# KÄUFER-LEITFADEN FÜR PENETRATIONSTESTS

**Komplexität war gestern: die Wahl von Scanner, Penetrationstest, Bug Bounty-Programm oder plattformbasiertem Sicherheitstest für Ihre Anforderungen leicht gemacht**

Synack

## Inhalt


Einführung 1

Die Entstehung von Sicherheitstests 1

Effektive Sicherheitsstrategie 2

Arten von Sicherheitstests 3

- Scans 3
- Herkömmliche Penetrationstests 4
- Bug Bounty-Testprogramme 4
- Plattformansatz für Crowdsourcing-basierte Sicherheitstests 6

Der ROI von Penetrationstests 8

Darum setzt Synack auf eine sichere vertrauenswürdige Plattform 10

Synack-Produkte – Vergleich anhand von Funktionen 12

Fazit 13

Anhang A: Checkliste: Auswahl von Penetrationstest-Anbietern 14

Anhang B:
Features und Vorteile von plattformbasiertem Crowdsourcing 17

Anhang C: Begriffsglossar 19

Cyberangriffe sind Alltag, denn Cyberkriminelle sind äußerst gut organisiert und gehen bei ihren Attacken sehr zielgerichtet vor. In 31 % der Fälle verliert ein Vertreter des C-Level-Managements infolge eines Angriffs seinen Job.1 Doch das müssen nicht Sie sein – oder Ihr Unternehmen.

Die richtige Testlösung ist entscheidend, um Sicherheit zu gewährleisten. Wenn Sie auf der Suche nach der für Ihr Unternehmen am besten geeigneten Lösung sind, ist eines besonders wichtig: Priorisieren Sie Ihre Ziele. Wünschen Sie sich ganzheitliche Sicherheit, um das Risiko eines Angriffs zu minimieren? Ist Compliance Ihr einziges Ziel? Drängt ein Kunde oder Partner auf eine Prüfung? Suchen Sie nach einem zeitpunktgenauen Test oder wünschen Sie sich dauerhaft Sicherheit, die mit der Weiterentwicklung von Netzwerk und Anwendungen Schritt hält?

Behalten Sie diese Ziele im Hinterkopf, während Sie diesen Leitfaden lesen. So können Sie die Erkenntnisse für Ihren Anwendungsfall nutzen. Bevor wir jedoch in die Welt aus Alternativen und Testkomponenten eintauchen, möchten wir ein paar grundlegende Informationen vermitteln.

## Die Entstehung von Sicherheitstests

Penetrationstests gibt es bereits seit den frühen 1970er Jahren. Etabliert haben sie sich, als IT-Systeme und -Services zum festen Bestandteil von Geschäftsprozessen wurden.

Dabei beauftragen Unternehmen Spezialisten, die die gleichen Taktiken, Technologien und Prozeduren (TTP) anwenden wie Angreifer. Solche externen Tests bieten eine präzise neutrale Bewertung der Netzwerksicherheit.

Digitale Umgebungen – und damit auch die Angriffsflächen – haben sich ständig weiterentwickelt. Wir Menschen sind kreativ, und gleichzeitig sind unsere Möglichkeiten beschränkt. Daher wurden in den späten 1990er Jahren Scanner entwickelt, um Sicherheitstests großflächiger (obgleich nicht tief greifender) einsetzen zu können. Und schließlich entwickelten sich in den frühen 2000er Jahren Crowdsourcing-basierte Sicherheitstest, und zwar weil es einen starken Bedarf an Fachkräften gab und mehr Gründlichkeit bei der proaktiven Ermittlung und Behebung von Schwachstellen erforderlich wurde.

### VORTEILE VON PENETRATIONSTESTS

- **Das Management überzeugen:** 28 % der aufgedeckten Schwachstellen sind schwerwiegend.[1] Sprich, ohne Tests und Abhilfemaßnahmen besteht ein erhebliches Risiko für eine Datenpanne. Das ist ein Aspekt, der für das Management von Bedeutung ist.
- **Umsetzbare Daten:** Um hilfreiche Erkenntnisse zu gewinnen, gilt es, jede ermittelte Schwachstelle anhand von eindeutigen Schritten zu bewerten, damit sie auf Kundenseite schnell behoben werden kann.
- **Geringeres Schwachstellen-Risiko:** Unternehmen werden sicherer, wenn mehr Schwachstellen ermittelt und behoben werden, denn infolge gibt es weniger Möglichkeiten für eine Datenpanne.
- **Neutrale Bewertung: Branchen-Best Practices dienen dazu, Ihr Unternehmen abzusichern, indem Tester Sicherheits-Checklisten durcharbeiten und dabei Richtlinien und Compliance-Kriterien empfehlen.**

## Effektive Sicherheitsstrategie

Effektive Sicherheit bedeutet, hochwertige Assets zu schützen und das grundsätzliche Sicherheitsniveau im gesamten Unternehmen zu intensivieren. 2019 wurden in den USA mehr als 17.000 Schwachstellen gemeldet (und die Zahl der unentdeckten Schwachstellen liegt vermutlich sogar noch wesentlich höher).[2] Wenn Unternehmen sicher sein wollen, müssen sie jede kritische Schwachstelle in jedem wichtigen System finden und schließen, denn Angreifer benötigen nur ein Schlupfloch für eine erfolgreiche Attacke.

## Was meinen wir mit Reichweite und Detailgenauigkeit beim Testen?

Sicherheits- und Penetrationstests haben sich weiterentwickelt, um mit den ununterbrochenen Software-Entwicklungszyklen Schritt halten und den damit verbundenen dauerhaften Bedarf an aussagekräftigen Sicherheitserkenntnissen erfüllen zu können.

**DETAILTIEFE**

*Kriminelle konzentrieren sich manchmal auf ein bestimmtes Asset und starten zig kleinschrittige Angriffsversuche, um den Fuß in die Tür zu bekommen. Solchen Angriffen können Sie mithilfe von tief greifenden Tests Vorschub leisten.*

**REICHWEITE**

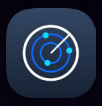
*Angreifer nutzen häufig automatisierte „Bots“, um einfache Wege zu finden, in ein Netzwerk oder Asset einzudringen. Großflächige (aber oberflächliche) Tests mit Scannern können solche Schwachstellen sogar noch verstärken.*

1 Synack Red Team-Daten, 12-Monats-Zeitraum vor dem 1.01.2020.

2 National Vulnerability Database, https://nvd.nist.gov/vuln/search.

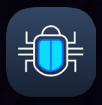
## Arten von Sicherheitstests

Sicherheitstests lassen sich in vier grundlegende Kategorien gliedern:



**Softwaregestützte Scans** für die Suche nach anfälligen oder unautorisierten Systemen und Services [maschinell durchgeführt]

**Herkömmliche Penetrationstests,** sprich checklistenbasierte Bewertungssysteme für gängige Schwachstellen, basierend auf dem Standard Web Application Security Project (OWASP) oder anderen Standards [von Beratern durchgeführt]



