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

TeleTrusT-interner Workshop

Berlin, 01.07.2025

Zwischen Regulierung und Realität - Threat Intelligence als Schlüsselfaktor für mehr IT-Sicherheit

Giulia Vaccaro, valantic

Threat Intelligence als Baustein der IT-Sicherheit

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

- **Was ist Threat Intelligence?**
  - Analyse und Sammlung von Informationen über potenzielle und bestehende Bedrohungen.
  - Ziel ist es, Bedrohungen frühzeitig zu erkennen und angemessen zu reagieren.

- **Arten von Threat Intelligence:**
  - **Strategische TI:** Langfristige Bedrohungstrends und strategische Planung.
  - **Operative TI:** Kurzfristige Bedrohungen und direkte Gegenmaßnahmen.
  - **Taktische TI:** Techniken und Tools von Angreifern für detaillierte Analysen.

.

Regulatorische Rahmenwerke wie DORA oder TIBER fordern den Einsatz von Threat Intelligence, um digitale Resilienz zu stärken, aktuelle Bedrohungen zu identifizieren und strategische Risiken langfristig zu mindern.

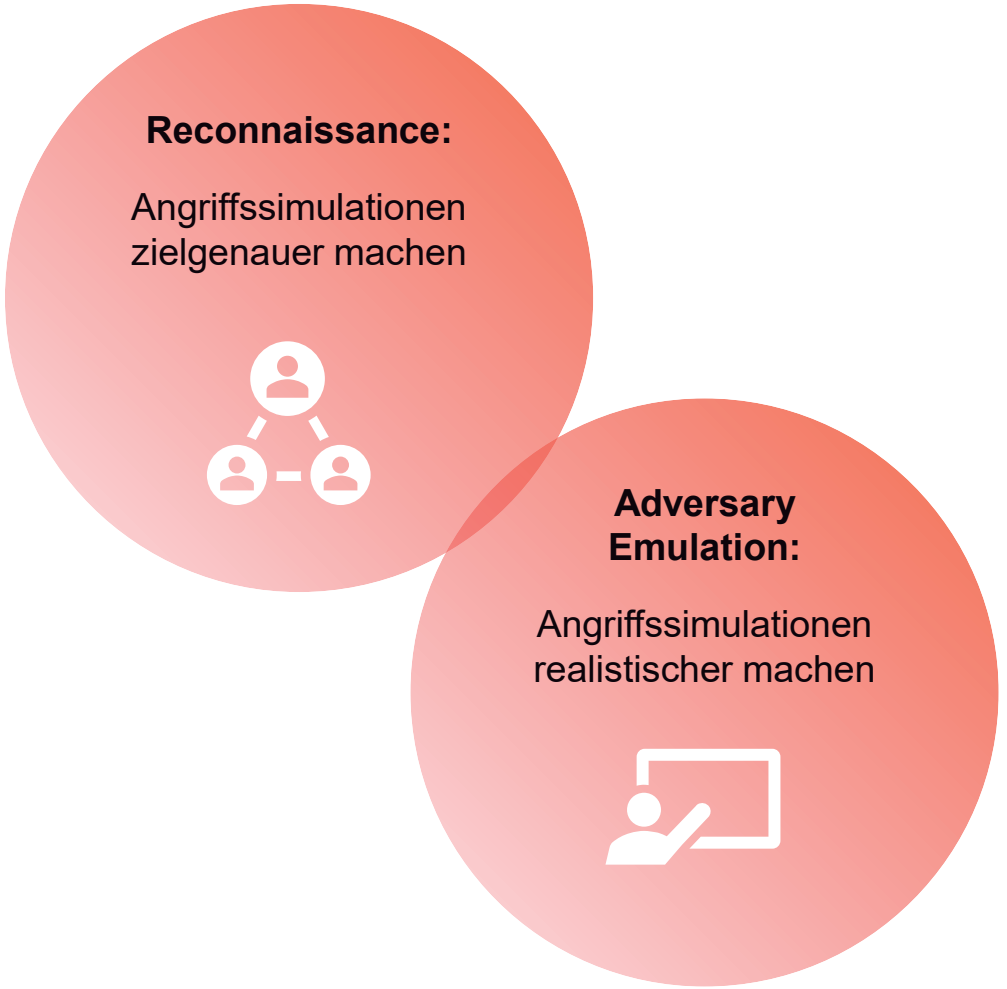
Threat Intelligence in DORA und TIBER

Reconnaissance

- Open Source Intelligence (OSINT) Analyse von öffentlich verfügbaren Informationen über den Kunden.
- Je nach Bedarf Nutzung von Darknet Quellen, Clearnet Quellen sowie Analyse der öffentlich einsehbaren Infrastruktur.
- Aufbereitung der identifizierten Angriffsvektoren für weitere Penetration Tests.
- Recon als Vorbereitung für die Adversary Emulation

Adversary Emulation

- Auswahl relevanter Bedrohungsakteure und Modellierung von Angriffsverhalten.
- Zusammenstellung von verschiedenen Szenarien anhand der ausgewählten Akteure und deren Angriffsvektoren.



