



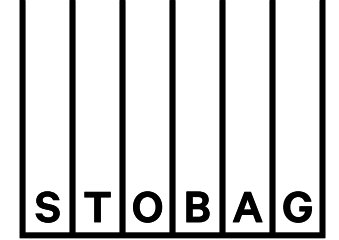
S T O B A G



GEMEINSAM LEBENSÄÄUÄME
WERTVOLLER GESTALTEN.

STOBAG SONNEN- & WETTERSCHUTZ.

BREITES PORTFOLIO IN 3 KERNSEGMENTEN.



SENKRECHT

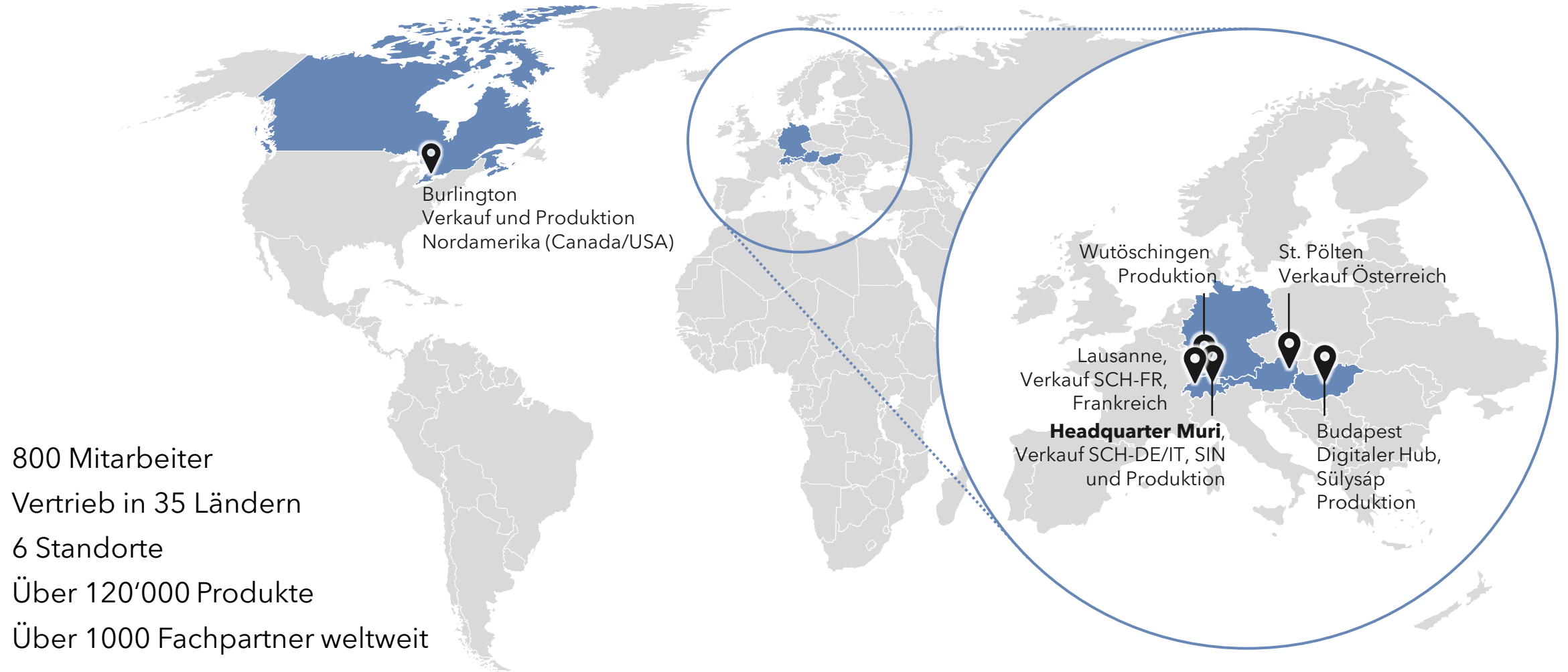


KLASSISCHE MARKISEN



OUTDOOR-LIVING

INTERNATIONALE PRÄSENZ MIT FOKUS AUF EUROPA UND AMERICAS.



