Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

SECURITY

Grundlagen und Definitionen

April 26, 2024

Marc Stöttinger

Im Mittelpunkt jeder Sicherheitsbetrachtung steht menschliches Handeln und Unterlassen.

Sebastian Klipper

WIEDERHOLUNG: SECURITY VS. SAFETY

Tauschen Sie sich mit Ihrem Sitznachbar 3 Minuten aus:

- → Überlegen Sie am Beispiel eines Autos oder Getränkeautomatens, wie jeweils ein Security-Vorfall und ein Safety-Vorfall aussehen könnte.
- → Können Sie auf Basis der beiden Vorfälle eine generelle Aussage formulieren, die den Unterschied zwischen Security und Safety klar stellt?

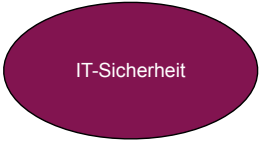
DEFINITION VON IT-SICHERHEIT

IT-Sicherheit

"IT-Sicherheit beschäftigt sich mit der Absicherung von technischen Systemen durch angemessene Maßnahmen auf ein tragbares Maß." - BSI

IT-Sicherheit beschränkt sich in der Regel auf die Absicherung informationstechnischer Systeme:

- → Netzwerk
- → Server
- → eMail
- → ...



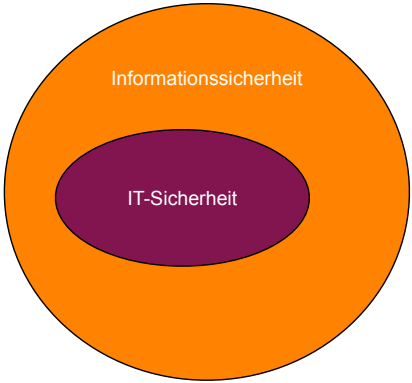
DEFINITION VON INFORMATIONSSICHERHEIT

Informationssicherheit

"Informationssicherheit beschäftigt sich mit der Sicherheit von technischen oder nicht-technischen Systemen zur informationsverarbeitendung, -speicherung und -lagerung." - BSI

Informationssicherheit betrachtet die Sicherung von Informationen generell:

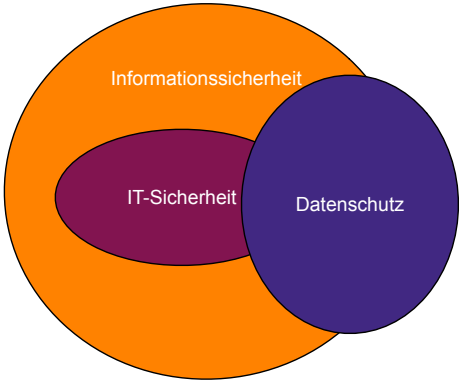
- → Verschlussakten
- → Personenkontrolle
- → Geschäftsmodelle
- → ...



DEFINITION VON DATENSCHUTZ

Datenschutz

"Datenschutz soll das Individuum davor schützen, durch den Umgang mit den eigenen personenbezogenen Daten im Persönlichkeitsrecht beeinträchtigt zu werden. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet." - BSI



Zusätzliche Aspekte zum Schutz der Informationen:

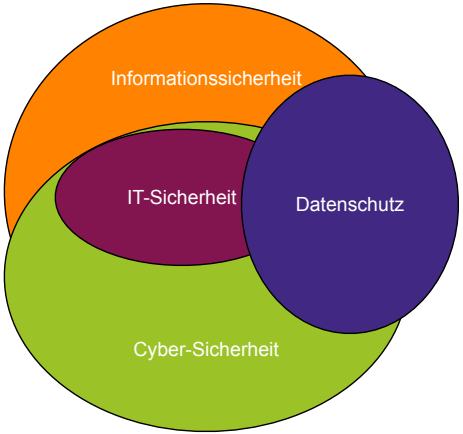
- → Rechte und Genehmigungen von Datenerhebung
- → Verwendung und Löschung der erhobenen Daten
- → ...

