anapur AG

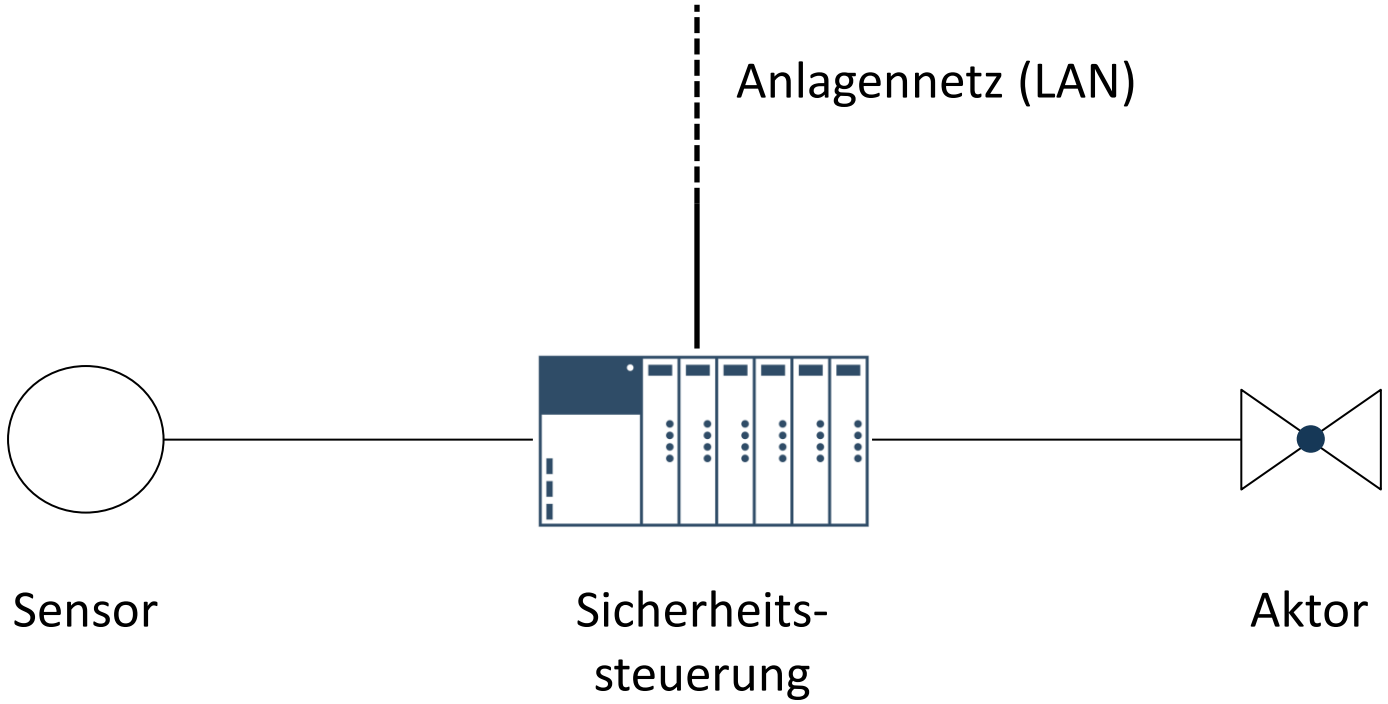
SICHERHEIT VON SICHERHEITSSTEUERUNGEN

anapur AG

AGENDA

- Angreifbarkeit von Sicherheitssystemen
- Angriffsbeispiele
  - Verschlüsselung Schreib-/Leseschutz-Passwort
  - Grenzen des netzwerkseitigen Zugriffschutzes

SICHERHEITSSYSTEM (SAFETY INSTRUMENTED SYSTEM)



ANGRIFFSVEKTOREN

- **Ausnutzung von Firmware-Schwachstellen**
  Ausnutzung von Schwachstellen, z.B. in der Implementierung der Kommunikationsstacks
- **Manipulation der Programmbausteine**
  Upload/Download von Bausteinen um den Programmablauf zu beeinflussen
- **Manipulation der verarbeiteten Daten**
  Verändern von Daten / Parametern, um den Programmablauf zu beeinflussen

