



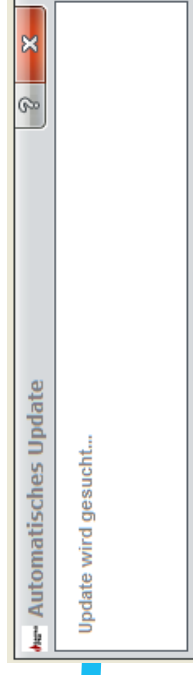
Wenn ein CVSS Score von 10.0
ein leeres Bankkonto bedeuten kann



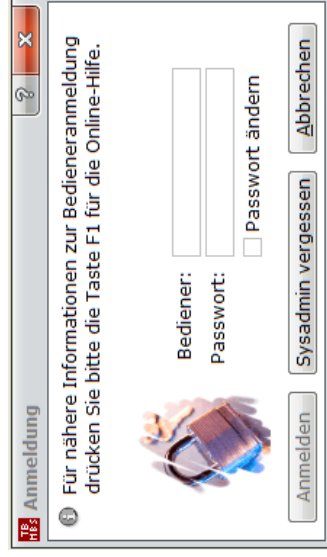
The Beginning: Can you spot the issue?



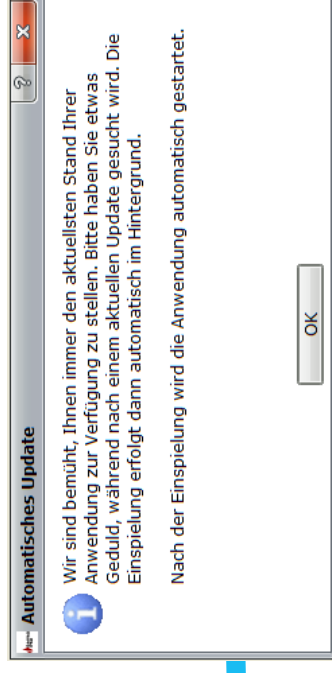
Launch the Online
Banking Windows Client



