Den richtigen Pentest-Anbieter finden

turingpoint.

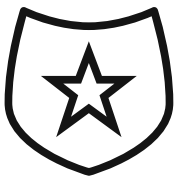
Einleitung

Die Suche nach dem richtigen Anbieter für Pentests kann einen problematischen Prozess darstellen, insbesondere für diejenigen, die mit IT-Sicherheit nicht vertraut sind. Was benötige ich? Wie weiß ich, wer genügend technische Expertise vorweisen kann? Wie identifiziere ich unqualifizierte Anbieter? Wie erkenne ich gute Reputation und Kompetenz? Wie sollte die Dokumentation aussehen?

In diesem eBook nennen wir Ihnen 6 Fragen, die Sie potentiellen Dienstleistern Ihres nächsten Pentests stellen sollten. Sie werden wissen, worauf Sie bei der Anbieterauswahl achten müssen, wie Sie die verschiedenen Angebote vergleichen können und schließlich die beste Wahl für Ihre speziellen Anforderungen treffen können.

Wenn Sie sich nicht sicher sind, wie Sie Pentest-Anbieter vergleichen können oder worauf Sie achten müssen, ist dieses eBook für Sie genau richtig.

Auswahlkriterien

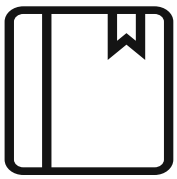


Reputation

Der Ruf des Anbieters als qualitativ hochwertig und vertrauenswürdig ist ein wichtiger Aspekt, den Sie berücksichtigen sollten. Bevor Sie eine Besprechung einberufen, sollten Sie sich über den Hintergrund und die Fachkenntnisse des Anbieters informieren. Wenn Sie sie googeln, was können Sie finden? Gibt es detaillierte Fachkenntnisse oder Blogeinträge, die sich auf Ihre technischen Bedürfnisse beziehen? Dieser Hintergrund wird Ihnen einen besseren Einblick in die Firma geben und für mehr Diskussionen während des Anrufs sorgen.

Technische Expertise

Wie beurteilen Sie die technische Kompetenz des Anbieters? Forschung und Entwicklung kann ein guter Kompetenz-Indikator sowohl für die Ihnen zugeteilten Pentester als auch für das Unternehmen sein. Durch Recherche können Sie sich ein besseres Bild von der Kompetenz und dem Angebot des Anbieters machen. Diejenigen, die keine progressive Forschung und Entwicklung betreiben, sind möglicherweise in Ihren Fähigkeiten veraltet oder nicht in der Lage eine angemessene technische Untersuchung Ihrer Anwendung oder Infrastruktur zu bieten.



Dokumentation

Eine korrekte Berichterstattung ist entscheidend, aber die Qualität der Dokumentation kann sehr unterschiedlich sein. Fragen Sie zum Beispiel nach Berichten über jeden der benötigten Pentests (Webanwendung, Infrastruktur, mobile App usw.) und stellen Sie sicher, dass Sie die Schwachstellen im Beispiel vollständig verstehen. Nichts kann frustrierender sein als ein schlechter Schreibstil oder uneindeutige Schwachstellendetails.

01

Wie stark ist der Pentest automatisiert?

Fokus: Technische Expertise

Warum ist das wichtig?

Automatisierte Werkzeuge und Scanner sind der Anfang eines jeden Pentests, aber diese übersehen oft die größeren Risiken.

Der Umfang der manuellen Tests ist eine weitere einfache Möglichkeit, potenzielle Qualitätsprobleme bei dem jeweiligen Anbieter festzustellen.

Ein Qualitäts-Pentest wird weitgehend ein manueller, tiefgehender Prozess sein. 90% des Tests sollten manuelle Arbeit wiederspiegeln.

Wonach ist zu suchen?

Die Erfahrung des Pentesters wird einen größeren Einfluss haben als die spezifischen Werkzeuge.

Scanner und andere automatisierte Tools tragen nur wenig zu einem gründlichen Pentest bei. Das Gespräch über den Tool-Fokus kann auch zur nächsten Sektion führen, die sich mehr auf die Methodik und den Prozess des Testens konzentriert.

Erkenntnis

Wenn der Anbieter angibt, dass der größte Teil des Tests automatisiert ist oder nicht viele Fragen zu Ihrer Umgebung stellt, sollten Sie vorsichtig sein.

Diese Security Assessments können ein falsches Sicherheitsgefühl vermitteln - und dabei zusätzliche Risiken mit sich bringen. Gründliche und umfassende Pentests sind manuell, strukturiert und liefern somit die besten Ergebnisse.

02 Nach welchen Standards und Methoden wird getestet?

Fokus: Effektiver Prozess

Warum ist das wichtig?

Jeder Pentest braucht eine klar definierte Methodik und muss einem strukturiertem Prozess folgen. Dies hilft, einen angemessenen Arbeitsablauf zu etablieren, um Konfusionen zu minimieren und gleichzeitig den Sicherheitsnutzen und die Testergebnisse zu maximieren.

