CONSIST
Business Information Technology

IT that works.

Insider Threat Management

Mythos & Glaube! Was steckt dahinter?

Teilnehmer der
Allianz für
Cyber-Sicherheit

CONSIST
Business Information Technology

Christian-Albrechts-Universität zu Kiel

Diplom-Informatiker

Service Manager im Online-Handel

Prüfverfahrens-Kompetenz für §8a BSIG

KRITIS-Unternehmen

Dennis Buroh

Domain Administrator

ISMS Auditor

Datenschutzbeauftragter
(TÜV)

Projektmanager (IPMA)

Finanz- und Gesundheitssektor

IT Security Consultant

Mythos & Glaube!

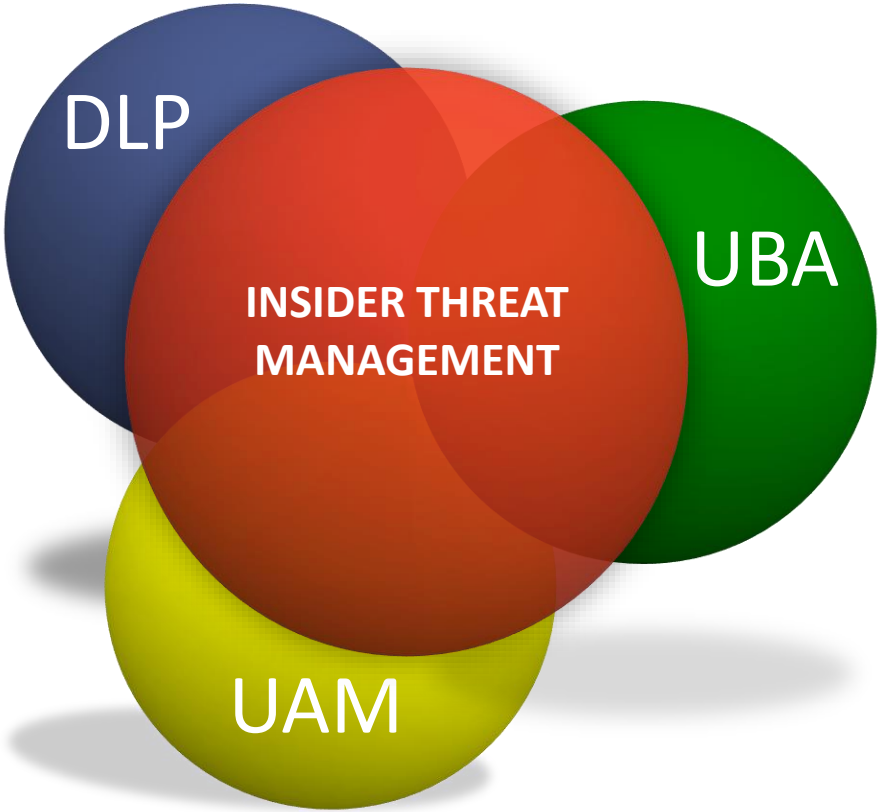
CONSIST
Business Information Technology

IT that works.

CONSIST
Business Information Technology

Was ist Insider Threat?

