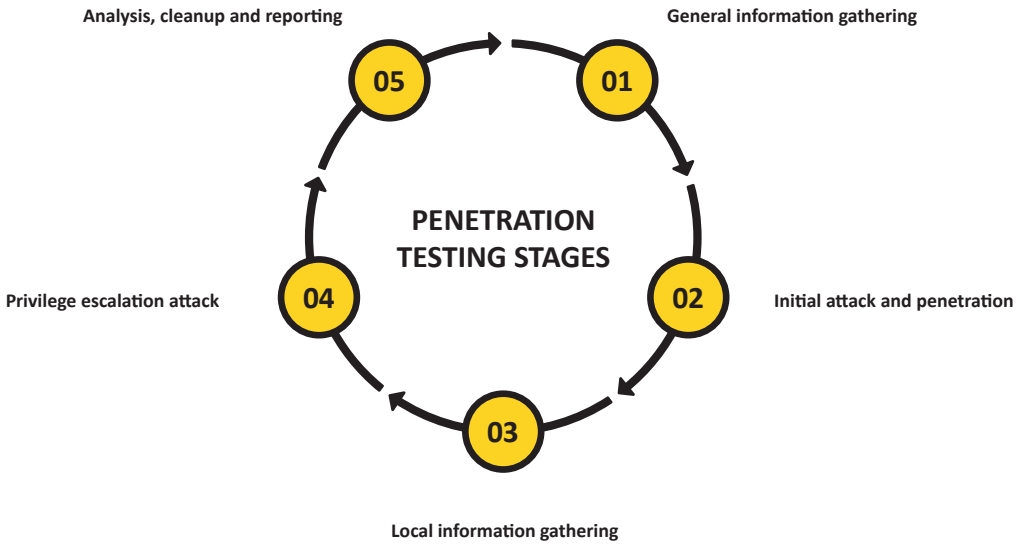
Penetration Test as a Service: Ihre Verteidigung unter Dauerstress.

Ständige Angriffe durch Viren halten unser Immunsystem auf Trab. Nach diesem Muster funktioniert unser Service ‘Penetration Test’. Wir setzen Ihre Verteidigung einem Dauerstress aus. Kennen Sie jeden Dienst, der in Ihrem Netzwerk läuft? Haben Sie die Kontrolle über jede Anwendung, zum Beispiel ERP und Webdienste? Können Sie mit Sicherheit sagen, dass diese nicht anfällig sind? Lassen Sie uns Ihre Schwächen aufdecken und warten Sie nicht, bis es ein Angreifer tut.

Erst simulierte Angriffe offenbaren, ob Ihr Sicherheitsdispositiv den Anforderungen genügt. Automatisierte und vor allem kontinuierliche Penetration-Tests, die über eine Software-as-a-Service (SaaS)-Plattform durchgeführt werden, liefern in Echtzeit wertvolle Daten. Damit haben Sie die Informationen, um Ihre Abwehr immer wieder zu stärken.



Wir können Angriffe innerhalb des Netzwerks simulieren. Unsere Spezialisten sind in der Lage, einen Ransomware-Angriff vorzutäuschen. Damit trainieren wir Ihr Unternehmen, wie man richtig darauf reagiert.

Erkennen Sie Ihre Schwachstellen, bevor es jemand anderes tut. Erfahren Sie, welche Informationen aufgrund Ihrer Dienste für jedermann zugänglich sind. Verbessern Sie Ihre Sicherheitsstrategie mit unseren Tipps basierend auf Testergebnissen.

Wie Penetration Test as a Service aufgebaut ist

Penetration Test as a Service von UMB gibt es in zwei Modulen. Diese Module können einzeln oder kombiniert bezogen werden:
- Internes Scanning & Testing: In einem definierten Netzwerk
- Externes Scanning & Testing: Vom Web aus (Web-Applikationen, SaaS-Services, etc.)

Innerhalb dieser Module werden gemeinsam mit dem Kunden verschiedene Tests definiert. Diese Tests werden entweder als Whitebox-, Greybox- oder Blackbox-Test durchgeführt.

Whitebox:
- Die Infrastruktur ist bekannt, User und Password vorhanden, normalerweise Admin Account
- Bei kundenspezifischen Webapplikationen ist der Source-Code verfügbar

Greybox:
- Die Infrastruktur ist nicht bekannt aber das Target ist klar und definiert, User und Password ohne Admin-Credentials vorhanden
- Allgemeine Informationen vorhanden (high level)

Blackbox:
- Nur Public oder Private IP / Domain Name sind bekannt
- Kein User / Password

Ihre Vorteile

- Sie schützen Ihre Infrastruktur, Ihre Geräte und Ihre Benutzer
- Sie legen Richtlinien und Verfahren zum Schutz Ihres Unternehmens fest
- Unser Service ist modular und flexibel
- Automatisiertes, kontinuierliches Testen der definierten Infrastruktur

Servicebestandteile

- Kontinuierliches Testing gemäss definiertem Testszenario (Whitebox, Greybox, Blackbox)
- Interpretation, Analyse & Priorisierung von Schwachstellen
- Bei kritischen Schwachstellen sofortige Meldung an den Kunden
- Umfassender, monatlicher Servicebericht mit konkreten Handlungsempfehlungen

Rundum sicher fühlen? Kontaktieren Sie uns!

Gerne beantworten wir Ihre Fragen zum Penetration Test as a Service

Kontakt

Markus Kaegi
Team Leader Strategic Sales Consulting
markus.kaegi@umb.ch
+41 58 510 16 98
www.umb.ch/security