# Leben am Limit

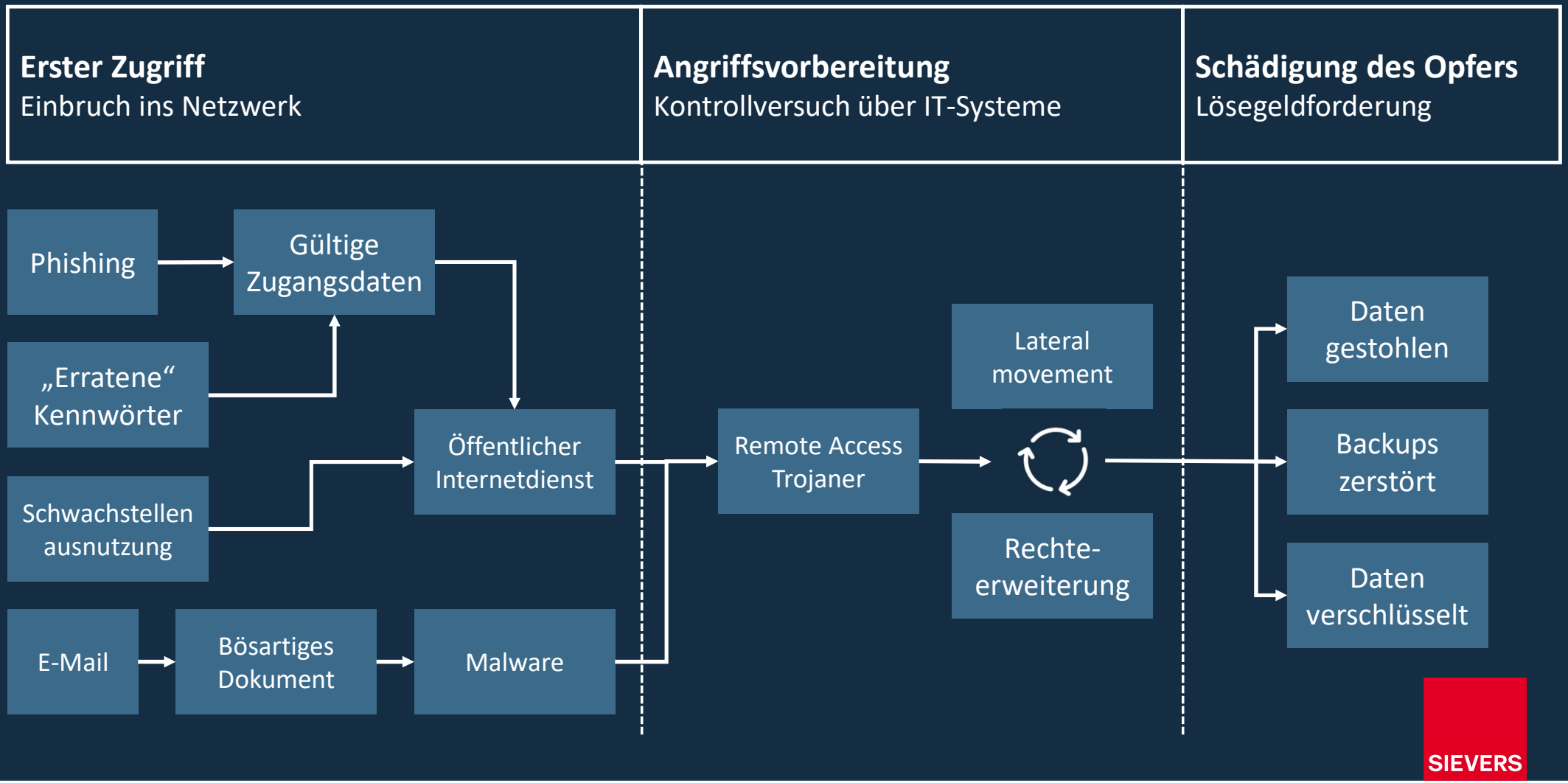
## 10 Tipps

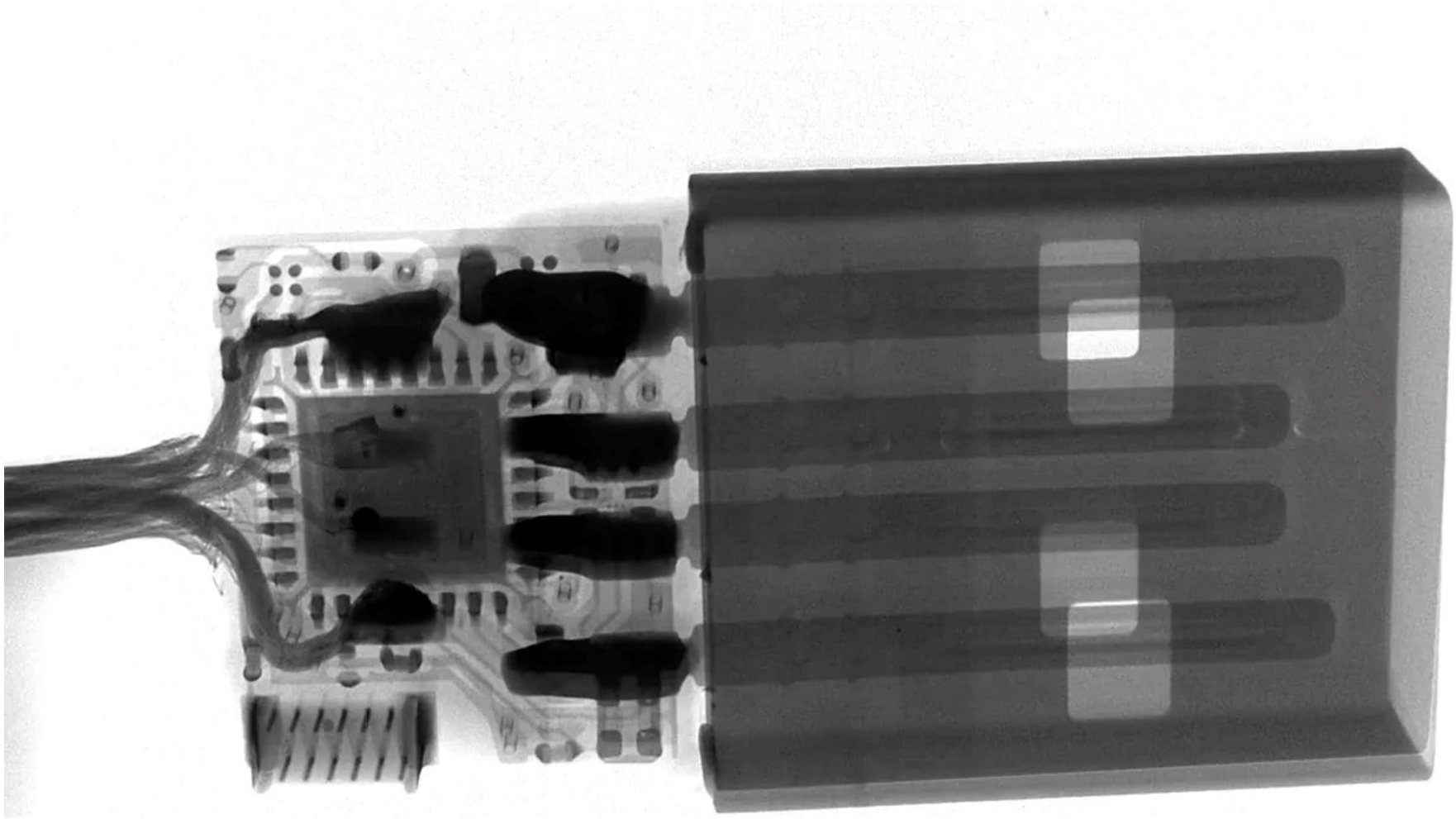
by Stefan Ohlmeyer

SIEVERS


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
30/10/2023 00:30:55
Time Left
02:23:57:37
Your files will be lost on
31/10/2023 04:50:20
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
bitcoin
ACCEPTED HERE
Send €500.000 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

