Cyber Attack Infrastructure

Studiengang: MAS Cyber Security

Präventive Cybersicherheitsmassnahmen senken die Eintrittswahrscheinlichkeit eines folgenschweren Cyberangriffs - jedoch um die Widerstandsfähigkeit gegen erfolgreiche Cyberangriffe steigern zu können, müssen Bedrohungsszenarien unternehmensweit trainiert werden.

Intro
Eine «Cyber Attack Infrastructure» ist eine IT-Infrastruktur, welche für die Ausführung von Cyberangriffen ausgelegt ist und stellt damit den Betreibern alle Dienste für einen geplanten Cyberangriff zur Verfügung. Im Kontext von «Red Team Exercises» kann man auch von einer «Red Team Infrastructure» sprechen.

Ausgangslage
Der Auftraggeber möchte vermehrt bedrohungsbasierte Sicherheitsüberprüfungen durchführen und ist daher auf eine moderne «Cyber Attack Infrastructure» angewiesen. Damit sollen die hohen Sicherheitsanforderungen der Kunden umfassend überprüft und sichergestellt werden können. Darüber hinaus sollen die Kunden des Auftraggebers verstärkt auf künftige Cyberangriffe vorbereitet werden, indem die Detektions-, Reaktions- und Wiederherstellungsfähigkeiten im Rahmen von Bedrohungsszenarien proaktiv addressiert werden.

Zielsetzung
In dieser Masterthesis soll eine «Cyber Attack Infrastructure» entwickelt und in einen Testbetrieb aufgenommen werden. Die Infrastruktur soll sich aktuellen Standards und Cyberbedrohungen orientieren. Um die funktionalen Anforderungen und die Einsatzbereitschaft sicherzustellen wurden zuvor Abnahmekriterien in Form von Anwendungsfällen definiert.

Anforderungsspezifikation
Zusätzlich zu einer sicheren, herkömmlichen IT-Infrastruktur, fordert eine «Cyber Attack Infrastructure» erweiterte Modularität, Portier- sowie Skalierbarkeit, um möglichst schnell den verändernden Anforderungen während eines laufenden Cyberangriffs gerecht werden zu können. Des Weiteren bedarf es einem automatisierten Bereitstellungsprozess, damit die In- und Ausserbetriebnahme bei Projektstart bzw. Projektende effizient und fehlerfrei gelingen kann.

Zusätzlich muss das Gesamtsystem vollständig «Multiuser»-fähig sein. Es muss also gewährleistet werden, dass die Infrastruktur sowohl gleichzeitig von mehreren Operatoren, als auch kollaborativ weiterentwickelt werden kann.

Mögliche Systemkomponenten einer modernen «Cyber Attack Infrastructure» sind:

- Phishing Infrastruktur wie bspw. Mail, Messenger-Apps etc.
- Command & Control Instanzen
- Unterschiedliche Webserver für: Schadsoftware Bereitstellung, Upload Funktionalitäten, Täuschungsmanöver etc.
- Reverse Proxies und Hide-NAT-Router
- Einen Pool an Domänen sowie auch public IPs
- Zentralisierte Logverwaltung
- Physische Komponenten wie USB-Sticks, WLAN Antennen etc.
- Weitere szenarioabhängige Komponenten

Resultat
Unter Einhaltung der partiell erwähnten Anforderungen und weiteren Vorgaben, resultierte eine «Cyber Attack Infrastructure», die jederzeit vollautomatisch und ortsunabhängig hochgefahren werden kann. Des Weiteren wurde das Gesamtsystem in eine Systemüberwachung und «Alert-Pipeline» integriert, sodass bei einer Fehlfunktion die Betreiber rund um die Uhr, sicher und zuverlässig über eine Mobile-App informiert werden.

Ausblick
Der aktuelle Stand der «Cyber Attack Infrastructure» erlaubt es, die Infrastruktur technisch und organisatorisch in die bestehende Systemlandschaft des Auftraggebers zu integrieren. Nach Abschluss der Systemintegration werden weitere, intensive Praxistests durchgeführt, bis das System produktiv verwendet werden kann.

Robin Helbling
bfh.wwzgu@slmails.com