AGENDA

- Angreifbarkeit von Sicherheitssystemen
- **Angriffsbeispiele**
  - **Verschlüsselung Schreib-/Leseschutz-Passwort**
  - Grenzen des netzwerkseitigen Zugriffschutzes

VERSCHLÜSSELUNG SCHREIB-/LESESCHUTZ-PASSWORT

```
0000   08 00 27 c9 16 19 20 87 56 70 29 44 08 00 45 00   ..'... .Vp)D..E.
0010   00 4d 57 6b 40 00 80 06 21 e7 c0 a8 00 07 c0 a8   .MWk@...!.......
0020   00 01 c1 28 00 66 58 68 10 6c 00 03 32 36 50 18   ...(.fXh.l..26P.
0030   fe 3f 51 4f 00 00 03 00 00 25 02 f0 80 32 07 00   .?QO.....%...2..
0040   00 09 00 00 08 00 0c 00 01 12 04 11 45 01 00 ff   ............E...
0050   09 00 08 26 21 12 06 33 1a 25 1c                  ...&!..3.%.
```

- Replay möglich
- Passwort: max. 8 Zeichen (ASCII)
- Qualität der Verschlüsselung?

ÜBUNG:
ANALYSE DES VERSCHLÜSSELUNGSALGORITHMUS

Plaintext	Hexadecimal	Ciphertext (Hexadecimal)
A	41	14 55 41 00 14 55 41 00
B	42	17 55 42 00 17 55 42 00
~	7e	2b 55 7e 00 2b 55 7e 00
AA	41 41	14 14 41 41 14 14 41 41
AB	41 42	14 17 41 42 14 17 41 42
AAA	41 41 41	14 14 00 41 55 14 00 41
AAAA	41 41 41 41	14 14 00 00 55 55 00 00
ABCDEFGH	41 42 43 44 45 46 47 48	14 17 02 06 12 15 00 08
test1234	74 65 73 74 31 32 33 34	21 30 07 11 63 76 05 17
startICS	73 74 61 72 74 49 43 53	26 21 12 06 33 1a 25 1c

ÜBUNG:
ANALYSE DES VERSCHLÜSSELUNGSALGORITHMUS

Plaintext	Hexadecimal	Ciphertext (Hexadecimal)
A	41	14 55 41 00 14 55 41 00
B		42 00
~		7e 00
AA		41 41
AAA		00 41
AAAA		00 00
AAAAAAAA		4 00 00
ABCDEFGH	41 42 43 44 45 46 47 48	14 17 02 06 12 15 00 08
test1234	74 65 73 74 31 32 33 34	21 30 07 11 63 76 05 17
startICS	73 74 61 72 74 49 43 53	26 21 12 06 33 1a 25 1c

Tool:

https://gchq.github.io/CyberChef/#recipe=From_Hex('Space')Magic(3,true,false,''/disabled)To_Hex('Space',0/disabled)

Lösung:

x = 0,1: plaintext [x] = cipher[x] XOR 55

x > 1: plaintext [x] = cipher[x] XOR plaintext [x-2]

anapur AG

AGENDA

- Angreifbarkeit von Sicherheitssystemen
- **Angriffsbeispiele**
  - Verschlüsselung Schreib-/Leseschutz-Passwort
  - **Grenzen des netzwerkseitigen Zugriffschutzes**

AUFBAU DER SICHERHEITSSTEUERUNG

Software

- *Betriebssystem*
- Logik- / Datenbausteine
  - Standard-Anwenderprogramm
  - Sicherheitsprogramm

