HADRIAN

EBOOK

Mit den Augen eines Hackers

Automatisierung der offensiven Sicherheit für externe Assets

Inhaltsübersicht

01	Einführung	001
02	Was ist Offensive Sicherheit?	002
03	Warum sollte man sich auf die externen Angriffsflächen konzentrieren?	003
04	Phasen der offensiven Sicherheit	004
05	Offensive Sicherheit automatisieren	005
06	Ansätze für offensive Sicherheit im Vergleich	006
07	Wert der automatisierten offensiven Sicherheit	007
08	Vorteile für die wesentlichen Interessensvertreter	008
09	Über Hadrian	009

Einführung

Die externe "Hacker-Perspektive" ist für eine robuste Cybersicherheit unerlässlich, da sie ein Maß an Kontrolle und Einblick bietet, die interne Teams oft nicht besitzen. Interne Sicherheitsexperten sind zwar für die Aufrechterhaltung und Stärkung des Schutzes eines Unternehmens von entscheidender Bedeutung, doch sind sie oft durch institutionelles Wissen, begrenzte Sichtweisen und Vertrautheit mit dem System gebunden, was ungewollt zu ‘Blind Spots’ führen kann. Hacker hingegen können sich einem System ohne vorgefasste Meinungen oder Einschränkungen nähern und simulieren reale Gegner, die genau diese Schwächen ausnutzen.

Ein wichtiger Aspekt dieser externen Perspektive ist die Fähigkeit, Schwachstellen aus der Sicht eines Angreifers zu erkennen. Hacker folgen nicht nur bekannten Taktiken, sie passen sich an, sind innovativ und denken kreativ darüber nach, wie sie die Abwehrmaßnahmen umgehen können. Durch die Simulation ihrer Vorgehensweise können Unternehmen Schwachstellen aufdecken, die von internen Teams, die sich auf eher routinemäßige oder theoretische Schwachstellen konzentrieren, sonst übersehen würden. Letztlich ermöglicht eine externe Perspektive einen umfassenderen Ansatz für die Cybersicherheit - einen Ansatz, der die dynamische, sich ständig verändernde Natur von Angriffen in der realen Welt widerspiegelt.

Was ist Offensive Sicherheit?

Selbst die beste Sicherheit kann umgangen werden, wenn sie nicht ordnungsgemäß implementiert oder kontinuierlich getestet wird. Offensive Sicherheit bezieht sich auf den proaktiven Ansatz, das Verhalten, die Taktiken und Techniken eines Angreifers zu simulieren, um die Sicherheitslage eines Unternehmens zu bewerten und zu testen.

Im Gegensatz zur traditionellen defensiven Sicherheit, die sich auf den Schutz von Systemen und die Reaktion auf Angriffe konzentriert, kehrt die offensive Sicherheit die Gleichung um. Sie versetzt Sicherheitsexperten in die Rolle des "Hackers", der absichtlich versucht, die Verteidigungsmaßnahmen des Unternehmens zu durchbrechen, um Lücken und Schwachstellen aufzudecken.

Ziel der offensiven Sicherheit ist es, die Strategien realer Gegner nachzuahmen - seien es externe Hacker, Insider-Bedrohungen oder sogar staatliche Akteure -, damit Unternehmen Schwachstellen erkennen und beheben können, bevor sie bei einem tatsächlichen Angriff ausgenutzt werden.

