



**Sicherheitsmanagement  
Was Entscheider über  
Sicherheitslücken und den  
Umgang mit diesen wissen sollten!**

Manuel (HonkHase) Atug

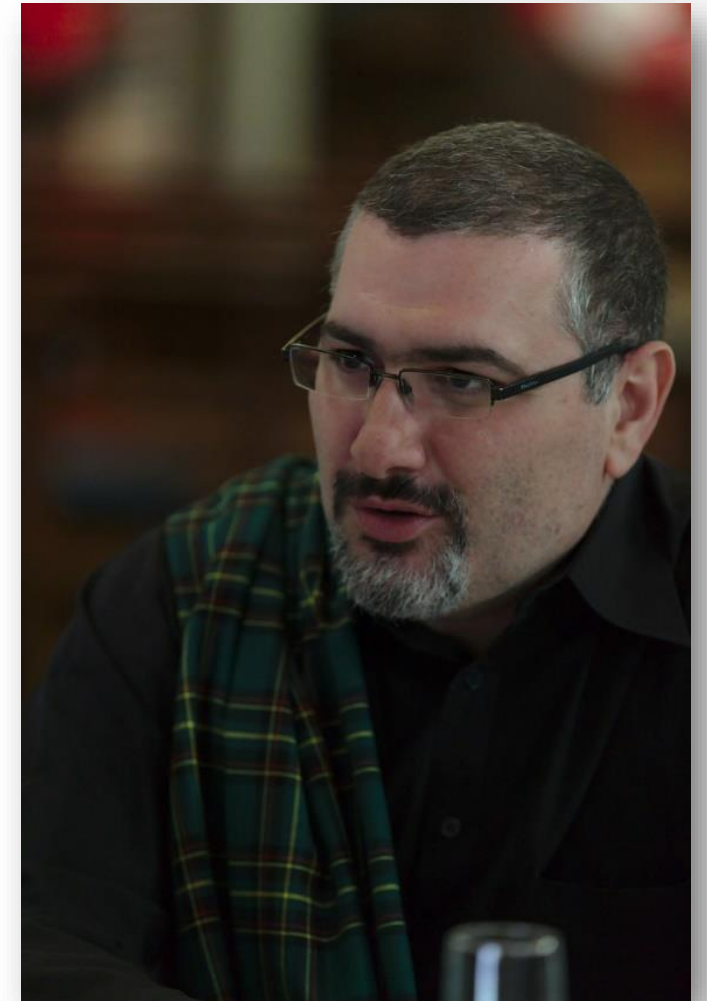
Ich habe #KRITIS im Endstadium

# Manuel (HonkHase) Atug

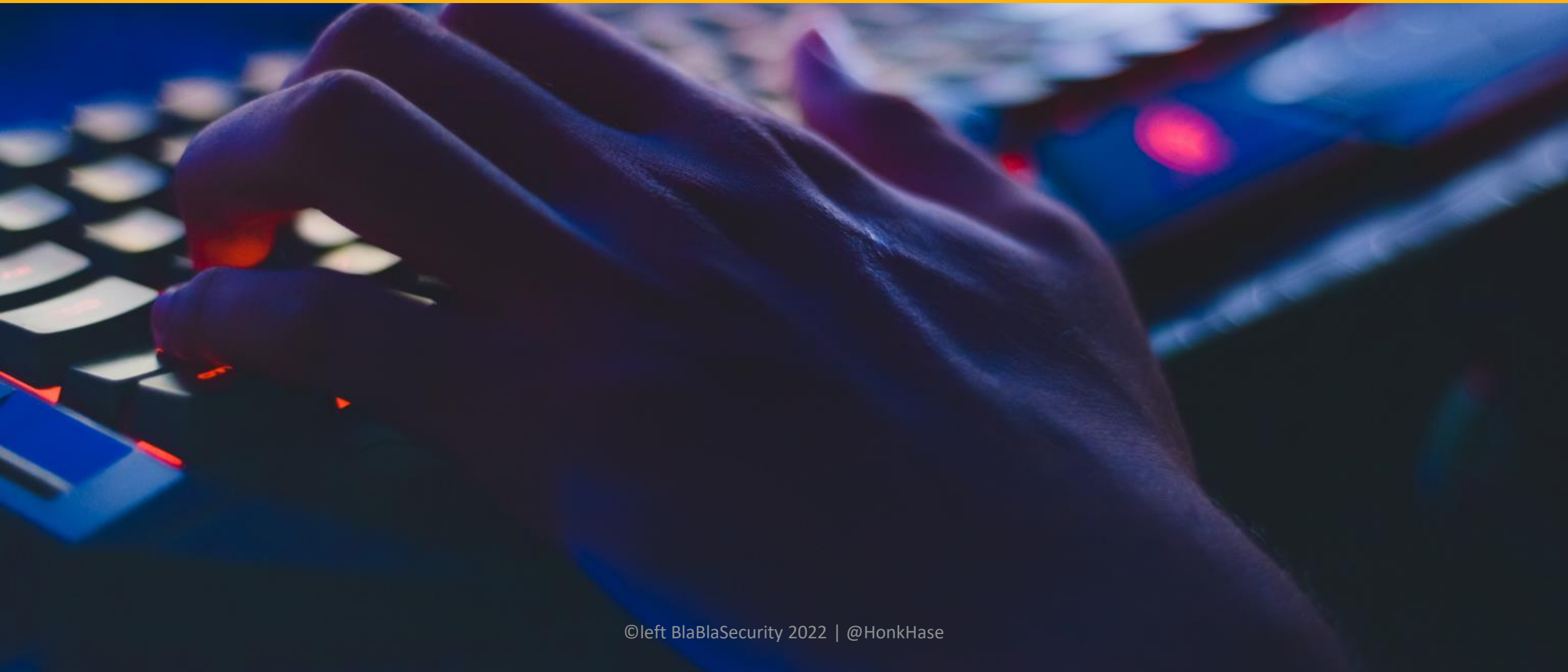
Head of Business Development bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- > 23 Jahren in der Informationssicherheit tätig
- Sachverständiger für das IT-SiG 2.0 im Bundestag
- Themen: KRITIS, Hackback, Ethik, Hybrid Warfare, Cyberresilienz, Bevölkerungs- und Katastrophenschutz
- Mitgründer der AG KRITIS: [ag.kritis.info](https://ag.kritis.info)
- Mitgründer der AGND: [www.agnd.eu](https://www.agnd.eu)

 [@HonkHase](https://twitter.com/HonkHase)



# Was sind die Ziele von Cybersicherheit?





# Quo vadis?

## ▪ **Verfügbarkeit**

Autorisierte Benutzer werden am Zugriff auf Informationen und Systeme behindert

