

Wenn ein CVSS Score von 10.0

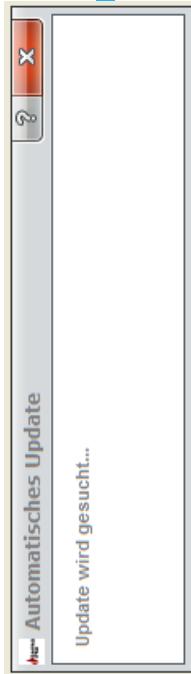
ein leeres Bankkonto bedeuten kann



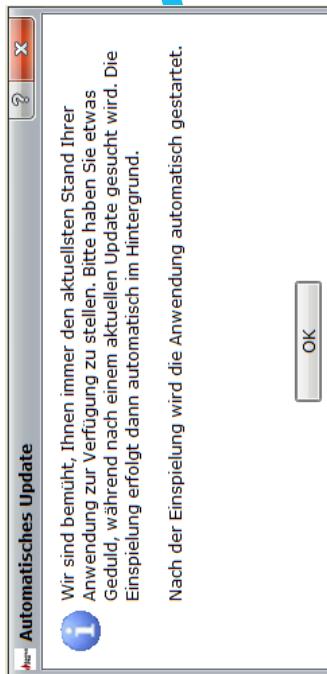
# The Beginning: Can you spot the issue?