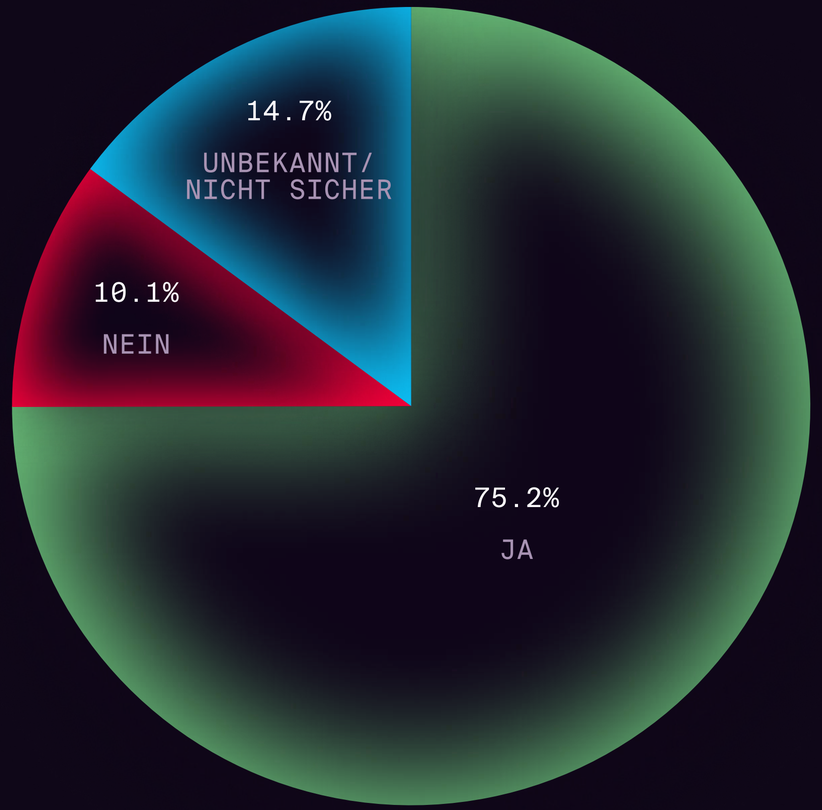
7/10

der Unternehmen haben einen Angriff erlebt, der auf ein unbekanntes, nicht verwaltetes oder schlecht verwaltetes externes Asset abzielte.[1]

69%

der Unternehmen geben an, dass ihr Sicherheitsansatz reaktiv und auf Vorfälle ausgerichtet ist.[2]

Führt ein unbekanntes Risiko dazu, dass Sie offensive/proaktive Sicherheitspraktiken verstärken?[3]



[1] ESG, Security Hygiene and Posture Management (2022) | [2] Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019) |
[3] SANS, Building a Resilient Offensive Security Strategy (2023)

Warum sollte man sich auf die externen Angriffsflächen konzentrieren?

Ein externer Angreifer könnte eine Schwachstelle oder einen Schwachpunkt ausnutzen, den interne Teams nicht vorhergesehen oder als zu geringes Risiko eingestuft haben, um ihm Priorität einzuräumen. Dies macht die Hacker-Perspektive zu einem unschätzbaren Werkzeug, um die Stärke der Sicherheitsabwehr zu überprüfen und sicherzustellen, dass sie gegen aktuelle und sich entwickelnde Bedrohungen widerstandsfähig ist.

Angreifer sind schneller innovativ, als Verteidigungsmaßnahmen entwickelt werden können. Die einzige Möglichkeit, einen Schritt vorruas zu sein, besteht darin, die Denkweise und die Methoden derjenigen, die sie auszunutzen versuchen, ständig zu hinterfragen. Ohne diesen Outside-in-Ansatz laufen Unternehmen Gefahr, die Raffinesse und Hartnäckigkeit moderner Bedrohungen zu unterschätzen und dadurch kritische Lücken in ihrer Sicherheitsstrategie zu hinterlassen.

Checkliste für die Hacker-Perspektive:

- ✓ Haben wir alle Zugangspunkte zu unserem Netz und unseren Systemen erfasst?
- ✓ Kennen wir alle Assets innerhalb unserer Umgebung, einschließlich Schatten-IT und Cloud-Dienste?
- ✓ Werden unsere nach außen gerichteten Assets (Websites, APIs, Cloud-Plattformen) kontinuierlich überwacht?
- ✓ Ziehen wir Drittanbieter und Auftragnehmer in Betracht, die neue Risiken in unser Umfeld einbringen könnten?
- ✓ Wann haben wir das letzte Mal ein Red Team oder einen Penetrationstest durchgeführt? Hat dieser alle Aspekte unserer Umgebung abgedeckt?

Phasen der offensiven Sicherheit

Die Hacker-Perspektive wird durch die Anwendung einer offensiven Sicherheitsmethodik offengelegt.

Aufklärungsarbeit

Die Aufklärung, der erste Schritt für offensive Sicherheit, konzentriert sich auf das Sammeln von Informationen über die Systeme, Netzwerke und die Organisationsstruktur des Ziels. In dieser Phase werden potenzielle Angriffsvektoren und Schwachstellen durch die Darstellung von Assets und Beziehungen identifiziert, so dass Angreifer die anfälligsten Einstiegspunkte ermitteln können.

Kontextualisierung

In dieser Phase werden die entdeckten Systeme systematisch untersucht, um wichtige Informationen wie aktive Hosts, offene Ports, laufende Dienste und Technologie-Stacks zu extrahieren. Mithilfe von Fingerprinting-Techniken identifizieren die Angreifer die zugrunde liegenden Systeme und Schwachstellen und können so Schwachstellen in der Umgebung ausfindig machen.

Validierung

In dieser Phase werden gezielt Schwachstellen ausgenutzt, um unbefugten Zugang zu erlangen oder Privilegien zu erweitern. Ziel ist es, zu prüfen, ob diese Schwachstellen ausgenutzt werden können, um die Ziele des Angreifers zu erreichen, z. B. den Zugriff auf sensible Daten oder das Eindringen in interne Netzwerke Gleichzeitig wird die Wirksamkeit der Sicherheitskontrollen und die Reaktion auf Vorfälle bewertet.

