ANTARES NETLOGIX

VULNERABILITY LIFECYCLE MANAGER:
SCHWACHSTELLEN LANGFRISTIG BEHEBEN

DOMINIK HANDL

Unser Antares Red Team Experte im VLM-Interview

Dominik Handl war jahrelang Leiter des Antares Operations Centers und führt jetzt als Chef des Red Teams Sicherheitsüberprüfungen und Penetrationstests durch. Außerdem plant er IT-Sicherheitsarchitekturen und berät und begleitet unsere Kunden mit seiner reichhaltigen Expertise in sicherheitstechnischen Fragen.

WAS IST EIGENTLICH VULNERABILITY MANAGEMENT UND WO LIEGEN DIE „SCHWACHSTELLEN“ DIESER SYSTEME?

Vulnerability Management hat das Ziel, im Rahmen regelmäßiger Schwachstellen-Scans unterschiedlichste **Sicherheitsrisiken** im Unternehmen **aufzudecken**. Dazu gehören beispielsweise fehlende Patches, Schwachstellen aufgrund von Konfigurationsfehlern oder nicht vertrauenswürdige Zertifikate. Ein Vulnerability Scan liefert jedoch eine **oft unüberschaubare Menge an Ergebnissen**.

Die Kategorisierung dieser Findings, ihre Zuweisung zu den jeweiligen System- oder Software-Verantwortlichen, sowie die Nachverfolgung des Bearbeitungsstandes kosten somit regelmäßig sehr viel Zeit. Weil wir von Antares-NetlogiX erkannt haben, dass viele unserer Kunden Unterstützung bei der Handhabung dieser Scans benötigen, haben wir dafür eine **spezielle Lösung entwickelt: Unseren Vulnerability Lifecycle Manager** (VLM).

WAS SAGEN EURE KUNDEN ZUM VLM?

Für unsere Kunden bietet der VLM echte Vorteile: Sie verfügen endlich über eine **zentrale Anlaufstelle** für ihr Schwachstellen-Management. Anhand **aussagekräftiger Reports und grafischer Darstellungen** können sie die Ergebnisse der Vulnerability Scans einfach und schnell nachvollziehen.

Dabei profitieren sie von der Unterstützung unserer Analysten, die mit ihrer Erfahrung die Einstufungen der Sicherheitslücken zuverlässig vornehmen können. So werden endlich auch Security Reports für den CISO automatisiert ermöglicht. Und natürlich stehen wir mit unseren Services auch bei der Behebung der Sicherheitslücken zur Seite.

WELCHE KERNFUNKTION BIETET DER VLM?

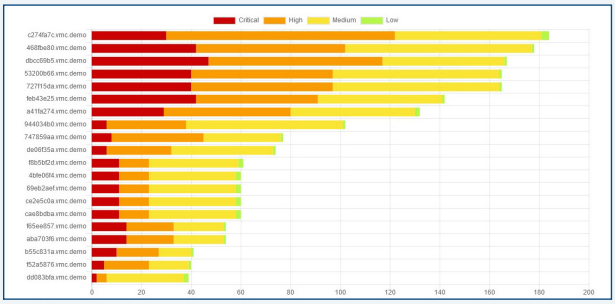
Die Aufgabe des VLM ist es, die genannten **Tasks** weitgehend zu **automatisieren**, damit mehr Zeit auf die eigentliche Behebung der Schwachstellen verwendet werden kann.

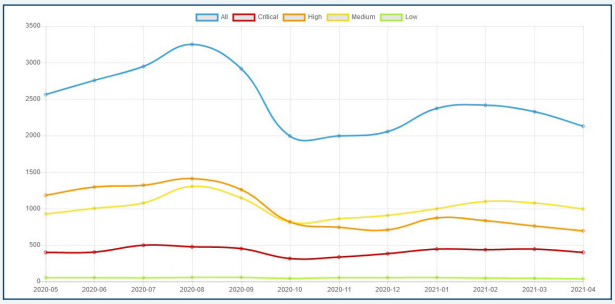
Deshalb besteht eine der Kernfunktionalitäten des VLMs in der Möglichkeit, **Verantwortliche für Systeme und Applikationen zu definieren**, denen identifizierte Schwachstellen automatisch zugewiesen werden können.

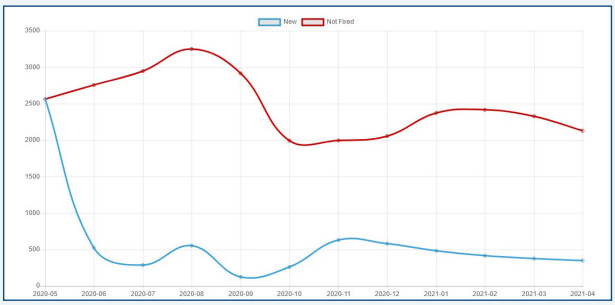
WOHER KOMMEN DIE DATEN, DIE DER VLM NUTZT?

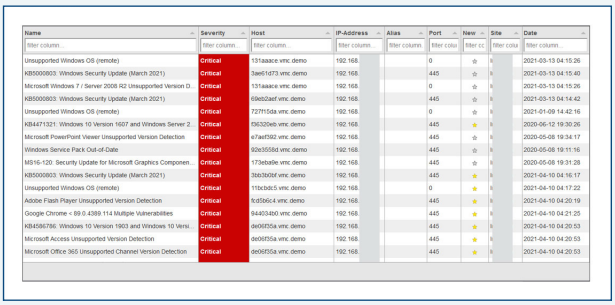
Die Daten liefern bewährte **Schwachstellen-Scanner** wie Tenable Nessus oder Microsoft Defender Vulnerabilty Management , die bei vielen unserer Kunden bereits im Einsatz sind. Durch unsere langjährige Erfahrung bringen wir hier detaillierte Produktkenntnisse mit und können auch bei der Implementierung unterstützen.

EINBLICKE IN UNSER VLM









DIE BESTEN FEATURES

- Zentrale Verwaltung von Vulnerability-Scanergebnissen für eine beliebige Anzahl von Scannern und automatische Übernahme der Scanergebnisse.
- Grafische Aufbereitung von Statistiken (Dashboard), z.B. neue, geschlossene und nicht geschlossen Schwachstellen, PDF-Report / Management-Summary, Delta-Reports im zeitlichen Verlauf.
- Zuweisung von Verantwortlichen für Schwachstellenbehebung (Vulnerability Ticketing), Self-Service-Portal für den Kunden, Zwei-Faktor-Anmeldung für die User.