digicert®

Leitfaden zur Bewertung der Reife von Zertifikats-lebenszyklen

Ihr Weg zur Senkung von Kosten und Vermeidung von Ausfällen mit einer agilen Public Key Infrastructure (PKI)

LEITFADEN

Einleitung

Unsere vernetzte Welt erfordert modernes Zertifikatsmanagement

PKI-Zertifikate bilden die Grundlage für Digital Trust in der vernetzten Welt. Moderne Netzwerke basieren auf immer komplexer werdenden Infrastrukturen, die kontinuierlich skaliert und in Anpassung an Unternehmensanforderungen weiterentwickelt werden. Diese Netzwerke existieren nicht isoliert. Moderne Systeme interagieren mit vielen anderen (internen und externen) Netzwerken. Um bei diesem Maß an Komplexität Vertrauen zu schaffen, benötigen Sie einen Ansatz für das Zertifikatsmanagement, der gleichermaßen skalierbar und anpassungsfähig ist.

Methodik

Was bedeutet der Reifegrad beim Management des Zertifikatslebenszyklus (Certificate Lifecycle Management; CLM)?

Die CLM-Reife bezeichnet die Entwicklung von manuellen, reaktiven Praktiken hin zu automatisierten, richtliniengesteuerten Abläufen. Mit zunehmender Reife sinken die mit CLM verbundenen Kosten und Risiken erheblich. Die Implementierung effektiverer Managementtools, Richtlinien und integrierter Automatisierung sind allesamt wichtige Elemente auf dem Weg zu kryptografischer Agilität.

Krypto-Agilität ist die Fähigkeit, kryptografische Algorithmen, Schlüssel und Protokolle schnell und automatisiert zu aktualisieren oder zu ersetzen, ohne den Betriebsablauf merklich zu stören. CLM ist eine wichtige Komponente der Krypto-Agilität. Dabei muss jedoch klar sein, dass dieser Bereich auch andere kryptografische Assets umfasst, z. B. kryptografische Schlüssel für Datenbanken, Computerfestplatten und MFA-Schlüssel (Multifaktor-Authentifizierung).

Die Renaissance der PKI

PKIs erleben derzeit ein Comeback, das vorauszusehen war. Dies wird durch eine Reihe von Ereignissen vorangetrieben, die Maßnahmen zur Bewältigung von Sicherheitsbedrohungen, Vorschriften, Skalierbarkeit und Herausforderungen beim Lebenszyklusmanagement erfordern. Die gute Nachricht ist, dass dieser Wandel zu einer neuen Generation von PKIs führen wird, die sicherer, widerstandsfähiger und flexibler sind.

Faktoren, die die Renaissance der PKI vorantreiben

- **Verkürzte Gültigkeitsdauer von Zertifikaten**
  Bis 2029 müssen Organisationen für alle Anwendungsbereiche im Zusammenhang mit öffentlichem Vertrauen Zertifikate mit einer Gültigkeitsdauer von 47 Tagen verwenden. Diese Entscheidung des CA/Browser Forum macht es praktisch unmöglich, manuelle Prozesse aufrechtzuerhalten.

- **Explosion der Geräteidentitäten**
  Von APIs und IoT-Geräten bis hin zu Containern und Multi-Cloud-Umgebungen sind Maschinen und Geräte heute für Milliarden von Verbindungen verantwortlich. Bald wird es dreimal so viele Geräte wie Menschen geben – die anstehende Flut von KI-Agenten, die ebenfalls vertrauenswürdige Identitäten benötigen, nicht mitgerechnet.

- **Umfang und Komplexität des Betriebs**
  In herkömmlichen Cloud- und Hybrid-Umgebungen verschwimmen die Grenzen zwischen externen, internen und föderierten PKIs. Diese Systeme erfordern große Mengen an unterschiedlichen Zertifikatstypen, wofür wiederum eine flexible CLM-Lösung benötigt wird, die alles nahtlos miteinander verbinden kann.

