PENTESTS

Auf dem Weg zur sicheren IT-Infrastruktur

Warum Penetrationstests?

Pentests dienen dazu Ihre IT-Infrastruktur und -Systeme einer umfassenden Prüfung zu unterziehen. Damit stellen Sie fest, wie empfindlich Ihre Infrastruktur gegenüber Angriffen von Hackern ist. Bei einem Pentest wird ein gefakter Angriff auf Ihre Systeme durchgeführt. Dabei kommen Methoden und Techniken zum Einsatz, die auch von echten Angreifern oder Hackern verwendet werden.

Sie betreiben eine eigene IT-Infrastruktur?
Eine komplexe Aufgabe, die permanente Pflege erfordert.

Beinahe täglich werden neue Schwachstellen von Betriebssystemen und Applikationen identifiziert. Bereits eine nicht behobene Sicherheitslücke kann die Verfügbarkeit und Integrität eines gesamten Unternehmensnetzes gefährden. Dies demonstrieren Fälle wie der Sicherheitsvorfall WannaCry 2017 und aktuell der Ransomware-Ragnarok-Fall eindrücklich.

Die Assets Ihrer IT-Infrastruktur stellen für Hacker äußerst lohnende Ziele dar. Sie verfügen häufig über hohe finanzielle Mittel, Know-how und die notwendige Zeit, um die Schwachstellen Ihres Netzwerks zu identifizieren. Viele Angriffe erfolgen sogar von innerhalb des Unternehmensnetzes. Ein reiner Schutz der Netzwerkgrenze greift erheblich zu kurz.

Aktuelle Schwachstellenscanner bieten aufgrund ihrer Fokussierung auf öffentliche Schwachstellen von Betriebssystemen und Applikationen keinen umfassenden Schutz: Schwache Passwörter oder Mängel in der Konfiguration werden kaum erkannt. In zahlreichen Szenarien liefern sie zudem viele irrelevante oder falsche Ergebnisse („False Positives“).

Unser Leistungsangebot und Vorgehen

hoch-automatisierte Pentests | **Reality Check** | **Ergebnisreport** | **Lückenschließung**

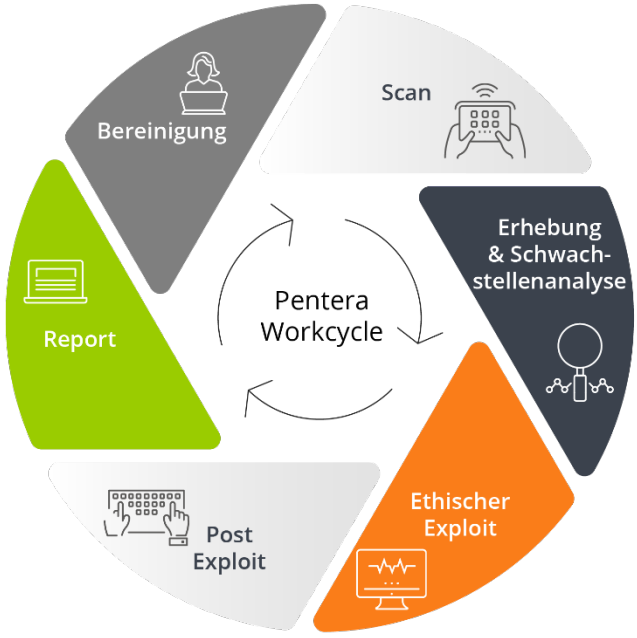
Klassische Penetrationstests bilden die Vorgehensweise realer Angreifer ab und identifizieren echte, ausnutzbare Schwachstellen in Infrastrukturen (ohne False Positives). Sie sind jedoch häufig sehr aufwendig. Ihr Vorgehen, sowie Schwerpunkte und Ergebnisse, hängen stark von den Fähigkeiten und dem Blickwinkel der Tester ab. Schwere Reproduzierbarkeit sowie nicht vorhandene Messbarkeit stellen zusätzlich ein großes Problem klassischer Penetrationstests dar.

Wesentlich einfacher und schneller zu realisieren sind hochautomatisierte Penetrationstests, die Ihnen syracom anbietet. Diese werden mit der Plattform PenTera unseres Partners Pcysys agentenlos durchgeführt. Sie müssen keine zusätzliche Software auf Ihren Geräten installieren. Im Zuge von Continuous Integration besteht die Möglichkeit eine Lizenz zu erwerben.

Unser IT-Security-Team übernimmt beim Pentest die Rolle des Hackers. Unter Zuhilfenahme von PenTera können wir eine hohe Anzahl von Angriffen durchführen, die manuell mehrere Wochen in Anspruch nehmen würden. In nur ein bis zwei Tagen liegen Ergebnisse vor. Dabei werden Ihre Systeme gezielt, mess- und reproduzierbar angegriffen.