## ▪ **Integrität**

Die Korrektheit der Informationen und der Funktionsweise von Systemen ist nicht mehr gegeben

## ▪ **Vertraulichkeit**

Vertrauliche Informationen werden unberechtigt zur Kenntnis genommen oder weitergegeben

\*BSI Grundschutz

Und was heißt das jetzt genau für mich?



# Die Gefahren des Home Office

Datensicherheit wird vernachlässigt

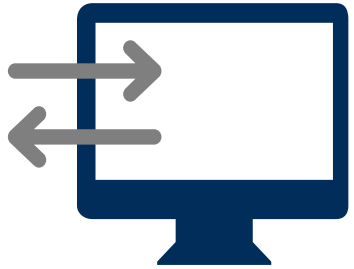
Keine gewohnten Strukturen

Keine klaren Grenzen

Keine sozialen Kontakte

# Digitale Selbstverteidigung für KMU und Konzerne

Home Office? Aber sicher!



Absicherung des  
Zugriffs auf  
Unternehmens-  
daten



Absicherung des  
Clients



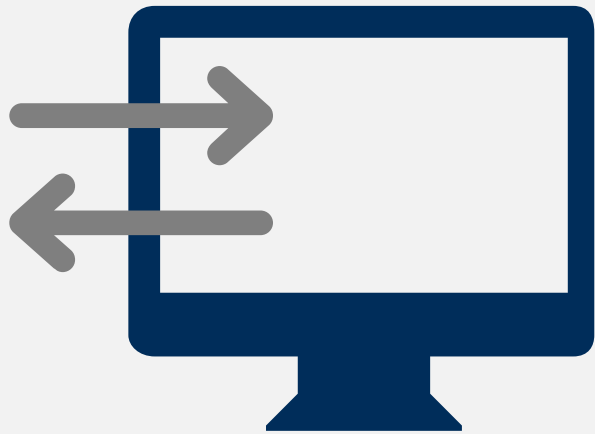
BYOD  
(Bring Your Own  
Device)



Postbearbeitung



Datenschutz



# Absicherung des Zugriffs auf Unternehmensdaten

Wieso sollte der Zugriff auf Unternehmensdaten bei Homeoffice mit betrachtet werden?