# Wie kommt es dazu?





SIEVERS

# Leben am Limit

## 10 Tipps

by Stefan Ohlmeyer

SIEVERS

# Platz 10:

## Fluide Notfallpläne

+ Es wissen ja alle was im Notfall zu tun ist
+ Ist doch nur ein Papiertiger

# Oder so:

Auf wesentliche Vorfälle vorbereitet sein

+ Was ist überhaupt ein Notfall? Und wer entscheidet darüber?
+ Wer ist im Krisenstab und wie kommt dieser zusammen?
+ Wer ist noch zu informieren und wie erreiche die?
+ Bekomme ich Hilfe?
+ Wiederanlauf / Wiederherstellung -> Wie konkret?
+ Üben
+ Verbessern
+ Üben
+ Verbessern
+ Üben

SIEVERS

# Platz 9: Sein sie naiv!

+Alle Menschen sind gut!

+Uns wird es schon nicht treffen!

+Wir sind für Hacker gar nicht interessant!

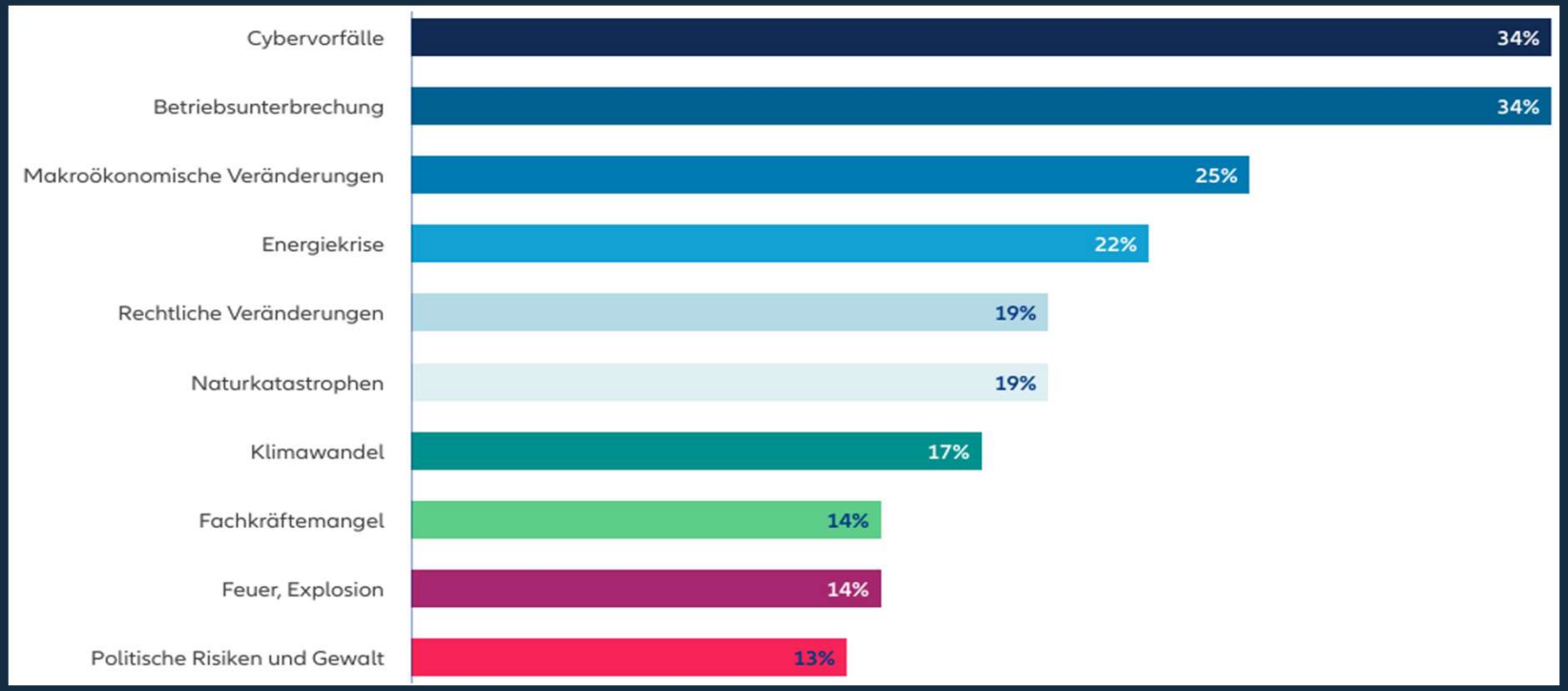
+Wir haben immer Glück!

