Fallstudie

Cyberint

Ströer deckt in großem Umfang die wichtigsten externen Risikopositionen auf

Maximale Sichtbarkeit über alle Portfolio-Unternehmen hinweg, proaktive Informationen für schnelle Abhilfemaßnahmen und einheitliche Cybersicherheit

Quelle: blowUP media GmbH

Die Herausforderung: Beseitigung externer Bedrohungen für alle Unternehmen des Portfolios

Ströer ist ein führender deutscher Anbieter von Außenwerbung und bietet Werbekunden individuelle und voll integrierte End-to-End-Lösungen entlang der gesamten Marketing- und Vertriebswertschöpfungskette an. Mit der Strategie "OOH+" setzt Ströer auf die Stärke des OOH-Geschäfts, flankiert von den Segmenten "Digital & Dialog Media" und "DaaS & E-Commerce". Das Unternehmen beschäftigt rund 10.000 Mitarbeiter an über 100 Standorten. Im Geschäftsjahr 2021 erzielte Ströer einen Umsatz von 1,63 Milliarden Euro. Die Ströer SE & Co. KGaA ist im MDAX der Deutschen Börse notiert.

Mit der Aufgabe betraut, eine einheitliche, gesunde und gemeinsame Sicherheitskultur in der gesamten Gruppe zu schaffen, wollte Benjamin Bachmann, Leiter des Group Information Security Office, zunächst einen vollständigen Überblick über die externen Angriffsflächen aller Portfolio-Unternehmen gewinnen. Das war keine leichte Aufgabe angesichts der schieren Größe der einzelnen Unternehmen und ihrer bekannten und unbekannten Assets.

Benjamin und sein Team bewerteten mehrere Lösungen, eine für das External Attack Surface Management (EASM) und eine für die Verringerung von Risiken. Das änderte sich während des POV von Cyberint mit Ströer, bei dem das Team das Ausmaß an Transparenz und umsetzbaren Erkenntnissen erkannte, das die Lösung bot.

„Während des POV stellten wir fest, dass Cyberint viel mehr als eine EASM-Lösung ist, es liefert einen großen Wert mit höchst relevanten Informationen aus dem Deep- und Dark-Web.“

Benjamin Bachmann, Leiter des Group Information Security Office

STRÖER

Herausforderungen

Umfassende integrierte Sichtbarkeit des externen Risikos für alle Portfolio-Unternehmen

Lösung

Bereitstellung von Cyberint Argos Edge™

Auswirkungen

- Kontinuierliches Aufdeckung und Verringerung der wichtigsten bekannten und unbekannten externen Risiken
- Durch die drastische Reduzierung von Fehlalarmen konnten sich die Teams auf die richtigen Maßnahmen konzentrieren, um das digitale Risiko zu minimieren
- Kontinuierliche Bereinigung der Daten und Optimierung der Ergebnisse mit laufender Unterstützung durch das Cyberint-Analystenteam

Die autonome Ermittlung war der Wendepunkt

Das Team begann sofort die Erkenntnisse, die Argos Edge™ erzielt hatte, umzusetzen und verbesserte die Cyber-Sicherheit in allen Unternehmen der Gruppe erhelblich.

Das Team nutzte die speziell auf Bedrohung der nach außen gerichteten Assets jedes Unternehmens zugeschnittenen Bedrohungsdaten und kommunizierte auf Unternehmensebene, was zu tun war. Es überwachte den Fortschritt und verbesserte kontinuierlich die Cyber-Sicherheit von mehr als 100 Portfolio-Unternehmen, wodurch sich die Sicherheit der gesamten Organisation erhöhte.

Auf dem Weg zu null falsch-positiven Fehlalarmen

Nach Abschluss der autonomen EASM-Ermittlung von Cyberint wurden die relevanten Bedrohungsdaten des Open, Deep und Dark Web den spezifischen exponierten Anlagen von Ströer zugeordnet.

Mit Hilfe des Cyberint-Analystenteams wurden die Ergebnisse bereinigt, der Algorithmus trainiert und die Anzahl der falsch-positiven Ergebnisse schrittweise auf ein Minimum reduziert. Das bildete die Grundlage für ein angemessenes Benchmarking und die Messung der Leistung.

"Das Cyberint-Team war bei jedem Schritt sehr entgegenkommend und hilfreich."

Erkenntnisse auf neuem Niveau

Neben der Transparenz auf Gruppenebene halfen Cyberints Bedrohungsberichte zum Deep und Dark Web Ben und seinem Team, ein klares Verständnis für das Gesamtbild zu erlangen: Trends, Hacker-Gruppen, Interessen der Bedrohungsakteure und mehr. Mit diesen Berichten können sie das Wissen und das Bewusstsein für Cybersicherheit in allen Portfolio-Unternehmen verbessern und mit der sich ständig weiterentwickelnden Bedrohungslandschaft Schritt halten.

"Es war keine Überraschung, dass wir unsere Anbieterbewertung nach dem POV mit Cyberint beendet haben", sagt Ben. "Es erfüllt einfach alle unsere Anforderungen. Transparenz, umsetzbare Erkenntnisse, Unterstützung und Wissen - alles auf einer einzigen, einfach zu bedienenden Plattform. Der Fokus, den es liefert, ist phänomenal."

Über Cyberint

Cyberint ist ein Anbieter von Cybersicherheitslösungen, der Pionierarbeit bei der Erkundung von Angriffsflächen geleistet hat. Die Lösung verbindet Bedrohungsdaten mit der Verwaltung von Angriffsflächen und bietet Unternehmen einen umfassenden integrierten Einblick in ihre externen Risiken. Durch die autonome Erkennung aller nach außen gerichteten Assets in Verbindung mit Informationen zu Open, Deep und Dark Web können die Teams von Cybersecurity die wichtigsten bekannten und unbekannten digitalen Risiken früher aufdecken. Globale Kunden, darunter Fortune 500 Unternehmen der großen Branchen, vertrauen Cyberint, wenn es darum geht, Phishing, Betrug, Ransomware, Markenmissbrauch, Datenlecks, externe Schwachstellen und vieles mehr zu verhindern, zu erkennen, zu untersuchen und zu beheben und so einen kontinuierlichen externen Schutz vor Cyberbedrohungen zu gewährleisten.

Besuchen Sie www.cyberint.com, wenn Sie mehr darüber erfahren möchten, wie cyberint gemeinsam mit den Unternehmen die wichtigsten externen Risiken aufdeckt und verringert.

Cyberint