# House of Br1cks

LIMES
SECURITY

# Initial Situation

**Complete loss of control of the building automation system**

- No operation of light
- No operation of heating and ventilation
- No operation of shutters
- Even dentist’s equipment failed due to missing compressed air

# Initial Situation

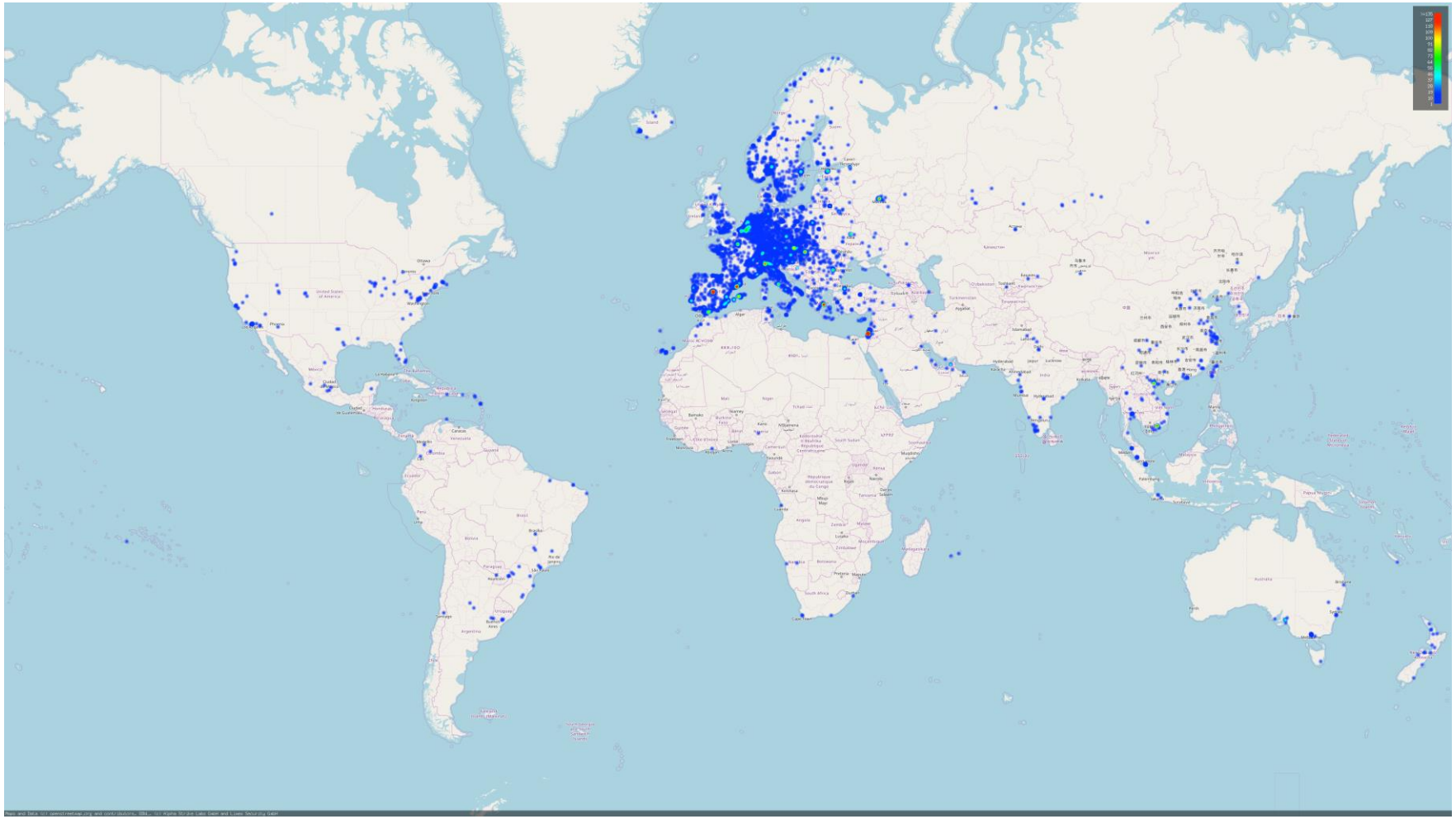
LIMES SECURITY

| | |
|---|---|
| **The Good** | The programming for the components was still available |
| **The Bad** | The building contained hundreds of KNX actuators and more than 75% of them were no longer operational |
| **The Ugly** | All contacted vendors considered the devices bricked and recommended replacing the components → costs >100K $ |