CONSIST
Business Information Technology

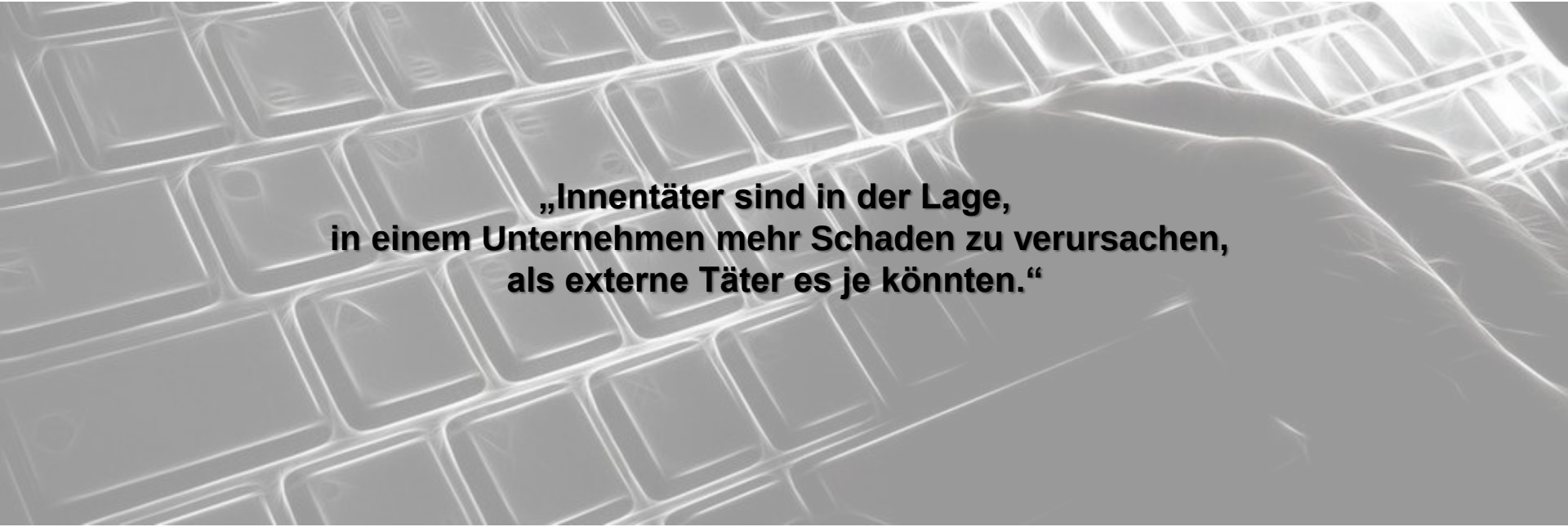


CONSIST
Business Information Technology

007

CONSIST
Business Information Technology

CONSIST
Business Information Technology



„Innentäter sind in der Lage,
in einem Unternehmen mehr Schaden zu verursachen,
als externe Täter es je könnten.“

Der Innentäter…

Auszug aus BSI Mitteilung CS_061

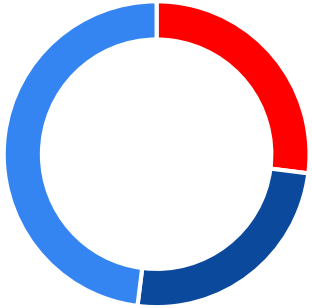
Lieferkette (Supply Chain) ist zu berücksichtigen, denn alle beteiligten Dienstleister und Geschäftspartner bilden als potenzielle Innentäter jeweils einen zusätzlichen Angriffsvektor.

Potenzielle Innentäter sind sämtliche Personen mit (privilegiertem) Zugriff auf bzw. Zutritt zu IT-Komponenten, IT-Diensten, Installationen, Dokumenten oder sonstigen ggf. kritischen Informationen und Geräten. Insbesondere sind hierbei folgende Personenkreise zu nennen:

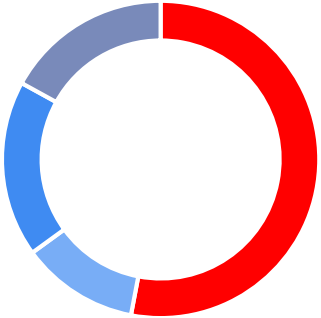
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_061.pdf?__blob=publicationFile&v=2

Geht vom Innentäter **die** Gefahr aus?