SIEVERS

# Oder so: Seien Sie realistisch!

## Nehmen Sie Ihre Verantwortung ernst

## Wichtigste Geschäftsrisiken:



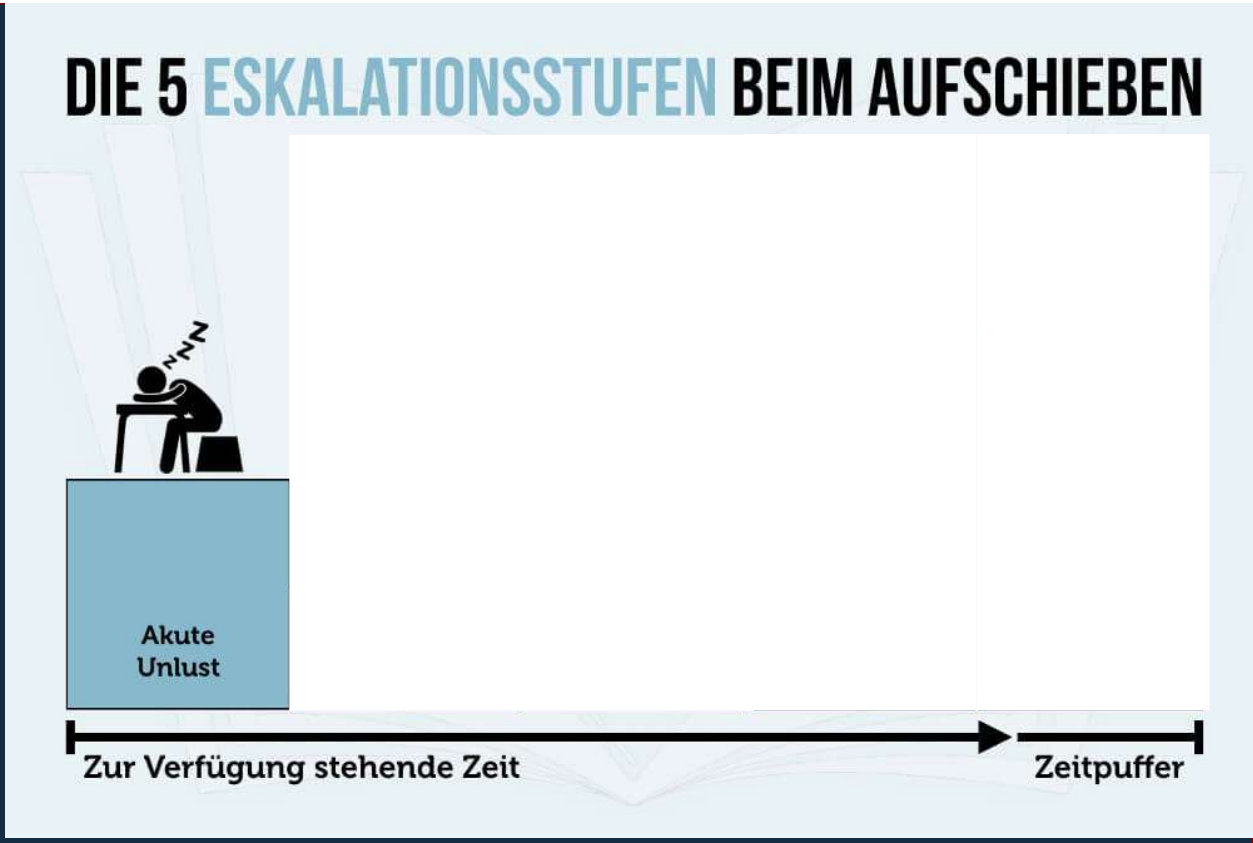

Quelle: Allianz Global Corporate & Specialty
Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.

SIEVERS

# Platz 8: Prokrastination

Was Du heute kannst verschieben, das kann auch noch bis morgen liegen!

+ Wir haben gerade sooo viele „wichtige“ Projekte!
+ Das Budget müssen wir schieben!




