TRIPWIRE IP360

Risiko- und Schwachstellenmanagement der Enterpriseklasse

Die effektivsten Lösungen für das Schwachstellenmanagement unterstützen Kunden bei der Priorisierung ihrer Sicherheitsinvestitionen. Tripwire® IP360™ ist eine erstklassige Lösung für das Schwachstellenmanagement, mit der Kunden ihre Ressourcen strategisch dort einsetzen können, wo das größte Risiko besteht und bei einem Cyberangriff der größte Schaden entstehen könnte. Dadurch sparen sie Kosten und stärken ihren Sicherheitsstatus.

Highlights

- Profitieren Sie von einer proaktiven Erkennung und Risikoeinschätzung von Ressourcen im Netzwerk, On-Premises oder in der Cloud.
- Reduzieren Sie das Geschäftsrisiko durch eine effektive, praxistaugliche Bewertung und Priorisierung von Schwachstellen.
- Sorgen Sie mit skalierbaren, fehlertoleranten Scan-Funktionen dafür, dass Ihnen keine Bedrohungen und Schwachstellen entgehen, und vermeiden Sie kostspielige Verzögerungen.
- Behalten Sie durch automatisierte, netzwerk- und agentbasierte Scans sämtliche Ressourcen und Aktivitäten im Blick.
- Unterstützen Sie mit Funktionen zur Identifizierung und Analyse von Containern Ihre DevOps-Teams.

Unsere Lösung baut auf einer skalierbaren Architektur auf, die eine schnelle, zuverlässige und präzise risikobasierte Schwachstellenanalyse fördert. Außerdem nutzt sie branchenführende Funktionen für die Schwachstellenbewertung und integrierte Bedrohungsdaten von Endpunkten, um eine zeitnahe Reaktion auf selbst ausgefeilte neue Bedrohungen zu ermöglichen.

Was Tripwire IP360 auszeichnet:

- Umfassende Funktionen zur Erkennung und Profilerstellung sämtlicher Ressourcen im Netzwerk, On-Premises und in der Cloud.
- Extrem skalierbare Architektur, die bei Scans und der Risikobewertung weder die Leistung noch die Verfügbarkeit des Netzwerks beeinträchtigt.
- Moderne Tools zur Bewertung und Priorisierung der größten Geschäftsrisiken.
- Von Tripwire Enterprise überwachte Ressourcen können wenn nötig mit den entsprechenden Schwachstellendaten getaggt werden, sodass Kunden die größten Risiken im Blick haben.

Flächendeckende Transparenz für Ihr Netzwerk

Mit Tripwire IP360 behalten Sie stets den Überblick über Ihr gesamtes Netzwerk, On-Premises und in der Cloud, inklusive aller Geräte (und deren Betriebssysteme), Anwendungen und Schwachstellen. Das expertengeführte Tripwire Vulnerability and Exposure Research Team (VERT) aktualisiert IP360 kontinuierlich mit neuen Bedrohungssignaturen, damit besonders auf große Organisationen abzielende Angriffe frühzeitig erkannt und abgewehrt werden können.

Mit dem einzigartigen, anwendungsbasierten Ansatz von Tripwire IP360 können Sie Ihre Schwachstellensuche sogar nach bestimmten Betriebssystemen, Anwendungen, Hosts oder Services filtern. Dadurch reduzieren Sie den Umfang der Scans auf das absolut Nötigste und vermeiden eine Beeinträchtigung der Anwendungsleistung.

Außerdem lässt sich mit IP360 die Ressourcenerkennung und -bewertung individualisieren. Zum Beispiel können Sie Schwachstellenscans dynamisch skalieren, um beliebig breite oder fokussierte Abschnitte Ihrer Netzwerkinfrastruktur zu überprüfen. Ressourcen auf Endpunkten mit dynamischer IP-Adresse, wie Laptops und Geräten, die nur wahlweise mit dem Netzwerk verbunden werden, können mit agentbasiertem Schwachstellenmanagement gescannt werden. Für Ressourcen, die in der Cloud gespeichert und genutzt werden, können vorautorisierte, automatisierte Scan-Funktionen in AWS und Azure eingesetzt werden. Und Organisationen, die ein DevOps-Modell sicher umsetzen wollen, können mit Tripwire IP360 sowohl aktive als auch inaktive Container identifizieren und analysieren.

Smarte Priorisierung

Tripwire IP360 stellt Ihnen umfassende, praxistaugliche Daten über die Hosts auf Ihrem Netzwerk zur Verfügung. Dabei werden Schwachstellen schnell erkannt und mit einer Bewertung von 1–50.000 versehen, sodass Ihre IT- und Sicherheitsteams stets wissen, welche Bereiche und Ressourcen am meisten gefährdet sind und den größten Schaden nehmen könnten. Das erlaubt Ihren Teams und anderen Sicherheitsverantwortlichen im Unternehmen, Zeit und Investitionen effektiv zu priorisieren.

