TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Assume Breach

The approach assumes that attackers have managed to overcome initial security precautions and get malware onto a computer (e.g. via a phishing email or file download). The next step is trying to execute the malware on the computer.

Objective

- Inventory and evaluation of technical safety
- Test of resistance to cyber attacks
- Increasing resilience
- Transparency as to how far an attacker could get in one's own infrastructure

Approach

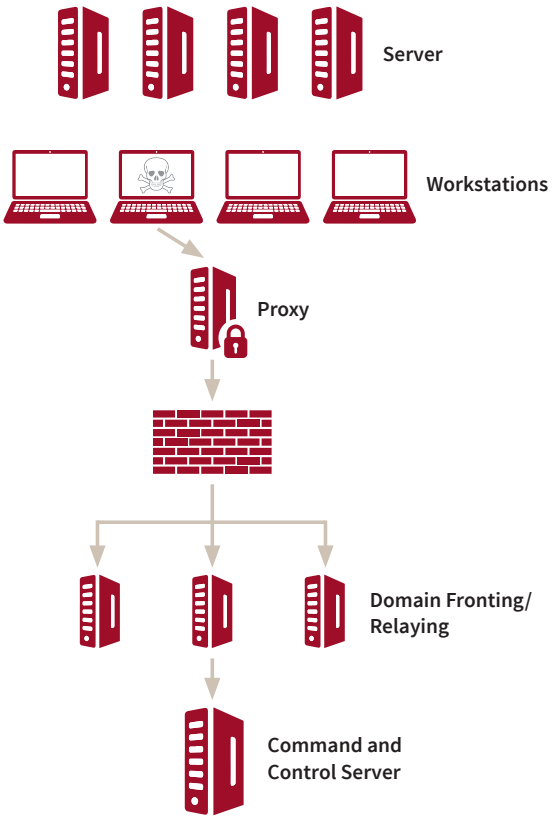
The Assume Breach approach can be used to visualise various scenarios, for example:

- Endpoint detection test for the detection of known and unknown malware (static and dynamic analysis)
- Determination of the attack surface (e.g. through Office macros or PowerShell code)
- Network analysis (Lateral Movement, Internal Reconaissance)
- Extending rights (Privilege Escalation)
- Domain analysis
- Access to sensitive data such as passwords or password hashes (Credential Access)
- Ransomware simulation (Crypto ransomware or data exfiltration)
- Creation of persistence
- Test of the logging and alerting processes (Blue Team)

The specific scenarios to be tested are agreed together.

Among other things, the Cobalt Strike command-and-control (C2) framework is used in the assessment. Cobalt Strike is an adversary simulation framework that is used in real attack campaigns. The assessment is simulated realistically.

The following illustration shows an example of a possible assessment setup:



TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Every action is logged precisely in time so that the activities can be assigned to possible events in security products. The events can also be used to optimise detection mechanisms. The assessment is based entirely on the MITRE ATT&CK ATT&CK Framework, an internationally recognised industry standard.

Your benefit

- Realistic attack simulation (individually customised to the customer's infrastructure)
- Identification of gateways
- Optimising detection mechanisms
- Identification of vulnerabilities (technical and organisational)
- Purple teaming (training of blue teams)
- Fulfilment of regulatory requirements (e.g. DORA)

TÜV TRUST IT GmbH
TÜV AUSTRIA Group

Waltherstraße 49–51
D-51069 Köln
Phone: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Phone: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com