SIEVERS

# Oder so: Prokrastination entgegenwirken

+ Wie isst man einen Elefanten?
+ Input von Externen holen. Eine andere Perspektive bringt Schwung rein.
+ Priorisieren – zuerst ran an die unangenehmen, dringenden Arbeitsbrocken, damit das Denken nicht mehr blockiert ist.

# Platz 7:
# Schwarz-weiß Denken

Es gibt kein „Dazwischen“

+ Alles in die Cloud, dann brauch ich mich nicht darum kümmern und ist viel billiger!

+ Early Adaptor! – Neu ist IMMER besser! ☺

+ Modern Work, BYOD, FlexiOffice!

+ Alles selber hosten, das ist viel sicherer und billiger! Die Cloud ist böse!

+ Alles bleibt wie es ist und früher war sowieso ALLES besser!

+ Privatnutzung?! – Auf keinen Fall!

# Oder so: Es gibt mindestens 256 Graustufen

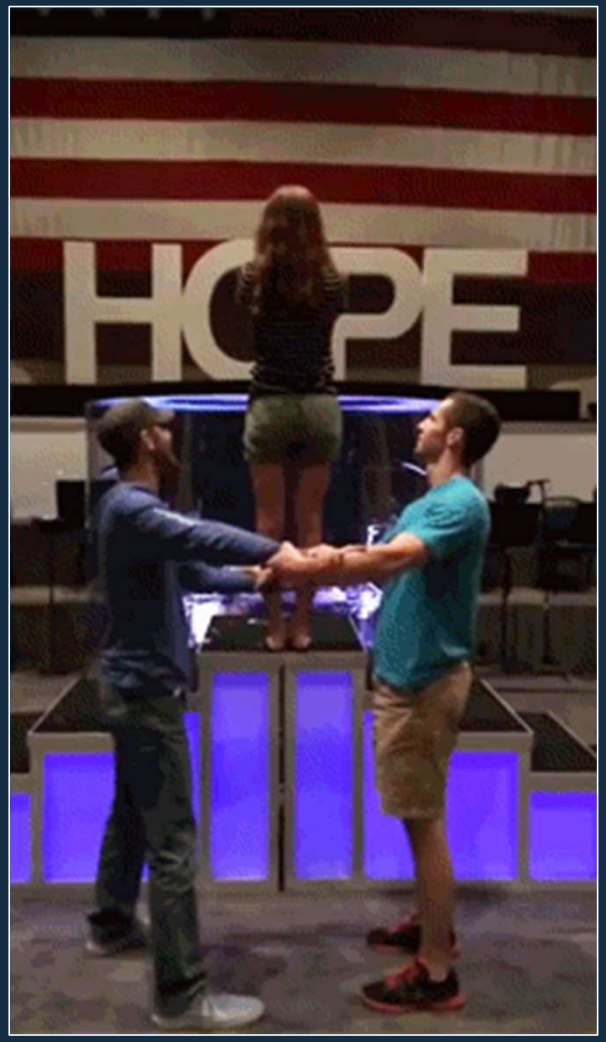
+ Berücksichtigen Sie unterschiedliche Perspektiven (GF / IT / Vertrieb / Mitarbeiter / DSB..).

+ Analysieren und behandeln Sie die jeweiligen Chancen und Risiken.

+ Gehen Sie auch mal Kompromisse ein.

# Platz 6: Verlassen Sie sich auf andere!

+ Mein Provider wird sich schon um die Datensicherung kümmern.
+ Wenn es ein wichtiges Software-Update gibt, dann werden **die** mich schon informieren!
+ Wenn es eine gesetzliche Änderung gibt, wird mich unsere Regierung schon informieren.




SIEVERS

# Oder so:

+ Etablieren Sie einen systematischen Prozess (mit klaren Verantwortlichkeiten), um über relevante:
  + aktuelle Schwachstellen
  + Bedrohungen
  + und geänderte Gesetze / Normen informiert zu sein.

