digicert®

IDENTIFIZIERUNG KRYPTOGRAFISCHER RESSOURCEN MIT DIGICERT®

Die verschiedenen Methoden für den Aufbau eines umfassenden Bestandsverzeichnisses

Überblick

Das Identifizieren von Ressourcen dient dem Zweck, ein zentrales Bestandsverzeichnis zu erstellen, das die Verwaltung verschiedener Ressourcengruppen ermöglicht. So können Sie Richtlinien anwenden, Schwachstellen identifizieren, Algorithmen aktualisieren und Automatisierungsfunktionen für die entsprechenden Zertifikatsklassen (oder andere Ressourcen) durchsetzen.

DigiCert® Trust Lifecycle Manager (TLM) ermöglicht zentrale Transparenz und Kontrolle, um kryptografische Schlüssel und Zertifikate in Unternehmensumgebungen zu finden, zu importieren und zu verwalten, sowie wichtige Funktionen für die Zentralisierung und die Vorbereitung auf quantensichere Algorithmen.

TLM bietet verschiedene Mechanismen zum Identifizieren und Verwalten sämtlicher Zertifikate im Unternehmen und hilft Ihnen damit, kostspielige Ausfälle zu vermeiden.

Die Fakten auf einen Blick

>50.000
Serverzertifikate

1.200
nicht verwaltete Zertifikate

47 %
der Unternehmen kämpfen mit nicht konformen Zertifikaten

500.000 USD
kostet ein Zertifikatsausfall pro Stunde

Methoden zur Identifizierung von kryptografischen Ressourcen

Integration in CertCentral und CA Manager
Durch diese Integration wird das Management des Zertifikatslebenszyklus vom Zeitpunkt der Ausstellung bis hin zur zentralen Verwaltung vereinfacht und Sie können diese Zertifikate jederzeit identifizieren. Eine solche umfassende Funktionalität bieten CA-unabhängige CLM-Lösungen in der Regel nicht.

Verknüpfung mit anderen CAs
Die meisten CA-basierten Lösungen können keine Zertifikate identifizieren, die nicht von ihnen ausgestellt wurden. Das ist eine Tatsache, die von den Anbietern CA-unabhängiger Lösungen immer wieder als Verkaufsargument angeführt wird. Trust Lifecycle Manager hingegen unterstützt sowohl von DigiCert als auch von anderen Zertifizierungsstellen ausgestellte Zertifikate.

Port-Scans
Port-Scans sind die einfachste Möglichkeit, Zertifikate zu identifizieren, die nicht direkt von einer Zertifizierungsstelle ausgestellt wurden. Dabei installiert die CLM-Lösung einen Sensor in Ihrer IT-Infrastruktur, den sie für die Zertifikatsuche nutzt.

Sensoren für die Zertifikatsuche auf Load-Balancern
Mithilfe von Sensoren kann Trust Lifecycle Manager Zertifikate automatisiert verwalten, die Load-Balancern nachgeschaltet sind. Angesichts der großen Anzahl von Zertifikaten, die im Zusammenhang mit Load-Balancern zu erwarten sind, ist dies eine wichtige Funktion.

Agentenbasierte Scan-Tools
Bestimmte Zertifikate, zum Beispiel auf Microsoft IIS- oder Apache-Webservern installierte Zertifikate, können mit Port-Scans nicht erkannt werden. Daher setzt TLM Agenten ein, die gewisse Informationen über solche Zertifikate erfassen.

Tools für die Schwachstellenanalyse
TLM nutzt vorhandene Tools für die Schwachstellenerkennung, die bereits jeden Winkel des Netzwerks durchsuchen, um ein komplettes Bestandsverzeichnis der Ressourcen und der Umgebungsstruktur anzulegen und zu pflegen.

Die Vorteile von DigiCert® Discovery

Mehr Transparenz
Verschaffen Sie sich einen zentralen Überblick über alle kryptografischen Ressourcen, um die Verwaltung und Ausstellung in allen Unternehmensumgebungen zu unterstützen.

Weniger Risiken
Finden und beheben Sie schnell Probleme wie schwache Algorithmen, nicht signierte Binärdateien und auslaufende, anfällige oder nicht konforme Zertifikate.

Strengere Durchsetzung von Richtlinien
Verringern Sie das Risiko der Ausstellung nicht konformer Zertifikate im Namen einer Zertifizierungsstelle und überwachen Sie die Einhaltung von Sicherheitsrichtlinien.

Krypto-Flexibilität
Die Erkennung von Ressourcen ist der erste Schritt bei der Vorbereitung auf die Post-Quanten-Kryptografie. Dieser Schritt ermöglicht Transparenz sowie den flexiblen Einsatz der kryptografischen Ressourcen eines Unternehmens.

Integration von Tenable
TLM unterstützt die Nutzung von Tenable – einer Lösung, die eigene Plug-ins für die Zertifikatsuche und die Identifizierung von Daten verwendet.

Integration von Qualys
Die Verzahnung von Qualys VMDR (Vulnerability Management, Discovery and Response) und DigiCert-Produkten ermöglicht Nutzern, die bei Schwachstellen-Scans gefundenen kryptografischen Ressourcen manuell oder automatisiert zu verwalten.

AWS und Microsoft-CAs
Aufgrund der verstärkten Cloud-Nutzung finden sich immer mehr Zertifikate, die von Zertifizierungsstellen wie AWS Private CA und Microsoft-CAs ausgestellt werden. Es ist wichtig, auch diese Zertifikate zu identifizieren, damit sie in das zentrale Bestandsverzeichnis eines Unternehmens aufgenommen und katalogisiert werden können.

Erste Schritte

Wenn Sie an den PKI-Diensten von DigiCert® interessiert sind, wenden Sie sich an Ihren DigiCert Account Manager oder senden Sie eine E-Mail an sales@digicert.com.

Über DigiCert, Inc.

Als einer der weltweit führenden Anbieter digitaler Vertrauenslösungen sorgt DigiCert dafür, dass Unternehmen und Einzelpersonen digitalen Interaktionen in dem Wissen vertrauen können, dass ihre digitale Infrastruktur und ihre Anbindung an eine Welt voller Online-Transaktionen sicher und geschützt sind. DigiCert® ONE, die Plattform für digitale Vertrauensdienste, bietet Unternehmen eine zentrale Anlaufstelle für Einblicke und die Kontrolle über eine Vielzahl von öffentlichen und privaten Anwendungsbereichen, in denen das Vertrauen eine wichtige Rolle spielt. Dazu gehören der sichere Zugriff auf Unternehmenssysteme, sichere Business-Kommunikation sowie der Schutz von Websites, Software, Identitäten, Inhalten und Geräten.

DigiCert bietet nicht nur preisgekrönte Softwarelösungen an, sondern hat sich nicht zuletzt auch durch seine branchenweite Führungsrolle bei Standards, Support und Betrieb als bevorzugter Anbieter digitaler Vertrauenslösungen bei Unternehmen auf der ganzen Welt einen Namen gemacht. Weitere Informationen finden Sie unter digicert.com/de oder in den sozialen Medien unter @digicert.