Search for Updates



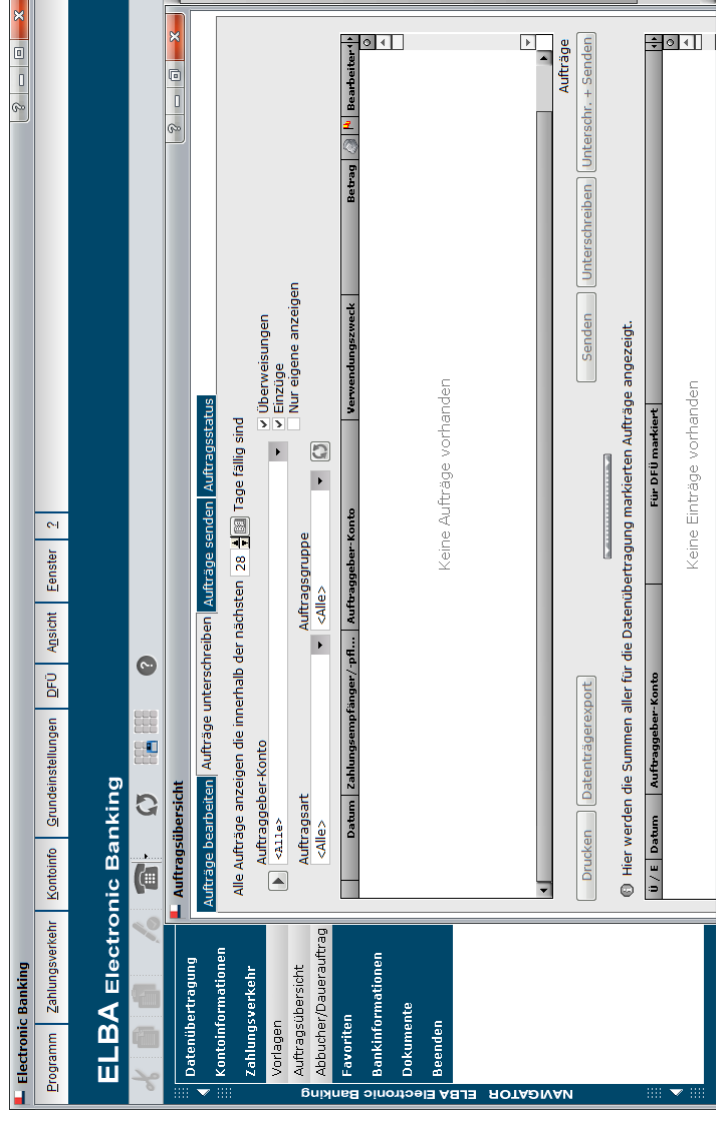
Login



Apply Updates



Disclosing a 0-Day in ELBA5



ELBA5 aka "telebankingMBS"
 Online Banking for businesses



Disclosing a 0-Day in ELBA5



ELBA5 aka "telebankingMBS"
Online Banking for businesses



Disclosing a 0-Day in ELBA5



ELBA5 aka "telebankingMBS"
Online Banking for businesses



ELBA5 is used by ...

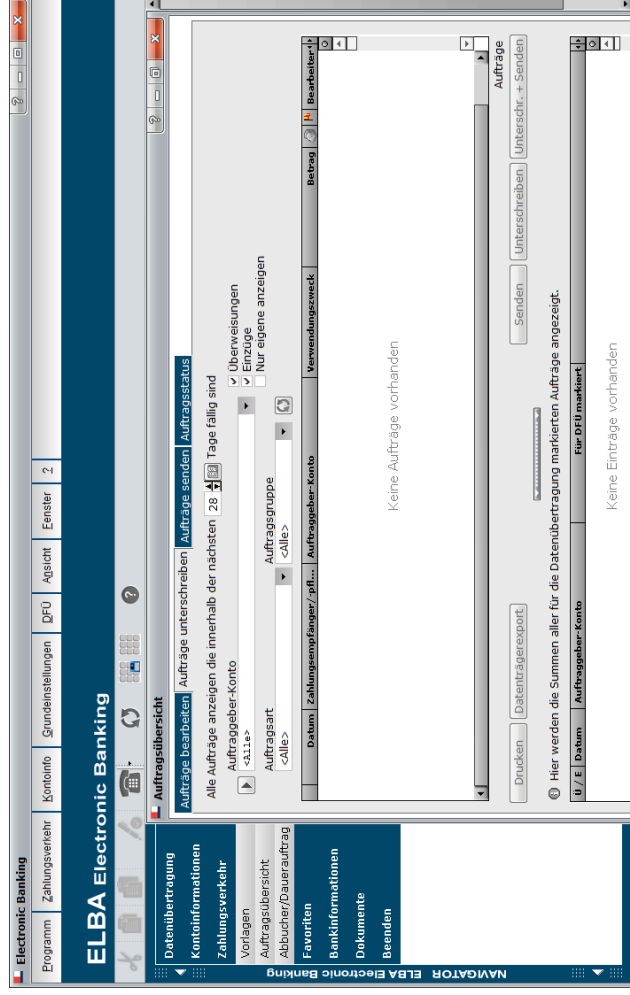
24 Banks

80.000 Installations

5.000 Vulnerable



ELBA5 comes in 2 Variants



Client only

Single seat installation
No network interaction (except with bank)