+ Steuern Sie Dienstleister & Cloud Provider möglichst aktiv und legen Sie **IHRE** Anforderungen vertraglich fest. (Entscheidungskriterium)

SIEVERS

# Platz 5: Never touch a running System


SIEVERS

# Oder so: Touch it!

Pseudo-Anglizismus: Never touch / change  a running System

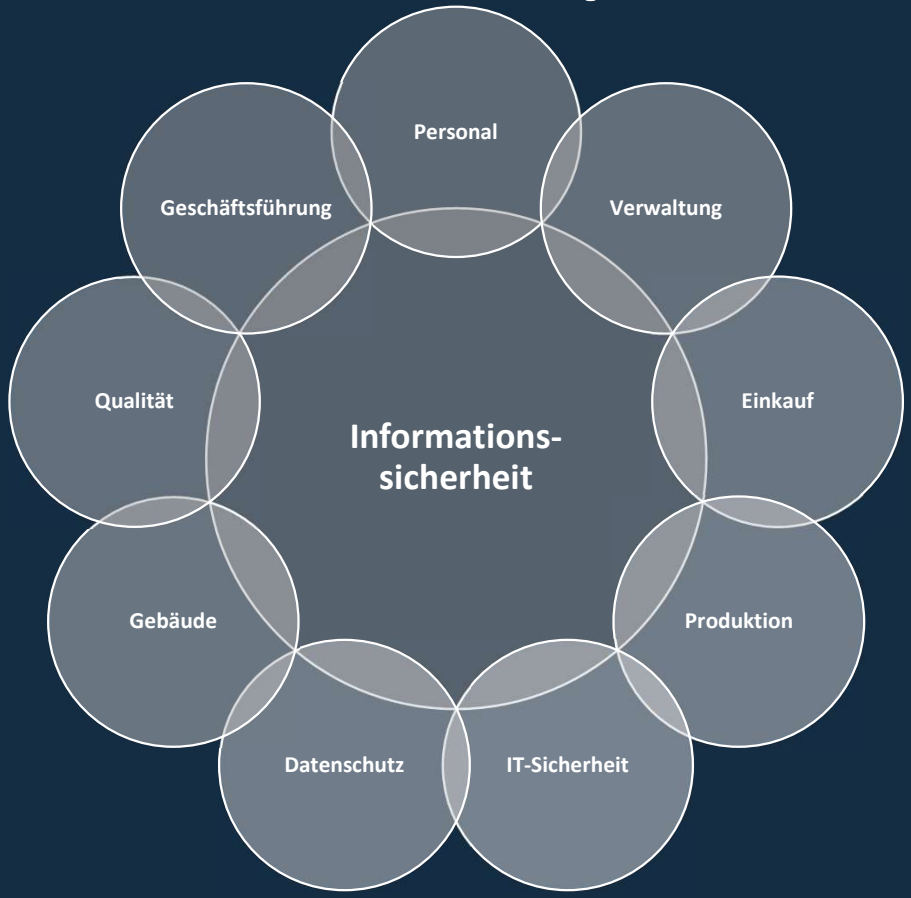
+ Bedeutet eigentlich: **Wartungsfenster** und nicht „nicht patchen“!
+ Erarbeiten Sie ein **Konzept** für das Patchmanagement – Auch ungeliebte IT-Systeme müssen betrachtet werden!

SIEVERS

# Platz 4: Informationssicherheit betrifft ausschließlich die „IT-Abteilung“!

SIEVERS

# Oder so:
# Informationssicherheit interdisziplinär betrachten




SIEVERS

# Platz 3: Die Annahme, die Wiederherstellung von Datensicherungen wird schon funktionieren!

+ Test einer Wiederherstellung ist Zeitverschwendung.
+ Wer testet ist feige!
+ Wir müssen ja sowieso immer mal wieder was wiederherstellen und das funktioniert doch!

+ Fallschirm? – Braucht kein Mensch.

SIEVERS

# Oder so: Testen Sie regelmäßig…

…und entwickeln Sie die Datensicherung weiter. (insbesondere die Resilienz)

SIEVERS

# Platz 2: Klären Sie bloß keine Verantwortlichkeiten!

+ Bei uns weiß jeder wofür er/sie verantwortlich ist,
+ und welche Aufgaben zu erledigen sind.
+ Außerdem ist jedem klar, welche Ressourcen / Spielräume dafür zur Verfügung stehen.
+ Und wenn nicht, ist im Zweifel Herbert verantwortlich die Aufgabe zu erledigen!
+ Es gibt immer einen „Herbert“!


