Schwachstellen dank crowdsourced Pentesting im Griff

Mit Penetration Tests, kurz Pentests, lassen sich Schwachstellen in Applikationen und Systemen aufdecken. Patrick Michel, Principal Consultant beim IT-Security-Distributor BOLL, schildert die Vorteile von Penetration Tests, die durch eine globale Ethical-Hacker-Community durchgeführt werden.

Wie werden Penetration Tests klassischerweise durchgeführt?
Patrick Michel: Ein Unternehmen, das seine Systeme auf offene Schwachstellen hin untersuchen will, erteilt einem spezialisierten Anbieter den Auftrag, bestimmte Anwendungen oder Systeme durch fingierte Hackerattacken zu testen. Diese Testform kommt einer realen Bedrohung am nächsten. Ein Pentesting-Service ist ein Realitätscheck, um getätigte Security-Investitionen in Technik und Menschen zu prüfen und um danach Verbesserungen durchzuführen. Anbieter traditioneller Penetration-Testing-Services agieren dabei aber mit ziemlich begrenzten Ressourcen. Gute Leute sind Mangelware.

Gibt es bessere Methoden?
Die Alternative respektive eine starke Ausweitung der eingesetzten Testing-Ressourcen ist Crowdsourcing. Dabei setzt der Pentesting-Anbieter nicht auf eine begrenzte Belegschaft aus eigenen Mitarbeitenden, sondern auf eine globale Community von gutwilligen Hackern, die als Freelancer im Auftragsverhältnis testen. Damit stehen massiv mehr Ressourcen zur Verfügung, die global verteilt sind und die unterschiedlichsten Skills aufweisen. Dies ist wichtig, denn die Sicherheitslandschaft ist heute derart komplex, dass sich auch Hacker – egal, ob kriminell oder «White Hat» – spezialisieren.

Community klingt gut, aber wie lässt sich garantieren, dass keine «schwarzen Schafe» die Pentests für echte Attacken ausnutzen?
Zunächst durch strenge Aufnahmeverfahren und das Screening der Kandidaten mit umfassenden Hintergrundchecks. Zweitens muss das Angebot für die Hacker attraktiv sein. Weiter werden die Aktivitäten der Pentester überwacht. Gerade wenn es darum geht, vom Internet her nicht erreichbare Systeme zu prüfen, kann das garantiert werden. Doch eine 100-prozentige Garantie gibt es natürlich nie. Das kann auch eine kleinere lokale Pentesting-Firma nicht bieten. Doch was sind denn die Alternativen? Wer sich nicht prüfen lässt, überlässt das Feld den Bad Guys und weiss nicht, wo seine Security steht. Das Risiko ist deshalb viel grösser.

Patrick Michel, Principal Consultant, BOLL

Ist communitybasiertes Pentesting ein theoretisches Modell, oder gibt es das in der Praxis?
Es gibt einen Anbieter, der das Modell seit mehreren Jahren erfolgreich anwendet und seine Dienste übrigens über Channelpartner verkauft. Er heisst Synack und kann auf über 1600 akkreditierte Ethical Hacker zurückgreifen, das sogenannte «Red Team» – dies gestützt durch eine cloudbasierte Plattform, über die sämtliche Tests laufen. Die Hacker arbeiten immer über diese Plattform. Zudem wird alles aufgezeichnet, was die Tester tun. Dadurch herrscht ein Höchstmass an Transparenz.

Welche Vorteile hat ein Synack-Kunde von der Plattform?
Neben der kontrollierten Sicherheit und den eingesetzten grösseren Ressourcen haben die Kunden stets den Überblick über die Aktivitäten der Spezialisten. Dank der Plattform sieht man sofort, wenn eine Schwachstelle entdeckt wurde, und kann sie zeitnah beheben. Das lange Warten auf einen Report, der bei anderen Anbietern erst nach Abschluss aller Tests vorliegt, entfällt. Zudem besteht die Möglichkeit, die gefundenen Schwachstellen direkt in einen systembasierten Security-Management-Prozess zu integrieren.

Heute werden Applikationen vermehrt agil entwickelt mit vielen Releases. Da reicht doch ein zeitlich begrenzter Pentest nicht aus.
Richtig. Genau deshalb bietet Synack auch ein permanentes Testen während 365 Tagen im Jahr. Dabei achtet Synack auch darauf, dass immer wieder andere Spezialisten zum Einsatz kommen. Dies ist nur mit einer grossen Zahl von Ethical Hackern möglich. Ein kleiner Anbieter kann so etwas nicht bieten.

Hand aufs Herz: Lohnen sich Pentests überhaupt?
Die Entscheidung ist einfach: Entweder man lässt nicht testen und wird von Kriminellen gehackt, oder man arbeitet mit Pentests im kontrollierten Umfeld und versucht so, die Risiken zu reduzieren. Dann ist man unmittelbar an der Realität und weiss, wo die Verwundbarkeiten liegen. Bei der immer stärkeren Abhängigkeit von digitalen Prozessen ist dies ein absolutes Muss. Wer dies unterschätzt, läuft Gefahr, das Versäumnis irgendwann teuer zu bezahlen.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch