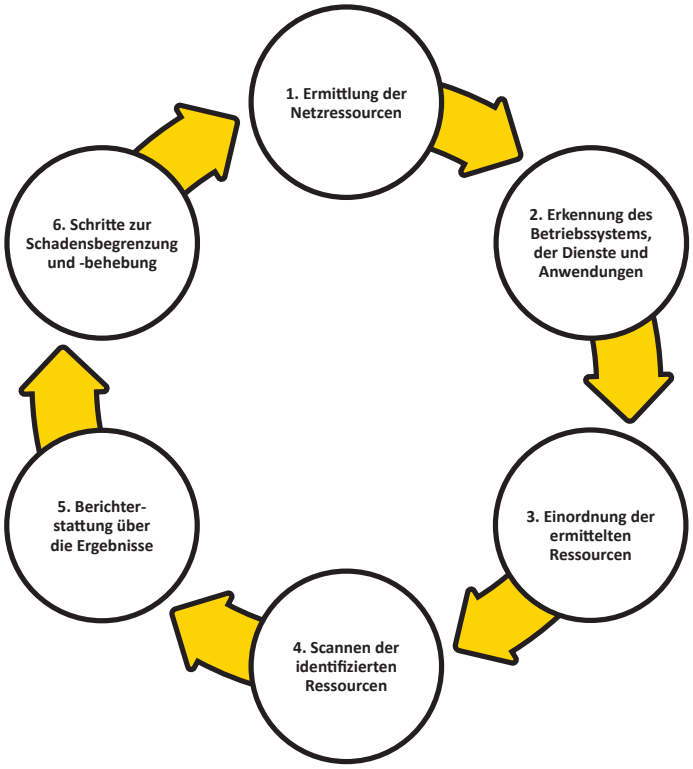
Gezielte Schwachstellenbeseitigung mit Vulnerability Management as a Service.

Isoliert betrachtet sind die Ergebnisse eines Schwachstellen-Scans nicht sehr aussagekräftig. Deshalb vergleichen wir deren Resultate mit Informationen aus unzähligen anderen Scans. So können wir Sie rechtzeitig auf schwerwiegende Schwachstellen aufmerksam machen und entsprechend reagieren.

Bei unserem Vulnerability Management as a Service bestimmen Sie die Häufigkeit der Scans (wöchentlich, monatlich) selbst und können ihn damit optimal auf Ihre Bedürfnisse abstimmen. Im Falle einer vermuteten Schwachstelle können Sie selbstverständlich kurzfristig zusätzliche Scans bestellen. Das ist unser Ansatz für das Schwachstellenmanagement:



Handlungsempfehlungen

Aus der Erkennung von Schwachstellen wird erst dann ein funktionierendes Schwachstellenmanagement, wenn auf die Erkennung einer Schwachstelle eine spezifische Massnahme folgt. Unsere Handlungsempfehlungen helfen, die Zeit für die Behebung von Schwachstellen drastisch zu verkürzen.

Die verschiedenenen Scan-Optionen

Externer Scan: Die Perspektive des Angreifers
Unser externe Scan-Service versetzt Sie in die Perspektive eines Angreifers auf Ihr Unternehmen. Gescannt werden die vordefinierten Netzwerkressourcen (Assets), die aus dem Internet erreichbar sind.

Agentenbasierter Scan: Scannen Sie Geräte überall
Durch den Einsatz eines digitalen Agenten auf Ihren Geräten können Sie sich unabhängig von deren Standort über deren Schwachstellen, installierte Anwendungen und allgemeine Risiken informieren.

Standort-Scan: Sicherheit im gesamten Netzwerk
Damit Sicherheit nicht an den Netzwerk-Grenzen endet, konzentriert sich Onsite-Scan auf Ihr lokales Netzwerk (LAN). Je nach gewünschter Tiefe des Scans werden einzelne oder mehrere Sensoren in Ihrem Netzwerk platziert. Dadurch kann das System Schwachstellen aufspüren, die Angreifer nutzen könnten, um sich seitlich im Netzwerk zu bewegen. Die Scan-Ergebnisse werden mit dem zentralen Berichtsmodul und den Ergebnissen von Remote-Scans kombiniert.

Discovery Scan: Finden Sie Assets in Ihrem Netzwerk
Der Discovery Scans fokussiert sich auf das Auffinden von Netzwerkressourcen. Die Netzwerkbereiche werden von Ihnen festgelegt und von UMB systematisch gescannt. Sie erhalten eine Auswertung des Betriebssystems und der Netzwerkdienste. Im Rahmen der Betriebssystemerkennung zeigt Ihnen UMB, welche Ports pro Dienst erreichbar sind, für welche Anwendungen ein entsprechender Port erreichbar oder offen ist, und welche Betriebssysteme verwendet werden.

Option: Automatisiertes Patch-Management für nahtlosen Schutz
Das automatisierte Patch-Management-Modul von UMB erleichtert die rechtzeitige Verteilung von Sicherheits-Patches für Ihre Systeme. Dies minimiert das Risiko von Angriffen, die bekannte Schwachstellen ausnutzen, und gewährleistet, dass Ihre Systeme stets auf dem neuesten Stand der Sicherheitsmassnahmen sind.

Dienstleistungskomponenten

- Standort-Scan
- Discovery-Scan
- Externer Scan
- Agentenbasierter Scan
- Handlungsempfehlungen
- Koordination der Abhilfemassnahmen
- Monatliche Berichterstattung

Ihre Vorteile:

- Sie erfahren, wo die Schwachstellen Ihrer Systeme liegen und haben die Bedrohungslage Ihrer Infrastruktur jederzeit unter Kontrolle.
- Sie werden über Konfigurationsfehler sowie neu installierte oder nicht autorisierte Systeme (auch Schatten-IT genannt) informiert.
- Sie erhalten Schwachstelleneinstufungen und Handlungsempfehlungen von erfahrenen Spezialisten.
- Sie werden frühzeitig über neue Schwachstellen informiert, die ein hohes Risiko darstellen.
- Sie können die Schwachstellenbeseitigung für alle Ihre IT-Assets vereinfachen und beschleunigen.

Klingt interessant? Kontaktieren Sie uns!

Gerne beantworten wir Ihre Fragen zum Thema Vulnerability Management as a Service und mehr.

Kontakt

Markus Kaegi
Team Leader Strategic Sales Consulting
markus.kaegi@umb.ch
+41 58 510 16 98
www.umb.ch