ANTARES NETLOGIX

VULNERABILITY LIFECYCLE MANAGER:
SCHWACHSTELLEN LANGFRISTIG BEHEBEN

STEFAN LANGEDER

Unser Antares Red Team Experte im VLM-Interview

Dipl.-Ing. Stefan Langeder, BSc ist seit 2013 als Senior Security Consultant Teil des Antares Red Teams und dort für die **Durchführung von Penetrationstests** verantwortlich. Bei der Überprüfung von Web-Applikationen und extern erreichbaren Services auf Schwachstellen setzt er auf seine langjährige Erfahrung in den Bereichen Pentesting und Vulnerability Management. Für unsere Kunden implementiert er Sicherheitslösungen, wie Web Application Firewalls und übernimmt die Beratung und Betreuung in den Bereichen Endpoint Security und Passwort Management.

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 ADD-ONS 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. Ergänzend dazu entwickeln wir zur Zeit ein VLM-Ticketsystem, mit dem sich der Bearbeitungsstatus automatisch nachvollziehen lässt. Ein weiterer echter Mehrwert des VLMs ist die Auswertung von Findings, die nicht direkt als Schwachstelle zu interpretieren sind. Dabei handelt es sich beispielsweise um

- die **Auflistung von Domänen-Accounts,** die auf Rechnern lokale Administrationsrechte besitzen,
- **Accounts**, deren Passwort noch nie gewechselt wurden, oder
- die **Zugriffsberechtigungen** auf Shares.

So können wir unseren Kunden einen aussagekräftigen Überblick bieten, an welchen Stellen Rechte weiter eingeschränkt werden sollten bzw. welche Accounts ein potenzielles Ziel für Hacker darstellen.

WOHER KOMMEN DIE DATEN, DIE DER VLM NUTZT?

Die Daten liefern bewährte **Schwachstellen-Scanner** wie Tenable Nessus oder Greenbone GSM, die bei vielen unserer Kunden bereits im Einsatz sind. Als langjähriger Partner beider Hersteller bringen wir hier detaillierte Produktkenntnisse mit und können auch bei der Implementierung unterstützen.

EINIGE EINBLICKE IN UNSER VLM