DEFINITION VON CYBER-SICHERHEIT

Cyber-Sicherheit

"Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik... ." - BSI

Cyber-Sicherheit fokussiert sich auf mit dem Internet verbundene Geräte und erweitert den Sicherheitsbegriff auf gesellschaftliche Werte.



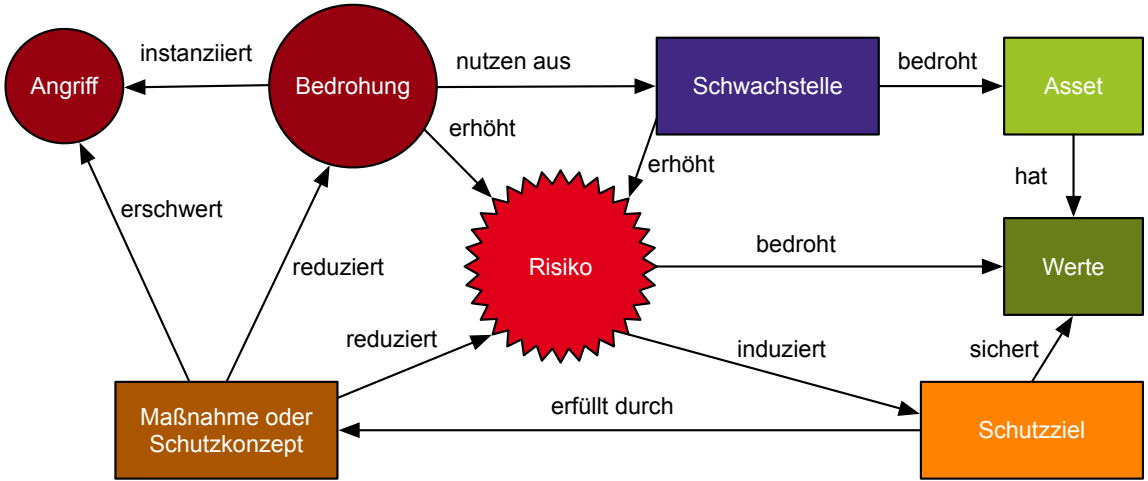
BEGRIFFLICHKEIT IN DER SECURITY

Wie Sie gesehen haben, gibt es verschiedene Bereiche mit **verschiedenen Schwerpunkten** im Kontext von Security. In den vier Bereichen gibt es **gemeinsame Begriffe**, um Sachverhalte zum Thema **Angriffe** und **Schutz** genauer zu spezifizieren.

In einem risikobasierten Ansatz ist es möglich, mit diesen Begriffen Angriffe zu quantifizieren, um beispielsweise folgende Fragen zu beantworten:

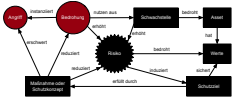
- → Was muss ich vor einem Angriff schützen?
- → Wie wahrscheinlich ist es, dass ein Angriff sattfindet?
- → Was bedeutet es, wenn der Angriff erfolgreich ist?
- → Wie verhindere ich, dass ein Angriff erfolgreich ist?

RISIKO-ZENTRISCHE SICHERHEITSBEGRIFFE



ANGRIFF UND BEDROHUNG

Ein Angriff ist eine Instanziierung einer Bedrohung, welche auf Basis konkreter Techniken und Vorgehensweisen eine Schwachstelle ausnutzen will.

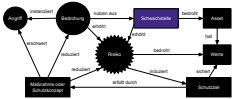


Oft wird keine Unterscheidungen von Bedrohungen und Angriffen gemacht. Jedoch kann dies nützlich sein, wenn viele potentielle Angriffe auf eine Schwachstelle existieren und diese durch eine Bedrohung zusammengefasst werden können.

- → Beispiel: Für ein System existiert die Bedrohung, dass das Passwort wird gebrochen, da es nur aus 8 Zeichen besteht.
  - → Einfacher Brutforce-Angriff
  - → Wörterbuch-Angriff
  - → Passwort-Spraying
  - → Phising-Angriff
  - → Keylogger-Angriffe

SCHWASCHSTELLEN

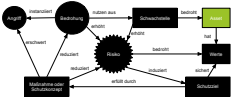
Schwachstellen sind eine Gefährdung für die Assets. Schwachstellen können somit eine Gefährdung für das System darstellen, wenn diese im Rahmen eines Angriffs ausgenutzt werden.



