Cyber-AUGE Automatisierte Erkennung von Cyber-Risiken

Erläuterung der Problemstellung, die mit der Idee gelöst werden soll:

Bewertung von Cyber-Angriffen sind vielerlei Aspekte zu berücksichtigen:

- Erfassung der Eigenschaften und Fähigkeiten von potenziellen Vorgehensweise von Akteuren im Cyberraum (Intelligence Preparation of the Cyber Battlefield)
- Erfassung von Hinweisen auf mögliche laufende Angriffe (Sensoren: IDS, OSInt, etc.)
- Interoperabler Austausch der Informationen über mögliche Angriffe - maschinenlesbar
- Interoperabler Austausch der Grundlageninformationen
- Bewertung von möglichen Gegenmaßnahmen
- Bewertung der Auswirkung eines Angriffs auf laufende eigene Aktivitäten (zum Beispiel eine militärische Operation) unter Berücksichtigung der Eigenschaften des angegriffenen System of Systems
- Darstellung der Auswirkungen geeignet für militärische Entscheider unter Berücksichtigung der operationellen Nutzung des angegriffenen System of Systems
- Risikobewertung
- Bewertung der Auswirkung möglicher Gegenmaßnahmen

Die verschiedenen Aspekte werden derzeit weitestgehend mit verschiedenen Methoden unter teilweiser Nutzung von IT-Unterstützung betrachtet. Eine durchgehende IT-Unterstützung von der Erkennung und Bewertung eines möglichen Angriffes ist nicht verfügbar. Dadurch besteht eine erhöhte Gefahr, dass zum Beispiel

- gefährliche Angriffe (hinsichtlich der Auswirkung auf die eigene Operationsführung) nicht von ungefährlichen unterscheidbar sind
- die Reaktion auf gefährliche Angriffe zu spät erfolgt
- Gegenmaßnahmen die eigene Operation behindern

Die Idee zielt darauf ab, alle genannten Aspekte unter Nutzung von modellbasierter KI zu verbinden und eine Gesamtbewertung der Cyber-Lage und der möglichen Gegenmaßnahmen zu unterstützen.

Zudem erlaubt die Architektur des Gesamtansatzes, bereits bei der Entwicklung von Systemen (zum Beispiel Waffensystemen) eine Vorabbewertung der Angreifbarkeit der Systeme unter gegebenen Annahmen (zum Beispiel hinsichtlich Fähigkeiten und Ziel möglicher Angreifer) und deren operationeller Auswirkungen auf die Fähigkeiten des Systems durchzuführen. Dabei kann die Analyse je genauer werden, je genauer die Architektur (operationelle und technische Architektur) des Systems im Verlauf der Beschaffung präziser wird.

Beschreibung der Idee und wie sie das Problem lösen soll:

Die Grundidee besteht in der Generierung und Nutzung von maschinenlesbaren und mittels KI-Verfahren auswertbaren Modellen, die jeweils auf einem Standard aufsetzen:

1. Beschreibung von Angreifern (Entität, Fähigkeiten, Absichten, Vorgehensweisen) mit einem an den Standard STIX (Structured Threat Information Expression) angelehnten Angreifermodells

- Beschreibung der Informationen aus Sensoren mit Hilfe des STIX Domain Objects "Indicator"
- Austausch der Angreifermodelle und Indikatoren mit Hilfe des mit STIX interoperablen Austauschmethode Trusted Automated Exchange of Intelligence Information
- Automatische Generierung eines KI-Modells aus dem Angreifermodell
- KI-basierte Erstellung eines aktuellen Lagebildes basierend auf Indikatoren und / oder Annahmen.

2. Nutzung der architekturbasierten Beschreibung von Systemen mit NAF / ADMBw

- Generierung eines KI-Modells aus dem Architekturmodell
- Verknüpfung des STIX-Modells mit dem Architekturmodell über gemeinsame Systembausteine
- Automatische Bewertung der technischen und operationellen Auswirkungen erfolgreicher Angriffe Bewertung von Gegenmaßnahmen.