**Bug Bounty-Testprogramme**, bei denen Experten die Möglichkeit haben, ein Asset nach allen Regeln der Kunst anzugreifen, die Vergütung erfolgt in Form eines „Kopfgelds“ für Funde [Crowdsourcing-basiert]

**Plattform für Crowdsourcing-basierte Sicherheitstests**, in der die besten Elemente aus den drei Kategorien oben zusammengeführt werden: Penetrationstests der nächsten Generation [plattformbasiert, von Menschen durchgeführt]

## Scans

Scanner kommen zum Einsatz, um für risikoarme Assets großflächigen Schutz vor Angriffen zu bieten. Scanner bieten nicht den Detailgrad von Sicherheitstests, die es für ein ganzheitliches Sicherheitskonzept braucht (Scanner können keine mehrschrittigen Angriffe simulieren oder kreativ denken, wie Experten es können). Sie sind eine „großflächige aber oberflächliche“ Schutzmaßnahme für bekannte Schwachstellen. Zu den führenden Anbietern dieser Kategorie gehören Tenable, Rapid7, WhiteHat und Qualys.[3]

Auf dem Markt gibt es ein großes und günstiges Angebot an Scannern. Allerdings bringen sie ein paar wesentliche Einschränkungen mit sich, wenn sie als eigenständige Lösung bereitgestellt werden. Wichtige Assets erfordern fast immer auch einen gewissen Grad an menschlicher Beteiligung. Scanner sind zudem auch nicht in der Lage, komplexe mehrschrittige Angriffsversuche zu unternehmen, wie Menschen es können. Scanner sind ein wichtiger Bestandteil von Sicherheitstests. Doch aus den angeführten Gründen sind sie allein nicht ausreichend, um das Sicherheitsrisiko realistisch zu bewerten.

3 Magic Quadrant von Garnter für Application Security Testing, Horvath, Zumerle, und Gardner, ID G00394281 29. April 2020

## Herkömmliche Penetrationstests (checklistenbasiert)

Unternehmen führen herkömmliche checklistenbasierte Bewertungen durch, um nachweisen zu können, dass sie Sicherheitskontrollen mit bestimmten Regeln oder nach einem bestimmten Standard implementiert haben, die für Compliance erforderlich sind. Dabei wird in der Regel direkt aus der Belegschaft eine kleine Gruppe an Mitarbeitern mit dieser Aufgabe betraut. Die Big Four der Beratungsfirmen (Deloitte, E&Y, PwC, KPMG) sind gute Beispiele für diese Kategorie. Zu den spezialisierteren Anbietern gehören NCC Group, Bishop Fox und Cipher. Außerdem gibt es noch einige kleinere unabhängige und lokal agierende Penetrationstest-Anbieter (auch als Beratungsboutiquen bezeichnet), die diese Testform einsetzen.

Wie effizient diese Methode ist, hängt vom Detailgrad der Bewertung ab, die ein Unternehmen benötigt, und der Kompetenz der vom Anbieter eingesetzten Tester. Die Vorteile dieser Methode: unkompliziert und ein abgesteckter Umfang. Die Nachteile sind der mangelnde Wettbewerb unter den Testern, kein Anreiz für kreative Ansätze, es kommt nur eingeschränkt Fachwissen für jede einzelne Schwachstelle zum Tragen, es gibt keine Erkenntnisse in Echtzeit zu den Ergebnissen, und Abhilfemaßnahmen können erst verzögert ergriffen werden.

## Bug Bounty-Testprogramme

Bug Bounty-Sicherheitstests vereinen verschiedenste Testkompetenzen. Manchmal wird auch eine Prämie ausgesetzt, um für ethische Hacker einen Anreiz zu schaffen, sich in die Rolle eines Angreifers zu begeben. Damit lässt sich die Sicherheit eines Ziels insgesamt bewerten, und es werden nicht einfach nur vordefinierte Sicherheitskontrollen getestet. In dieser Gruppe gibt es zahlreiche Unterkategorien (ausführliche Informationen finden Sie auf der nächsten Seite). Zu den bekannten Anbietern gehören Cobalt, Bugcrowd und HackerOne. Viele der oben genannten Unternehmen führen für viele ihrer Kunden eher checklistenbasierte Tests durch. Crowdsourcing-basierte Tests sind meist den Großkonzernen vorbehalten. Eine Kategorisierung wird aus Vereinfachungsgründen an dieser Stelle nicht vorgenommen.

Bug Bounty-Sicherheitstest bieten den Vorteil, dass ethischen Hackern ein attraktiver Anreiz geboten wird, mehr Schwachstellen zu finden, als das mit dem herkömmlichen Checklistenansatz möglich wäre. Mehr Experten, Kompetenzen (häufig arbeiten an einem Test mehr als 50 Fachleute) und Wettbewerb sorgen für eine insgesamt bessere Leistung und eine tiefer greifende Bewertung. Diese Kategorie ist sehr komplex und bietet unterschiedliche Kontrollebenen. Für eine gute Kaufentscheidung muss ein Käufer in der Lage sein, Angebote beurteilen zu können. (Auf der nächsten Seite werden die Vor- und Nachteile im Detail erläutert.)

# Wesentliche Aspekte von Bug Bounty-Testprogrammen

Es finden sich zwar alle Tests in der gleichen Kategorie wieder, allerdings gibt es verschiedene Arten von Bug Bounty- und Crowdsourcing-basierten Sicherheitstests, die unterschiedlich effektiv sind:

**PROGRAMME ZUR OFFENLEGUNG VON SCHWACHSTELLEN** (auch als Programme zur verantwortungsvollen Offenlegung bezeichnet): Eine Politik des „etwas sehen, etwas sagen“, bei der ein Unternehmen einen Anbieter beauftragt oder hinzuzieht, um ein Programm zu verwalten, in dem jeder die Entdeckung einer Schwachstelle melden kann.

**Vorteile:** kostengünstig, einfache Implementierung, Möglichkeit, eine positive Öffentlichkeitswahrnehmung zu fördern.

**Nachteile:** ggf. hoher Verwaltungsaufwand aufgrund von zahlreichen mangelhaften Meldungen, schlechte Kontrolle, da jeder Schwachstellen melden kann, einige Teilnehmer machen ihrem Ärger öffentlich Luft, wenn sie nicht in kürzester Zeit eine Antwort erhalten.

**DER MARKTPLATZ FÜR BUG BOUNTY-PROGRAMME:** Ein Topf voll Geld steht für ethische Hacker bereit, die ihrerseits versuchen, sich in IT-Assets von Unternehmen zu hacken. Dieses Vorgehen ist mit Programmen zur Schwachstellen-Offenlegung vergleichbar, mit der Ausnahme, dass es für Ergebnisse keine Prämien gibt. Manchmal werden Bug Bounty-Programme nur für eine bestimmte Gruppe von ethischen Hackern (sprich Sicherheitsexperten) geöffnet.

