DIE DSGVO ALS CHANCE NUTZEN

MONITORING DER INFORMATIONSSICHERHEIT

hagen.bauer@rusticus-consulting.de

ÜBER MICH

- Hagen Bauer
- Freiberuflicher IT Berater
- Datenschutzfreak
- Freifunker
- Serveradministrator
- Web Shop Betreiber

DISCLAIMER:

DIESE INFORMATIONEN SOLLEN NUR HELFEN DAS RICHTIGE ZU TUN.

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

AGENDA

- Informationssicherheit ist finanziell bewertbar
- Ein Fahrplan wird bereitgestellt
- Informationssicherheit bedarf einer ständigen Überwachung
- Aufrechterhaltung der Informationssicherheit ist ein neues geschäftsrelevantes Aufgabenfeld für Monitoring

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

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

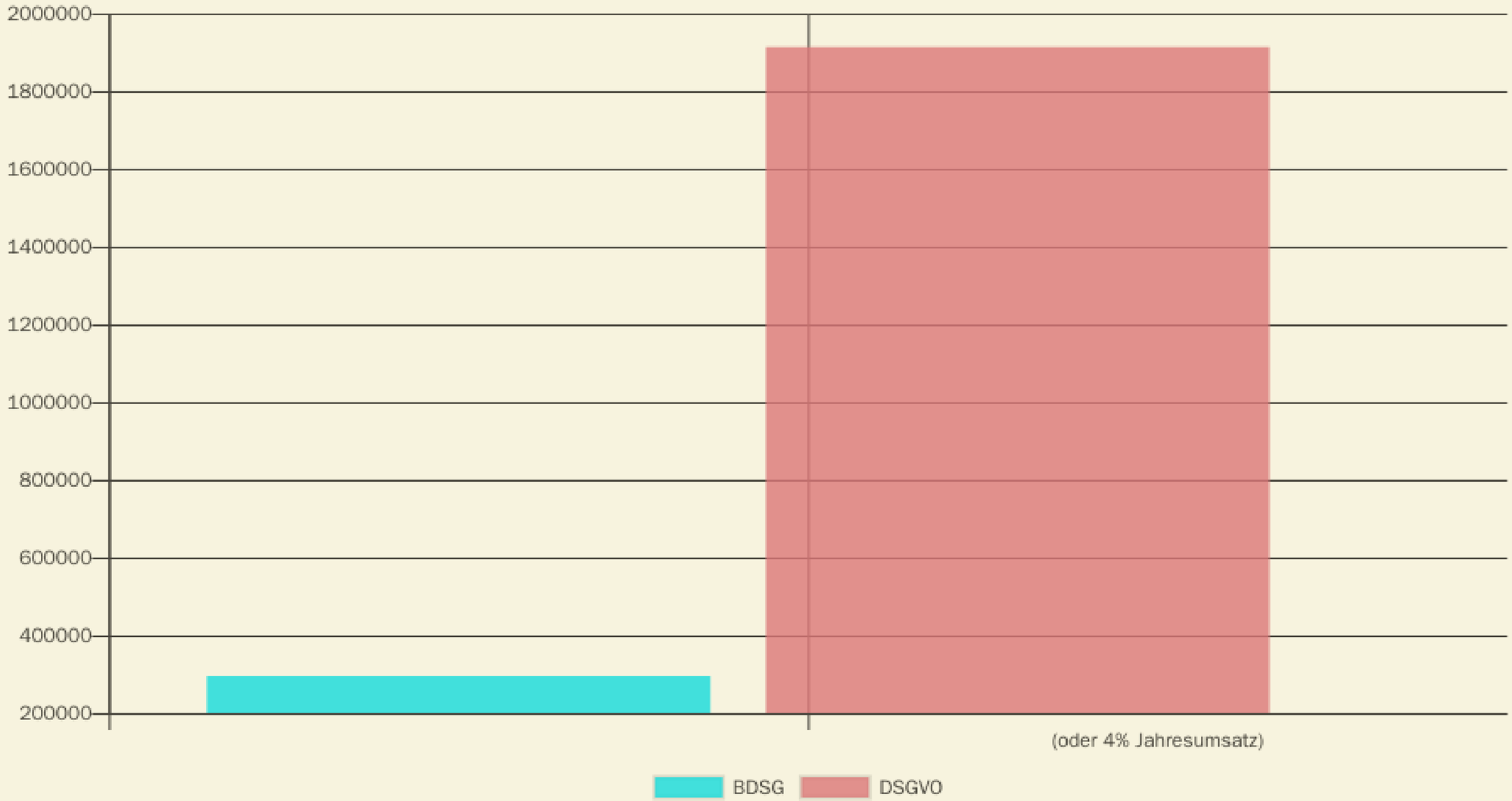
AKTUELLER STAND IST ERSCHÜTTERND

30% TEILWEISE ODER

GAR NICHT

- TÜV Süd Mai 2019

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

UND NICHT NUR IN DER THEORIE

agencia española protección datos

936-150719

Procedimiento Nº: PS/00300/2019

RESOLUCIÓN R/00499/2019 DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

En el procedimiento sancionador PS/00300/2019, instruido por la Agencia Española de Protección de Datos a ***VUELING AIRLINES, S.L.***, vista la denuncia presentada por ***A.A.A.***, y en base a los siguientes,

ANTECEDENTES

- Bußgeld über 30.000 Euro wegen Cookie-Banner

UND NICHT NUR IN DER THEORIE

BBC | Sign in | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Technology

UK watchdog plans to fine Marriott £99m

9 July 2019 Share

The UK's data privacy regulator has said it plans to fine the US hotel group Marriott International £99.2m.

