Compromise Assessment

Kompromittierungen erkennen und zielgerichtet handeln, um mit schnellen Gegenmaßnahmen Schäden zu vermeiden

Meistens agieren Cyber-Kriminelle leise und unauffällig - sie dringen unbemerkt in Netzwerke und Systeme ein und sind damit aber noch längst nicht am Ziel, denn sie wollen einen größtmöglichen Schaden anrichten.

> Mit professioneller Unterstützung kompromittierte Systeme erkennen und bereinigen, bevor der Angreifer sein Ziel erreicht

Angreifer versuchen deshalb, in möglichst viele Systeme einzudringen, Benutzerkonten zu kompromittieren und Passwörter auszuspähen - der zeitliche Aspekt spielt dabei keine Rolle, solange sie unentdeckt bleiben.

Genau an dieser Stelle setzt unser Compromise Assessment an, denn hier analysieren wir im Rahmen der Erstanalyse die technische Infrastruktur des Unternehmens, um eine mögliche Kompromittierung aufzuspüren, um das potenzielle Risiko zu ermitteln und den Stand der IT-Sicherheit festzustellen.

> Das schnelle und zuverlässige Erkennen von möglichen Kompromittierungen ermöglicht ein schnelles Handel und das Ergreifen von zielgerichteten Gegenmaßnahmen.

Wir orientieren uns dabei am Leitfaden des BSI und dem Standardvorgehen des SANS Institutes. Durch die Nutzung entsprechender Methoden und Werkzeuge gelingt es uns, mögliche Kompromittierungen schnell zu erkennen und notwendige Maßnahmen einzuleiten.

Ein Compromise Assessment gestalten wir immer nach der Größe des IT-Verbunds, den gängigen Standards und den individuellen Wünschen unserer Kunden. Unsere Cyber Security Consultants untersuchen während der Durchführung ausgewählte Teile der IT-Infrastruktur und halten alle Erkenntnisse in detaillierten Berichten fest.

> Ein detailliertes Lagebild als Basis für ein gezieltes Handeln

Auf diese Weise kann ein Lagebild erzeugt, das Ausmaß einer Kompromittierung eingeschätzt und notwendige Maßnahmen abgeleitet werden. Alle Ergebnisse des Assessments werden im Rahmen einer Abschlusspräsentation vorgestellt und mögliche Maßnahmen empfohlen. Das Compromise Assessment unterstützt dabei auch das Incident Response Management, welches bei Bedarf als zusätzlicher Service von uns erbracht werden kann.

IHRE VORTEILE

- Aufarbeitung eines möglichen Sicherheitsvorfalls
- Schnittstelle zum Incident Response Prozess
- Erkennen von Schwachstellen in der Infrastruktur
- Risikoanalyse zum technischen Stand der IT

OEDIV SecuSys GmbH
Brückenweg 5 | 18146 Rostock | **www.secusys.de**

Info@secusys.de +49 381 37573-0