"T.I.S.P. Community Meeting 2022"

Berlin, 09.-10.11.2022

Was Trüffelschweine mit unserem Team Red gemein haben

Warum Penetrationstests ein unumgänglicher Schritt zur Erhöhung der IT-Sicherheit sind

Carsten Vossel, CCVOSSEL GmbH

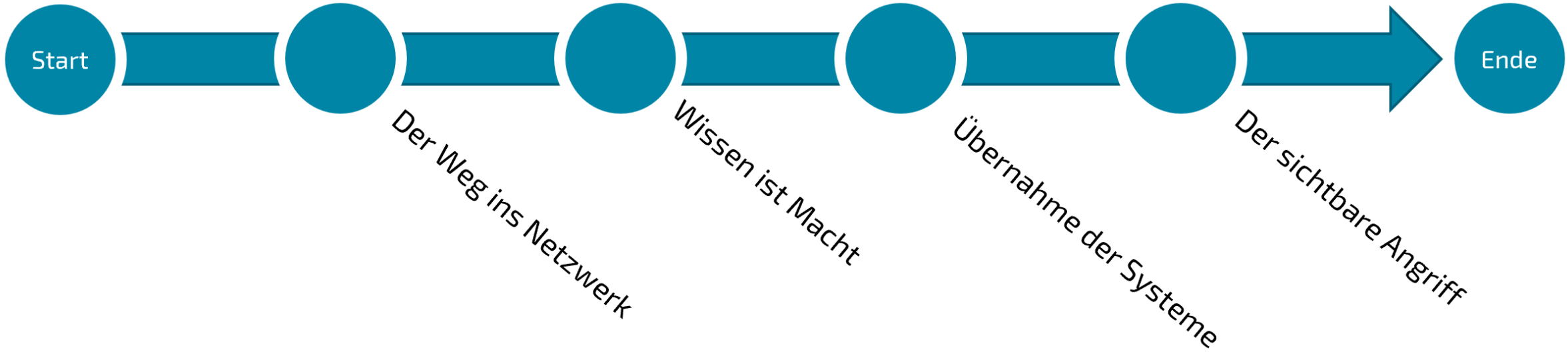
Systembetrieb versus Systemsicherheit

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Ziel: laufender Betrieb
- Rahmenparameter:
  - Zeitdruck bei Problemen
  - Inhomogene Systemlandschaft (Hardware, OS, Software)
  - Technischer Fokus
- Werkzeuge:
  - OS, RMM, Tickets, System

- Ziel: Probleme aufdecken
- Rahmenparameter:
  - nicht Zeitkritisch
  - Hubschrauberperspektive (toolgestützte Analyse)
  - Menschen, Technik & Prozesse im Fokus
- Werkzeuge:
  - Mikikatz, Vulnerability Scanner, PS