Launch the Online  
Banking Windows Client



Search for Updates



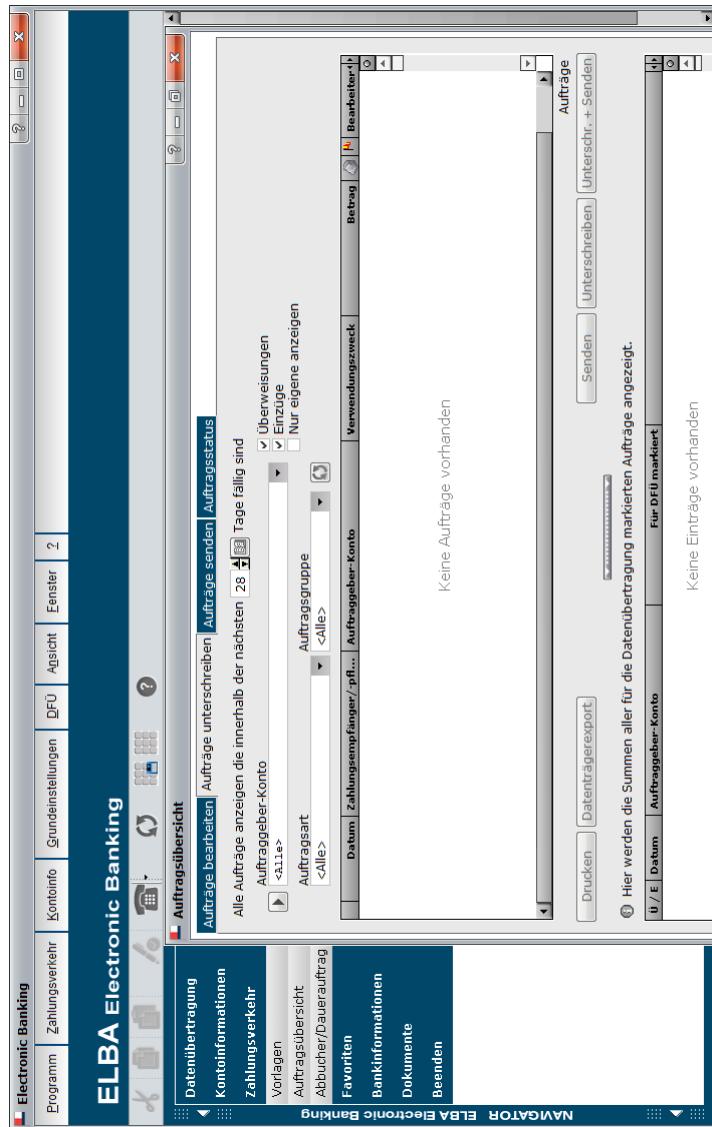
Apply Updates



Login



# Disclosing a 0-Day in ELBA5



**ELBA5 aka "telebankingMBS"**  
Online Banking for businesses

27/03/2018 // Overtaking your company's bank account



## Disclosing a 0-Day in ELBA5

FF



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

**ELBA5 aka “telebankingMBS”**  
Online Banking for businesses

## Disclosing a 0-Day in ELBA5

FF



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

**ELBA5 aka "telebankingMBS"**  
Online Banking for businesses

**ELBA5 is used by ...**

**24 Banks**

---

**80.000 Installations**

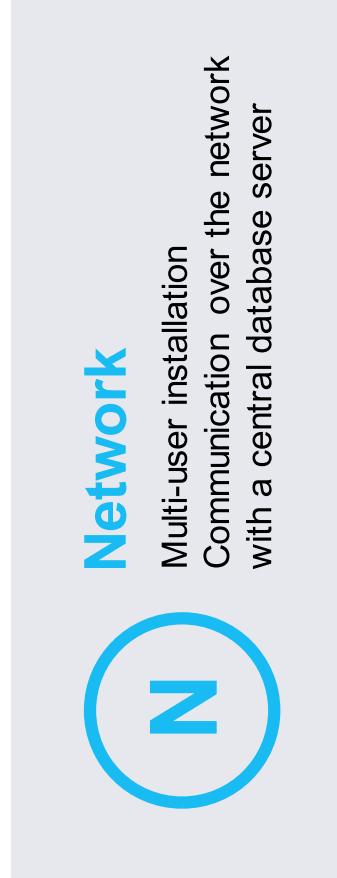
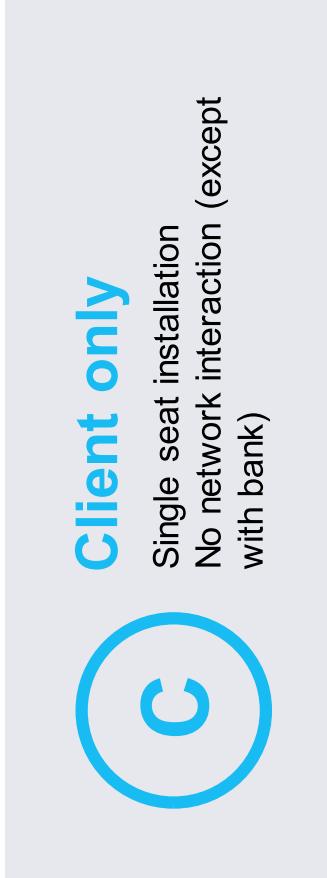
---

**5.000 Vulnerable**



## ELBA5 comes in 2 Variants

The screenshot shows the ELBA Electronic Banking software interface. The main menu bar includes 'Electronic Banking', 'Zahlungsservice', 'Kontoinfo', 'Grundseinstellungen', 'DFU', 'Ausdruck', 'Einstier', and 'Beenden'. The left sidebar has links for 'Datenübertragung', 'Kontoinformationen', 'Zahlungsverkehr', 'Vorlagen', 'Autrausübersicht', 'Autragsübertragung', 'Favoriten', 'Bankkundeninformationen', 'Dokumente', and 'Beenden'. The central window is titled 'Autragsübersicht' and displays a grid of orders. The grid columns include 'Datum', 'Zahlungsempfänger / pB...', 'Auftragsgeber-Konto', 'Verwendungszweck', 'Betrag', and 'Bearbeiter'. Filter options at the top of the grid allow selecting 'Alle Aufträge innerhalb der nächsten 28 Tage fällig sind', 'Überweisungen', 'Einzelne', and 'Nur eigene anzeigen'. At the bottom of the grid, there is a note: 'Hier werden die Summen aller für die Datenübertragung markierten Aufträge angezeigt.' A toolbar at the bottom of the window includes 'Drucken', 'Datenträgerexport', 'Senden', 'Unterschreiben', and 'Unterschr.+Senden'. The status bar at the bottom right shows 'NAVIGATOR ELBA Electronic Banking' and 'Keine Einträge vorhanden'.





BEE ITSECURITY

## ELBA5 comes in 2 Variants

The screenshot shows the ELBA Electronic Banking software interface. At the top, there are two tabs: "Client only" (selected) and "Network".

**Client only:** This variant is shown on the left side of the interface. It features a sidebar with navigation links: Datenübertragung, Kontoinformationen, Zahlungsverkehr, Vorlagen, Auftragsübersicht, Favoriten, Bankkundeninformationen, Dokumente, and Beenden. The main area displays a table for "Auftragsübersicht" (Order Overview) with columns: Datum, Zahnungsempfänger/-pBl., Auftragsgeber-Konto, Verwendungszweck, Betrag, and Bearbeiter. A message at the bottom states: "Keine Aufträge vorhanden".

**Network:** This variant is shown on the right side of the interface. It has a similar sidebar and table structure. A large red banner across the top of this section reads: "VULNERABLE". A message at the bottom of the table area states: "Hier werden die Summen aller für die Datenübertragung markierten Aufträge angezeigt." and "Keine Einträge vorhanden".