Anteil in berichteten Angriffen



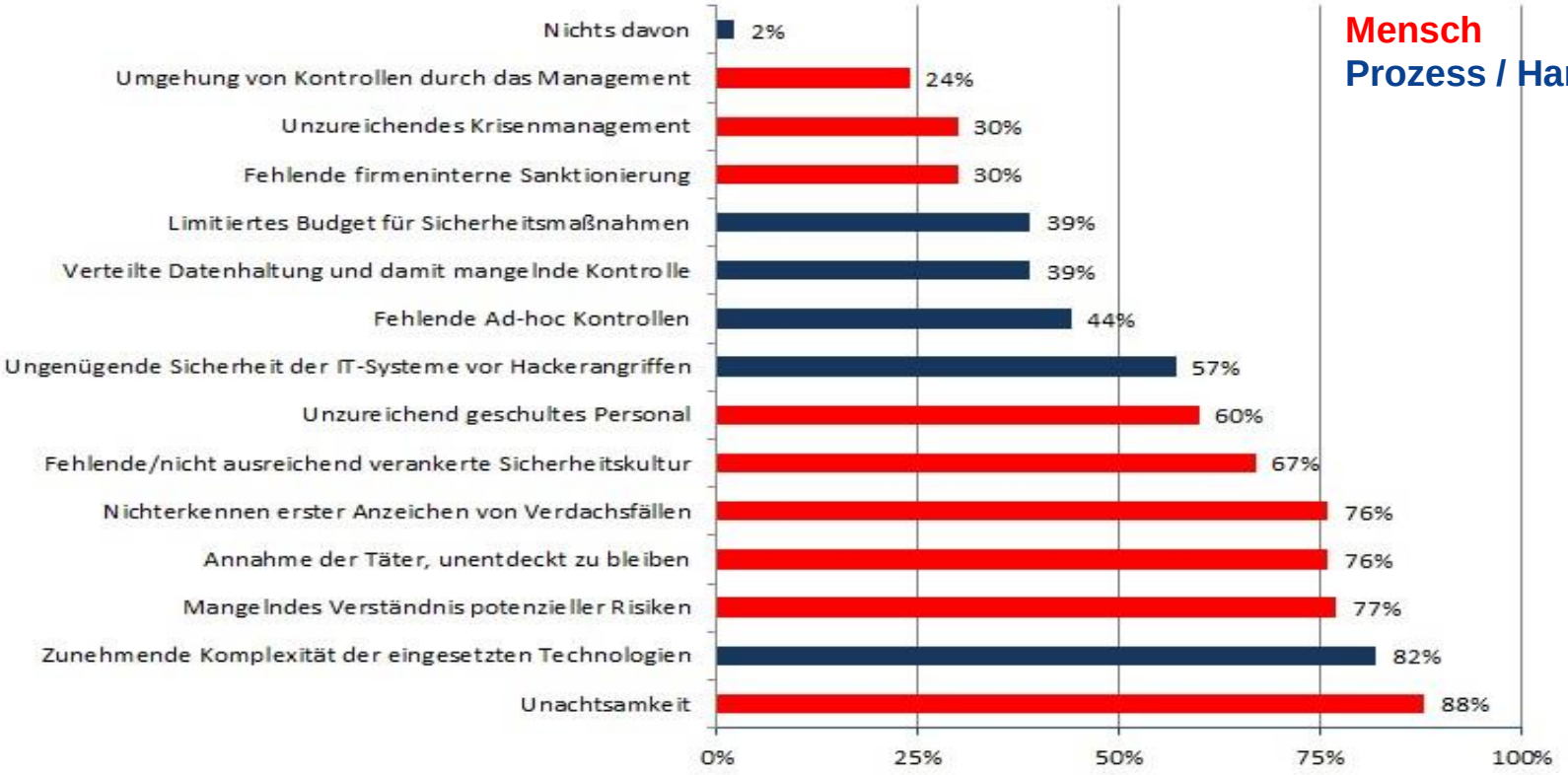
- 27% Human error
- 25% System glitch
- 48% Malicious or criminal attack



- 53% Maleware
- 12% APT
- 18% DDoS
- 17% andere

IBM Threat Monitoring Detection Response Report 2017
Ergebnisse der Cyber-Sicherheits-Umfrage 2018

CONSIST
Business Information Technology



Mensch
Prozess / Hardware

Ergebnisse der Cyber-Sicherheits-Umfrage 2015

IT Security ist **keine** Eintagsfliege!