The **penalty relates to a data breach** that resulted in about 339 million guests having had their personal details exposed.

The incident is thought to date back to 2014 but was only discovered in 2018.

It comes a day after the Information Commissioner's Office (ICO) said it **planned to fine British Airways £183m** over a separate breach.

TYPISCHE VERDRÄNGUNGSSTRATEGIEN

"DAS IST MIR EGAL.
ICH VERKAUFE EH IN 5 JAHREN"

GARTNER:

CYBERSECURITY IS CRITICAL TO THE M&A DUE DILIGENCE PROCESS

UND NICHT NUR IN DER THEORIE

BBC | Sign in | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Technology

UK watchdog plans to fine Marriott £99m

9 July 2019 Share

The UK's data privacy regulator has said it plans to fine the US hotel group Marriott International £99.2m.

The **penalty relates to a data breach** that resulted in about 339 million guests having had their personal details exposed.

The incident is thought to date back to 2014 but was only discovered in 2018.

It comes a day after the Information Commissioner's Office (ICO) said it **planned to fine British Airways £183m** over a separate breach.

ABER ICH WERDE SCHON NICHT GEHACKT

AKTUELLE HITLISTE

1. Postfehlversand
2. Hackingangriffe/Malware/Trojaner
3. E-Mail Fehlversand
4. Diebstahl eines Datenträgers
5. Versendung einer E-Mail mit offenem Adressverteiler
6. Verlust eines Datenträgers
7. Fax-Fehlversand
8. Quelle LfDI July 2019

ICH BIN KLEIN, WIRD SCHON NICHT SO TEUER WERDEN.

KOSTEN EINES VORFALLS?

- "Cost-of-a-Data-Breach“-Studie IBM
- Unternehmen mit weniger als 500 Mitarbeitern

