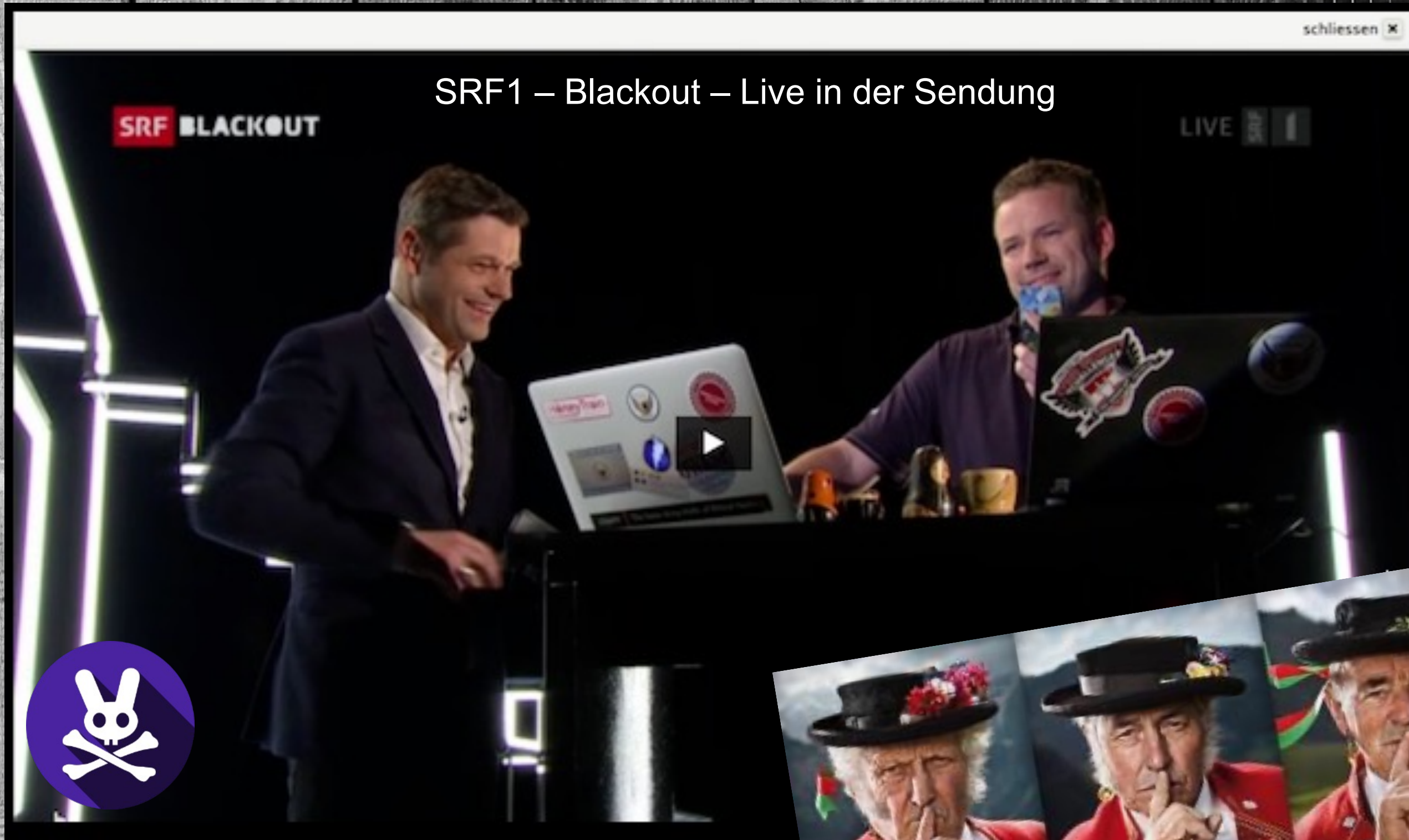
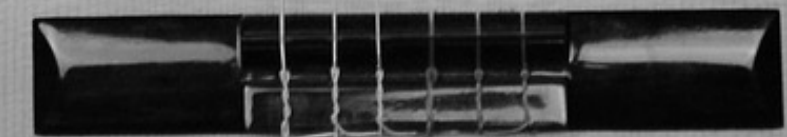


Safety meets Cyber Security



Ivan Bütler



Compass Security - seit 1999

80 Mitarbeiter in Jona, Zürich, Bern, Basel, Berlin, Toronto

Hacking-Lab™
Hands-On & Capture-the-Flag



Penetration Tests | Red Teaming | Security Reviews

Cyber Feuerwehr 7/24h (DFIR)

VBS Cyber Lehrgang

Die Kandidaten beim Assessment
in Jassbach.

Bild: VBS




106 Tarnen 1
Strassenbeleuchtung

- 040 Strassenbeleuchtung GH
- 041 Strassenbeleuchtung HH
- 044 Weihnachtsbeleuchtung
- 108 Strassenbeleuchtung

Diverses

- 045 Monatsrückstellung 1
- 047+046 Monatsrückstellung

RL CySec Rail

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK
Bundesamt für Verkehr BAV
Abteilung Sicherheit

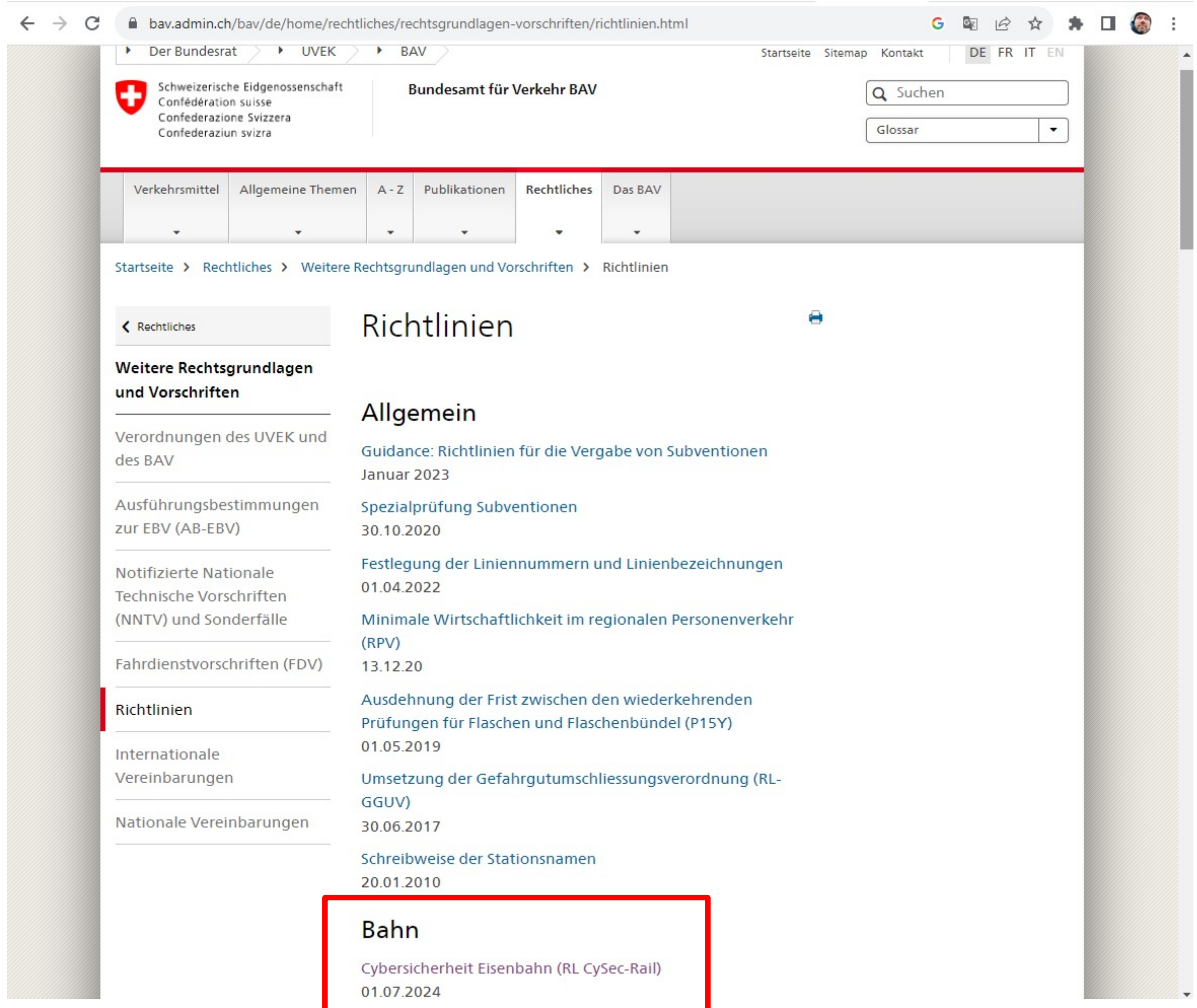
Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1
Datum: 22.09.2023
Version: V1.0

