Konzeptionelle Implementierung und Evaluation eines innerbetrieblichen Vulnerability Assessment Systems

Thema:
: Konzeptionelle Implementierung und Evaluation eines innerbetrieblichen Vulnerability Assessment Systems

Art:
: BA

Betreuer:
: Christian Wolff

Student:
: David Halbhuber

Professor:
: Christian Wolff

Status:
: in Bearbeitung

Stichworte:
: OpenVAS, IT-Security, Penetration Testing, Nexis GmbH

angelegt:
: 2018-08-20

Antrittsvortrag:
: 2018-10-29

Hintergrund

Informationstechnologie spielt heute in nahezu allen industriellen Bereichen eine zentrale Rolle und ist aus dem geschäftlichen Alltag nicht mehr weg zu denken. Un-abhängig von Geschäftsfeld (Tätigkeitsfeld) und Unternehmensgröße werden immer mehr Prozesse und Abläufe digitalisiert und in IT-Systeme eingebettet. Die Notwen-digkeit diese Systeme vor unbefugten Zugriffen abzuschirmen wird durch die stei-gende Digitalisierung immer präsenter. Der Schutz der unternehmenseigenen Werte, zu diesen zählen etwa Know-how, Kundendaten und Personaldaten, ist dabei als oberste Prämisse zu verstehen. Der Kontrollverlust über diese Daten kann für Un-ternehmen jeder Größe einen erheblichen wirtschaftlichen und reputativen Schaden verursachen. Neben herkömmlichen Schutzmaßnamen wie etwa Virenscanner, Firewall und moderierten Netzwerken, bieten Vulnerability Assessment Systeme eine aktive Möglichkeit die IT-Infrastruktur eines Unternehmens auf Schwachstellen zu untersuchen. Dabei wird das Untersuchungsobjekt anhand von bekannten An-griffsmustern und -methoden penetriert. Die so exponierten Schwachstellen können anschließend in einer Risikobewertung kategorisiert und von den Verantwortlichen behoben werden, um so den Zugriffsschutz eines Netzwerkes zu gewährleisten oder wiederherzustellen. Ziel dieser Arbeit ist es, ein Schwachstellen Analyse System auf Grundlage der Leitfäden des Bundesamts für Sicherheit zu implementieren. Das entwickelte Testszenario basiert auf der, vom BSI empfohlenen, OpenVAS-Technologie. Parallel soll der gesamte Prozess der Konzeption und Implementierung entsprechend dokumentiert werden. Anschließend soll der gesamte Prozess evaluiert werden, dabei soll Augenmerk auf die Machbarkeit des Einsatzes von OpenVAS für kleine bis mittlere Unternehmen und

Unternehmen ohne eigene IT-Abteilung gelegt werden. Abschließend soll, auf Grundlage des bisherigen Prozesses, eine Methodik und Empfehlung zum Einsatz von Vulnerability Assessment Systeme in KMUs erar-beitet werden.

Zielsetzung der Arbeit

Ziel der Arbeit ist es, ein Vulnerability Assessment Systeme auf Grundlage des Leitfadens des Bundesamts für Sicherheit zu implementieren. Das entwickelte Testszenario basiert auf der, vom BSI empfohlenen, OpenVAS-Technologie. Dabei soll der gesamte Prozess der Konzeption und Implementierung entsprechend dokumentiert werden. Anschließend soll der gesamte Prozess evaluiert werden, dabei soll Augenmerk auf die Machbarkeit eines solchen Sicherheitskonzepts für kleine bis mittlere Unternehmen und Unternehmen ohne eigene IT-Abteilung gelegt werden. Abschließend soll, auf Grundlage des bisherigen Prozesses, eine Methodik und Empfehlung zum Einsatz von Vulnerability Assessment Systeme in KMUs erarbeitet werden.

Konkrete Aufgaben

- Einarbeitung in Themen der IT-Sicherheit (Allgemein)
- Einarbeitung in VAS(Allgemein)
- Einarbeitung in VAS (OpenVas, detailiert)
- Konzeptionierung OpenVas Einsatz
- Implementierung OpenVas
- Schwachstellen Analyse OpenVAS
- Evaluation der Schwachstellen Analyse
- Evaluation des gesamten Prozesses (Konzeption, Implementierung)
- Ausarbeitung einer Empfehlung und Methodik zum Einsatz von Schwachstellen Analyse auf Basis der OpenVAS-Technologie für KMUs
- Schriftliche Ausarbeitung

Erwartete Vorkenntnisse

- Netzwerktechniken (OSI,TCP,IP,usw.)
- Linux-Server (Kali)
- Allgemeine Konzepte der IT-Sicherheit

Weiterführende Quellen

- Claudia Eckert (2014): IT-Sicherheit - Konzeption, Verfahren, Protokolle
- Open Web Application Security Projekt: https://www.owasp.org/index.php/Main_Page
- Open Vulnerability Assesment System: http://www.openvas.org/index.de.html
- Bundesamt für Sicherheit in der Informationstechnik, OpenVAS: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Tools/OpenVAS/OpenVAS.html
- Budesamt für Sicherheit in der Informationstechnik, Leitfaden PenTest: https://www.bis.bund.de/ContentBSI/Publikationen/pentest/index_htm.html
- Ross Anderson (2001): Security Engineering