Threat Intelligence in der Realität: Wertschöpfungsketten

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

Zunehmende **Professionalisierung** von Cyberkriminellen über **Modularisierung** und **Arbeitsteilung**

Forschung & Entwicklung

Schwachstellenforscher: Identifizieren Schwachstellen in Software und Systemen.

Malware-Entwickler: Entwickeln Schadsoftware, die für Angriffe und insbesondere den Initial Access verwendet wird.

Initial Access & Verbreitung

Initial Access Broker: Verkaufen Zugang zu bereits kompromittierten Systemen.

Spammer und Phisher: Versenden schädliche E-Mails oder Nachrichten, um Malware zu verbreiten oder Zugangsdaten zu erlangen.

Ausführung des Angriffs

Exploit-Entwickler: Spezialisieren sich auf die Entwicklung von technischen Exploits

Attack Operators: Führen die Angriffe durch, unter Verwendung von gekauften Exploits oder Zugangsdaten

Datendiebstahl- & Handel

Datenhändler: Spezialisieren sich auf den Kauf und Verkauf gestohlener Daten.

Informationsbroker: Aggregieren und verkaufen spezifische Informationen, die aus verschiedenen Quellen stammen.

Monetarisierung

Ransomware-Operatoren: Verschlüsseln Daten und fordern Lösegelder.

Finanzspezialisten: Spezialisten, die sich mit Geldwäsche und dem Transfer von digitalen Währungen beschäftigen.

Unterstützende Dienste

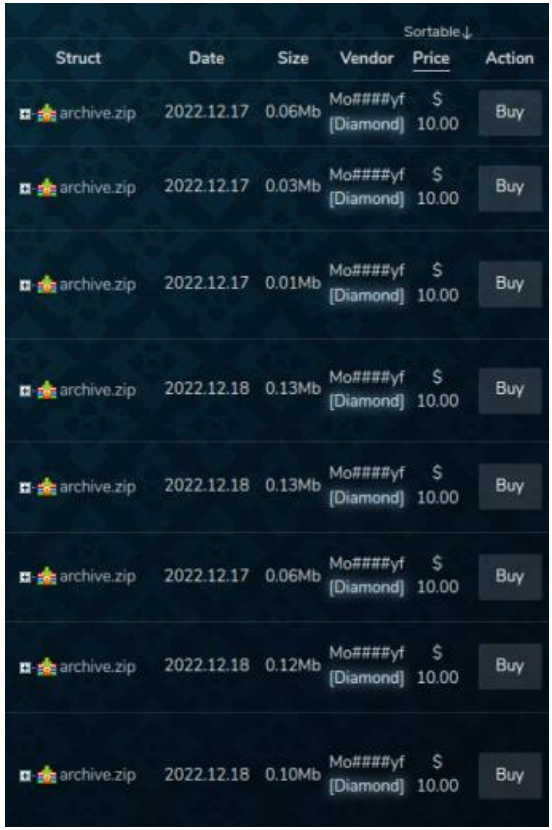
Hosting-Dienste: Bieten anonyme Hosting-Lösungen, unteranderem im Darknet an.

Sicherheitsexperten: Bieten Schutzdienste für die Infrastrukturen und Operationen anderer krimineller Akteure.

Threat Intelligence in der Realität: Initial Access Broker

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

- Unter den Berufsgruppen besonders spannend: die **Initial Access Broker**
- Die Immobilienmakler unter den Cyberkriminellen
- Über quantitative Malware-Kampagnen erhaltene Pakete von Zugangsdaten werden teilautomatisiert in Darknet Foren zum Verkauf angeboten
- Dabei werden die Inhalte der Pakete nur selten gesichtet und bewertet – für den Käufer aber auch vorab als „Marketing“ zur Verfügung gestellt
- Andere Cyberkriminelle kaufen diese Zugänge, um von dort aus weiteren Schaden anzurichten
- Der Verkauf nimmt oftmals eine längere Zeit in Anspruch
- Eine Analyse dieser Pakete bietet Aufschluss über daraus resultierende Gefahren für betroffene Unternehmen



Fazit

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

Zwischen Regulierung und Realität - Threat Intelligence als Schlüsselfaktor für mehr IT-Sicherheit

Technik

Threat Intelligence umfasst unterschiedliche Arten, die je nach Anwendungsbereich und Zielgruppe variieren – von strategischen Analysen für Führungskräfte bis hin zu operativen und taktischen Einblicken für IT- und Sicherheitsteams.

Regulatorik

DORA und TIBER schaffen solide Grundlagen für den Finanzsektor und etablieren Threat Intelligence als essenziellen Bestandteil der Cybersicherheitsstrategie. Angesichts der breitgefächerten Bedrohungslage sollte TI jedoch in allen Branchen ein integraler Bestandteil der Sicherheitsstrategie sein.

Praxis

Operative Threat Intelligence ermöglicht die Identifizierung bereits erfolgter Angriffe. Proaktive Unternehmen integrieren kontinuierliche Bedrohungsüberwachung und etablieren Prozesse zur effizienten Erkennung und Abschwächung potenzieller Risiken."

Vielen Dank für Ihre Aufmerksamkeit!

GIULIA VACCARO

Head of Threat Intelligence

+49 170 8408139

giulia.vaccaro@mc.valantic.com

Dreieich Plaza 2A
63303 Dreieich
Germany