Universität der Bundeswehr München

Call for Paper Innovationstage 2018
Vulidity

Vollautomatisiertes Sicherheitsassessment für Behörden-, Ämter- und Unternehmensumgebungen

Christian Siegert
Heinz Siegert
Bastian Karschat
Stefan Masuch

Die Vision von Vulidity ist es Behörden, Ämtern und Firmen jeglicher Größe endlich ein Werkzeug an die Hand zu geben, sodass diese erstmals eine Analyse ihres tatsächlichen Sicherheitsniveaus ohne IT-Sicherheitsexperten durchführen können. Dabei wurde Vulidity als Komplettpaket entwickelt, welche die wichtigsten Bereiche der IT Sicherheit für diese Umgebungen abdeckt. Dieses Komplettpaket ist ein Softwarebundle, welches auf jeder Hardware oder virtualisiert laufen kann.

1 Team

Das Team von Vulidity besteht aus sechs Experten, unter Anderem in den Bereichen IT-Sicherheit, Softwareentwicklung und Datenschutz. Darunter sind ehemalige Google Mitarbeiter, Datenschutzbeauftragte und Forensiker.

2 Intention

Die Idee hinter Vulidity war kein Gedankenblitz. Durch eine ausführliche Marktanalyse, hat sich der Bedarf an verschiedenen Modulen bzw. Tests herauskristallisiert. Während andere Produkte die Sicherheit marginal erhöhen, analysiert unsere Technologie das tatsächliche Sicherheitsniveau. Dabei prüft es nicht nur die aktuelle Infrastruktur auf Schwachstellen, sondern erkennt auch Konfigurationsfehler oder eine falsche Implementation von verschiedenen Sicherheitsprodukten und zeigt Ihnen entsprechende Lösungsvorschläge auf.

3 Technologie

Das Bundle für Behörden, Ämter und Unternehmen umfasst alle Testmodule, die nötig sind, um das Sicherheitsniveau qualitativ zu bestimmen und funktionierende Angriffsvektoren aufzuzeigen. Dabei ist der Ansatz, dass selbst unerfahrene Administratoren ohne Vorkenntnisse im IT-Sicherheitsbereich, alle Module ohne Schulung bedienen können. Aus diesem Grund sind die zwei fundamentalen Aspekte des Projekts *Automatisierung* und *Benutzerfreundlichkeit*. Dies ist einzigartig bei einem IT-Sicherheitsprodukt dieser Komplexität. Von automatisierten Social Engineering Angriffen (Phishing Mails, USB Dropping, QR Angriffe, ...) über fortgeschrittenen OSINT Analysen bis zu einer vollautomatisierten Tunneling Suite die ihre Firewall-/ IDS-Systeme ausgiebig testet. Als Programmiersprache wird Golang verwendet, welches zusammen mit anderen Konzepten (Machine Learning, Blockchain, ...) uns technologisch von anderen Projekten stark abhebt.
Aktuell befinden wir uns in der Implementationsphase. In der Zukunft werden

wir weitere Module anbieten wie z.B. ein Datenschutzmodul und eine automatisierte Forensiksuite mit Machine Learning Komponenten.

4 Anwendung

Unser Projekt ist als Hardwarebundle oder virtuelles Image zu erhalten. Social Engineering, und im Speziellen Phishing Mails, gelten aktuell als größter und gefährlichster Angriffsvektor. Schulungen und Belehrungen bieten meist nur eine trügerische Sicherheit, da diese Methoden sehr ineffizient sind und bei einem Großteil der Teilnehmer schon nach Verlassen des Unterrichtsraums die Themen wieder vergessen sind. Wir benutzen eine Kombination aus psychologischen Faktoren, welche Soldaten und Mitarbeiter nachhaltig in vorgefertigten oder selbst erstellten Szenarien schulen. Eine mögliche Anwendung ist, dass jede Kaserne bzw. Dienststelle einmal im Monat bei zufälligen Soldaten einen Social Engineering Test durchführt. Durch die enorme Benutzerfreundlichkeit von Vulidity können diese Szenarien sogar von ungeschulten und unerfahrenen Administratoren durchgeführt werden, die keine Erfahrungen oder Kenntnisse in der IT-Sicherheit vorweisen können, ebenso aber auch von Administratoren mit Kernpunkt IT-Sicherheit. Das Ergebnis sind Soldaten, die nachhaltig IT-Sicherheitsbewusstsein aufgebaut haben, damit der größte Angriffsvektor der heutigen Zeit in der Bundeswehr professionell abgesichert ist.