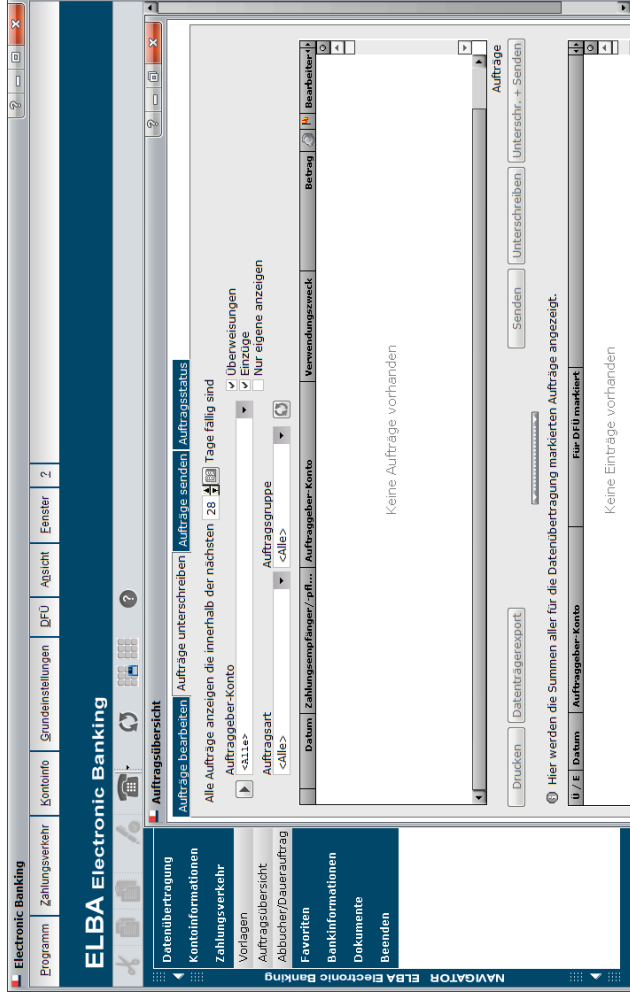


Network

Multi-user installation
Communication over the network with a central database server



ELBA5 comes in 2 Variants



Client only

Single seat installation
No network interaction (except with bank)



Network

Multi-user installation
Communication over the network with a central database

VULNERABLE



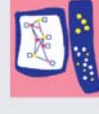
#whoami



Florian Bogner

*IT Security Expert
aka "Professional Hacker"
Speaker and Trainer
Bug Bounty Hunter*

More than 50 vulnerabilities reported to:



Check Point
SOFTWARE TECHNOLOGIES LTD.



