Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

CTEM
Continuous Threat Exposure Management

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten,** regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

Was wir dabei oft vergessen, sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten, sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

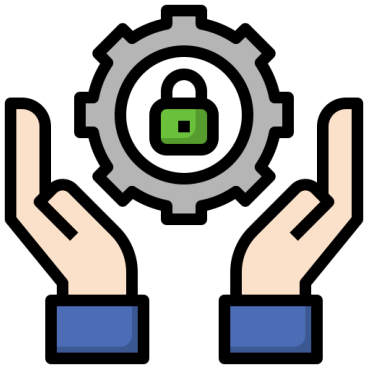
Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

CTEM – Was ist das?

Continuous Threat Exposure Management (CTEM) oder **kontinuierliches Bedrohungsmanagement** ist ein strategischer Ansatz für die Cybersicherheit in Unternehmen. Bedrohungen und Anfälligkeiten eines Unternehmens werden ständig in Echtzeit überwacht und verwaltet.

So werden **potenzielle Schwachstellen** und **Bedrohungen** aufgespürt, bevor Angreifer sie ausnutzen können. Es handelt sich um eine **proaktive Sicherheitstechnik**, um sich nicht ausschließlich auf reaktive Maßnahmen wie Firewalls und Antivirensoftware zu verlassen.



Wie funktioniert CTEM?

Die CTEM lässt sich in 5 Phasen unterteilen – Rahmenuntersuchung, Entdeckung, Priorisierung, Validierung und Mobilisierung.

Rahmenuntersuchung
Identifizierung der wichtigsten Werte des Unternehmens sowie Bestimmung der damit verbundenen Risiken. Diese Phase ist die Grundlage der nachfolgenden Schritte.

Entdeckung
Identifizieren und Katalogisieren der gefährdeten Ressourcen (Applikationen, Soft-/Hardware, Datenbanken, Netzwerkinfrastruktur); Einsatz verschiedener IT-Entdeckungs-Tools, Penetrationstests und Sicherheitsaudits.

Priorisierung
Bewertung der erkannten Schwachstellen, Bewertung der damit verbundenen Risiken für den Geschäftsbetrieb und Festlegung einer Rangfolge.

Validierung
Bewertung der ergriffenen Maßnahmen zur Bedrohungsabwehr und deren Anpassung.

Mobilisierung
Definition des Umfangs der Maßnahmen, Festlegen der Ziele sowie eine „Bereitschaftsbewertung"; Identifizieren von Interessengruppen und Ressourcen.

5 Phasen von CTEM

Wem nutzt CTEM?

Unternehmen und andere Organisationen sehen sich immer weiter entwickelten und raffinierteren Cyber-Bedrohungen gegenüber. Um durch einen proaktiven Ansatz den Cyber-Kriminellen einen Schritt voraus zu sein, muss ein ständiges Exposure- (Bedrohungs-) Management Bestandteil jedes IT-Sicherheitskonzeptes sein. Diese Methode hilft Sicherheitsteams dabei, **frühzeitig Bedrohungen zu identifizieren und abzuwehren**. Der Markt bietet verschiedenste Software-Tools, die hilfreich bei der Umsetzung sind. **Externe Anbieter** können bei der Beschaffung und Implementierung unterstützen. Die Expertise dieser Dienstleister hilft bei den ersten Schritten und der effektiven Durchführung.

Cyber-Sicherheitsrat Deutschland e.V.

Welche Chancen gibt es?

Ergreifen von Maßnahmen, um potenzielle Bedrohungen und Schwachstellen zu erkennen und zu verhindern, bevor diese ausgenutzt werden.

CTEM hilft mittels fortschrittlicher Analysen, maschinellen Lernens und künstlicher Intelligenz dabei, **Bedrohungen zu identifizieren und zu priorisieren**. Inwieweit sind die digitalen Assets eines Unternehmens für Cyberangreifer zugänglich, exponiert und ausnutzbar?

CTEM verschafft Unternehmen einen **Echtzeitüberblick** über die Bedrohungs-/Risikolage im Bereich Cybersecurity und hilft dabei, Sicherheitsentscheidungen fundierter zu treffen, wie z.B. bezüglich des erforderlichen Ressourceneinsatzes, um diese Angriffe abzuwehren.

Unternehmen, die einen grundlegenden Plan für die Reaktion auf Bedrohungen und Vorfälle entwickelt haben, können nachteilige Auswirkungen minimieren. Durch den Einsatz automatisierter Systeme zur Erkennung und Reaktion auf diese Bedrohungen **verhindern sie effektiv eine Ausweitung von Cyber-Angriffen**.

Welche Risiken gibt es?

In Zeiten knapper Ressourcen ist CTEM eine weitere Herausforderung für IT-Teams und möglicherweise auch ein **Investment** in die Ausbildung der Mitarbeiter.

Auf technologischer Seite erfordert die Einführung von CTEM (bzw. der erforderlichen Tools) vernachlässigbare Ressourcen. Eine **korrekte Implementierung und Regelzuweisungen** müssen gewährleistet sein. Die Lösung muss in die Arbeitsabläufe integriert und Verantwortlichkeiten zugewiesen werden.

Es kann jedoch gefährlich sein, sich ausschließlich auf die automatische Behebung durch das Programm zu verlassen. Der Lösungsvorschlag des CTEM-Programms sollte dabei nicht vollautomatisch implementiert werden, ohne nachzudenken. Das Sicherheitsteam muss, gestützt durch das Management, die finale Entscheidung treffen und Genehmigungen erteilen.

Fazit

Planen, überwachen und reduzieren sie kontinuierlich die Bedrohungen und Anfälligkeiten sowie die damit verbundenen Risiken im Unternehmen. Nutzen sie Priorisierungs- und Validierungstechnologien, die kontextbezogen priorisierte Abhilfemaßnahmen veranlassen.

Die Informationen dieser Technologien helfen dabei, die Bedrohungen besser zu verstehen und geeignete Maßnahmen ergreifen zu können. Damit können sie eine **Ergänzung zu automatisierten und reaktiven Maßnahmen** darstellen.