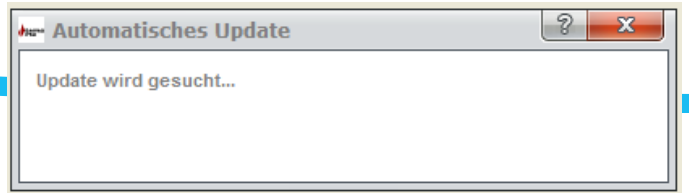
BEE ITSECURITY

Wenn ein CVSS Score von 10.0 ein leeres Bankkonto bedeuten kann

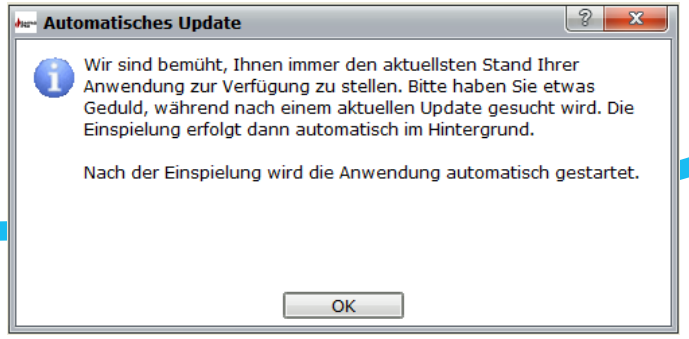
★ ★ ★ ★ ★

The Beginning: Can you spot the issue?

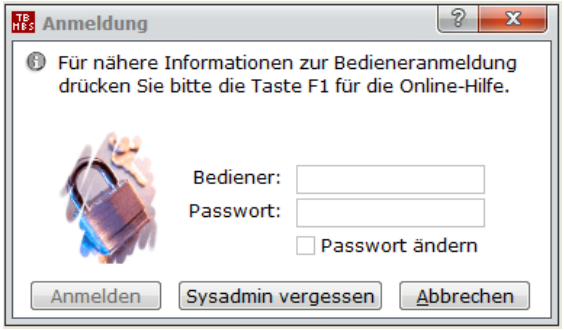
Launch the Online Banking Windows Client