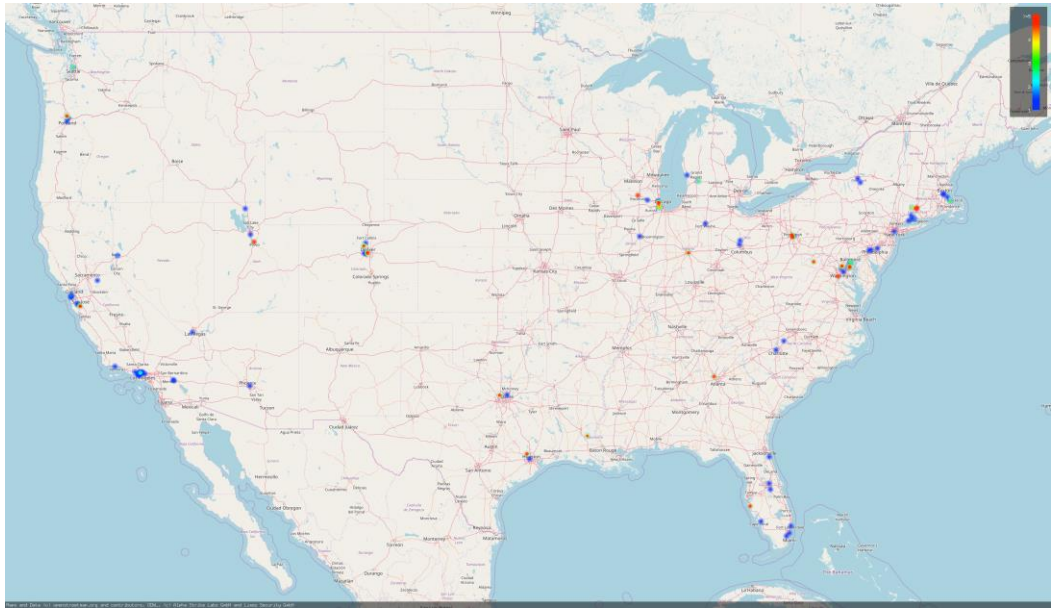
# Building Automation with KNX

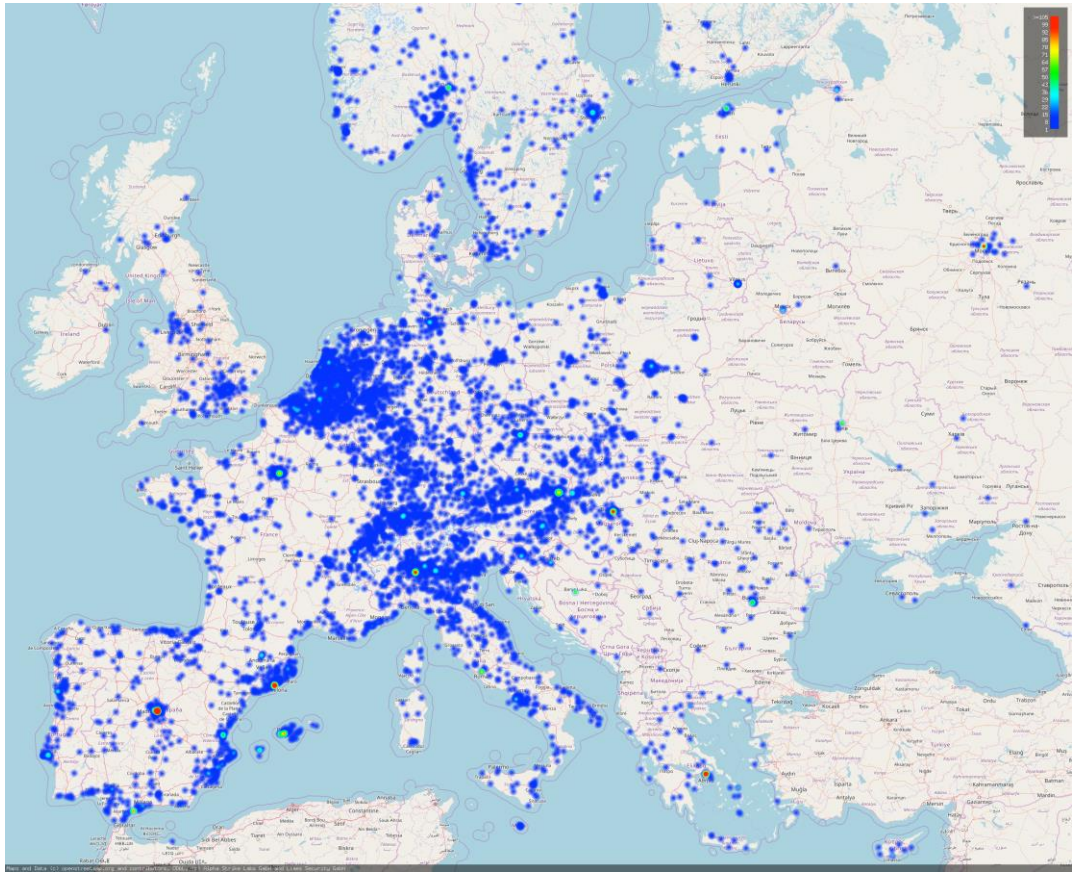
- KNX is used in many corporate and home automation scenarios
- Decentral: there is no master to rule them all
- Programmed via engineering software ETS
- Usually, a local, twisted pair bus
- KNX IP
  - UDP based (via port 3671 or via broadcast)
  - Insecure per Default

# Global Attack Surface



# Attack Surface USA vs. Europe





# Meet the BCU Key

- The BCU Key allows to set a device password to protect against modification
- 4-byte key and transmitted as hex over the wire
- Once the BCU key is set, the following actions are no longer possible:
  - Change the parameters / memory
  - Change the programming
  - Reset the device -> Bricked
- Hardly documented
- Helpful for ransomware for your building automation

# Incident Theory

- No logs or any kind of network traffic were available
- Our theory is
  - Attacker connected to the KNX IP GW that was accessible via the Internet
  - Enumerated the devices on the KNX Bus
  - Emptied the programming of the devices
  - Set the BCU Key on the device

# The Incident Resolution

- Customer sent four different bricked devices
- So far, we knew:
  - No idea if the key is unique per device
  - The devices had the old address
- How should we proceed?