Raphael Zoidl

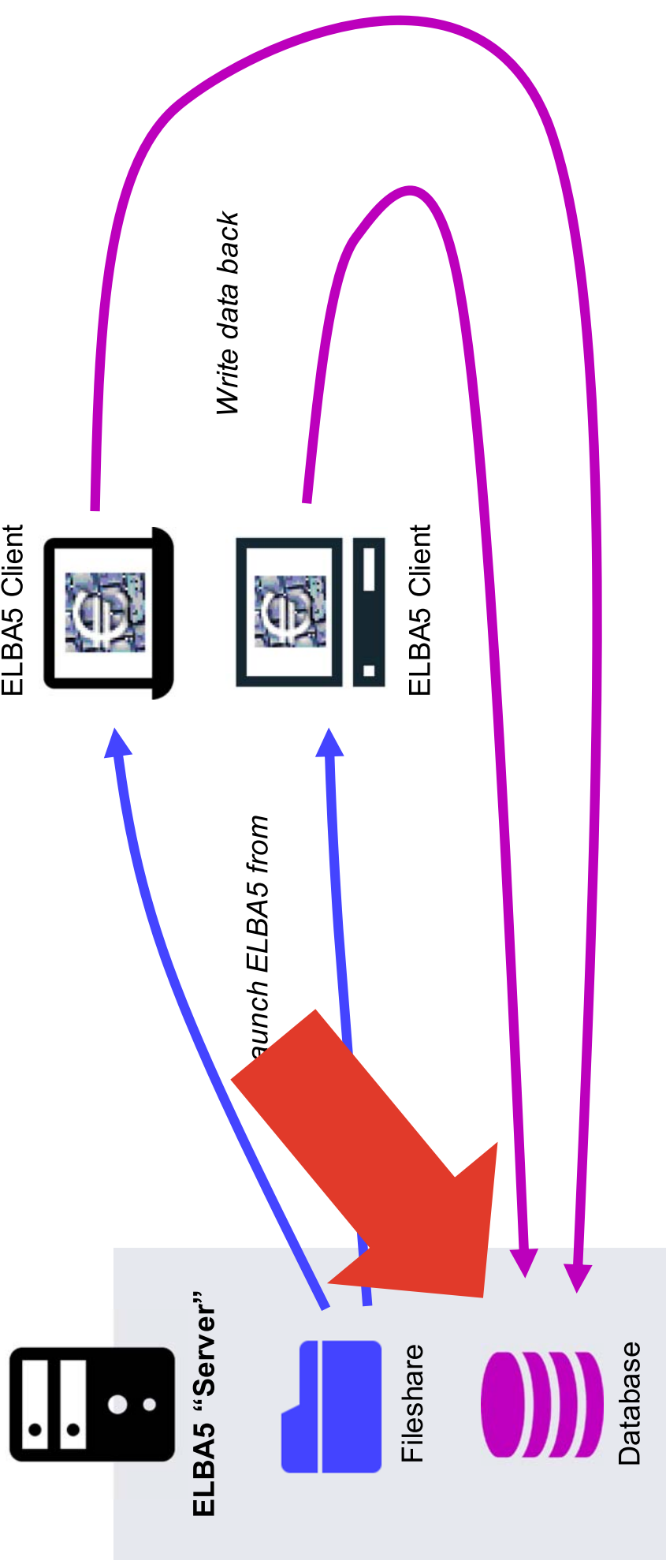
Application Security Manager



- Produktgruppe Electronic Banking (ELBA)