Search for Updates

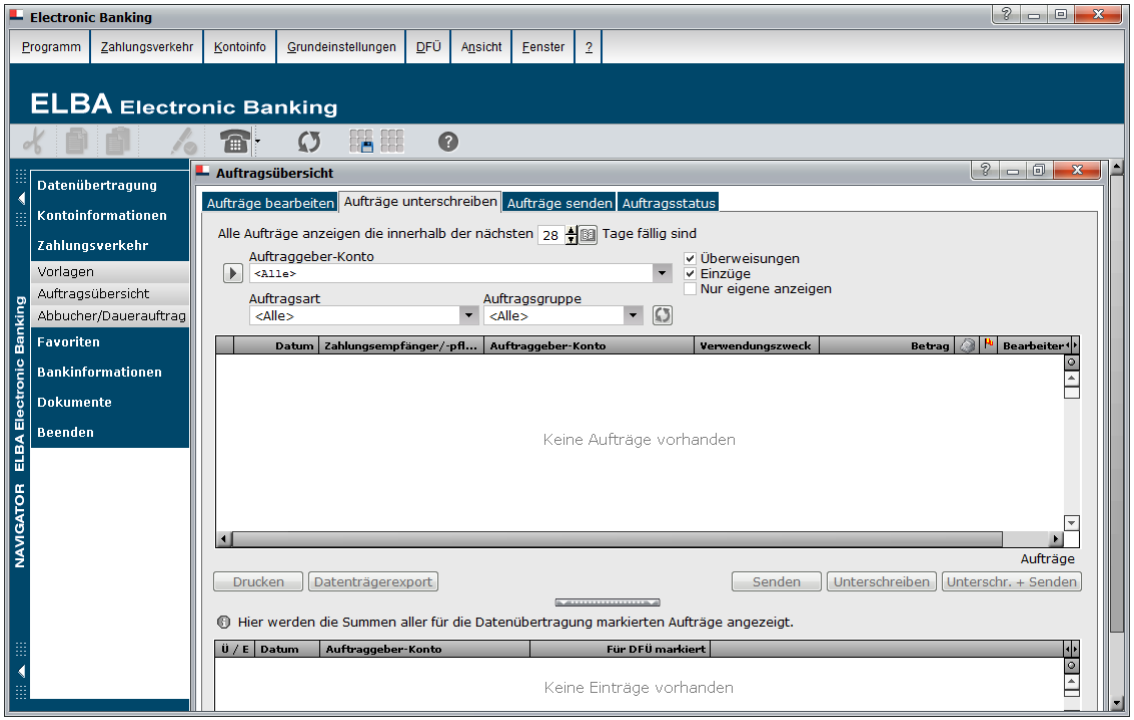


Apply Updates



Login

Disclosing a 0-Day in ELBA5



ELBA5 aka “telebankingMBS”
Online Banking for businesses

Disclosing a 0-Day in ELBA5

CVSSv3: 10.0

CRITICAL

(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

ELBA5 aka “telebankingMBS”

Online Banking for businesses

Disclosing a 0-Day in ELBA5

“

CVSSv3: 10.0

~~CRITICAL~~

(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

ELBA5 aka “telebankingMBS”