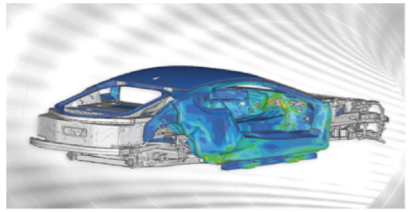
3. Automatisches Einlesen von Modellen unter Nutzung der entsprechenden Metamodelle Umsetzung:

- Vollständige Implementierung der automatischen Modellgenerierung
- Implementierung von für verschiedene Stakeholder passenden Nutzeroberflächen
- Operationelle Implementierung der modellbasierten KI
- Organisatorische Sicherstellung der Verfügbarkeit der Ausgangsmodelle (zum Beispiel Erstellung der Angreifermodelle durch Kdo CIR, Bereitstellung der Architekturmodelle durch Planungsamt / BAAINBw)

Die erforderlichen Metamodelle und Austauschmethoden liegen im Grundsatz vor (STIX-Metamodell, NAF-ADMBw, TAXII).Die automatische Generierung von Modellen wurde in mehreren Forschungsprojekten entwickelt und ausprobiert, muss aber noch operationalisiert werden.
Für eine erfolgreiche Implementierung muss sichergestellt werden,

- dass eine systematische Erstellung von Angreifermodellen unter Nutzung eines gemeinsamen Metamodells erfolgt
- dass eine qualitätsgesicherte Architektur der jeweiligen Systeme vorliegt
- dass der Informationsaustausch der entsprechenden Informationen (Modelle und aktuelle Informationen) bundeswehrweit medienbruchfrei unter Nutzung der maschinenlesbaren Metamodelle erfolgt.

Im Kommando CIR wurde bereits damit begonnen, den STIX-Standard anzuwenden. Die Erstellung einer NAF-Architektur für Systeme ist im CPM bereits hinterlegt. Die kontinuierliche Aktualisierung und Qualitätssicherung der Modelle ist sicherzustellen.


AUTOMOTIVE


INFOKOM


MOBILITÄT, ENERGIE & UMWELT


LUFTFAHRT


RAUMFAHRT


VERTEIDIGUNG & SICHERHEIT

Cyber-AUGE
Automatisierte Erkennung von Cyber-Risiken

Jürgen Ziegler
IABG

Code-Tagung München, 10.07.2019

Elemente eines Lagebilds

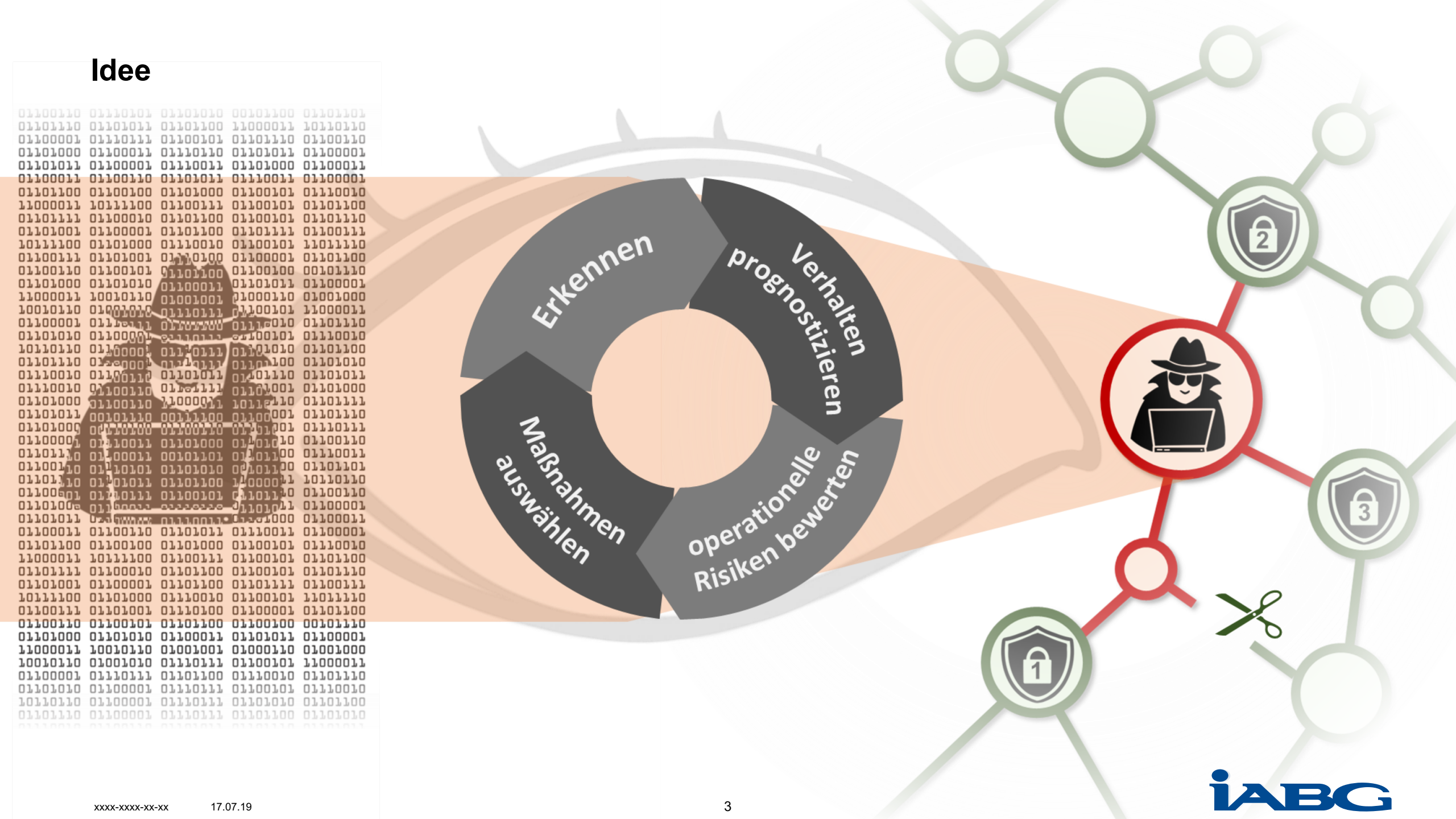
Welche Bedrohungen sind für mich relevant?

