

Ivanti Exposure Management

Erweitern Sie Ihr Schwachstellenmanagement, um Sicherheitsverletzungen proaktiv zu verhindern

Herkömmliche Verfahren für das Schwachstellenmanagement sind nicht auf den Umfang und die Vielfalt der heutigen Assets und Gefährdungen ausgelegt. Aus diesem Grund ist es Unternehmen oftmals gar nicht bewusst, wie vielen Cyberbedrohungen sie tatsächlich ausgesetzt sind. Die Exposure-Management-Lösung von Ivanti löst dieses Problem, indem sie einen vollständigen Einblick in alle Assets und Risiken sowie eine risikobasierte Priorisierung der Bedrohungen ermöglicht und so einen strategischen Ansatz für die Behebung von Schwachstellen verfolgt.





Was ist CTEM?

Das von Gartner entwickelte Continuous Threat Exposure Management (CTEM) umfasst eine Reihe von Prozessen und Funktionen, die es Unternehmen ermöglichen, die Zugänglichkeit, die Gefährdung und die Ausnutzbarkeit ihrer digitalen sowie physischen Ressourcen kontinuierlich und konsistent zu bewerten. CTEM-Praktiken werden vorwiegend durch Cloud-basierte Funktionen realisiert, wie beispielsweise in der Exposure-Management-Lösung von Ivanti.

Die Angriffsflächen werden immer größer und komplexer. Herkömmliche Verfahren für das Schwachstellenmanagement sind oft nur schwer anpassbar, wodurch sie moderne IT-Umgebungen häufig nicht ausreichend sichern können.

- Wenn ausschließlich die traditionelle IT-Umgebung überwacht wird – bestehend aus Servern und Endgeräten – werden mobile Geräte, Websites, Anwendungen und andere Ressourcen vernachlässigt.
- Durch eine strikte Fokussierung auf allgemeine Schwachstellen und Gefährdungen (CVEs) werden andere Risikofaktoren ignoriert, wie etwa Fehlkonfigurationen, die ebenfalls eine erhebliche Bedrohung für das Unternehmen darstellen.

- Wenn die Priorisierung von Abhilfemaßnahmen mit dem Common Vulnerability Scoring System (CVSS) vorgenommen wird, das den Schweregrad von Verwundbarkeiten, nicht aber deren Risiko misst – mit anderen Worten, wie einfach eine Verwundbarkeit ausgenutzt werden könnte und nicht ob sie ausgenutzt wurde.

Daher besteht für Unternehmen, die auf traditionelle Methoden im Schwachstellenmanagement setzen, trotz aller Anstrengungen ein höheres Risiko, Ziel eines Sicherheitsvorfalls zu werden – mit potenziellen Folgen wie Ausfallzeiten, Reputationsverlust und weiteren Schäden, wie zum Beispiel das Abfließen von Daten. Meist reagieren solche Unternehmen lediglich, indem sie versuchen, Tausende von hochgefährlichen Schwachstellen zu beheben, anstatt proaktiv die wenigen anzugehen, die ein echtes Risiko darstellen.

Das Exposure-Management behebt die Mängel des Schwachstellenmanagements. Es stellt eine Weiterentwicklung dar, die herkömmliche Methoden

modernisiert. Zudem sorgt es für einen umfassenden Einblick in die Assets und Gefährdungen und ermöglicht eine entsprechende Priorisierung der Risiken. Laut Gartner werden Unternehmen, die Sicherheitsinvestitionen auf der Grundlage eines CTEM-Programms (Continuous Threat Exposure Management) priorisieren, die Zahl der Sicherheitsverletzungen bis 2026 um zwei Drittel reduzieren.¹

Einführung von Ivanti Exposure Management

Durch die umfassende Sichtbarkeit der Angriffsfläche und die risikobasierte Priorisierung sorgt die Exposure-Management-Lösung von Ivanti dafür, dass Unternehmen alle ihre Assets und Risiken kennen – einschließlich diejenigen, die beim herkömmlichen Schwachstellenmanagement oft übersehen werden. So können sie das tatsächliche Risiko zuverlässig identifizieren und bewerten.

Wichtige Fähigkeiten

Vollständige Sichtbarkeit

Erweitern Sie Ihren Aktionsradius, indem Sie über die bekannten Server und Endgeräte hinausblicken und ein ganzheitliches Bild der zu schützenden Angriffsfläche entwickeln. Ein einziger Blindspot kann bereits ausreichen, um einem Cyberangreifer den Zugang zu Ihrem Unternehmen zu ermöglichen. Ivanti Exposure Management erkennt alle Geräte, die sich mit dem Netzwerk verbinden – seien es bekannte oder unbekannte – sowie die darauf installierte Software. Dies erfolgt sowohl durch aktives als auch passives Scannen sowie über Drittanbieter-Konnektoren, sodass keine potenzielle Schwachstelle unentdeckt bleibt.