Online Banking for businesses

BEE ITSECURITY

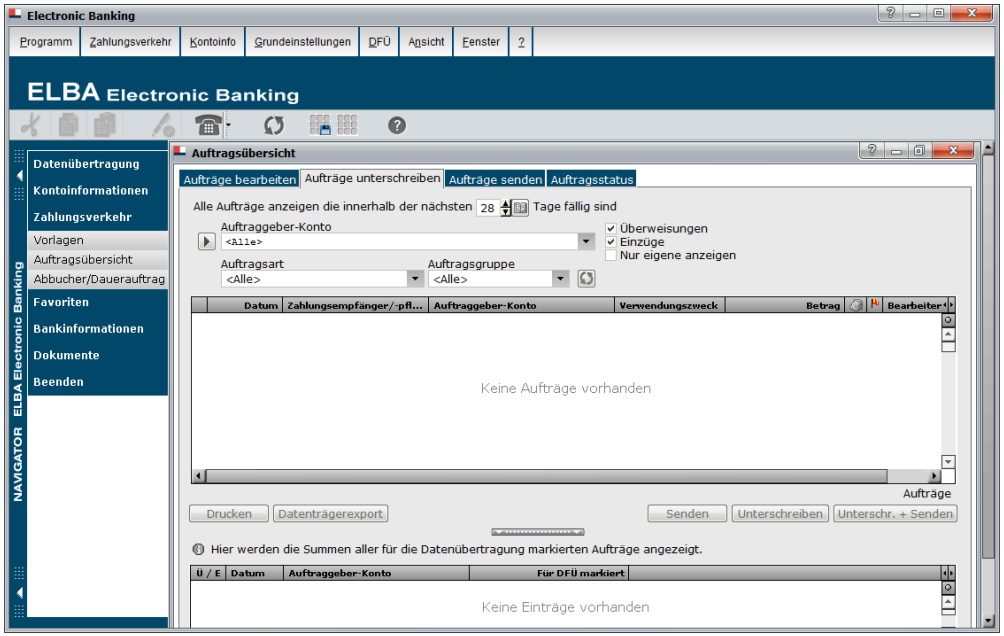
ELBA5 is used by …

24 Banks

80.000 Installations

5.000 Vulnerable

ELBA5 comes in 2 Variants



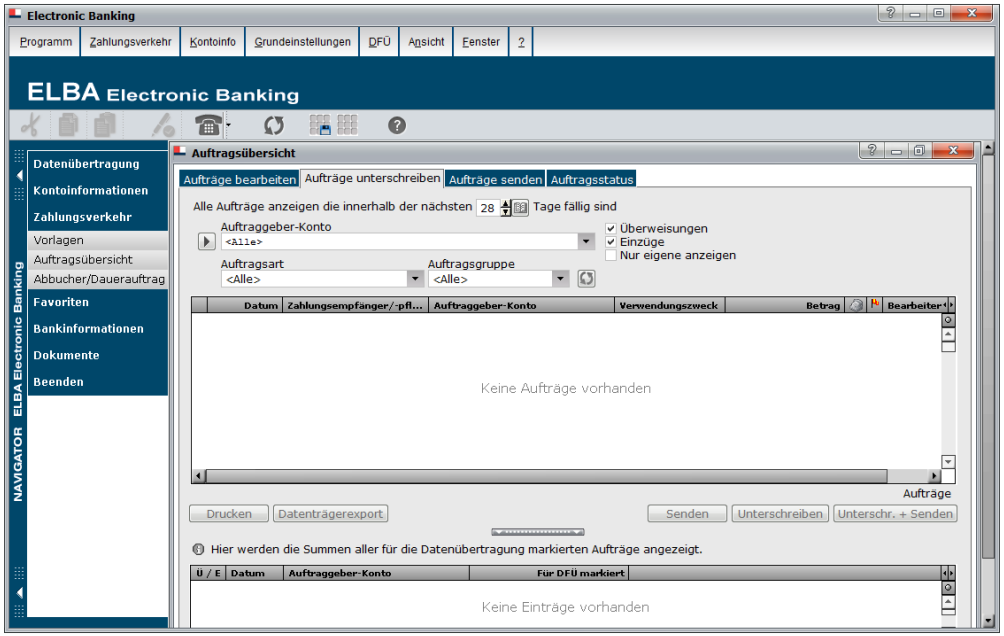
Client only

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



C — Client only

Single seat installation
No network interaction (except with bank)

N — Network

Multi-user installation
Communication over the net
with a central dat

VULNERABLE

BEE ITSECURITY

#whoami

Florian Bogner

IT Security Expert
aka “Professional Hacker”
Speaker and Trainer
Bug Bounty Hunter

More than 50 vulnerabilities reported to:

