DSGVO IT SICHERHEITSDOKUMENTE MIT VERINICE VERWALTEN

hagen.bauer@rusticus-consulting.de

rusticus consulting
IT | BODENSTÄNDIG & INNOVATIV

ÜBER MICH

- Hagen Bauer
- IT Berater (Software / Infrastruktur)
- Datenschutzfreak
- Freifunker
- Serveradministrator
- Jekyll Webseiten
- Web Shop Administrator

DISCLAIMER:

DIESE INFORMATIONEN SOLLEN NUR HELFEN DAS RICHTIGE ZU TUN.

SIE ERSETZEN KEINE RECHTSBERATUNG UND ERHEBEN KEINEN ANSPRUCH AUF VOLLSTÄNDIGKEIT UND/ODER RICHTIGKEIT.

DIE DATENSCHUTZGRUNDVERORDNUNG

- 2016 durch EU festgelegt
- ersetzt die Datenschutzrichtlinie aus dem Jahr 1995
- ist in der gesamten EU als Gesetz anerkannt
- Mitgliedstaaten mussten bis Mai 2018 Umsetzung sicherstellen

NEUE ANFORDERUNGEN

- neue Datenschutzerklärung auf Webseiten notwendig
- Vertrag zur Auftragsverarbeitung für externe Dienstleister
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutzbeauftragter bei besonders geschützten Daten
- Weitere Rechte des Verbrauchers (Auskunft, Löschung, Übertragung…)
- Meldepflicht von Vorfällen

