THE DAY WE'VE BEEN HACKED
ABOUT ME

- Principal Network & Systems Architect
- 20+ years experience
- Work for Quickline, 2nd largest cable operator in CH
INTRODUCTION

THIS PRESENTATION IS ABOUT

- tech stuff
- legal stuff
- humans
INTRODUCTION

This presentation _is not_ about Blockchain.
INTRODUCTION

THIS PRESENTATION IS NOT ABOUT

Machine Learning
I can consult for 5000 CHF / day to put this on all your servers

root@server:~#alias gdpr_compliant="rm -rf /; sync; halt;"
STORY
TICKETS

- ticket about rejected email
- and another one...
- and another one...
- ...
SWISSCOM

- blacklisted specific range
- discussion about details with Swisscom
- mass UCE/SPAM/SCAM email from a specific IP range
NETWORK TOPOLOGY

THE INTERNET

BRAS/BNG

Layer3 aggregation
AAA

Layer2 aggregation

FAN

FAN

FAN

eRouter
IPv4 NAT
IPv6 Routed
NETWORK TOPOLOGY

Huawei HG8247H
INVESTIGATION
INVESTIGATING THE ORIGIN

- obviously not customer originated
- netflow
- direct tapping
- netstat-like on the CPE
Assumptions will make you blind!
INVESTIGATING THE ORIGIN

SSH !
(POSSIBLY) PROPRIETARY IMPLEMENTATION

root@hn::~# ssh root@
root@hn::~'s password:

User name or password is wrong, please try it again!
Login:
(POSSIBLY) PROPRIETARY IMPLEMENTATION

- **-D [bind_address:]port**
  Specifies a local “dynamic” application-level port forwarding

- **-N**
  Do not execute a remote command. This is useful for just forwarding ports
(POSSIBLY) PROPRIETARY IMPLEMENTATION

SSH CLIENT ➔ SSHD ➔ PAM / UNKN

- **Valid PW**: SSHD ➔ PAM / UNKN via /bin/sh
- **Invalid PW**: SSHD ➔ PAM / UNKN via /bin/login
- **Invalid PW & no cmd**: SSHD ➔ PAM / UNKN via (null)
CAUSE

- SSH open to the world!
- Misunderstanding, unclear documentation
- Vendor said “Works as expected”
RESOLUTION

- Correction of the CPE settings
SOLVED

- Yaaaayyy!!
LAWFUL INTERCEPT

- BÜPF / LSCPT - Federal Law for surveillance of Post and Telecommunications services
- 6 months of data retention for IP/timestamp to customer association
6 months of data retention for IP/timestamp to customer association
STORY AS IT HAPPENED

**LAWFUL INTERCEPT**

- Massive requests for LEA (ÜPF) in the following months
- Unsuccessful arrangement with MELANI & ÜPF
- Comment all request explaining the unlikeness that the customer was responsible
LESSONS LEARNED
DO NOT DEPLOY IN A HURRY!

Quick portscan with different CPE configs
if ( true_positive > 0 ) {
    process_request();
} else {
    reject();
    messy_legal_case();
}

translated quote by Prof. Dr. Simon Schlauri
Planning Breaches

- Inform the public (website, press release)
- Inform the affected customers!
QUESTIONS?
THANK YOU

PASCAL GLOOR @SPALE75