CONSIST
Business Information Technology

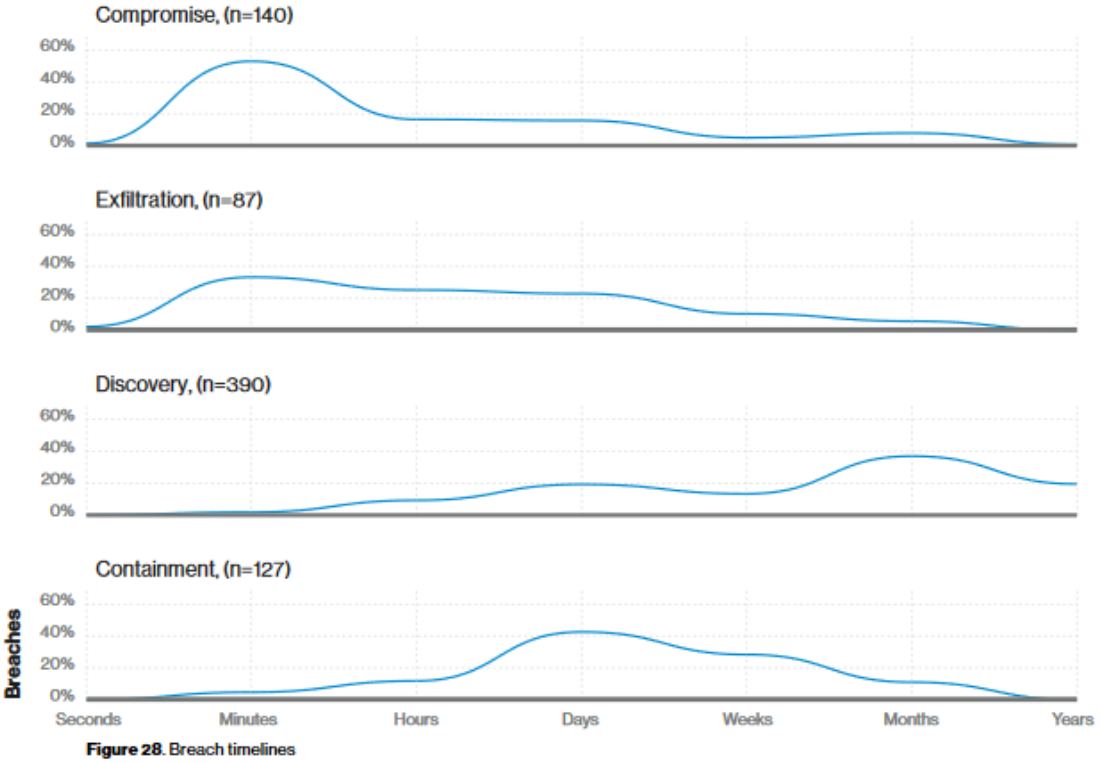


Figure 28. Breach timelines

Data Breach Investigations Report 2019

Beispiele

CONSIST
Business Information Technology

Snapchat-Mitarbeiter

Tools zum Ausspähen der Benutzer missbraucht

Ein Medienbericht enthüllt, dass interne Software bei Snapchat offenbar in zahlreichen Fällen zum Auskundschaften persönlicher Nutzerdaten missbraucht wurde.

35

30.000 US-DOLLAR SCHADEN

Admin wegen Sabotage nach Kündigung verurteilt

Nach Meinungsverschiedenheiten hatten sich ein Systemadministrator und sein Arbeitgeber getrennt. Das hielt den Admin aber nicht davon ab, noch zahlreiche Dateien und Konten zu löschen oder deren Passwörter zu ändern. Dafür wurde der US-Amerikaner nun verurteilt.