Richtlinie

Cybersicherheit Eisenbahn

RL CySec-Rail


Auf Grundlage von Art. 5c der Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV – SR 742.141.1) und deren Ausführungsbestimmungen.



bav.admin.ch/bav/de/home/rechtliches/rechtsgrundlagen-vorschriften/richtlinien.html

Der Bundesrat > UVEK > BAV

Startseite Sitemap Kontakt DE FR IT EN

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Verkehr BAV

Suchen

Glossar

Verkehrsmittel Allgemeine Themen A - Z Publikationen Rechtliches Das BAV

Startseite > Rechtliches > Weitere Rechtsgrundlagen und Vorschriften > Richtlinien

< Rechtliches

Richtlinien

Weitere Rechtsgrundlagen und Vorschriften

Verordnungen des UVEK und des BAV

Ausführungsbestimmungen zur EBV (AB-EBV)

Notifizierte Nationale Technische Vorschriften (NNTV) und Sonderfälle

Fahrdienstvorschriften (FDV)

Richtlinien

Internationale Vereinbarungen

Nationale Vereinbarungen

Allgemein

Guidance: Richtlinien für die Vergabe von Subventionen
Januar 2023

Spezialprüfung Subventionen
30.10.2020

Festlegung der Liniennummern und Linienbezeichnungen
01.04.2022

Minimale Wirtschaftlichkeit im regionalen Personenverkehr (RPV)
13.12.20

Ausdehnung der Frist zwischen den wiederkehrenden Prüfungen für Flaschen und Flaschenbündel (P15Y)
01.05.2019

Umsetzung der Gefahrgutumschliessungsverordnung (RL-GGUV)
30.06.2017

Schreibweise der Stationsnamen
20.01.2010

Bahn

Cybersicherheit Eisenbahn (RL CySec-Rail)
01.07.2024

Rail Slang

Type	Category	Transit
Operational Systems	Control Systems	Train Control System Bus Control Systems
	SCADA	Traction Power Emergency Ventilation System Monitoring (Pumps, Alarms)
	Signaling	Train Signals Signal Priority Systems
	Communications	Communications DSRC
	Fare Collection Systems	Entry/Exit Gates Ticket Vending Machines, Fare Boxes, Fare Validators, Ticket Encoding
	HVAC/Building Management	HVAC systems (not integral part, but loss could result in failure of critical systems) “People Movers”
Enterprise Data Systems	Business/Revenue/3 rd Party systems: Finance, HR, Messaging (email), Archives	Asset Management BYOD
Engineering Systems	Design, Construction	Track Inspection