Die Tripwire VERT-Experten führen eine objektive Analyse jeder Schwachstelle durch und prüfen dabei, wie einfach sie sich ausnutzen lässt und auf welche Ressourcen und Systeme ein Hacker nach erfolgreichem Eindringen Zugriff hätte. Danach wird eine wie in Abbildung 1 veranschaulichte Risikomatrix erstellt, die Teams einen klaren Überblick über die risikoreichsten

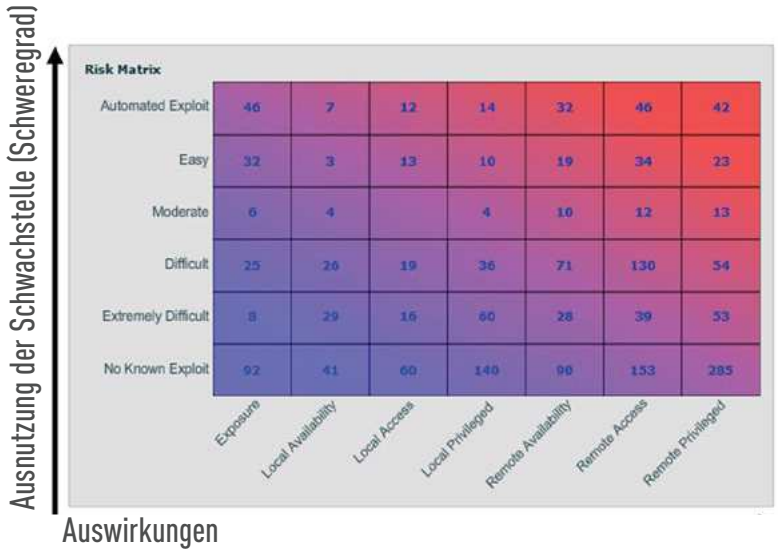

Abb. 1: Mit Tripwire IP360 stehen Ihnen moderne Funktionen für die Risikobewertung zur Verfügung, sodass Sie Geschäftsrisiken besser einschätzen können.

Sicherheitsverstöße vermeiden

Durch die Integration mit Tripwire Enterprise haben Sie Zugang zu Adaptive Threat Protection, einem integrierten, automatisierten Service für die Risikoeinschätzung. Damit lassen sich risikobehaftete Ressourcen in Enterprise mit Schwachstellendaten anreichern und mit Tags versehen, sodass Sie den Status dieser Ressourcen stets im Blick haben. Werden Schwachstellen gepatcht, können Sie die betroffenen Ressourcen erneut scannen und über Tripwire Enterprise die entsprechenden Tags aktualisieren lassen. Und indem Sie die Konfigurationsmanagement-Funktionen von Enterprise mit Tripwire IP360 kombinieren, können bei Konfigurationsänderungen an Dateien oder am System automatisch Schwachstellenanalysen eingeleitet werden.

Schwachstellen bietet. Bei der Auswertung der Risikofaktoren wird ebenfalls berücksichtigt, wie lange die Schwachstelle ungepatcht im Netzwerk vorhanden war. Anhand all dieser Faktoren wird schließlich eine Risikobewertung generiert, die es Sicherheitsanalysten ermöglicht, die Maßnahmen zur Risikoeinschätzung und -minimierung in der gesamten IT-Umgebung zu überwachen und Management-Sponsoren von der Effektivität des Schwachstellenmanagements der Organisation zu überzeugen.

Zentralisierte Administration

Mit Tripwire IP360 steht Kunden eine zentrale, benutzerfreundliche Konsole für die Verwaltung, Konfiguration, Berichterstellung und Workflow-Kontrolle zur Verfügung. Dadurch, dass Sie Zugangskontrollen detailliert und rollenbasiert zuweisen können, lassen sich neue administrative Prozesse wie das Zugriffsmanagement gut in vorhandene Sicherheitsabläufe und -systeme einbinden.

Automatisierung durch Integration

Tripwire IP360 basiert auf offenen Standards und lässt sich daher reibungslos mit vorhandenen Geschäftsprozessen und IT-Systemen für Support, Ressourcenmanagement, SIEM, Erkennung/Abwehr von Angriffsversuchen und anderen Sicherheitslösungen integrieren. Hinzu kommen die umfassenden, von IP360 gesammelten Bedrohungsdaten an Endpunkten, mit denen Sie Ihre IT-Managementlösungen stärken und die Automatisierung Ihrer Sicherheitsmaßnahmen vorantreiben können.

Robuste Architektur

IP360 lässt sich ohne großen Aufwand implementieren und nutzt Linux-basierte virtuelle oder physische Appliances, die sich bei Bedarf für eine größere Fehlertoleranz und schnellere Scans bündeln lassen.

Fordern Sie eine Demo an

Erleben Sie Tripwire IP360 in einer Demo in Aktion und stellen Sie uns Ihre Fragen. Näheres erfahren Sie unter **tripwire.com/contact/request-demo**

tripwire®

Tripwire stellt Kunden branchenführende Produkte zur Stärkung ihrer Cybersicherheit zur Verfügung. Wir schützen prominente Unternehmen auf der ganzen Welt vor Sicherheitsverletzungen und Cyberangriffen – und weil Hacker immer raffinierter werden, entwickeln auch wir unsere Technologien seit mehr als 20 Jahren ständig weiter. Unsere Lösungen sind sowohl On-Premises als auch in der Cloud verfügbar, wo sie Ihre digitale Infrastruktur schützen sowie Bedrohungen aufdecken und abwehren, ohne den Geschäftsbetrieb oder die Produktivität zu beeinträchtigen – sozusagen als unsichtbare Schutzbarriere für Ihre Systeme. **Weitere Informationen erhalten Sie unter tripwire.com.**

***The State of Security*: Aktuelles, Trends und interessante Einblicke finden Sie unter tripwire.com/blog**
Folgen Sie uns auf LinkedIn, Twitter und Facebook