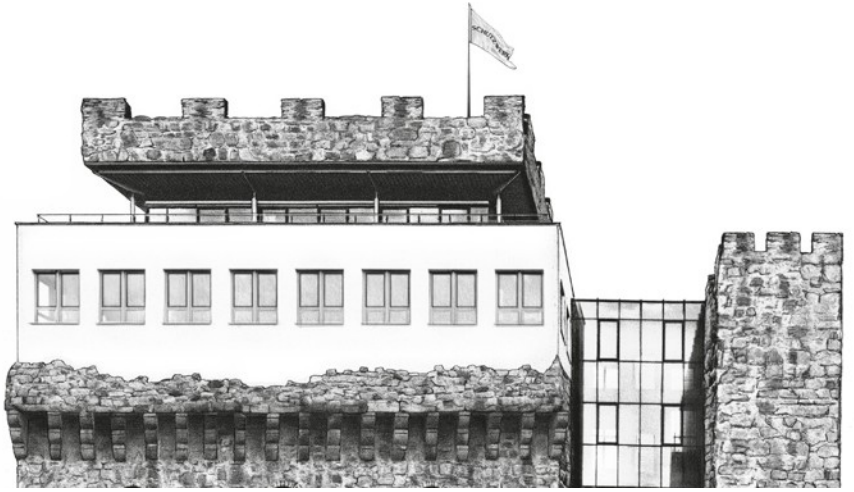
Meistern, worauf es in Informations-, IT- und Cybersicherheit ankommt