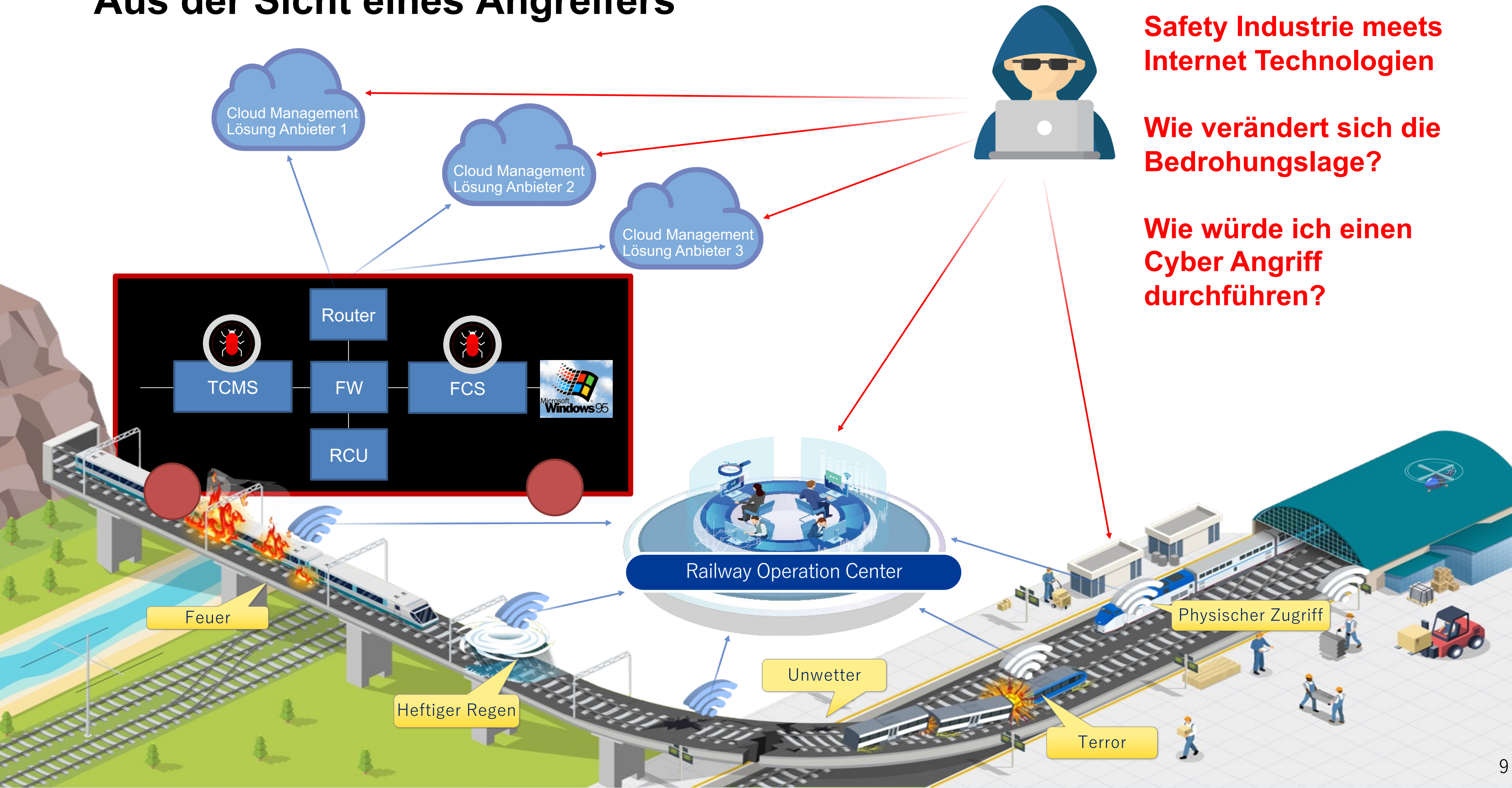


Aus der Sicht eines Angreifers

**Safety Industrie meets
Internet Technologien**

**Wie verändert sich die
Bedrohungslage?**

**Wie würde ich einen
Cyber Angriff
durchführen?**



Mitre Attack Framework

mitre-attack.github.io/attack-navigator/

ICSI x layer x layer by operation x +

selection controls layer controls technique controls

Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Shodan IoT Suchmaschine

← → ↻ shodan.io/search?query=railway&page=4 🔍 📄 ☆ ⚙️ 🗂️ 👤

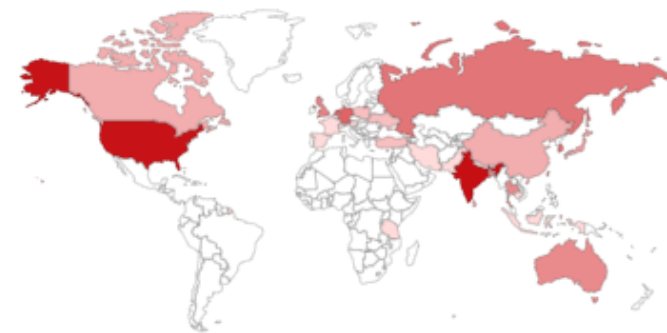
Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing ↗️ railway 🔍 Account

TOTAL RESULTS

199

TOP COUNTRIES



India	41
United States	39
Netherlands	14
Germany	12
Singapore	10

[More...](#)

View Report Download Results Historical Trend Browse Images View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

301 Moved Permanently ↗️

2023-10-23T20:47:54.356935

2a01:488:42:1000:b24
d:5511:ffd1:9fa2
railway-service.de
[Host Europe GmbH](#)

Germany, Frankfurt
am Main

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Mon, 23 Oct 2023 20:47:53 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: <https://railway-service.de>

302 Found ↗️

2023-10-23T20:44:51.490676

193.47.89.177
[HUBER+SUHNER AG](#)

Switzerland, Pfäffikon

HTTP/1.1 302 Found
Date: Tue, 24 Oct 2023 11:33:00 GMT
Server: Apache
Location: <https://railway-data.hubersuhner.com/>
Content-Length: 221
Content-Type: text/html; charset=iso-8859-1

Open Source Intelligence

→ crt.sh?q=stadlerrail.com

crt.sh Identity Search



[Group by Issuer](#)

Criteria Type: Identity Match: ILIKE Search: 'stadlerrail.com'

Certificates	crt.sh ID	Logged At ↑	Not Before	Not After	Common Name	Matching Identities
	10701130222	2023-10-10	2023-10-10	2024-01-08	dev.stadlerrail.com	dev.stadlerrail.com
	10702310075	2023-10-10	2023-10-10	2024-01-08	dev.stadlerrail.com	dev.stadlerrail.com
	10699114849	2023-09-26	2023-09-26	2023-12-25	recruiting.stadlerrail.com	recruiting.stadlerrail.com
	10261435770	2023-08-31	2023-08-31	2024-08-31	etk-dev.stadlerrail.com	etk-dev.stadlerrail.com
	10261435861	2023-08-31	2023-08-31	2024-08-31	etk-dev.stadlerrail.com	etk-dev.stadlerrail.com
	10411762495	2023-08-26	2023-08-26	2023-11-24	oetiker.ch	varem.stadlerrail.com
	10394309797	2023-08-26	2023-08-26	2023-11-24	oetiker.ch	varem.stadlerrail.com
	10220858221	2023-08-25	2023-08-25	2024-08-25	test-sb20230825.stadlerrail.com	test-sb20230825.stadlerrail.com
	10220858219	2023-08-25	2023-08-25	2024-08-25	test-sb20230825.stadlerrail.com	test-sb20230825.stadlerrail.com
	10116069205	2023-08-11	2023-08-11	2023-11-09	dev.stadlerrail.com	dev.stadlerrail.com

Default Passwords

<https://github.com/scadastrangelove/SCADAPASS>

	A	B	C	D	E	F
1	#SCADA StrangeLove Default/Hardcoded Passwords List					
2	#Find more at http://www.scada.sl					
3	#Please contact us at scadastrangelove@gmail.com and @scadasl					

siemens	Simatic S7-300 (pre-2009 versions)	Hardcoded password:, Basisk:Basisk
siemens	Scalance	admin:admin, user:user
siemens	Scalance (x 200, W788-1PRO, W788-2PF	Admin:admin, User:user, for FTP access:
siemens	SyncoTM living Web server OZW772 V2	Administrator:Password
siemens	Siemens WinCC 7.x	winccd:winccpass, wincce:winccpass, DM
siemens	Ruggedcom RMC30	admin:admin
siemens	RuggedSwitch, RS8000 / RS1600 / RS900	admin

