5,00 von 5

SEHR GUT

Empfehlung

Bewertung und Zitate des Auftraggebers:

„Wir wurden seit 2015 sehr gut durch das Team der canacoon in unseren IT Sicherheitsthemen begleitet und nehmen die Experten der canacoon auch weiterhin gerne in Anspruch - Empfehlung ohne Einschränkung!“

canacoon Case Study

Umsetzung eines Schwachstellenmanagements

Der Kunde in Stichpunkten

- deutsche Finanzgesellschaft eines Automobilherstellers, die 1949 gegründet wurde
- weltweit mehrere Landesgesellschaft
- 130,1 Milliarden Euro Umsatz weltweit
- verwaltet die Finanz-, Leasing- und Mietgeschäfte des Automobilherstellers und seiner Marken

Das Unternehmen unterliegt einer Vielzahl von Regularien und Bankaufsichtsbehörden, unter Anderem PCI-DSS, BaFin, EZB und MaRisk und BAIT, sowie der Datenschutzverordnung (GDPR).

Die Aufgabenstellung

Als Finanzunternehmen unterliegt der Kunde regulatorischen Auflagen, insbesondere IT-Sicherheitsvorgaben, unter anderem der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) oder EZB (Europäischen Zentralbank). Diese bestimmen auch den Umgang mit Schwachstellen in IT-Bereichen zur Reduzierung von Risiken, die zum Ausfall der IT-Infrastruktur führen können.

Der Kunde suchte nach einer Lösung, um bestehende Schwachstellen zu identifizieren, sie zu analysieren und dann risikobasiert beheben zu können. Die dazu nötigen Prozesse sollten entworfen und im Unternehmen verankert werden, sodass eine nachhaltige Bearbeitung ermöglicht wird. Im Scope befanden sich neben Vorgaben des CERT-Bund auch konzerneigene Kriterien, die durch die Lösung erkannt werden sollten.

In einem initialen Scan wurden Schwachstellen im fünfstelligen Bereich identifiziert, die auf mehr als 3.000 Assets gefunden wurden. Diese sollten nachhaltig behoben und dokumentiert werden. Hierzu waren systemverantwortliche Abteilungen zu identifizieren und mit der Behebung der Schwachstellen zu beauftragen.

Die Lösung

Zur Schwachstellenerkennung wurde ein Scanner gewählt, der es ermöglichte, eigene Schwachstellendefinitionen festzulegen. Auf diese Weise konnten konzerneigene Vorgaben implementiert und geprüft werden. Es wurden *credentialed Scans* (Host Scan) gewählt, um die Netzwerkbelastung zu reduzieren und genauere Ergebnisse zu erzielen. Die Angreifersicht sollte nicht dargestellt werden.

Die Scanergebnisse sollten in einem wöchentlichen Report übermittelt und zur Auswertung an entsprechende Stellen weitergegeben werden. Im Rahmen der Analyse wurde eine Datenbankstruktur genutzt, um zusätzliche, dem Scanner nicht zu Verfügung stehende Informationen sammeln und auswerten zu können. Hierbei waren beispielsweise das erst- und letztmalige Auftreten der Schwachstellen relevant, auf diese Weise konnten jedoch auch Schwachstellen getrackt werden, die im letzten Scandurchlauf nicht mehr identifiziert wurden, oder die nicht zur Adressierung weitergegeben werden mussten. Es konnten Informationen wie Ausnahmeregelungen, Mitigationslösungen und vorherige Adressierung bekannter Schwachstellen nachverfolgt werden, wodurch sich Overhead durch doppelte und unnötige Adressierungen vermeiden ließ.

Zur Realisierung der risikobasierten Behebung wurde der *Common Vulnerability Scoring System* (CVSS) Standard genutzt. Durch dieses Bewertungssystem können besonders kritische Schwachstellen identifiziert und priorisiert bearbeitet werden. So können die schwerwiegendsten Schwachstellen bereits früh im Projekt abgestellt werden.

Zur Adressierung der Findings konnte auf ein bestehendes IT Service Management System zurückgegriffen werden. Dieses griff auf eine *Configuration Management Database* (CMDB) zu, in welchem bereits alle Systeme eingepflegt und unter anderem verantwortliche Kontaktpersonen hinterlegt wurden. Durch eine Verknüpfung der im Scanreport aufgelisteten Systeme mit den Informationen aus der CMDB, konnten über dem Service Manager Schwachstellen gezielt an Systemverantwortliche adressiert und die Bearbeitung nachverfolgt werden.

Zur Behebung der Schwachstellen wurden Gegenmaßnahmen erarbeitet, die den Systemverantwortlichen bei der Deaktivierung der Schwachstelle unterstützen sollten. Neben der Verankerung im Patch-Prozess des Kunden konnten somit auch Härtungsvorgaben angepasst werden, um das Neuauftreten von Schwachstellen von vornerein Nachhaltig zu unterbinden.

Nachdem canacoon alle Anforderungen an das Schwachstellenmanagement erfüllt hat, konnten die anfänglich bekannten Schwachstellen problemlos behoben werden. Die durch optimale Planung verfügbare Kapazität erlaubte, im Verlauf des Projekts hinzukommende Schwachstellen ebenfalls aufzunehmen und somit 120% der beauftragten Schwachstellen zu beheben.