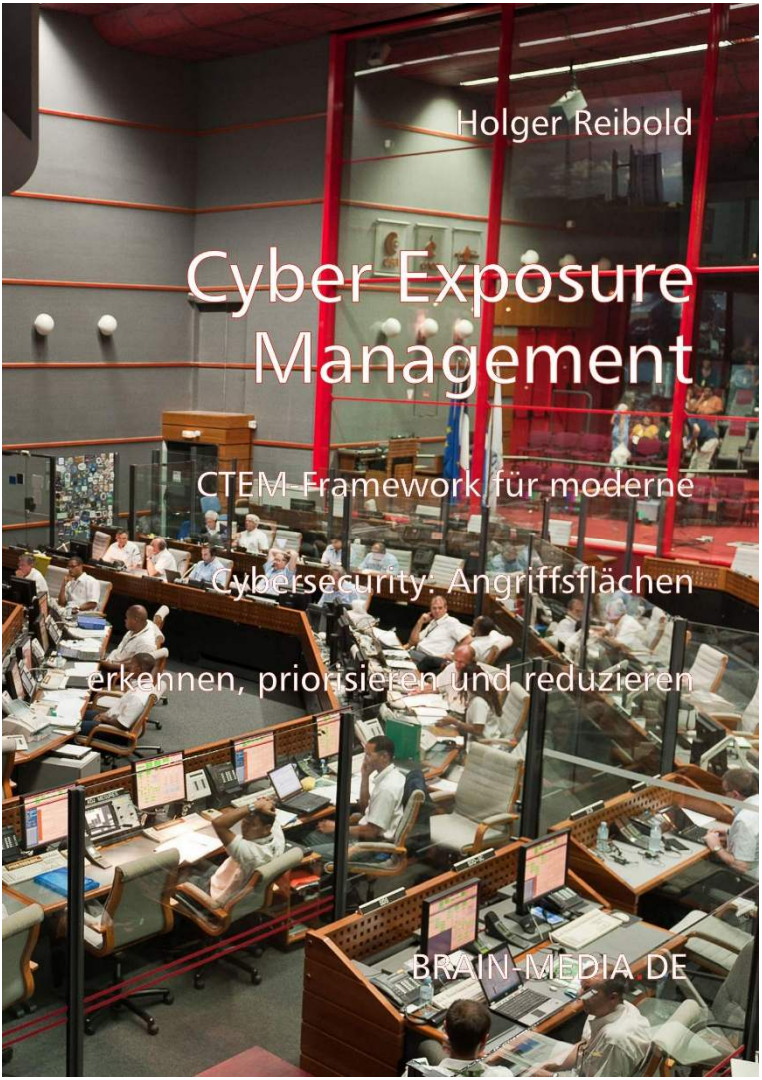

CTEM-Reifegradmodell zur Selbsteinschätzung

Die Einführung von Continuous Threat Exposure Management erfolgt in den meisten Organisationen nicht auf einen Schlag. Stattdessen entwickelt sich der Ansatz schrittweise über mehrere Reifestufen hinweg. Unternehmen beginnen häufig mit isolierten Sicherheitsanalysen und entwickeln ihre Fähigkeiten im Laufe der Zeit zu einem strukturierten, kontinuierlichen Management ihrer Cyber-Exposures weiter.

Das folgende Reifegradmodell bietet eine Orientierung, um den aktuellen Stand der eigenen Organisation einzuschätzen und mögliche nächste Entwicklungsschritte zu identifizieren.