Unser Security-Team agiert hierbei nicht nur als Angreifer, sondern auch als Ratgeber und hilft bei der Interpretation der Ergebnisse während und nach dem Penetrationstest.

Ablauf Penetration Testing



syracom führt auf Basis aktueller Hacking-Techniken ethische Exploits auf der Grundlage der Schwachstellen Ihrer Infrastruktur aus. Diese sind unabhängig von Größe und Branche durchführbar und lassen sich aufgrund ihrer automatisierten Ausführung komplett reproduzieren. Gleichzeitig behalten Sie immer den Überblick und die Kontrolle!

Im Anschluss an den ausführlichen Penetrationstest erhalten Sie zudem von uns ein aussagekräftiges Ergebnis. Auf Basis dieses Ergebnisses stellen wir Ihnen direkt einen individuellen, priorisierten Report zur Verfügung, bei dessen Umsetzung wir Sie gerne unterstützen und unabhängig beraten. Dabei stellen wir Ihnen die Menge an Abfolgen von Angriffen, die zum erfolgreichen Exploit geführt haben, mittels Angriffsvektoren dar. Anbei ein exemplarischer Auszug der Hauptergebnisse eines solchen Reports.

Top4Actions

9,8

Der Host ist anfällig auf BlueKeep (CVE-2019-0708)

Es wird empfohlen den Host für BlueKeep (CVE-2019-0708) zu patchen. Bitte klicken Sie für weitere Informationen auf folgenden Link: https://technet.microsoft.com/library/security/CVE-2019-0708

9,3

Der Host ist anfällig auf MS17-010

Es wird empfohlen den Host für diese Anfälligkeit zu patchen. Bitte klicken Sie für weitere Informationen auf folgenden Link: https://technet.microsoft.com/library/security/MS17-010

8,8

Anti Virus blockierte keine böswilligen Nutzdaten

Verstärken Sie Ihre Antiviren-Richtlinien und beobachten Sie verdächtiges Verhalten im Netzwerk.

7,8

Entschlüsselte Chrome Passwörter

Während der Durchsuchung von Webbrowsern nach Informationen kann ein Angreifer gespeicherte Anmeldedaten finden und diese dazu benutzen, die internen und externen Vermögenswerte der Organisation zu missbrauchen.

Ganzheitlicher IT-Security-Ansatz

Durch unseren ganzheitlichen Ansatz werden Sie in der Lage sein, die aktuelle Sicherheit Ihrer IT-Infrastruktur fundiert zu beurteilen und nachhaltig zu verbessern.

Dieser Ansatz wird durch weitere Lösungsbausteine unterstützt. So hilft Ihnen in diesem Zusammenhang unser Reality-Check dabei, Angriffe von außen zu verstehen und das Verhalten im Unternehmen zu prüfen. Zudem bieten wir Ihnen Audits zur Prüfung Ihrer Identity- und Access-Systeme an und beraten Sie zu Themen wie der Multifaktor-Authentisierung. All diese Methoden sind sowohl unternehmensspezifisch als auch auf die aktuelle Situation angepasst. So können wir Penetrationstests komplett remote durchführen und weitere Lösungsbausteine mit einem Minimum an physischer Präsenz realisieren.

Warum syracom?

Unser syracom IT-Security-Team bündelt fachspezifisches Know-how mit neuesten Technologien und verfügt über ein umfassendes Partnernetzwerk. Wir beraten unabhängig und verstehen uns als ganzheitliche Begleiter bei der Umsetzung.

Planen Sie noch heute mit uns individuell auf Ihr Unternehmen zugeschnittene Penetrationstests und profitieren Sie von hervorragendem Security-Know-how. Unser Vier-Säulen-Modell bestehend aus Web Application Security, Identity- und Accessmanagement, Datenschutz und Social Engineering bietet priorisierte Bausteine für die Informationssicherheit Ihres Unternehmens.

Kontaktieren Sie uns gerne

Im Zuge Ihres individuellen Angebots überzeugen wir Sie gerne bei einem Termin mittels Proof of Value von unserem Vorgehen. Kommen Sie einfach auf uns zu!

brandeins /thema 2020 Heft 15 Beste Unternehmensberater

syracom

Frank Hoffmann
Leiter Themenbereich IT-Security
syracom AG
Otto-von-Guericke-Ring 15
65205 Wiesbaden (Germany)
Fon: 06122 9176 0
frank.hoffmann@syracom.de
www.syracom.de