DDoS – Phishing – Verwundbarkeitstest

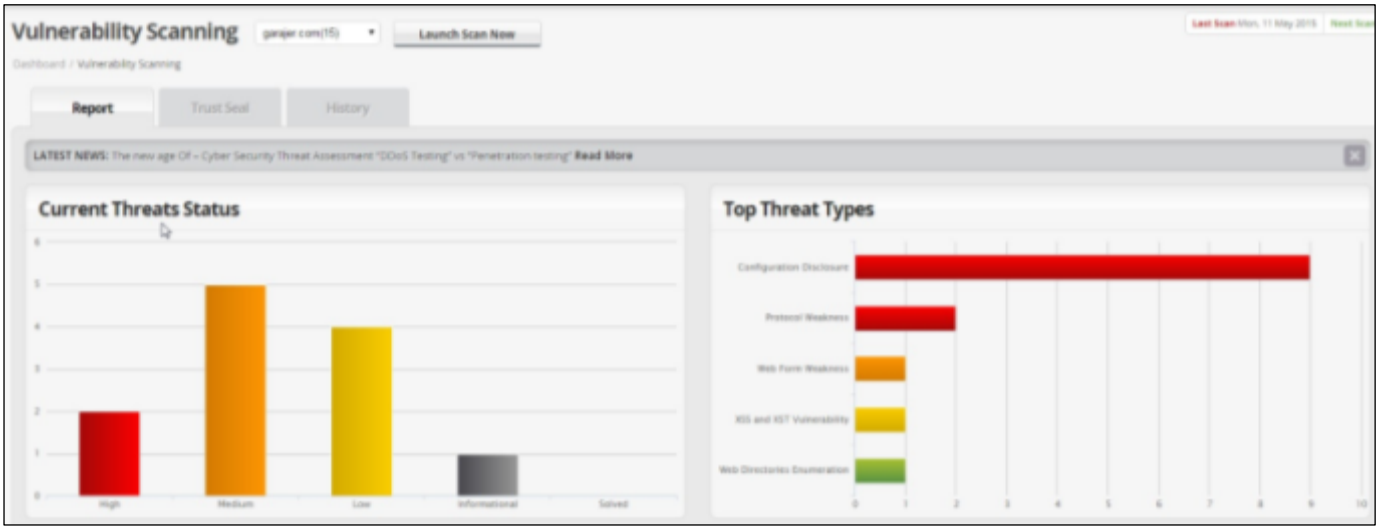
Die IT Infrastruktur ihrer Firma, die mit Kunden, Zulieferer und anderen Niederlassungen kommuniziert, muß vor äußeren Angriffen geschützt werden. Mit den Modulen Distributed Denial of Service (DDoS), Phishing Simulation und Verwundbarkeitstest haben sie die Möglichkeit gezielt und geplant Angriffe zu simulieren und die Schwachstellen in ihrer Infrastruktur aufzudecken und anzuzeigen.

Zentrales Dashboard

- Überblick über Ergebnisse aus allen Modulen
- Direkter Zugriff auf sämtliche Detailinformationen
- Steuerung der Prozesse

Vulnerability Scanning

- Kostenloser erster Scan über: https://mazebolt.com/sign-up
- Scan auf Komponenten Ebene unter Einbeziehung der Vernetzungen/Verbindungen untereinander
- Neue umfassende und intelligente, patentierte Scan Algorithmen zum Auffinden von Sicherheitslücken
- Priorisierung von Angriffszenarien für eine schnelle Behebung nach Dringlichkeit
- Transfer der gewonnen Informationen über Sicherheitslücken in die Optimierung ihrer Arbeitsprozesse



Art der Verwundbarkeit	Details
Injections & File Inclusions	SQL injections, RFI, LFI
Bekannte Verwundbarkeiten	Die aktuellen Verwundbarkeiten von Apache, IIS, FTP, SSH etc. die die gesamte Serverlandschaft angreifen und ausschalten könnte
Cross Site Scripting	XSS und XST, CSRF
Protokoll Schwachstellen	SSL Schwachstellen und nicht abgesicherte HTTP Klassen
WordPress Schwachstellen	Verwundbare plug-in's
Web Verzeichnis Auflistungen	Beschreibbare Webverzeichnisse
Konfigurationsprobleme	Unerlaubte Zugriffe auf Sicherungskopien, Passwörtern, Installationsjournale (log files) etc.
Malware Entdeckung	C99, R57 und andere Shellcodes die die IT-Infrastruktur gefährden