**Vorteile:** Wettbewerb sorgt für eine bessere Leistung, verschiedene Kompetenzen und Erfahrungen kommen beim Testen zum Tragen.

**Nachteile:** eingeschränkte Kontrollmöglichkeiten und mögliche Risiken, wenn die Beteiligten nicht ausführlich geprüft und gemanagt werden, möglicher Verwaltungsaufwand wegen zahlreichen gemeldeten Schwachstellen, die nicht immer erstklassig sind.

**MICRO-CROWDSOURCING:** Einige Unternehmen, die auf Crowdsourcing-basierte Tests oder Bug Bounty-Programme setzen, beschäftigen nur eine feste Gruppe an Fachleuten (manchmal nur 1-2), die ein reguläres Gehalt beziehen und keine Prämien erhalten und in der Regel checklistenbasiert arbeiten.

**Vorteile:** kostengünstig und verhältnismäßig schnell (obgleich auch etwas irreführend)

**Nachteile:** Dieser Ansatz wirkt wie ein Crowdsourcing-basierter Test, wenig Experten und mangelnder Wettbewerb nehmen diesem Ansatz die Effizienz, die wahres Crowdsourcing auszeichnet. Diese Vorgehensweise gehört tatsächlich in die Kategorie „herkömmliche Penetrationstests“.

# Plattformansatz für Crowdsourcing-basierte Sicherheitstests

## Die grundlegenden Elemente eines Sicherheitstests vereint

Bei der wohl solidesten Testlösung, d. h. eine Plattform für Crowdsourcing-basierte Sicherheitstests, treffen Kreativität und Einfallsreichtum der Crowdsourcing-basierten Schwachstellenermittlung, der methodengesteuerte Penetrationstestansatz und die Skalierbarkeit und Abdeckung eines High-End-Scanners aufeinander. Damit können Unternehmen zielgerichtet Penetrationstests durchführen, unbekannte Schwachstellen finden und neu gewonnene Erkenntnisse großflächig umsetzen. Die Gesamtheit der Erkenntnisse fließt in ein maschinell gesteuertes und mit menschlicher Expertise erweitertes Scansystem, das lernen kann, wie Schwachstellen möglicherweise aussehen. Die Plattform bietet damit eine skalierbare und weitreichende Abdeckung der Angriffsfläche der verbleibenden Assets und erkennt Risikoquellen, die das Expertenteam dann untersuchen kann.

Die Crowdsourcing-basierte Sicherheitstest-Plattform verwandelt all diese Komponenten in einen fortlaufenden Penetrationstest-Prozess. Besonderes Merkmal: In dem Prozess sind die Arbeit der Experten, der Einsatz von Scannern und Compliance-Vorgänge besonders aufeinander abgestimmt. Dabei werden eine Gruppe aus Top-Experten, ein KI-/ML-fähiger High-End-Scanner und aufeinander abgestimmte Workflows gemeinsam eingesetzt, um die Test-Crowd zu koordinieren. Mit anderen Worten: alle drei oben genannten

Aspekte vereint und über eine intelligente Plattform verwaltet, um sich alle Vorteile zu sichern. Aktuell ist Synack der einzige Vertreter dieser Kategorie, obgleich es Anbieter im Bug Bounty-Sektor gibt, die diese Kategorie für sich beanspruchen.

Experten und intelligente Technologie arbeiten über eine integrierte Plattform zusammen, die die gemeinsamen Interaktionen koordiniert. So ergänzen sich die beiden Faktoren Mensch und Maschine, um hochwertige Erkenntnisse zu gewinnen und unterbrechungsfreie Abdeckung zu bieten. Durch die intelligente Anwendungsabstimmung wird ein hoher Grad an Präzision erreicht. Und statt einfach nur die Prämie zu deckeln, übernimmt der Anbieter die volle Verantwortung für die Testkosten und alle wichtigen Schwachstellen, über die er informiert wird.

> *Synack hat uns überzeugt – durch ein hohes Maß an Professionalität und Ansprechbarkeit. Außerdem bieten sie ein Produkt, das sich in puncto Konzeption und Funktion von anderen abhebt.*
>
> **CEO UND MITBEGRÜNDER,**
> **INTERNATIONALES UNTERNEHMEN IM FINANZDIENSTLEISTUNGSSEKTOR**

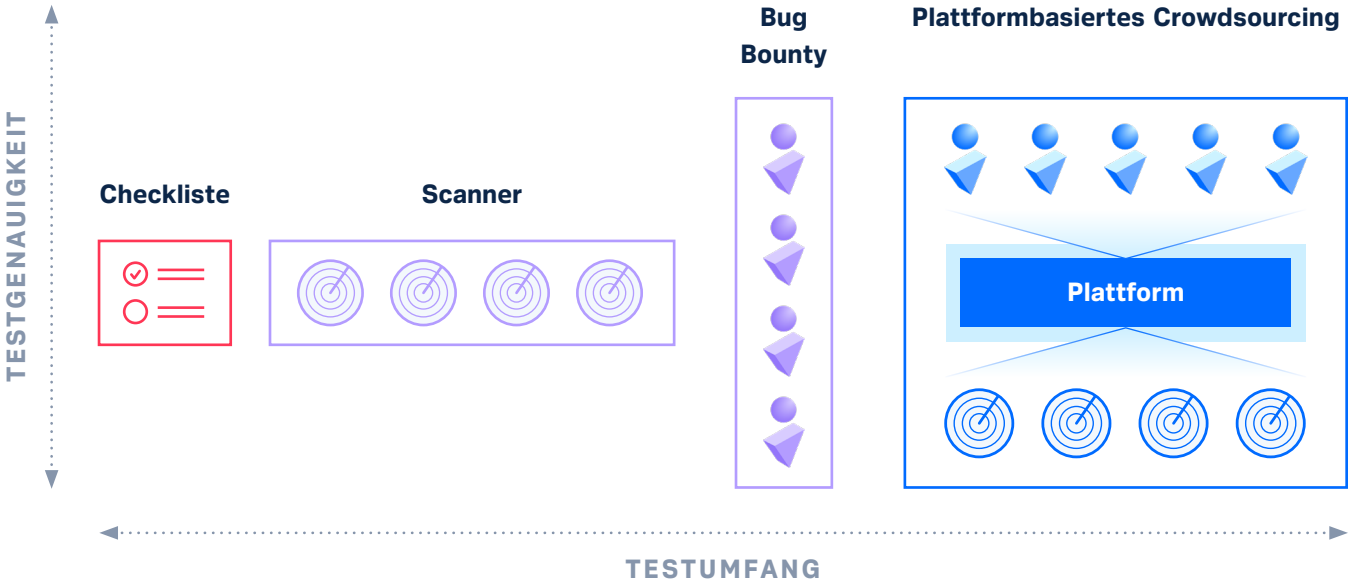
## Welche Vorteile bieten Plattformen für Crowdsourcing-basierte Sicherheitstests?