Home Office und IT-Sicherheit

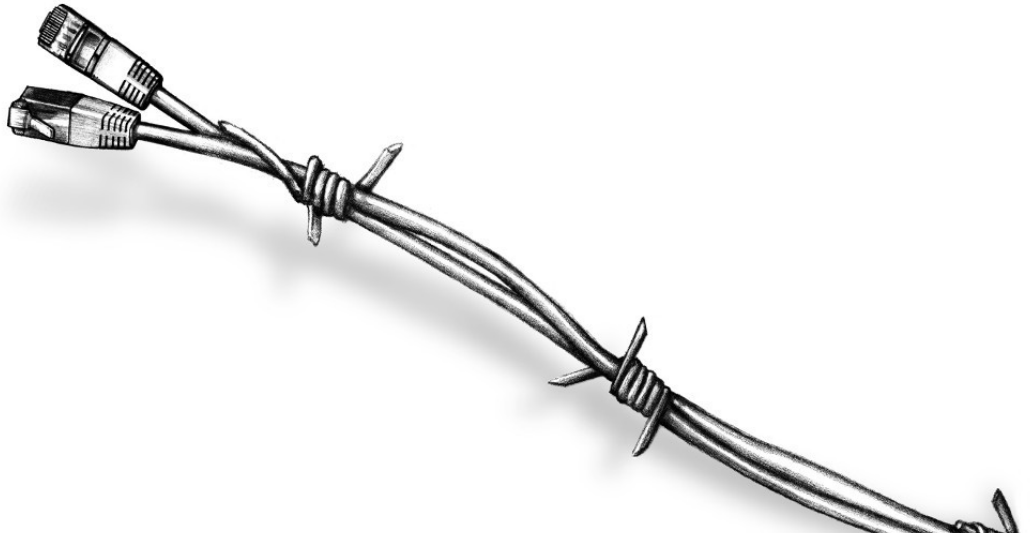
WEBINAR | TOBIAS ARNOLD | 17.04.2020

SCHUTZWERK

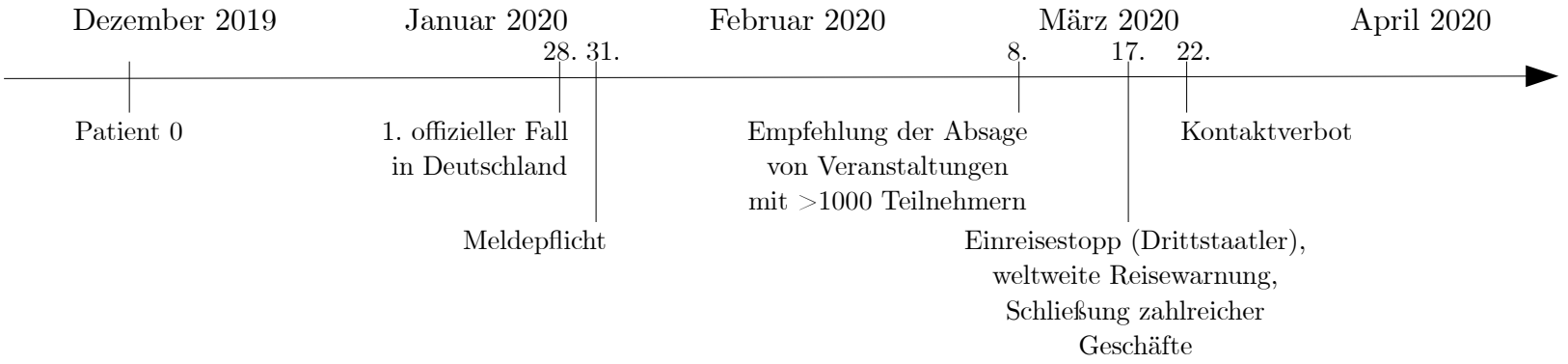
UNABHÄNGIGE PRÜFUNG - GANZHEITLICHE OPTIMIERUNG

SCHUTZWERK ist Ihr Partner für die unabhängige Prüfung
und ganzheitliche Optimierung aller Aspekte der
Informations-, IT- und Cybersicherheit in Ihrem Unternehmen.

1 | Einführung und Motivation



Aktuelle Situation



- **Home Office Bedarf ad hoc gestiegen**
- **Neue Angriffsformen**

Medizinische Einrichtungen laut Interpol verstärkt im Visier von Ransomware

Warnung vor Phishing-Mails mit Antragsformular "Familien- und Krankenurlaub"

Vorsicht Corona-Phishing: Aktuelle Mails setzen auf Angst und Verunsicherung

Quellen: https://www.heise.de/
https://de.wikipedia.org/wiki/COVID-19-Pandemie_in_Deutschland

Home Office: Herausforderungen

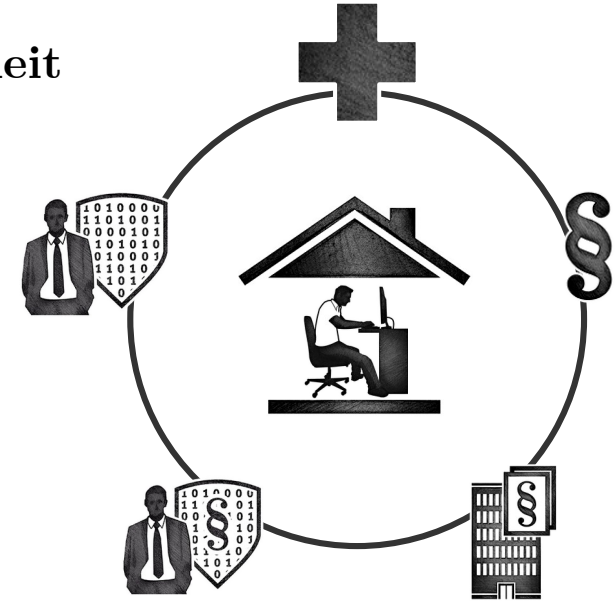
- **Konzeptentwicklung (inklusive IT-Sicherheit)**
- **Schaffen von Infrastruktur und Endgeräten**
- **Beschaffen von (Software-) Lizenzen**
- **Schaffen einer geeigneten Arbeitsumgebung zu Hause**
- **Schulung der Mitarbeiter**
- **...**