- Die branchenübliche Methodik für Web- und API-Dienste sowie mobile Apps ist der **OWASP Testing Guide**.
- Weitere Standards für Infrastruktur-Pentests sind **OSSTMM**, **NIST**, **PTES**, **BSI** und **ISSAF**.
- Der **Leitfaden für die Durchführung von Penetrationstests** des **BSI** wird benötigt, um **Grundschutz**-Normen einzuhalten.
- **PCI DSS** legt den Mindeststandard für die Datensicherheit bei Zahlungssystemen fest.

Wonach ist zu suchen?

Professionelle **Analysten** werden immer strukturierte Prozesse und Verfahren anwenden. Stellen Sie sicher, dass der Pentest mit der Erkundungs- oder Informationsbeschaffungs-Phase beginnt. Dies ist nur ein kleines Detail, aber die richtige Aufklärung wird oft vernachlässigt und kann dazu führen, dass Sicherheits-Chancen verpasst werden.

Eine engagierte Kommunikation ist entscheidend für die Minderung potenzieller Probleme und das Team sollte bei Bedarf für einen direkten Kontakt zur Verfügung stehen.

Erkenntnis

Stellen Sie sicher, dass der Anbieter eine klare und gut definierte Methodik eingeführt hat, die den Industriestandards entspricht. Methoden helfen bei der Definition von Standards und dem Arbeitsablauf, um Pentests mit Ihrem Umfang, Ihren Testzielen und Erwartungen in Einklang zu bringen.

03 Wie sieht der Dokumentationsprozess aus?

Fokus: Dokumentation

Warum ist das wichtig?

Pentest-Berichte sind entscheidend, damit Sie verstehen, wo in Ihrer Umgebung IT-Sicherheitsrisiken und -schwächen bestehen. Diese Dokumente werden nach Abschluss der Bewertung auch an diejenigen versandt, die nie mit dem Anbieter interagiert haben. Eine klare und gründliche Dokumentation ist deshalb entscheidend!

Das ist leichter gesagt als getan, denn die Berichte müssen die Bedürfnisse einer Reihe von Personen erfüllen - von den technischen Experten bis hin zum Management. Diese Bandbreite an Bedürfnissen bedeutet eine größere Herausforderung.

Durch die Durchsicht der Beispielberichte werden Sie schnell merken, ob diese Ihren internen sowie externen Bedürfnissen entsprechen.

Wonach ist zu suchen?

Es gibt eine große Auswahl an Berichtsoptionen für Pentests, aber es gibt einige Punkte, die immer vorhanden sein sollten:

- Die **Management Summary** beschreibt den Überblick über das Engagement auf hoher Ebene. Dieses wird bereitgestellt für das Management und bietet nicht-technische Schwerpunkte zur Überprüfung der Ergebnisse.
- Die **Schwachstellenübersicht** ist sowohl für Führungskräfte als auch für Pentester. Diese sollte somit auch eine zusammenfassende Abhilfe für jedes damit verbundene Problem enthalten.
- Die **Details zu Schwachstellen** sind eine risikopriorisierte technische Aufschlüsselung der Funde nachdem **CVSS 3.0** Standard. Die Analyse sollte auch beinhalten, wie die Schwachstelle ausgenutzt wurde.
- **Detaillierte Behebungs-Schritte** sind Teil jeder Schwachstellen-Beschreibung und sollten mögliche Behebungen für einen bestimmten Fehler skizzieren.

Erkenntnis

Fordern Sie einen Beispielbericht von jedem potenziellen Dienstleister an. Gute Anbieter werden immer Muster von jeder Art von angebotenem Pentest für Sie zur Überprüfung bereithalten.

04

Werden kostenlose Nachtests durchgeführt?

Fokus: Umfang

Warum ist das wichtig?

Das Ziel eines Pentests sollte neben der Bewertung der Sicherheit einer Anwendung oder Infrastruktur, auch die Verbesserung eben dieser sein. Ob die von Ihnen, auf Basis des Abschlussberichts, getroffenen Gegenmaßnahmen den gewünschten Effekt haben, lässt sich in einer anschließenden **Validierungsphase** bewerten.

Bei einem Nachtest werden alle während des Pentests identifizierten Schwachstellen erneut überprüft. Die Ergebnisse eines solchen Nachtests werden in den Abschlussbericht eingearbeitet und dieser wird Ihnen in einer aktualisierten Version zur Verfügung gestellt. Mit einem solchen Bericht können Sie auch externen Beteiligten belegen, dass ihr Unternehmen entsprechende Gegenmaßnahmen getroffen hat.

Wonach ist zu suchen?

Wenn ein Dienstleister einen effizienten Dokumentationsprozesse etabliert hat und identifizierte Schwachstellen, mit sogenannten **Proof-of-Concepts**, also kleinen Beispielen für die Ausnutzung der Schwachstelle, versieht, fällt der Zusatzaufwand nur sehr gering aus. Aus diesem Grund werden Nachtests von einigen führenden Anbietern als kostenlose Ergänzung zu einem Pentest angeboten.

