# Physical Red Teaming

## #48 OWASP Stammtisch Frankfurt

28.04.2021 - Mihael Stanojevic

# Who am I



## Mihael Stanojevic

- ISO27001 Lead Auditor / Lead Implementer, CISSP, red team, white hat, (physical-) pentester

- Over 15 years of Security experience, ~10 years Banking Security experience

- Stands obviously in a museum in Norway

# Overview

What is physical security and how it
relates to ISO 27001

# Common issues  / Examples

"Oh, we have to lock that door?"
How to attack the home office?

# How to fix the issues

Why every measure counts
Don't trust anyone - Raise awareness

# What is physical security and how it relates to ISO 27001

## Secure Areas

### Annex A.11.1 - Objectives

Prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

### Controls

A.11.1.1 Physical Security Perimeter
A.11.1.2 Physical Entry Controls
A.11.1.3 Securing Offices, Rooms and Facilities
A.11.1.4 Protecting against External & Environmental Threats
A.11.1.5 Working in Secure Areas

## Equipment Security

### Annex A.11.2 - Objectives

Prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations

### Controls

A.11.2.1 Equipment Siting & Protection
A.11.2.2 Supporting Utilities
A.11.2.3 Cabling Security
A.11.2.4 Equipment Maintenance
A.11.1.5 Working in Secure Areas
…
A.11.2.8 Unattended User Equipment
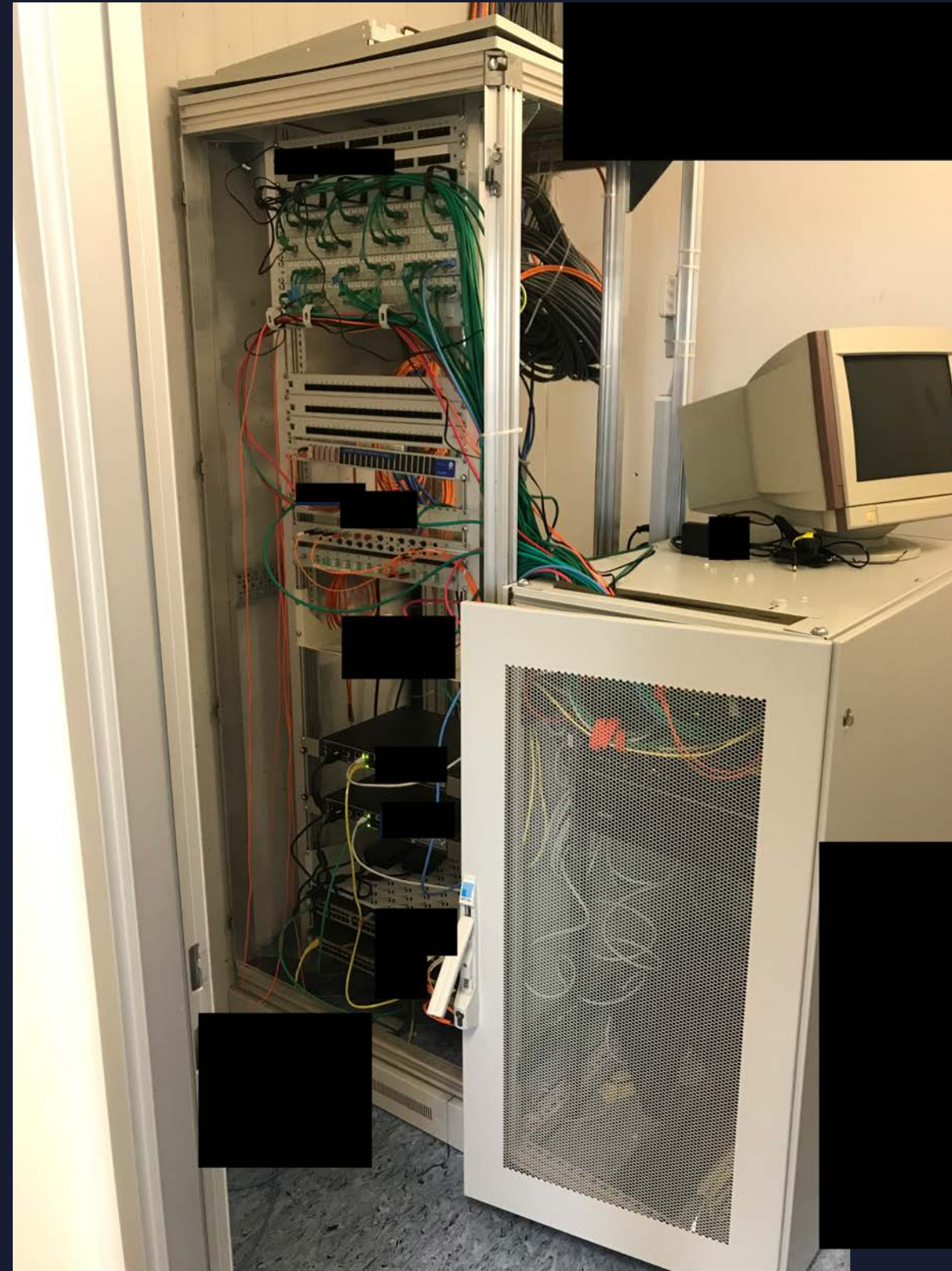…