Home Office: Herausforderungen in Zeiten von Corona

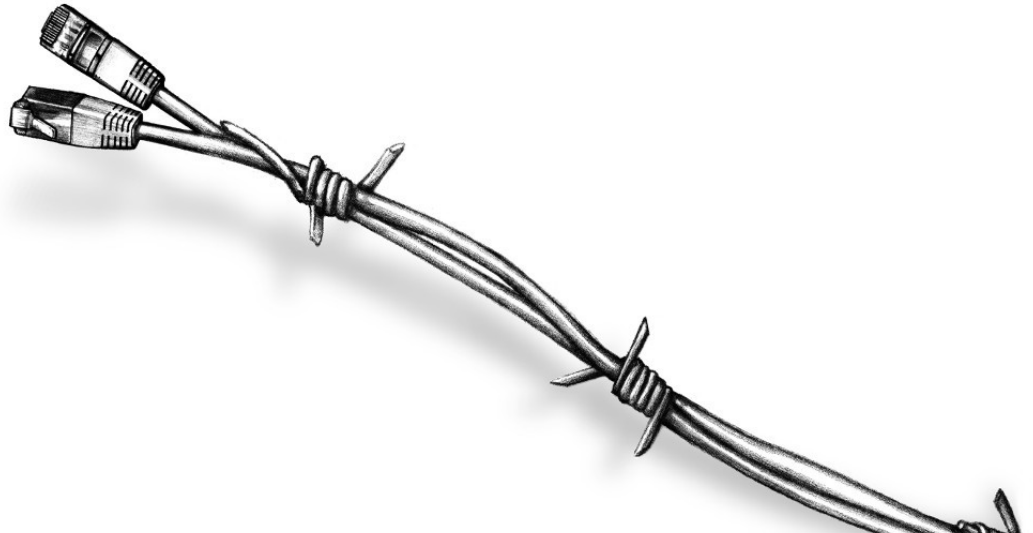
- **Konzeptentwicklung (inklusive IT-Sicherheit)**
- **Schaffen von Infrastruktur und Endgeräten**
- **Beschaffen von (Software-) Lizenzen**
- **Schaffen einer geeigneten Arbeitsumgebung zu Hause**
- **Schulung der Mitarbeiter**
- **...**
- **Maßnahmen gegen neue Angriffsszenarien und -wellen**

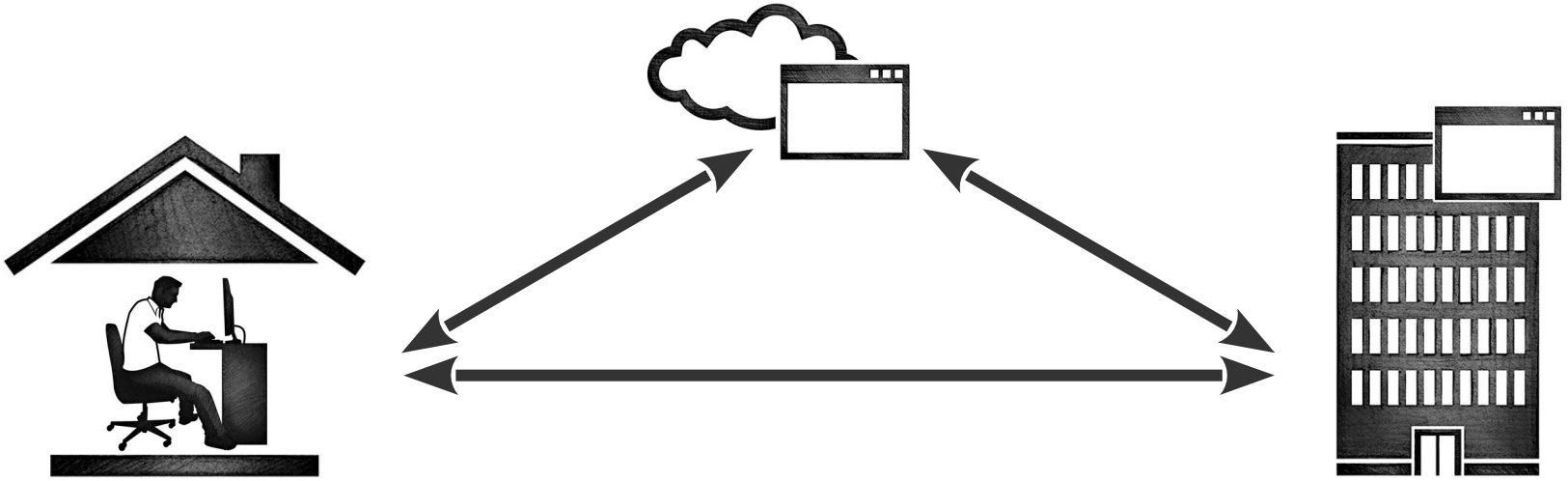
Home Office: Rahmenbedingungen

- **Gesundheitsprävention / Arbeitssicherheit**
- **Arbeitsrecht**
- **Betriebsverfassung**
- **Datenschutz**
- **IT-Sicherheit (Security und Safety)**