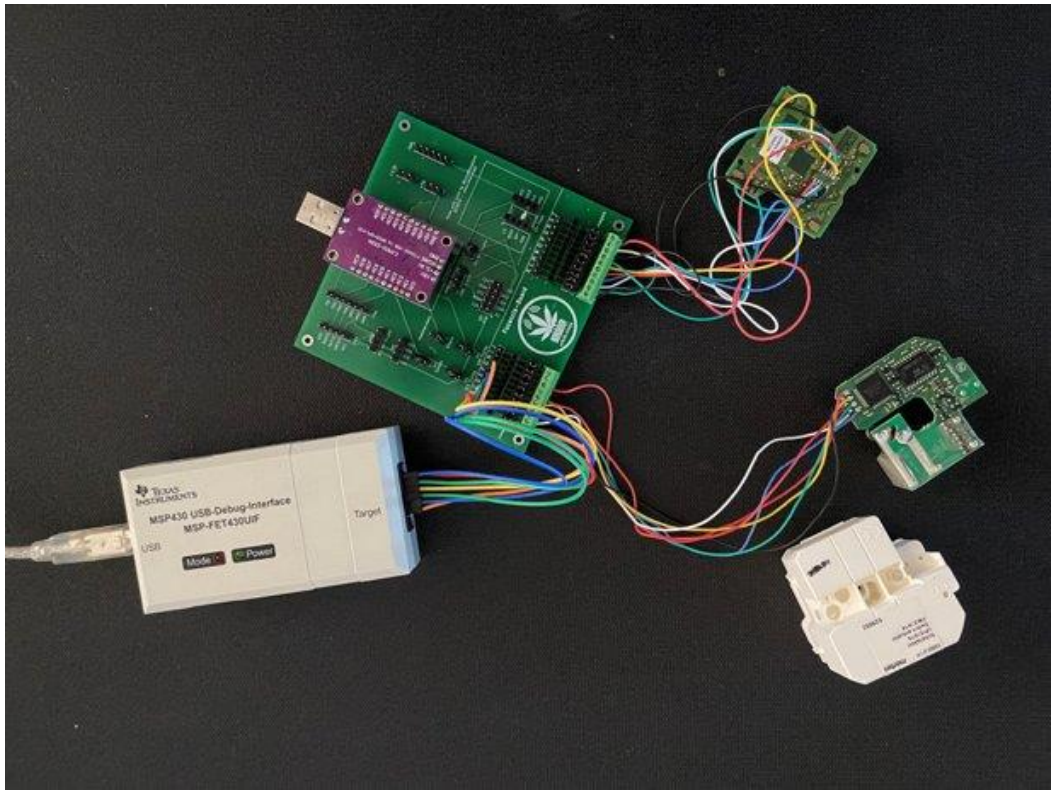

# Less promising …

- Brute Force
  - Takes too long on bus (9600 BAUD, ~10Keys/sec)
  - Maybe by accessing internal bus (UART), but not our first choice
- Circumvent
  - Looked for functions without authentication
  - Very simple fuzzing
  - No luck, deeper testing too time consuming
- Debug and jump execution
  - What about no?

# More promising …

- Read key from device
- First, we tried to dump the ARM based KNX Devices
  - Devices are based on a STM32
  - JTAG pinout is present on the device
  - Connect and …
  - No access to the memory because memory protection bits are set
- Next up was the ATMEGA based device …
- No access to the memory because memory protection bits are set as well

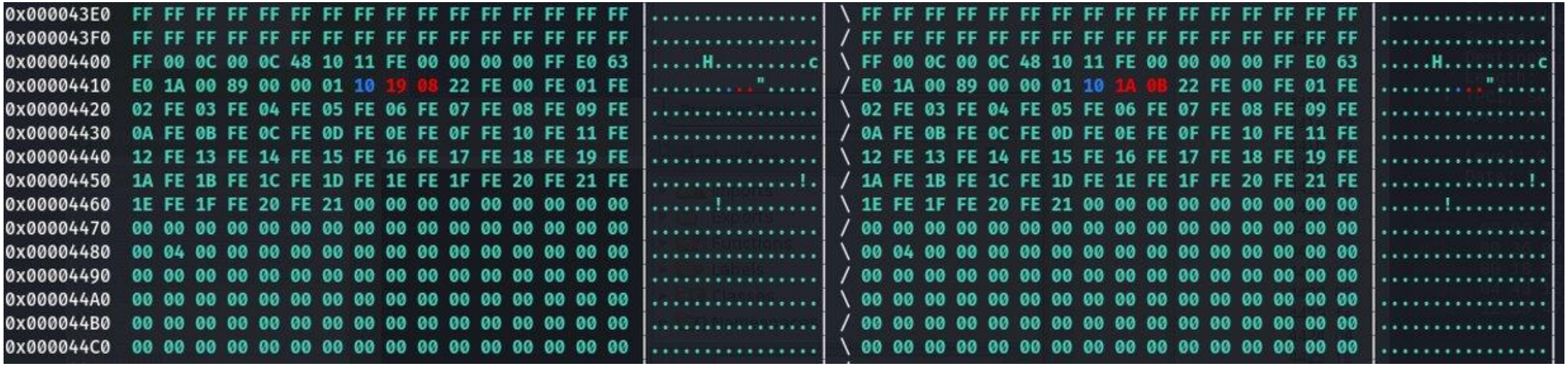
# Incident Resolution
# Dump of the Firmware




- As last device we tried the MSP430
  - No memory protection enabled
  - Dump of the firmware worked
  - No symbols, no strings
- Ghidra and PoC||GTFO 11 helped a lot in identifying possible key locations