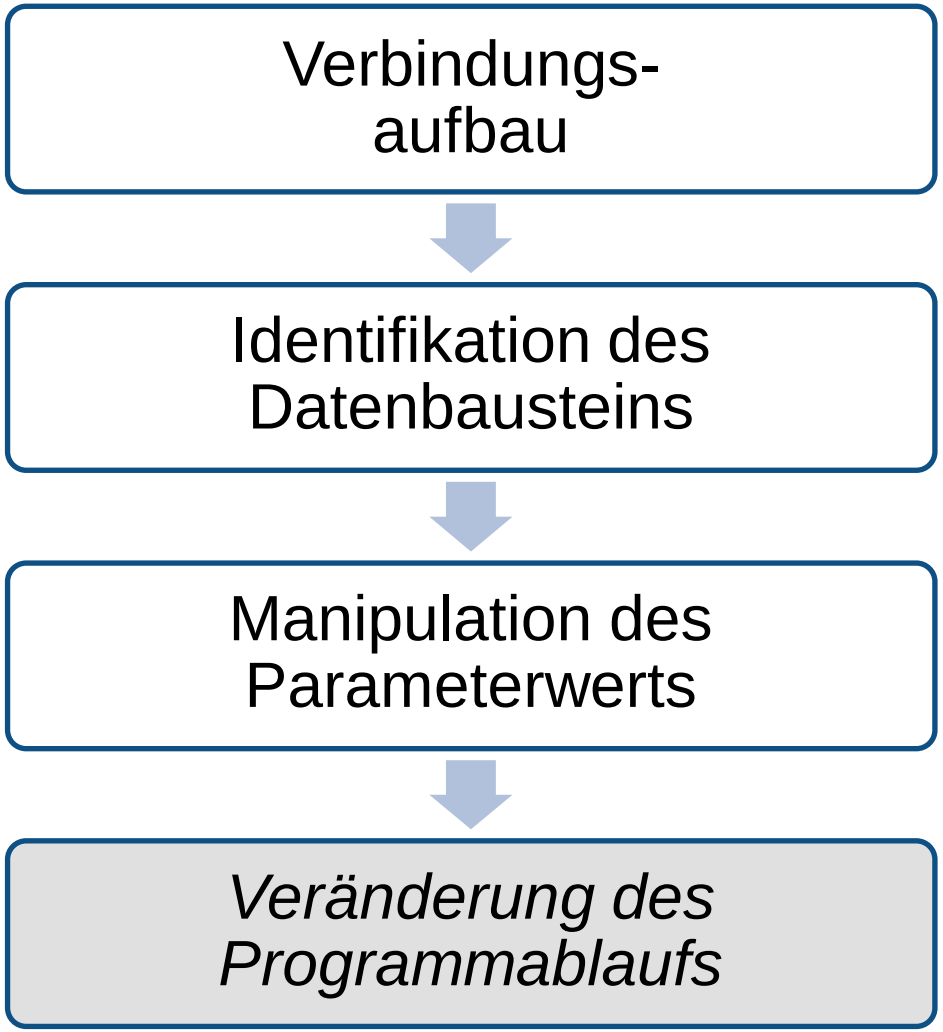
Daten

- Geräteinformationen (Bestellnummer, HW/SW-Stände, CPU-Status)
- Metadaten zu Logik- / Datenbausteinen
- Datenbausteine-Inhalte (Aktualwerte)
- Lokale Variablen / Funktionsparameter (Aktualwerte)

GRENZEN DES NETZWERKSEITIGEN ZUGRIFFSCHUTZES

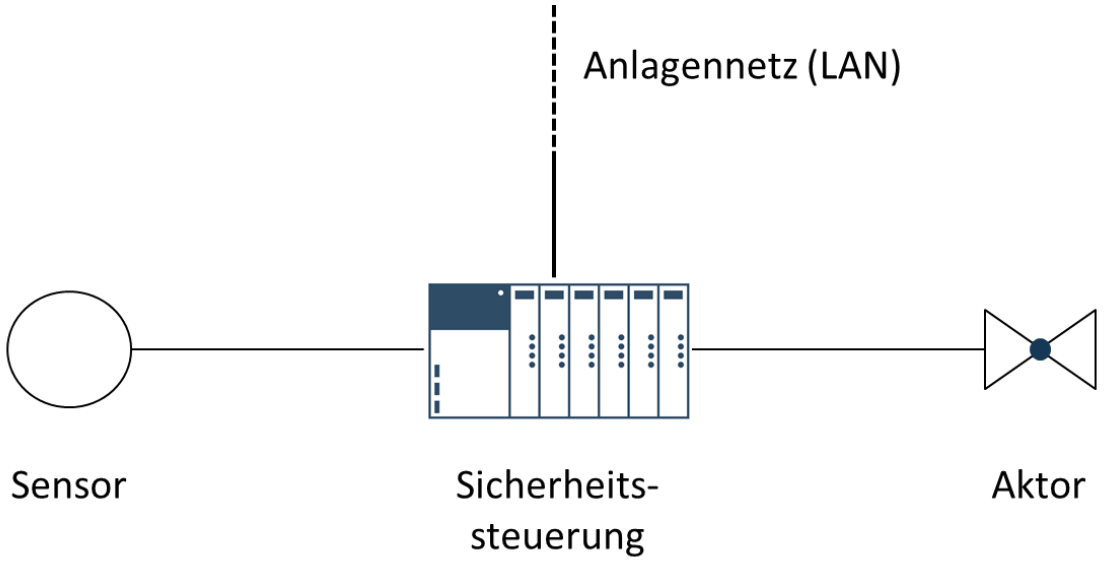
Element	Zugriffschutz
Standard-Anwenderprogramm	Passwort (Schreib-/Leseschutz)
Sicherheitsprogramm	Passwort (Schreib-/Leseschutz)
Geräteinformationen	/
Metadaten	/
Datenbausteine-Inhalte	/
Lokale Variablen / Funktionsparameter	*netzwerkseitig kein Zugriff*