Sollte ein Anbieter Ihnen diese Leistung zusätzlich in Rechnung stellen, deutet dies meist auf ineffiziente Prozesse oder Fehlkalkulationen hin.

Erkenntnis

Ein Nachtest ist ein wichtiger Bestandteil eines Pentests. Der von Ihnen gewählte Dienstleister sollte Ihnen diese Leistung nicht zusätzlich in Rechnung stellen.

05 Gibt es Kompetenz im Bereich Security Engineering?

Fokus: Technische Expertise

Warum ist das wichtig?

Gefundene Schwachstellen und die daraus resultierenden Sicherheitsprobleme sollten entsprechend der Maßnahmenempfehlungen behoben werden. Security Engineering bildet den Übergang zwischen Softwareentwicklung und IT-Sicherheit. Erfahrene Security Engineers können Sie im hektischen und schnelllebigen Entwicklungsalltag bei der Behebung von in Pentests identifizierten Schwachstellen, sowie auch schon während des Entwicklungsprozesses bei der Implementierung von sicherheitskritischen Programmteilen unterstützen.

Wonach ist zu suchen?

Auftragnehmer, ohne eigene IT-Sicherheitsabteilung oder Security Engineers, können auf erfahrene Berater zurückgreifen, sollte es bei der Behebung von Schwachstellen zu Engpässen oder Schwierigkeiten kommen.

Erkenntnis

Das Pentest-Dienstleister Schwachstellen nicht nur identifizieren, sonder auch bei der Behebung dieser unterstützen können, sollte bei der Auswahl berücksichtigt werden.

06

Werden kontinuierliche Sicherheitsprozesse angeboten?

Fokus: Technische Expertise

Warum ist das wichtig?

Kontinuierliche Sicherheit bedeutet, dass in modernen Entwicklungsumgebungen (**DevOps**, **NoOps**, etc.) Sicherheitsprozesse nicht nur punktuell, sondern fest in die Softwareentwicklung und Systemintegration eingebunden werden. Pentests sind nur Momentaufnahmen und bei kurzlebigen Software-Artefakten schnell überholt. Automatisierte Sicherheit in der Entwicklungsumgebung bietet nicht den gleichen Sicherheitsstandard wie ein vollwertiger Pentest, jedoch kann so dauerhaft ein befriedigendes Maß an Sicherheit gewährleistet werden.

Wonach ist zu suchen?

Auch bei der Suche nach einem Anbieter für manuelle Pentests sollte die Qualifikation im Bereich der automatisierten Sicherheit abgefragt werden. So kann sichergestellt werden, dass langfristige Zusammenarbeit möglich ist und tiefergehende Kompetenz existiert. Weiterhin ist gewährleistet, dass der Anbieter sich am Puls der Zeit befindet und für zukünftige Projekte im Bereich DevOps Security genutzt werden kann.

Erkenntnis

Fundierte Kenntnisse und Angebote im Bereich der automatischen Sicherheit bieten eine hervorragende Erweiterung des Portfolios eines Pentestdienstleisters und sollten während Ihrer Auswahl berücksichtigt werden.

Fazit

Die Suche nach einem Anbieter für Penetrationstests und deren Überprüfung kann entmutigend sein, aber die obigen Fragen werden Sie durch den Prozess führen.
Wenn Sie die oben genannten Fragen an jeden Anbieter stellen, haben Sie die Möglichkeit, eine fundierte Entscheidung zu treffen - es ist keine technische Expertise erforderlich!

Vertrauen, technische Expertise, die Qualität des Personals und die Tiefe der Berichterstattung sind einige der wichtigsten Aspekte bei der Auswahl eines Pentest-Anbieters. Dies sind jedoch nicht die einzigen Details, die berücksichtigt werden sollten. Auch die Preisstruktur, potenzielle frühere Referenzen und die Erfahrung in der Branche können wichtige Überlegungen sein.

Formulieren Sie zusätzlich zu den hier gestellten Fragen Ihre eigenen Fragen und stellen Sie sicher, dass Sie sich bei dem von Ihnen gewählten Anbieter wohlfühlen - Ihre Sicherheit ist zu wichtig, als dass Sie damit spielen könnten!

Über uns

Unsere erfahrenen Sicherheits-Experten helfen Ihnen, Ihre Anwendungen und Systeme zu schützen und progressive Sicherheitskonzepte umzusetzen.

Das visionäre Denken treibt uns zum Erreichen immer neuer Meilensteine an und sorgt für die nachhaltige Entwicklung des Unternehmens. Besonders im Bereich der IT-Sicherheit glänzen wir durch neue Ideen, Kreativität und sorgfältiger Arbeit. In diesem Bereich bieten wir vollumfängliche Beratungen an.

turingpoint.

hello@turingpoint.de
+(49) (040)
52477883
turingpoint.de