# "Oh, we have to lock that door?" – Common issues
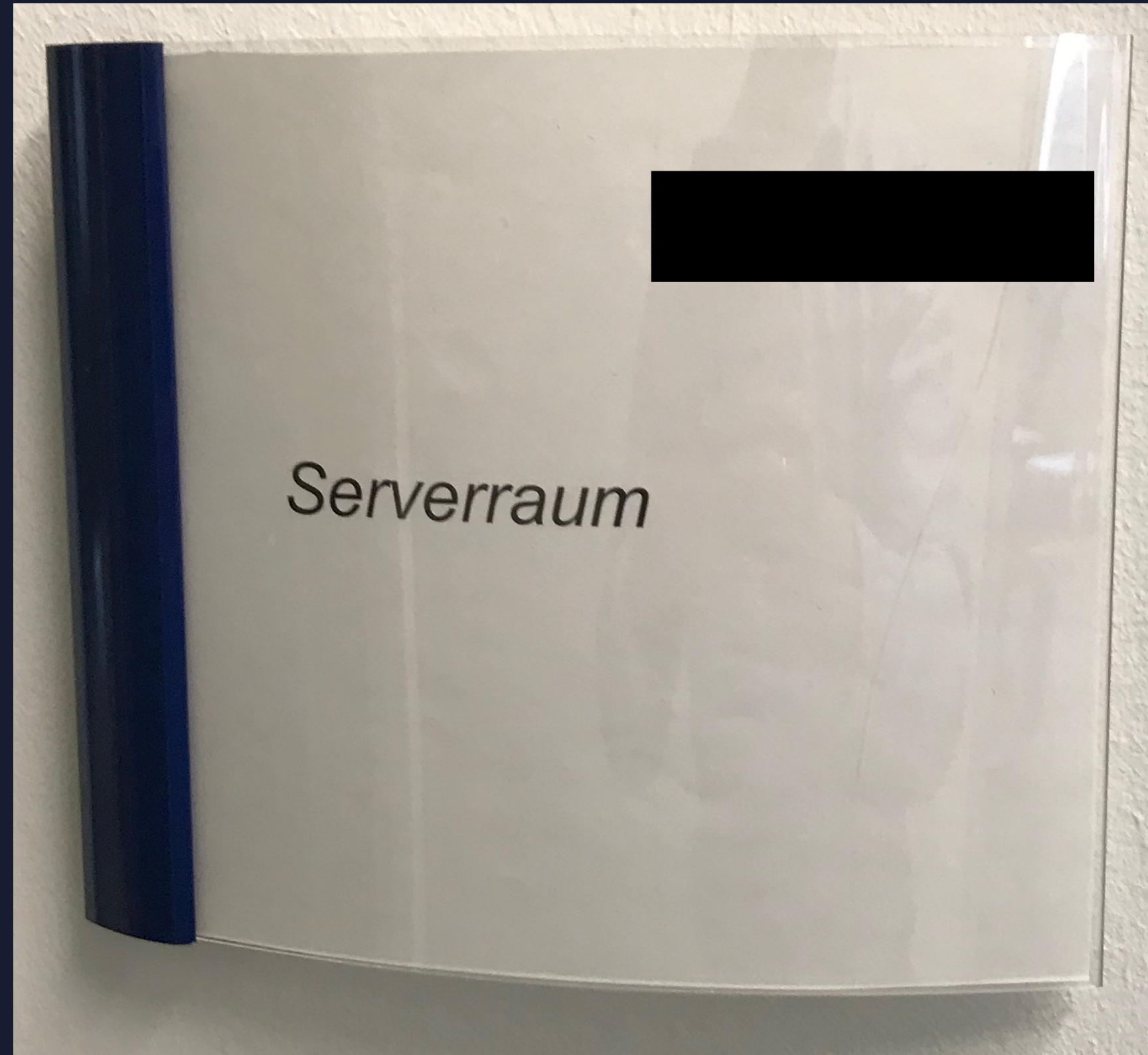
# "Oh, we have to lock that door?" – Common issues

# "Oh, we have to lock that door?" – Common issues

# "Oh, we have to lock that door?" – Common issues

# "Oh, we have to lock that door?" – Common issues

# ”Oh, we have to lock that door?” – Common issues

# How to attack the home office?

## Insecure infrastructure

- Unmanaged infrastructure
- Unknown Devices
- Rogue access point -> POC

## Unsafe environment

- Untrained People around you
- Kids and Pets
- Theft risk

# How to fix the issues

## Every measure counts

Breaches are caused by the concatenation of many small things

## Don't be gullible

Do not open doors for anyone if you do not know them

## Protect

Lock your assets if you do not use them

## Keep your eyes open

If you see something – say something!

THANK YOU!