Vorgehensweise beim Angriff



Start

Der Weg ins Netzwerk

Wissen ist Macht

Übernahme der Systeme

Der sichtbare Angriff

Ende

Start

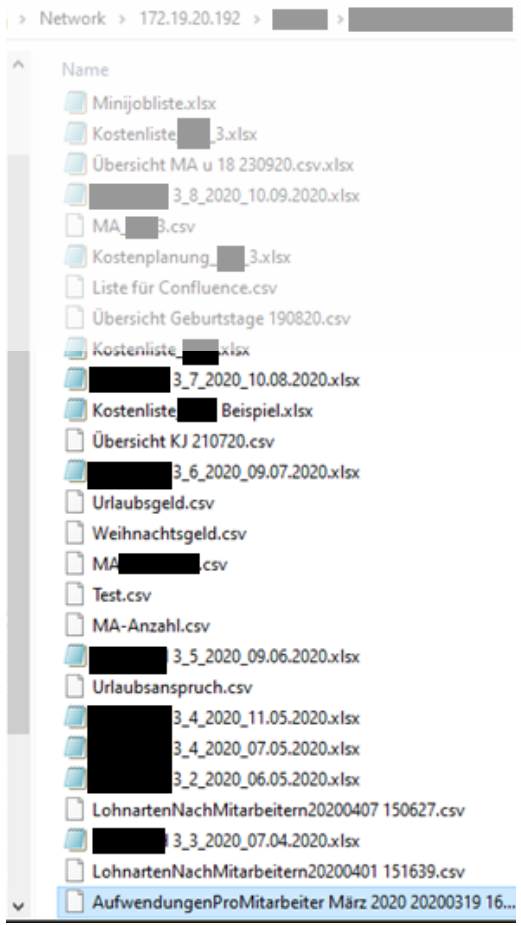
Der Weg ins Netzwerk

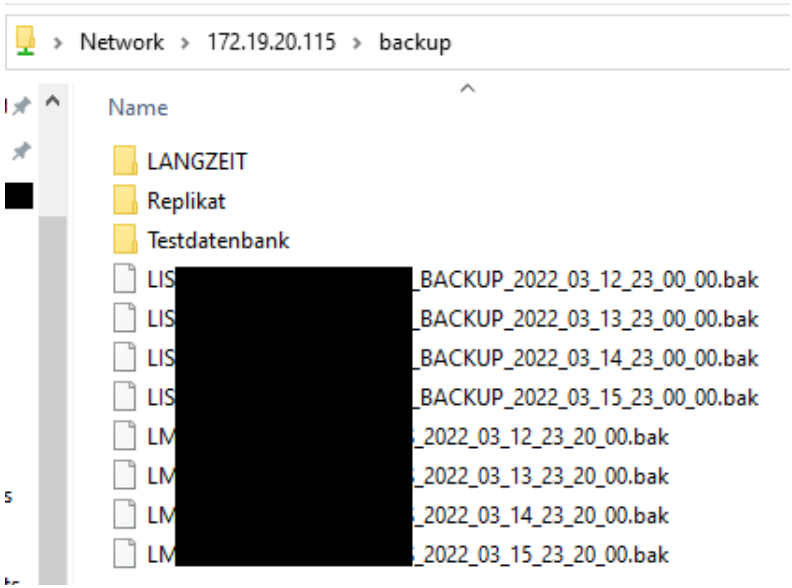
Wissen ist Macht

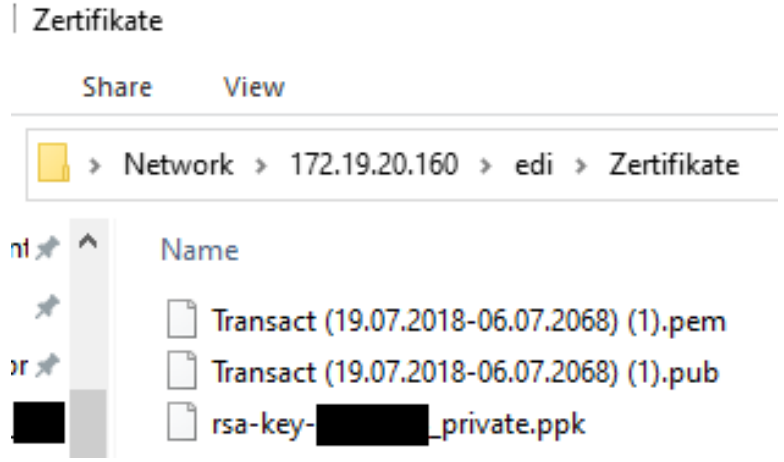
Übernahme der Systeme

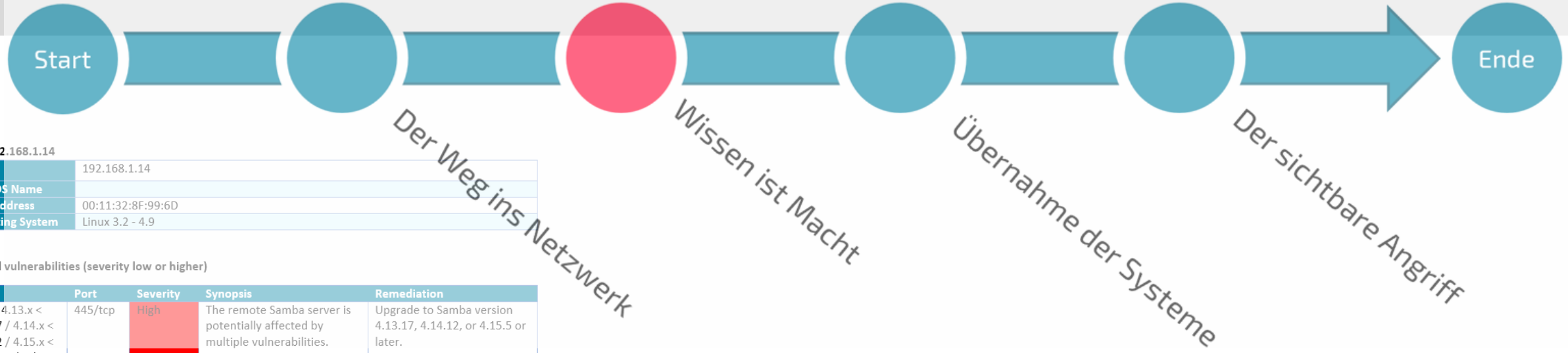
Der sichtbare Angriff

Ende







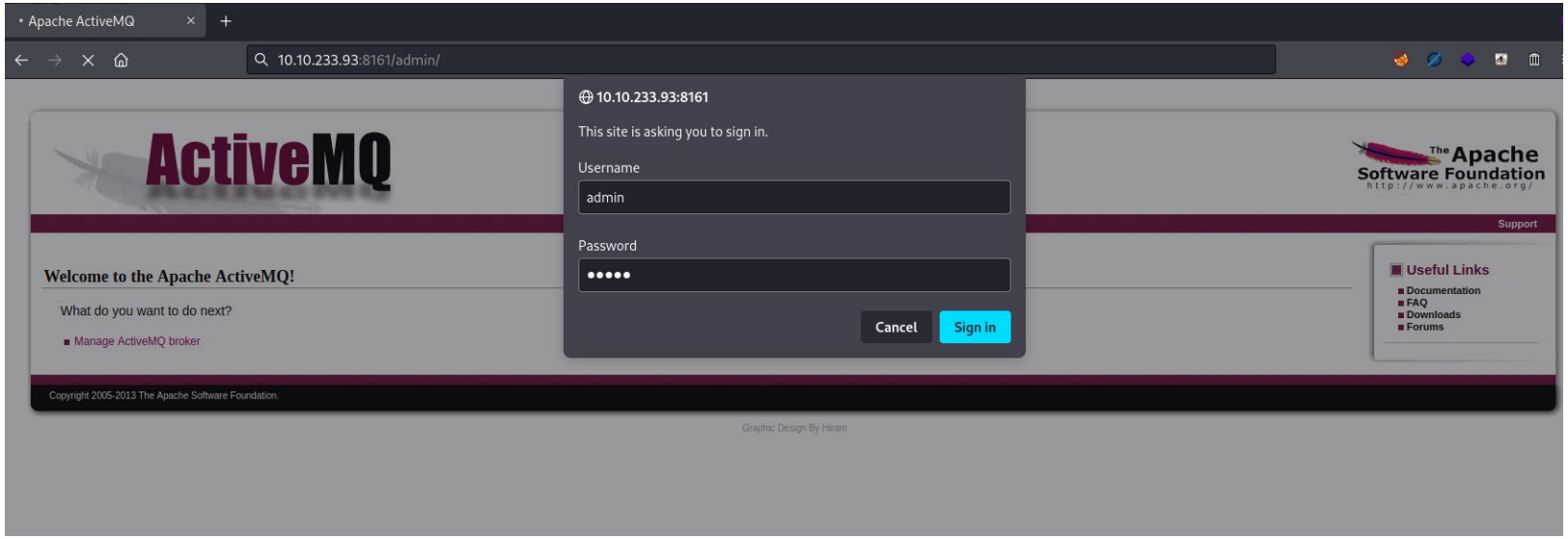


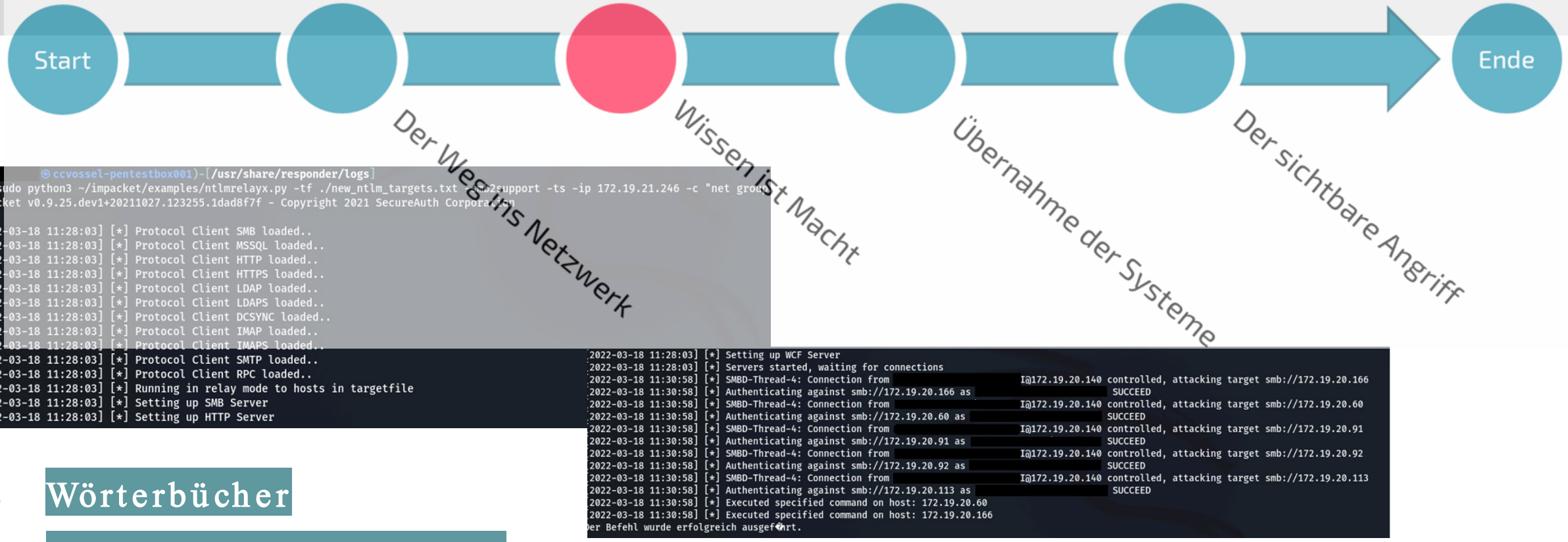
Host 192.168.1.14

IPv4	192.168.1.14
NetBIOS Name	
MAC Address	00:11:32:8F:99:6D
Operating System	Linux 3.2 - 4.9

Affected vulnerabilities (severity low or higher)

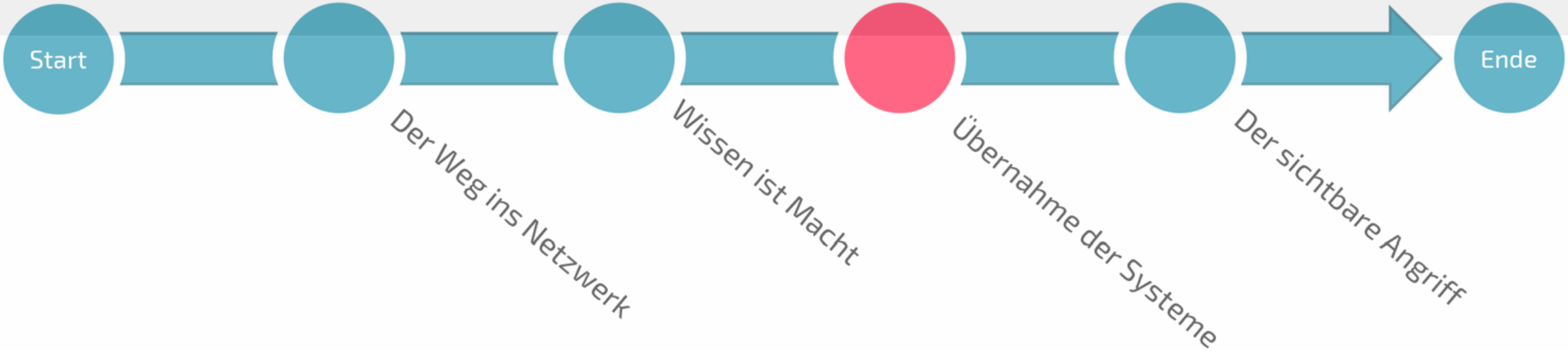
Name	Port	Severity	Synopsis	Remediation
Samba 4.13.x < 4.13.17 / 4.14.x < 4.14.12 / 4.15.x < 4.15.5 Multiple Vulnerabilities	445/tcp	High	The remote Samba server is potentially affected by multiple vulnerabilities.	Upgrade to Samba version 4.13.17, 4.14.12, or 4.15.5 or later.
SSL Certificate with Wrong Hostname	443/tcp	Medium	The SSL certificate for this service is for a different host.	Purchase or generate a proper SSL certificate for this service.
SSL Certificate with Wrong Hostname	5001/tcp	Medium	The SSL certificate for this service is for a different host.	Purchase or generate a proper SSL certificate for this service.
SSL Certificate Cannot Be Trusted	443/tcp	Medium	The SSL certificate for this service cannot be trusted.	Purchase or generate a proper SSL certificate for this service.
SSL Certificate Cannot Be Trusted	5001/tcp	Medium	The SSL certificate for this service cannot be trusted.	Purchase or generate a proper SSL certificate for this service.
SMB Signing not required	445/tcp	Medium	Signing is not required on the remote SMB server.	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.





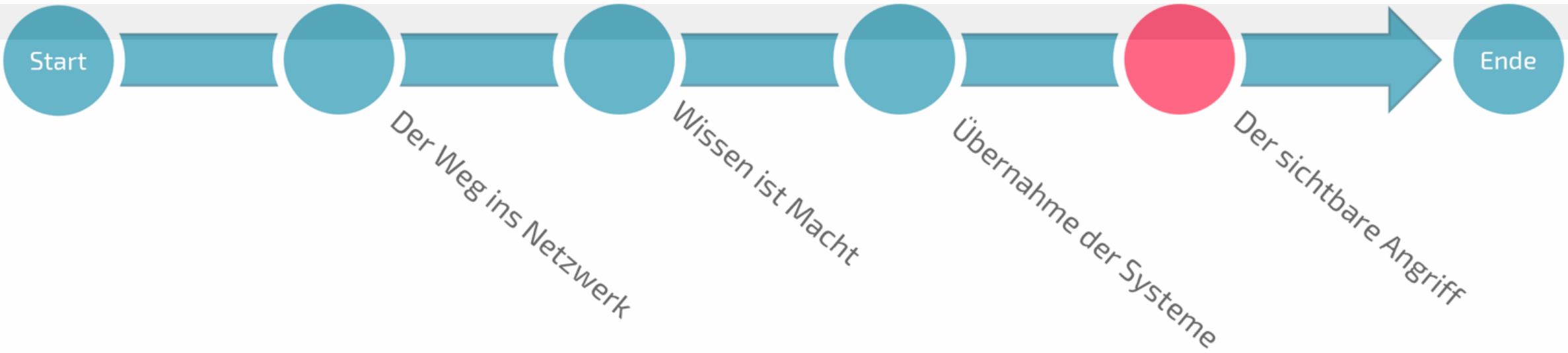
- Wörterbücher
- zusätzliche Informationen
  z.B. Kundennamen (Webseite)
- Straßennamen

```
Admin:1000:aad3b435b51404eeaad3b435b51404ee:e10adc3949ba59abbe56e057f20f883e:::
Tino:2000:aad3b435b51404eeaad3b435b51404ee:77d5c5a637ae1c047fb3d73394000081:::
Tatjana:1718:aad3b435b51404eeaad3b435b51404ee:85DEEEC2D12F917783B689AE94990716:::
Silvio:1717:aad3b435b51404eeaad3b435b51404ee:F3E6B2997D0AAA15C50E8DD0EE057882:::
Systemhaus:1714:aad3b435b51404eeaad3b435b51404ee:94F789887FDD9CA9764A7818F7324FDE:::
Stephan:1711:aad3b435b51404eeaad3b435b51404ee:6671560CB362AC42E3B1182269A0F6BA:::
Karsten:1711:aad3b435b51404eeaad3b435b51404ee:4D973148C582C4F7D8CE31F837C74AE8:::
```



Nachdem identifizieren von Schwachstellen in Systemen und Netzwerkkomponenten….

- Nutzen wir geeignete Einbruchswerkzeuge (Exploits)
- Suchen nach Lücken die der Schwachstellenscanner nicht identifizieren konnten
- Holen uns immer weitere Daten/Informationen (PWD, Personen, BWA)



Was passiert nach der Übernahme eines Domänenbenutzers oder Domänencomputers?

- Spionage
- Manipulation
- Verschlüsselung
- Veröffentlichung

Top 10 der häufigsten technischen Erkenntnisse

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- **Passwort Policy**

  Fehlende Regeln und Überwachung

- **Netzwerksegmentierung**

  Das interne Netzwerk ist nicht segmentiert.

  Server, Clients, Gäste befinden sich im gleichen Netzwerk

- **Account-Verwendungszweck**

  Es gibt keine Trennung zw. Administrativen und Nutzeraccounts

Top 10 der häufigsten technischen Erkenntnisse

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- **Anzahl der Administratoren**

  Es gibt zu viele Domain-Administratoren (max. 2)

- **Active Directory**

  Das AD ist unsauber - ungenutzte Objekt wurden nicht gelöscht

- **Firewall**

  Es bestehen „any-any“ Regeln auf der Firewall

- **Patchmanagement**

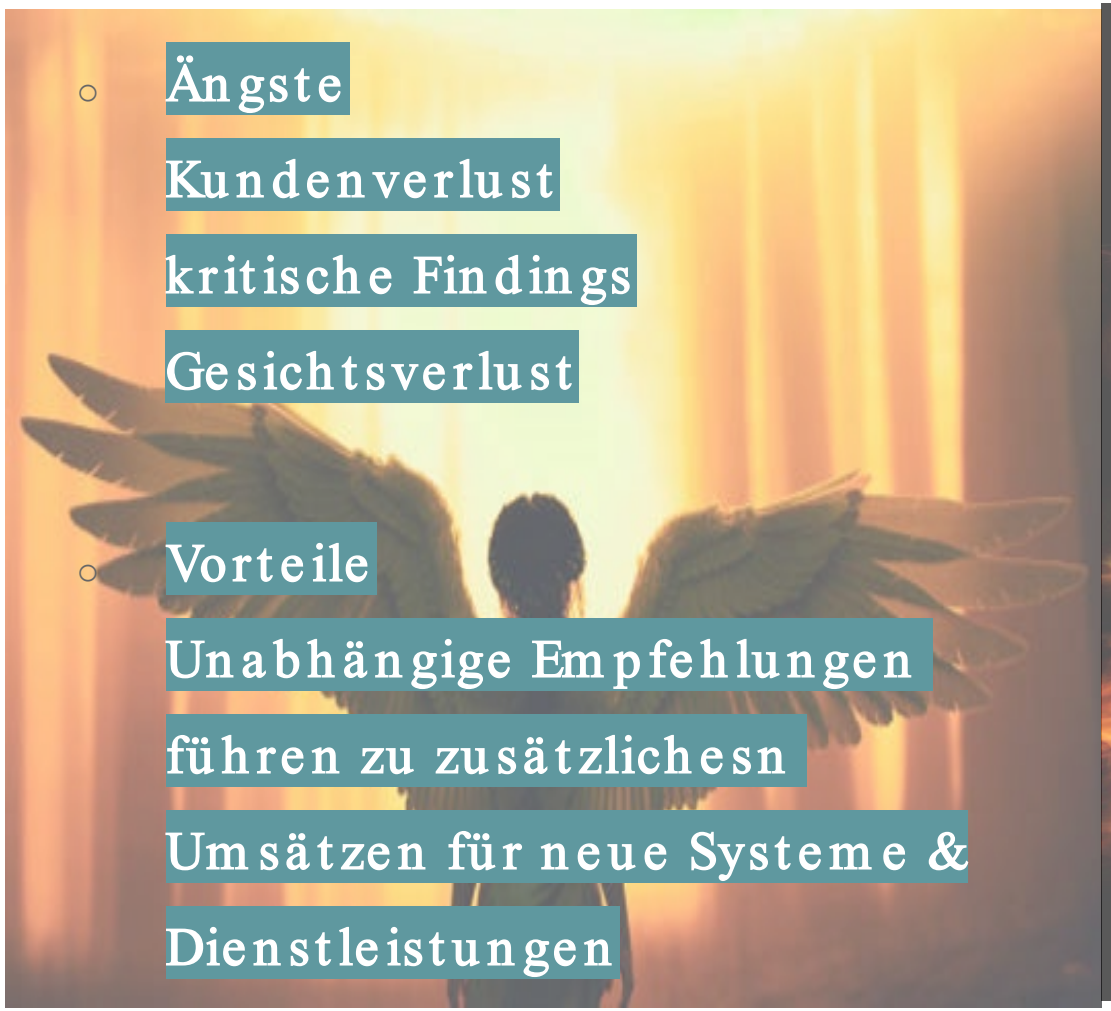
  Es gibt kein funktionierendes Patchmanagement

Top 10 der häufigsten technischen Erkenntnisse

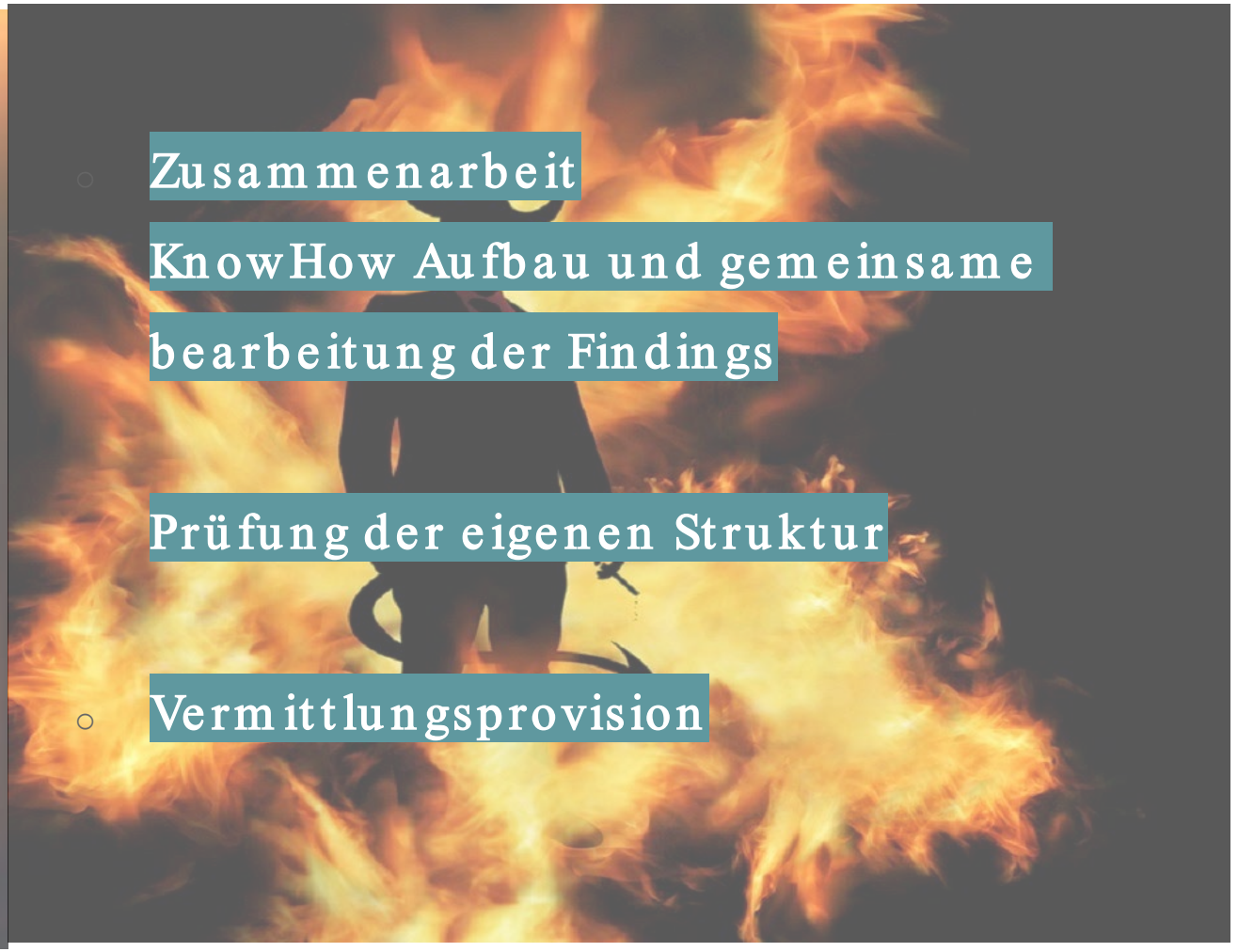
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- **Firmwaremanagement**
  Es gibt kein funktionierendes Firmwaremanagement
- **Assetverwaltung**
  Die CMDB ist nicht vorhanden bzw. gepflegt
- **Informationsstand**
  Die für die IT verantwortliche Person ist nicht hinreichend
  über den aktuellen Zustand der internen Infrastruktur informiert

Zusammenarbeit Systemhaus <-> Advocatus Diaboli



- Ängste
  - Kundenverlust
  - kritische Findings
  - Gesichtsverlust
- Vorteile
  - Unabhängige Empfehlungen führen zu zusätzlichesn Umsätzen für neue Systeme & Dienstleistungen



- Zusammenarbeit
  - KnowHow Aufbau und gemeinsame bearbeitung der Findings
  - Prüfung der eigenen Struktur
  - Vermittlungsprovision

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Carsten Vossel

c.vossel@ccvossel.de

T 030609840910