ABLAUF DES ANGRIFFS



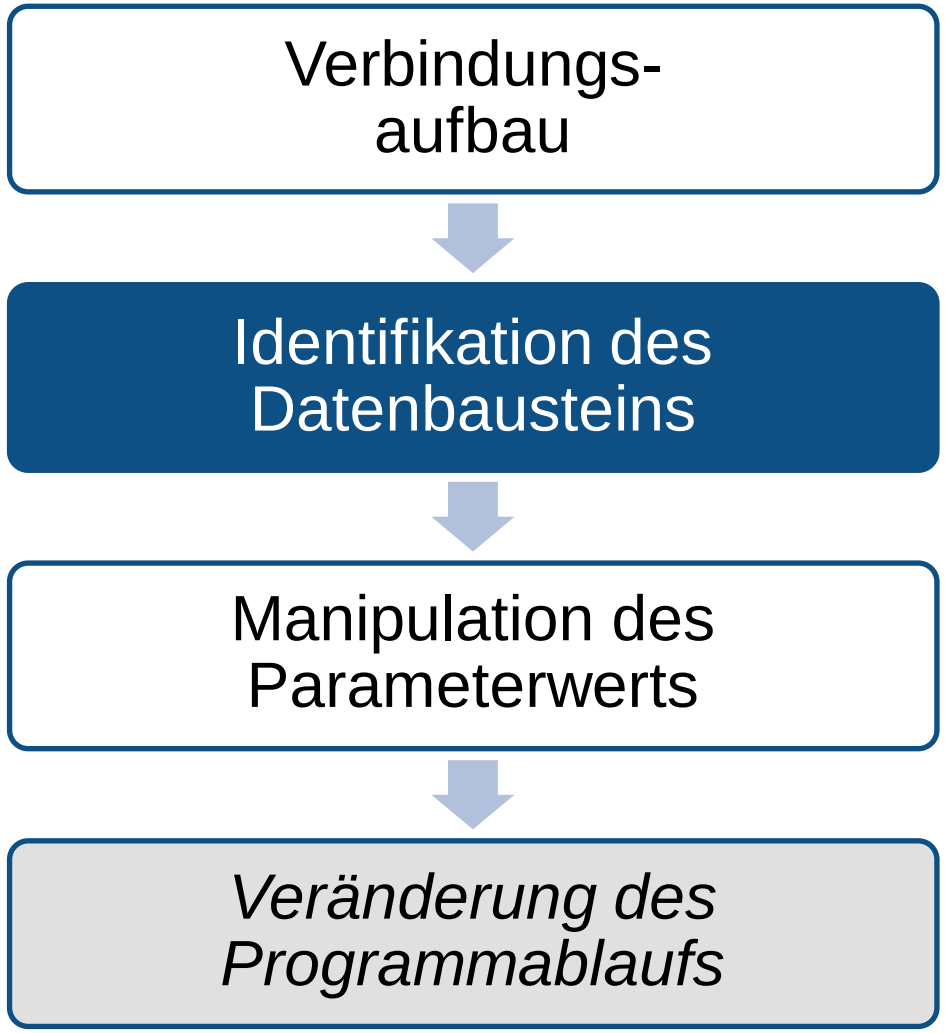
ABLAUF DES ANGRIFFS

- Verbindungs-aufbau
- Identifikation des Datenbausteins
- Manipulation des Parameterwerts
- *Veränderung des Programmablaufs*