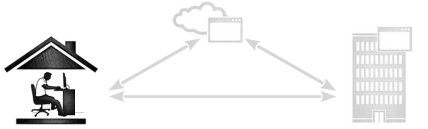
2 | Risikobereiche





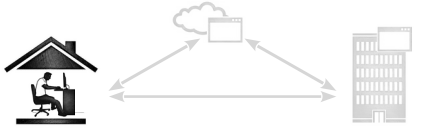
Home Office **Kommunikation** **Büro**

- **Risikobereich Heimarbeitsplatz**
- **Risikobereich Arbeitsgerät**
- **Risikobereich Kommunikation**
- **Risikobereich Arbeitgeber/Büro**



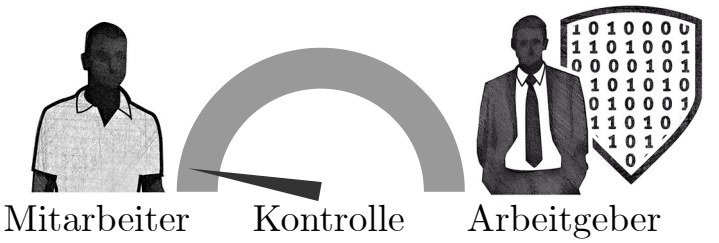
Risikobereich Heimarbeitsplatz

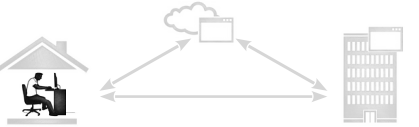
- ⚠ **Mithören von Konferenzen / Telefonaten durch Außenstehende**
  - 🔒 **Abgeschlossenen Arbeitsbereich schaffen**
  - 🔒 **Zimmer verlassen / Telefonat unterlassen**
- ⚠ **Shouldersurfing**
  - 🔒 **Abgeschlossenen Arbeitsbereich schaffen**
  - 🔒 **Schutzfolie / Vereinbarung mit Angehörigen**
- ⚠ **Zugriff auf Datenträger und Akten durch Unbefugte**
  - 🔒 **Abgeschlossenen Arbeitsbereich schaffen**
  - 🔒 **Akten und Datenträger wegschließen / verschlüsseln**



Risikobereich Heimarbeitsplatz

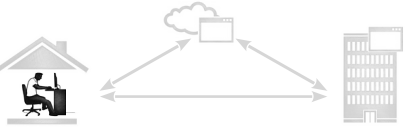
- ⚠ **Verlust / Diebstahl / Zerstörung von Geräten, Datenträgern, Akten**
  - 🔒 **Abschließbaren Arbeitsbereich schaffen**
  - 🔒 **Akten und Datenträger wegschließen / verschlüsseln**
  - 🔒 **Regelmäßige Offsite Backups**
- ⚠ **Heimnetz als private Infrastruktur**
  - 🔒 **Absicherung des Netzwerks**
  - 🔒 **Einfache Segmentierung**
- ⚠ **Ausfall von Internet / Strom / ...**
  - 🔒 **Fallback-Lösung bereitstellen**