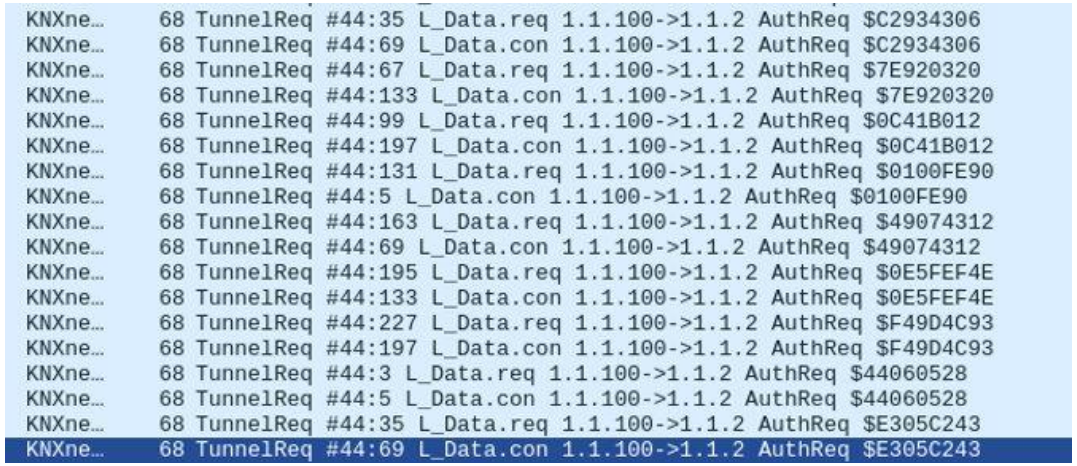
# Incident Resolution
# Key Location

- Debugger did not work -> dynamic analysis was off the table
- You can still change the address even when the BCU key is set
  - Change the address, dump the firmware, diff and got the location of address in memory
  - Looked for a key like pattern close by -> non found