- Scans ermöglichen eine weitreichende Abdeckung von risikoarmen Assets,
- KI/ML koordiniert die von Experten durchgeführten Arbeiten
- In fortlaufenden Penetrationstests rund um die Uhr während des gesamten Jahres konzentrieren sich Experten mit ihrem gesamten Know-how auf gefährdete Assets
- Experten gehen bei Ihrer Suche nach allen Regeln der Kunst vor, bringen umfassende
- Kompetenzen und Taktik, Technik und Prozeduren ein, und im Gegensatz zu Bug Bounty-Programmen, sind Prämien nicht gedeckelt
- Sie behalten von Anfang bis zum Ende die Kontrolle über den Testprozess (Sie entscheiden über den Start und Pausen, Asset-Schutz durch ein sicheres Gateway)
- Die Plattform bietet umsetzbare Ergebnisse und Analysen in Echtzeit

## Funktionen nach Kategorie

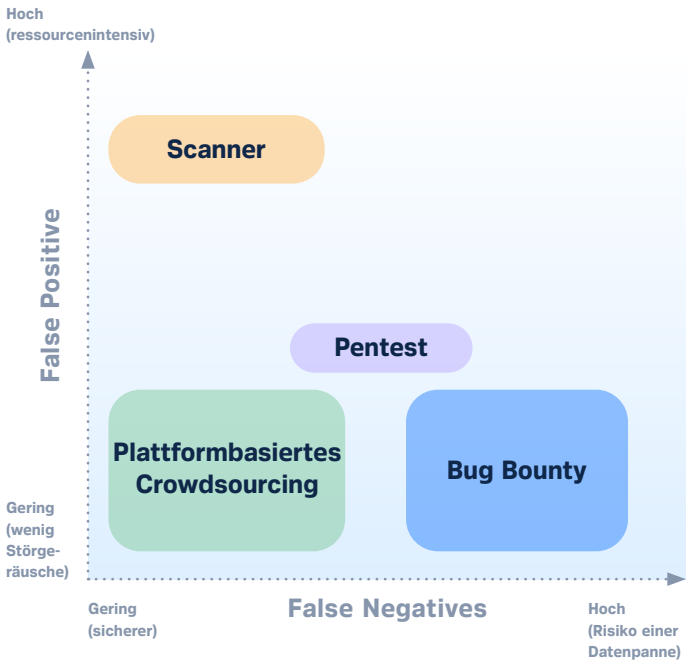
| ✓ Gut<br>✗ Schlecht | Scanner | Herkömmlicher Pentest | Bug Bounty-Test | Crowdsourcing-basierte Sicherheitstests |
|---|---|---|---|---|
| **Wert (Abdeckung/ Kosten)** | ✓ | ✓ | ✓ Für bestimmte Assets | ✓ |
| **Sicherheit/ Pozessvertrauen** | ✓ | ✓ | ✗ | ✓ |
| **Skalierbarkeit auf die ganze Angriffsfläche** | ✓ | ✗ | ✗ Nur hochwertige Assets | ✓ |
| **Testgenauigkeit (Qualität der Schwachstellen)** | ✗ Falsche positive Ergebnisse | ✗ Falsche positive Ergebnisse | ✗ Einige extrem tiefe Kategorien | ✓ |
| **Vollständiger Servicesupport** | ✗ | ✗ | ✗ | ✓ |

### VERGLEICH UNTERSCHIEDLICHER SICHERHEITSTEST-MODELLE




## Wie gestaltet sich der ROI von Penetrationstests?

Unter dem Strich bietet der plattformbasierte Crowdsourcing-Ansatz im Vergleich zu herkömmlichen Penetrationstests einen viermal so hohen ROI. In Zahlen ausgedrückt ergibt das einen ROI von 159 % wegen dem Plus an Effektivität, Effizienz und des großen Umfangs.[4]




4 *ROI-Schätzung, basierend auf Synack-Daten des 1. Quartals 2020. Grundlage ist ein Vergleich mit einem herkömmlichen Penetrationstest, Gegenwert 30.000 USD für 80 Teststunden, 6 Wochen bis zum Arbeitsbeginn bei einem Neukunden und 1 Arbeitswoche für die Berichtserstellung

## ROI DER PLATTFORM FÜR CROWDSOURCING-BASIERTE SICHERHEITSTESTS

**159 %**

**4-mal höherer ROI als bei herkömmlichen Penetrationstests**

**3-mal**

**mehr Time on Target im Vergleich zu herkömmlichen Penetrationstests**

**20 %**

**weniger fehlgeschlagene Patches aufgrund des Patch-Überprüfungsprozesses**

**<72 Std**

**für das Onboarding im Vergleich zum herkömmlichen Modell**

# Darum setzt Synack auf eine sichere vertrauenswürdige Plattform

Bei Crowdsourcing-basierten Lösungen ist Vertrauen das Wichtigste. Wenn Risiken innerhalb der Community (im Hinblick auf die Offenlegung der Schwachstellen gegenüber der Öffentlichkeit) nicht eingedämmt werden, können Unternehmen in einen unkontrollierbaren Prozess gelangen, in dem Schwachstellen schneller entdeckt werden, als sie sich beheben lassen. Viel Ergebnislärm ohne ein klares Signal, und/oder Experten drohen damit, Schwachstellen offenzulegen, wenn sie nicht innerhalb eines gewissen Zeitrahmens behoben werden.