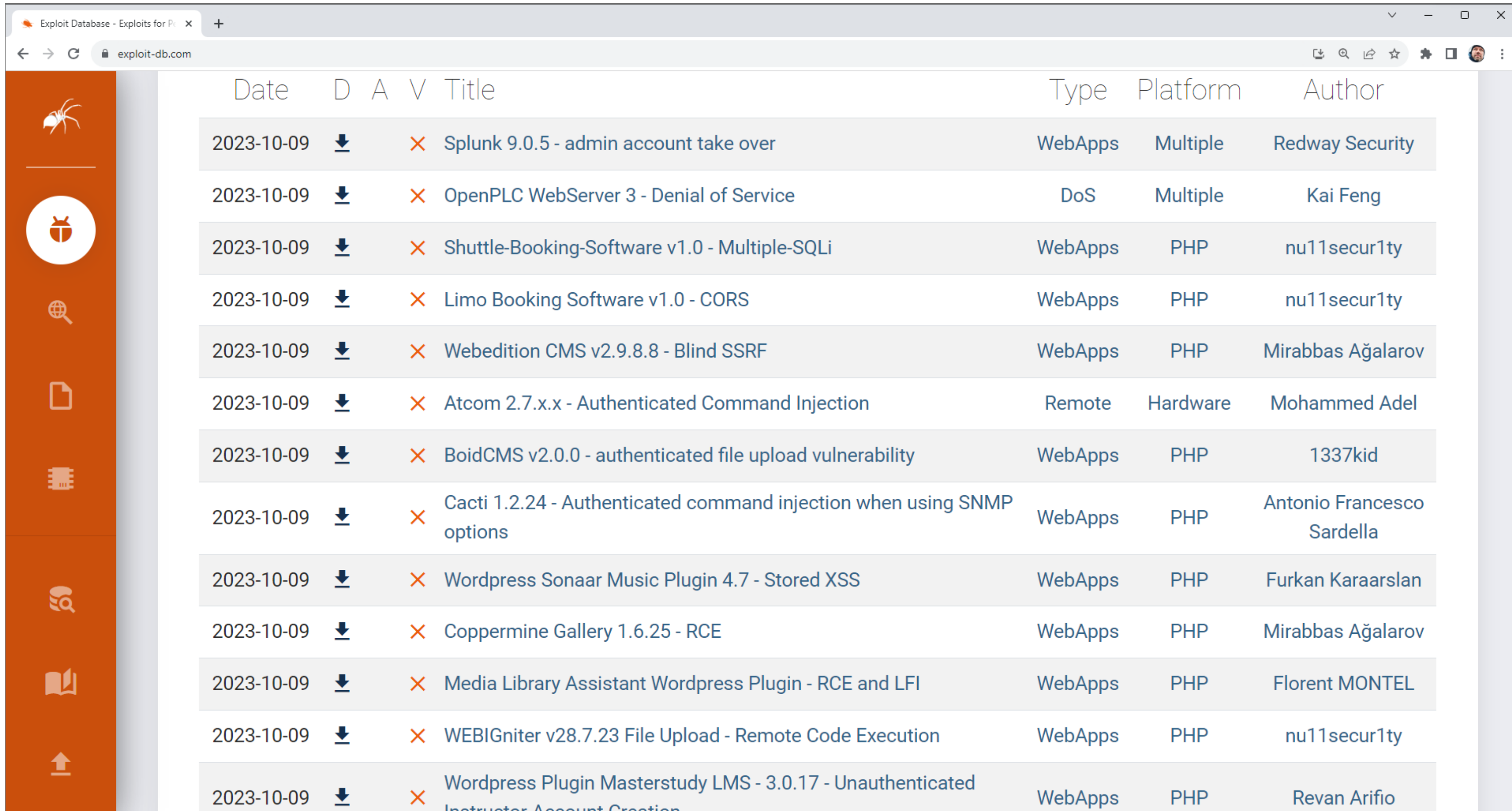
19	BinTec Elmeg	any routers	(##unknown - means not known or any ch	Router	
20	BinTec Elmeg	BinTec R230aw	admin:funkwerk	Router	
21	BinTec Elmeg	bintec W2002T-n,	admin:funkwerk, admin:admin	WLAN Access Point f	
22	Contemporary Control Systems	BASRT-B	admin:admin	80/tcp	Router http
23	Datasensor	UR5i/UR5i SL	root:root	80/tcp	Router http
24	Digi	DC-ME-01T-S	root:dbps		Network http
25	Digi	Digi Connect SP, Digi Connect Wi-SP, Di	root:dbps	80/tcp	Network http
26	Digi	Digi Connect ES 4/8 SB with Switch, Digi	root:dbps	80/tcp	Concentra http



Leaked Passwords

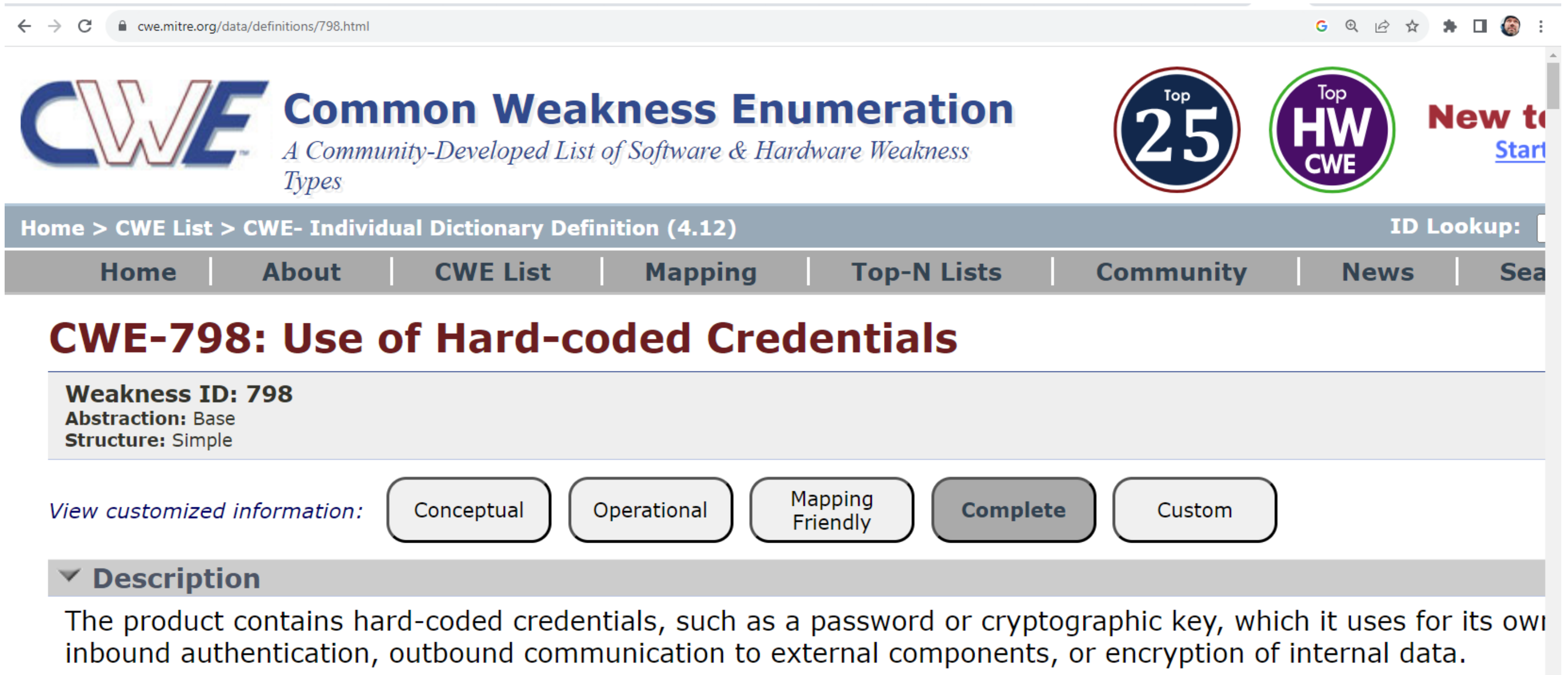
The screenshot shows the DeHashed search interface. At the top, the browser address bar displays 'dehashed.com/search?query=csnc.ch'. The DeHashed logo and search bar are visible, with 'csnc.ch' entered in the search field. Below the search bar, a navigation menu includes 'Home / Results', 'Search', 'Pricing', 'Data Wells', 'Blog', 'Support', 'FAQ', 'API', 'WHOIS', 'Monitoring', and 'My Account'. A summary bar at the top right of the results area shows: 33 RESULT(S) FOUND, 219MS SEARCH ELAPSED TIME, 14,453,524,343 ASSETS SEARCHED, and 48,796 AGGREGATED DATA WELLS. The main results section is titled 'Results:' and includes a disclaimer: 'Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.' Three search results are displayed as cards, each with an email address, source information, and a 'Request entry removal' link. The first result is 'walter.sprenger@csnc.ch' sourced from '16,624 Separate Data Breaches data'. The second result is 'team@csnc.ch' sourced from 'sps-magazin.de data'. The third result is 'walter.sprenger@csnc.ch' also sourced from 'sps-magazin.de data'. To the right of the results, there are three informational sections: 'What's DeHashed and those results?', 'What can I search for?', and 'How can I protect myself or remove my data?'. The footer of the page contains the URL 'compass-security.com' and the page number '11'.