800 Mitarbeiter
Vertrieb in 35 Ländern
6 Standorte
Über 120'000 Produkte
Über 1000 Fachpartner weltweit

LOSGRÖSSE 1

STOBAG

HILFE!
WIR WURDEN
GEHACKT

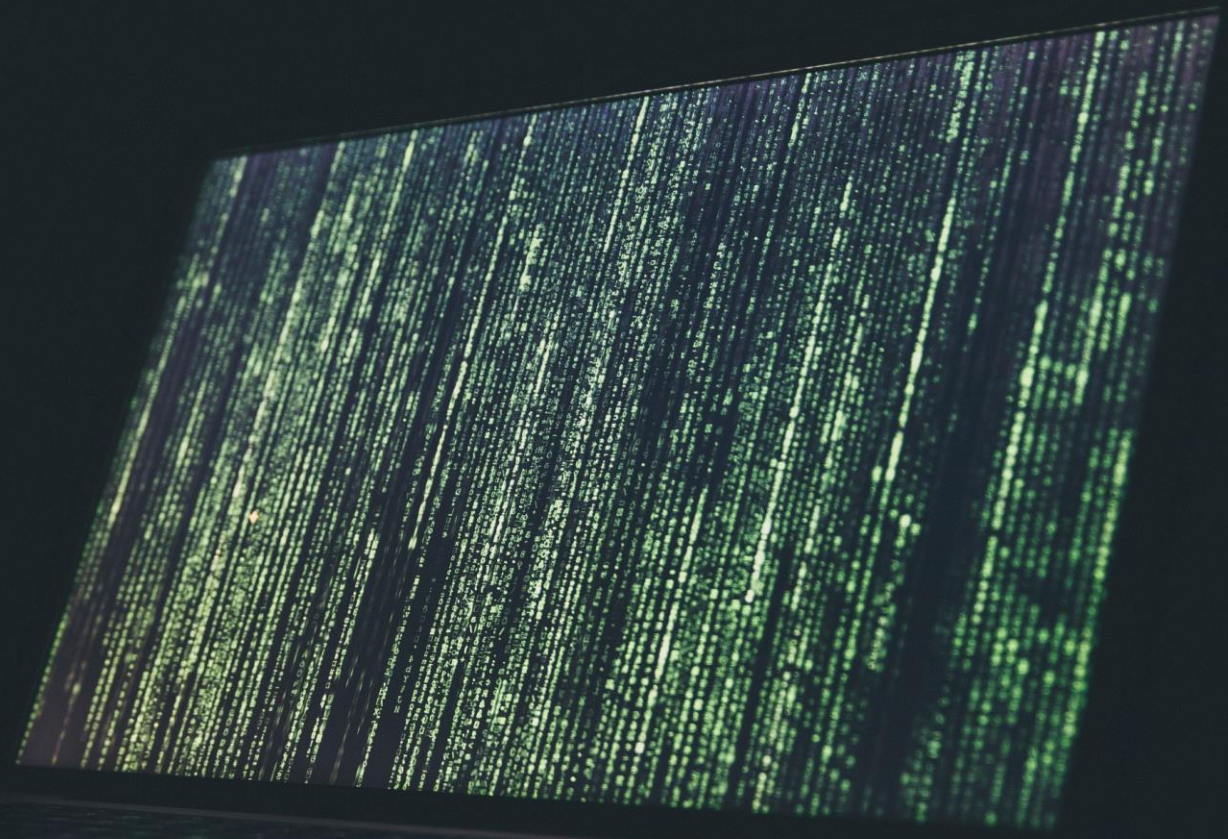
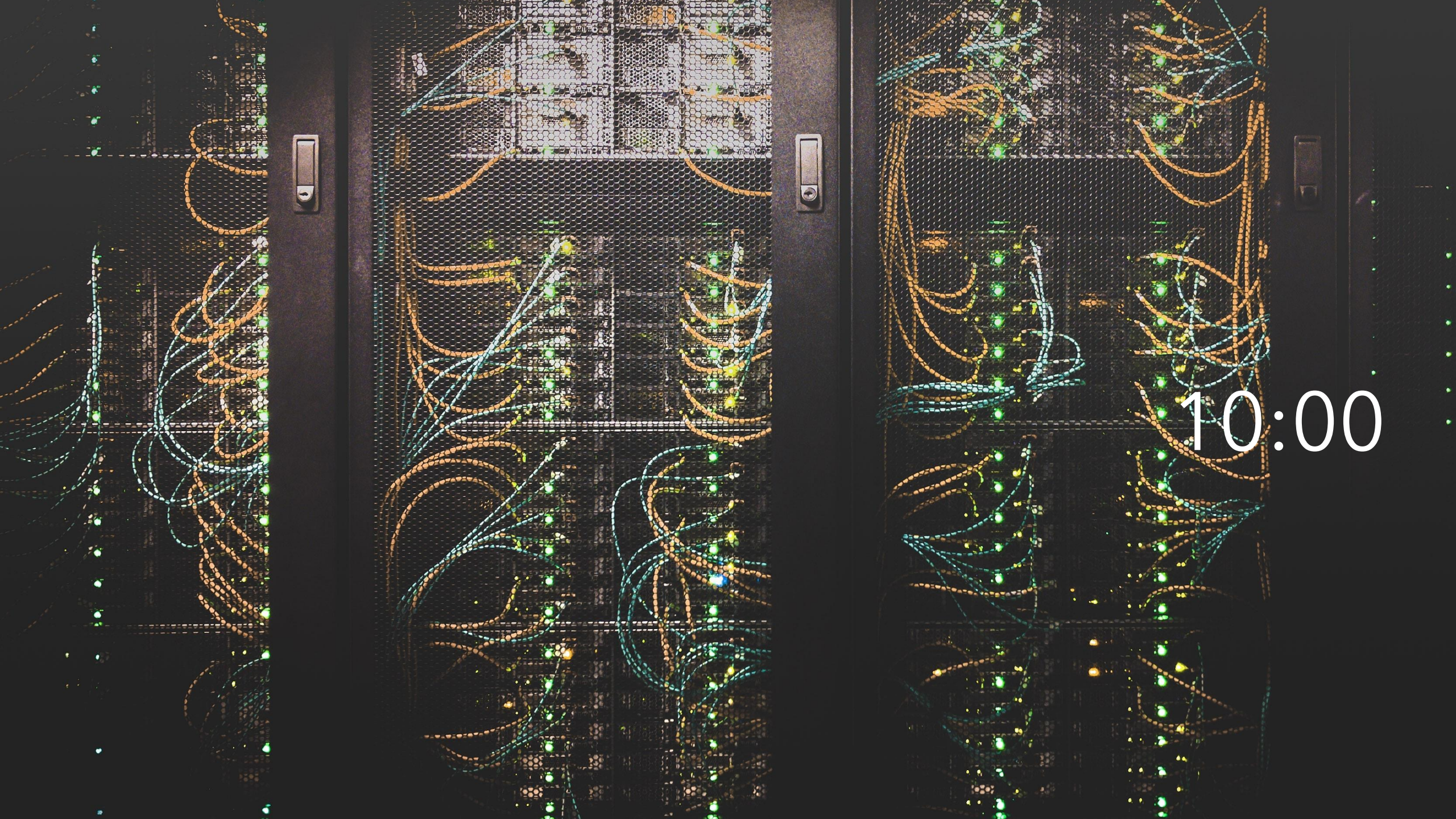