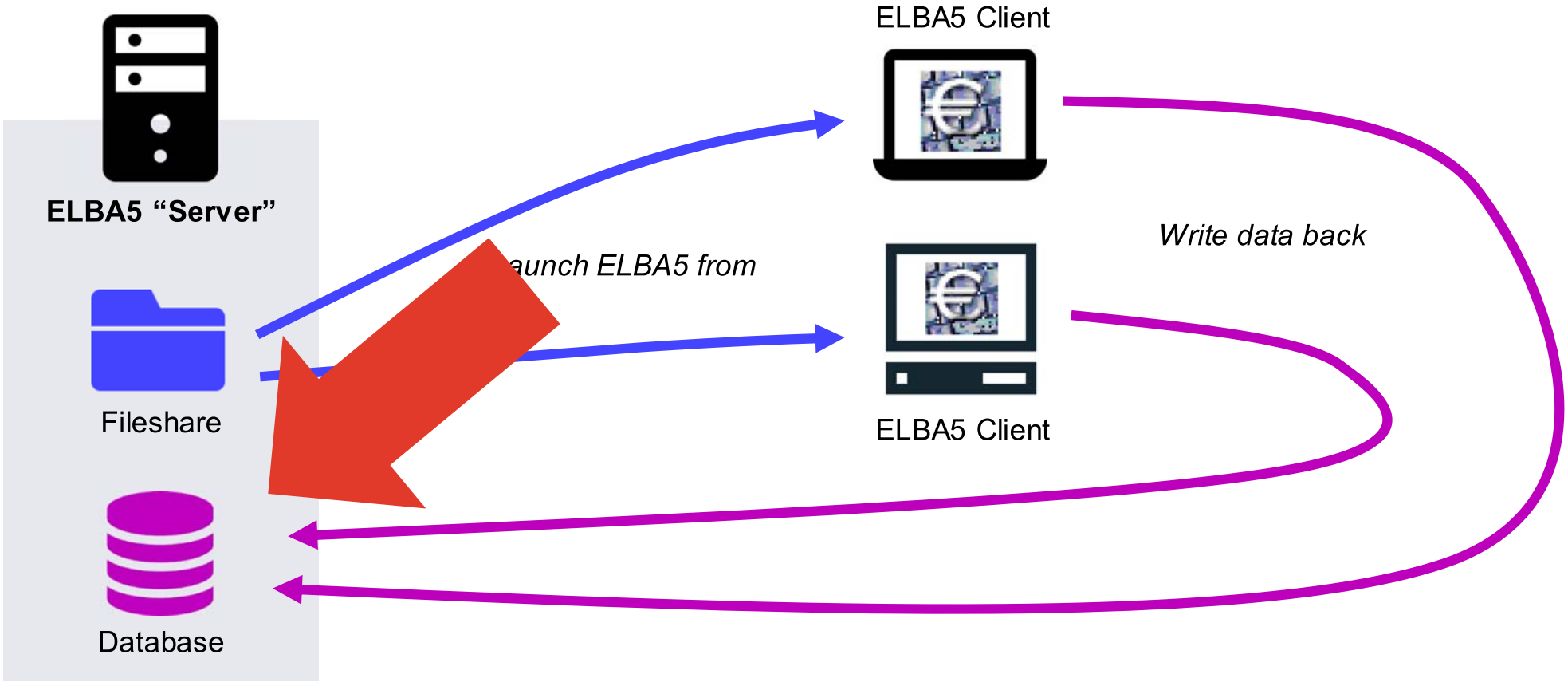
Google, Barracuda, Trend Micro, Cisco, Intel, F-Secure, AVG, Avira, Java, Check Point Software Technologies Ltd.

Raphael Zoidl

Application Security Manager

- Produktgruppe Electronic Banking (ELBA)