Es gelten nicht die gleichen Sicherheitsvorkehrungen wie im Unternehmen!

Welche Maßnahmen sollten ergriffen werden?

- Multifaktorauthentifizierung
- Nutzung der Bildschirmsperre
- Nutzung von Bildschirmschutzfolien
- Adäquater Schutz der IT und der Informationen  
z.B. abschließbare Schränke, Türen & Fenster schließen,  
sichere Entsorgung
- Sicherer Remote-Zugriff auf Unternehmensdaten



# Absicherung des Clients



## Welche Maßnahmen sollten ergriffen werden?

- Nur notwendige Dienste / Anwendungen aktivieren
- Need-to-Know- Prinzip umsetzen (kein lokaler Admin)
- Datensicherung konfigurieren
- Aktuelle Patches und AV-Signaturen automatisiert einspielen
- Einsatz einer lokalen Firewall
- Festplattenverschlüsselung

# Bring-Your-Own-Device (BYOD)



## Wieso muss BYOD genauer betrachtet werden?

Fortführung von Geschäftsprozessen aus dem Homeoffice ist in der Notfall- und Krisenbewältigung eine wichtige Option für Unternehmen

Nutzung privater Geräte fordert einen gewissen Mindestschutz für die Unternehmensdaten

## Welche Maßnahmen können definiert werden?

- Sensibilisierung der Mitarbeiter
- Risikoabwägung hinsichtlich möglicher Sicherheitslücken
- Definition von Mindestanforderungen  
z.B. lokale Firewall, Benutzer ohne administrativen Berechtigungen
- Technische Überprüfung auf Mindestanforderungen (z.B. Patchlevel)

# Drum prüfe, wer sich (ver)bindet

- Öffentliche WLANs sollten gemieden werden
- Eigenes WLAN sollte sicher konfiguriert werden
  - Starke Passwörter (keine Standardpasswörter)
  - Am besten WPA2/WPA3 (kein WEP) verwenden
- VPN verwenden
- Darauf achten, dass keine unsichere Seiten aufgerufen werden und auf https zu achten
- Dateien vor dem Öffnen speichern





# Postbearbeitung

Wieso muss die Postbearbeitung jetzt genauer betrachtet werden?

Zustellungen von Postsendungen muss weiterhin korrekt erfolgen  
Datenschutz und Briefgeheimnis müssen gewahrt bleiben  
Liegen bleiben kann die Post aber auch nicht!

Welche Maßnahmen können definiert werden?

- Prozess zum Umgang mit dem Posteingang und -ausgang definieren
- Digitalisierung des Schriftverkehrs
- Temporär schriftliche Prozesse digitalisieren, ggfs. vereinfachen



# Datenschutz im Homeoffice

## Was bedeutet Datenschutz im Homeoffice?

Das Datenschutzrecht schließt Arbeit im Homeoffice natürlich nicht aus  
Mindestschutz für personenbezogenen Daten gefordert

