APT-CC – Errichtung eines APT Competence Centers in Österreich

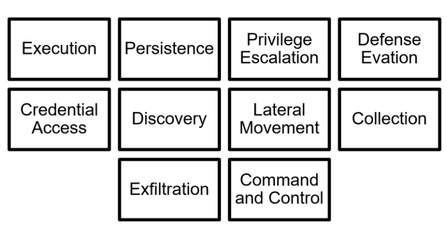
Projektziel

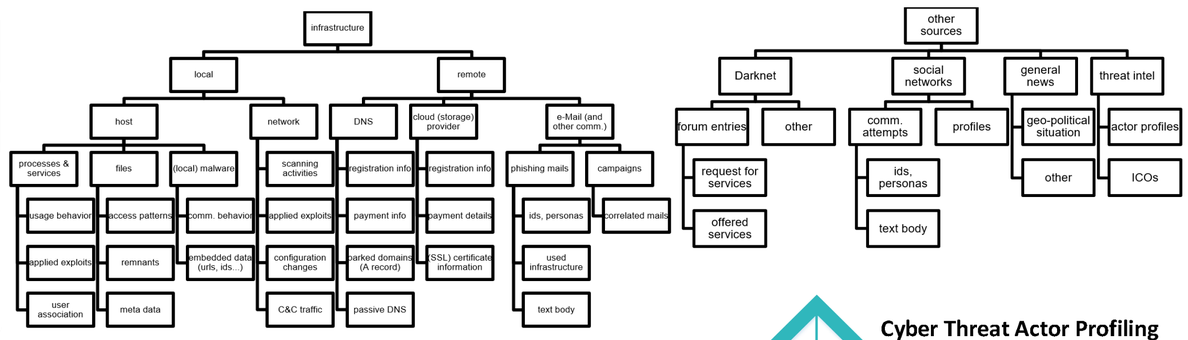
Advanced Persistent Threats (APT) sind komplexe, zielgerichtete und effektive Angriffe auf kritische IT-Infrastrukturen (KIs) und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen. Der **Aufbau eines APT-Kompetenzzentrums (APT-CC)** zur Beobachtung und Ermittlung in Bezug auf Spionage- und Sabotageakte bei staatsschutzrelevanten Organisationen bzw. kritischen Infrastrukturen ist erklärtes Ziel der österreichischen Sicherheitsressorts im Sinne der Steigerung einer gesamtstaatlichen Resilienz. Um diesen Aufbau effektiv durchführen zu können, ist es im Vorfeld essentiell die Basis für grundlegende Entscheidungen mit Bezug auf Ressourcen, Ausstattung und relevanter Befugnisse eines solchen APT-CC zu schaffen. Dieses Vorhaben wurde im Zuge der KIRAS Studie APT-CC verfolgt. Insbesondere wurde untersucht, inwiefern Sensornetze zur proaktiven Erkennung von APTs eingesetzt werden können, wie die Prozesse zur forensischen Aufarbeitung von APTs aussehen und welche Möglichkeiten der Etablierung eines Rapid Response Teams existieren. Die Ergebnisse wurden einerseits durch rechtliche Betrachtungen ergänzt und andererseits anhand anwendungsnaher Fallbeispiele diskutiert.

Projektlaufzeit: 01.11.2018 – 31.05.2020

APT C²

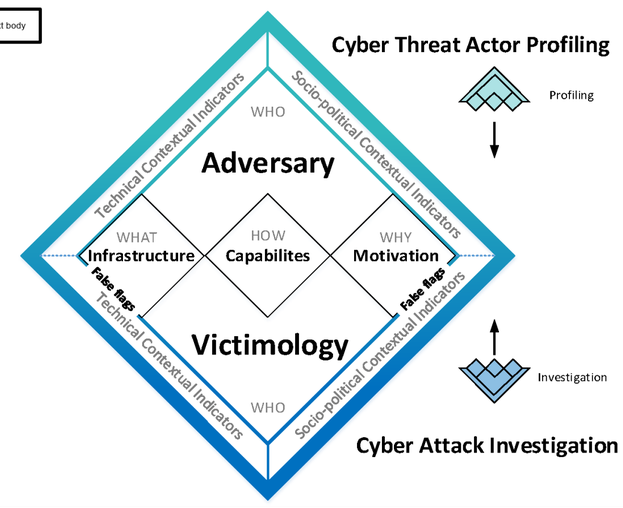
Forensische Artefakte für die Attribuierung von Cyberangriffen





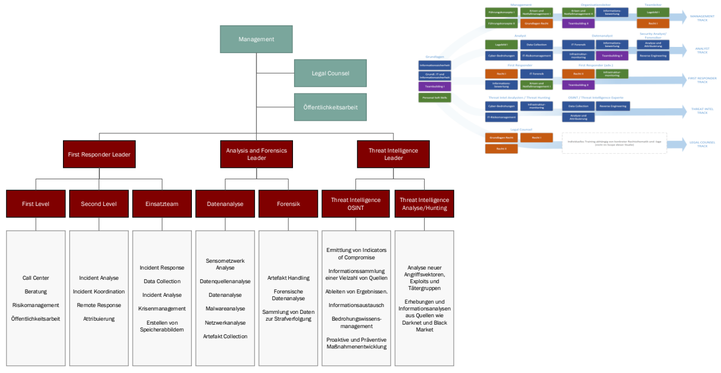
Was sind **FALSE FLAGS**?

