Success Story
COMET

FFG

SBA Research

SBA2
Secure Business Austria 2
Programm: COMET – Competence Centers for Excellent Technologies
Programmlinie: K1-Zentren
COMET-Einzelprojekt, Laufzeit und Projekttyp
Systems & Software Security, 04/2014 – 03/2017, multi-firm

Data-Cube: Nessus-basierte Vulnerability-Analyse

Vulnerability-Management umfasst das wiederholte Scannen und Analysieren von gesammelten Daten und ist ein aufwendiges Unterfangen. Verschiedene Interessensgruppen verlangen unterschiedliche Ansichten von Daten. SBA Research analysierte die Anforderungen jeder Gruppe. Dabei lag der Fokus auf einer dynamischen und anpassbaren Generierung von Berichten. Unsere Software deckt die gesamte Palette ab – Scannen, Sammlung von Daten, Extract-Transform-Load (ETL) und Berichte.

Dynamisches Nessus-Reporting

Vulnerability Management umfasst die Evaluierung und Präsentation von System- und Netzwerk-Scans. Basierend auf diesen Berichten wird über weitere Maßnahmen entschieden. Nessus-Scans werden in einem bestimmten Beobachtungszeitraum automatisch und wiederholt ausgeführt. Verschiedene Interessensgruppen analysieren die gesammelten Daten, um die Qualität und Sicherheit von Systemen zu beurteilen. Nessus stellt jedoch nicht von vornherein die für alle Interessenten passenden Berichte zur Verfügung. Ein CISO z. B. benötigt kompakte Überblicke über ein System, während ein System-Administrator detaillierte Informationen braucht. Wir entwickelten eine Software, bei der Nessus-Scans von modernsten Business-Intelligence-Systemen importiert und verarbeitet werden. Sensible Daten werden zur Verfügung gestellt, wobei Sicherheit in allen Bereichen essenziell ist.

Der erste Meilenstein unserer Forschung konzentrierte sich auf das Sammeln von Daten von Nessus API. Administratoren konfigurieren Nessus-Metadaten und Datenimporte mittels einer Web-Applikation. Ein REST-client durchsucht die Berichte vom Nessus-Server und verharrt bei relevanten Informationen. Die gesammelten Daten werden in den Extract-Transform-Load (ETL) eingespeist und in einem Data-Cube gespeichert.

Benutzer erhalten die Cube-Daten via Excel Power Pivot. Sie haben volle Flexibilität und können eigene Berichte und Gesamtsummen erstellen. Zusätzlich stellen wir Vorlagen für häufige Anwendungsfälle zur Verfügung. Der Cube ist flexibel genug, um einzelne Nessus-Scans zu analysieren oder über einen Zeitraum zu vergleichen, um die Entwicklung der Systemqualität zu beobachten. Zukünftig wären u.a. automatische, Benutzer-konfigurierte Alarmierung bei Ereignissen und die musterbasierte Suche zu erforschen.

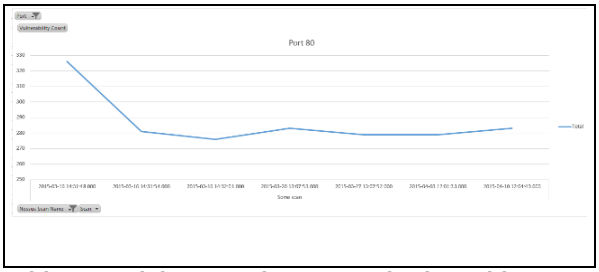

Abb. 1: Bericht, generiert von Cube (Anzahl von Port-80-Vulnerabilities im Zeitverlauf)

bmwfw Federal Ministry of Science, Research and Economy

bmvit Austrian Ministry for Transport, Innovation and Technology

Wirkungen und Effekte

Die entwickelte Software bietet eine flexible Applikation für Nessus-Reporting, die in der Lage ist, unterschiedliche Interessensgruppen zu bedienen. Der hauptsächliche Vorteil ist die Analyse von Daten mit Informationen, die anhand geschäftlicher Anforderungen gefiltert wurden. Ein weiterer Nutzen ist die zentrale Speicherung von zugeordneten Nessus-Berichten, die andernfalls über zahlreichen Nessus-Instanzen und Accounts verteilt wären.

Kontakt und Informationen
K1-Zentrum SBA2

SBA Research gGmbH
Favoritenstr. 16, 1040 Wien
T +43 1 505 36 88
E mklemen@sba-research.org, www.sba-research.org

Projektkoordination
Mag. Markus Klemen

Projektpartner

Organisation	Land
Anovis it-services and trading GmbH	Österreich
ISCP GmbH	Österreich
Raiffeisen Informatik GmbH	Österreich
SEC Consult Unternehmensberatung GmbH	Österreich