UND DAS IST AUCH RICHTIG SO

NORDRHEIN-WESTFALEN

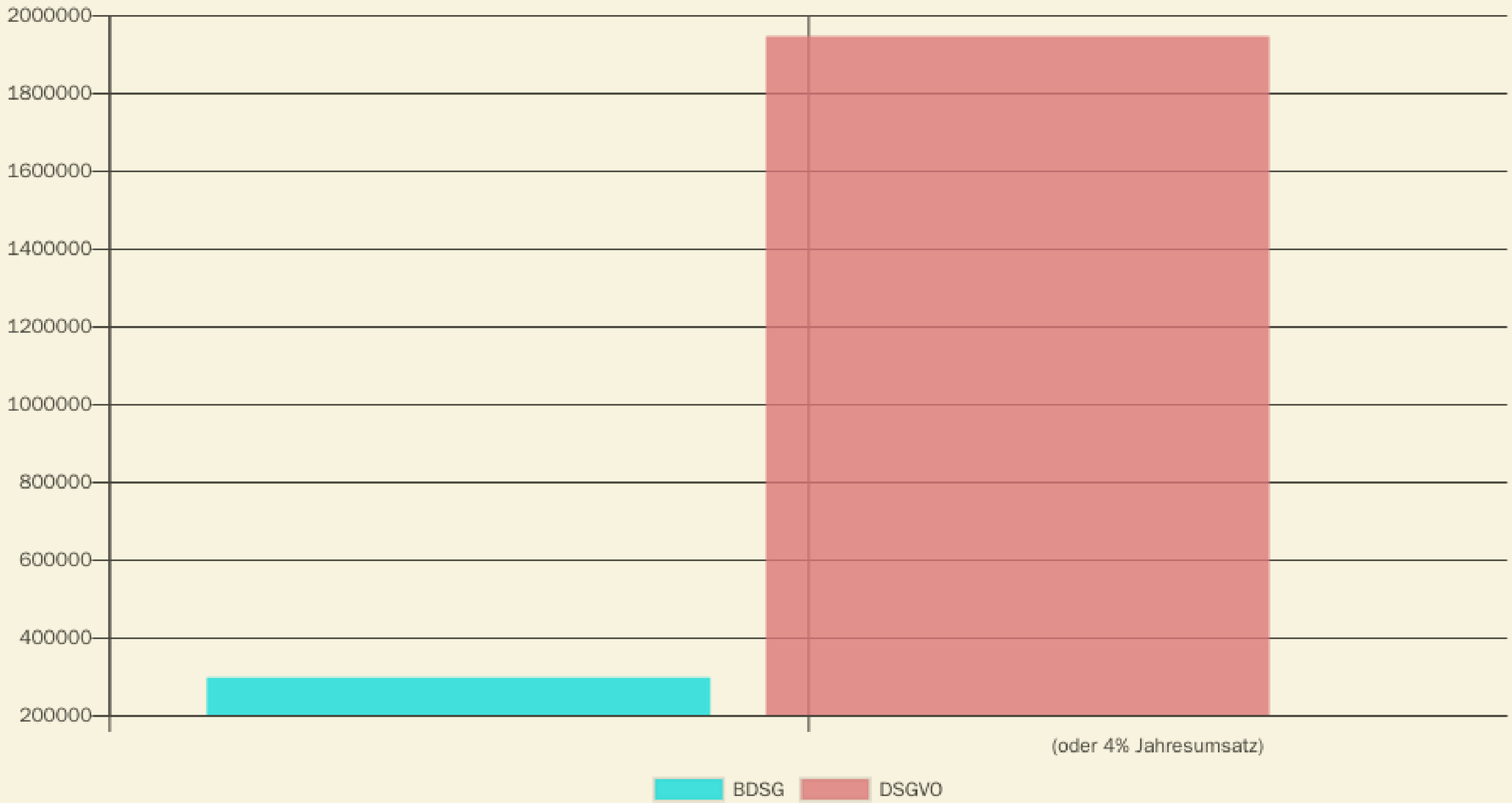
NORDRHEIN-WESTFALEN JVA EUSKIRCHEN

Häftling findet Stick mit sensiblen JVA-Mitarbeiter-Daten

Ein Gefängnis-Mitarbeiter verliert einen USB-Stick – ausgerechnet mit sensiblen Daten vieler JVA-Bediensteter. Ein Häftling findet ihn – und will ihn wieder verloren haben. Wo sich der Stick derzeit befindet, sei unklar.

Ein verlorener USB-Stick mit sensiblen persönlichen Daten von rund 80 Vollzugsbeamten des Gefängnisses Euskirchen ist ausgerechnet in die Hand eines Häftlings gelangt. „Der Stick ist gefunden worden, von einem

DATENSCHUTZ MIT ZÄHNEN



UND NICHT NUR IN DER THEORIE


IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal

heise online 〉News 〉10/2018 〉**DSGVO-Verstoß: Krankenhaus in Portugal soll 400.000 Euro zahlen**