SIEVERS

# Oder so: Organisieren sie die Informationssicherheit

+ Weisen sie Verantwortlichkeiten und damit verbundene Aufgaben eindeutig zu.
+ Definieren Sie welche Ziele erreicht werden sollen.
+ Stellen Sie klar, welche Ressourcen zu Verfügung stehen um die Verantwortlichkeit wahrzunehmen.

+ Klären sie, wer die Verantwortlichkeiten kontrolliert.

SIEVERS

# Platz 1

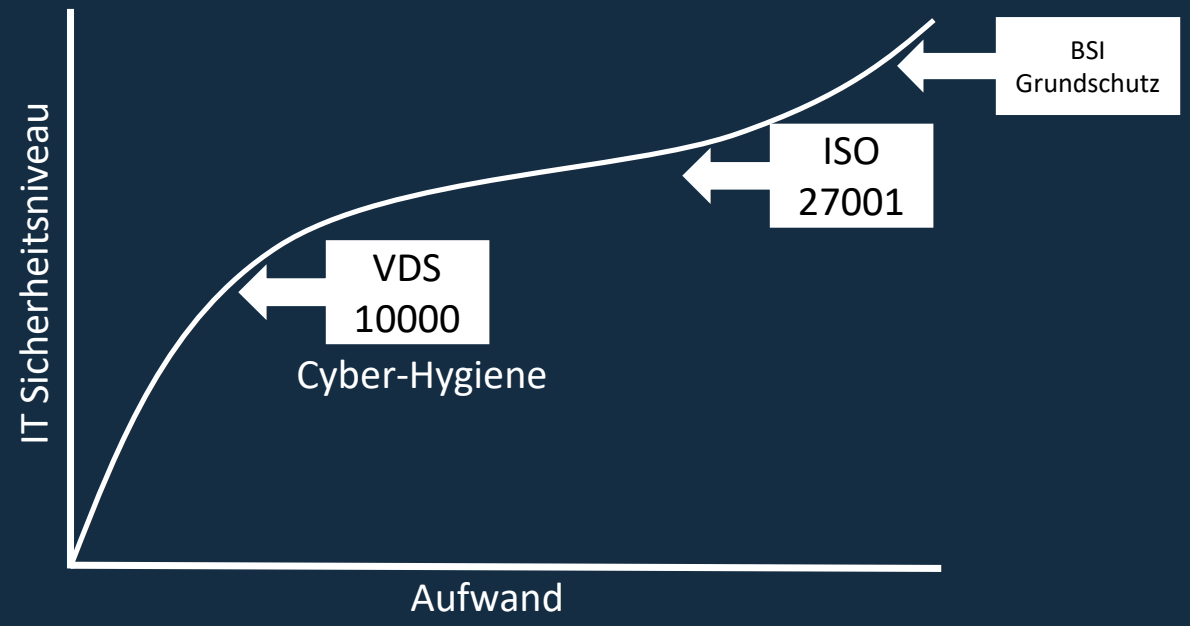
SIEVERS


寅生威
常開


NAC
SDN
DDoS Protection
DNS Security
Network Firewall
SASE
Deception
Network Analysis & Forensics
Endpoint Detection & Response
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Risk Quantification
Pen Testing & Breach Simulation
CRC
Security Awareness & Training
Security Operations & Incident Response
SIEM
Security Incident Response
Security Analytics
SIEVERS GROUP
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting & Services
Blockchain
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB

# Oder so: Orientieren Sie sich an einem Standard

Aber an welchem?




SIEVERS

# Vielen Dank!

**Stefan Ohlmeyer**
Team-Lead ISMS

VdS •Berater für Cyber-Security

TÜV NORD Information Security Officer

Allianz für Cyber-Sicherheit

**SIEVERS-SNC Computer & Software GmbH & Co. KG**

Hans-Wunderlich-Straße 8
49078 Osnabrück

T +49 541 9493-160

sohlmeyer@sievers-group.com

www.sievers-group.com

SIEVERS