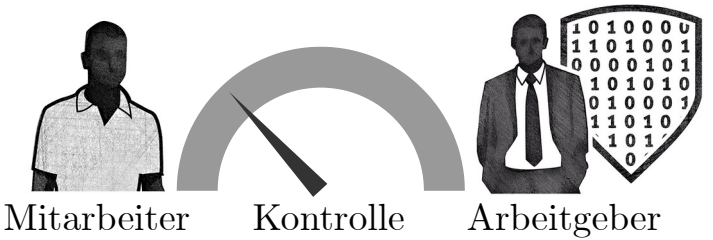
Risikobereich Arbeitsgerät

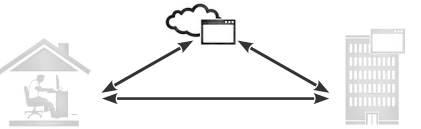
- ⚠ **Nutzung von privaten Geräten**
  - 🔒 **Nutzung von dedizierten, gestellten, Arbeitsgeräten (MDM)**
- ⚠ **Private Nutzung des Arbeitsgeräts**
  - 🔒 **bestehende Kontrollmechanismen nutzen (via VPN)**
  - 🔒 **Richtlinien für private Nutzung festlegen**
- ⚠ **Schadsoftware und Hacker-Angriffe**
  - 🔒 **Installation von Schutzsoftware**
  - 🔒 **Härten der Arbeitsgeräte**
  - 🔒 **Updaten**



Risikobereich Arbeitsgerät

- ⚠ **Ungeschützter Zugang**
  - 🔒 **Account schützen / starke Authentifizierung (2-Faktor)**
  - 🔒 **Datenträger verschlüsseln (PIN)**
  - 🔒 **Sperren / Herunterfahren**
- ⚠ **Mitnutzung von Arbeitsgeräten durch Dritte**
  - 🔒 **Untersagen**
  - 🔒 **Dedizierte Accounts / Installationen**
- ⚠ **Nutzung private Speichermedien**
  - 🔒 **Untersagen / technische Maßnahmen**





Risikobereich Kommunikation

⚠ **Phishing durch ungewohnte Kommunikationskanäle**

🔒 **Kommunikationswege definieren und kommunizieren**

⚠ **Kommunikation über unsichere Kanäle**

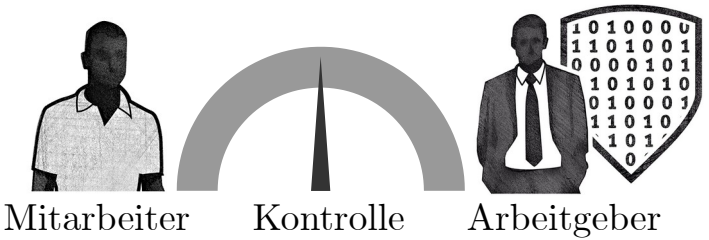
🔒 **Kanäle zur sicheren Kommunikation bereitstellen**

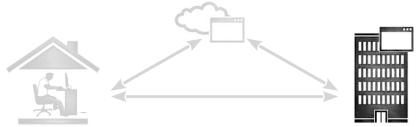
⚠ **Datenübertragung über unsichere Kanäle**

🔒 **Zentralen Dienst zum Datenaustausch bereitstellen**

⚠ **Nutzung von unsicheren, externer Dienste**

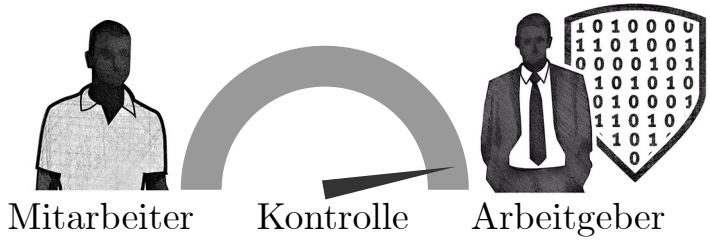
🔒 **Prüfung und Kontrolle externer Dienstleister**