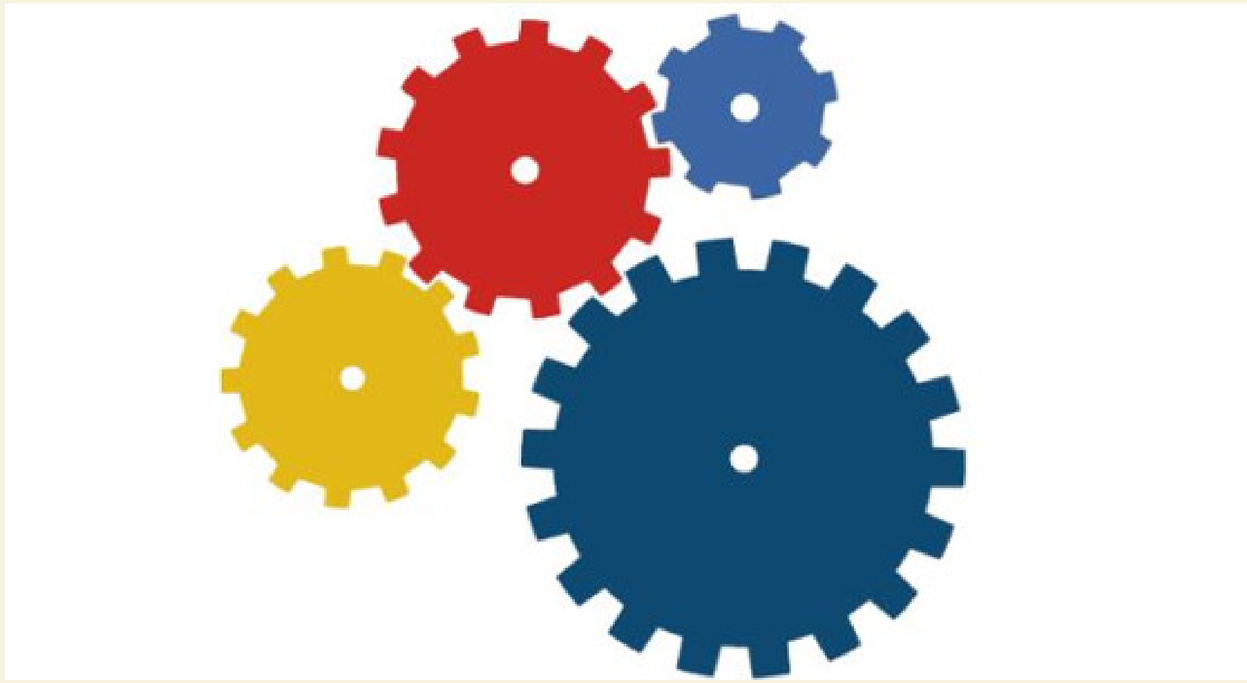
2,2 MIO. EURO PRO VORFALL

FEHLENDE INFORMATIONSICHERHEIT BEDEUTET

- steigendes Risiko für empfindliche Strafen
- sinkende Unternehmenswerte
- steigende Versicherungskosten
- Risiken beim Kauf/Verkauf von Unternehmen oder Sparten

LÖSUNGSANSATZ: IT SICHERHEITSKONZEPTION

- BSI IT Grundschutz bietet eine systematische Herangehensweise
- Pragmatische Auslegung möglich



