SHD.
WIR BEWEGEN IT.



IT-Sicherheit

SHD Penetration Test

Hält Ihr Unternehmen einem Hackerangriff stand?

Durch die zunehmende Professionalisierung von Phishing-Angriffen ist es nur eine Frage der Zeit, bis ein potenzieller Angreifer Zugriff auf ein Endgerät hat und sich somit in Ihrem internen Netzwerk befindet.

Auch die extern verfügbaren Informationen und erreichbaren Dienste stehen an vorderster Front, wenn es Cyberkriminelle auf Ihre IT-Infrastruktur abgesehen haben.



Unsere Lösung:

Die individualisierten Penetrationstests (Pentests) von SHD sind ein ideales Mittel, um Ihr IT-Sicherheitsniveau nachhaltig zu erhöhen. Unsere simulierten Cyberattacken spüren gezielt technische Sicherheitslücken in Ihrem Unternehmen auf und leiten konkrete Maßnahmen für Sie ab.

Ob das Identifizieren potenzieller Angriffspunkte in Ihrer DMZ-Infrastruktur, das Überprüfen des Active Directory oder eine Analyse Ihrer entwickelten Webapplikationen: Im gemeinsamen Austausch mit unseren qualifizierten Penetration Testern finden wir definitiv die passenden Ansatzpunkte zum Ausbau Ihrer IT-Sicherheit.

Auf Wunsch sind auch simulierte Phishing-Angriffe zum Testen Ihrer E-Mail-Security möglich.

Ihre Vorteile:

- Aufgedeckte Sicherheitslücken in realistischen Szenarien
- Konkrete Handlungsempfehlungen und Verbesserungsvorschläge für Ihr Unternehmen
- Verständliche Lösungen, die zu Ihren angestrebten Schutzzielen und verfügbaren Ressourcen passen
- Unterstützung durch zertifizierte Experten (u.a. OSCP, CRTO, OSWP, CEH, ECSA)

OffSec OSCP

OffSec OSWP

EC-Council ECSA CERTIFIED

EC-Council CEH CERTIFIED

CISSP® Certified Information Systems Security Professional

Angriffspunkt #1: Active Directory

Der initiale Zugriff auf Ihr Unternehmensnetzwerk erfolgt oft durch die zielgerichtete Zustellung schadhafter E-Mails in Verbindung mit der Aufforderung, ausführbare Inhalte zu aktivieren (z.B. Macros oder Javascript-Dateien).

Um die Auswirkung einer auf diesem Wege kompromittierten Unternehmensentität zu erkennen, ist eine Tiefenanalyse des Active Directory notwendig. Das Ziel ist, Lücken im Berechtigungskonzept zu finden oder Fehlkonfigurationen und schwache Kennworte aufzuspüren, welche zur Ausdehnung der eigenen Rechte genutzt werden können. Dies trägt in Verbindung mit der Betrachtung Ihrer etablierten Schutzmaßnahmen, wie der Endpoint Protection oder der Firewall, zur ganzheitlichen Analyse Ihrer IT-Sicherheit bei. Im Rahmen des Pentests prüfen wir unter anderem folgende Punkte:

- AD-Berechtigungen
- Schwache Zugangsdaten
- Administrative Konten
- Prüfung der Endpoint Protection
- Offene Dateifreigaben
- Vorhandene Konfigurationen im Windows-Umfeld
- Wege zur Rechteeskalation

Ergebnis: Empfehlung von Härtungsmaßnahmen für Ihre AD-Umgebung



Angriffspunkt #2: Externe Ressourcen

Aus dem Internet erreichbare Assets sollten einer regelmäßigen Sicherheitsüberprüfung unterzogen werden, um etwaige Schwachstellen zu identifizieren. Unser Penetrationstest konzentriert sich unter anderem auf folgende Angriffspunkte:

- Zugänge zu internen Ressourcen / Remote-Zugriff
- Exponierte Dienste (z.B. Ticketsysteme, Webportale)
- Selbst entwickelte Lösungen (Prüfung nach OWASP Top 10)
- Verwendete Software-Versionen
- Mailgateway (z.B. SPF-Record, Dateianhänge)
- Web-Applikationen

Ergebnis: Darstellung der externen Angriffsfläche inkl. Verbesserungsvorschläge

Angriffspunkt #3: (W)LAN-Infrastruktur

Ein (W)LAN-Penetrationstest bewertet die Resilienz Ihrer Netzwerkinfrastruktur gegenüber dem unautorisierten Zugriff mit fremden Geräten. Dabei wird untersucht, ob ein Angreifer mithilfe eines unbekannten Endgeräts in Ihr Unternehmensnetzwerk eindringen kann oder ob schwache Zugangsdaten über drahtlose Verbindungen abgegriffen werden können. Weiterhin werden die eingesetzten Protokolle und deren Konfiguration überprüft.

Im Fokus stehen dabei unteranderem folgende Punkte:

- Unautorisierter Netzwerkzugriff
- Schwachstellen in WLAN-Protokollen
- (W)LAN-Profile auf Endgeräten
- 802.1X Konfiguration
- Ethernet-Anschlüsse

Ergebnis: Aufzeigen der Möglichkeiten für den unautorisierten Netzwerkzugriff

Wir bieten Penetration Tests auch als Teil eines umfassenden IT-Security-Checks an:



> Unser IT-Security-Check liefert einen umfassenden Überblick über das interne Sicherheitsniveau. Da wir unseren empfohlenen Maßnahmen-Fahrplan auf die Ihnen zur Verfügung stehenden Ressourcen abstimmen, bauen wir keine unrealistischen IT-Luftschlösser. Ganz im Gegenteil: Die gemeinsam abgestimmten Prioritäten helfen bei der Planung und schnellen Umsetzung.



Ihr Security-Experte

Christian Müller · Principal Technology Consultant

Jetzt Pentest oder Beratung vereinbaren:

kontakt@shd-online.de +49 (0)351 42 32 151

CISSP CCSP ECSA EC-Council Certified Security Analyst CHFI Computer Hacking Forensic Investigator

SHD. WIR BEWEGEN IT.

www.shd-online.de

ISO 9001 zertifiziert www.isocert.de TÜV SÜD ISO/IEC 27001

SHD System-Haus-Dresden GmbH
Zertifiziert nach ISO 9001 und ISO 27001

INDIVIDUELLE BERATUNG, PROJEKTARBEIT UND SERVICES RUND UM:

- IT-Infrastruktur & Cloud
- IT-Sicherheit
- Prozessmanagement & KI

400-2.5-12.TFR