ELBA5 Network System Overview

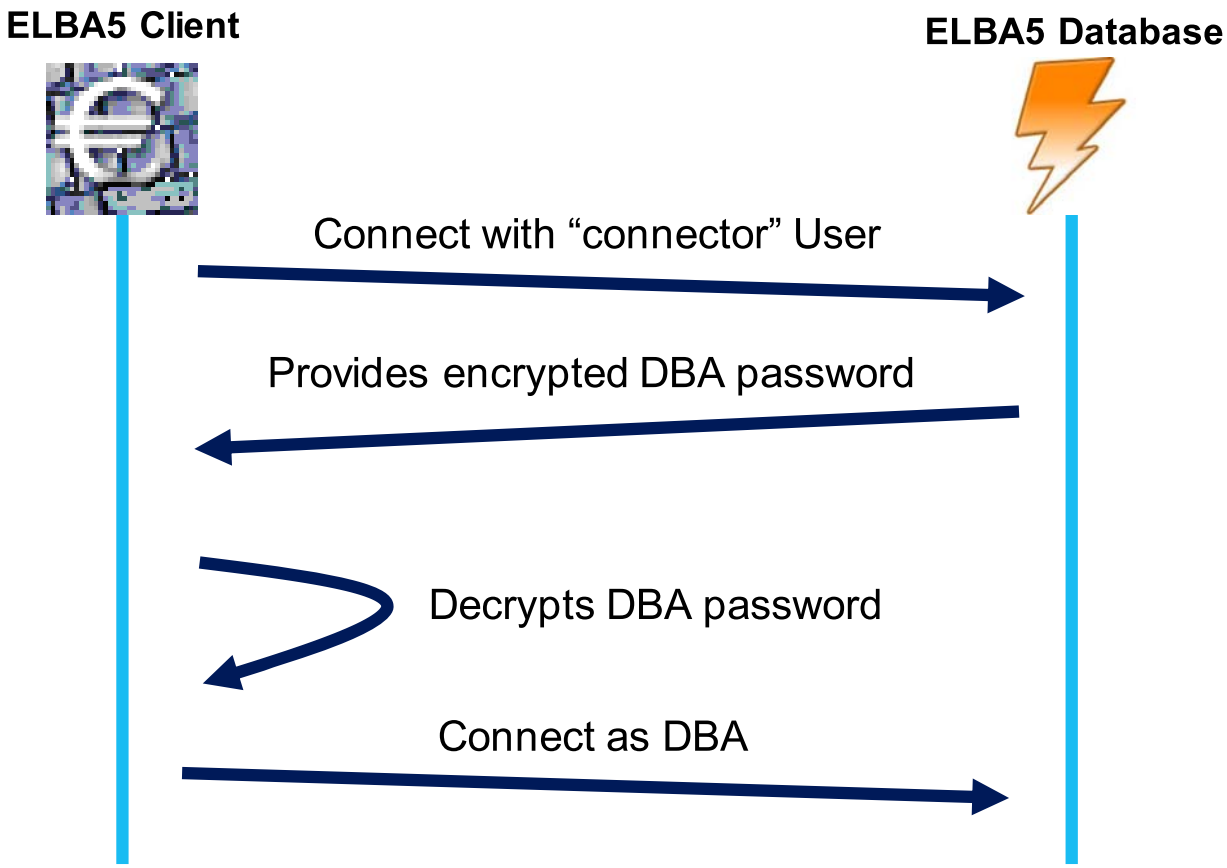


BEE ITSECURITY

Live Demo:
Desintegrating ELBA5

★ ★ ★ ★ ★

Summary



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

Summary

What can we do now?

EVERYTHING!


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

BEE ITSECURITY

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 …

2 Remote Code Execution

Because we don't care about money:
SQL: xp_cmdshell('the command')
We are SYSTEM! Mimikatz anyone?

