IT-SECURITY

Auf dem Weg zur sicheren IT-Infrastruktur

PENTESTS RICHTIG EINGESETZT

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.

syracom

SICHERHEITSLÜCKEN GEFÄHRDEN DAS GESAMTE UNTERNEHMEN

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 Qakbot oder Okta und der Ransomware-Fall der Hotelkette Motel One, bei den Millionen von Namen und Reisedaten von den Gästen abgegriffen wurden und im Netzt gelandet sind.

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 („falsch-positive Ergebnisse“).

IHR VORSPRUNG MIT SYRACOM

HOCHAUTOMATISIERTE PENTESTS

REALITYCHECK

ERGEBNIS-REPORT

LÜCKEN-SCHLIEßUNG

Klassische Penetrationstests bilden die Vorgehensweise realer Angreifer ab und identifizieren echte, ausnutzbare Schwachstellen in Infrastrukturen (ohne falsch-positive Ergebnisse). 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.

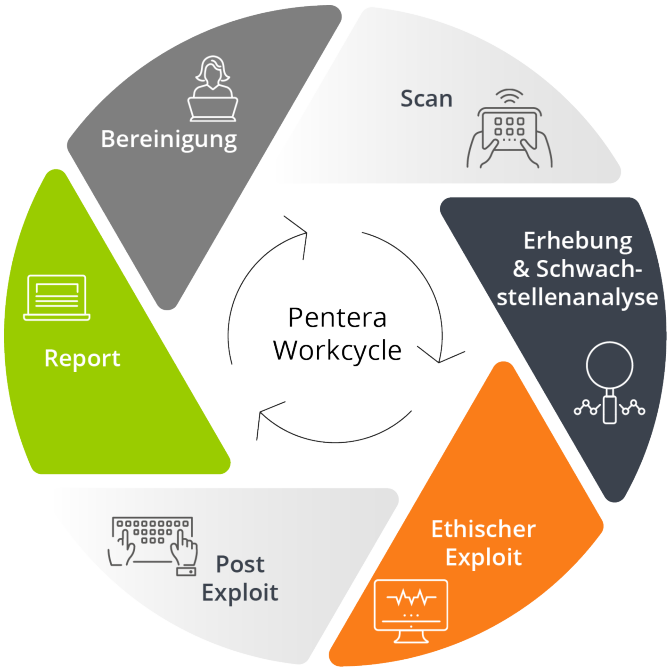
Wesentlich einfacher und schneller zu realisieren sind hochautomatisierte Penetrationstests, die Ihnen syracom anbietet. Diese werden mit der Plattform Pentera agentenlos und optional auch remote durchgeführt. Sie müssen keine zusätzliche Software auf Ihren Geräten installieren. Wir führen diese entweder as a Service (PTaaS) durch und bringen Geräte, sowie Know-how und Durchführung aus einer Hand zu Ihnen. Im Zuge von Continuous Integration besteht die Möglichkeit, eine Lizenz zu erwerben.

Unser IT-Security-Team übernimmt beim Pentest die Rolle des Hackers (Redteaming). 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 IT-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 Unternehmensgröße und Branche durchführbar. Aufgrund ihrer automatisierten Ausführung lassen sie sich komplett reproduzieren. Gleichzeitig behalten Sie immer den Überblick und die Kontrolle!

Im Anschluss an den ausführlichen Pentest erhalten Sie von uns einen aussagekräftigen Ergebnisbericht. Auf Basis der Ergebnisse stellen wir Ihnen direkt einen individuellen, priorisierten Report zur Verfügung, beraten Sie und unterstützen Sie gerne bei der Umsetzung. 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



TOP ATTRACTIONS

Extreme	**Potential Log4Shell (CVE-2021-44228)**	6 occurrences
Serious	**Website using self-signed certificate**	20 occurrences
Serious	**Website using expired certificate**	7 occurrences

LIZENZMODELLE: WÄHLEN SIE IHREN WEG ZUR NÄCHSTEN SICHERHEITSSTUFE!

PENTESTS AS A SERVICE (PTAAS)

- Hausbesuche
- Redteaming as a Service
- Customer Specific Scenarios

MANAGED SECURITY SERVICE PROVIDER (MSSP)

- All-in-One Lösung
- Setup, Betreuung, Best Practice
- Continuous Validation

SUBSCRIPTION

- Your own license
- Named Solution Architect, Support, Customer Success
- Full Exposure Management

IHR VORSPRUNG MIT SYRACOM

Unser 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. Unsere Governance, Risk & Compliance Säule besteht aus den Produkten Archer, Nachhaltigkeitsberatung, Business Continuity Management, Identity- und Accessmanagement, Datenschutz und Social Engineering die priorisierten Bausteine für die Informationssicherheit Ihres Unternehmens bieten.

brandeins /thema 2024 Beste Unternehmens-berater

25
Jahre im Dienste der Kunden

180
Mitarbeiter

25
Mio. € Umsatz

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!

Ihre Ansprechpartnerin:

Katharina Siemund
Product Manager
Governance, Risk & Compliance / IT-Security
+49 151 52314204
katharina.siemund@syracom.de

syracom AG
Otto-von-Guericke-Ring 15
65205 Wiesbaden
+49 61 22 9176 0

syracom.de
Part of Consileon Group