TREND MICRO™

TREND MICRO RED TEAMING

Testen & Verbessern Sie systematisch das Cyber-Abwehrkonzept Ihres Unternehmens.

> *It's what you don't see that ultimately gets you. And you can't know what you don't see until someone makes you see it.*
>
> **Mike Gibson**
> Vice President Security Research

Ein organisierter Stresstest für Ihr Unternehmen

Das Trend Micro Red Team testet die Widerstandsfähigkeit Ihrer Infrastruktur und Ihres Unternehmens gegen moderne Cyberangriffe. Wir agieren aus der Perspektive eines Angreifers, decken Schwachstellen auf und stellen Ihre Reaktionsfähigkeit in Angriffsszenarien auf die Probe. Dabei setzen wir TTP (Tactics, Techniques and Procedures) aus tatsächlichen Cyberangriffen ein, die von unseren eigenen Incident Response und Forward Looking Threat Research Teams erforscht, analysiert und für Red Teaming adaptiert wurden.

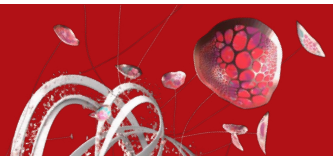
Die Angriffe unseres Red Teams folgen dabei dem EU-TIBER Framework (Threat Intelligence Based Ethical Red Teaming) und anderen Standards und imitieren exakt für Ihre Branche relevante und realistische Bedrohungsszenarien.

Strukturierter Erfahrungsaustausch mit Purple Teaming

Sie möchten die Red-Team-Erfahrung für Ihr Team noch intensiver gestalten? In Abhängigkeit vom aktuellen Reifegrad Ihrer Cyber-Abwehr ist es möglich, die Red-Team-Übung mit einer Blue-Team-Übung zu verbinden. Das Blue Team setzt sich aus Ihren eigenen Cyber-Experten zusammen und arbeitet eng mit dem Trend Micro Red Team zusammen.

Bei der Zusammenstellung eines Blue Teams weisen wir Ihrem Sicherheitsteam einen Trend Micro Incident Response Analysten zu, der Sie bei der Erkennung und Beantwortung des laufenden Red-Team-Angriffs anleitet. Eine konstante Feedbackschleife zwischen Red und Blue Team stellt sicher, dass die Übung für Ihre Mitarbeiter eine nachhaltige und noch intensivere Lernerfahrung bietet.

.



Wie funktioniert Red Teaming?

1. Vorbereitungsphase

- EIN ERSTES INTERVIEW hilft uns bei der Bewertung Ihres aktuellen Cybersicherheitsprofils. Wir untersuchen dabei Ihre Sicherheitskonzepte, -prozesse und -organisation. Darüber hinaus definieren wir die Angriffsziele für das Red Team, wie zum Beispiel die Exfiltration bestimmter Zieldaten.

- THREAT LANDSCAPE REPORT Das Ergebnis des initialen Interviews ist ein Threat Landscape Report, der uns die Entwicklung realistischer Angriffsszenarien ermöglicht. Der Report basiert auf gezielter Threat Intelligence und spezifischen Aufklärungsdaten zu Ihrer Organisation sowie auf dem bekannten Verhalten realer Akteure in der Bedrohungslandschaft.

- FINALE ABSTIMMUNG Vor dem Beginn der Übung führen wir ein vorbereitendes Meeting durch, in dem der Threat Landscape Report, die Rollen und Erwartungen aller Beteiligten besprochen werden. Wir definieren die Regeln der Übung und diskutieren über Eskalationspfade. Dabei ist es sehr wichtig, dass die Reichweite der Übung mit der Vorstandsebene abgestimmt wird.