Datenklau und Netzstörungen: Pannenserie bei Swisscom

08.02.2018 13:28 Uhr – Tom Sperlich vorlesen

(Bild: dpa, Karl-Josef Hildenbrand/Symbol)

Unbekannte haben im letzten Jahr Zugriff auf 800.000 Kundenkontaktdaten des Schweizer Telekommunikationsunternehmens Swisscom erlangt. Netzstörungen und ein geplanter Stellenabbau belasten den Konzern zusätzlich.

DATENSCHUTZ

E.on Hanse nutzt gesperrte Daten

Wiebke Schwirten

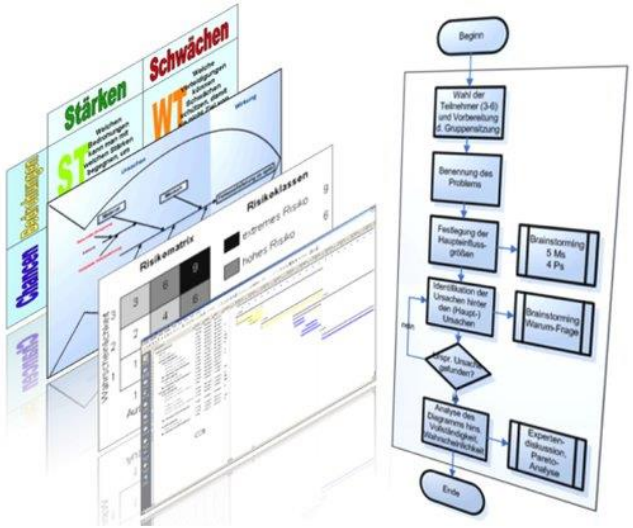
0

Fünfhausen. Wird einem Versorgungsunternehmen eine Einzugsermächtigung erteilt, dann können vereinbarte Summen vom Konto abgebucht werden. Erlischt die Ermächtigung, dann sind Abbuchungen nicht mehr möglich. Sollte man meinen.

Warum denn überhaupt?

- ISO:IEC 27001:2013
- ISO:IEC 27002:2013
- ISO:IEC 29151:2017
- BAIT, VAIT, KAMaRISK
- Branchenspezifische Sicherheitsstandards (B3S)