Die agentenlose Überwachung identifiziert externe Ressourcen, die oft außerhalb der Kontrolle von Sicherheitsteams liegen – wie beispielsweise QA- und Entwicklungsumgebungen oder vernachlässigte Marketing-Websites. Die Ivanti-Lösung geht über die CVEs hinaus und sucht nach externen Sicherheitsrisiken in den folgenden Vektoren:

- Anwendungssicherheit
- Datenlecks
- DNS-Zustand
- E-Mail-Sicherheit
- Netzwerksicherheit
- Social Engineering

Risiken berücksichtigen

Verabschieden Sie sich vom CVSS und dem damit verbundenen Aufwand. Ivanti bietet zwei proprietäre Methoden zur Risikobewertung, mit deren Hilfe Sie gezielte Maßnahmen zur Risikominderung dort ergreifen können, wo sie am effektivsten sind, um erfolgreiche Angriffe und die damit verbundenen Folgen zu verhindern.

Das Vulnerability Risk Rating (VRR) bewertet Gefährdungen aufgrund ihrer Eigenschaften und des realen Bedrohungskontexts - nicht nur anhand des Schweregrads. Durch die genaue Bewertung jedes Risikos zeigt VRR, welche Gefährdungen sofortige Aufmerksamkeit erfordern und welche kein Risiko darstellen.

VRR wird mit der Kritikalität von Assets, Bedrohungsdaten und externem Zugriff kombiniert, um die Ivanti RS³-Scores zu berechnen. Diese Scores zeigen an, welche Assets das größte Risiko darstellen. Sie werden zudem zu einer quantifizierten Übersicht des Risikoprofils eines Unternehmens zusammengefasst, die den Erfolg des Risikomanagements in einem bestimmten Zeitraum veranschaulicht.

Maßnahmen ergreifen

Was nützt die Bewertung von Gefährdungen, wenn man auf Grundlage dieser Analyse keine konkreten Maßnahmen zur Risikominderung ergreift? Mit Ivanti können Sie gezielte Schritte zur Risikominderung unternehmen, indem Sie kritische Schwachstellen beheben, bevor diese ausgenutzt werden können.

Eine API-Integration ermöglicht es Ihnen, priorisierte Schwachstellenlisten direkt von unserer Schwachstellen-Management-Lösung an unser Patch-Management-Modul zu übermitteln, um deren Behebung zu erleichtern. Mit Unterstützung für Windows, MacOS, Linux und Drittanbieteranwendungen können Sie einen Großteil der in den meisten modernen Umgebungen auftretenden Schwachstellen beheben.

Ivanti kann Sie zudem mit automatisierten Bots unterstützen, die proaktiv Probleme auf Endgeräten und Edge-Geräten erkennen, diagnostizieren und beheben.

Über Ivanti

Ivanti baut die Barrieren zwischen IT und Sicherheit ab, damit Everywhere Work erfolgreich ist. Ivanti hat die erste eigens entwickelte Technologieplattform für CIOs und CISOs geschaffen, die IT- und Sicherheitsteams umfassende Softwarelösungen bietet. Diese skalieren mit den Anforderungen ihrer Unternehmen, um positive digitale Erfahrungen der Mitarbeitenden zu ermöglichen, zu sichern und zu verbessern. Die Ivanti-Plattform wird von Ivanti Neurons betrieben – einer intelligenten, Cloud-fähigen Hyper-Automatisierungsebene, durch die wir proaktive Heilung und eine benutzerfreundliche Sicherheit unternehmensweit ermöglichen und den Usern eine angenehme Erfahrung bieten können. Mehr als 40.000 Kunden, darunter 85 der Fortune-100-Unternehmen, haben sich für Ivanti entschieden, um die Herausforderungen mit den eigenen End-to-End-Lösungen zu meistern. Unser Ziel bei Ivanti ist, ein Umfeld zu schaffen, in dem alle Meinungen gehört, respektiert und geschätzt werden. Und wir setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten ein. Weitere Informationen finden Sie unter www.ivanti.com/de und folgen Sie @Golvanti.

The logo for Ivanti Neurons, featuring the word "ivanti" in a bold, lowercase, sans-serif font, followed by "neurons" in a lighter, lowercase, sans-serif font. The "i" in "ivanti" has a small square above it. The text is red.A vertical red bar with a slight gradient, positioned to the left of the text.

Für weitere Informationen oder um Ivanti zu kontaktieren, Bitte besuchen Sie ivanti.com/de.