## ACHTUNG: STOLPERFALLEN

- **Fremdvergabe von externen Penetrationstests** — Häufig vergeben Anbieter von Sicherheitsservices Penetrationstests an eine Fremdfirma, um das eigene Angebot zu stärken, oder auch an verschiedene Fremdfirmen, um sich eine vielseitige Expertengruppe zu sichern. Das Problem dabei ist, dass es keine klaren Verantwortlichkeiten gibt. Häufig endet das in gegenseitigen Schuldzuweisungen, und in der Regel ist die Koordination zwischen zwei und mehr Unternehmen nicht unproblematisch.
- **Penetrationstest mit gefaktem Crowdsourcing** — Viele Unternehmen, die angeben, eine Experten-Crowd zu beschäftigen, buchen für Ihr Projekt in Realität dann nur 1-3 Experten. Damit ist weder ausreichend Umfang noch der geeignete Detailgrad für einen Test gegeben. Das wird „Zwei Tester, zwei Laptops, zwei Wochen“ genannt.
- **Mangelnder Crowd-Wettbewerb** — Eine unzureichende Crowd-Umgebung kann dazu beitragen, dass der Wettbewerb leidet. In einem Crowdsourcing-basierten Penetrationstest, der diesen Namen auch verdient, ist die Crowd, sprich die am Test beteiligten Personen, offen, und es wird derjenige bezahlt, der eine Schwachstelle am schnellsten entdeckt. Wie würde wohl ein Boxkampf mit nur einem Boxer aussehen?
- **Bug Bounty-Checkliste** — Der gewisse Reiz des Crowdsourcings verleitet einige Unternehmen dazu, das Konzept des prämienbasierten Crowdsourcings in einem einfachen Checklistenmodell aufzurollen. Beide Modi sind wichtig, wenn Sicherheit erreicht werden soll. Aber verwehren Sie sich gegen den Irrglauben, dass eine „Crowdsourcing-basierte Checkliste“ ein Ersatz für Crowdsourcing-basierte Sicherheitstests ist.
- **Manuelle Analyse** — Bei Analysen gilt: Garbage in, Garbage out. Umsetzbare Analysen müssen datenbasiert sein. Einige Plattformen nutzen Analysen, deren Grundlage manuelle Prozesse oder durch Menschen vorgenommene Bewertungen bilden, anstelle von soliden neutralen Algorithmen. Und das macht solche Analysen unzuverlässig.
- **Illusion von Kontrolle** — Viele Crowdsourcing-basierte Sicherheitsplattformen preisen insbesondere an, dass der Kunde die Kontrolle über die Crowd hat. Weiterhin wird zwischenzeitlich die „gründliche Prüfung“ der Experten in etwa mit Kontrolle gleichgestellt. Käufer sollten Anbietern die Frage stellen, wie viele Schritte ihre umfassende Prüfung der Crowd beinhaltet, ob die Crowd-Aktivitäten fortlaufend überwacht werden und, sofern das der Fall ist, ob es rund um die Uhr einen Einblick in die Testvorgänge über die Plattform gibt, darunter auch die Möglichkeit, den gesamten Testprozess anzuhalten und erneut zu starten.
- **Fehlende Patch-Überprüfung** — Hüten Sie sich vor Organisationen, die bei der Patch-Überprüfung keine Tests vornehmen. Laut Statistik schlagen 30 % der ersten Patches fehl. Ohne einen Nachtest können Sie nicht sicher sein, dass der Patch funktioniert. Um mit Sicherheit zu wissen, ob der Patch erfolgreich war, muss ein Nachtest durchgeführt werden.

Um diesen Problemen vorzubeugen, fährt Synack zweigleisig. Als Erstes prüfen wir jeden Penetrationstester auf Herz und Nieren, um sicherzustellen, dass nur diejenigen, die professionell und ethisch agieren – zusätzlich zum Nachweis ihrer umfassenden Kompetenzen und Erfahrung – für das Synack Red Team ausgewählt werden. Als Zweites werden alle Tests über ein sicheres Gateway durchgeführt und über unsere Plattform verwaltet. So können wir die Testvorgänge fortlaufend überwachen und kontrollieren und infolge sicherstellen, dass der Test unsere hohen Standards erfüllt. Für Kunden in hochgradig regulierten Branchen bieten wir sogar sichere, virtualisierte Umgebungen für unsere eigenen Sicherheitsexperten. Durch die komplette Endpunktkontrolle ist ein höheres Datenschutzniveau gegeben.

> *Sie beauftragen viele wirklich erfahrene und hochgradig qualifizierte Experten für den Test. Sie zahlen nicht mehr, um mehr Tester zu bekommen... Ich freue mich wirklich, sagen zu können, dass unsere Erwartungen übertroffen wurden.*
>
> **SENIOR CLOUD SECURITY ANALYST IN DER DIENSTLEISTUNGSBRANCHE**

## Synack-Produkte — Vergleich anhand von Funktionen

In der folgenden Tabelle erhalten Sie einen Überblick über die wichtigsten Funktionen und welche Kombinationen mit den zahlreichen SKUs möglich sind. Damit können Sie die wichtigsten Funktionen und die Vorteile, die sie bieten, besser einordnen.

| | **Discover:** Crowdsourcing-basierte Schwachstellen-Entdeckung | **Certify:** Crowdsourcing-basierte Pentests | **Synack365:** Fortlaufende Crowdsourcing-basierte Pentests |
|---|---|---|---|
| **Dauer** | Zeitgebunden | Fortlaufend | Fortlaufend |
| **Intelligente Plattform mit Ergebnissen und Analysen in Echtzeit** | ✓ | ✓ | ✓ |
| **Programm zur Offenlegung von Schwachstellen (VDP)** | ✓ Enthalten, beim Kauf von vier weiteren Tests | ✓ | ✓ |
| **Prämienbasierte Jagd nach Schwachstellen** | ✓ | ✓ | ✓ |
| **SmartScan mit Prüfung** | ✓ | ✓ | ✓ |
| **Methodenbasierte Tests (Checkliste)** | | ✓ | ✓ |
| **Testabdeckung durch das Synack Red Team rund um die Uhr** | | | ✓ |

## Fazit

Eigenständige Scanner bieten Ihnen eine großflächige (und gleichzeitig oberflächliche) Abdeckung Ihrer Angriffsfläche für geringwertige Assets. Herkömmliche Penetrationstests sind dazu geeignet, die von Auditoren und Investoren geforderten Sicherheitstests zu erfüllen. Bug Bounty-Sicherheitstests bieten Ihnen tiefer greifende Testmöglichkeiten für eines oder mehrere wertvolle Assets.

Umfangreiche und gleichzeitig tief greifende Bewertungen, die die Grundlage für echte Sicherheit bilden, bietet die Crowdsourcing-basierte Plattformlösung – der Sicherheitstest der nächsten Generation. Dabei kommen die Leistungsfähigkeit, das Talent und der Detailgrad einer Crowd aus ethischen Hackern mit der großflächigen Abdeckung eines Scanners und die Compliance-Anforderungen einer Checkliste zusammen. Im Ergebnis erhalten Sie eine umfassende Sicherheitsabdeckung rund um die Uhr. Ausschließlich eine vollständig und umfassend geprüfte Crowd, unterstützt von einer durchgängig verfügbaren intelligenten Plattform, bietet Ihnen eine komplette Sicherheitsabdeckung und einen echten ROI.

> *Sicherheitstests stehen bei CEOs und Sicherheitsingenieuren ganz oben auf der Prioritätenliste. Prognosen zufolge werden sich die Kosten für Cyberkriminalität weltweit bis 2021 auf 6 Billionen US-Dollar summieren. Unternehmen können nicht einfach DEN Experten einstellen, der den Kampf gegen diese Bedrohung aufnimmt. Es ist auch keine Option, sich auf antiquierte Schutzmechanismen zu verlassen. Unternehmen, die ihr Sicherheitsrisiko effektiv senken möchten, benötigen skalierbare, umfassende Sicherheitstest-Plattformen, die kompromisslos sowohl umfangreiche als auch tief greifende Bewertungen ermöglichen.*
>
> **—B CAPITAL GROUP**

# Anhang A: Checkliste: Auswahl von Penetrationstest-Anbietern

Wenn Sie sich mit herkömmlichen Penetrationstests, Bug Bounty-Programmen und plattformbasierten Crowdsourcing-Alternativen auseinandersetzen, erleichtert Ihnen diese Liste die Bewertung verschiedener Anbieter.