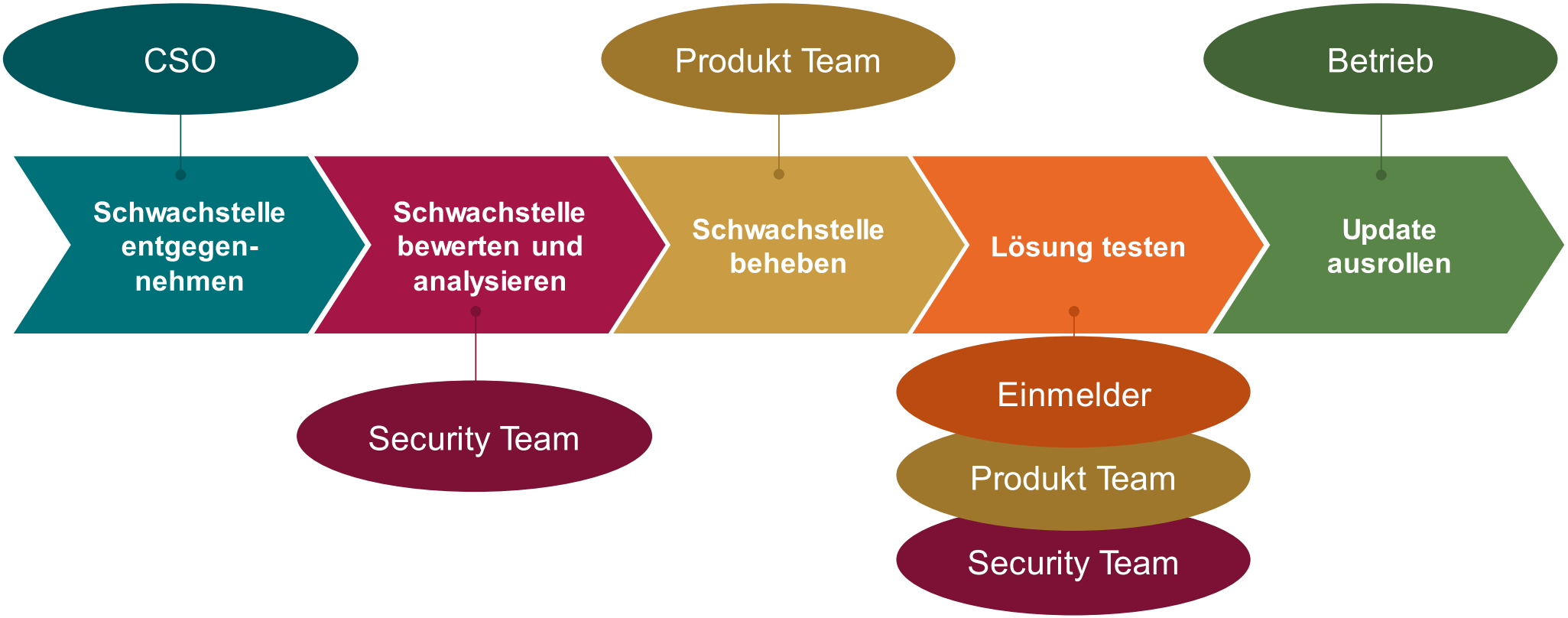
BEE ITSECURITY

Live Demo:
Because I can!