Prioritätensetzung

Nachdem ausnutzbare Schwachstellen identifiziert wurden, werden im Rahmen der Priorisierung der Schweregrad und das Risiko dieser Schwachstellen für Systeme, Netzwerke und Anwendungen bewertet. In dieser Phase wird festgelegt, welche Probleme auf der Grundlage der potenziellen Auswirkungen zuerst angegangen werden sollten.

Wiederherstellung

In der letzten Phase, der Wiederherstellung (Remidation), werden die Ergebnisse in einem Bericht zusammengefasst, auf den das Unternehmen reagieren kann. Der Bericht enthält den Angriffspfad, die ausgenutzten Schwachstellen und Empfehlungen für Abhilfemaßnahmen und dient sowohl als unmittelbare Anleitung für Korrekturmaßnahmen als auch als strategischer Fahrplan für langfristige Sicherheitsverbesserungen.

Offensive Sicherheit automatisieren

Automatisierung und KI können die offensive Sicherheit in jeder Phase verbessern

Aufklärungsarbeit

KI sammelt und analysiert schnell große Datenmengen von externen Assets, Netzwerken und Systemen und automatisiert Aufgaben, wie: Asset-Erkennung, Datenerfassung und Zusammenstellung von Bedrohungsdaten.

Das Ergebnis: Erhöhte Transparenz der externen Angriffsfläche und Ausweitung der Tests auf alle Assets.

Kontextualisierung

Die Automatisierung identifiziert Live-Hosts, offene Ports, Dienste und Technologien schneller und präziser und setzt sie mit bekannten Exploits und Angriffstechniken in Beziehung, was einen tieferen Einblick in potenzielle Risiken ermöglicht.

Das Ergebnis: Verbesserte Genauigkeit bei der Erkennung von Bedrohungen durch Identifizierung aller potenziellen Schwachstellen.

Validierung

Die Automatisierung simuliert Angriffe, um ausnutzbare Schwachstellen zu validieren, während die KI raffinierte Taktiken der Angreifer nachahmt und so die Wirksamkeit der Sicherheitskontrollen testet.

Das Ergebnis: Gewährleistung realistischer Tests von Sicherheitsmaßnahmen und Vermeidung von Fehlalarmen.

Prioritätensetzung

KI hilft bei der Einstufung von Schwachstellen auf der Grundlage der potenziellen Auswirkungen, der Ausnutzbarkeit und des organisatorischen Risikos, so dass sich Sicherheitsteams auf die wichtigsten Probleme konzentrieren können.

Das Ergebnis: Bessere Ressourcenzuweisung durch Ermittlung der am stärksten gefährdeten Stellen.

Wiederherstellung

Die Automatisierung generiert umsetzbare Berichte mit maßgeschneiderten Empfehlungen und verfolgt den Fortschritt bei den Korrekturen, während die KI die Abhilfestrategien auf der Grundlage des organisatorischen Kontexts und der Ressourcenbeschränkungen optimiert.

Das Ergebnis: Bessere Ressourcenzuweisung durch Ermittlung der am stärksten gefährdeten Stellen.

Ansätze für offensive Sicherheit im Vergleich

Die Anwendungsfälle und Stärken jedes Ansatzes sind unterschiedlich und sollten für ganzheitliche Sicherheitstests überlagert werden

	Scannen auf Schwachstellen	Penetrationstests	Red Teaming	Automatisierte offensive Sicherheit
Umfang	Bekannte Assets	Kritische Infrastrukturen	Zielgerichtet	Alle externen Assets
Geschwindigkeit	Stunden	Tage bis Wochen	Wochen bis Monate	Protokoll
Raffinesse	Grundlegend	Hoch	Hoch	Mittel
Frequenz	Geplant	Vierteljährlich bis jährlich	Jährlich	Ereignisbezogen
Werkzeugbau	Automatisiert	Gemischt	Handbuch	Automatisiert
Kosten	Niedrig	Mittel	Hoch	Niedrig
Ziel	Tests auf bekannte Schwachstellen und Konformitätsprobleme	Identifiziert Schwachstellen in bestimmten Systemen oder Anwendungen	Bewertung der allgemeinen Sicherheitsmaßnahmen und der Resilienz	Enthüllt die Hacker-Perspektive für proaktive Abhilfemaßnahmen

Wert der automatisierten offensiven Sicherheit

Die Denkweise eines Hackers zeigt, wie reale Angriffe Anwendungen und Infrastrukturen gefährden können. Automatisierte offensive Sicherheit ermöglicht es Unternehmen, diese Perspektive zu verstehen und Bedrohungen proaktiv zu entschärfen.

