Schwachstellenbewertung für VMware

ALLGEMEINE BESCHREIBUNG DER DIENSTLEISTUNGEN[1]

Die VMware-Sicherheitsbewertung ist ein rein beratender Sicherheits- und Compliance-Bewertungsdienst, der von Park Place Technologies (PPT) erbracht wird. Der Dienst verwendet ein von PPT verwaltetes, vollständig automatisiertes VMware-Scan-Tool und eine Sicherheitsanalyse-Engine, um schreibgeschützte Konfigurationsdaten zu sammeln und Sicherheitsbewertungsberichte automatisch zu erstellen und bereitzustellen. Alle Analyse-, Validierungs- und Empfehlungsaktivitäten werden von Sicherheitsexperten von PPT durchgeführt.

Dieser Dienst bietet eine umfassende Bewertung der VMware-Virtualisierungsumgebung des Kunden, einschließlich vCenter Server, ESXi-Hosts, Clustern, virtuellen Netzwerken, virtuellen Maschinen und Speicherelementen.

Die Bewertung identifiziert Fehleinstellungen, Sicherheitslücken und Abweichungen in der Compliance, die mit führenden Rahmenwerken wie den CIS Benchmarks, DISA STIGs, VMware-Hardening-Guidelines, dem NIST-Cybersecurity-Framework und SOC 2 Trust Services Criteria in Einklang stehen.

DIENSTLEISTUNGEN UND ERGEBNISSE

PPT führt VMware-spezifische Schwachstellenidentifikation, Konfigurationsanalysen und Compliance-Bewertungen („Dienstleistungen“) durch. Alle Dienstleistungen werden remote bereitgestellt.

Bewertungsaktivitäten

PPT nutzt ein von PPT-verwaltetes, schreibgeschütztes, automatisiertes VMware-Skript und eine Analyse-Engine, um:

- VMware-Konfigurationsmetadaten ohne gespeicherte Anmeldedaten und ohne Änderungen an der Konfiguration zu sammeln.
- Konfigurationen anhand von über 200 VMware-basierten Sicherheitskontrollen zu bewerten.
- Fehlkonfigurationen, unsichere Einstellungen und Konfigurationsabweichungen zu erkennen.
- Ergebnisse gleichzeitig mit mehreren Compliance-Rahmenwerken abzugleichen.
- Probleme in vCenter, ESXi-Hosts, Clustern, VMs, Netzwerken, Zertifikaten, Authentifizierung und Protokollierung zu identifizieren.
- Ergebnisse zu validieren und identifizierbare Fehlalarme zu entfernen.

Ergebnisse

Onboarding

- Implementierung und Erste Bewertung.

[1] Das Scan-Tool („Software“) ist ein proprietäres Produkt von Kalosys, lizenziert durch PPT. Alle Patente, Urheberrechte, Geschäftsgeheimnisse und anderen geistigen Eigentumsrechte verbleiben ausschließlich bei Kalosys und seinen Lizenzgebern. Der Kunde erwirbt nur ein eingeschränktes Nutzungsrecht der Software, jedoch kein Eigentum. Der Kunde darf die Software nicht (a) kopieren, modifizieren oder abgeleitete Werke erstellen; (b) zurückentwickeln, dekompilieren oder zerlegen; (c) Eigentumshinweise oder Etiketten entfernen; (d) unterlizenzieren, vermieten, verleasen oder übertragen; (e) zur Bereitstellung von Dienstleistungen an Dritte verwenden; oder (f) Schutzmaßnahmen umgehen. Der Endbenutzer versteht, dass diese Software für Sicherheitsbewertungen konzipiert ist und stimmt zu, sie nur auf Systemen zu verwenden, die er autorisiert ist zu testen.

- Executive-Briefing, das die grundlegende Sicherheitsbewertung, hoch-stufige Ergebnisse, den Compliance-Status und empfohlene nächste Schritte zusammenfasst.

Commented [RM1]: Sollten wir diese Punkte zur besseren Lesbarkeit als zwei Aufzählungen darstellen?

Automatisierter wiederkehrender Bericht

Automatisch bereitgestellt im vom Kunden gewählten Rhythmus (monatlich, vierteljährlich oder wöchentlich):

- Compliance-Ergebnisse, die mit CIS, DISA STIG, VMware Hardening Guides, NIST CSF und SOC 2 abgeglichen sind.
- Inventar der Sicherheitsbefunde, kategorisiert nach Schweregrad.
- Schwachstellenklassifikation einschließlich CVEs und CVSS-Schwereskalierung.
- Leitfaden zur Behebung mit empfohlenen Korrekturmaßnahmen.
- Priorisierter Aktionsplan, abgestimmt auf Risiko und betriebliche Auswirkungen.
- Berichte, die in verschiedenen unterstützten Formaten bereitgestellt werden.