Photo by [Markus Spiske](#) on [Unsplash](#)



MO, 28.10.2019 - 06:30



10:00

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN – files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
DO NOT use any recovery software with restoring files overwriting encrypted.
This may lead to the impossibility of recovery of the certain files.

11:00

To get info (decrypt your files) contact us at your personal page:

1. Download and install Tor Browser: <https://www.torproject.org/download/>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar:

<http://q7wp5u55lhtuafjtsl6lkt24z4wvon2jexfzhzqqfrt3bqnpqboyqoid.onion/order/e334>

4. Follow the instructions on the site
5. You should get in contact in 48 HOURS since your systems been infected.
6. The link above is valid for 21 days.
After that period if you not get in contact link and the key for your data
would be erased completely.
7. Questions? e-mail: JosephAtkins@protonmail.com
If email not working – new one you can find on a tor page.

WORST CASE SZENARIO



2 Wochen
Stillstand

1 Woche
Datenverlust

14:00

Prio

0

1

APP
DC/DHCP/DNS

iwacs

D: KLUG FOLDER 'DRIVE'
MAYBE OOD

ENVIRONMENT VARIABLES: -JAVA_HOME
-JAVA_PATH

ACCESS For A. Tunnings when

2

SAP - DATABASE
ERP

MSSQL EITHER BACKUP
OR MSSQL LIVE

3

parallel

Mail -0365
• OVERNIGHT

4 3

Fileserver
• OVERNIGHT

5

R+D (CAD/PDM)

6 1

DEPLOYMENT.

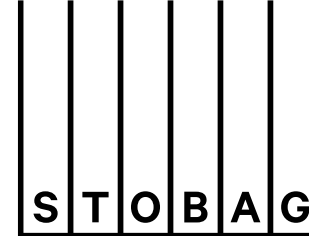
7 2

SQL

SIAM Server (A. Tunnings)