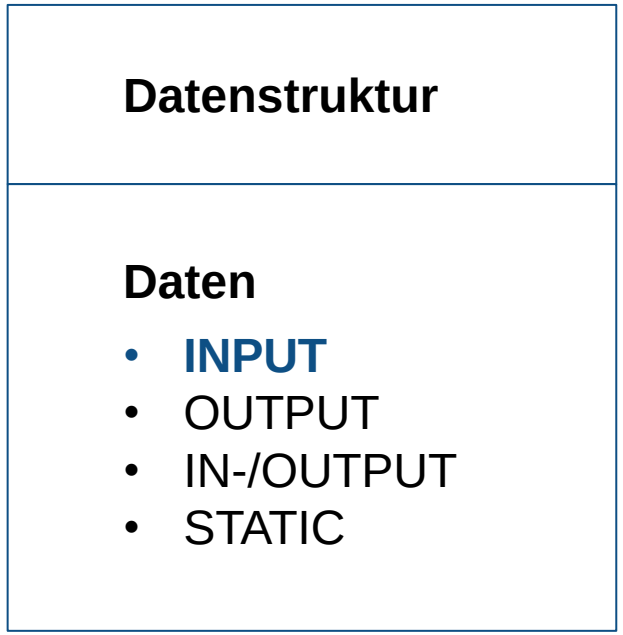
- Geräteinformationen
- Metadaten
- Datenbausteine-Inhalte