#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





**BEE IT SECURITY**

# Live Demo:

# Desintegrating ELBA5





## Summary

ELBA5 Client



ELBA5 Database



Connect with “connector” User

Provides encrypted DBA password

Decrypts DBA password

Connect as DBA



```
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  
elndba.connection
```



**BEE IT SECURITY**

# Live Demo:

# Weaponizing our Knowledge!





## Weaponizing our Knowledge!

### Transaction Tampering

Add a backdoor user:

**Password Hash: SHA256(password + bedienerKey + userDir)**

**SQL: INSERT INTO BEDIENER ...**

1



2

### Remote Code Execution

Because we don't care about money:

**SQL: xp\_cmdshell('the command')**

We are SYSTEM! Mimikatz anyone?





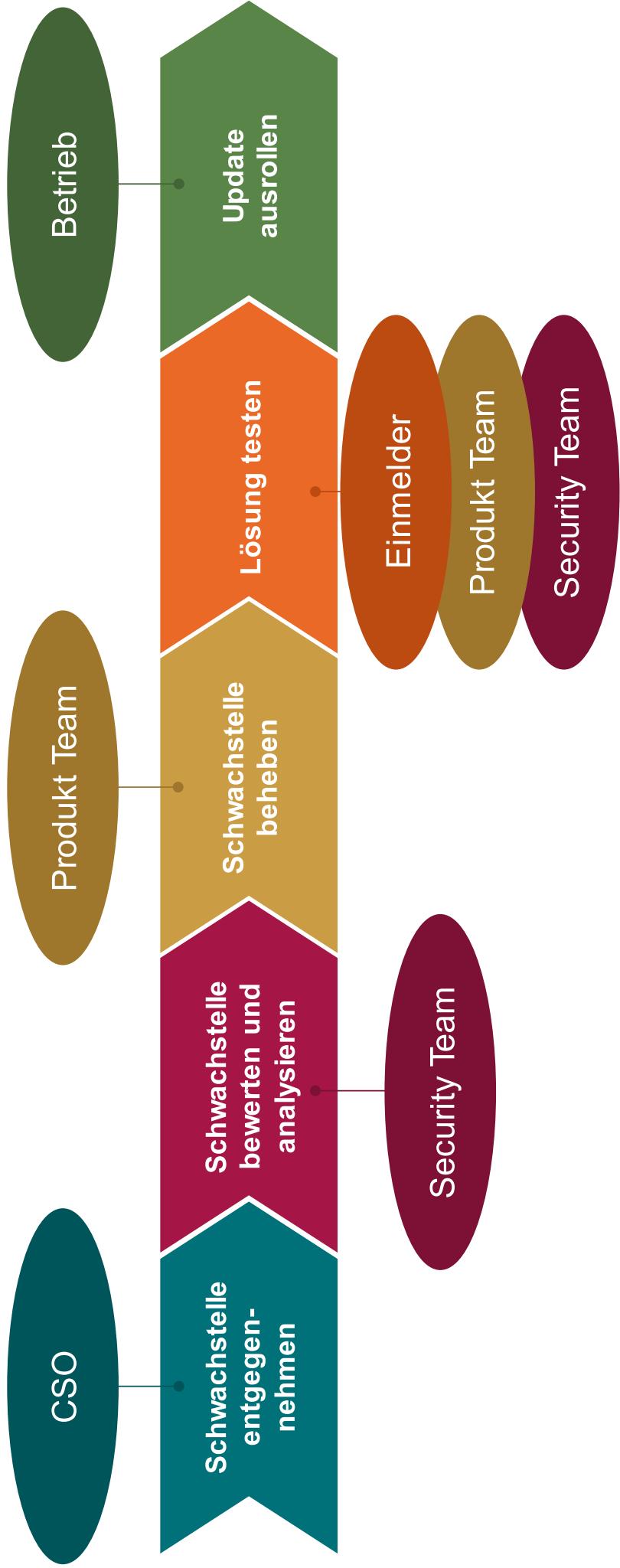
**BEE IT SECURITY**

**Live Demo:** **Because I can!**



# Security Incident Management

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





# Public Disclosure

# (needed for update object)  
file\_info = FileInfo("http://some-uri-to-object")  
# (needed for update object) create a deliverable, version, just  
# (needed for update object) ASSET\_ID, file\_info, report, format  
# (needed for update object) Deliverable = False, report  
# (needed for update object) rollback\_capable = True,  
# (needed for update object) domain\_id = "1",  
# (needed for update object) update object to new value

27/03/2018 // Overtaking your company's bank account

A vertical column of five solid red five-pointed stars.

<https://www.bee-itsecurity.at> // Page 20

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

On November 16<sup>th</sup>, 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



On Launch: Connect to database with "connector" User

Provides encrypted DBA password

Decrypt DBA password with static key

Connect as DBA (=Admin) and execute malicious SQL statements

### 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](mailto:florian@bee-itsecurity.at) or <https://bee-itsecurity.at>