Bekannte Schwachstellen



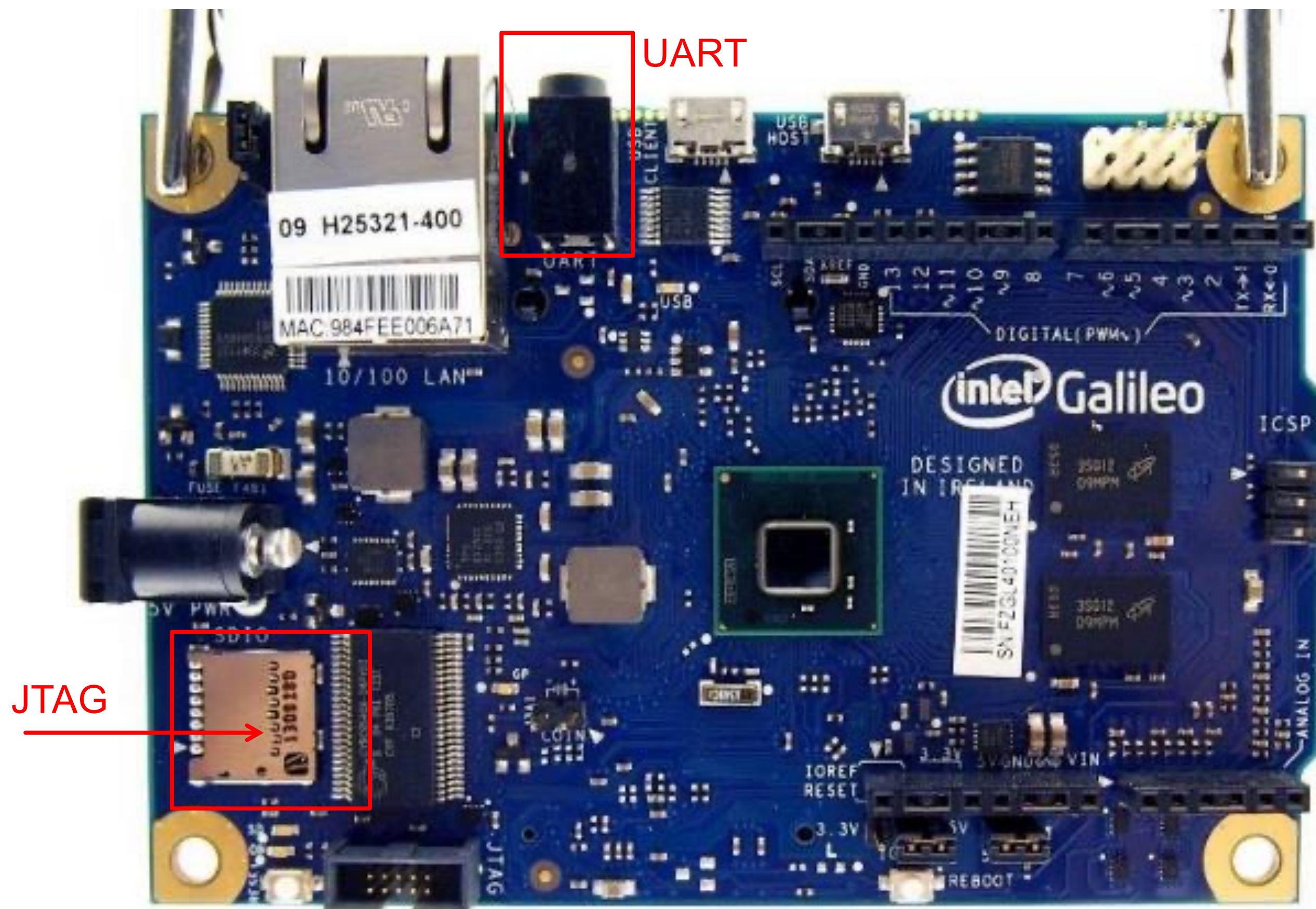
Date	D	A	V	Title	Type	Platform	Author
2023-10-09	↓	×		Splunk 9.0.5 - admin account take over	WebApps	Multiple	Redway Security
2023-10-09	↓	×		OpenPLC WebServer 3 - Denial of Service	DoS	Multiple	Kai Feng
2023-10-09	↓	×		Shuttle-Booking-Software v1.0 - Multiple-SQLi	WebApps	PHP	nu11secur1ty
2023-10-09	↓	×		Limo Booking Software v1.0 - CORS	WebApps	PHP	nu11secur1ty
2023-10-09	↓	×		Webedition CMS v2.9.8.8 - Blind SSRF	WebApps	PHP	Mirabbas Ağalarov
2023-10-09	↓	×		Atcom 2.7.x.x - Authenticated Command Injection	Remote	Hardware	Mohammed Adel
2023-10-09	↓	×		BoidCMS v2.0.0 - authenticated file upload vulnerability	WebApps	PHP	1337kid
2023-10-09	↓	×		Cacti 1.2.24 - Authenticated command injection when using SNMP options	WebApps	PHP	Antonio Francesco Sardella
2023-10-09	↓	×		Wordpress Sonaar Music Plugin 4.7 - Stored XSS	WebApps	PHP	Furkan Karaarslan
2023-10-09	↓	×		Coppermine Gallery 1.6.25 - RCE	WebApps	PHP	Mirabbas Ağalarov
2023-10-09	↓	×		Media Library Assistant Wordpress Plugin - RCE and LFI	WebApps	PHP	Florent MONTEL
2023-10-09	↓	×		WEBIGNiter v28.7.23 File Upload - Remote Code Execution	WebApps	PHP	nu11secur1ty
2023-10-09	↓	×		Wordpress Plugin Masterstudy LMS - 3.0.17 - Unauthenticated Instructor Account Creation	WebApps	PHP	Revan Arifio