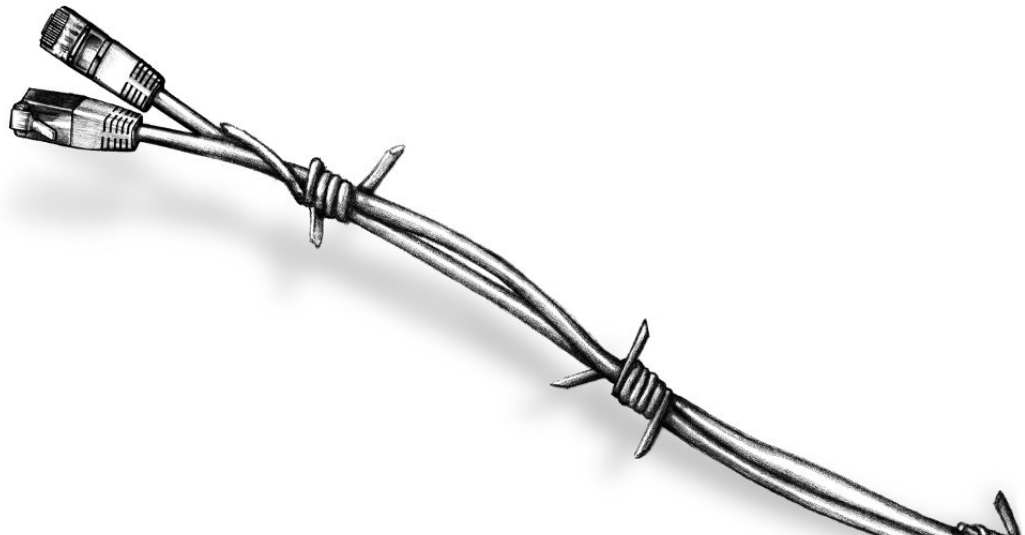


Risikobereich Arbeitgeber/Büro

- ⚠ **Dienste im Internet exponiert**
  - 🔒 **Nur notwendige Dienste exponieren / VPN nutzen**
  - 🔒 **Absicherung der Dienste (starke Authentifizierung, aktuelle Sicherheitsupdates einspielen)**
- ⚠ **Zugriffskontrolle durch externen Zugang umgangen**
  - 🔒 **Korrekte Zuweisung externer Mitarbeiter in vorgesehene Netzbereiche mit passenden Berechtigungen**

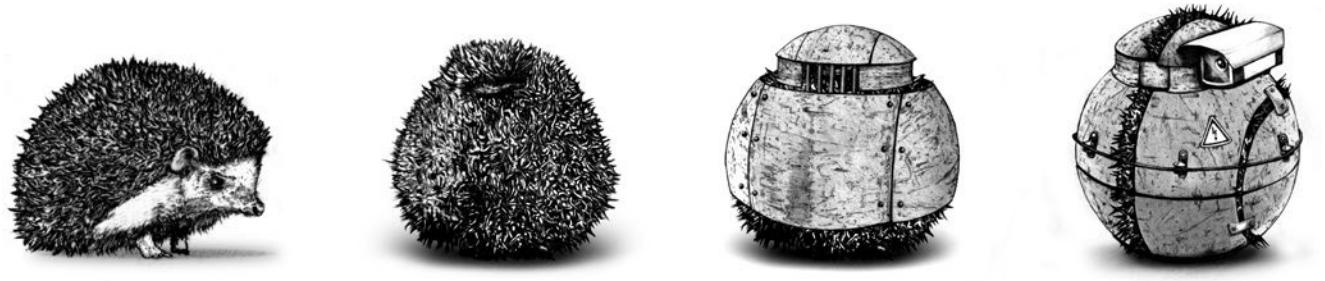


3 | Zusammenfassung



- **Verantwortung für Mitarbeiter steigt - Kontrolle für Arbeitgeber sinkt**
- **Maßnahmen**
  - Dediziertes, gehärtetes Arbeitsgerät
  - Sicheren Arbeitsbereich schaffen (geschlossen und abschließbar)
  - Verschlüsselung aller Datenträger / Wegsperren aller Dokumente
  - Regelmäßige offsite Backups
  - Software aktuell halten und Sicherheitssoftware nutzen
  - Kommunikationswege definieren
  - Nutzung von VPN und anderen sicheren Kanälen
  - Starke Authentifizierung nutzten
  - Minimale Daten daheim halten
  - Ad hoc Maßnahmen dokumentieren
- **Dokumentiertes Konzept und Schulung der Mitarbeiter essentiell**

Für Fragen stehen wir Ihnen gerne zur Verfügung



SCHUTZWERK GmbH
Ulm | Hamburg

Telefon +49 731 977 191 0
Fax +49 731 977 191 99

www.schutzwerk.com
info@schutzwerk.com