ELBA5 Network System Overview

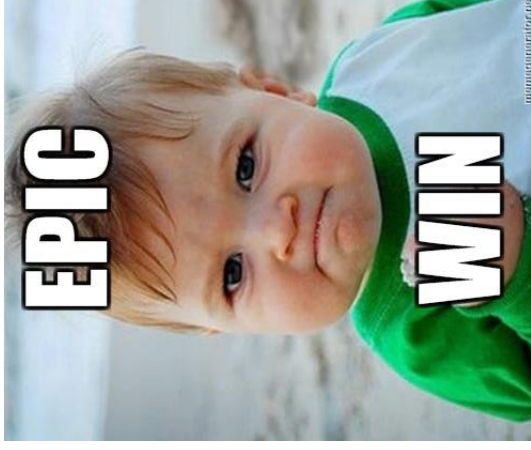
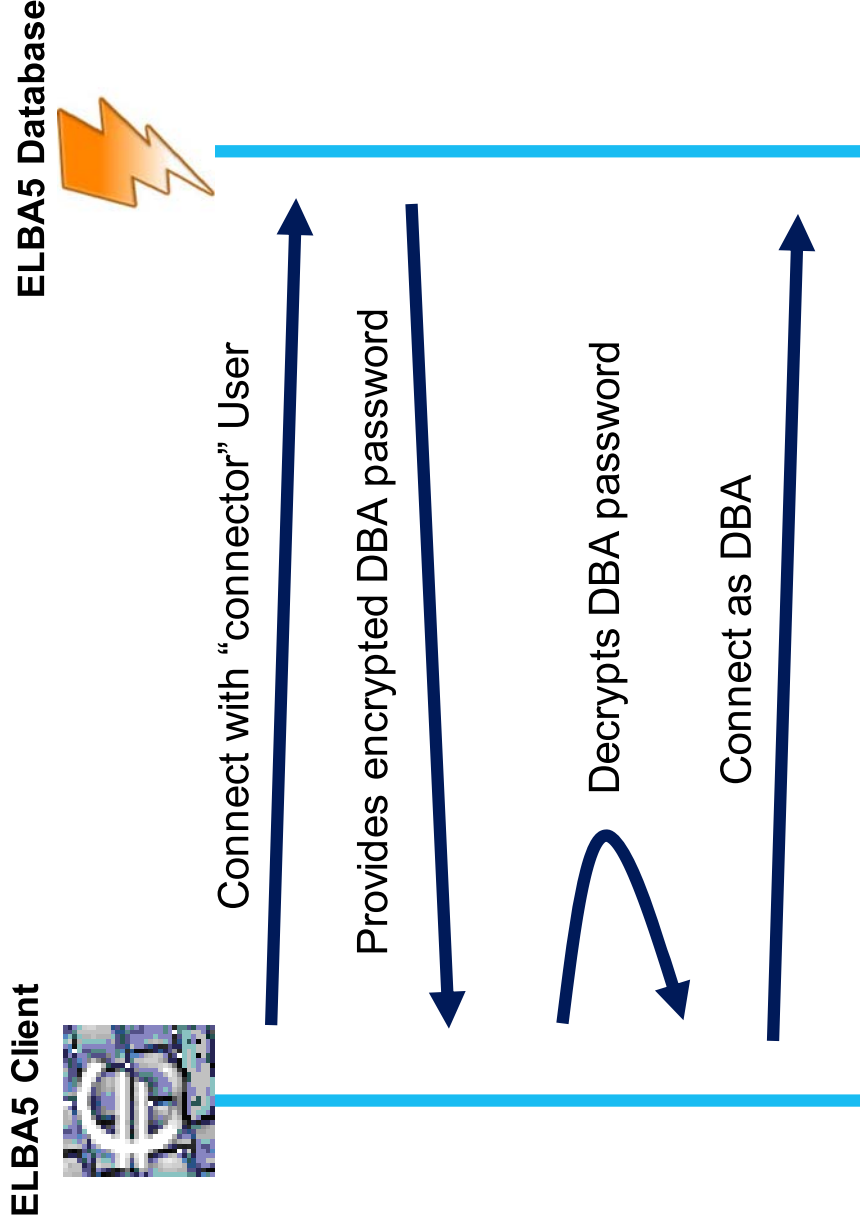