| | Angebot des Anbieters: |
|---|---|
| **Experten** | |
| Crowd aus Hunderten verfügbaren Testern (im Schnitt 50–80/Test), um verschiedenste Kompetenzen und große Erfahrung für tief greifende Analysen zu gewährleisten | ◯ |
| Umfassend geprüfte Experten-Community, dazu gehören Prüfungen der Qualifikation, Interviews und Prüfungen zum Hintergrund, um Sicherheit und Qualität zu garantieren | ◯ |
| Prämienbasiertes Modell, um eine kreative Herangehensweise zu belohnen und Wettbewerb zu fördern | ◯ |
| Experten, die on demand verpflichtet werden und unabhängig arbeiten und eben nicht auf der Gehaltsliste stehen, bringen ihre Kompetenzen ein und beschäftigen sich bedarfsgerecht mit Ihrer Sicherheitslage | ◯ |
| **Schutz und Vertrauen** | |
| Der Kunde trägt keine Verantwortung für die zukünftige Beschäftigung der Experten | ◯ |
| Dem Kunden gehören die Daten und die Schutzmechanismen für entdeckte Schwachstellen (nicht dem Anbieter oder Experten) | ◯ |
| Abdeckungsanalyse, wann/welche/wie (z. B. Angriffsversuche) die zu schützenden Anwendungen basierend auf der Arbeit der Experten bewertet wurden | ◯ |
| Die Vergütung erfolgt über den Anbieter, um den Kunden zu schützen | ◯ |
| Keine „letzter Ausweg“-Ausnahme, Datenschutz-bedingt, für das Melden von Schwachstellen | ◯ |
| Kundenkontrolle über Funktionen zum Starten, Anfangen und Wiederaufnehmen der Testaktivitäten | ◯ |

| | |
|---|---|
| **Technologie** | |
| Automatisierte Schwachstellen-Scans, die die Kompetenzen der Experten erweitern und Ergebnisse für ihre Arbeit liefern | ○ |
| Ein zentralisiertes SaaS-Portal, das Kunden rund um die Uhr Einblick in die Tests, Ergebnisse, Kennzahlen und Berichte bietet | ○ |
| Koordination/Prüfung der Experten mithilfe einer intelligenten Administrationsplattform | ○ |
| Sicheres Gateway, über das alle Testvorgänge laufen | ○ |
| **Prozess der Schwachstellenermittlung** | |
| Compliance-gestützte, methodenbasierte Tests, die auf bekannte Schwächen prüfen | ○ |
| Prämienmodell für die Entdeckung von Schwachstellen | ○ |
| Erfüllt die Anforderungen von Audit- und Compliance-Mandaten wie PCI, NIST | ○ |
| Beseitigung von Duplikaten | ○ |
| Echtzeit-Protokolle und -Updates für alle Testvorgänge | ○ |
| Anzahl an Experten, Teststunden, protokolliert für Nachverfolgung und Rechenschaftspflicht | ○ |
| Möglichkeit, direkt mit den Experten zu kommunizieren | ○ |
| **Effektive Sicherheit** | |
| Bewertung der Patch-Wirksamkeit zur Nachverfolgung des Fortschritts | ○ |
| Vollständig verwalteter Service zur Patch-Überprüfung mit garantierten Prämien | ○ |
| Risikofreier Patch-Prozess: Prüfanfragen werden nur an die Person gestellt, die die ursprüngliche Meldung vorgenommen hat | ○ |
| **Bericht und Bewertung** | |
| Revisionssichere, professionelle und anpassbare Berichte (PDF) on demand | ○ |
| Von Menschen verfasste Analysen im Abschlussbericht | ○ |
| Eindeutige, objektive Bewertung der Assethärtung | ○ |
| Bewertete Ergebnisse, um den Fortschritt im eigenen Unternehmen und im Vergleich zu Branchenkollegen nachzuverfolgen | ○ |

| | Angebot des Anbieters: |
|---|---|
| **Sicherheitsexperten-Software-Plattform** | |
| Einfacher Workflow vom Scan, über das Testen und die Prüfung bis zur Patch-Überprüfung | ○ |
| Einmalige Erkennungstechnologien für Host, Web, Mobilgeräte | ○ |
| Echtzeit-Workflow zur Bewertung der Möglichkeit der Ausbeutung | ○ |
| **Weniger Störgeräusche und optimierter Kundenservice** | |
| Ausführliche Expertenanweisungen zur Behebung | ○ |
| Vollständige Prüfung jeder gemeldeten Schwachstelle | ○ |
| Fester Ansprechpartner | ○ |

# Anhang B: Features und Vorteile von plattformbasiertem Crowdsourcing

Eine Crowdsourcing-basierte Sicherheitstest-Plattform bietet im Vergleich zu einer herkömmlichen Bewertung viele Vorteile.

| FEATURE | VORTEIL |
|---|---|
| **Bewertung** | Eine einfache Liste an Schwachstellen bietet keine umsetzbaren Risikoinformationen, der eigentliche Wert besteht in der Bewertung von Schwachstellen. Synack nutzt die Kennzahl Attacker ARS zur Messung der Widerstandsfähigkeit gegen Angreifer (Resistance Score). Damit werden Variablen beziffert, wie die Schwierigkeit, eine Schwachstelle zu entdecken, der Schweregrad einer Schwachstelle und wie effektiv Schwachstellen behoben werden können. |
| **Datengestützte Erkenntnisse** | Es ist entscheidend, dass Informationen zu den relevanten Personen gelangen, sprich zu denen, die sie benötigen. Synack stellt Penetrationstestern Daten zu Schwachstellen zur Verfügung und ermöglicht es ihnen damit, fundierte Entscheidungen zu treffen und Schwachstellen schneller zu finden. Damit erhalten Sie ganz präzise Daten, die Sie für die Bewertung Ihres Risikos nutzen können. |
| **Mustererkennung** | Fortlaufende Scans und Tests bringen Änderungen an der Angriffsfläche und mögliche Risikobereiche zutage. Für Unternehmen ist es von unschätzbarem Wert, solche Entwicklungen zu kennen, um beurteilen zu können, ob sie Opfer eines zielgerichteten Angriffs wurden oder ob Richtlinien und Verfahren im Unternehmen möglicherweise nicht ausreichend sind, um Sicherheitsanforderungen zu erfüllen. |
| **Weitreichende Kompetenzen** | Mache Beraterfirmen beauftragen für Penetrationstests gerade mal eine Person. Dadurch bedingt kommen nur eingeschränkte Kompetenzen zum Tragen, und bei der Suche nach Sicherheitslöchern werden nur wenige Tools eingesetzt. Die echte Crowdsourcing-Methode von Synack gewährleistet einen umfassenden Kompetenzbereich für die Tests. Darüber hinaus sorgen wir bei der Zusammenstellung und Prüfung des Teams dafür, dass in puncto Kompetenzen und Integrität nur Top-Experten für Sie arbeiten. |
| **Sicherheit (vs Compliance)** | Am Ende der meisten herkömmlichen Penetrationstests erhalten Unternehmen eine abschließende Bestätigung, dass sie Compliance-Anforderungen erfüllen. Doch damit ist im Hinblick auf Sicherheit nicht viel erreicht. Die Kombination aus Compliance-Checklisten und prämienbasierten Crowdsourcing-Sicherheitstests UND fortlaufenden Prüfungen, die über eine intelligente Plattform verwaltet werden, bietet Ihrem Unternehmen Compliance UND Sicherheit. |
| **Ergebnisse und Prämien** | Die Kosten für herkömmliche Penetrationstests setzen sich aus Zeit- und Materialaufwand zusammen.  Sprich, die Beraterfirma erhält das Honorar unabhängig davon, ob alle Sicherheitslöcher entdeckt, geprüft und gemeldet wurden. Mit der Methode von Synack erfolgt eine Bezahlung nur für bestätigte Schwachstellen und Exploits. Damit stehen die Kosten auf Kundenseite einem echten Wert gegenüber und entfallen nicht nur auf Arbeitszeit, die für einen Auftrag verwendet wurde. |