- **Die Quantenbedrohung**
  Die Grundlage jeder PKI – kryptografische Algorithmen, die mit der heutigen Rechenleistung weder erraten noch per Brute Force geknackt werden können – ist nun bedroht. Quantencomputer werden bald in der Lage sein, vorhandene Krypto-Algorithmen auszuhebeln. Es gibt bereits neue, quantensichere Algorithmen, aber diese müssen nach Aussagen von Gartner und anderen Branchenexperten bis 2029 noch getestet und implementiert werden.

Die Skala der CLM-Reife

Die nachstehende Skala zeigt drei Stufen des CLM-Reifegrads auf: Ad hoc, in Entwicklung und solider Reifegrad. Hier finden Sie einen Überblick darüber, wie Ihr Zertifikatsmanagement im jeweiligen Stadium aussehen könnte. In den folgenden Abschnitten wird diese Skala auf sechs wichtige Best-Practice-Bereiche im CLM angewandt – mit einer auf die jeweilige Disziplin abgestimmte Beschreibung des Reifegrads für jede Stufe.

- Ad hoc
  Das Management erfolgt in erster Linie in Form von reaktiven, manuellen Prozessen, die kaum einen Einblick in die gesamte Zertifikatslandschaft oder bestehende Risiken bieten. Die Prozesse sind schwer zu kontrollieren und Richtlinien sind unterentwickelt oder existieren isoliert, so dass sie nur schwer durchgesetzt werden können. Der Zertifikatsbestand wird häufig in Tabellenkalkulationen verwaltet.

- In Entwicklung
  Die Managementprozesse ermöglichen einen zentralen Überblick mit teilweiser Kontrolle über Risikoaufklärung und -minderung. Die Umstellung auf richtliniengesteuertes Management ist im Gange und die Erneuerung von Zertifikaten ist für mehr als 30 % der Systeme automatisiert. Für einige wenige kritische Systeme und Anwendungen erfolgt eine automatische Bereitstellung von Zertifikaten. Ausfälle aufgrund von Fehlern beim manuellen Zertifikatsmanagement sind keine Seltenheit.

- Solider Reifegrad
  Die Managementprozesse ermöglichen einen zentralen Überblick mit fast kompletter Kontrolle über Risikoaufklärung und -minderung. Eine richtliniengesteuerte Governance ist hier eher die Regel als die Ausnahme. Zertifikatserneuerungen sind für über 50 % der Systeme automatisiert und für die wichtigsten Systeme erfolgt die Bereitstellung automatisiert. Der Schwerpunkt liegt auf dem Onboarding und der Integration von Tier-2- und Tier-3-Systemen als Teil einer umfassenderen kryptoagilen Strategie.

Anwendung des Modells auf Ihre Organisation

Da die Bedürfnisse Ihrer Organisation einzigartig sind, erfordert die Anwendung kryptoagiler Tools und Prozesse auf Ihre Zertifikatslandschaft ein Verständnis dafür, wo Sie sich im Reifegradmodell befinden. Dieser Leitfaden hilft Ihnen, sechs Schlüsselbereiche beim Management des Zertifikatslebenszyklus zu bewerten, um die Position Ihres Unternehmens auf dem Weg zur Krypto-Agilität zu ermitteln.

Bewertung

Bewertung der CLM-Reife Ihres Unternehmens

Diese Best Practices beschreiben einen Idealzustand für Lösungen, Arbeitsabläufe und Governance rund um eine kryptoagile PKI. Nutzen Sie diese Beschreibungen, um Ihren derzeitigen Status zu beurteilen und Maßnahmen zur Steigerung des Reifegrads einzuleiten.

Kategorie 1

Zertifikatsuche und Bestandsaufnahme

Sie müssen wissen, wo sich Ihre Zertifikate befinden, wie sie konfiguriert sind, wann sie ablaufen, wem sie zugeordnet sind und welche Bedeutung sie für das Unternehmen haben. Für die Erstellung eines Inventars sind Daten aus verschiedenen Quellen erforderlich, um Ihre externen, internen und eingebetteten PKIs vollständig zu erfassen.