4

Webshop



17:00

LEARNING I: OFFEN KOMMUNIZIEREN

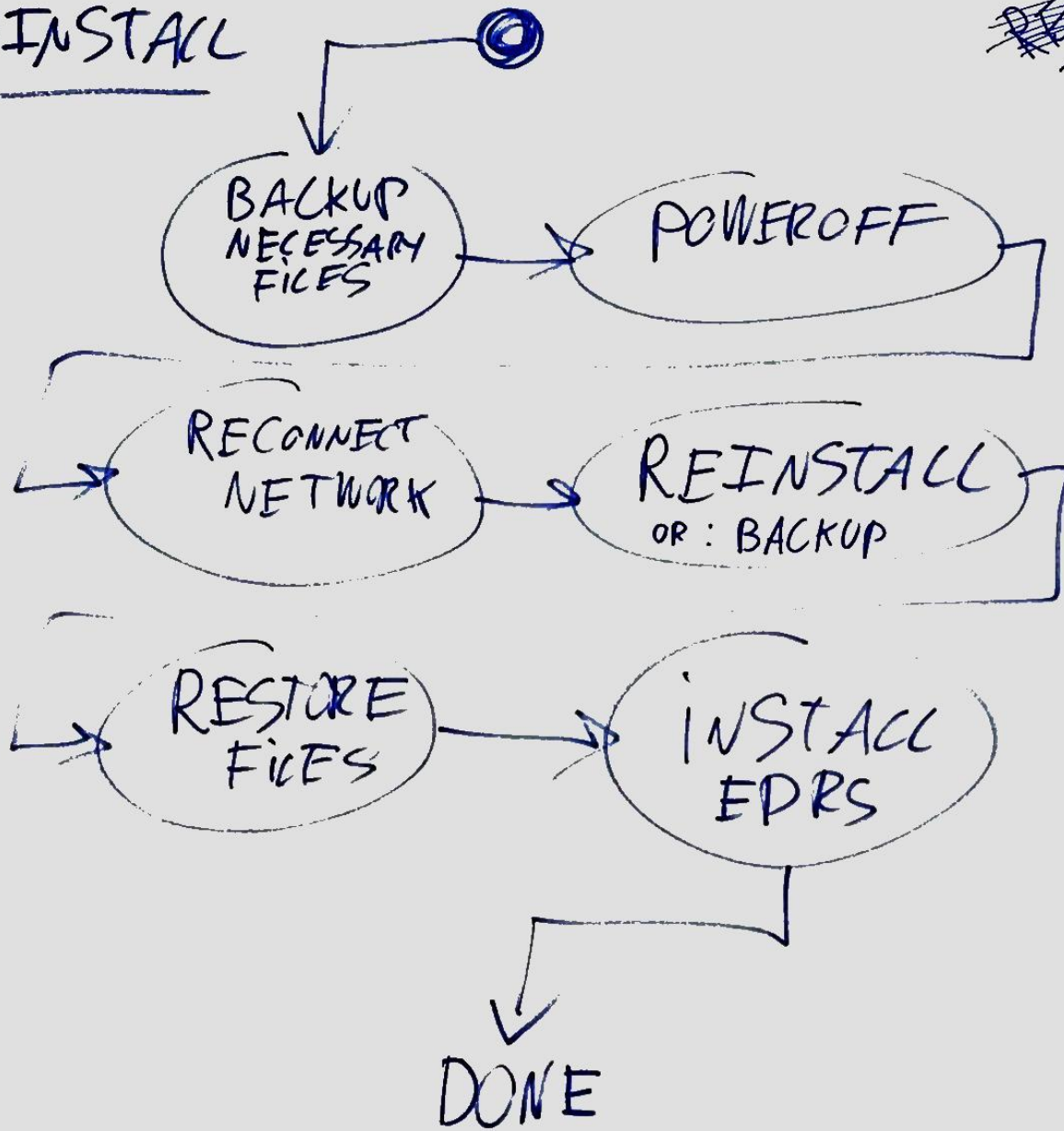
S T O B A G



STOBAG

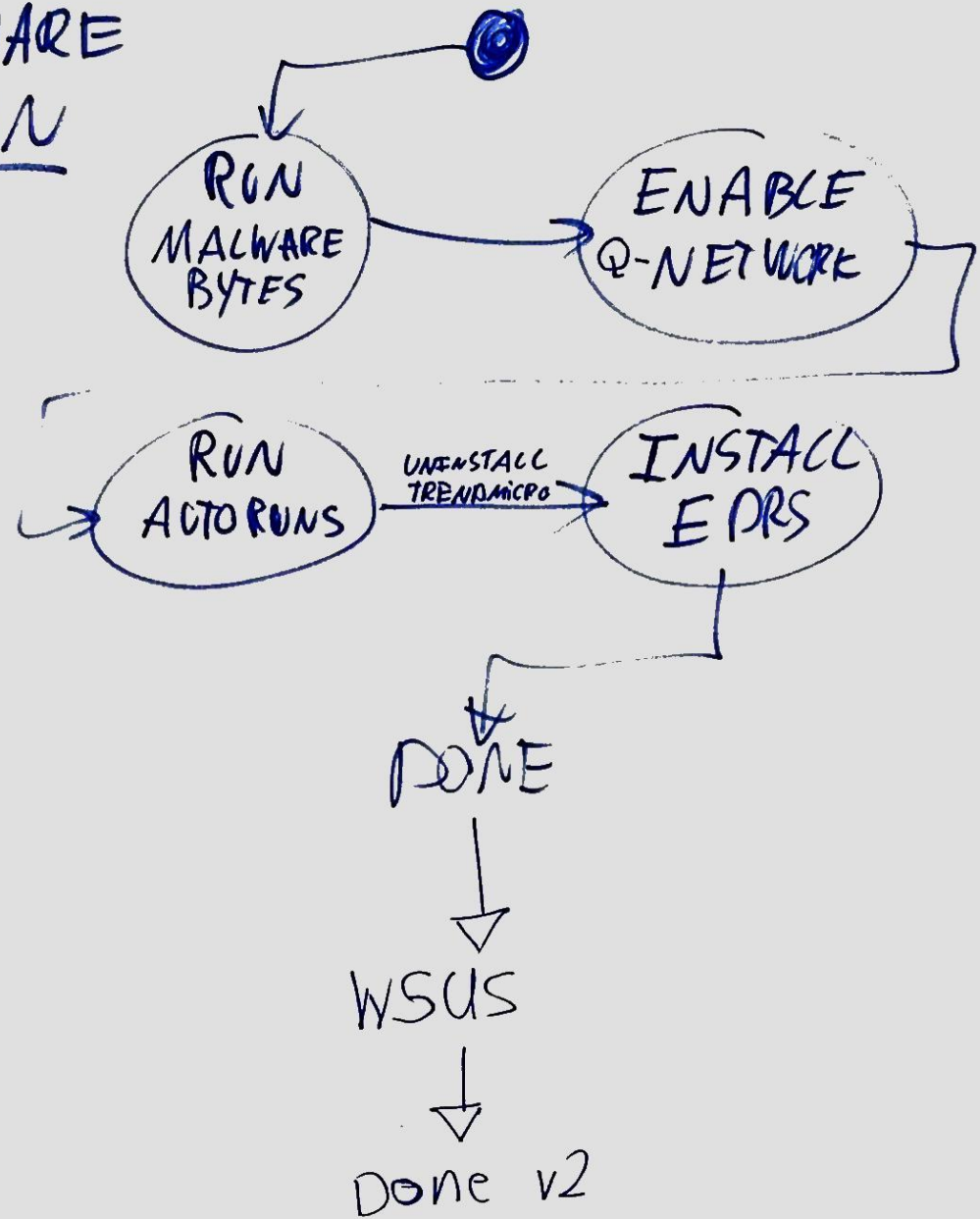


REINSTALL