→ Siehe Vorlesung **Einführung** Folie 10 bis 12.

ASSETS

Eine Asset ist jede Komponente, jedes System, alle Daten, jede Anwendung oder jede Ressource, die für ein System, ein Unternehmen oder eine Organisation von immenser Bedeutung ist und geschützt werden muss.

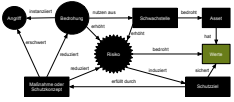


Ein Asset ist alles (materielle oder immaterielle) von besonderem Wert.

- → Datenbestände
- → Businessplan
- → Schlüssel

In manchen Fällen wird auch noch zwischen primären und sekundären Assets unterschieden. Sekundäre Assets hängen von primären Assets ab.

SCHÄDEN UND WERTE



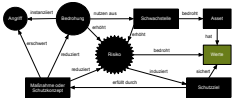
Bei Verlust des ursprünglichen Werts eines Assets hat dies Auswirkungen auf das System, Unternehmen oder die Organisation. Der Schaden der mit dem Wertverlust einhergeht kann sich verschieden stark in verschiedenen Bereichen auswirken.

Schadensklassifikation nach BSI IT-Grundschutz:

- → normal - Auswirkung ist begrenzt
- → hoch - Auswirkung sind beträchtlich
- → sehr hoch - Auswirkung ist existenziell bedrohlich und katastrophal

Beschreibung der Klassifizierung muss für jede betrachtete Schadenskategorie definiert sein. Klassifizierung und Schadensstufen sind oft domänenspezifisch.

SCHÄDEN UND WERTE



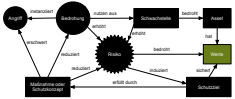
Bei Verlust des ursprünglichen Werts eines Assets hat dies Auswirkungen auf das System, Unternehmen oder die Organisation. Der Schaden der mit dem Wertverlust einhergeht kann sich verschieden stark in verschiedenen Bereichen auswirken.

Schadenskategorie im BSI IT-Grundschutz:

- → Verstoß gegen Gesetze/Vorschriften/Verträge
- → Beeinträchtigung des informationellen Selbstbestimmungsrechts
- → Beeinträchtigung der persönlichen Unversehrtheit
- → Beeinträchtigung der Aufgabenerfüllung
- → Negative Innen- oder Außenwirkung
- → Finanzielle Auswirkungen

SCHÄDEN UND WERTE

Bei Verlust des ursprünglichen Werts eines Assets hat dies Auswirkungen auf das System, Unternehmen oder die Organisation. Der Schaden der mit dem Wertverlust einhergeht kann sich verschieden stark in verschiedenen Bereichen auswirken.

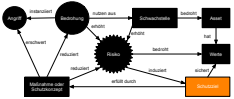


Schadenskategorie im Bereich Automotive nach der ISO21434:

- → Safety Schaden
- → Finanzieller Schaden
- → Operativer Schaden
- → Privatsphärenschaden

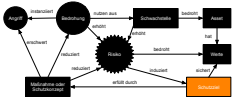
SCHUTZZIELE

Schutzziele definieren abstrakte Sicherheitsanforderungen an ein Asset. Das Schutzziel muss erfüllt sein, damit das Asset nicht sein Wert verliert. Diese Verletzung kann sich auch auf die ursprünglichen Eigenschaften des Systems sich auswirken.



- → Jedes Schutzziel konkretisieren den abstrakten Sicherheitseigenschaft die wichtig für die Eigenschaft und die Funktionalität des Assets ist.
- → Jede Sicherheitseigenschaft eines Schutzziels kann einen generische Art von Bedrohung gegenüber gestellt werden.
- → Die Anzahl der Schutzziel und deren art hängt von dem jeweiligen Schutzzielmodel ab.