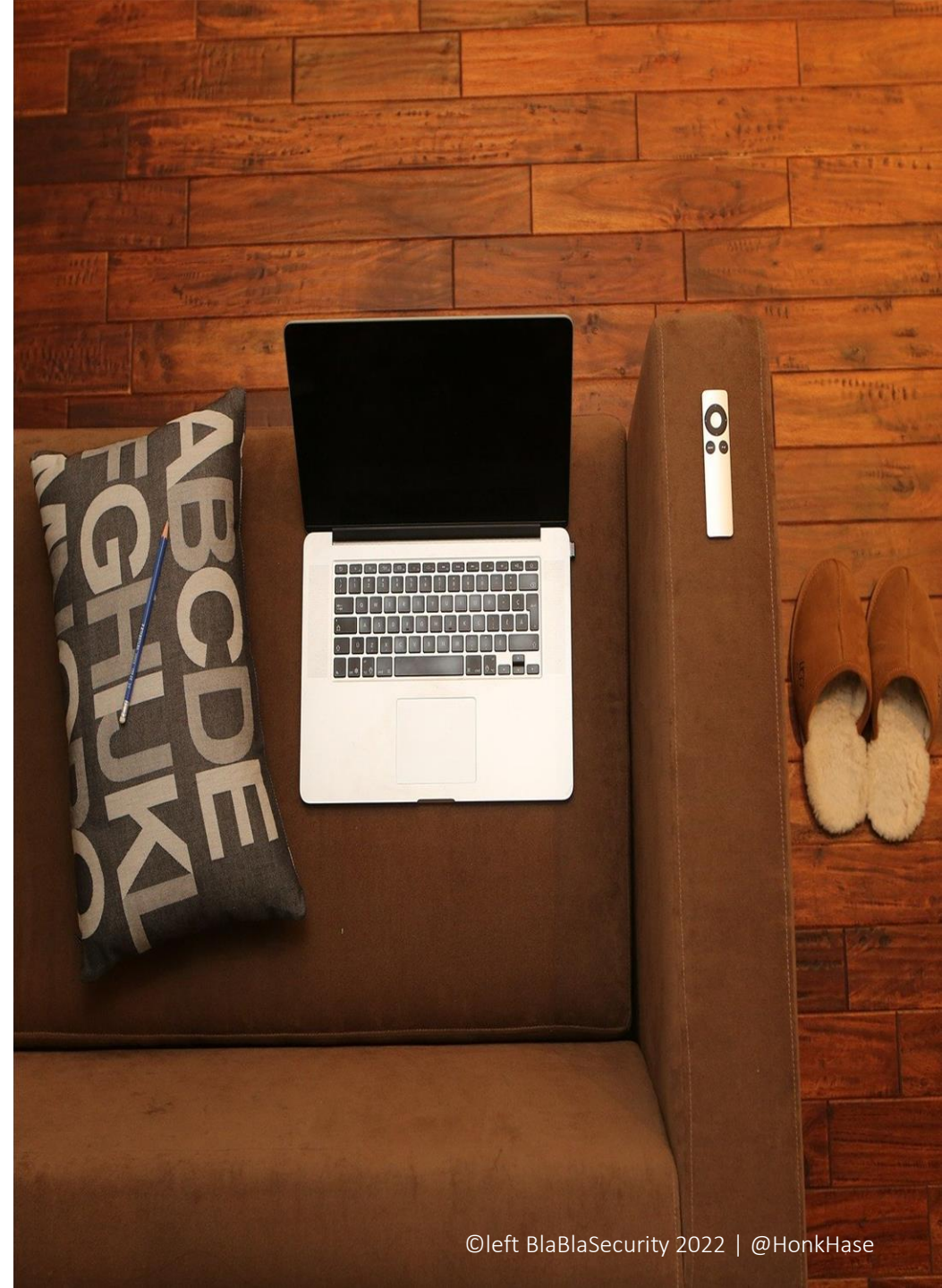
Insbesondere geeignete technische und organisatorische Maßnahmen

## Welche Maßnahmen können definiert werden?

- Organisatorische Vorgaben hinsichtlich der Absicherung des Arbeitsplatzes definieren
- Technische Maßnahmen, wie beispielsweise Festplattenverschlüsselung und Multifaktorauthentifizierung

# Themen für eine ad-hoc Schulung der Mitarbeiter im Homeoffice

- Was muss ich beachten, um von zu Hause sicher arbeiten zu können?
- Welche Voraussetzungen müssen dafür erfüllt sein?
- Welche Risiken können durch die Arbeit von zu Hause entstehen?
- Wie kann ich diese Risiken minimieren oder vermeiden?