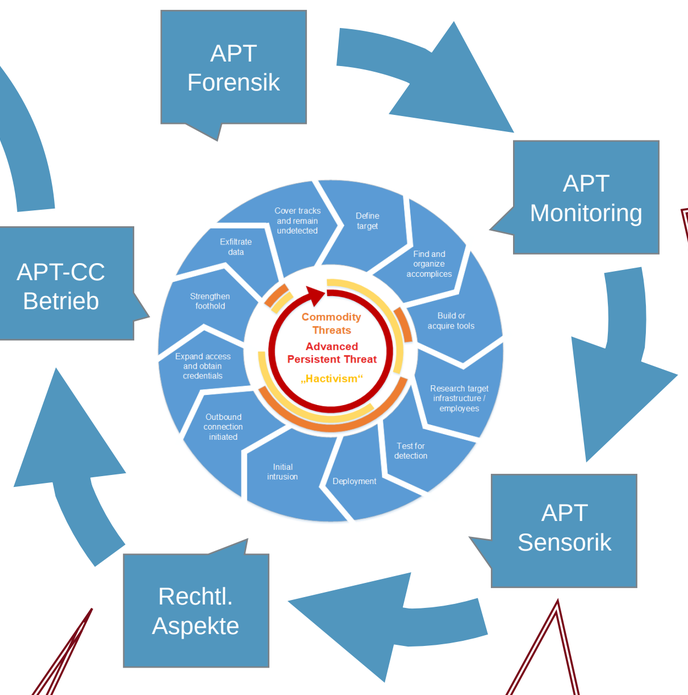
- Bei Exploits werden recycelte Codes / Varianten aus früheren Angriffen verwendet, die im Internet in der Vergangenheit erfolgreich waren und veröffentlicht wurden.
- Exploits werden entwickelt, um das Verhalten und die Komplexität von bekannter, attribuierter Malware nachzuahmen.
- Exploits und Malware werden eher gekauft als entwickelt bzw. als Dienst gemietet.
- Malware verbindet sich mit einer bekannten C&C-Infrastruktur, obwohl sie nicht von den Serverbetreibern entworfen wurde.
- Ein C&C-Server nutzt Infrastrukturen eines Dritten, die nicht mit den Angrei-fern in Verbindung stehen, z.B. ausgenutzter Webserver in einem anderen Land.
- Ein Vorfall ist konstruiert um Ermittlungen fehlzuleiten.
- Die Durchführung böswilliger Handlungen verbirgt die tatsächliche Absicht und soll Ermittler in die Irre führen.



Dienstleistungs- und Betreibermodell eines APT-CCs

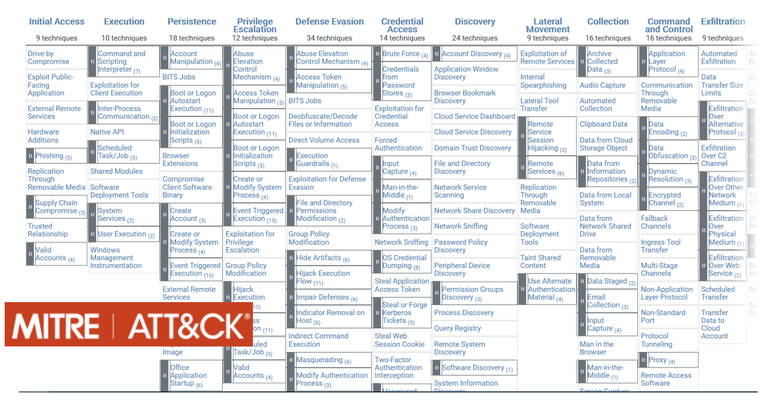
- Aufklärung des Umfangs des Angriffs und der aktiven Zugangskanäle
- Hilfestellung bei der Aussperrung des Angreifers
- Beobachtung neuer Angriffsversuche und Ursachenanalyse
- Säuberung manipulierter Systeme und Verhinderung erneuter Vorfälle
- Suche und Erkennung möglicher Angriffe (APT-Hunting)





Datenquellen für Monitoring

- Welche **Techniken** werden von **APT**s und Angriffs-Software bei Angriffen auf Enterprise IT-Systeme **am öftesten** eingesetzt?
- Mittels der Verarbeitung welcher Datenquelle ist es möglich, **die meisten** von APT angewandten **Techniken** auf Enterprise IT-Systeme zu **detektieren**?
- Mit der Verarbeitung welcher Datenquelle ist es möglich, die meisten Techniken, welche zusätzlich am öftesten bei Angriffen auf Enterprise IT-Systeme zur Anwendung kommen, zu detektieren?