Wie gefährlich sind potenzielle Bedrohungen für mich?

Was tut sich aktuell?

Was muss und was kann ich tun?

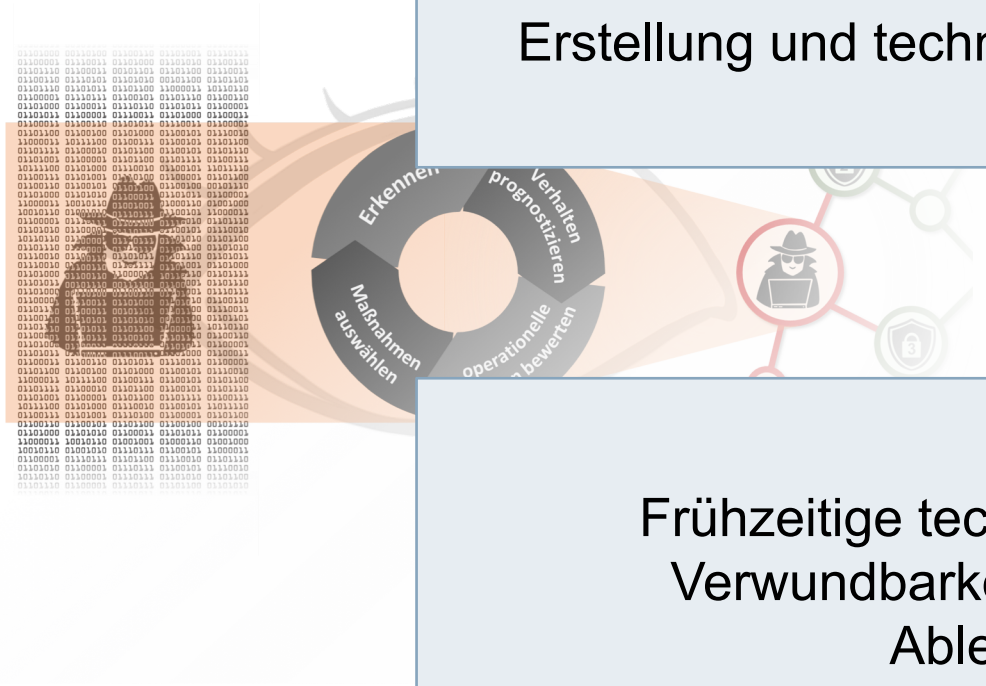
Idee


Erkennen
Verhalten prognostizieren
operationelle Risiken bewerten
Maßnahmen auswählen
1
2
3

Bausteine

Technik	&	Organisation
Standards STIX und TAXII – Angreifermodell / Datenaustausch		Grundlagenerstellung und Pflege – Intelligence Preparation of the Cyber Space
„Standard“ NAF / ADMBw – Modell der bedrohten SoS		Wiederverwendung von Modellen
„Ergonomie“ – Erklärungsfähiges Lagebild		Sicherstellen Datenaustausch
Sensoren – Beobachtungen / Indikatoren		
„Model Learning“ – Generierung „KI-Modelle“		
Algorithmen - Lagebilderstellung & Bewertung		

Anwendungsspektrum



Operationell

Erstellung und technisch-operationelle Bewertung Cyberlage

CPM

Frühzeitige technisch-operationelle Bewertung der Verwundbarkeit / Resilienz zukünftiger Systeme
Ableitung von Anforderungen

Ihr Ansprechpartner

IABG mbH
Defense and Security / CC20
Competence Centre NG&A
Jürgen Ziegler
Einsteinstraße 20
85521 Ottobrunn
Telefon +49 89 6088-2575
zieglerj@iabg.de
www.iabg.de