Hadrian deckt ausnutzbare Schwachstellen auf, indem es kontinuierlich Bedrohungen für Ihren gesamten externen Angriff bewertet und dabei die gleichen Techniken und Verhaltensweisen wie Hacker anwendet.

Im Gegensatz zu statischen Penetrationstests bietet Hadrian einen dynamischen, sich entwickelnden Sicherheitsansatz, der sich an Ihre sich verändernde Angriffsfläche anpasst. Mit automatisierten Erkenntnissen und der Priorisierung kritischer Risiken versetzt Hadrian Sicherheitsteams in die Lage, Bedrohungen immer einen Schritt voraus zu sein und ihre Verteidigung zu verstärken, bevor Angriffe stattfinden.

10x SICHTBARKEIT DER KRITISCHEN RISIKEN	Verschaffen Sie sich in Echtzeit einen Überblick über alle Assets und Schwachstellen in Ihrer digitalen Angriffsfläche. Die 24/7/365-Analyse von Hadrian hält Sie ständig auf dem Laufenden und minimiert das Fenster der Verwundbarkeit.
10 STUNDEN EINSPARUNG PRO WOCHE IM DURCHSCHNITT	Konzentrieren Sie sich auf ausnutzbare Risiken und eliminieren Sie falsch-positive Ergebnisse durch gründliche Penetrationstests. Die vollautomatischen Bewertungen von Hadrian sind nahtlos und mit Bedrohungsdaten angereichert.
80% VERKÜRZUNG DER DURCHSCHNITTLICHEN ZEIT BIS ZUR ABHILFE	Beschleunigen Sie die Reaktionszeit und sorgen Sie für eine schrittweise Veränderung der Sicherheitslage. Hadrian löst Workflows aus und orchestriert sie, um Abhilfemaßnahmen zu optimieren und Angriffe von Bedrohungsakteuren zu verhindern.

Vorteile für die wesentlichen Interessensvertreter

Interessensvertreter	Nutzen	Verbesserte Bereiche
CISO	CISOs erhalten einen tieferen Einblick in die Sicherheitslage des Unternehmens und können so fundiertere Entscheidungen zum Risikomanagement treffen.	▪ Geringere Risikoexposition ▪ Verbesserte Berichterstattung auf Vorstandsebene ▪ Bessere Ressourcenzuweisung
Penetrationstester	Durch die Automatisierung werden zeitaufwändige Aufgaben wie das Scannen von Schwachstellen und die Datenanalyse rationalisiert, so dass sich die Tester auf die Probleme konzentrieren können, die höchste Priorität haben.	▪ Schnelles Testen von Zero-Day-Exploits ▪ Automatisierung von zeitaufwändigen Aufgaben ▪ Umsetzbare Empfehlung
SOC-Team	Für das SOC-Team ist es hilfreich, sich in die Denkweise von Hackern hineinzuversetzen, um fortschrittliche Angriffsmethoden zu erkennen und die Erkennungsfunktionen zu optimieren.	▪ Schnellere Erkennung von Risiken ▪ Weniger falsch-positive Ergebnisse ▪ Geringere Behebungszeit
Entwicklungsteams	Entwickler können Sicherheit nahtlos in den Bereitstellungsprozess integrieren, was zu sichereren Anwendungen in der Produktion führt.	▪ Weniger Schwachstellen in der Produktion ▪ Schnelleres Patching nach der Veröffentlichung ▪ Geringeres Risiko von Markenschäden
Abteilung Finanzen	Das Finanzteam kann die potenziellen finanziellen Auswirkungen von Cyber-Bedrohungen besser quantifizieren und bei der Priorisierung von Investitionsentscheidungen helfen.	▪ Deutlichere finanzielle Auswirkungen von Cyberrisiken ▪ Verbesserte Budgetierung von Investitionen ▪ Besserer ROI für Sicherheitsausgaben

Über Hadrian

Hadrian revolutioniert die offensive Sicherheit durch Automatisierung und ermöglicht es Sicherheitsteams, schneller zu arbeiten und mühelos zu skalieren. Um Bedrohungen aufzudecken, testet unsere autonome Orchestrator-KI kontinuierlich, um die mit dem Internet verbundenen Assets umfassend zu bewerten. Die hochmoderne Technologie ist cloudbasiert, komplett agentenlos und wird von dem Ethical-Hacker-Team von Hadrian ständig aktualisiert und verbessert.

Marktführer vertrauen uns

NBC	amadeus	CRÉDIT AGRICOLE
AUTODESK	ABN·AMRO	London Business School
RITUALS...	SIEMENS energy	BLINQX

Orchestrator AI