



Dipl.-Inform. Sebastian Schreiber  
Managing Director  
+49 7071 - 407856-0  
sebastian.schreiber@sysss.de



# Live Hacking



# ZUM UNTERNEHMEN

- 1998: Gründung der SySS GmbH durch S. Schreiber
- Heute: 170 Mitarbeiter
- Sitz in Frankfurt/M., Tübingen, München und Wien.
- Weltweit tätig
- Ab Juli 2009 in eigenem Bürogebäude
- Ab Juni 2017 im neuen Campus
- Dienstleistungen:
  - Penetration Testing & Sicherheitsanalysen
  - Incident Response/Schulungen/Auftritte



# AGENDA LIVE HACKING

1. Web-Applikations-Angriff
2. Krypto-USB-Drives: Code-Sperre
3. Angriff auf Alarmanlage
4. Krypto-USB-Drives: Fingerabdruck-Scanner
5. SMS fälschen
6. Thermostat-Hack
7. Hacking ABB RTUs
8. APT-Einstieg über Funktastaturen
9. Virens Scanner überlisten
10. Trojaner-Angriff gegen Smartphone
11. USB-Tools
12. Paywall Piercing bei der FAZ





# WHY TO HACK A THERMOSTATE?



# SHODAN



- Shodan =nmap+Google
- Remote Terminal Units
- ABB RTU560

Default user name	Default password	Assigned user roles	Default user role
Show	Show	Viewer	Viewer
Load	Load	Installer	Installer
Control	Control	Installer Engineer	Installer
Admin	Admin	Engineer Administrator	Engineer
Operator	Operator	Operator	Operator
Default	Default	Viewer Operator Installer Engineer SECAUD RBACMNT SECADM Administrator	Viewer

Table 4: Default user accounts in the RTU

# SHODAN



- Shodan =nmap+Google
- Fernwirktechnik! "Remote Terminal Units"
- ABB RTU560
- `http.title:"Nordex Control" "Windows 2000 5.0 x86" "Jetty/3.1 (JSP 1.1; Servlet 2.2; java 1.6.0_14)"`
- <https://github.com/jakejarvis/awesome-shodan-queries#industrial-control-systems>

Default user name	Default password	Assigned user roles	Default user role
Show	Show	Viewer	Viewer
Load	Load	Installer	Installer
Control	Control	Installer Engineer	Installer
Admin	Admin	Engineer Administrator	Engineer
Operator	Operator	Operator	Operator
Default	Default	Viewer Operator Installer Engineer SECAUD RBACMNT SECADM Administrator	Viewer

Table 4: Default user accounts in the RTU

# FRAGEN? INTERESSE AN PENETRATIONSTESTS?



SySS GmbH  
Schaffhausenstraße 77  
72072 Tübingen  
Germany

Dipl.-Inform.

**Sebastian Schreiber**

Managing Director

p +49 (0)7071 - 40 78 56-50  
f +49 (0)7071 - 40 78 56-19  
m +49 (0)173 - 35 02 72 5  
sebastian.schreiber@syss.de

PGP Fingerprint: 4DA8 5ED3 B6C9 1F58 F4C5 E0E4 2D3D A586 6246 E21A

<https://www.linkedin.com/in/sebastian-schreiber-72958/>



THE PENTEST EXPERTS

[WWW.SYSS.DE](http://WWW.SYSS.DE)