SCHUTZZIELE IM DETAIL (1/3)

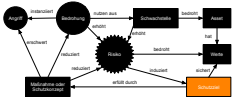


→ **Vertraulichkeit**: Schutz vor unbefugter Preisgabe von Informationen.
  → Veröffentlichung privater Bankdaten

→ **Integrität**: Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.
  → Ändern des Betrages bei einer Paypal-Überweisung

→ **Authentizität**: Kommunikationspartner ist tatsächlich diejenige Person, die sie vorgibt zu sein bzw. die Informationen wurden tatsächlich von der angegebenen Quelle erstellt.
  → Senden von Messanger-Nachricht unter falschem Namen

SCHUTZZIELE IM DETAIL (2/3)

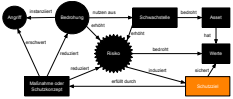


→ **Verfügbarkeit**: Sicherstellung des vorgesehenen Nutzbarkeit eines IT-Systems.
  → Stören der Compass Systems

→ **Autorisierung**: Freischaltung der eingeräumten Rechte für eine erfolgreich authentifizierte Person oder Identität.
  → Cheat-Code im Spiel eingeben

→ **Nicht-Abstreitbarkeit**: Empfangen/Senden einer Nachricht oder Durchführen einer Aktivität kann nicht abgestritten werden.
  → Beschuldigung des Autopiloten am Absturz des Flugzeugs

SCHUTZZIELE IM DETAIL (3/3)

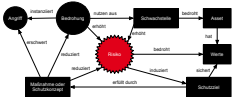


- Verschiedene gängige Sicherheitsziel-Modelle:
  - **CIA**: **C**onfidentiality, **I**ntegrity, **A**vailability
  - **CIAA**: CIA + **A**uthenticity
  - **STRIDE**: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privileges

Sicherheitsziel	Sicherheitsziel (eng.)	Bedrohung	Bedrohung (eng.)
Vertraulichkeit	Confidentiality	Unbefugtes Auslesen	Information Disclosure
Integrität	Integrity	Manipulation	Tampering
Authentizität	Authenticity	Fälschen	Spoofing
Verfügbarkeit	Availability	Störung des Betriebs	Denial-of-Service
Autorisierung	Authorization	Erhöhung von Rechten	Elevation of Privileges
Verbindlichkeit	Non-Repudiation	Abstreiten von Aktionen	Repudiation

RISIKO

Alleine die Existenz einer Schwachstelle mit einer potentiellen Bedrohung führt nicht zu einer 100% Ausnutzung. In der Regel wird für einen Angriff der Weg des geringsten Widerstands gewählt.

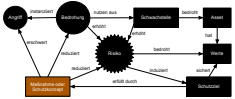


Das Risiko kann zur Priorisierung der Umsetzung der Maßnahmen genutzt werden

- → Alle Maßnahem umzusetzen steht oft nicht im Kosten/Nutzen-Verhältnis
- → Systematische Betrachtung der gesamten Bedrohungslandschaft
- → In die Risikobewertung geht sowohl die Wahrscheinlichkeit eines Angriffs ein als auch der zu erwartende Schaden auf das Asset oder Gesamtsystem

SCHUTZMASSNAHME

Maßnahmen können entweder technischer, prozessualer oder organisatorischer Art sein. Final wird mit der Maßnahme erreicht, dass Risiko soweit zu verringern, dass es akzeptierbar ist oder transferiert wird.

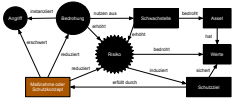


Maßnahmen für die verschiedenen Stadien einen Angriffs

- → **Präventive Maßnahmen** - Abwehr des Angriffs und Erhalt der Schutzziele
- → **Detektierende Maßnahme** - Maßnahme zur Detektion, wenn eine präventive Maßnahme den Angriff nicht abwehren konnte
- → **Reaktive Maßnahme** - Operative Maßnahme zum Wiederherstellen des Soll-Zustandes nach Detektion eines Sicherheitsereignisses

SCHUTZMASSNAHME

Maßnahmen können entweder technischer, prozessualer oder organisatorischer Art sein. Final wird mit der Maßnahme erreicht, dass Risiko soweit zu verringern, dass es akzeptierbar ist oder transferiert wird.