| FEATURE | VORTEIL |
|---|---|
| **Bewertung der behobenen Schwachstellen** | Im Rahmen von herkömmlichen Penetrationstests wird nicht immer überprüft, ob Sicherheitslöcher auch wirklich geschlossen wurden. Stattdessen bleibt dem Kunden die Aufgabe, das Loch zu schließen und die Wirksamkeit der Maßnahme selbst zu prüfen. Synack stellt verfahrensmäßig sicher, dass Kunden eine klare Anleitung zur Nachbildung erhalten und dass Exploits, die bislang wirksam waren, geschlossen sind. So wird vermieden, dass bereitgestellte Patches wirkungslos sind. Experten, die Schwachstellen erfolgreich entdecken und melden, erhalten weitere Prämien, wenn Sie nachweisen, dass sie behoben wurden. |
| **Protokolle** | Nicht alle Tests erfassen geeignete Informationen über die Testvorgänge, die es für einen erfolgreichen Abschluss braucht. Zu Compliance-Zwecken und zur Gestaltung von Best Practices für Sicherheit erfasst Synack Protokolle und auch technische Kontrollen und stellt dem Kunden diese Informationen komplett zur Verfügung. |
| **Tests beginnen und anhalten** | Die Kontrolle über den Testprozess zu haben, ist wichtiger als Sie vielleicht denken.  Es könnte ein Überraschungsaudit angekündigt werden, das es notwendig macht, Tests anzuhalten, um unangenehme Situationen zu vermeiden. Synack bietet eine sichere, geprüfte und flexible Plattform, über die Sie nicht nur über eine globale Community verfügen können – Sie haben auch die Kontrolle darüber. Dazu gehört auch, dass Sie die Möglichkeit haben, selbst über den Beginn und Pausen zu entscheiden, praktisch per Knopfdruck. |
| **Eigentum an Schwachstellen und Schutzmechanismen** | Nachdem Tests durchgeführt und Abhilfemaßnahmen ergriffen wurden, ist es besonders wichtig, dass Sie die Schwachstellendaten unter Ihrer Kontrolle haben. Bei manchen Verträgen ist die Offenlegung von Schwachstellen nach einem bestimmten Zeitraum zulässig, unabhängig vom Verfahrensstatus. Mit Synack gehören die entdeckten Schwachstellen und das damit verbundene geistige Eigentum dem Kunden. |
| **Intelligente Plattform** | Für einen wirklich effektiven Penetrationstest sind drei zentrale Komponenten vonnöten. Als Erstes benötigen Sie eine auf Herz und Nieren geprüfte, hochqualifizierte Expertengruppe, die verschiedenste Kompetenzen und Tools mitbringen. Als Zweites braucht es eine intelligente Scantechnologie, damit die Crowd arbeiten kann und der Prozess der Schwachstellenermittlung beschleunigt wird. Und als Drittes benötigen Sie eine Plattform, auf der die Experten ihre Arbeit machen können (und über die Sie die Testvorgänge überprüfen und kontrollieren und die Ergebnisse ansehen können). Das gibt Ihnen beispiellose Expertise in einem kontrollierbaren Paket, oder mit anderen Worten, Qualität und eindämmbares Risiko. |

## Anhang C: Begriffsglossar

**Black-Box-Modell**—Bei einem Black-Box-Penetrationstest werden die Schwachstellen in einem System ermittelt, die von außerhalb des Netzwerks ausgebeutet werden können. Der Penetrationstester verfügt über keinerlei Wissen zum Zielsystem, Quellcode, zur Architektur usw.

**Blue Team**—Interne Teams, deren Aufgabe es ist, das Unternehmen vor realen Angreifern zu schützen, indem es mehr über ihre Taktiken, Techniken und Prozeduren in Erfahrung bringt und die Schutzmechanismen mit Blick auf den Gegner weiterentwickelt.

**Bug Bounty-Modell**—Ein Modell, in dem die Vergütung ergebnisbasiert erfolgt, sprich es gibt ein bestimmtes Prämienbudget für die Bezahlung der Experten, wenn sie Schwachstellen finden. In der Regel ist der Test dann zu Ende, wenn das Budget verbraucht ist. Bei diesen Tests geht es weniger um Vollständigkeit und Sicherheit, sie dienen vielmehr als Ausgangspunkt für eine Härtung der Umgebung.

**Compliance-Checkliste**—Eine konkrete Checkliste (wie z. B. OWASP, NIST 800-53 oder PCI) fungiert für die Experten als Richtschnur, um nach bestimmten Schwachstellen zu suchen, und zwar basierend auf bestimmten Compliance- und Audit-Standardprüfungen. Mit dieser Methode kann effektiv Compliance nachgewiesen werden, Sicherheit wird darüber nicht erzielt.

**Fortlaufende Tests**—Abdeckung rund um die Uhr während des gesamten Jahres. Diese Tests können abonnementbasiert in Form eines jährlichen Engagements erfolgen und beispielsweise folgende Leistungen abdecken: einen Scanner und/oder einen vollständig verwalteten Service mit regelmäßigen Compliance-Prüfungen, einen eigenen Programmmanager, Services zur Anpassung des Umfangs, Management für ein Programm zur Offenlegung von Schwachstellen und ausführliche Datenanalysen und Berichte. Ziel ist, die Lebenszeit von ausbeutbaren Schwachstellen zu verkürzen und/oder diese gänzlich auszumerzen und die Widerstandsfähigkeit von Systemen gegenüber Cyberangriffen fortlaufend zu verbessern.

**Crowdsourcing-basierte Entdeckung von Schwachstellen**—Ein Testmodell, bei dem eine große Gruppe an ethischen Hackern sich prämienbasiert im Wettbewerb untereinander auf die Suche nach Schwachstellen macht. In der Regel setzt sich diese Gruppe aus 50-100 Experten mit unterschiedlichsten Kompetenzen und Erfahrungen zusammen, die jeweils verschiedene Taktiken, Techniken und Praktiken anwenden.