Live Demo: Desintegrating ELBA5



Summary



```
SELECT DECRYPT(daten,
'Af&Pw_dw7$Yd9#','AES') FROM
elbndba.connection
```





Summary

ELBA5 Client



ELBA5 Database



What can we do now?

Provides encrypted DBA password

EVERYTHING!

Decrypts DBA password

Connects as DBA



```
SELECT DECRYPT(daten,
'Af&Pw_dw7$Yd9#',AES') FROM
elbnda.connection
```





Live Demo: Weaponizing our Knowledge!





Weaponizing our Knowledge!

1

Transaction Tampering

Add a backdoor user:

Password Hash: SHA256(password + bedienerKey + userDir)

SQL: INSERT INTO BEDIENER ...



YO DAWG, I HEARD YOU LIKE EXPLOITS

2

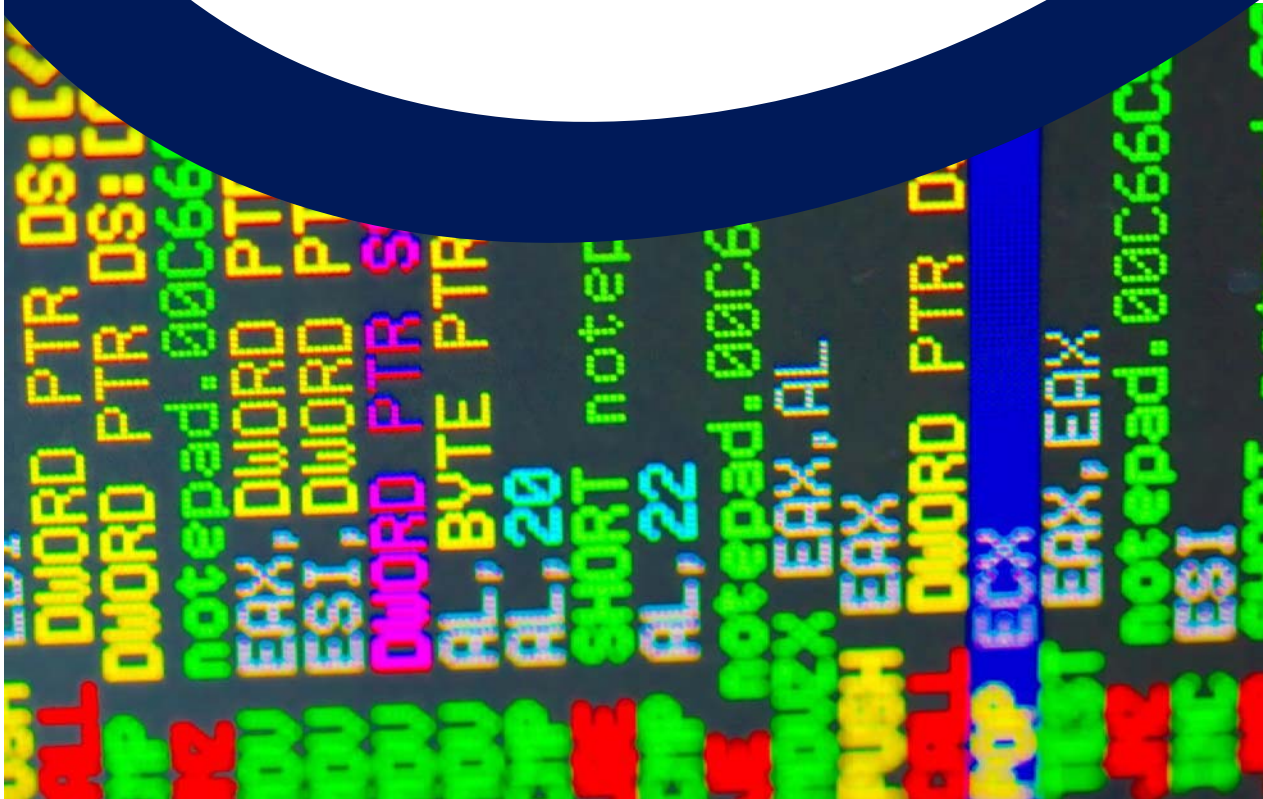
Remote Code Execution

Because we don't care about money:

SQL: xp_cmdshell('the command')

We are SYSTEM! Mimikatz anyone?



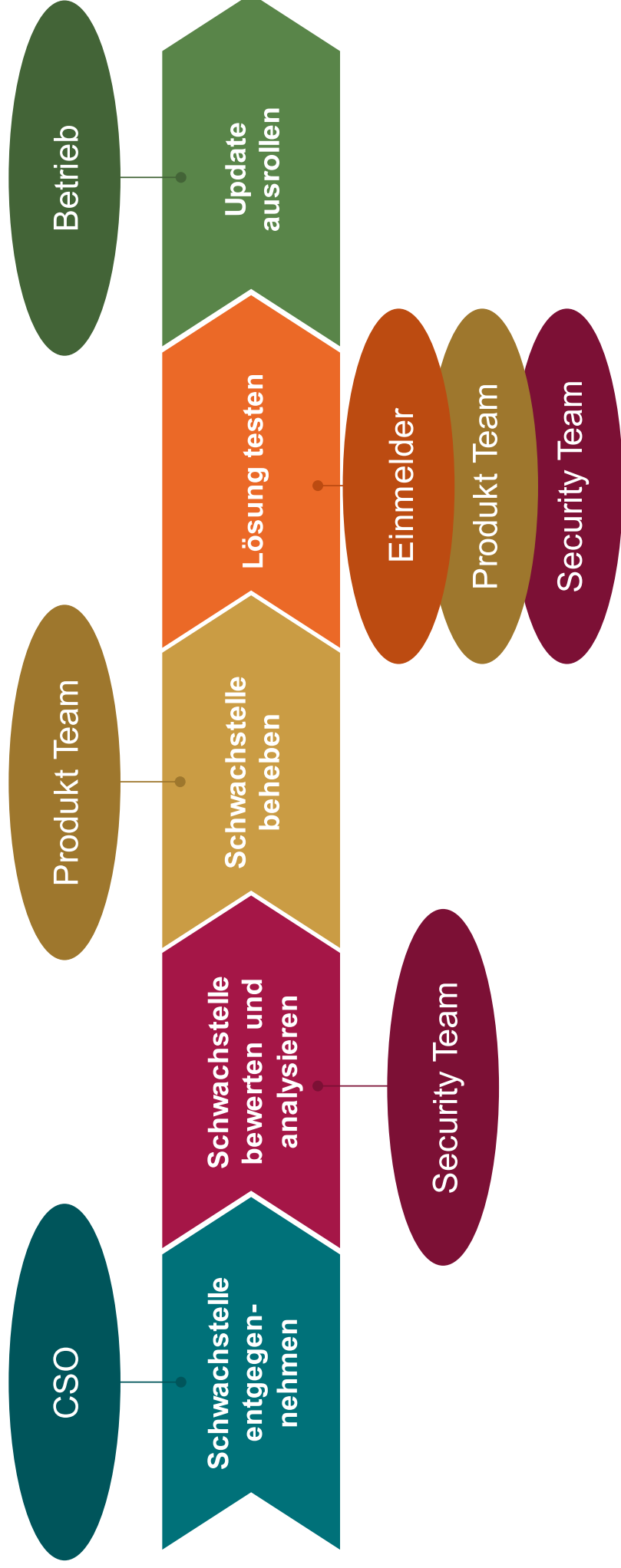


Live Demo: Because I can!