Maßnahme	präventiv	detektierend	reaktiv
prozessual und organistorisch	Schulungen, Richtlinien, Vulnerability-Management	Audit, SOC	CERT-Team, Blue und Red Team, Securtiy Responce Prozess
technisch	Verschlüsselungstechnologie, Firewall, Virenscanner, DMZ	Intrusion Detektion Systeme	Reaktive DMZ und Backup-System

WIEDERHOLUNG: SECURITY VS. SAFETY

Tauschen Sie sich mit Ihrem Sitznachbar 5 Minuten aus:

- → Identifizieren Sie zwei Assets von Ihrem Beispiel Heute morgen (Auto oder Getränkeautomat).
- → Identifizieren Sie pro Asset mindestens zwei Schutzziele basierend auf potentiellen Bedrohungen.

ANREIFERMODELL

Es ist wichtig für die Sicherheitsbetrachtung im Bezug auf potentielle Angriffe und Bedrohungen, verschiedene Arten von Angreifern zu berücksichtigen.

→ Grundsätzlich geschieht ein Angriff immer aus einer Motivation heraus.

Angreifer

Ein Angreifer ist immer ein Mensch; auch Organisationen bestehen aus Menschen.

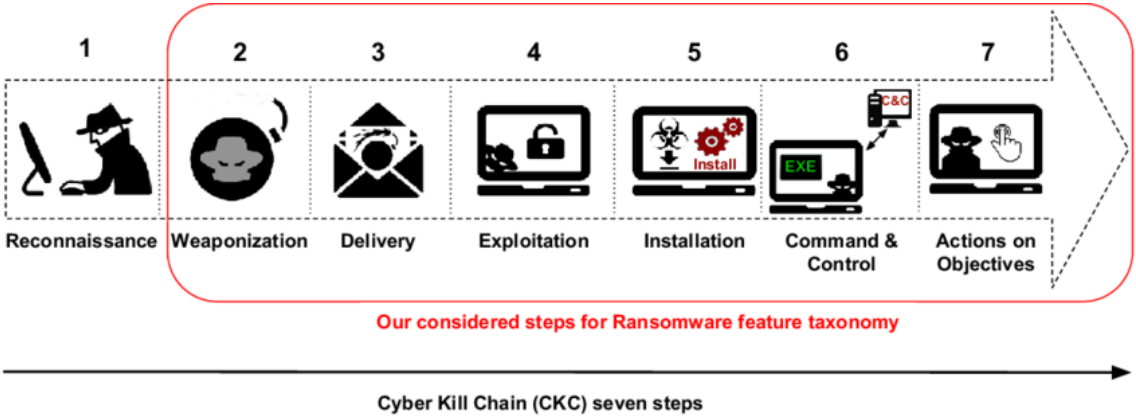
→ Die Fähigkeiten und Ressourcen zum Durchführen eines Angriffs häng auch vom Angreifertyp ab.

→ Die Motivation der Angreifer ist wichtig, da diese Rückschlüsse auf potentielle Ziele preisgibt.

ANGREIFER UND IHRE MOTIVATION

Angreifer	Motivation	Vorgehen
Anwender	Persönlicher Vorteil	Anwendung von Tools oder Anleitungen; Anheuerung organisierter Krimineller
Mitarbeitende	Rache; Geld; Ideologie	Zugriff auf und Kompromittierung von internen Systemen
Ethische Hacker	Anerkennung; Herausforderung; Geld; Ethische Überzeugung	Identifikation von Schwachstellen; Ausnutzung unter ethischen Richtlinien
Hacktivisten	Anerkennung; Herausforderung; Politische oder ideologische Ziele; Vandalismus; Geld	Identifikation und Ausnutzung von Schwachstellen; Offenlegung des Eindringens
Kriminelle	Geld	Identifikation und Ausnutzung von Schwachstellen; Kompromittierung des Systems; Monetarisierung
Konkurrenz	Störung; Entwendung von Technologie; Diskreditierung	Reverse-Engineering von Produkten; Anheuerung organisierter Krimineller
Organisierte Kriminelle	Geld	Systematische Identifikation und Ausnutzung von Schwachstellen; Kompromittierung des Systems; Bereitstellen von Services; Monetarisierung
Staaten / Geheimdienste	Wirtschaftliche Vorteile, Destabilisierung	Kompromittierung der Infrastruktur, Komponenten oder Standards; Tarnung vor Entdeckung