- **Ad hoc:** Manuelle Erfassung, in der Regel mithilfe von Tabellenkalkulationen. Aufgrund fragmentierter, begrenzter Sichtbarkeit haben Unternehmen nur wenig Einblick in die gesamte Zertifikatslandschaft und die damit verbundenen Risiken.

- **In Entwicklung:** Geplante Zertifikatsuche mit begrenzter Automatisierung. Es wird identifiziert, wem Zertifikate zugeordnet sind, und es gibt grundlegende Benachrichtigungen für Zertifikatserneuerung und -ablauf, was die Sichtbarkeit und Rückverfolgung verbessert.

- **Solider Reifegrad:** Kontinuierliche Zertifikatsuche in Echtzeit in internen und externen PKI-Quellen sowie in PKIs von Drittanbietern. Zuständigkeiten werden zentral dokumentiert und umfassend für proaktive Warnungen, Genehmigungsworkflows und Governance genutzt. Das System ermöglicht auch Analysen zur Kostenverfolgung und Prognose.

Erklärung

Die Zertifikatsuche ermöglicht die Inventarisierung, die wiederum den Weg für Richtlinien und letztlich die Automatisierung ebnet. Dank Such- und Inventarisierungsfunktionen sind Sie immer darüber im Bilde, wo sich Ihre Zertifikate (auch Zertifikate aus der Schatten-IT) befinden, wie sie konfiguriert sind, wann sie ablaufen, wem sie zugeordnet sind und welche Bedeutung sie für das Unternehmen haben.

Kategorie 2

Richtlinien und Governance

Hier geht es um die Einführung und Durchsetzung klar definierter Richtlinien, die das Ausstellen, Erneuern und Widerrufen von Zertifikaten auf der Basis von Regeln ermöglichen. Diese Richtlinien verhindern Missbrauch, minimieren das Risiko von zertifikatsbedingten Ausfällen und unbefugtem Zugriff und stellen sicher, dass die Organisation Standards und Vorschriften einhält.

- **Ad hoc:** Governance, sofern vorhanden, erfolgt punktuell und in der Regel reaktiv. Es gibt keine wirksame Möglichkeit, Richtlinien umgebungsweit anzuwenden und zu überprüfen, was Konsistenz und Rückverfolgung nahezu unmöglich macht.
- **In Entwicklung:** Zwar ist die Kommunikation konsistent und es gibt ein gewisses Maß an Governance, aber die Durchsetzung von Richtlinien erfolgt immer noch weitgehend manuell. Es ist nach wie vor schwierig, Richtlinien in allen Geschäftsbereichen oder Regionen einheitlich anzuwenden.
- **Solider Reifegrad:** Governance ist durch richtliniengesteuerte Automatisierung in die CLM-Prozesse eingebettet. Regeln werden dynamisch angewandt und sorgen für konsistente Ausstellungs-, Erneuerungs- und Widerrufabläufe. Teams können schnell über den Status von PKI-Assets Bericht erstatten.

Erklärung

Strenge Richtlinien und Governance-Prozesse reduzieren Bedienfehler, beschleunigen Problembehebung und sorgen für team- und umgebungsübergreifende Rückverfolgbarkeit. So wird das Zertifikatsmanagement von einer reaktiven Belastung zu einem proaktiven, strategischen Vorteil.

Kategorie 3

Integrierte CLM-Automatisierung

Dabei handelt es sich um die Möglichkeit, die Erneuerung und Bereitstellung von Zertifikaten bei den entsprechenden Zertifizierungsstellen sowie die Bereitstellung von Zertifikaten für bestimmte Server, Anwendungen, Geräte usw. auf einer wiederholbaren Basis mit minimalem menschlichem Eingreifen zu automatisieren. Zu den Voraussetzungen gehören ein zuverlässiges, zentralisiertes Inventar mit definierten Inhabern und Richtlinien sowie unterschiedliche Integrationsmethoden und -protokolle, je nach den Anforderungen der einzelnen Systeme.

Hinweis: Obwohl das ACME-Protokoll (Automated Certificate Management Environment) oft synonym mit dem Thema CLM-Automatisierung verwendet wird, stellt ACME jedoch nur einen kleinen Teil der CLM-Automatisierung dar.

