

# DIE DSGVO ALS CHANCE NUTZEN

---

## MONITORING DER INFORMATIONSSICHERHEIT

[hagen.bauer@rusticus-consulting.de](mailto: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

The screenshot shows the top navigation bar of the 'welt' website. The logo 'welt' is on the left. On the right, there are links for 'Abonnement', 'Ticker' (with a notification icon), 'Suche', and 'Login'. Below the navigation bar is a menu with categories: HOME, WELTPLUS, LIVE-TV, MEDIATHEK, POLITIK, WIRTSCHAFT, SPORT, PANORAMA, WISSEN, KULTUR, M, MEHR >, and PRODUKTE. The breadcrumb trail reads: HOME » REGIONALES » NORDRHEIN-WESTFALEN » Häftling findet in JVA Euskirchen Stick mit sensiblen Daten. The main heading is 'NORDRHEIN-WESTFALEN' with sub-links for 'POLITIK IN NRW', 'WETTER IN NRW', and 'STELLENANGEBOTE'. The article title is 'Häftling findet Stick mit sensiblen JVA-Mitarbeiter-Daten'. The sub-headers are 'NORDRHEIN-WESTFALEN' and 'JVA EUSKIRCHEN'. The text of the article begins with: '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.' Below the text, there is a large letter 'E' followed by the text: 'in 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'. On the left side of the article, there is a small number '3' and a Facebook icon.

welt

Abonnement Ticker Suche Login

HOME WELTPLUS LIVE-TV MEDIATHEK POLITIK WIRTSCHAFT SPORT PANORAMA WISSEN KULTUR M MEHR > PRODUKTE

HOME » REGIONALES » NORDRHEIN-WESTFALEN » Häftling findet in JVA Euskirchen Stick mit sensiblen Daten

## NORDRHEIN-WESTFALEN

POLITIK IN NRW WETTER IN NRW STELLENANGEBOTE

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.

