Grobkonzept zentrales Vulnerability Management

Studiengang: MAS Cyber Security

Um der aktuellen und zukünftigen Cyberlage gerecht zu werden, hat das Unternehmen eine Überarbeitung des heute genutzten Vulnerability Management vorgesehen. Im Rahmen der Master-Thesis wurde mit der konzeptuellen Erstellung eines zentralen Abteilung und Team übergreifendes Vulnerability Management der erste Meilenstein erreicht.

Ausgangslage

Zurzeit verfügt das Unternehmen über ein dezentrales Vulnerability Management. Durch dieses Verfahren gehen wertvolle Ressourcen und Zeit verloren. Die Informationen über Zuständigkeiten der auszuführenden Arbeiten im Bereich Vulnerability Management sind aus prozessualen und technischen Gründen schwierig zu determinieren. Somit sind die Prozesse zum Teil Unternehmens-Intern nicht gelebt.
Das Inventar, LifeCycle, Patch, Asset und Incident Management sind nicht überall in den Vulnerability Management Prozess integriert. Dies führt zu diversen Fehlern im Inventar und zu versteckten Schwachstellen im Bereich der veralteten und nicht mehr patchbaren Komponenten.
Die IKT Komponenten sind teilweise keinem aktiven IT-Service zugeordnet. Die Auswirkungen einer Schwachstelle auf einen bestimmten Service sind nicht immer identifizierbar. Das Risiko pro Service kann nicht immer kalkuliert werden.

Zielsetzung

Das Ziel der Arbeit besteht in der Erstellung der Grundlagen des neuen Vulnerability Management innerhalb des Unternehmens.
Das zukünftige Vulnerability Management des Unternehmens muss:

- zentralisiert werden;
- einheitlich und standardisiert sein;
- eine hohe Akzeptanz der betroffenen Stellen geniessen.

Die Grundlagen in Form eines Konzepts dienen zur internen Beauftragung für die Erstellung eines Detailkonzepts und anschliessend der Realisierung und Implementierung der Lösungen.

Lösung

Im Rahmen der Arbeit wurde eine neue Prozesslandschaft für das Vulnerability Management des Unternehmens erstellt das folgende Prozesse beinhaltet:

- der zyklische Kernprozess mit Scan, Prioritize, Assess, Report, Fix, Verify;
- Security Guidelines Management;
- Meldestelle und Bug Bounty Program;
- Security Champions Program;
- Ausnahme-Management und URL-Whitelisting-Management;
- Patch-Management und Configuration-Management;
- und weitere Support Prozesse.

Im weiteren wurden technische Anforderungen und Massnahmen erstellt zu:

- Infrastruktur und Vulnerability Scan und dessen Toolset;
- Schwachstellen Tracking und dessen Verwaltungstool;
- Bewertung und Priorisierung von Schwachstellen;
- Organisatorische Schwachstellen;
- Threat Modeling und Threat Intelligence;
- Schwachstellen Behandlung (Behebung und Eindämmung);
- Eskalationsverfahren
- und weitere technischen Themen.

Abschliessend wurden Entwürfe für die noch nötigen Richtlinien des Unternehmens erstellt (Vulnerability Management Policy und Vulnerability Disclosure Policy).

Fazit

Während der Erstellung des Konzeptes wurde die Implementierung gewisser Prozesse via des bestehenden Reorganisation-Projekt gestartet. Die Teilnahme von den betroffenen Teams und die Unterstützung der Geschäfts-Leitung ist eine vielversprechende Ausgangslage für die Implementierung des Vulnerability Management Konzepts.

Yann Clavel

Asmer Medar