~~RE~~

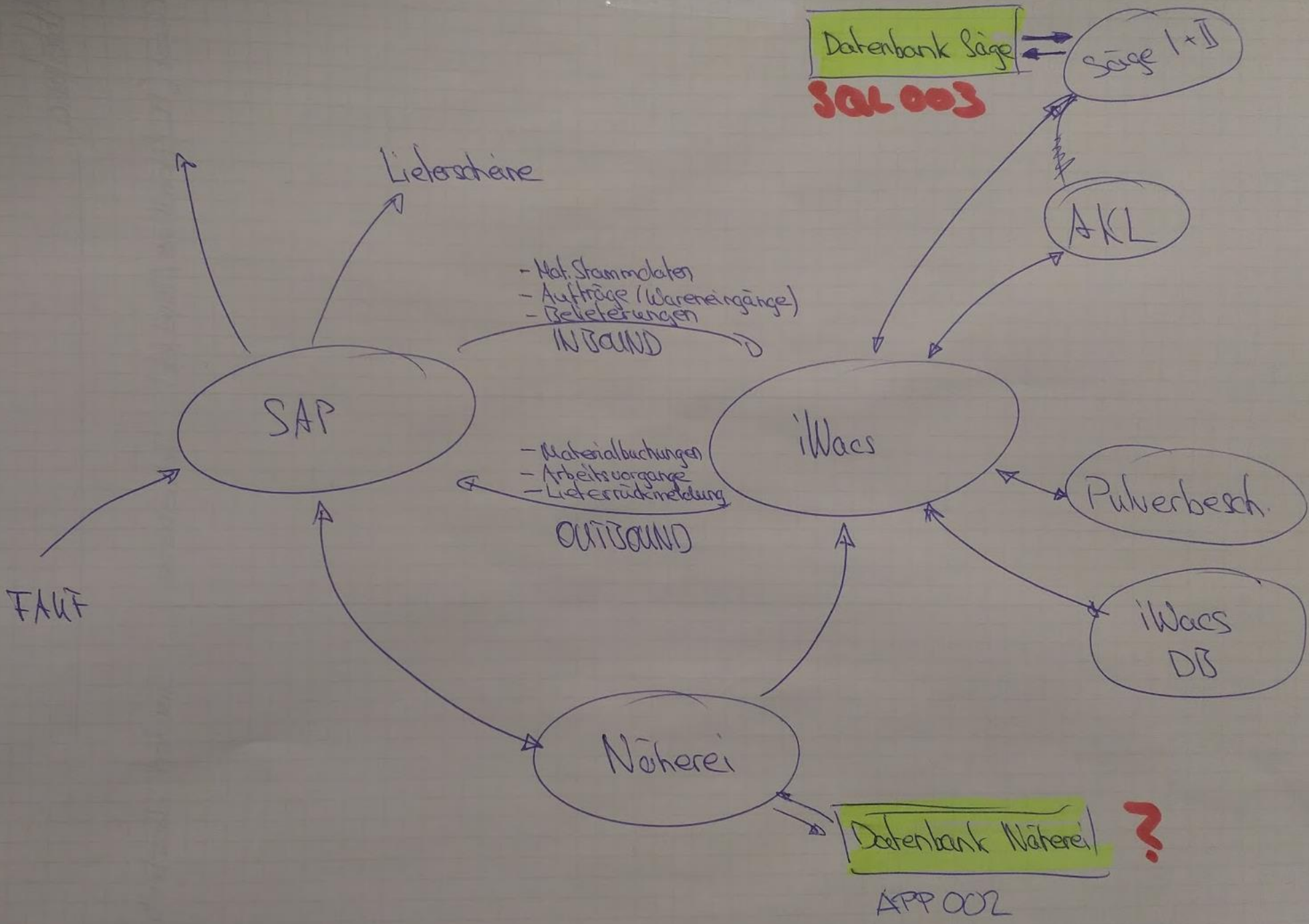
MALWARE SCAN



LEARNING II:
DIE SPEZIALISTEN IN RUHE
ARBEITEN LASSEN

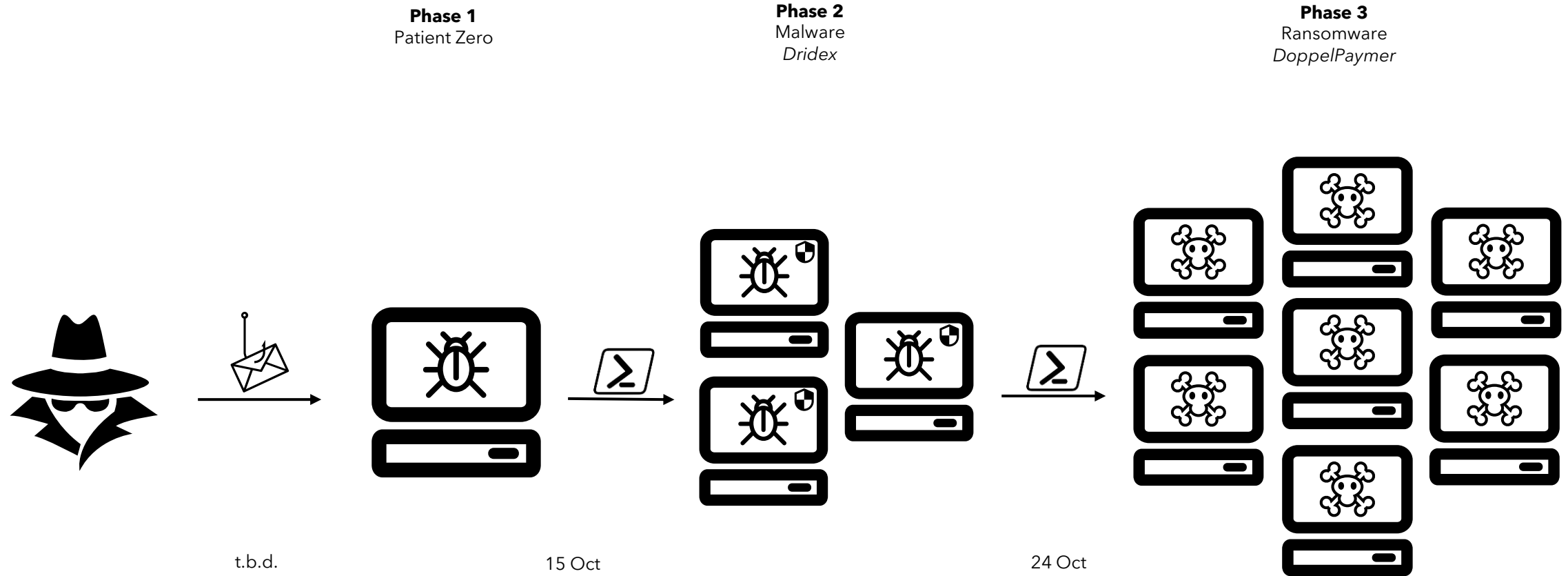