3

**E** in 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

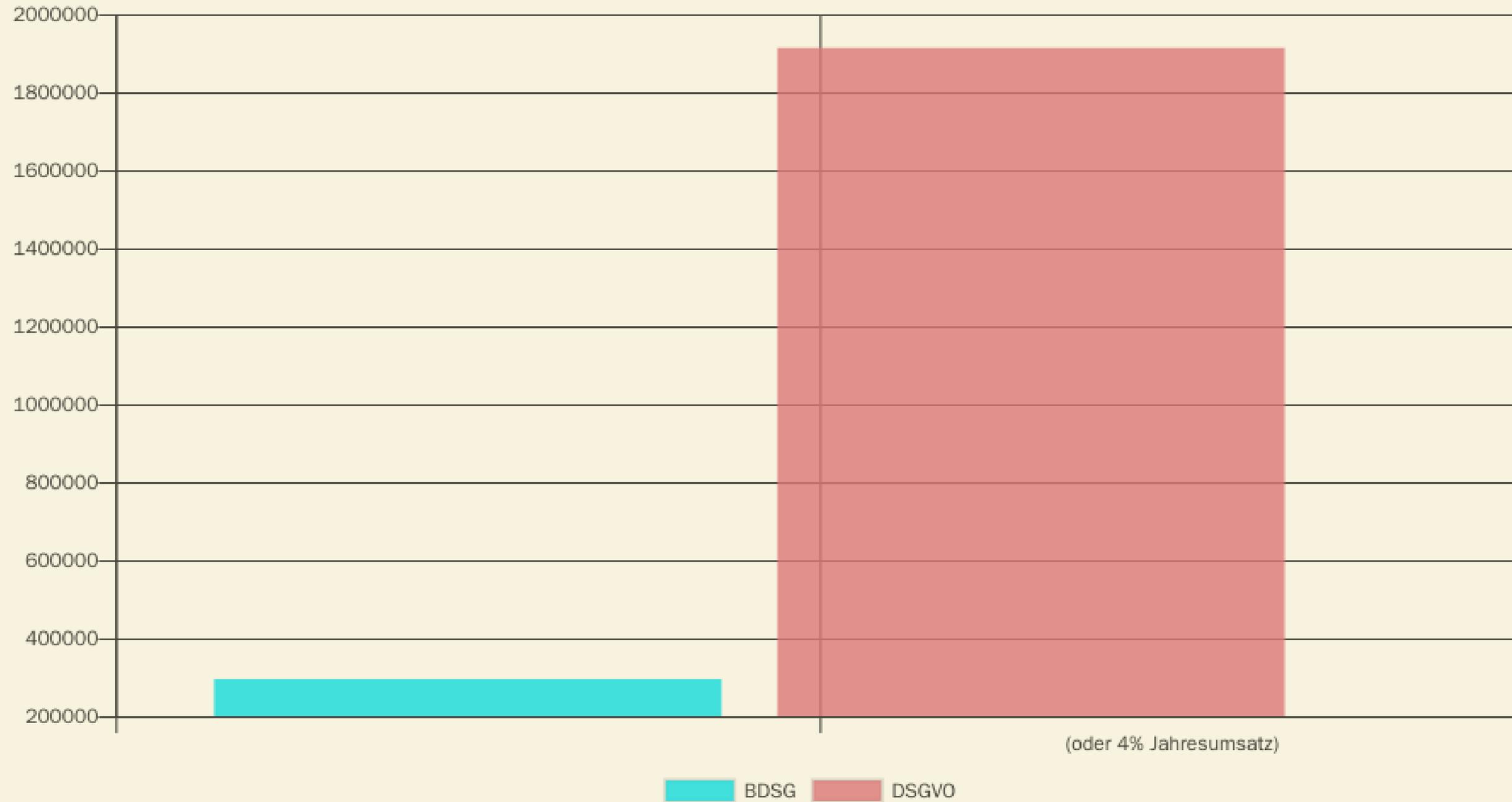
**AKTUELLER STAND IST ERSCHÜTTERND**

**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



1/7

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



The image is a screenshot of a BBC News article. At the top, the BBC logo is on the left, and navigation links for 'Sign in', 'News', 'Sport', 'Reel', 'Worklife', 'Travel', and 'Future' are on the right. Below this is a red banner with the word 'NEWS' in white. Underneath the banner is another row of navigation links: 'Home', 'Video', 'World', 'UK', 'Business', 'Tech', 'Science', 'Stories', and 'Entertainment & Arts'. The article is categorized under 'Technology'. The main headline reads 'UK watchdog plans to fine Marriott £99m'. Below the headline is the date '9 July 2019' and a row of social media sharing icons for Facebook, Messenger, Twitter, Email, and a general 'Share' button. The article text begins with 'The UK's data privacy regulator has said it plans to fine the US hotel group Marriott International £99.2m.' It then explains that the penalty relates to a data breach that exposed the personal details of about 339 million guests. The incident is noted to date back to 2014 but was only discovered in 2018. Finally, it mentions that this comes a day after the Information Commissioner's Office (ICO) planned to fine British Airways £183m over a separate breach.

**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

f Messenger Twitter Email 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



The image is a screenshot of a BBC News article. At the top, the BBC logo is on the left, and navigation links for 'Sign in', 'News', 'Sport', 'Reel', 'Worklife', 'Travel', and 'Future' are on the right. Below this is a red header with the word 'NEWS' in white. Underneath the header is a secondary navigation bar with links for 'Home', 'Video', 'World', 'UK', 'Business', 'Tech', 'Science', 'Stories', and 'Entertainment & Arts'. The article is categorized under 'Technology'. The main headline reads 'UK watchdog plans to fine Marriott £99m'. Below the headline is the date '9 July 2019' and a row of social media sharing icons: Facebook, WhatsApp, Twitter, Email, and a general 'Share' button. The article text begins with 'The UK's data privacy regulator has said it plans to fine the US hotel group Marriott International £99.2m.' It then explains that the penalty relates to a data breach that exposed the personal details of about 339 million guests. The incident is noted to have occurred in 2014 but was only discovered in 2018. Finally, it mentions that this fine comes a day after the Information Commissioner's Office (ICO) planned to fine British Airways £183m over a separate breach.

**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

f WhatsApp Twitter Email 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 INFORMATIONSSICHERHEIT 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-Sicherheitscheck
6. Realisierung von Sicherheitsmaßnahmen
7. Kontinuierliche Verbesserung / Überwachung