23.10.2018 11:06 Uhr

DSGVO-Verstoß: Krankenhaus in Portugal soll 400.000 Euro zahlen

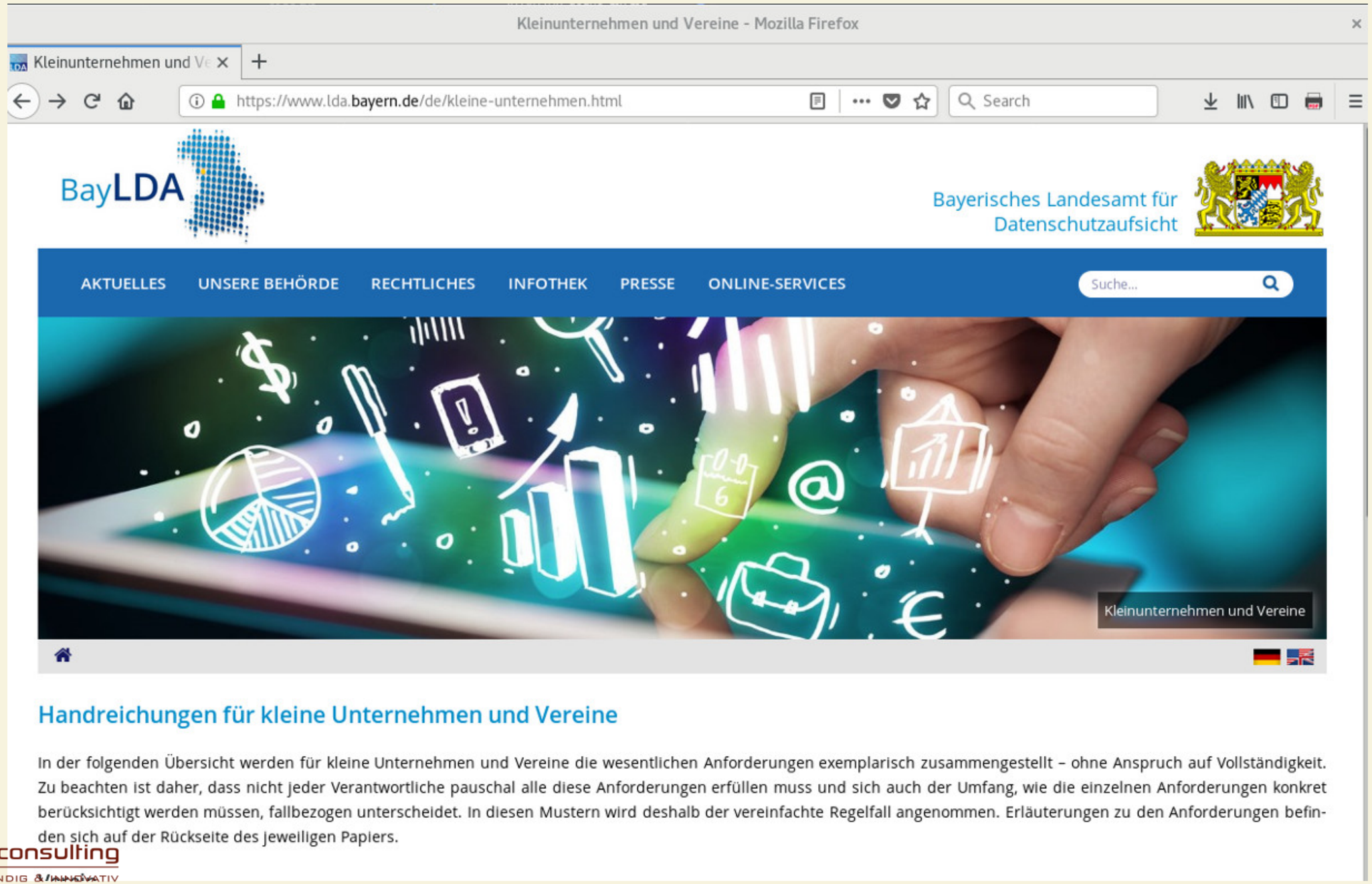
In einem Krankenhaus in Portugal hatten nicht nur Ärzte Zugriff auf Patientendaten. Dafür wurde nun eine empfindliche Geldstrafe verhängt.

