:AMBER STRICT (AG und AN)

Dieses Dokument beschreibt die Anforderungen der AG an den von der AN zu erbringenden Dienst aus Sicht der Informationssicherheit und des Datenschutzes, insbesondere an die vorgehaltene und betriebene Infrastruktur sowie die Prozesse und Verfahren, die für die zu implementierende Cloud-Lösung der AG verwendet werden.

Autoren:

Oliver Göbel, CISO der Universität Stuttgart, ZENDAS

[1] Zur internen Statusverfolgung bei der AN. Bitte auf „FINAL" ändern, sobald es an die AG geschickt wird. Sollte Klärungsbedarf bestehen, kann es als „ENTWURF" an die AG geschickt werden, um Fragen per Telefon oder Videokonferenz zu klären, sofern zulässig. ACHTUNG: Zur Auswertung seitens der AG, z.B. im Rahmen von Ausschreibungen können nur Dokumente im Status „FINAL" akzeptiert werden!

[2] Diese Weitergaberegelung (TLP) gilt ab dem Zeitpunkt, ab dem dieses Dokument ausgefüllt wurde und dadurch ggf. vertrauliche Daten enthält. Die Weitergabe des ausgefüllten Dokuments ist geregelt durch das Traffic Light Protocol https://de.wikipedia.org/wiki/Traffic_Light_Protocol

UNIVERSITÄT STUTTGART RUS CERT STABSSTELLE INFORMATIONSSICHERHEIT

ZENDAS
Zentrale Datenschutzstelle der baden-württembergischen Universitäten

4. Auf ortsfesten Geräten, die für die Diensterbringung eingesetzt werden (Arbeitsplatzgeräte, Server usw.), die der Zutrittskontrolle unterliegen (siehe Abschnitt 3.1.5) SOLLTE der **nichtflüchtige Speicher** (Festplatte) **verschlüsselt** sein.

   ☒ Erfüllt ☐ Erfüllt ab 01.01.2024 ☐ Nicht erfüllt ☐ Nicht anwendbar

   Anmerkungen zur Erfüllung der Anforderung können hier eingetragen werden.

3.1.12 Datenträger – Handhabung, Entsorgung, Transport

Mobile und feste Datenträger können schutzbedürftige Daten enthalten. Der Zutritt zu ihnen während und nach Ende ihrer Nutzung und beim Transport muss daher geregelt werden. Die AN hat hierfür ein **Konzept** umgesetzt, das folgende Anforderungen erfüllt:

Anforderungen

1. Der **Zutritt** zu Datenträgern MUSS mindestens die Anforderungen des Zutrittskonzepts (3.1.5) erfüllen.

   ☒ Erfüllt ☐ Erfüllt ab 01.01.2024 ☐ Nicht erfüllt ☐ Nicht anwendbar

   Bitte begründen Sie, **warum** diese Anforderung **nicht erfüllt** oder **nicht anwendbar** ist. Anmerkungen zur Erfüllung der Anforderung können ebenfalls eingetragen werden.

2. Mobile Datenträger (z.B. USB-Devices) MÜSSEN mindestens beim **Transport** außerhalb der Geschäftsräume der AN gemäß des Verschlüsselungskonzepts (3.1.11) kryptographisch stark verschlüsselt sein.

   ☒ Erfüllt ☐ Erfüllt ab 01.01.2024 ☐ Nicht erfüllt ☐ Nicht anwendbar

   Bitte begründen Sie, **warum** diese Anforderung **nicht erfüllt** oder **nicht anwendbar** ist. Anmerkungen zur Erfüllung der Anforderung können ebenfalls eingetragen werden.

3. Für neue Zwecke verwendete Datenträger MÜSSEN vor der Neuverwendung sicher **gelöscht**[14] werden.

   ☐ Erfüllt ☐ Erfüllt ab 01.01.2024 ☐ Nicht erfüllt ☒ Nicht anwendbar

   Bitte begründen Sie, **warum** diese Anforderung **nicht erfüllt** oder **nicht anwendbar** ist. Anmerkungen zur Erfüllung der Anforderung können ebenfalls eingetragen werden.

   Datenträger werden nur einmal verwendet und dann vernichtet.

4. Außer Betrieb genommene Datenträger MÜSSEN sicher **vernichtet** werden, entweder durch eine beauftragte Fachfirma oder durch physische Zerstörung. Dies gilt auch für Datenträger, die nicht mehr lesbar sind. Datenträger, die z.B. im Rahmen von Garantiefällen ausgetauscht werden, müssen vor Rücksendung zur Verkäuferin bzw. zum Verkäufer datenschutzgerecht gelöscht werden. Kann die Löschung nicht

[14] Bundesamt für Sicherheit in der Informationstechnik: „Daten endgültig Löschen", https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html, BSI Grundschutzkompendium Maßnahme CON.6 „Löschen und Vernichten": https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2021.pdf?__blob=publicationFile&v=2

Vielen Dank!

Haben Sie Fragen?

goebel@cert.uni-stuttgart.de

0711/685 8 3678 (O. Göbel)

https://cert.uni-stuttgart.de/