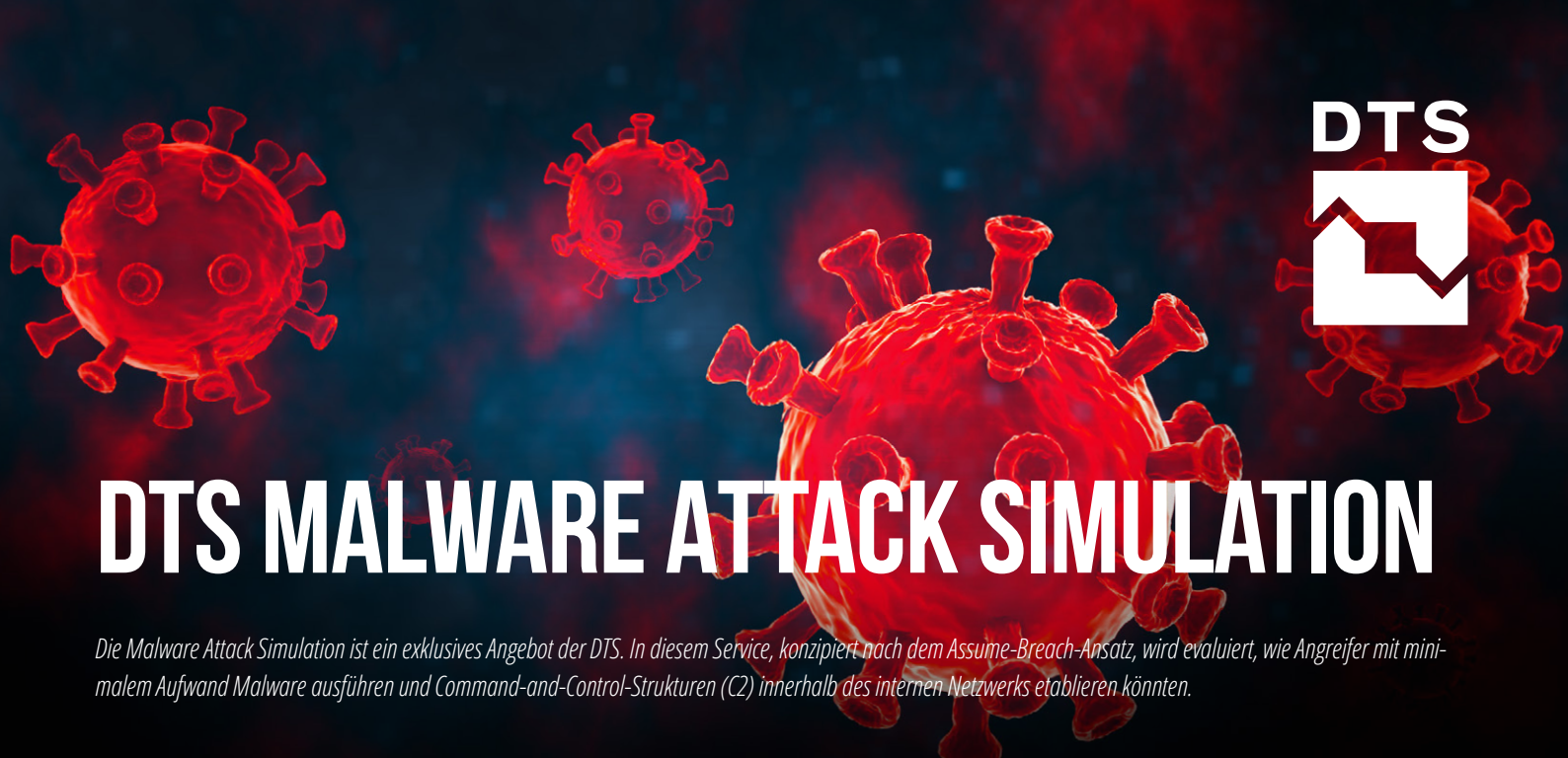

DTS MALWARE ATTACK SIMULATION

Die Malware Attack Simulation ist ein exklusives Angebot der DTS. In diesem Service, konzipiert nach dem Assume-Breach-Ansatz, wird evaluiert, wie Angreifer mit minimalem Aufwand Malware ausführen und Command-and-Control-Strukturen (C2) innerhalb des internen Netzwerks etablieren könnten.

ZUR AUSWAHL STEHEN ZWEI SZENARIEN:

- Verhalten von Ransomware-Malware
- Verhalten von Industriespionage-Malware

Das Ziel des Assessments ist es, Sicherheitslücken zu identifizieren, die einem Angreifer die Möglichkeit geben, Systeme zu kompromittieren, Daten zu exfiltrieren oder kritische Geschäftsprozesse zu stören.

Im Fokus stehen folgende Fragestellungen:

- Ransomware-Szenario: Wie resilient ist das Unternehmen gegen Angriffe, die auf die Verschlüsselung und Erpressung abzielen? Kann ein Angreifer erfolgreich Malware etablieren, im Unternehmen verbreiten und eine Steuerung von extern aufrechterhalten?
- Industriespionage-Szenario: Wie anfällig ist das Unternehmen für den Diebstahl sensibler Daten durch gezielte Angriffe? Kann ein Angreifer erfolgreich Malware etablieren und sensible Daten über einen Command-and-Control-Kanal extern abführen, ohne erkannt zu werden?

LEISTUNGSBESTANDTEILE

1. Schwachstellenanalyse: Als Grundlage dient eine initiale Sammlung von Informationen über verfügbare Systeme und Services. Diese Daten zeigen auf, wo Angriffsvektoren für Malware existieren.
2. Simulation realistischer Malware-Angriffe: Cyber-Security-Spezialisten der DTS führen gezielte Simulationen durch, um die Ausführung von Malware und die Etablierung von C2-Strukturen zu überprüfen. Dabei werden gängige Methoden des MITRE ATT&CK Frameworks genutzt, z. B. aus den Phasen Execution, Persistence, Defense Evasion sowie Command and Control. Es wird davon ausgegangen, dass der initiale Zugang bereits existiert.
3. Post-Exploitation-Phase: Nach erfolgreicher Malware-Ausführung wird evaluiert, wie Angreifer die Präsenz ausbauen könnten, mit Fokus auf:
   - Lateral Movement: Angriffe zur Ausbreitung innerhalb des Netzwerks
   - Privilege Escalation: Gewinnung administrativer Rechte
   - Credential Access: Versuch, Zugangsdaten zu stehlen, um unbefugten Zugriff auf Systeme zu erhalten
   - Collection: Sammeln von Daten oder Informationen aus einem kompromittierten System
   - Command and Control: Kommunikationskanal, über den ein Angreifer Kontrolle über ein infiziertes System erhält & es steuern kann
   - Exfiltration: Angreifer überträgt gestohlene Daten aus einem kompromittierten System heraus & an einen externen Ort

ABLAUF IM DETAIL

- Onboarding: Geräte & Zugangsdaten werden bereitgestellt, außerdem erfolgt die Registrierung auf der DTS Reporting Plattform
- Kick-Off Meeting: Gemeinsame Erörterung der technischen Details & Ziele des Assessments
- Projektarbeit: Durchführung der Malware-Simulation & Dokumentation der Befunde
- Abschlussgespräch: Präsentation der Ergebnisse & Diskussion möglicher Gegenmaßnahmen
- Optionale Weiterführung: Auf Wunsch können Sie die Ergebnisse auf der DTS Reporting Plattform weiter analysieren & Retests anfordern

IHRE VORTEILE

- Realistische Simulation von Malware-Angriffen, um mögliche Angriffspfade & Schwachstellen zu identifizieren
- Individuelle Anpassung an den Business-Kontext & die Sicherheitsziele des Unternehmens
- Realistische Einblicke in die Effektivität der bestehenden Sicherheitsmaßnahmen
- Detaillierte Handlungsempfehlungen für kurzfristige Maßnahmen & langfristige Strategien

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de

DTS Malware Attack Simulation 12703.2025