Hard-coded Credentials



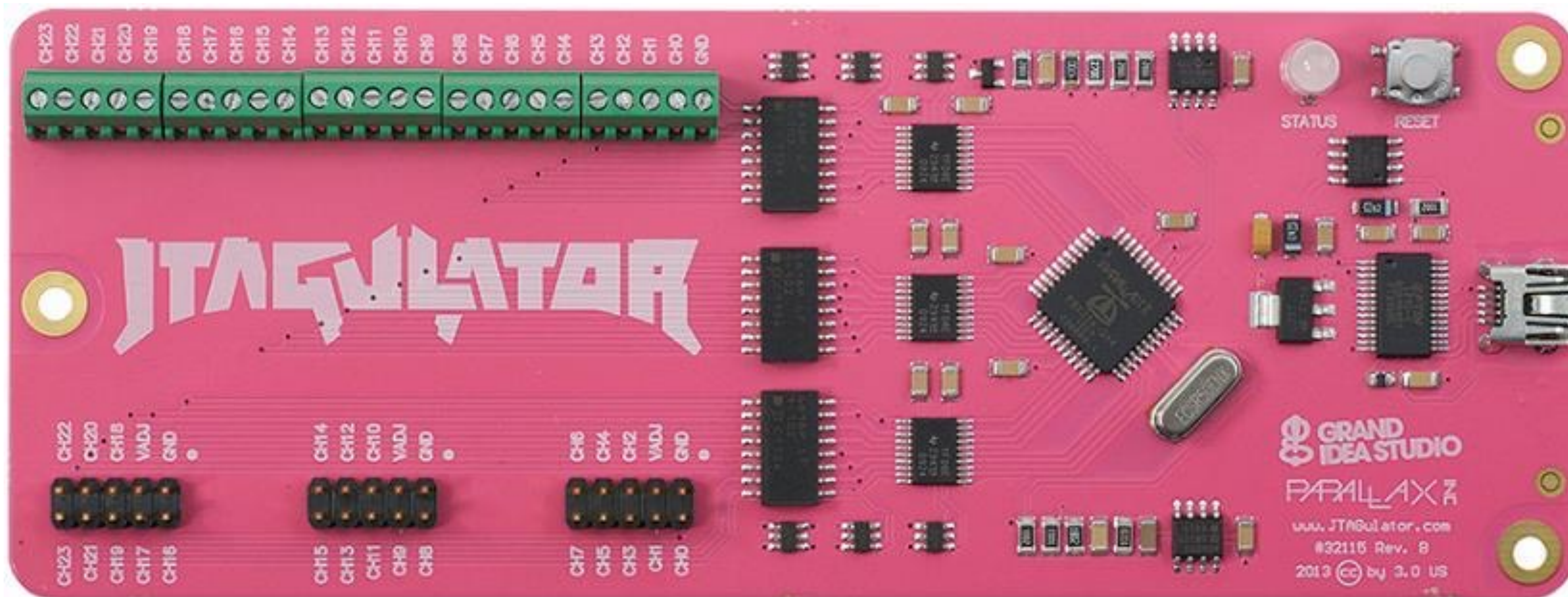
The screenshot shows a web browser window with the URL `cwe.mitre.org/data/definitions/798.html`. The page header features the CWE logo and the text "Common Weakness Enumeration" with the subtitle "A Community-Developed List of Software & Hardware Weakness Types". There are also two circular badges: "Top 25" and "Top HW CWE". A navigation bar includes links for Home, About, CWE List, Mapping, Top-N Lists, Community, News, and Search. The main heading is "CWE-798: Use of Hard-coded Credentials". Below this, the "Weakness ID: 798" is listed with "Abstraction: Base" and "Structure: Simple". A "View customized information:" section contains five buttons: "Conceptual", "Operational", "Mapping Friendly", "Complete" (which is highlighted), and "Custom". A "Description" section is expanded, showing the text: "The product contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data."

JTAG und UART Hacking



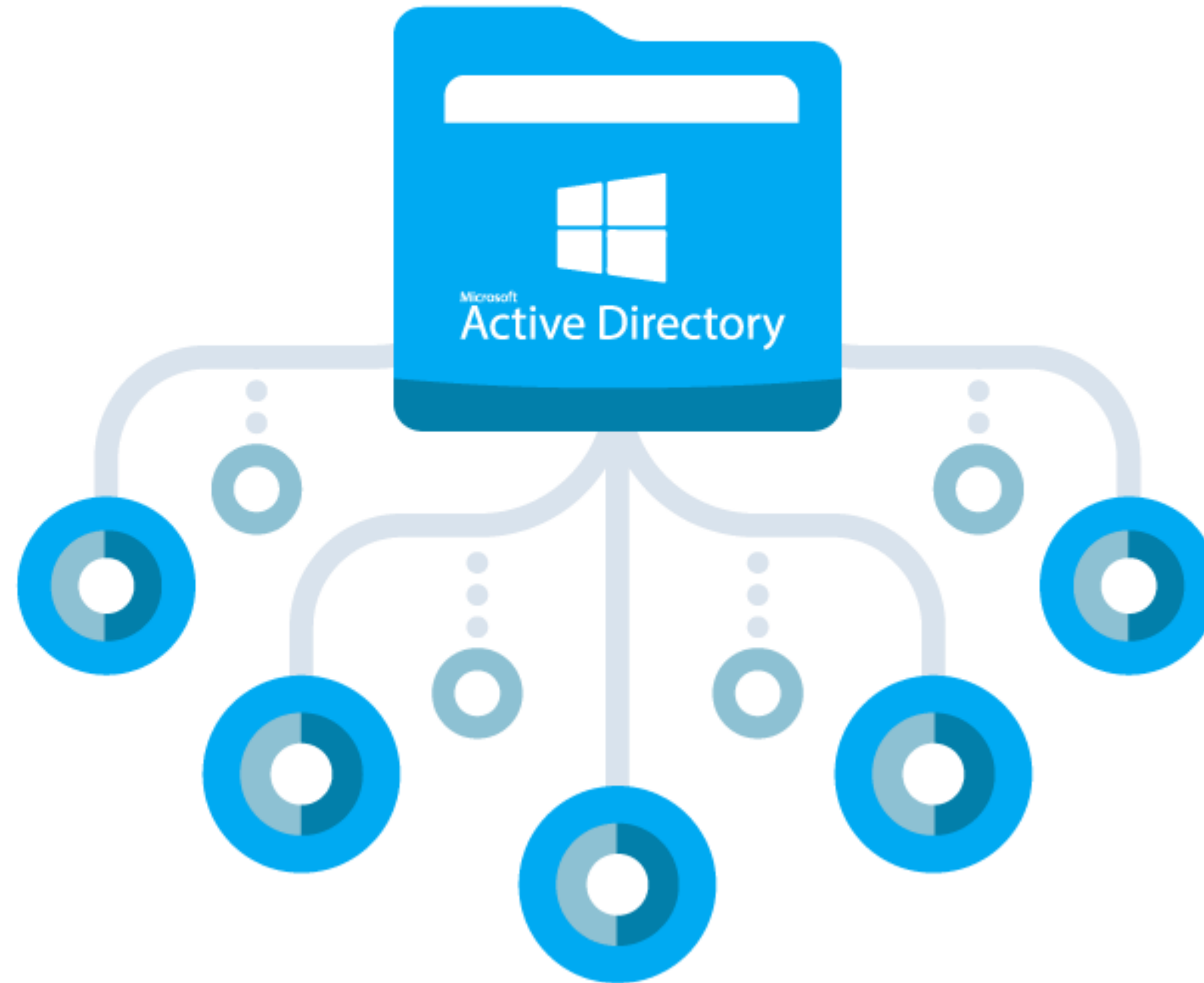
JTAGulator

On-chip debug (OCD) interfaces can provide chip-level control of a target device and are a primary vector used by engineers, researchers, and **hackers** to extract program code or data, modify memory contents, or affect device operation on-the-fly



