

Ivanti betrachtet Angriffsflächen aus der Perspektive eines Hackers

Ivanti Neurons for EASM identifiziert Schwachstellen in extern zugänglichen Systemen

Frankfurt – 30. Juli 2024 – Das Technologieunternehmen [Ivanti](#), das Everywhere Work verbessert und sichert, hat [Ivanti Neurons for External Attack Surface Management](#) (EASM) vorgestellt. Diese Lösung dient zur Identifizierung und Absicherung der externen Angriffsfläche eines Unternehmens.

Auch wenn sie im Unternehmenseinsatz nicht mehr aktiv genutzt werden, bleiben viele Webserver, Domain Controller oder Cloud-Dienste immer noch aktiv und über das Internet zugänglich. Häufig werden im Tagesgeschäft der IT Testsysteme eingerichtet oder projektspezifische Lösungen aufgesetzt. Nach Projektende werden diese Systeme dann nicht mehr produktiv genutzt, sind aber weiterhin online erreichbar und ermöglichen im ungünstigen Fall einen Zugriff auf interne Ressourcen. Das Problem: Die schiere Menge dieser öffentlich zugänglichen Systeme erschwert eine wirksame Abwehr – und wenige von ihnen sind dokumentiert. Diese vernachlässigten Ressourcen stellen ein latentes Sicherheitsrisiko dar. EASM betrachtet diese Angriffsflächen aus der Perspektive eines Hackers und nutzt automatisierte Tools, um potenziell gefährdete Ressourcen zu identifizieren.

Ivanti Neurons für EASM deckt verschiedene extern zugängliche Anlagen und Systeme auf, wie Webanwendungen, Internetprotokolle (IPs), Domännennamen, SSL-Zertifikate (Secure Sockets Layer) oder Cloud-Dienste. Die Lösung erkennt Schwachstellen, wie ungeschützte Server, Anmeldedaten, Fehlkonfigurationen und Sicherheitslücken im Drittanbietercode.

EASM als integraler Bestandteil der Cyber-Resilienz

Das EASM-Produkt bietet umfassende Funktionen zur Erkennung und Bewertung von Risiken durch extern zugängliche Assets. Es scannt aktiv Cloud-, IT-, IoT- und OT-Umgebungen, analysiert Systeme in Bezug auf Risiken und priorisiert diese basierend auf geschäftlichen Auswirkungen und Exploit-Wahrscheinlichkeit. Durch die Integration mit Ticketing-Systemen und SOAR-Lösungen (Security Orchestration, Automation and Response) optimiert es den Workflow zur Behebung der Schwachstellen.

Findet Ivanti Neurons for EASM eine Schwachstelle, so weist die Lösung ihr einen Risiko-Score (VRS) zu. Der VRS ermöglicht eine fundierte Entscheidungsfindung, indem er Sicherheitsteams in die Lage versetzt, das von einer Sicherheitslücke ausgehende Risiko zu quantifizieren und ihren Bedrohungskontext zu verstehen.

Der Einsatz einer EASM-Lösung eröffnet Unternehmen einen Blick auf potenzielle Angriffsvektoren, die auch Hacker sehen: So spürten im Rahmen der Pilotphase von Ivanti Neurons for EASM 31 Prozent der Unternehmen unwissentlich offengelegte sensible Daten auf und 30 Prozent entdeckten unbekannte Web-Assets. Fast ebenso viele (29 Prozent) identifizieren Fehlkonfigurationen und anfällige Systeme.

„EASM ist eine entscheidende Komponente für ein umfassendes Cyber-Asset-Management. Sie stärkt die Cyber-Resilienz, indem sie alle digitalen Assets erkennt und die damit verbundenen Risiken priorisiert“, sagt Dr. Srinivas Mukkamala, Chief Product Officer bei Ivanti. „Wir wollen unseren Kunden Technologien zur Verfügung stellen, die einen nahtlosen und sicheren Arbeitsplatz ermöglichen.“

Neben der Analyse und Priorisierung von Risiken hilft Neurons for EASM bei der Erkennung und Inventarisierung von digitalen Assets sowie der Eindämmung von Cloud-Wildwuchs und Schatten-IT. Ein

weiterer wichtiger Anwendungsfall ist die Durchführung von Risikobewertungen für Tochtergesellschaften oder Akquisitionsziele.

KI im Service Management

Neben Ivanti Neurons for EASM hat Ivanti eine Reihe seiner Lösungen um neue Funktionen ergänzt:

- **Ivanti Neurons iPaaS:** Diese Low-Code/No-Code-Plattform ermöglicht die nahtlose Integration extern zugänglicher Anwendungen in die Ivanti Service- und Asset-Management-Lösungen. Mit vorgefertigten Konnektoren und einem benutzerfreundlichen Drag-and-Drop-Editor können IT-Teams die Automatisierung erweitern und die Produktivität erhöhen.
- **KI-Funktionen in Ivanti Neurons for ITSM:** Neue generative KI-Funktionen verbessern die User Experience und steigern die Produktivität von ITSM-Analysten. Dazu gehören Ticket- und Vorfall-Zusammenfassungen, die Erstellung von Wissensartikeln und ein zentraler Konfigurations-Hub.
- **Verbesserte Dashboards und Berichte:** Ein Dashboard-Designer erleichtert die Erstellung KPI-relevanter Dashboards, während KI-gestützte Umfragezusammenfassungen verbesserte Analysen bieten.

Über Ivanti

Ivanti überwindet Barrieren zwischen IT und Sicherheit, damit sich Everywhere Work (Arbeiten von jedem Ort) entfalten kann. Ivanti hat dazu die erste zweckgerichtete Technologieplattform für CIOs und CISOs entwickelt. Sie bietet IT- und Sicherheitsteams umfassende Softwarelösungen und wächst mit den Anforderungen der Organisationen, die Mitarbeitererfahrung zu gestalten, zu sichern und zu verbessern. Die Ivanti-Plattform wird von Ivanti Neurons getragen - einer intelligenten Hyperautomatisierungsschicht im Cloud-Maßstab, die eine proaktive Wartung von IT-Assets und benutzerfreundliche Sicherheit im gesamten Unternehmen schafft. Sie verbessert die Mitarbeitererfahrung, die Anwender begeistert. Über 40.000 Kunden haben sich für Ivanti entschieden, um mit End-to-End-Lösungen ihren Herausforderungen zu begegnen. Darunter sind 85 der Fortune 100-Unternehmen. Bei Ivanti sind wir bestrebt, eine Umgebung zu schaffen, in der alle Perspektiven gehört, respektiert und geschätzt werden. Wir engagieren uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeiter und den Planeten. Für weitere Informationen besuchen Sie www.ivanti.de und folgen Sie @Golvanti.