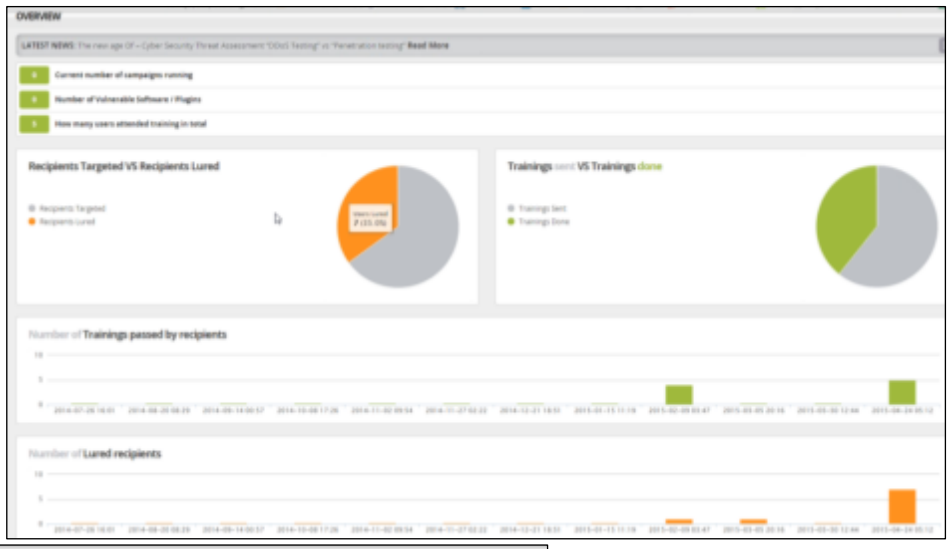
DDoS – Phishing – Verwundbarkeitstest

Asset Monitoring

- Übersicht der Netzwerk Leistung nach Standort
- Permanente Aktualisierung
- Detailansicht auf der Zeitachse über einfache Anwahl des Standortes

Phishing Simulation

- Zentrale Schaltstelle und Dashboard
- Aufsetzen von internen und externen e-mails (Senders) für eine Gruppe von Empfängern (Recipients)
- Einfaches Aufsetzen und Nutzen von selbst erzeugten Internet Domainen wie z.B. www.deutschebank-service.de
- Kopieren von existierenden Internetseiten und Änderen der darauf existierenden URL's (Webadressen)
- Prozess: Starten der Phishing Kamapagne –> Training der Anwender –> fortlaufende Kontrolle



DDoS – Phishing – Verwundbarkeitstest

DDoS – Distributed Denial of Service

- Gezieltes und kontrollierts Ausschalten ihrer IT Infrastruktur durch Angriffe von Außen (Cyber Attacks)
- PoC mit einer 3 Studen Baseline DDoS Attacke (SYN, ACK, RST, FIN + ACK, ASP + ACK, UDP Garbage flood, DNS Request Flood) mit Abschlußreport und Übersicht über alle gefundenen Sicherheitslücken
- Israelisches Team mit langjährigen kommerziellen DDoS Angriffs- und Verteidigungserfahrungen (z.B. RedWare)