VORGEHENSWEISE NACH DER CYBER KILL CHAIN VON LOCKHEED MARTIN



Quelle: T. Dargahi et al., A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, Spriunger, 2019

CYBER KILL CHAIN - STUFE 1/RECONNAISSANCE: ZIELE SUCHEN

Aktivität der Angreifer:

- → Gezieltes Suchen nach Angriffszielen und sammeln von Informationen über einen längeren Zeitraum.
- → Aktives Abfangen von Daten und Ausnutzen menschlicher Schwächen.
- → Oft werden offene Tools wie Nmap und OpenVAS oder selbst entwickelte Tools verwendet.
- → Ebenso werden Informationen aus dem Darknet genutzt, um Angriffe vorzubereiten.

Mögliche Abwehr:

- → Die Reconnaissance ist schwer zu erkennen, wenn sie ausgeführt wird.
- → Unauffälliges Verhalten in Social Media. Prüfen ob Accounts auf Leaking-Plattformen wie “haveibeenpwned” auftauchen

CYBER KILL CHAIN - STUFE 2/WEAPONIZATION: AUSWAHL DES WERKZEUGS

Aktivität der Angreifer:

- → Gezieltes suche nach Schwachstellen im Unternehmen.
- → Nuzten leicht zugänglicher Angriffstools oder -anleitungen oder Erstellen eigener Tools mit Hilfe von Informationsmaterialien.
- → Botnets werden oft gemietet, um temporäre oder dauerhafte Angriffe durchzuführen.
- → Zusätzlich können auf dem Schwarzmarkt erwerbliche Zero-Day-Exploits zum Angriff genutzt werden.

Mögliche Abwehr:

- → Keine Gegenmaßnahme möglich

CYBER KILL CHAIN - STUFE 3/DELIVERY: AUSLIEFERN

Aktivität der Angreifer:

- → Ausliefern der Malware durch:
  - → Spam-Mail, Phishing-Mails
  - → Dateien in Antworten auf offizielle Anfragen (Bewerbungen und Angebote)
  - → Dateien und Links in Social Media
  - → Präparierte Webseiten

Mögliche Abwehr:

- → Awareness-Schulungen des Personals, Umsetzen von Sicherheitsrichtlinien
- → Verwenden von Antivirus Software, Email- und Webfilter

CYBER KILL CHAIN - STUFE 4/EXPLOITATION: AUSNUTZEN DER SCHWACHSTELLE

- → Ausnutzen von Schwachstellen, um später vollständigen Zugang zum Unternehmensnetzwerk zu erhalten.
- → Dies kann entweder still erfolgen oder direkt zu einer aktiven Beeinflussung der produktiven Systeme führen.
- → Angreifer nutzen neben technischen Werkzeugen oft auch Social Engineering, um Zugang zu erhalten.

Mögliche Abwehr:

- → Aktives Patch-Management, um das System up-to-date zu halten
- → Durchführen von Vulnerability Management mit automatischen Schwachstellenscans im System

CYBER KILL CHAIN - STUFE 5/INSTALLATION: ZUGANGSPERSISTIERUNG

- → Persistieren der Malware und des Zugriffs auf das System.
- → Oft werden Backdoors installiert und Reverse Shell genutzt und etabliert.
- → Translative Bewegung im System zum Auskundschaften des Netzwerks durch den dauerhaften Zugang zum infizierten System.
- → Ein Advanced Persistent Threat (APT) kann sich über einen längeren Zeitraum im System verstecken und dadurch auch Lieferanten und Kunden in der Lieferkette infiltrieren.

