

Case Study: Penetrationstests für ein namhaftes deutsches Unternehmen

Branche

Versicherungen

Projekthalt

Ziel des Projektes war eine detaillierte Sicherheitsanalyse der aus dem Internet erreichbaren Systeme eines namhaften deutschen Unternehmens. Die Untersuchungen erfolgten aus Sicht eines externen Angreifers in Form eines „Zero-Knowledge“ Ansatz. Es sollten potentielle Schwachstellen aufgedeckt, anhand einer Risikoanalyse bewertet und entsprechende Gegenmaßnahmen aufgezeigt werden.

Die Durchführung des Penetrationstests geschah unter Zuhilfenahme von öffentlich verfügbaren Tools und Informationen sowie selbstentwickelten Werkzeugen und Exploits.

Das Projekt umfasste insbesondere folgende Aktivitäten:

- ▶ Infrastruktur-Aufklärung (Netzstruktur, Server, Systeme, Dienste, Applikationen)
- ▶ Analyse von Web-, Mail- und DNS-Servern sowie VPN-Gateways
- ▶ Untersuchung der eingesetzten Verfahren zur Authentifizierung, Verschlüsselung und Sessionmanagement von Web-Applikationen
- ▶ Exploiting von Schwachstellen
- ▶ Brute-Force Angriffe
- ▶ Denial of Service Angriffe
- ▶ Detaillierte Ergebnisberichte inkl. Schwachstellenbewertung, Risikoanalyse und Handlungsempfehlungen

Während der Sicherheitsanalyse konnten einige, zum Teil kritische Schwachstellen aufgedeckt und in enger Zusammenarbeit mit dem Auftraggeber schnell behoben werden. Anhand der erstellten Risikoanalyse wurden für die einzelnen Schwachstellen konkrete Handlungsempfehlungen in Anlehnung an Security Best Practices und internationale Standards erarbeitet.

Zeitraumen und Aufwand

Der Zeitrahmen für dieses Projekt war auf 2 Wochen ausgelegt. Einige der Aktivitäten wurden explizit außerhalb der allgemeinen Arbeitszeiten des Auftraggebers durchgeführt, um mögliche Beeinträchtigungen des laufenden Betriebs zu vermeiden.

Eingesetzte Techniken

- ▶ Port- und Schwachstellenscans
- ▶ Service-Detection und Fingerprinting
- ▶ SQL- und XML-Injection
- ▶ Cross-Site Scripting (XSS)
- ▶ Exploiting
- ▶ DoS- und Brute-Force-Angriffe

Fazit

Auf Grundlage der genauen Sicherheitsanalyse und -bewertung konnten eine Reihe von Schwachstellen identifiziert und anhand der entwickelten Handlungsempfehlungen zügig behoben werden. Der Penetrationstest hat damit

unmittelbar dazu beigetragen, das Sicherheitsniveau der Infrastruktur und deren Komponenten deutlich zu erhöhen.