Die Bestandteile



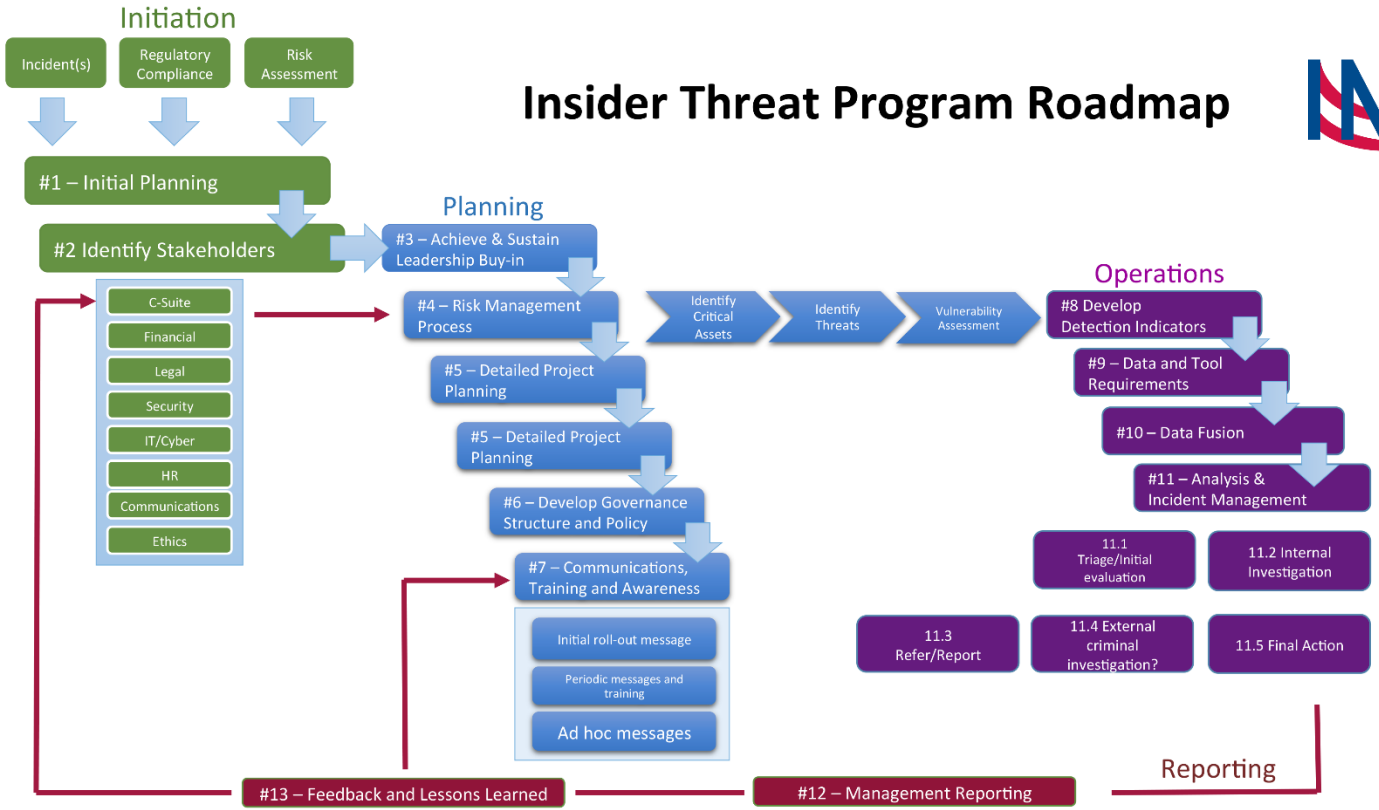
- ✓ vorhandene Baseline
- ✓ Risikoanalyse
- ✓ Log-Management
- ✓ Insider Threat System
- ✓ User Behavior Monitoring
- ✓ Awareness Programm

- ✓ **Zeit & Transparenz**

IT that works.