MITRE | ATT&CK®

Technik (ID) Taktik	Rang R Wert R	Rang S Wert S	Rang E_{APT} Wert E_{APT}
Remote File Copy (T1105) Lateral Movement, Command And Control	1 201.67	2 126	8 23
Standard Application Layer Protocol (T1071) Command And Control	2 196.09	1 127	10 21
Command-Line Interface (T1059) Execution	3 187.67	4 112	9 23
Registry Run Keys / Startup Folder (T1060) Persistence	4 168.67	6 93	6 23
System Information Discovery (T1082) Discovery	5 167.35	3 118	15 15
Obfuscated Files or Information (T1027) Defense Evasion	6 166.96	7 88	5 24
Scripting (T1064) Execution, Defense Evasion	7 154.99	15 53	1 31
Credential Dumping (T1003) Credential Access	8 149.83	11 61	3 27
File and Directory Discovery (T1083) Discovery	9 1		

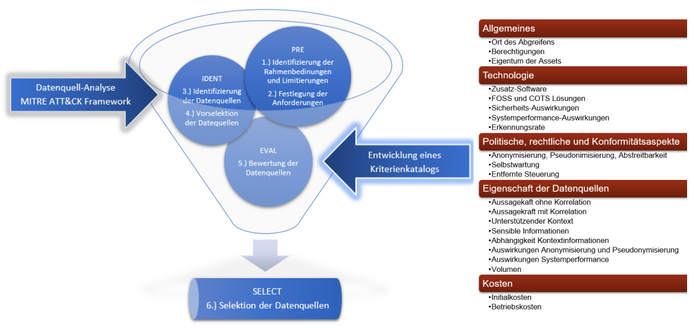
Datenquellen (Taktiken)	Rang	Anzahl
Process monitoring (11/11)	1	157
File monitoring (11/11)	2	90
Process command-line parameters (9/11)	3	87
API monitoring (8/11)	4	41
Process use of network (10/11)	5	37
Windows Registry (8/11)	6	34
Packet capture (9/11)	7	32
Authentication logs (8/11)	8	28
Netflow/Enclave netflow (9/11)	9	24
Windows event logs (6/11)	10	19
Binary file metadata (7/11)	11	18
Network protocol analysis (7/11)	12	18
DLL monitoring (6/11)	13	17
Loaded DLLs (5/11)	14	12
Malware reverse engineering (2/11)	15	9
System calls (6/11)	16	9
SSL/TLS inspection (3/11)	17	8
Antivirus (5/11)	18	7
Network intrusion detection system (3/11)	19	7
Data loss prevention (5/11)	20	6

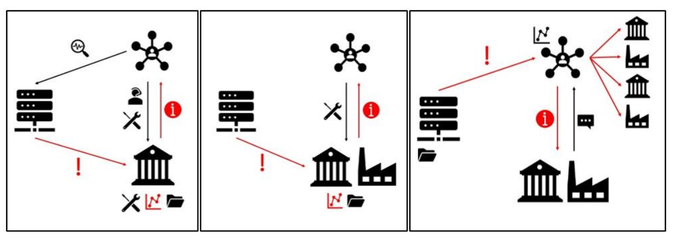
Rechtliche Aspekte

- Rechtliche Bewertung des **Einsatzes eines Sensornetzwerks**
- Rechtliche Aspekte von **Rapid Response** Fähigkeiten

Cyber Security Sensornetze

- Welche **typischen Datenquellen** gibt es **in Enterprise IT** Umgebungen, die bei der Detektion von APTs relevant sind?
- Wie kann man diese Datenquellen miteinander hinsichtlich ihrer **Wertigkeit bei der Detektion von APT-Angriffen** vergleichen?
- Wie könnte ein **Vorgehensmodell für die Selektion von Datenquellen** aussehen?





Gefördert/finanziert durch das Sicherheitsforschungs-Förderungsprogramm KIRAS des Bundesministeriums für Landwirtschaft, Regionen und Tourismus (BMLRT).

Kontakt
Dr. Dr. Florian Skopik
E-Mail: florian.skopik@ait.ac.at
Web: https://www.ait.ac.at/cyber-security/