Evaluation der Security Assets in einer Hybrid Cloud Umgebung für ein Pflichtenheft

Studiengang: MAS Cyber Security

Cyber Security oder Cyber Defence sind in letzter Zeit vermehrt in den Medien thematisiert worden: erfolgreiche «Hacks», Cyber Defense als Staatsauftrag, Cyber Angriffe als militärisches Mittel oder das Geschäft mit Cyber Versicherungen.

Ob offensiv oder defensiv eingesetzt - Informationen sind der Schlüssel zum Erfolg.

In dieser Thesis will ich aufzeigen welche Informationen in den vorhandenen Logs Hinweise auf Angriffe geben könnten und wie diese zu korrelieren sind.
Ziel ist es, Attacken zu erkennen und zu unterbinden. Unabhängig, ob es sich um einen neuen oder bereits erfolgten Angriff handelt.
Cyber Angriffe können nie vollständig vermieden werden. Durch ein einfaches Mittel wie ein Security Monitoring und viel Zeit, kann das Risiko eines Angriffes reduziert werden. Beim Monitoring geht es nicht darum für jeden Zugriff einen Event zu generieren, sondern in der Menge von Log Daten Anomalien zu erkennen und entsprechend zu alarmieren. Die richtigen Informationen zur richtigen Zeit aufbereitet zu erhalten.

Angriffe werden immer raffinierter und komplexer. Die Unternehmen ihrerseits verlagern immer mehr Assets in die Cloud. Dies kann zu einer gefährlichen Mischung führen.

Das Fundament jedes guten Security Monitoring ist das Erkennen und Reduzieren von Angriffsvektoren, ein konsequentes und regelmässiges einspielen von Updates und die Wartung der Systemlandschaft sowie regelmässige Schwachstellen Scans.

Der Asset, Vulnerability und Threat Kreislauf ist entscheidend bei der Bekämpfung von Cyber Bedrohungen. Nur mit ihm ist es möglich die Angriffsvektoren nachhaltig zu reduzieren. Der Prozess zur Reduktion von Angriffsflächen muss von jedem Team mitgetragen werden. Die grösste Schwierigkeit dabei ist der Einsatz von Subapplikationen oder Bibliotheken, welche mit der eigentlichen Applikation installiert werden. Hier sind die Verantwortlichkeiten meist nicht restlos geklärt.

Security Monitoring ist kein Verkaufsschlager. Doch zur Aufklärung und Bekämpfung von Cyber Attacken ist es eines der besten Werkzeuge eines Security Operation Centers.

Ein grosser Punkt in meiner Arbeit ist das Erstellen einer Lagebeurteilung. Hier gibt es kein Standardwerkzeug, da jedes Unternehmen anders ist. Zudem gibt es Faktoren wie die geopolitische Lage oder eine neue hochkritische Schwachstelle, welche die Bedrohungslage innert kürzester Zeit verändern und erst im Nachhinein in eine Beurteilung einfliessen. Das eigens dafür entworfene Flussdiagramm soll dem Unternehmen helfen die Bedrohungslagen basierend auf vorhandenen Informationen einzuschätzen.

Philipp Scheiwiler

Asset, Vulnerability, Threat Kreislauf