Source <http://www.grandideastudio.com/jtagulator/>

Abhängigkeiten zum Active Directory



Quelle Bild: <https://cyberhoot.com/cybrary/active-directory-ad/>

AES Decryption

Filter by title

- 2.2.1.1.3 COMPRESSION
- Attributes
- 2.2.1.1.4 Password Encryption
- 2.2.1.1.5 Expanding Environment Variables
- > 2.2.1.2 DataSources
- > 2.2.1.3 Devices
- > 2.2.1.4 Drives
- > 2.2.1.5 EnvironmentVariables
- > 2.2.1.6 Files
- > 2.2.1.7 FolderOptions
- > 2.2.1.8 Folders

Download PDF

Learn /



2.2.1.1.4 Password Encryption

Article • 02/14/2019

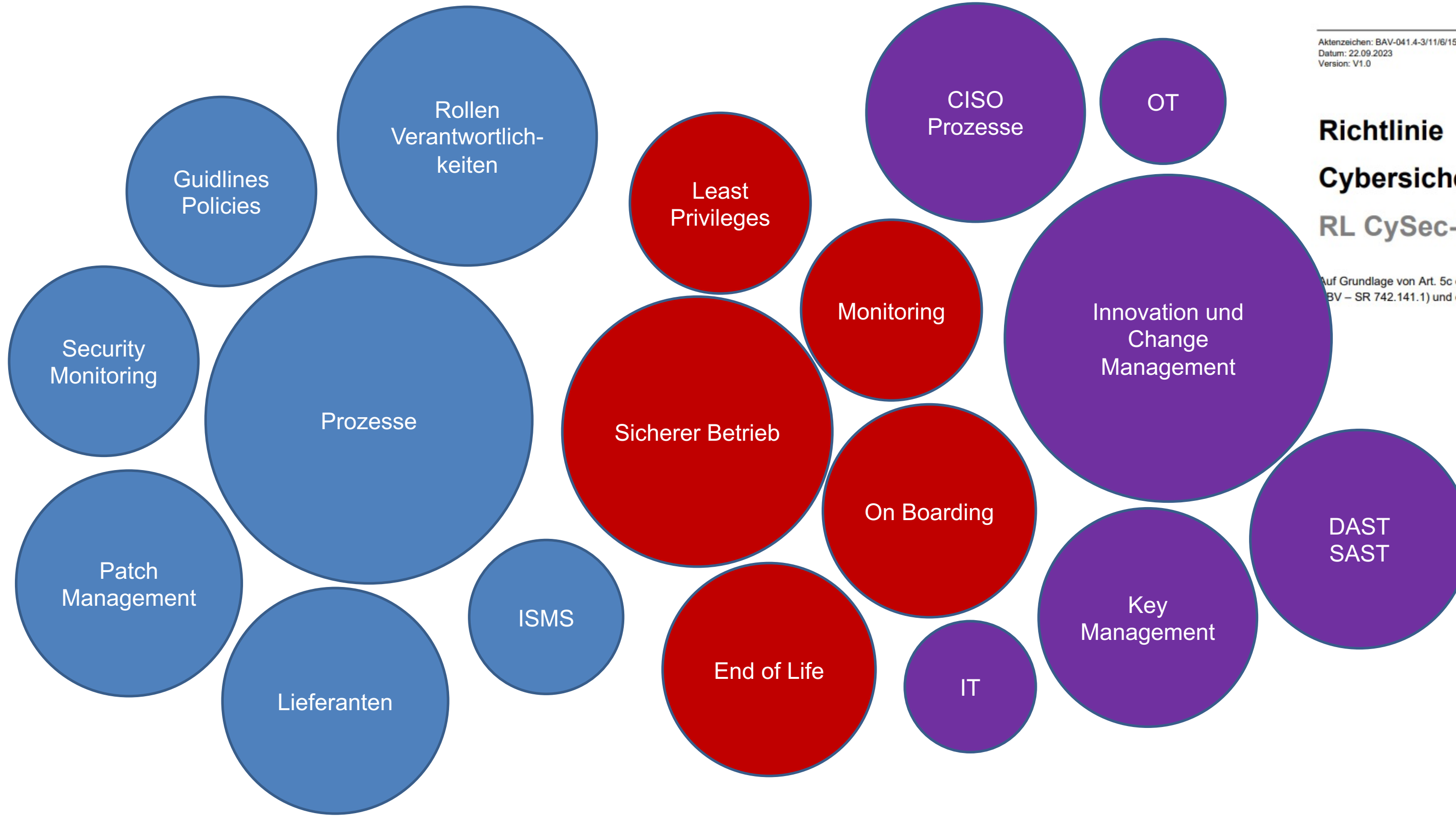
Feedback

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

```
4e 99 06 e8 fc b6 6c c9 fa f4 93 10 62 0f fe e8  
f4 96 e8 06 cc 05 79 90 20 9b 09 a4 33 b6 6c 1b
```

Empfehlungen Cyber Sicherheit



Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1
Datum: 22.09.2023
Version: V1.0

Richtlinie Cybersicherheit Eisenbahn RL CySec-Rail

Auf Grundlage von Art. 5c der Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, BV – SR 742.141.1) und deren Ausführungsbestimmungen.