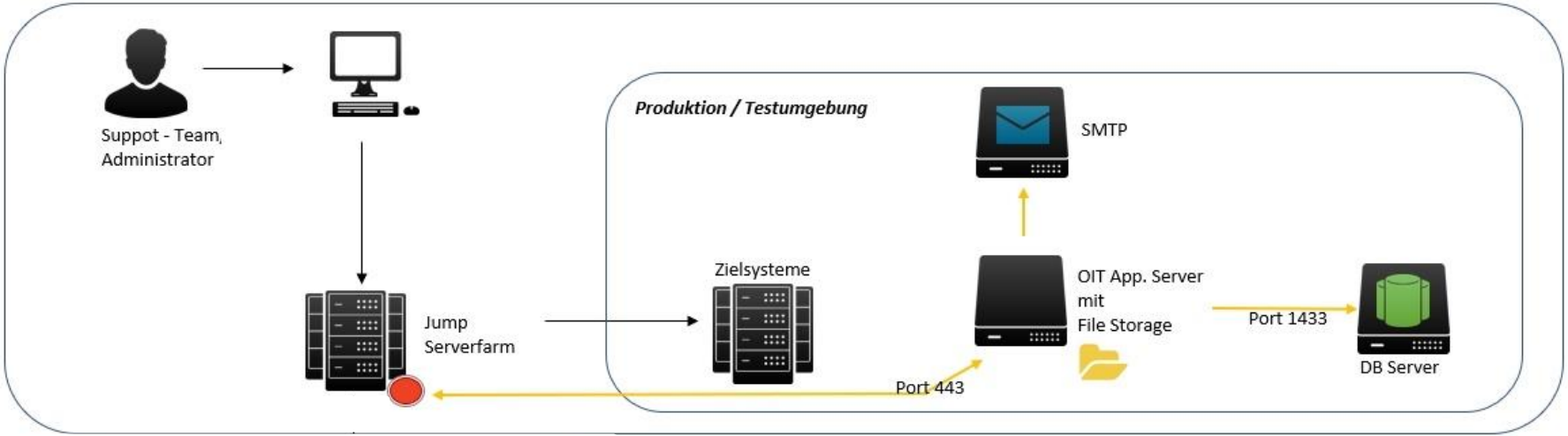
Die Einführung

CONSIST
Business Information Technology



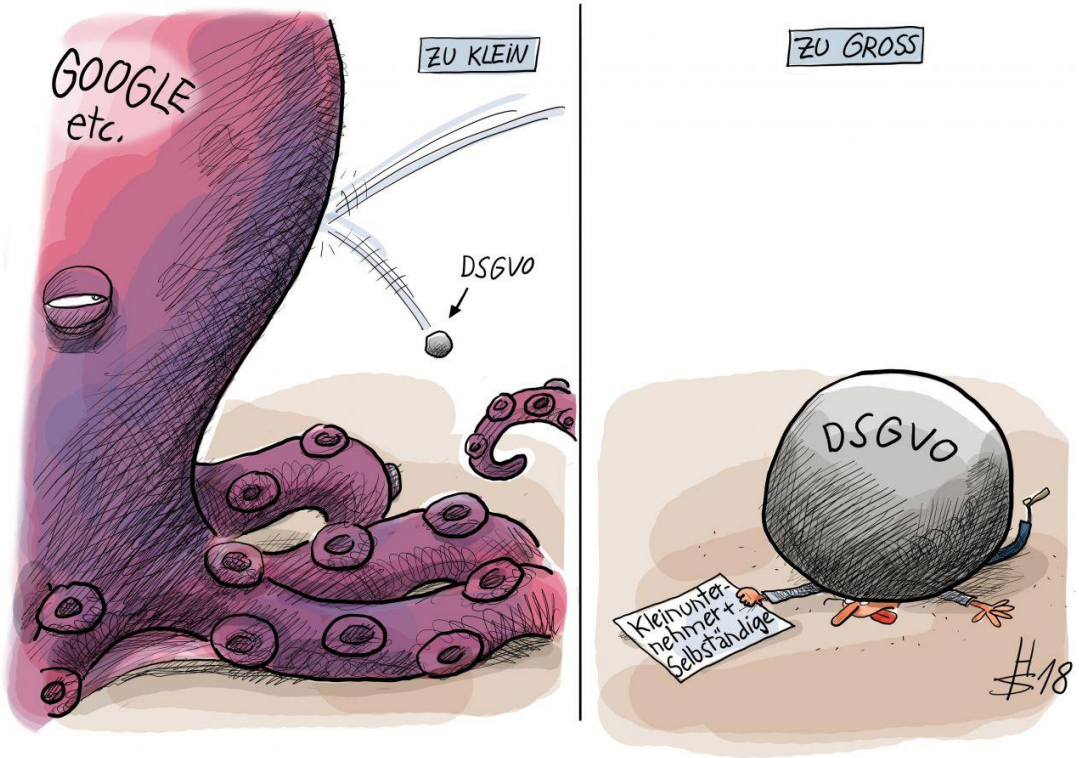
https://www.insaonline.org/insider-threat-roadmap/

Architektur



Es ist immer eine Frage der Perspektive

CONSIST
Business Information Technology



Unser Portfolio

CONSIST
Business Information Technology

IT that works.

Kontakt

Dennis Buroh
Senior Consultant Security

Phone: +49 (0) 431 / 3993 - 758
E-Mail: buroh@consist.de

CONSIST
Business Information Technology

IT that works.