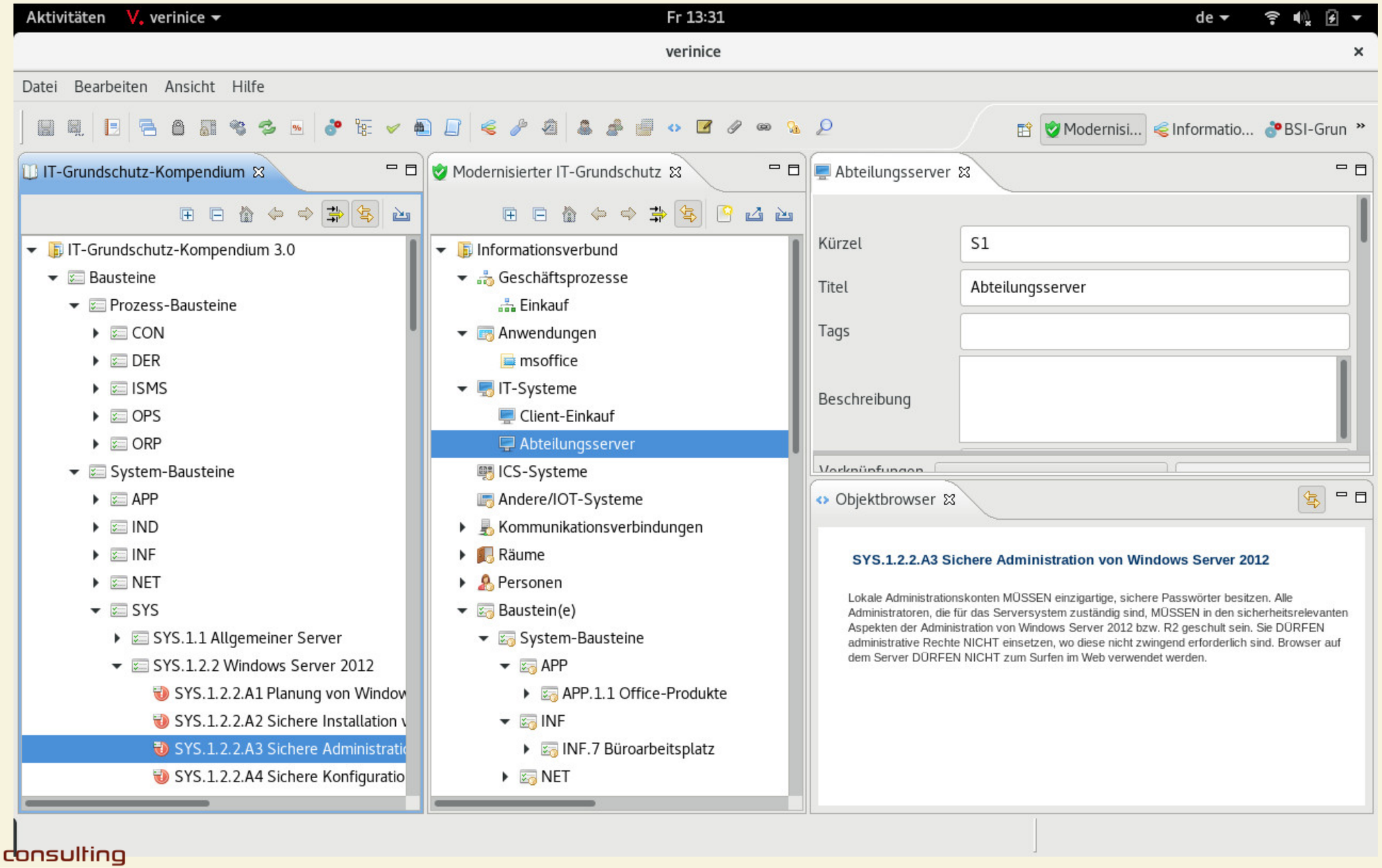
DIE IDEE HINTER DEM BSI GRUNDSCHUTZ

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

VORGEHENSWEISE

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

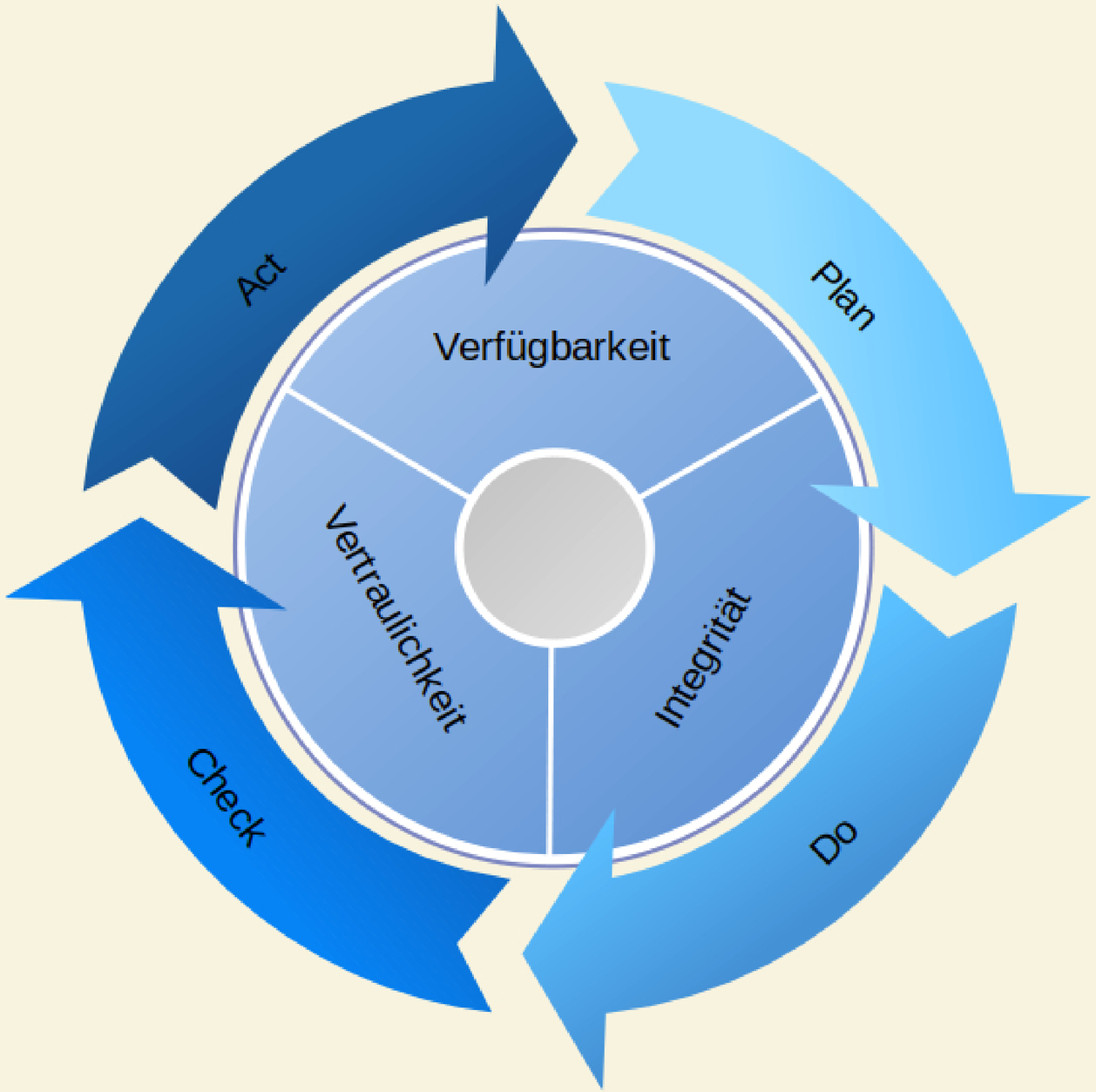
GRUNDSCHUTZ MIT VERINICE



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

GRUNDPRINZIPIEN



DSGVO RELEVANTES MONITORING

- Geschäftsprozesse überwachen
- Verfügbarkeit der Anwendungen
- Infrastruktur Monitoring
- Verifikation Backups
- Anomalien in den Produktionsanlagen
- Fehlerhafte Anmeldeversuche
- Alarmierung
- Ergebnisse Security Scanner
- Software Installationsstatus
- Aktualität Virenscanner

DSGVO RELEVANTES MONITORING

- Berichte über durchgeführte Schulungen
- Aktualität von Dokumentationen
  - Kontrolle Clean Desk