Beratungsumfang

PPT stellt ausschließlich Analysen und Empfehlungen bereit. Der Kunde ist vollständig verantwortlich für die Durchführung aller Maßnahmen zur Behebung, Konfigurationsänderungen und operativen Aufgaben.

Unterstützter VMware-Umfang

- VMware vSphere 6.7 und höher
- vCenter Server-Dienste, Authentifizierung, Berechtigungen, Protokollierung
- ESXi-Host-Hardening (Dienste, Firewall, Zertifikate, NTP, Passwortrichtlinien/Lockdown-Richtlinien)
- Cluster-Dienste (HA, DRS, EVC, vSAN)
- vSwitch/vDS-Konfiguration und Portgruppen-Sicherheit
- VM-Konfigurationseinstellungen, VMware Tools, Isolationsrichtlinien
- Datenspeicher- und vSAN-Konfiguration

PROZESS UND SLA

Erstbewertung & Implementierung

- Bereitstellung des Scan-Skripts auf einem vom Kunden-festgelegten System.
- Validierung der Werkzeugvoraussetzungen.
- Überprüfung der vCenter-Konnektivität und -Berechtigungen.
- Durchführung der grundlegenden VMware-Bewertung.
- Einrichtung der automatisierten Berichtsbereitstellung.

Executive- und technische Zusammenfassung

- Überblick über grundlegende Ergebnisse.
- Zusammenfassung des Compliance-Status.
- Priorisierte Empfehlungen zur Behebung (nur beratend).

Fortlaufende Bewertungen

- Automatisierte Scans im vom Kunden-definierten Rhythmus.
- Erkennung neuer Schwachstellen und Regressionen.
- Überwachung von Konfigurationsabweichungen.

Berichterstattung über den Fortschritt

- Trends in der Sicherheitslage von VMware.
- Fortlaufende Erkennung von Problemen.

- Einblick in den Fortschritt der Behebungsmaßnahmen.

SERVICE-EINSCHRÄNKUNGEN

Dieser Dienst umfasst nicht:

- Echtzeitüberwachung, SIEM/SOC oder Vorfallreaktionen.
- Untersuchung von Sicherheitsverletzungen oder forensische Analysen.
- VMware-Patching, Upgrades oder Lifecyle-Operationen.
- Durchführung von Behebungs- oder Konfigurationsänderungen.
- Leistungsproblemlösung (Compute, Storage oder Netzwerk).
- Architekturdesign, Engineering oder Kapazitätsplanung.
- Benutzerdefinierte Automatisierung, Skripting oder Integrationen.
- Vorbereitung für Compliance-Zertifizierungen (ISO, PCI, SOC 2).
- ITSM-Unterstützung (Tickets, Workflows, CAB).
- Lizenzbeschaffung oder Berechtigungsmanagement.
- Onsite-Engineering oder Hardware-Dienste.

VERANTWORTLICHKEITEN DES KUNDEN

Der Kunde muss:

- VMware- und Sicherheitspersonal zur Unterstützung der Zusammenarbeit bereitstellen.
- Nur-Lese-Zugangsdaten und Autorisierung für die Bewertungsziele bereitstellen.
- Sicherstellen, dass alle VMware-Systeme während der Scanzeiten zugänglich sind.
- Alle Maßnahmen zur Behebung und operativen Tätigkeiten eigenständig durchführen.
- Die Klassifizierung, Handhabung und Speicherung von Bewertungsdaten verwalten.
- Die vorübergehende Ressourcenbelastung während der Bewertung anerkennen.
- Governance und Änderungsmanagement für alle VMware-Konfigurationen aufrechterhalten.

SICHERHEIT DES SCAN-TOOLS, DATENSCHUTZ & UMFANG DER DATENERFASSUNG

PPT stellt den sicheren und kontrollierten Betrieb des Scan-Tools sicher. Die wichtigsten Elemente umfassen:

- Nur-Lese-, nicht-intrusive Datenerfassung.
- Keine Installation von Agents; es werden keine Änderungen an der Konfiguration vorgenommen.
- Anmeldedaten werden nur während aktiver Sitzungen verwendet und niemals gespeichert.
- Es werden ausschließlich VMware-Konfigurations-Metadaten erfasst (vCenter, ESXi, Cluster, Speicher, Netzwerk, Authentifizierung, Zertifikate, Protokollierung, NTP und maskierte Lizenzdetails).
- Keine Erfassung von Gast-OS-Inhalten, Anwendungsdaten, Benutzerdaten, Passwörtern oder vollständigen Lizenzschlüsseln von VMs.
- Alle Kommunikation ist über HTTPS (Port 443) verschlüsselt.
- Bewertungsartefakte sind während des Transports und der Speicherung verschlüsselt.
- Zugriff ist auf autorisierte PPT- und Kundenmitarbeiter beschränkt.