2. Red Teaming Phase

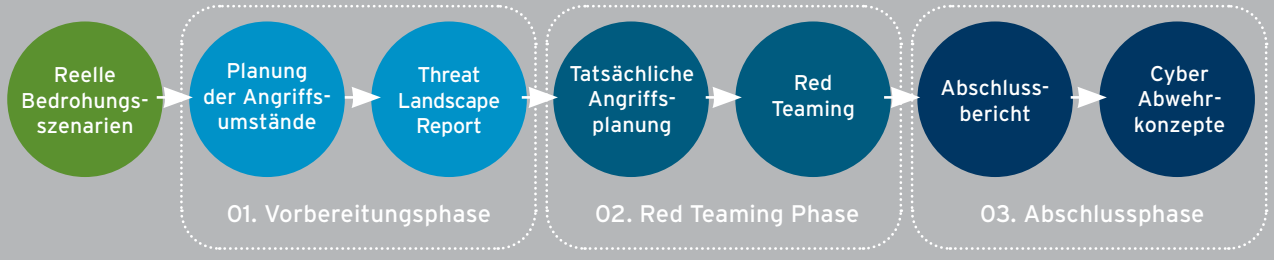
- ATTACK FRAMEWORK Nachdem wir Ihre Infrastruktur und die bestehenden Sicherheitskontrollen verstanden haben, entwickeln wir ein Attack Framework, das genau auf Ihre Organisation zugeschnitten ist. Dabei berücksichtigen wir unter anderem Ihre Branche und Unternehmensart. In Abhängigkeit von diesen Faktoren werden TTP ausgewählt, die auch in realen Angriffsszenarien gegen Sie eingesetzt werden würden.

- DURCHFÜHRUNG DES ANGRIFFS Daraufhin beginnt die Live-Übung. Mithilfe unseres Threat Intelligence Playbook führen wir einen Angriff auf Ihr Unternehmen durch. Bei einer Purple-Team-Übung führt Sie unser Incident Response Analyst im Blue Team durch die Erkennung und Abwehr des Angriffs.

3. Abschlussphase

- ABSCHLUSSBESPRECHUNG UND BERICHT Die Übung endet nach dem vereinbarten Zeitrahmen oder sobald das Angriffsziel erreicht wurde. Wir erstellen einen vollständigen Bericht, der über erfolgreiche und nicht erfolgreiche TTPs informiert. Darüber hinaus weisen wir auf weitere festgestellte Risiken hin und sprechen Empfehlungen aus.

- VERBESSUNG DES ABWEHRKONZEPTS In einem abschließenden Meeting werden die Ergebnisse vorgestellt und Optionen zur Verbesserung der Sicherheitskontrollen diskutiert.



Der Trend Micro Vorteil

Viele andere Red-Team-Angebote decken nur einige Aspekte unseres Services ab. Für uns ist Red Teaming deutlich mehr als nur ein Penetrationstest, bei dem Hacker nach neuen Wegen in Ihr Netzwerk suchen. Mit unserem Service wollen wir die Auswirkungen von Angriffen analysieren, Risiken identifizieren und überwachen sowie die Widerstandsfähigkeit Ihres Unternehmens systematisch verbessern.

Während einer Red-Team-Übung befinden wir uns mit Ihnen in einer engen Feedbackschleife, sodass die Regeln und Begrenzungen der Übung klar definiert sind und jederzeit eingehalten werden. Unser Attack Framework basiert auf dem Threat Landscape Report, der Ihnen bereitgestellt wird. Dabei handelt es sich um einen fokussierten Threat Intelligence Report, der speziell für Sie maßgeschneidert wird. Gezielte Threat Intelligence, spezifische Aufklärungsdaten zu Ihrer Organisation und Erfahrungen zum Verhalten realer Angreifer bilden die Grundlage, auf der wir realistische Angriffsszenarien entwickeln.

Nach Abschluss der Red- oder Purple-Team-Übung erhalten Sie unseren Abschlussbericht, in dem wir über unsere Erkenntnisse zur Widerstandsfähigkeit Ihrer Organisation berichten. Der Bericht wird ergänzt durch konkrete Hinweise zur Verbesserung der technischen Kontrollen, Prozesse, Richtlinien und Funktionen. Im Anschluss unterstützen wir Sie gerne bei der Umsetzung der Empfehlungen für optimierte Sicherheitskontrollen.

Kontakt

Denis Gallagher
Sales Development Specialist
Denis_Gallagher@trendmicro.com
Tel.: +49 175 4518 170

Andreas Glück
Sales Development Specialist
Andreas_Glueck@trendmicro.com
Tel.: +49 151 541 005 37

TREND MICRO™
Securing Your Connected World