- z.B. 985 aktive Benutzer mit einem Profil "Arzt" bei 296 Ärzten

VEREINFACHTE TODO LISTE

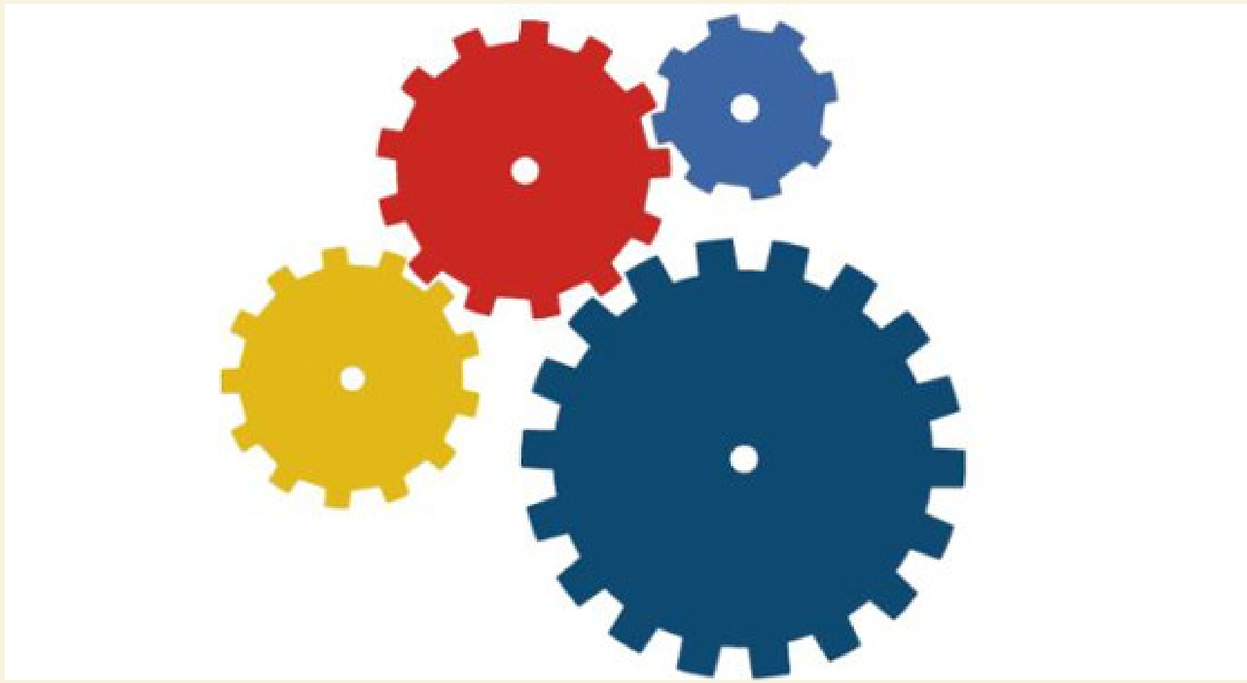
Tätigkeit	Prio	Aufw.
Datenschutzerklärung/Cookie Banner / Social Media	1	N
Datenschutzbeauftragter?	1	N
Verzeichnis von Verarbeitungstätigkeiten	2	H
Prozess für Auskunft/Löschen	2	M
Basis IT Sicherheitskonzept	2	M
Datenschutzfolgeabschätzung	3	H

GUTE HILFESTELLUNGEN AUS BAYERN



PFLICHT: IT SICHERHEITSKONZEPTION

- z.Z. Keine "handhabbaren" Standards
- Stand der Technik???
- BSI IT Grundschutz bietet eine systematische Herangehensweise
- Pragmatische Auslegung möglich