106 Tarnen 1
Strassenbeleuchtung



040 Strassenbeleuchtung GH



041 Strassenbeleuchtung HH

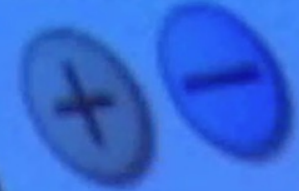


044 Weihnachtsbeleuchtung



108 Strassenbeleuchtung

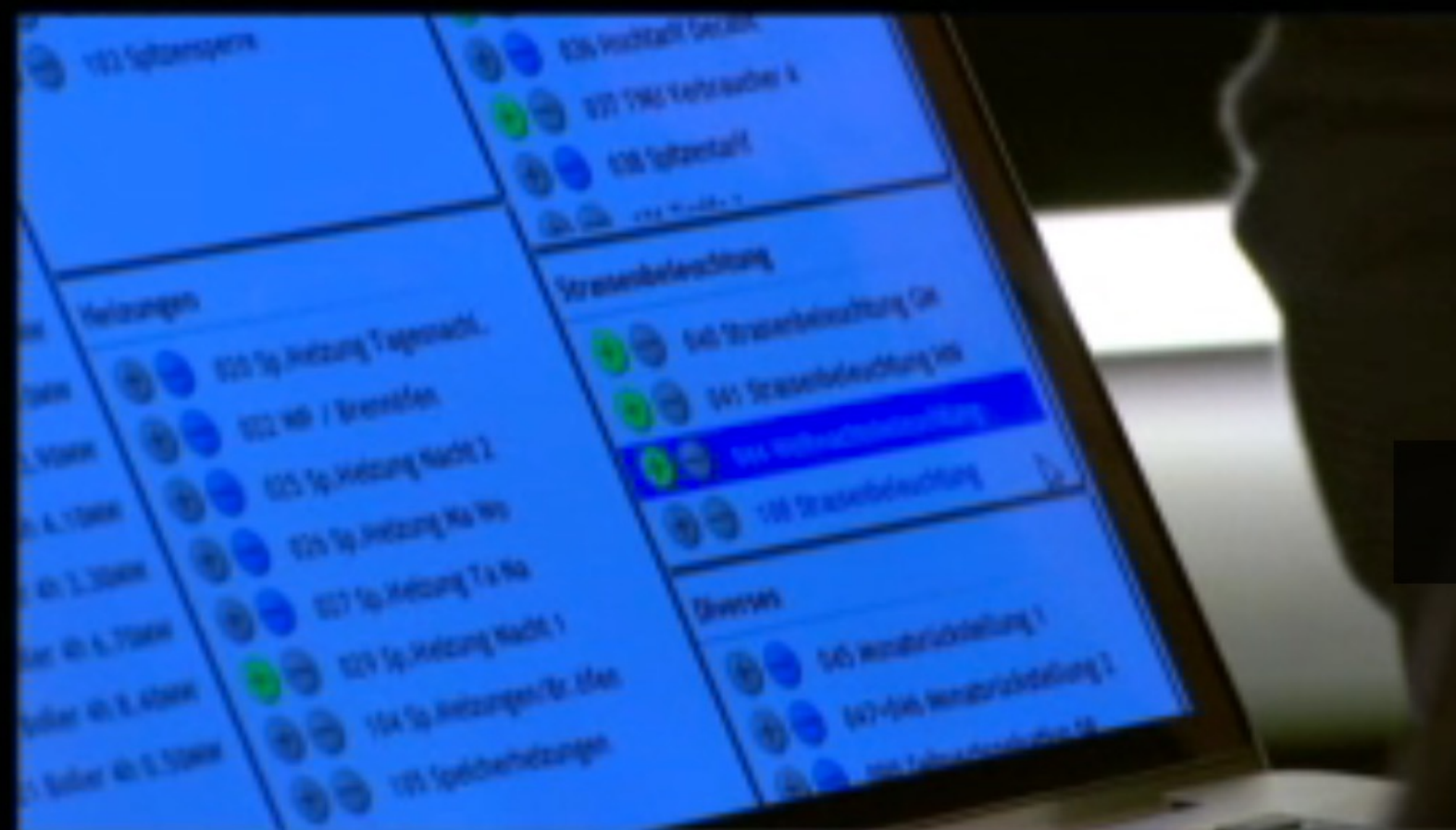
Diverses



045 Monatsrückstellung 1

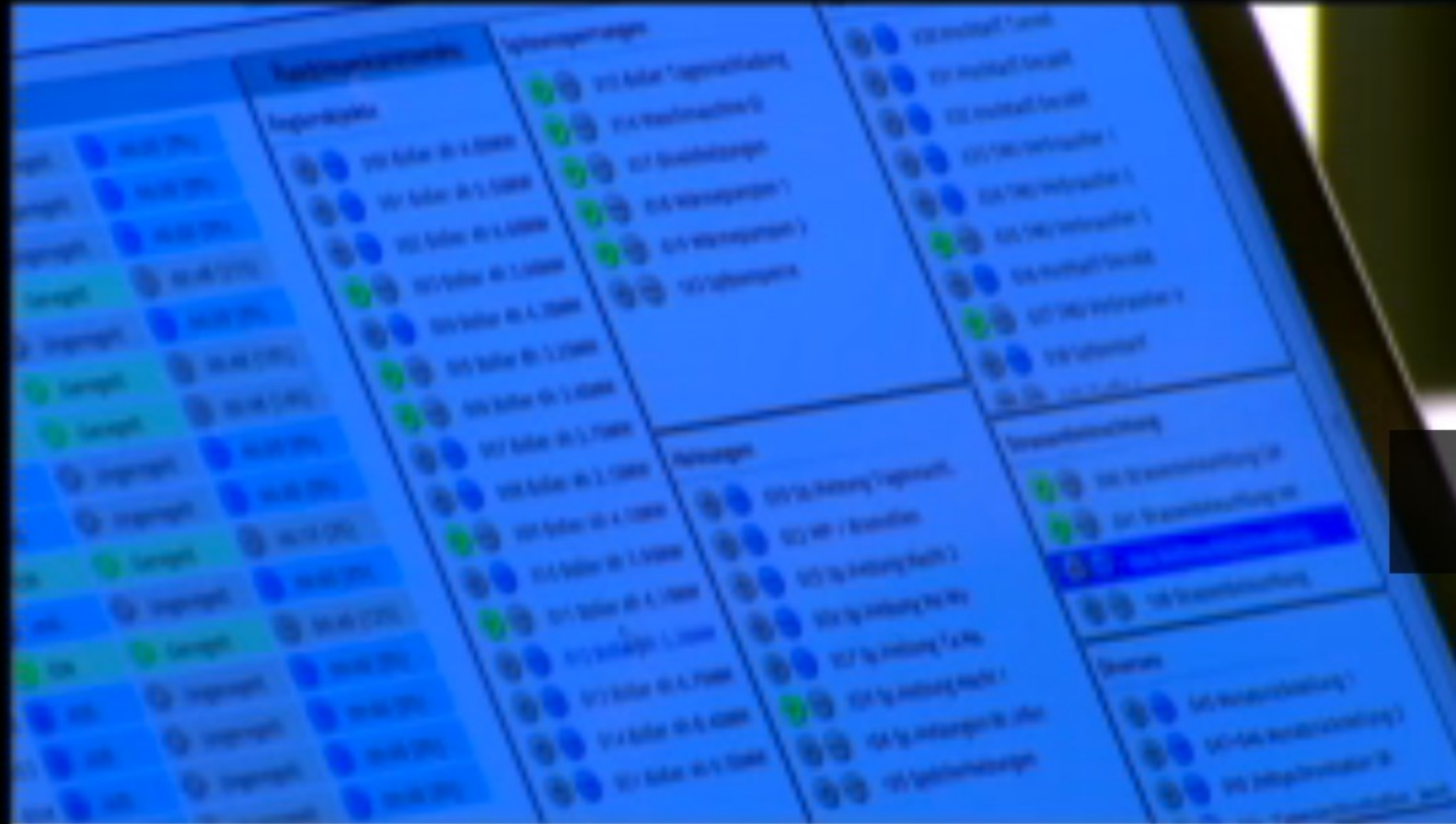


047+046 Monatsrückstellung



STUDIO ZÜRICH

LIESTAL ALTSTADT



STUDIO ZÜRICH



LIESTAL ALTSTADT

Vielen Dank für Ihre Aufmerksamkeit



Ivan Bütler, Compass Security AG
Ethical Hacking & Penetration Testing
Incident Response

ivan.buetler@compass-security.com
<https://www.compass-security.com/>