Berliner Hochschule für Technik

Fachbereich VI - Informatik und Medien
Studiengang IT-Sicherheit Online / Medieninformatik

Vertiefung 7

PARETO CONSULTING

Modul: Sicherheitsmanagement

Dozent: Sven Zehl

vorgelegt von: Gruppe 1
Christine Kuczera
Dirk Drutschmann
Hicham Naoufal
Michael Schröter
Jan Zimmermann
Ivo Valls

Aufgabe a) Füllen Sie Abbildung 4 mit weiteren Beispielen zum Schädigungspotential!

Antwort

	Aktivisten	**Script Kiddies**	**Organisiertes Verbrechen**	**Staatliche Organisationen**
Spaß, Grenzen testen	Gezielte Malware, Social Engineering	Vorgefertigte Scripts und Anleitungen	-	-
Intellektuelle Herausforderung	-	-	-	-
Politische Motivation: Fanatismus	DDoS-Angriffe mittels Botnetzen	-	Malware (z.B. Scareware), Mehrstufige Angriffe	Malware (z.B. Rootkits)
Persönliche Motive: Genugtuung	Malware (z.B. Würmer)	Vorgefertigte Scripts und Anleitungen	Ungezielte Malware (Drive-by-Exploits)	Malware (z.B. Trojaner)
Finanzielle Motive	Whaling	-	Identitätsdiebstahl, Social Engineering, Pharming	Social Engineering, Spionage (z.B. Spyware)
Internationale Konflikte	Gezieltes Hacking	-	Gezieltes Hacking von Webservern	Gezieltes Hacking von Webservern, Hybride Kriegsführung

Aufgabe b) Skizzieren Sie die Selbstlegitimation des "Gray Hat". Wie würden Sie vorbeugen?

Antwort

Selbstlegitimation

Die Selbstlegitimations von Gray Hats ist das Streben nach Verbesserung der Sicherheit und dem Aufdecken von Schwachstellen.
Hierfür verwenden sie sowohl legalen als auch illegalen Methoden zur Identifikation/Nutzung von Schwachstellen unter den Vorgaben des ethical Hackings. Sie grenzen sich damit klar von Black Hats ab, verfügen aber meist ebenso über umfassende Kenntinsse und Fähigkeiten.

Vorbeugende Maßnahmen:

Die Etablierung von Richtlinien und Standards und die Entwicklung der Richtlienen durch das Unternehmen für das Testen von Sicherheitslücken. Auch die Beschränkung des Zugangs zu Systemen und Daten auf Notwendigkeitsbasis und die Implementierung von Kontrollen und Überwachungen zur Erkennung/Reaktion von verdächtige Aktivitäten können potentiellen Angriffen entgegen wirken.

Aufgabe c) Skizzieren Sie, wie ein Unternehmen sein Asset ändern könnte, sollten die Maßnahmen zur Behebung der Schwachstellen nicht mehr wirtschaftlich sein.

Antwort

Wird in der Bedrohungsmodellierung der Kausalkette Angreifer - System - Asset festgestellt, dass es sich wirtschaftlich nicht lohnt die gefundenen Maßnahmen umzusetzen, hat ein Unternehmen, folgende Möglichkeiten:

- Ändern der angebotetnen Services mit neu Modelierung der Bedrohung
- Auslagern der Services an einen Dienstleister um Scaleneffecte zu nutzen
- Einstellung des Dienstes so dass das Asset nicht mehr geschütz werden muss

Grundsätzlich gilt auch hier, den Zugang zu Systemen und Daten auf Notwendigkeitsbasis zu beschtränken und eine Implementierung von Kontrollen und Überwachungen zur Erkennung/Reaktion von verdächtige Aktivitäten.

Aufgabe d) Ermitteln Sie für Ihren Use Case folgende Eckpunkte:

Antwort

Unternehmenswerte	Anwenderanforderungen	Sicherheitsziele	Angreifer
Auktionsdaten müssen vertrauenswürdig und unveränderlich sein	Auktionsdaten dürfen nicht manipulierbar sein	Integrität	Insider-Bedrohungen, Hacker
Zahlungsinformation	Zahlungsinformationen dürfen nicht an Unbefugte gelangen	Vertraulichkeit	Finanzamt, Hacker
Nur berechtigte User dürfen auf ihre Konten zugreifen und persönlicher Informationen müssen vertraulich behandelt werden	Sichere Authentifizierung mittels zweifelsfreier Identitätsprüfung	Authentizität	Phishing-Angreifer, Identitätsdiebe

Aufgabe e) Modellieren Sie die Webapplication Ihres Use Cases mittels MTMT DFD

Antwort

Siehe MTMT Report