ABLAUF DES ANGRIFFS

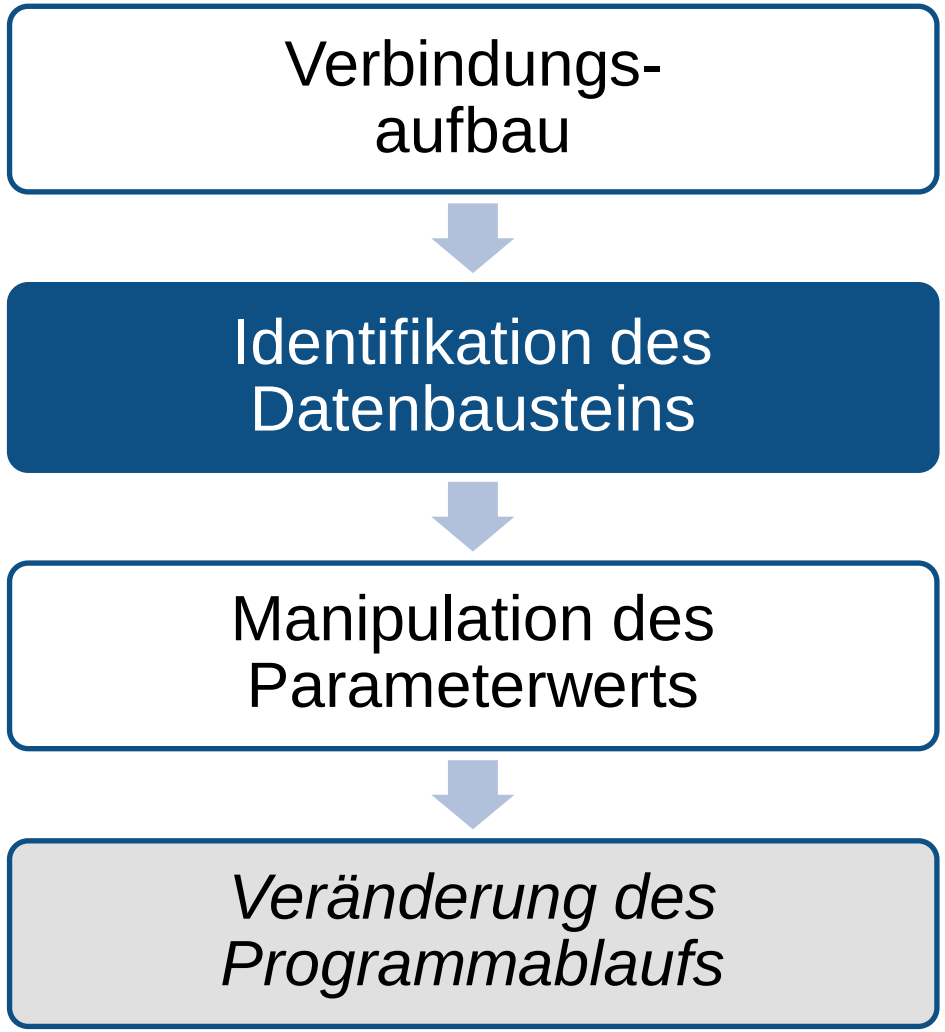


A. Leseschutz nicht aktiviert

- Upload der Logik- und Datenbausteine
- Identifikation relevanter Daten-bausteine und Speicherbereiche



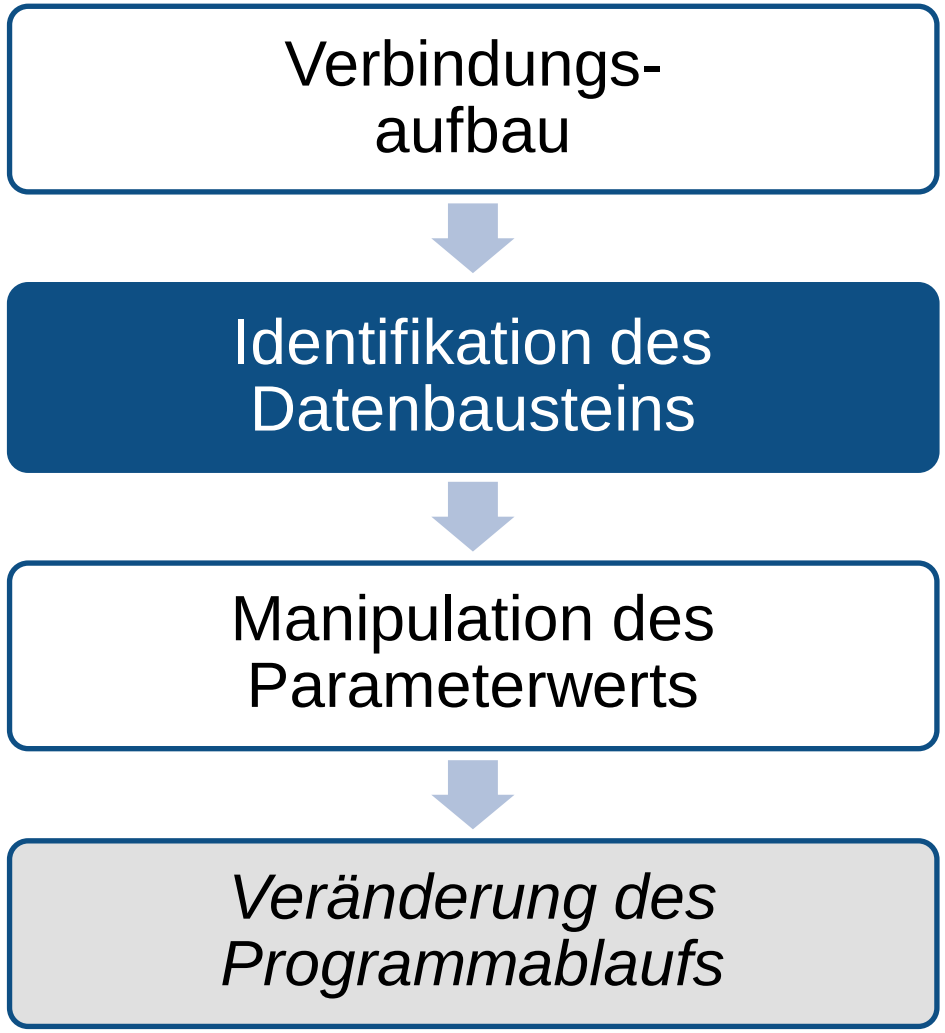
ABLAUF DES ANGRIFFS



B1. Fingerprinting - Metadaten

Block type	Code date
Block number	Interface date
Block language	Author
Block flags	**Family**
*[code]*Size	**Header**
Load memory size	
Local data	
SBB Length	
Checksum	
Version	

