Konzeption, Implementierung und Evaluation eines innerbetrieblichen Vulnerability Assessment Systems

Thema:
: Konzeption, 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

Hintergrund

Informationstechnologie spielt heute in nahezu allen Bereichen eine zentrale Rolle. Unabhängig von Geschäftsfeld und Unternehmensgröße werden immer mehr Prozesse und Abläufe digitalisiert und in IT-Systeme eingebettet. Die Notwendigkeit diese Systeme vor unbefugten Zugriffen zu schützen wird durch die steigende 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 Unternehmen jeder Größe einen erheblichen wirtschaftlichen Schaden verursachen. Neben herkömmlichen Schutzmaßnamen wie etwa Virenscanner, Firewall und moderierten Netzwerken, bieten Penetrationstest eine weitere Möglichkeit die IT-Infrastruktur eines Unternehmens auf Schwachstellen zu untersuchen. Dabei wird das Untersuchungsobjekt anhand von bekannten Angriffsmustern und -methoden penetriert. Die so exponierten Schwachstellen können anschließend in einer Riskobewertung kategorisiert und von den Verantwortlichen behoben werden, um so den Zugriffsschutz einens Netzwerkes zu gewährleisten oder wiederherzustellen. In dieser Arbeit soll, anhand des Leitfadens zum Einsatz von Penetrationstests des Bundesamtes für Sicherheit in der Informationstechnik, auf Basis der OpenVAS-Technologie, eine Methodik zur Implementierung von Penetrationstests in der IT-Sicherheitsstruktur von KMUs entstehen.

Zielsetzung der Arbeit

Ziel der Arbeit ist es, ein Whitebox-Penetationstest 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 Penetrationstests in KMUs erarbeitet werden.

Konkrete Aufgaben

- Einarbeitung in Themen der IT-Sicherheit (Allgemein)
- Einarbeitung in VAS(Allgemein)
- Einarbeitung in Penetrationstest (OpenVas, detailiert)
- Konzeptionierung OpenVas Einsatz
- Implementierung OpenVas
- Penetrationstest (Whitebox-Ansatz) OpenVas
- Evualation des Penetrationstests
- Evaualtion des gesamten Prozesses (Konzeption, Implementierung)
- Ausarbeitung einer Empfehlung und Methodik zum Einsatz von Penetrationstests 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