Stufe 1 – Initial

In der Anfangsphase existieren Sicherheitsmaßnahmen meist in Form einzelner, voneinander unabhängiger Aktivitäten. Schwachstellen werden beispielsweise durch regelmäßige Scans identifiziert, jedoch häufig ohne systematische Priorisierung oder Kontextanalyse. Cybersecurity wird in dieser Phase häufig als reaktive Aufgabe verstanden, die primär auf einzelne Sicherheitsmeldungen reagiert. Typische Merkmale:

- punktuelle Vulnerability-Scans
- begrenzte Transparenz über die gesamte Angriffsfläche
- manuelle Analyse einzelner Sicherheitsprobleme
- kaum Integration zwischen verschiedenen Security-Tools

Stufe 2 – Visibility

Organisationen beginnen damit, ihre digitale Angriffsfläche systematischer zu erfassen. Asset-Inventare werden aufgebaut, Cloud-Ressourcen werden sichtbarer und erste Attack-Surface-Analysen werden durchgeführt. Der Fokus liegt in dieser Phase vor allem darauf, ein vollständigeres Bild der eigenen Infrastruktur und potenzieller Angriffspunkte zu erhalten. Typische Merkmale:

- zentrale Asset-Inventare oder CMDB-Strukturen
- erste External-Attack-Surface-Analysen
- Integration mehrerer Sicherheitsdatenquellen
- verbesserte Transparenz über Cloud- und SaaS-Ressourcen

Stufe 3 – Risk-Based

In dieser Phase entwickelt sich der Sicherheitsansatz von reiner Sichtbarkeit hin zu einer risikobasierten Analyse. Schwachstellen werden nicht mehr ausschließlich nach technischen Scores bewertet, sondern im Kontext ihrer möglichen Auswirkungen auf das Unternehmen betrachtet. Security-Teams beginnen, Cyberrisiken stärker mit geschäftlichen Auswirkungen zu verknüpfen. Typische Merkmale sind:

- kontextbasierte Priorisierung von Schwachstellen
- Berücksichtigung von Asset-Kritikalität
- Integration von Threat-Intelligence-Daten
- erste Analysen möglicher Angriffspfade

Stufe 4 – Continuous

Exposure Management wird nun als kontinuierlicher Prozess betrieben. Sicherheitsanalysen erfolgen regelmäßig und automatisiert, während neue Systeme und Veränderungen in der Infrastruktur fortlaufend in die Risikobewertung einbezogen werden. Cybersecurity entwickelt sich zunehmend zu einem integrierten Bestandteil operativer IT-Prozesse. Typische Merkmale:

- kontinuierliche Attack-Surface-Überwachung
- automatisierte Sicherheitsanalysen
- regelmäßige Validierung von Sicherheitskontrollen
- strukturierte Remediation-Prozesse

Stufe 5 – Optimized

In der höchsten Reifestufe ist Exposure Management vollständig in die Sicherheits- und Risikostrategie der Organisation integriert. Sicherheitsanalysen, Priorisierung und Remediation sind weitgehend automatisiert und eng mit Geschäftsentscheidungen verbunden. Organisationen erreichen in dieser Phase ein hohes Maß an Transparenz über ihre Angriffsflächen und können Cyberrisiken systematisch steuern. Typische Merkmale:

- automatisierte Risikoanalysen und Priorisierung
- integrierte Angriffspfadmodellierung
- automatisierte Remediation-Workflows

Selbsteinschätzung

Organisationen können dieses Modell nutzen, um ihren aktuellen Reifegrad zu bewerten. Dabei ist zu beachten, dass viele Unternehmen Elemente mehrerer Stufen gleichzeitig aufweisen. Ziel des Modells ist nicht eine perfekte Einordnung, sondern eine Orientierung für die kontinuierliche Weiterentwicklung der eigenen Sicherheitsstrategie.

Der Weg zu einem vollständig etablierten CTEM-Programm ist ein langfristiger Prozess. Jede Reifestufe stellt dabei einen wichtigen Schritt dar, um Cyberrisiken besser zu verstehen, gezielter zu priorisieren und nachhaltiger zu reduzieren.

Mehr zum Thema CTEM

Der vollständige Leitfaden „Cyber Exposure Management – CTEM-Framework für moderne Cybersecurity: Angriffsflächen erkennen, priorisieren und reduzieren“