Mögliche Abwehr:

- → Sicherheitslösungen zur Erkennung, Protokollierung oder Whitelisting von erlaubter Software
- → Mehrfaktor-Autentifizierung, gutes Rechtemanagement

CYBER KILL CHAIN - STUFE 6/C2: KONTROLL UND KOMMUNIKATION

- → Verdeckte Kommunikation zu einem Control und Command Server wird aufgebaut um:
  - → Sensible Informationen und Daten zu exfiltrieren; werden oft im Darknet per Erpressungsversuch zum Rückkauf angeboten
  - → Nachladen von weiterer Schadsoftware und zur “Pflege” und Wartung der bereits installierten Malware
  - → Nutzen des infizierten Systems, um weitere Angriffe auf andere Systeme zu starten

Mögliche Abwehr:

- → Unterbinden der Kommunikation zum CC-Server mit Firewalls, Intrusion Detektion Systemen
- → Wechseln in den Notbetrieb (nur unbedingt notwendige Systeme und Kommunikationskanäle sind nutzbar), um den Schaden zu minimieren

CYBER KILL CHAIN - STUFE 7ACTION ON OBJECTIVE: AKTIVIERUNG NACH BEDARF

- → Je länger die Persistierung im System stattfindet desto mehr Aktivitäten können die Angreifer durchführen
- → Typische Aktivitäten zur Monetarisierung sind:
  - → Veröffentlichung von sensiblen Daten
  - → Verschlüsselung oder Manipulation von Daten
  - → Verwendung des infizierten Systems als Bot in einem Botnetzwerk

Mögliche Abwehr:

- → Durchführen einer IT-forensischen Analyse zur Rekonstruktion des Angriffs
- → Backup-System und ein Notfallmangamentplan haben (Business Continuity Management und Incedent Response Prozess)

ATT&CK-FRAMEWORK

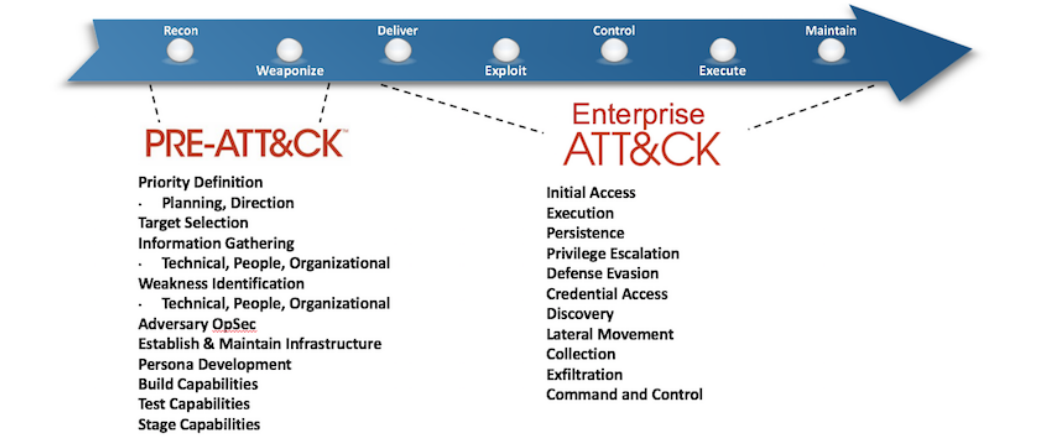


Figure: Att&ck-Framework

Quelle: https://www.ecrimelabs.com/blog/2020/4/5/mitre-attampck-for-improved-metrics-and-kpi-on-detection-capabilities - letzter Besuch 26.03.2023

ZUSAMMENFASSUNG

- → Angreifer sind immer Menschen oder Organisationen
- → Alle Sicherheitsarten (IT, Cyber, Informartionssicherheit) haben Gemeinsamkeiten aber auch Schwerpunkte
- → Schutzziel und Gegenmaßnahmen können mit einem risikobasierten Ansatz zur Abwehr von Bedrohungen identifiziert und priorisiert werden
- → Es gibt verschiedene Angreifertypen mit unterschiedlicher Motivation
- → Alle Schritte eines Angriffes auf IT-Systeme lassen sich generische durch die Phasen der Cyber Kill Chain abbilden