  - Schlüsselverzeichnis
- Alarmierung
- Durchgeführte Phishing Testläufe
- Meldung von Sicherheitsvorfällen

HR - IT Security Dashboard

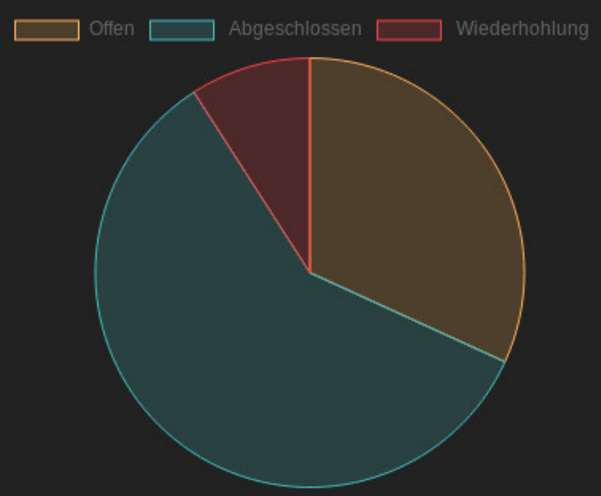
Upcoming Events

Clean Desk	12.11.
Feuer Alarm	04.12.
Phishing Mail	12.12.

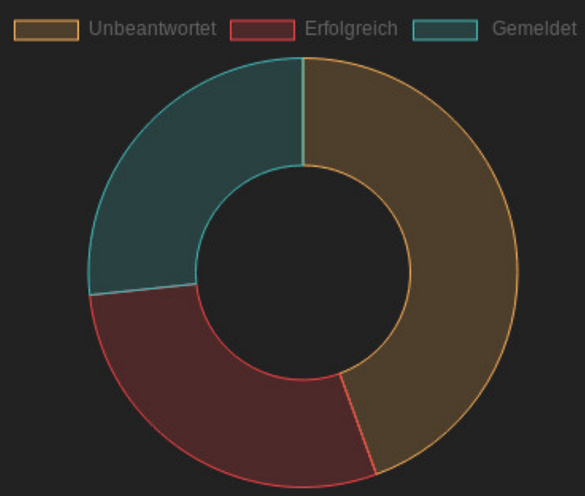
Last updated at 10:51

Security Incidents

Sicherheitsunterweisung 2019



Phishing Mail Übungen



ZUSAMMENFASSUNG

- Informationssicherheit ist finanziell bewertbar
- Ein Fahrplan wird bereitgestellt
- Monitoring ist der Schlüssel zur Aufrechterhaltung der Informationssicherheit
- Aufrechterhaltung der Informationssicherheit ist ein neues geschäftsrelevantes Aufgabenfeld für Monitoring

DIE DSGVO ALS CHANCE NUTZEN

MONITORING DER INFORMATIONSSICHERHEIT

hagen.bauer@rusticus-consulting.de