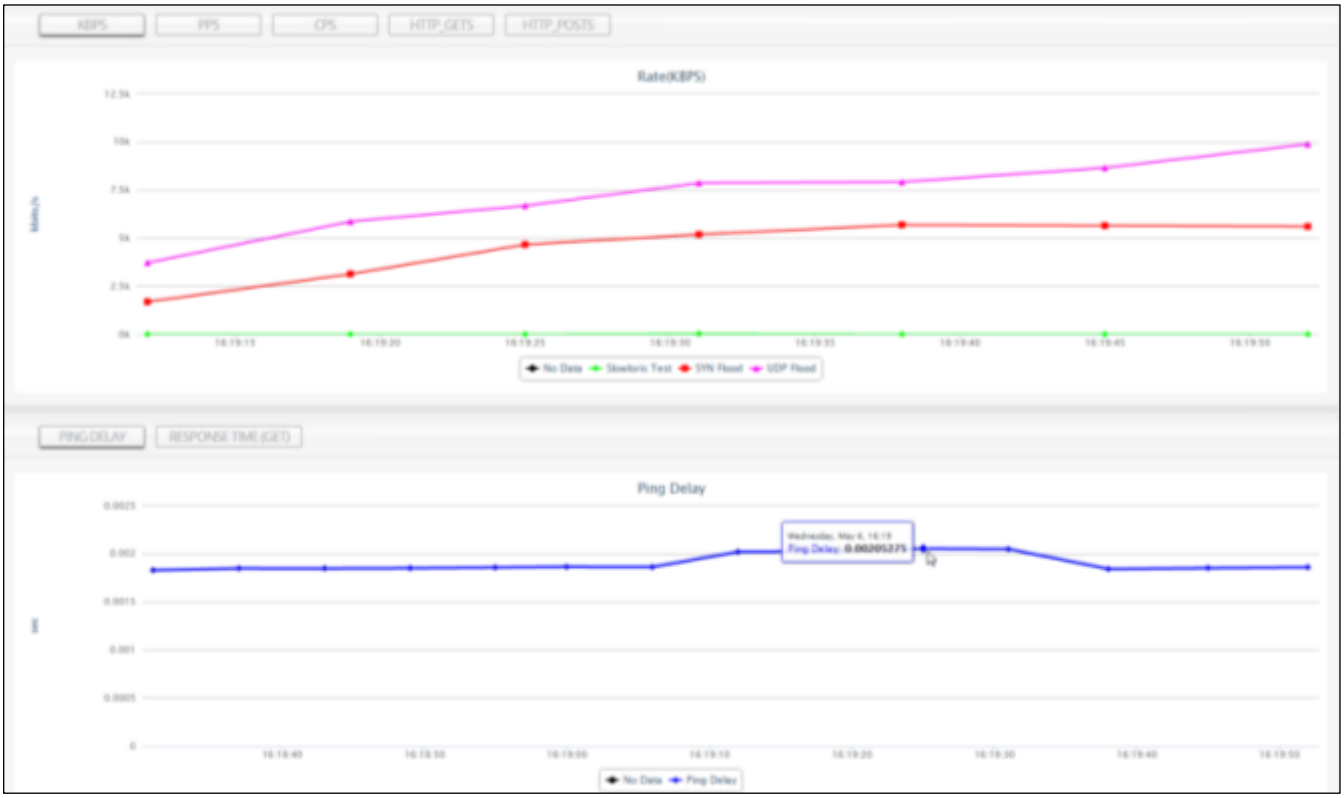
Probleme

- Nicht verifizierte Annahmen über den Sicherheitsschutz des gesamten IT-Systems
- Die Prozesse mit Attacken umzugehen sind nicht definiert oder vorhanden
- Das System ist falsch oder unzureichend konfiguriert
- Es ist keine DDoS Sicherung installiert
- Es gibt neue Arten von Angriffen

Testverfahren

- Test mit 18 verschiedenen Angriffstypen auf der Applikation-/Serviceschicht oder über Massenanfragen an oder im Netzwerk
- **APT** (Advanced Persistent Threat) Test: Angriff durch „White Hat Hackers“ - Kann der Service und die Sicherheit bei Attacken aufrecht erhalten bleiben:
  - Kundenangepasste Angriffsszenarien
  - Andauernde Angriffssimulation
  - Verstärkte Analyse der L4 und L7 Schwachstellen
  - Strategie zur Schwachstellenbehebung
  - Verbesserungen der erweiterten Notfall Reaktionsprozesse
  - Bestätigung der Abwehrmechanismen der L7 Herausforderungen

Tests	Test Details
Level 3 Attacken	• ICMP Flood Type 8 • ICMP Flood Type 1
Level 4 Attacken	• SYN • ACK • RST • FIN + ACK • ASP + ACK • UDP Garbage flood • DNS Request Flood
Level 7Attacken	• HTTP Flood - Single links • HTTP Flood - Dynamic links • HTTP Range • Brobot simulation • Slowloris • SSL Renegotiation



DDoS – Phishing – Verwundbarkeitstest

Ergebnis

- Report und Verbesserungsvorschläge um die IT-Infrastruktur zu härten
- DDoS sollte integraler Bestandteil der Bedrohungsabwehr sein