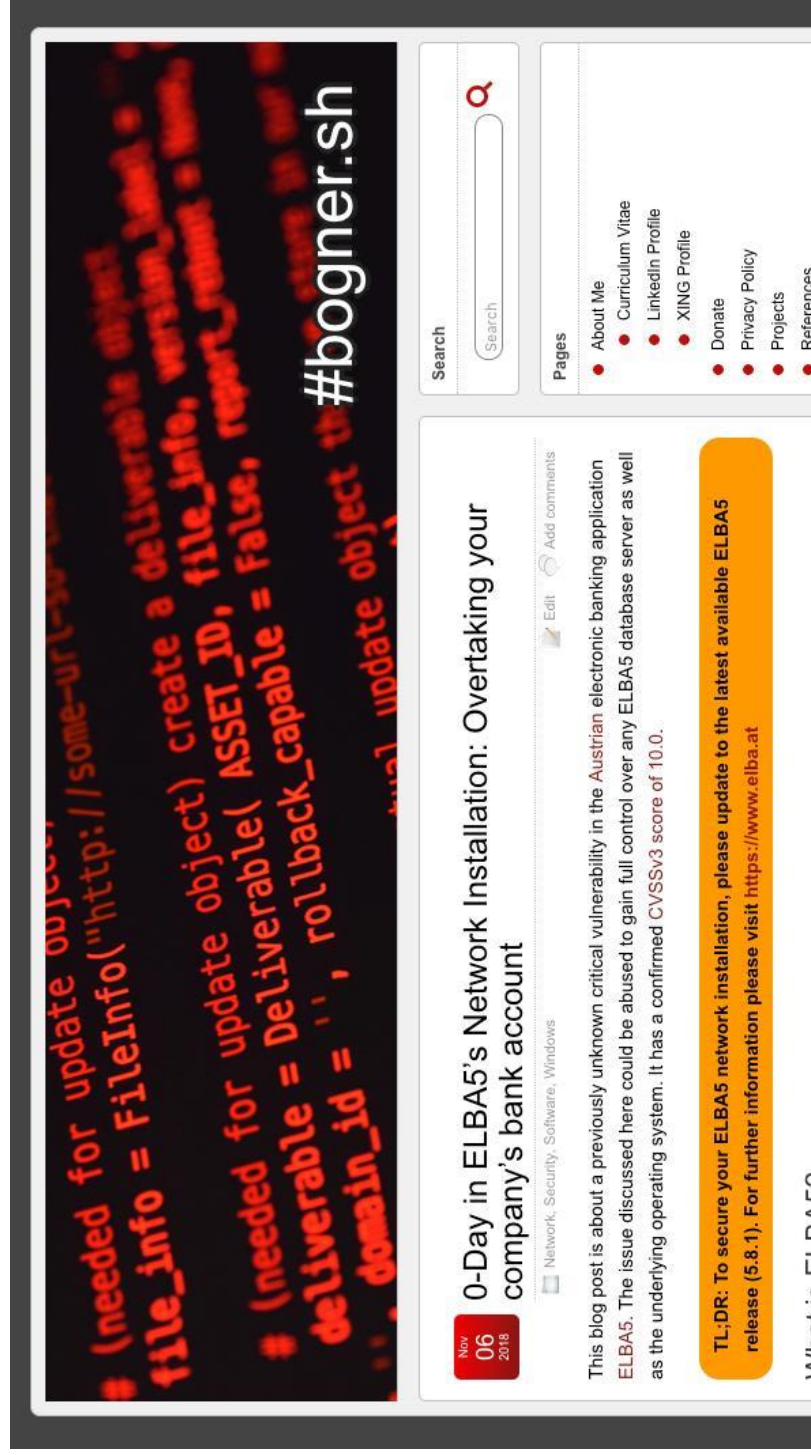


Security Incident Management

... mit 800 Mitarbeitern, auf 7 Standorten, für 800+ Applikationen:



Public Disclosure



Nov 06 2018

0-Day in ELBA5's Network Installation: Overtaking your company's bank account

Network Security, Software, Windows

This blog post is about a previously unknown critical vulnerability in the Austrian electronic banking application ELBA5. The issue discussed here could be abused to gain full control over any ELBA5 database server as well as the underlying operating system. It has a confirmed CVSSv3 score of 10.0.

TL;DR: To secure your ELBA5 network installation, please update to the latest available ELBA5 release (5.8.1). For further information please visit <https://www.elba.at>

WIKI: <https://www.elba.at>

(needed for update object) create a deliverable object
file_info = FileInfo("http://some-url-30...
(needed for update object) ASSET_ID, file_info, version_base =
deliverable = Deliverable(ASSET_ID, file_info, report_relevant = True,
domain_id = '', rollback_capable = False, report_relevant = True)
... update object the ...

#bogner.sh

Search

Pages

- About Me
- Curriculum Vitae
- LinkedIn Profile
- XING Profile
- Donate
- Privacy Policy
- Projects
- References

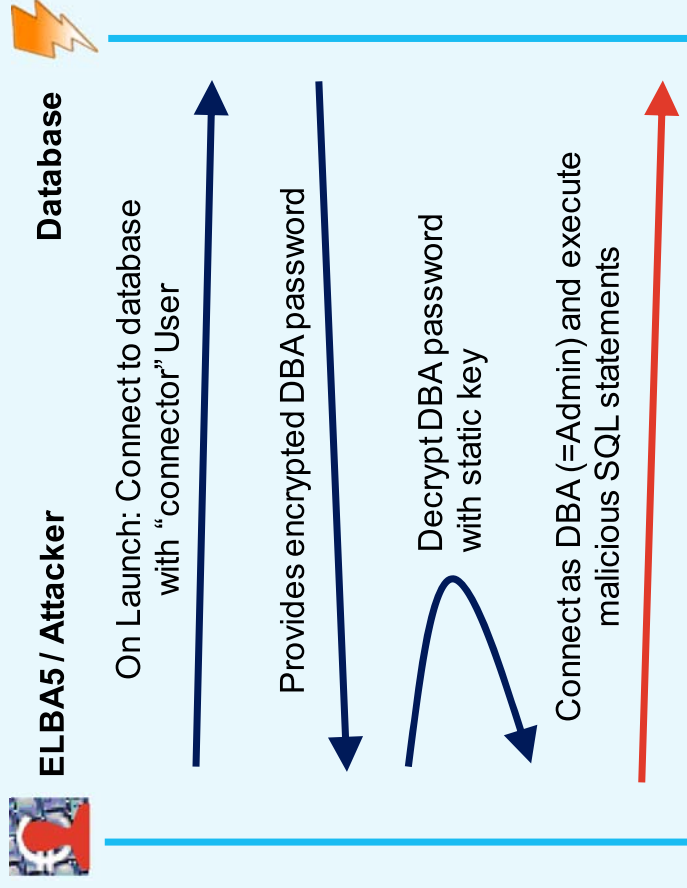
<https://bogner.sh/elba>



0-Day in ELBA5's Network Installation: Overtaking your company's bank account

On November 16th, 2018 the security experts of Bee IT Security disclosed a previously unknown vulnerability in the Austrian banking software ELBA5. It could be abused to remotely compromise any ELBA5 network installation as well as the underlying OS.

Attack Overview



Impact

Backdoor access

A new administrative user can be added to the ELBA5 network installation. This can be abused to create new transactions or to modify existing one's.

Remote Code Execution

As this issue can also be exploited to run arbitrary commands on the affected ELBA5 database server, it can be abused to overtake the complete system.



Solution: Update to the latest ELBA5 release (5.8.1)

Visit <https://www.elba.at> for more information.