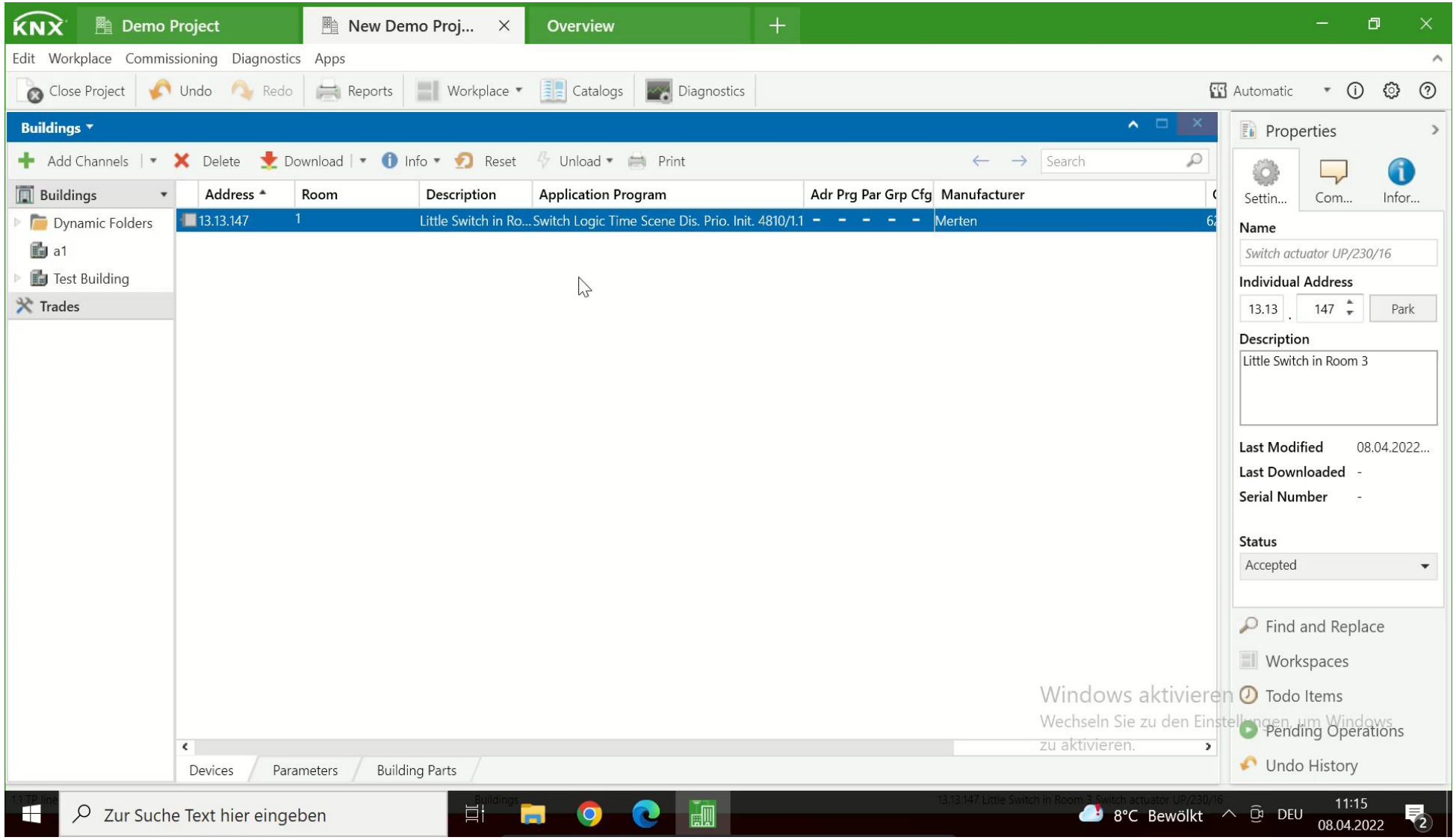


# Incident Resolution
# Brute Force the Key

- Next, we built 4-bytes chunks over the "data" section of the memory via a sliding window
  - Possible key candidates -> dictionary for a brute force
- Patched the tool knxmap to use the custom dictionary
- And …
- The key was in the memory in clear!!!
- And worked on all devices



# Demo Video


KNX
Demo Project
New Demo Proj...
Overview
Edit Workplace Commissioning Diagnostics Apps
Close Project
Undo
Redo
Reports
Workplace
Catalogs
Diagnostics
Automatic
Buildings
Add Channels
Delete
Download
Info
Reset
Unload
Print
Search
Buildings
Dynamic Folders
a1
Test Building
Trades
Address
Room
Description
Application Program
Adr Prg Par Grp Cfg
Manufacturer
13.13.147
1
Little Switch in Ro...
Switch Logic Time Scene Dis. Prio. Init. 4810/1.1
Merten
Devices
Parameters
Building Parts
Properties
Settin...
Com...
Infor...
Name
Switch actuator UP/230/16
Individual Address
13.13
147
Park
Description
Little Switch in Room 3
Last Modified
08.04.2022...
Last Downloaded
-
Serial Number
-
Status
Accepted
Find and Replace
Workspaces
Todo Items
Pending Operations
Undo History
Windows aktivieren
Wechseln Sie zu den Einstellungen, um Windows zu aktivieren.
Zur Suche Text hier eingeben
8°C Bewölkt
DEU
11:15
08.04.2022

# How to fix this

- The solution is obvious to security experts or even IT staff in general
- However, these systems are set up by experts in another field: electricians

- Never directly connect your building automation system to the Internet!!!!
- Use network segmentation and VPN
- Use KNX Secure
- Set the BCU key yourself
- Add a logger to your KNX Bus

# Can similar devices be locked as well?

- Most devices we have seen, have some sort of factory reset
- Except for the ABB AC500 v3

## 2.2 User Management at AC500 V3 PLC's

User management at PLC Side is available for

- PLC General
- OPC UA
- Visualization/Web Visualization
- FTP server

CAUTION!

If you have lost the administrator password, there is no way to recover it and the PLC must be send back for repair!

# Key Take-Aways

LIMES SECURITY

1. Security vulnerabilities saved the day
2. Criminals are constantly looking for new business opportunities
   Especially in areas that are not in focus by the security folks
3. Secure technology is useless without awareness

LIMES
SECURITY

**Felix Eberstaller**