ABLAUF DES ANGRIFFS



B2. Fingerprinting - Datenplausibilität

Datenbausteine

Datenstruktur

Daten

- **INPUT**
- **OUTPUT**
- IN-/OUTPUT
- STATIC

ABLAUF DES ANGRIFFS

Verbindungs-
aufbau

Identifikation des
Datenbausteins

Manipulation des
Parameterwerts

*Veränderung des
Programmablaufs*

Datenbausteine

Datenstruktur

Daten

- **INPUT**
- OUTPUT
- IN-/OUTPUT
- STATIC

F-Datentypen

Datenwert
ID
Komplementwert

FAZIT

Die betrachtete Sicherheitssteuerung ist funktional sicher (“safe”), aber nicht vollständig gegen gezielte Angriffe geschützt (“secure”)

- **Verschlüsselung Schreib-/Leseschutz-Passwort**

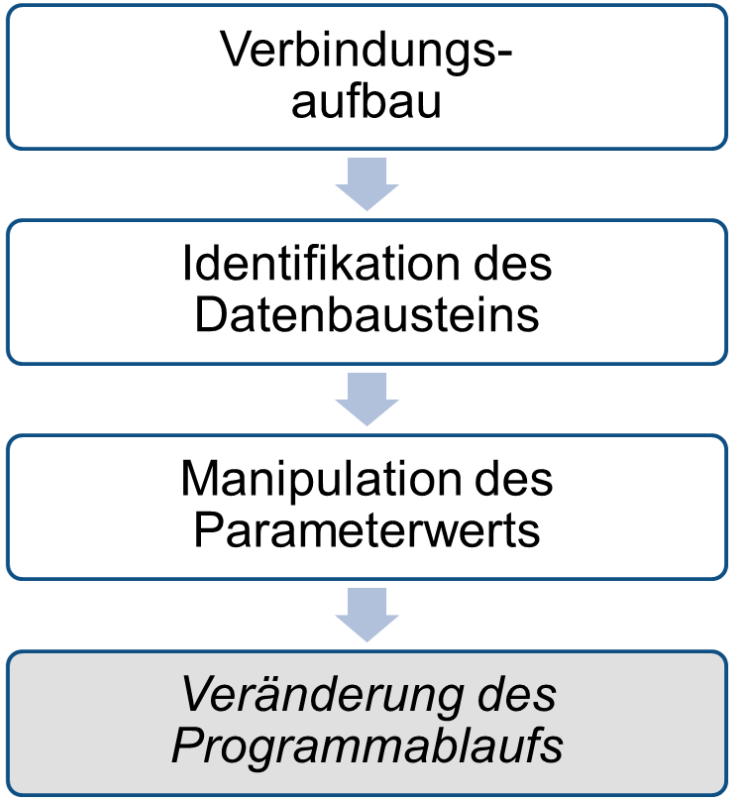
```
0000   08 00 27 c9 16 19 20 87 56 70 29 44 08 00 45 00
0010   00 4d 57 6b 40 00 80 06 21 e7 c0 a8 00 07 c0 a8
0020   00 01 c1 28 00 66 58 68 10 6c 00 03 32 36 50 18
0030   fe 3f 51 4f 00 00 03 00 00 25 02 f0 80 32 07 00
0040   00 09 00 00 08 00 0c 00 01 12 04 11 45 01 00 ff
0050   09 00 08 26 21 12 06 33 1a 25 1c
```

Lösung:

x = 0,1: plaintext [x] = cipher[x] XOR 55

x > 1: plaintext [x] = cipher[x] XOR plaintext [x-2]

Grenzen des netzwerkseitigen Zugriffschutzes



anapur AG

DIE BETRACHTETE SICHERHEITSSTEUERUNG IST FUNKTIONAL SICHER (“SAFE”), ABER NICHT VOLLSTÄNDIG GEGEN GEZIELTE ANGRIFFE GESCHÜTZT (“SECURE”)

Vielen Dank!

Dr. Felix Kahrau

Tel: +49 (6233) 880393-15 Fax: -29
mailto: f.kahrau@anapur.de

anapur AG