AVENIQ

Das Maximum aus Ihrem Penetration Test herausholen

aveniq.ch →

Die richtigen Ziele setzen

Um den Nutzen eines Penetrationtests zu maximieren, ist es unerlässlich, dass der Test auf Ihre spezifischen Risiken zugeschnitten ist. Daher ist die Bewertung der besonderen Bedrohungen für Ihre Organisation und die zu testende Umgebung eine wichtige Voraussetzung, um sicherzustellen, dass ein Penetration Test auf Ihre Risiken und Kontrollen abgestimmt ist. Das bedeutet, nicht nur zu verstehen, welche Assets Sie haben, sondern auch, wie Angreifer diese realistischerweise ins Visier nehmen könnten.

Berücksichtigen Sie die Art des Tests und den Reifegrad Ihrer Organisation. Wenn Ihre Organisation bereits ein hohes Sicherheitsniveau hat und beispielsweise regelmässig den Perimeter überprüft sowie über ein solides E-Mail-Gateway verfügt, bringt es möglicherweise wenig Mehrwert, einen Angreifer mit geringem technischen Reifegrad zu simulieren.

Das Ergebnis wird vorhersehbar sein: Externe Scan-Aktivitäten werden blockiert und Phishing-E-Mails werden ohne Auswirkungen abgefangen. Infolgedessen wird der Wert des durchgeführten Tests minimal bis nicht vorhanden sein. In solchen Fällen ist ein Purple Teaming oder Red Teaming weitaus angemessener, um Ihre bestehenden Abwehrmassnahmen zu testen und an ihre Grenzen zu bringen.

Wenn Sie hingegen noch keine erste Bewertung durchgeführt haben und gerade ein Cybersicherheitsprogramm aufbauen, wäre es hingegen wenig sinnvoll, viel Geld für ein Red Team auszugeben, das Ihre nicht vorhandenen Abwehrmassnahmen testet und eine entsprechend limitierte Aussage treffen kann. Hier wäre es weitaus geeigneter und budgetschonender, mit einem Active Directory Audit oder einem externen Penetrationstest zu beginnen, um sich einen ersten Überblick zu verschaffen, wie exponiert Sie derzeit sind.

Exemplarische Relation verschiedener Tests und Security-Maturität

Testumfang (Scope) sauber definieren

Die Definition des Testumfangs (Scoping) ist ein entscheidender Teil des Prozesses. In dieser Phase kann Ihr Penetration-Test-Partner Ihre Anforderungen, Ziele und Rahmenbedingungen verstehen und darauf basierend einen Vorschlag unterbreiten, der bestmöglich zu Ihrer Ausgangslage passt. Ein übereilt oder unklar definierter Prüfrahmen (Scope) führt häufig zu falschen Erwartungen und enttäuschenden Ergebnissen.

Wenn Sie bei irgendeinem Aspekt unsicher sind, ist diese Phase eine perfekte Gelegenheit, Ihren Anbieter um Unterstützung bei diesem Prozess zu bitten. Idealerweise sollten Sie Ihrem Anbieter beschreiben, warum Sie einen Penetration Test benötigen, welche Assets getestet werden müssen und welche spezifischen Ziele Sie erreichen möchten. Ein guter Anbieter wird zuhören und auf Ihre Anforderungen eingehen, um eine massgeschneiderte Lösung für Sie zu finden, anstatt Ihnen ein Standardangebot zu «verkaufen».

Hier findet der Grossteil des Erwartungsmanagements statt und es wird sichergestellt, dass ein gemeinsames Verständnis darüber entsteht, was getestet werden muss und welche Fragen beantwortet werden sollen. Es lohnt sich auch, etwaige Einschränkungen im Voraus zu besprechen – sei es Testzeitfenster, sensible Systeme, die besondere Sorgfalt erfordern, oder Compliance-Anforderungen, die erfüllt werden müssen.

Den grössten Mehrwert erzielen

Das Ziel eines Penetration Tests besteht nicht darin, die Arbeit Ihres internen IT-Teams zu diskreditieren oder herabzusetzen, sondern die Sicherheitslage Ihrer Organisation zu verbessern. Die Ergebnisse des Penetration Tests werden Ihrem IT-Team helfen, ihre Aufgaben effektiver zu erfüllen. Diese Perspektive intern zu kommunizieren, hilft dabei, eine kollaborative statt eine konfrontative Dynamik aufzubauen.

Indem Sie die richtigen Voraussetzungen für den Penetration Test schaffen, maximieren Sie den Nutzen für Ihre Organisation. Zum Beispiel durch:

- Die richtigen Personen darüber zu informieren, dass ein Penetration Test stattfindet, um ein aktives Blockieren des Testers während der Bewertung zu vermeiden
- Unterstützung während des Tests zu bieten – die erfolgreichsten Engagements sind kollaborativ
- Whitelisting auf etwaigen WAFs/IPS-Systemen
- Bereitstellung vorheriger Penetration-Test-Berichte, falls verfügbar

Feedback

Ein guter Anbieter wird eine offene Kommunikation mit Ihnen pflegen und während dem Test Feedback geben. Falls während des Tests eine kritische Schwachstelle entdeckt wird, kann der Tester Sie sofort informieren, sodass Sie diese so schnell wie möglich beheben können. Diese Echtzeitkommunikation ist besonders wichtig bei Schwachstellen, die ein aktives Risiko für Ihre Umgebung darstellen.

Projektabschluss

Wir bieten unseren Kunden immer ein Debriefing-Gespräch an, um die wichtigsten Ergebnisse zu besprechen, eine Diskussion zu ermöglichen und eventuelle Fragen zu klären. Dies ermöglicht es Ihnen, eine professionelle Einschätzung vom Tester zu erhalten und ein Gefühl für die allgemeine Sicherheitslage der getesteten Assets zu bekommen.

Abschliessende Gedanken

Was den Erfolg eines Tests wirklich bestimmt, liegt auf der menschlichen Seite – Scoping, Erwartungsmanagement und Kommunikation. Der technisch gründlichste Test wird ins Leere laufen, wenn die Ergebnisse nicht verstanden oder kein gemeinsames Verständnis geschaffen wurde.

Unsicher über Ihre Sicherheitslage? Lassen Sie uns gemeinsam Ihre individuelle Security Journey gestalten und auf das nächste Level bringen.

Pascal Brunner
Teamlead Penetration Testing
Pascal.Brunner@aveniq.ch
+41 58 059 42 95