# GRUNDSCHUTZ MIT VERINICE

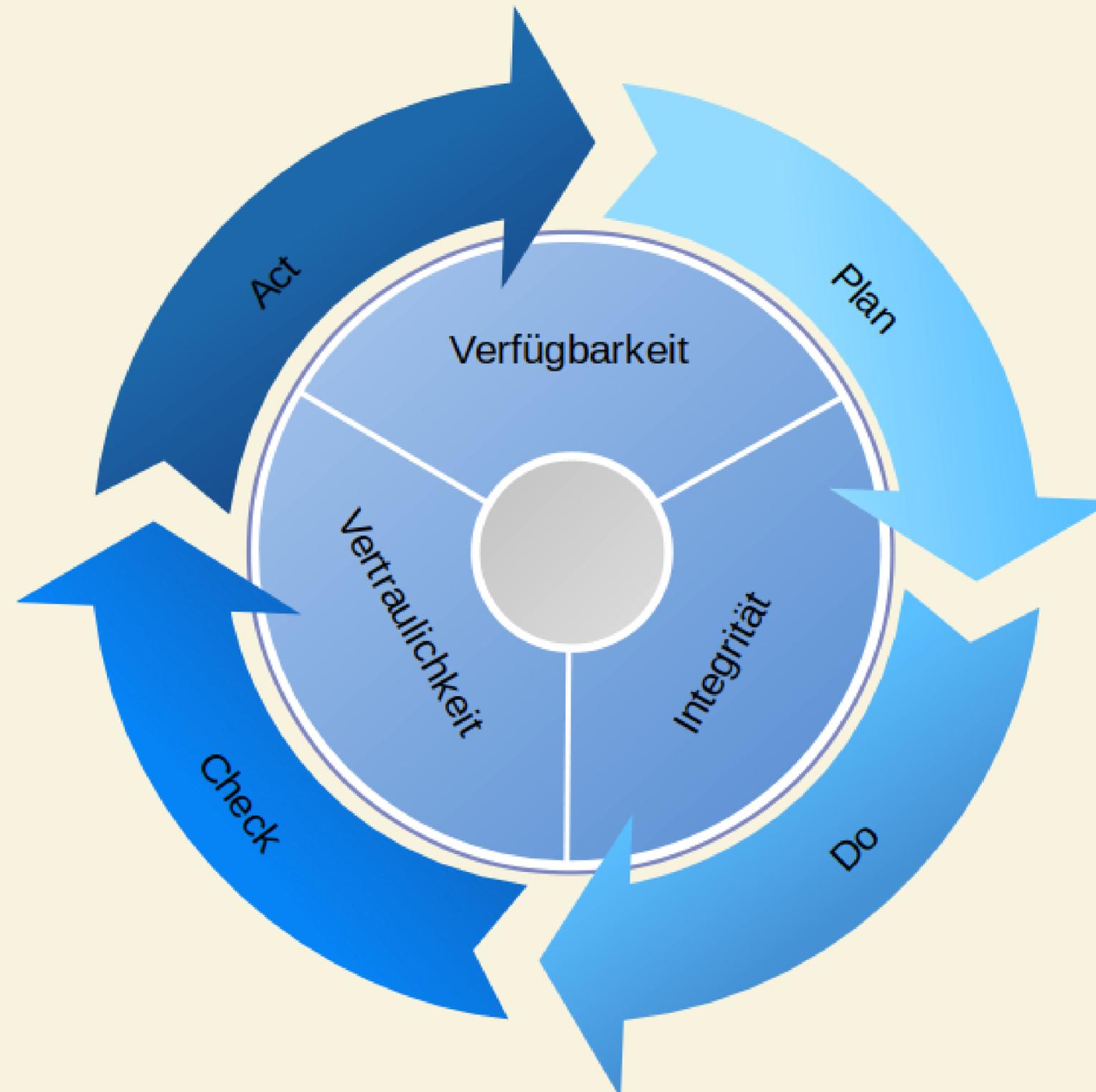
The screenshot displays the Verinice software interface. The top bar shows the application name 'verinice' and the system clock 'Fr 13:31'. The main window is divided into several panes:

- IT-Grundschutz-Kompodium 3.0:** A tree view showing the hierarchy of security measures. The selected item is 'SYS.1.2.2.A3 Sichere Administration von Windows Server 2012'.
- Modernisierter IT-Grundschutz:** A tree view showing the modernized security measures. The selected item is 'Abteilungsserver'.
- Abteilungsserver:** A detailed view of the selected measure, showing fields for 'Kürzel' (S1), 'Titel' (Abteilungsserver), 'Tags', and 'Beschreibung'.
- Objektbrowser:** A pane showing the selected measure's details, including the title 'SYS.1.2.2.A3 Sichere Administration von Windows Server 2012' and the description: 'Lokale Administrationskonten MÜSSEN einzigartige, sichere Passwörter besitzen. Alle Administratoren, die für das Serversystem zuständig sind, MÜSSEN in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2012 bzw. R2 geschult sein. Sie DÜRFEN administrative Rechte NICHT einsetzen, wo diese nicht zwingend erforderlich sind. Browser auf dem Server DÜRFEN NICHT zum Surfen im Web verwendet werden.'

# 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 verfügbar
- Quellcode auf <https://github.com/SerNet/verinice>

# GRUNDPRINZIPIEN



# DSGVO RELEVANTES MONITORING

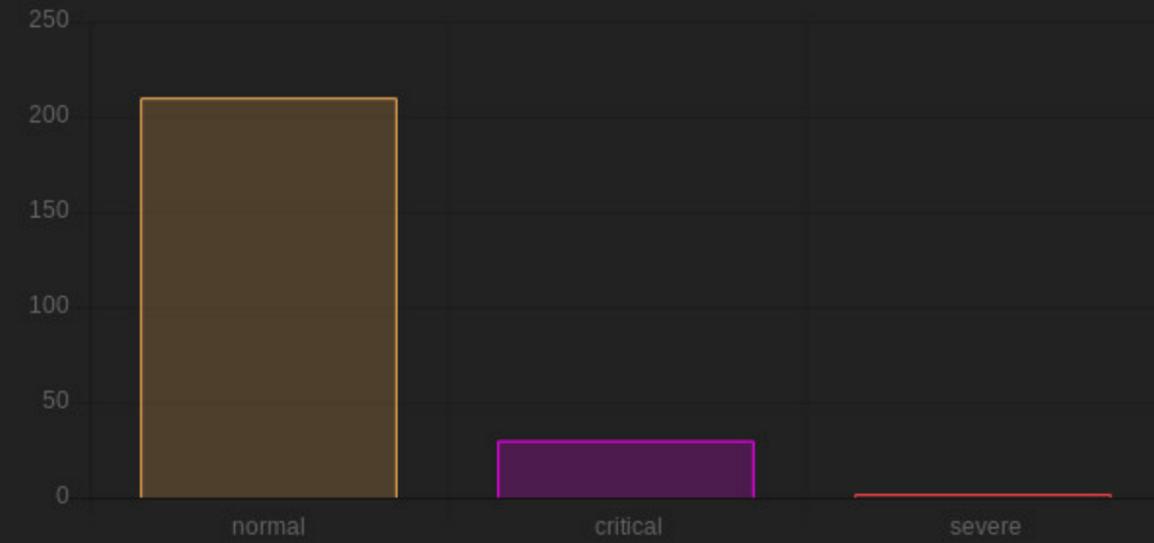
- Geschäftsprozesse überwachen
- Verfügbarkeit der Anwendungen
- Infrastruktur Monitoring
- Verifikation Backups
- Anomalien in den Produktionsanlagen
- Fehlerhafte Anmeldeversuche
- Alarmierung
- Ergebnisse Security Scanner
- Software Installationsstatus
- Aktualität Virens Scanner

# DSGVO RELEVANTES MONITORING

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

# HR - IT Security Dashboard

## Security Incidents



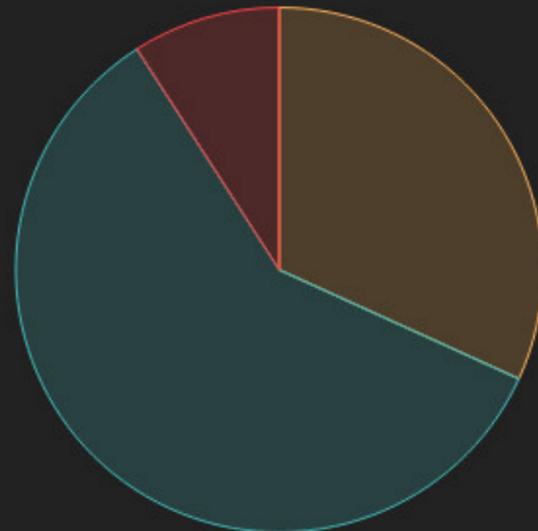
## Upcoming Events

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

Last updated at 10:51

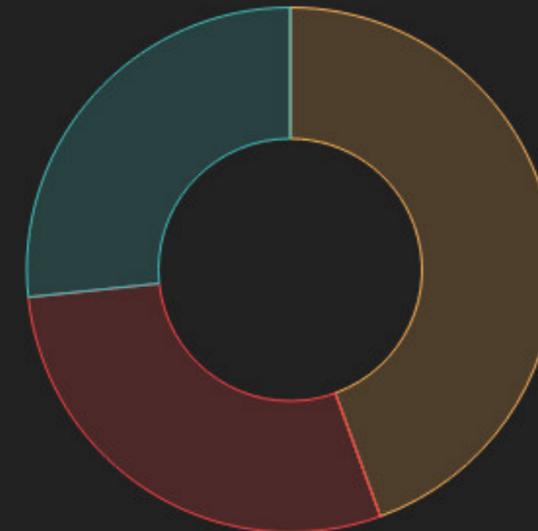
## Sicherheitsunterweisung 2019

Offen Abgeschlossen Wiederholung



## Phishing Mail Übungen

Unbeantwortet Erfolgreich Gemeldet



# 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](mailto:hagen.bauer@rusticus-consulting.de)