# Sicherheitslücken

# Sicherheitslücken

## CERT Bund Sicherheitswarnungen

- <https://wid.cert-bund.de/portal/wid/kurzinformationen>

Stand	Risiko	CVSS Base	ID	Titel
<input type="text" value="TT.MM.JJJJ"/> - <input type="text" value="TT.MM.JJJJ"/>	<input type="text" value="KRITIK"/>		<input type="text" value=""/>	
<input type="text" value="11.10.2022, 10:34"/>		9.9	WID-SEC-2022-1654	Fortinet FortiOS: Schwachstelle ermöglicht Privilegienskalation
<input type="text" value="07.10.2022, 12:09"/>		10.0	WID-SEC-2022-0778	Apple macOS: Mehrere Schwachstellen
<input type="text" value="05.10.2022, 10:24"/>		9.8	WID-SEC-2022-1406	Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen





# Beteiligung hoffnungslos?

## **Botschaft an Behörden, Politik & Wirtschaft:**

**Die SicherheitsforscherInnen Community sagt nicht, ob ihr unsichere Apps betreiben sollt oder nicht**

**Sie zeigt euch nur, wie krude defekt die sind!**



Und sonst so?

On-Prem vs. Outsourcing

# Was betreibe ich wie?



Digitalisierung als Produkt statt als Prozess

# Wie lebt die Firma echte & sichere Digitalisierung?



Fachkräftemangel

Wie gehe ich mit dem  
Fachkräftemangel um?