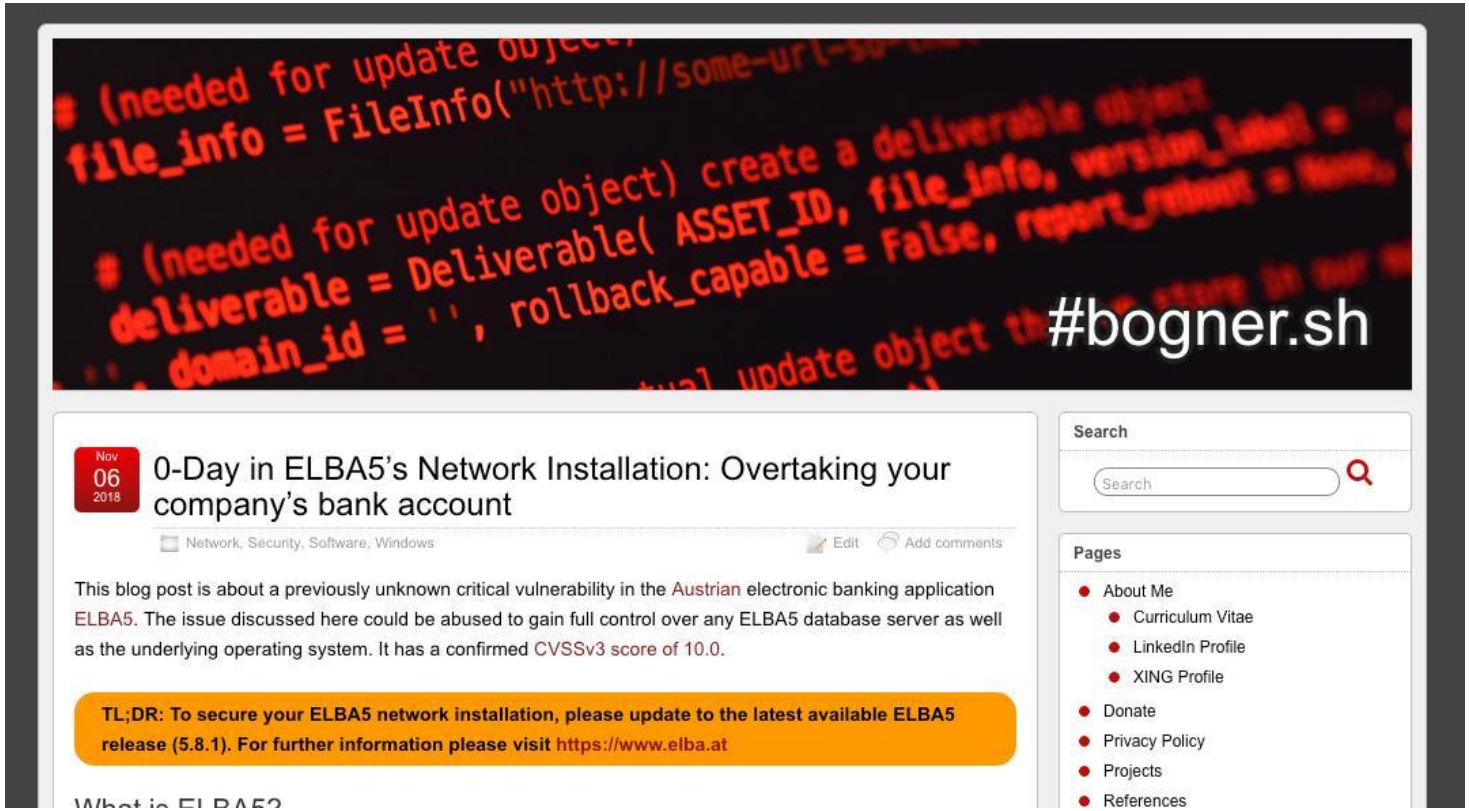
★ ★ ★ ★ ★

Security Incident Management

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



Public Disclosure



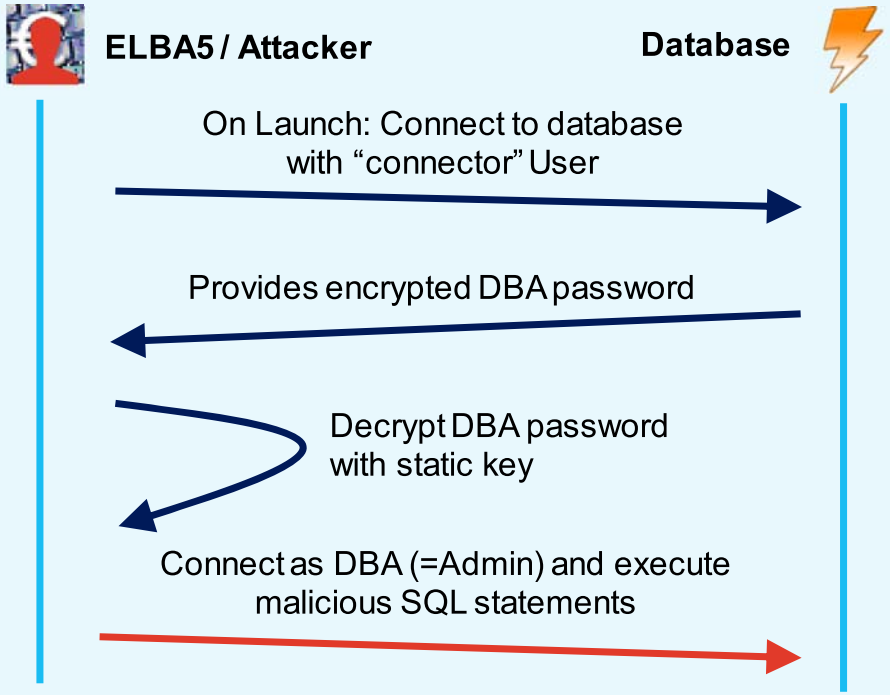
https://bogner.sh/elba

BEE ITSECURITY

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 ELBA 5 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.

If you have any questions, contact us at: florian@bee-itsecurity.at or https://bee-itsecurity.at