**Gray-Box-Modell**—Penetrationstester haben in der Regel Kenntnis über Netzwerkinterna, darunter ggf. Entwicklungs- und Architekturdokumentation, und einen Account im Netzwerk. Das ermöglicht eine zielgerichtetere Bewertung der Netzwerksicherheit als bei einer Black-Box-Bewertung.

**Tests für interne Assets**—Bei diesen Tests wird der Versuch eines Angreifers simuliert, sich über das WLAN-Netzwerk Zugang zum internen Netzwerk zu verschaffen. Die Zielsetzung ist für gewöhnlich identisch mit der von externen Penetrationstests. Der größte Unterschied ist jedoch, dass der „Angreifer“ entweder über einen autorisierten Zugriff verfügt oder an einem Punkt innerhalb des Netzwerks startet. Bei internen Asset-Tests (IAT), die von Synack durchgeführt werden, wird ein privater Kanal hinter einer Firewall zwischen den vertrauenswürdigen Experten und den Kunden-Assets aufgebaut, zum Beispiel sensitive oder vorab veröffentlichte Apps. Wenn ein Site-to-Site-VPN zum Einsatz kommt, stehen die Funktionen von Synack LaunchPoint nicht nur dem Kunden-Asset, sondern auch dem Experten zur Verfügung.

**Missionscheckliste**—Dieses Element gibt es nur bei Synack. Dabei werden der Experten-Crowd vermutete Schwachstellen zugewiesen, für die ein Exploit-Versuch unternommen werden soll. Die Anweisung wird vom Scansystem (SmartScan) ausgegeben, das auf maschinellem Lernen basiert. Die Steuerung und das Timing der Exploits wird vom Scanner (und final vom Kunden) kontrolliert. Synack bietet checklistenbasierte Tests als Ergänzung zur freien Schwachstellenermittlung. Im Ergebnis erhalten Sie eine hochwertige Version eines Compliance-basierten Penetrationstests, dabei bildet die Durchführung und Protokollierung bestimmter Tests die Grundlage für den Erfolg. Experten des Synack Red Team führen eine Reihe bestimmter Missionen (oder Aufgaben) durch und dokumentieren ihre Ergebnisse, die die Vergütungsgrundlage darstellen. Die Experten werden basierend auf der Qualität ihrer Arbeit und dem Detailgrad ihrer Einreichungen bezahlt. Checklisten sind entweder für OWASP- oder PCI/OWASP-basierte Richtlinien konzipiert.

**Offene Schwachstellenentdeckung**—Dieser Prozess wird manchmal auch als kreative Schwachstellenermittlung bezeichnet. Dabei versuchen ethische Hacker, in ein Netzwerk, einen Host, ein Gerät oder eine Anwendung einzubrechen. Die Prämie kann entweder ein „Kopfgeld“ oder Gehalt sein, sofern der Experte im Unternehmen angestellt ist.

**Penetrationstest**—Ein autorisierter simulierter Cyberangriff auf ein Computersystem, durchgeführt mit dem Ziel, die Sicherheit des Systems zu bewerten. In der Regel arbeiten 1-2 Experten im Auftrag einer Beraterfirma daran, dabei wird eine Checkliste abgearbeitet, manchmal erfolgt auch eine kreative Jagd auf Schwachstellen.

**Zeitpunktgenaue Tests**—Diese Methode unterscheidet sich von fortlaufenden Tests und wird in der Regel angewendet, wenn ein Test aufgrund eines zwingenden Grunds durchgeführt werden muss, z. B. ein Audit, eine Anfrage eines wichtigen Kunden oder bei einer Akquisition. Standardmäßig werden solche Tests innerhalb von zwei Wochen durchgeführt.

**Synack Red Team (SRT)**—Dieser Begriff ist Synack-eigen und steht für das private Netzwerk aus hochgradig vertrauenswürdigen, vielseitigen und geprüften Sicherheitsexperten. Über das SRT kommen die weltweit talentiertesten Experten über eine Plattform zusammen, um das zu tun, was sie lieben und wofür sie bezahlt werden.

**Purple Teams**—Purple Teams optimieren den Informationsaustausch zwischen den Red und Blue Teams, um die gemeinsame Effizienz zu optimieren.

**Scanner**—Ein Tool, das nach Sicherheitsschwachstellen und Schlupflöchern sucht. Diese Suche erfolgt automatisiert und ist skalierbar. Allerdings werden dabei meist immense Datenmengen produziert, die IT-Teams belasten können, wenn die Prüfung nicht auf Anbieterseite erfolgt.

**Social Engineering-Test**—Das Vorgehen bei Social Engineering-Penetrationstest ist, anhand von Social Engineering-Praktiken, denen die Mitarbeiter des Unternehmens ausgesetzt werden, herauszufinden, in welchem Grad ein Unternehmen gegen diese Form von Exploits gewappnet ist. Diese Tests sind in der Regel nicht im Umfang eines Penetrationstests enthalten.

**Prüfung**—Der Dispositionsprozess für gemeldete Schwachstellen durch einen Experten oder ein Team, das sich mit Schwachstellen befasst, um tatsächlich zu bestimmen, ob eine Schwachstelle ausgebeutet werden kann.

**TTP**—Diese Abkürzung steht für Taktiken, Techniken und Prozeduren, die Cyberkriminelle anwenden, um Angriffe zu verwalten. In diesem Zusammenhang kann sie auch für die Methoden stehen, die „White-Hat“-Experten einsetzen, um Schwachstellen während eines Penetrationstests zu entdecken.

**VDP**—Das Programm zur Offenlegung von Schwachstellen ist ein Prozess, in dem unabhängige Hacker Schwachstellen in den Assets eines Unternehmens melden können und diese Schwachstellen dem Unternehmen formell einreichen. Das VDP kann vom Unternehmen selbst oder von einem Drittanbieter verwaltet werden.

**Schwachstellenbewertung** (oder intelligente Schwachstellenbewertung) – der Marktkategoriename für Netzwerkscanner.

**Schwachstellenermittlung**—eine Testmethode, die vielseitig ist, Kreativität und das Fachwissen des vertrauenswürdigen Synack Red Team erfordert, um die Methoden von Hackern nachzuahmen. Diese Methode kommt zur Anwendung, um ausbeutbare und zuvor unbekannte Schwachstellen in der Angriffsfläche des Kunden zu finden. Dabei werden

Schwachstellen offengelegt, die im Rahmen von checklistenbasierten Tests häufig unentdeckt bleiben. Nachdem die Meldung einer Schwachstelle als valide bestätigt ist, wird der SRT-Experte im Rahmen eines prämienbasierten Bug Bounty-Modells vergütet. Unternehmen haben über die Schwachstellenermittlung die Möglichkeit, die Risiken zu managen, die mit unbekannten Schwachstellen einhergehen.

**White-Box-Modell**—Im Gegensatz zu Black-Box-Tests haben die Penetrationstester vollständigen Zugriff auf den Quellcode, die Architekturdokumentation und auf weitere Daten.