Produktblatt

Vulnerability Management

Nur, wer seine Schwachstellen genau kennt, kann Sicherheitsmaßnahmen gezielt einsetzen. Vulnerability Management hat die Aufgabe, die Verwundbarkeit der IT-Infrastruktur zu identifizieren und zu beheben. Es ist ein wichtiges Element im Gesamtkontext der Cyber Intelligence. Ziel ist die Verringerung der Angriffsfläche und die Steigerung der Sicherheit. Wir finden Sicherheitslücken, bevor Cyberkriminelle diese ausnutzen können. Unsere umfangreichen Services stimmen wir auf die Anforderungen des Netzwerkes sowie auf individuelle Bedürfnisse ab.

Für wen kommt es infrage?

Unsere Vulnerability-Management-Services richten sich grundsätzlich an alle Firmen, die schützenswerte Assets wie Daten oder Geschäftsabläufe haben.

Aufgabe

Um Ihnen ein effektives Vulnerability-Monitoring anzubieten, evaluieren wir in einem ersten Schritt spezifische Anforderungen (z. B. Compliance). Daraufhin definieren wir in Zusammenarbeit die Art und den Umfang des Servicepakets. Schwachstellenscans geben uns Aufschluss über die Sicherheitslage im Unternehmen. Relevante Maßnahmen besprechen wir mit Ihnen und setzen sie gegebenenfalls schnellstmöglich um.

Leistungsangebot

- Regelmäßige unabhängige Überprüfung Ihrer Systeme sowie Compliance-Checks
- Schwachstellenübersicht mit Kurzbeschreibung
- VSS-Basisbewertung für mögliche identifizierte Schwachstellen
- Empfehlung zur Beseitigung von Schwachstellen gemäß industriellen Best Practices
- Unterstützung durch unsere erfahrenen und zertifizierten Sicherheitsexperten bei der Risiko-Analyse, Risiko-Verifikation und -Minderung

Nutzen & Vorteile

Unsere Vulnerability-Management-Lösungen ermöglichen Ihnen eine automatisierte Analyse und Erkennung der Schwachstellen Ihrer Systeme. Mithilfe leistungsfähiger Scan-Technologien können wir Netzwerke proaktiv und kontinuierlich auf eventuelle Sicherheitslücken überprüfen. Unsere Experten bieten individuellen Support und liefern Empfehlungen für die Priorisierung der Updates und Beseitigung der Schwachstellen. Der Prozess – von der Erkennung bis zur Behebung und Kontrolle – läuft in einem beständigen Kreislauf. So sind Sie den Angreifern immer einen Schritt voraus.