

# Cyber Security Techniken messen und priorisieren

Studiengang : MAS Cyber Security

Die Digitalisierung hält in immer mehr Bereichen Einzug. Doch welche Sicherheitstechnologien sollen eingeführt werden, um sich optimal vor Sicherheitsvorfällen zu schützen und wie können diese bewertet und priorisiert werden? Mit Hilfe anerkannter Cyber Security Frameworks können diese Fragen beantwortet werden.

## Ausgangslage

Cyber Security befasst sich mit der bestmöglichen Abwehr von Bedrohungen und Angriffen aus dem digitalen Raum. Dies geschieht auf verschiedenen Ebenen wie den Benutzer und Benutzerinnen, technischen sowie organisatorischen Massnahmen. Es gibt Handlungsempfehlungen in Form von Frameworks, welche Schutzmassnahmen angewendet werden sollten. Aufgrund der begrenzten personellen Ressourcen ist eine genaue Planung sowie eine Priorisierung für die Umsetzung dieser Massnahmen notwendig.

## Zielsetzung

Im Rahmen dieser Master-Thesis soll eine Möglichkeit entwickelt werden, wie Techniken und deren Bewertungskriterien aus anerkannten Frameworks abgeleitet werden können. Ziel ist eine Roadmap, die durch transparente und leicht nachvollziehbare Bewertungen überzeugt. Dazu ist es im Vorfeld notwendig, die Threat Actors für das Unternehmen zu kennen und zu bewerten.

## Entwicklung

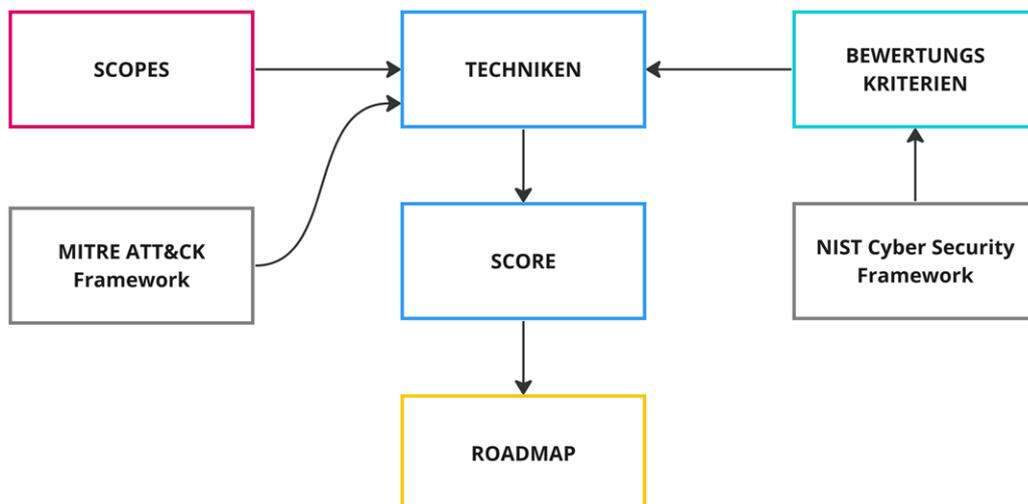
Durch die detaillierte Auseinandersetzung mit den Frameworks wurden 16 Techniken in fünf „Scopes“ aus dem „MITRE ATT&CK“ Framework abgeleitet. Die Bewertungskriterien, für jede der vier Cyber Security Prozessphasen des Unternehmens, wurden mit dem „NIST Cyber Security“ Framework verknüpft. Dies ermöglichte eine transparente Priorisierung anhand einer Punktzahl, dem sogenannten „Score“, sowie die Erstellung einer Roadmap und Handlungsempfehlungen für das Unternehmen.



David Lüthi

## Fazit

Cyber Security ist eine kontinuierliche Disziplin für ein Unternehmen insbesondere für die Informatik. Durch die Umsetzung der verschiedenen Projekte anhand der erstellten Roadmap, kann die Informatik die Herkulesaufgabe bewältigen, ihr Möglichstes getan zu haben, um sich vor einem Sicherheitsvorfall zu schützen.



Visualisierung Framework Einfluss