POSSEHL. SECURE

MANAGED SERVICE / IDENTIFY

PENTESTING

HABEN WIR SCHWACHSTELLEN IN UNSERER IT-LANDSCHAFT?

Die Probe aufs Exempel für Ihre IT-Sicherheitslandschaft

Unsere Experten prüfen ihr Unternehmen auf Schwachstellen. Teils mit denselben Tools, Taktiken und Prozeduren wie reale Angreifer, teils mittels strategischer Prüfung und Beratung. Aufgrund unserer langjährigen Erfahrung und Kompetenz auf den Gebieten der offensiven und defensiven Sicherheit bieten wir Ihnen maßgeschneiderte Empfehlungen und Lösungen zur Identifizierung und Minimierung Ihrer Angriffsfläche.

Durch einen Pentest erhalten Sie eine detaillierte Übersicht ihrer Schwachstellen (u.a. zu Software, Konfiguration und Design) und dazu praxiserprobte Empfehlungen zu geeigneten Gegenmaßnahmen.

Die 3 Testmethoden

	AUSGANGSBASIS	ZUGANGSEBENE
BLACK-BOX	Die realistischste Simulation eines Cyberangriffs durch unbekannte Angreifer.	Kein Zugang und keine internen Informationen werden zur Verfügung gestellt.
GREY-BOX	Es wird ein gewisses Maß an internem Zugang und Wissen gewährt. Dadurch erhöht sich die Effizienz.	Hintergrundinformationen wie bspw. IP-Bereiche, Domain-Namen, Identitäten werden vorab übergeben.
WHITE-BOX	Es wird ein Angriff simuliert, bei dem der Angreifer Zugang zu Unternehmensinterna hat (bspw. einen Account).	Vollumfänglicher Zugang zu Anwendungen und Systemen. Ggf. auch Source Code.

Was kann getestet werden?

INFRASTRUKTUR

- Interne IT-Infrastrukturen – Server, Intranet, Netzwerk, WLAN
- Externe IT-Infrastruktur – Extern erreichbare Systeme
- AD Sicherheitsanlayse – Microsoft Active Directory

APPLIKATIONEN

- Quellcode
- Website, Shop, Portal
- Mobile Applikationen – Android, iOS
- API Schnittstellen – REST, SOAP

LECKAGEN (INTERNET, DEEP WEB, DARKNET)

- Passwort- Audit – Unsicher oder geleaked
- Open Source Intelligence – Identifikation von sensiblen Informationen

SZENARIO TESTS

- Evil Employee – Mitarbeiter, Praktikant, Gäste
- Stolen Asset – Verlust oder Diebstahl (Notebook, Smartphone, …)

Warum Pentesting?

Pentesting ist ein stetiger Kreislauf, der ein Unternehmen begleitet. Denn was dieses Jahr noch geschützt hat, kann nächstes Jahr schon eine Schwachstelle sein. Die stetige Entwicklung im Sicherheitsbereich erfordert eine wiederkehrende Überprüfung der IT Systemlandschaft.

Zudem der Faktor „Mensch“ eine der größten Sicherheitslücken darstellt. Weiter erhalten Sie mehr Klarheit über die Sicherheit Ihres Unternehmens im Falle eines Angriffes. Anforderungen für eine Zertifizierung werden erfüllt, wie zum Beispiel ISO 27001.

Durch den Pentest ist eine detaillierte Abbildung der digitalen Angriffsfläche möglich und somit kann gezielt die IT-Sicherheit verbessert werden. Das Ergebnis kann als Investitionsentscheidungsgrundlage dienen, so können anhand der Ergebnisse gezielt Investitionen getätigt werden.

Pentesting Ablauf

1 KICK-OFF-GESPRÄCH

Aufnahme des Status quo, unser Team unterstützt Sie bei der Auswahl des Testes um Ziel und Umfang des Penetrationstestes individuell auf Sie abzustimmen. Wir unterstützen bei der Beschaffung der wichtigen Informationen und relevanten Dokumente.

2 RECONNAISSANCE / INTELLIGENCE GATHERING

Informationsbeschaffung, unteranderem werden sicherheitsrelevante Informationen aus frei verfügbaren offenen Quellen gesammelt (OSINT). Ziel ist ein vollständiger Überblick über die digitale Angriffsfläche.

3 VULNERABILITY ASSESSMENT

Weiter werden Portscans durchgeführt und ein Schwachstellenscan. Mögliche Schwachstellen werden noch nicht tiefergehend ausgenutzt. Es wird geprüft, ob es sich um sogenannte False-Positves handelt.

4 EXPLOITATION

Es startet der eigentliche Angriff in ihr IT-System. Die vorher identifizierten Schwachstellen werden aktiv genutzt um in das System einzudringen und an unterschiedliche Daten zu gelangen. Es werden je nach Absprache kritische Schwachstellen ausgenutzt, Exploits die schon vorhanden sind werden genutzt oder angepasst, um diese dann einzusetzen.

5 POST-EXPLOITATION

In dieser (optionalen) Phase erfolgt der tiefere und breitere Zugang zu Ihrer Unternehmung. Unsere Experten persistieren Ihre Zugänge und bewegen sich lateral, um weiter Systeme auszukundschaften und zu kompromittieren.

6 REPORT / DOKUMENTATION

Im Ergebnisbericht werden die gefunden Schwachstellen entsprechend des Risikos klassifiziert, sowie eine Maßnahmenkatalog erstellt zur Behebung der Schwachstelle. Der Ergebnisbericht wird ihnen, nach der Ergebniskonferenz, inklusive eines Management Summary zur Verfügung gestellt.

Possehl Secure GmbH
info@possehl-secure.de | T +49 221 466 195-20

www.possehl-secure.de

POSSEHL. SECURE