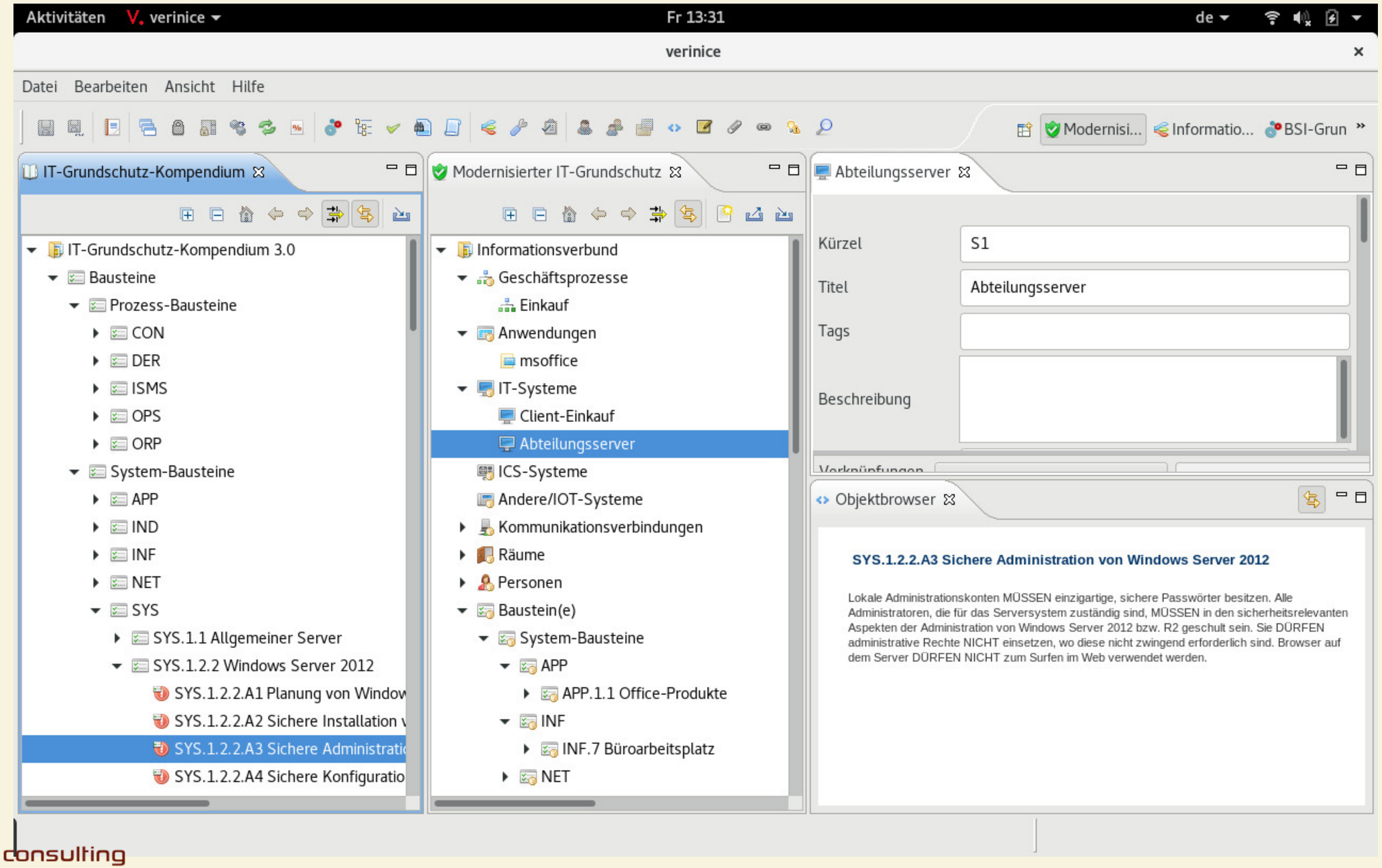
DIE IDEE HINTER DEM BSI GRUNDSCHUTZ

- Wiederverwendbarkeit, Anpassbarkeit, Erweiterbarkeit
- Benennung der typischen
  - Gefährdungen, Schwachstellen und Risiken
  - Geschäftsprozesse und Anwendungen
  - IT-Komponenten
- Empfehlungen und Maßnahmen werden bereitgestellt
- Quelle / ITGrundschutzkompendium

VORGEHENSWEISE

1. IT-Sicherheitsprozess starten
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung nach IT-Grundschutz
5. Basis-Sicherheitsscheck
6. Realisierung von Sicherheitsmaßnahmen
7. Kontinuierliche Verbesserung

GRUNDSCHUTZ MIT VERINICE



VERINICE

- Open Source Information Security Management System (ISMS)
- GNU General Public License
- Windows, Linux and OS X
- Demo und Kaufversion auf Hersteller Webseite
- Einzelplatz und Serverversion vefügbar
- Quellcode auf https://github.com/SerNet/verinice

DEMO

OFFENE PUNKTE

- Holistische Abdeckung DSGVO Anforderungen erfordert Zusatzmodul oder Eigenentwicklung
- Installation und Einrichtung OpenSource Version ist "hackelig"

ERGEBNISS: EIN BESSERER SCHUTZ DER DATEN MEINER ORGANISATION UND MEINER KUNDEN


rusticus consulting

DSGVO IT SICHERHEITSDOKUMENTE MIT VERINICE VERWALTEN

hagen.bauer@rusticus-consulting.de

rusticus consulting
IT | BODENSTÄNDIG & INNOVATIV