LEARNING III:
GUTE PARTNER SIND GOLD
WERT

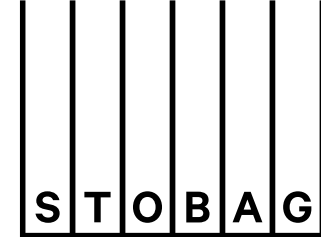


URSACHE

S	T	O	B	A	G
---	---	---	---	---	---



LEARNING IV: EINEN PLAN HABEN



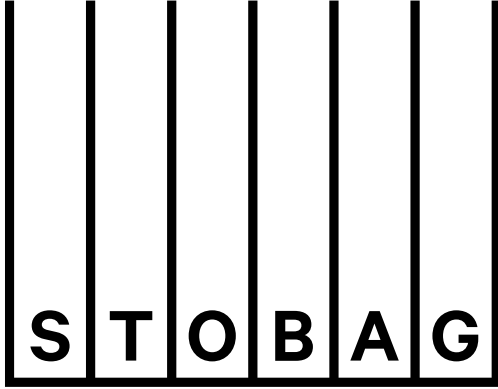


Daniel Fiechter

Group CIO
Executive Board Member

daniel.fiechter@stobag.com
+41 79 213 77 21





VIELEN DANK

ProCloud, 25. Oktober 2022