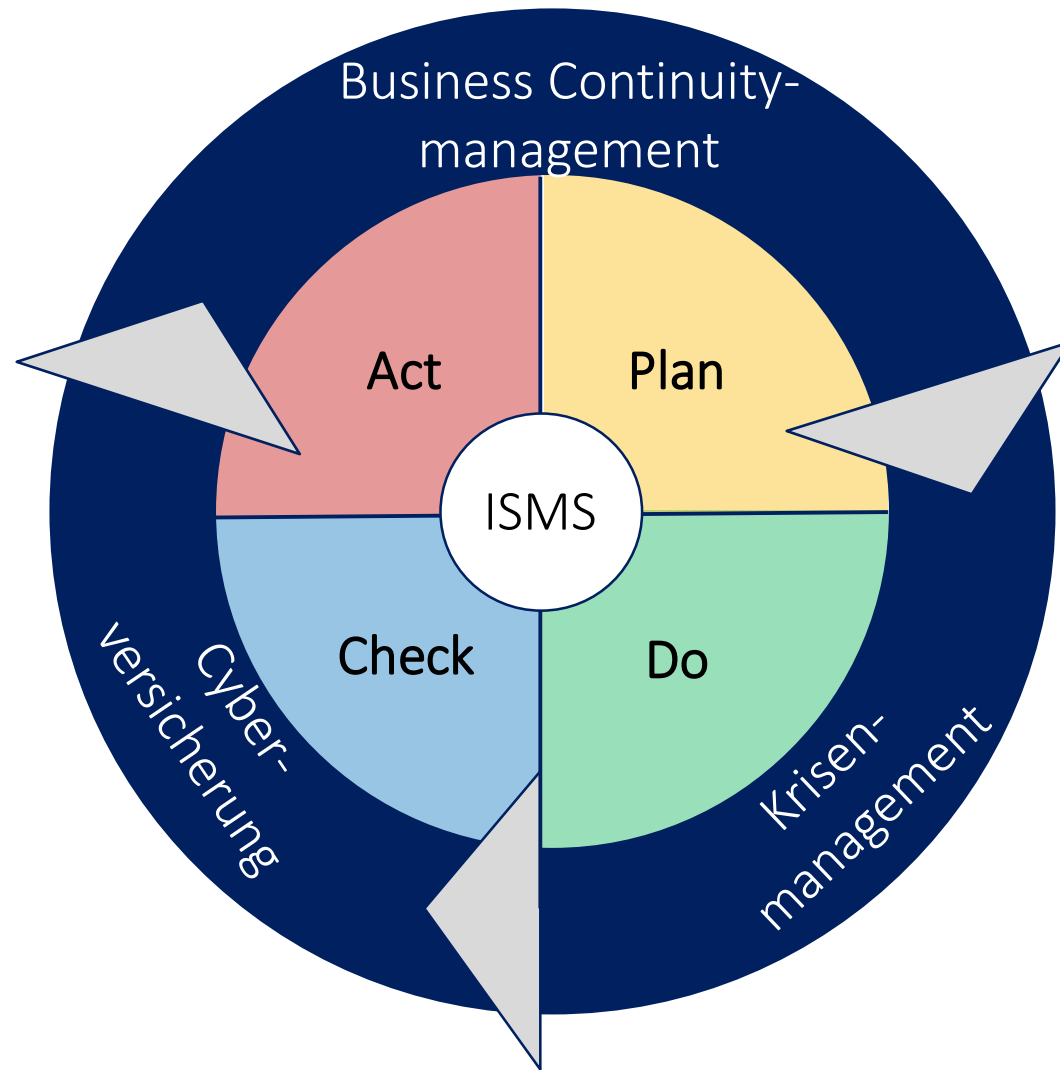


# Datenschutz vs Datensicherheit

- Bedeutung der IT-Sicherheit für datenschutzrechtlich verantwortliche Stelle
- Beide Sichtweisen müssen für Entscheider beachtet werden, das eine ergibt aber nicht immer das andere in vollständig
- Informatiker und Techies mit Juristen zusammenbringen
  
- Nehmen wir uns ein Beispiel:
  - Luca-App



# Digitale Selbstverteidigung für KMU auf Basis BSI IT-Grundschutz



# Cyber-Sicherheit für KMU

(Die TOP 14 Fragen)

Frage 1: Wer ist verantwortlich?

Frage 2: Wie gut kennen Sie Ihre IT-Systeme?

Frage 3: Führen Sie regelmässig eine Datensicherung durch?

Frage 4: Spielen Sie regelmässig Updates ein?

Frage 5: Haben Sie Makros deaktiviert?

Frage 6: Verwenden Sie Virenschutzprogramme?

Frage 7: Haben Sie eine Richtlinie für sichere Passwörter festgelegt?

Frage 8: Haben Sie eine Firewall eingerichtet?



Cyber-Sicherheit  
für KMU

Die TOP 14 Fragen



# Cyber-Sicherheit für KMU

(Die TOP 14 Fragen)

Frage 9: Wie sichern Sie Ihre Mailaccounts ab?

Frage 10: Wie trennen Sie unterschiedliche IT-Bereiche?

Frage 11: Haben Sie IT-Risiken im Homeoffice und bei Geschäftsreisen im Griff?

Frage 12: Wie informieren Sie sich? Wie sensibilisieren Sie Ihre Mitarbeiter?

Frage 13: Deckt Ihre Versicherungspolice auch Cyber-Risiken ab?

Frage 14: Wissen Sie, wie Sie bei einem Cyber-Angriff reagieren müssen?



Cyber-Sicherheit  
für KMU

Die TOP 14 Fragen

# Backup!

Habt ihr ein Backup erstellt?

Ist es frisch oder fermentiert es vor sich hin?

Habt ihr das sogar Offline vorliegen?

Habt ihr mal die Wiederherstellung getestet?

Braucht das Wiedereinspielen viel zu lang?

Denkt dran:

Cloud Speicher ist kein Backup!



# Weiterführende Link Empfehlungen

- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

Informationen und Hilfestellungen für KMU

- [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html)

Informationssicherheit für kleine und mittelständische Unternehmen (KMU)

- [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Grundschutz-Profil/it-grundschutz-profile\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Grundschutz-Profil/it-grundschutz-profile_node.html)

BSI Newsletter für KMU

- [https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Newsletter-bestellen/newsletter-bestellen\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Newsletter-bestellen/newsletter-bestellen_node.html)

# Weiterführende Link Empfehlungen

- **Allianz für Cyber-Sicherheit (ACS)**
  - [https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/topservice\\_hidden\\_node.html](https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/topservice_hidden_node.html)
- **Cyber Security Cluster Bonn (CSCB)**
  - Cyber-Sicher im Home Office  
<https://cyber-security-cluster.eu/de/aktuelles/sicher-home-office.html>
  - Cyber-Sicher durch die Krise  
<https://cyber-security-cluster.eu/de/leistungen/veroeffentlichungen.html>
- **Linus Neumann**
  - CCC Congress 36C3 “Hirne Hacken”  
<https://www.youtube.com/watch?v=BreKdM7CKnY>

Und wenn alles nicht hilft gegen den Wahnsinn?



# Irgendwas mit Holz?

# Kokosnusspflücker!

[www.kokosnusspfluecker.de](http://www.kokosnusspfluecker.de)