- **Ad hoc:** Es gibt keine automatisierten Management- oder Erneuerungsfunktionen. Administratoren erneuern und installieren Zertifikate manuell, wobei sie durch Kalendereinträge oder andere Benachrichtigungsfunktionen daran erinnert werden. Mit steigendem Zertifikatsvolumen und abnehmender Gültigkeitsdauer steigt der Aufwand für diese Arbeit und die Anzahl der Ausfälle nimmt zu.
- **In Entwicklung:** Einzelne Geräte sind so konfiguriert, dass sie den Zertifikatsstatus prüfen und Zertifikate automatisch erneuern und installieren, wobei sie nach einem Zeitplan arbeiten. Die Automatisierung läuft dezentral ab und es gibt keine Möglichkeit, den Status zentral zu überwachen, auf Fehler zu reagieren oder Richtlinien anzuwenden.
- **Solider Reifegrad:** Zertifikatserneuerung, -austausch und -installation erfolgen über zentralisierte Automatisierungsfunktionen auf der Grundlage eines zentralen Inventars und der durch globale Richtlinien definierten Inhaberschaft. Die Automatisierung trägt dazu bei, die geplante Einführung kryptografischer Änderungen, einschließlich der Post-Quanten-Kryptografie, zu erleichtern.

Erklärung

Da ACME auf jedem Endpunkt konfiguriert werden muss, ist die Skalierbarkeit in komplexen Umgebungen schwierig. Selbst wenn verschiedene Teams oder Systeme als Zertifikatsinhaber definiert sind, ist ein zentraler Managementansatz unerlässlich, um Transparenz, Konsistenz und Kontrolle zu ermöglichen. Das kann ACME allein nicht bieten. Sie benötigen andere Protokolle und Integrationen, um alle Aufgaben in Ihrem

gesamten Ökosystem zentral zu verwalten.

Kategorie 4

Audit-Bereitschaft

Dies ist die Fähigkeit, alle Zertifikate automatisiert zu verfolgen und proaktiv zu protokollieren, wobei die erforderlichen Analysen und Berichte unterstützt werden, um schnell Nachweise für die Einhaltung von Vorschriften zu erbringen. Dazu gehört auch Vereinheitlichung von Zertifikatsdaten, zugehörigen Änderungsprotokollen in Unternehmenssystemen (einschließlich Active Directory) und Asset-Management-Plattformen wie SAP EAM und ITSM-Tools.

- **Ad hoc:** Es gibt praktisch keine Nachweise für die Einhaltung von Vorschriften bzw. fehlt die Fähigkeit, diese zeitnah zu produzieren. Ohne einen Überblick über die vorhandenen Ressourcen, Risiken und Anforderungen ist ein Unternehmen nicht in der Lage, auf Audit-Anforderungen zu reagieren oder Ausfälle zu verhindern.
- **In Entwicklung:** Inventare und Nachweise über die Einhaltung von Richtlinien sind vorhanden, aber nicht zentralisiert. Richtlinien und Verfahren werden nicht konsistent für alle Zertifikate und Anwendungen verfolgt. Das Unternehmen kann sich einen Überblick verschaffen und Audit-Anforderungen nachkommen, aber beides ist ressourcenintensiv.
- **Solider Reifegrad:** Zertifikate, Richtlinien und Verfahren sind für die Mehrzahl der Anwendungen im Unternehmen vollständig erfasst. Zur Erfüllung von Betriebsprüfungen kann die Durchsetzung von Richtlinien schnell belegt werden.

Erklärung

Um Compliance-Verletzungen zu vermeiden, müssen Sie wissen, wo sich Ihre Zertifikate befinden. Außerdem müssen Sie eine Möglichkeit haben, sie aktiv zu verwalten. Das geschieht über eine umfassende Prüfung aller CAs und Systeme mit der Möglichkeit, Berichte zu erstellen, die den Branchenstandards entsprechen.

Kategorie 5

Öffentliche, interne und föderierte PKI

Hier geht es um umfassende Transparenz und Kontrolle über alle PKIs (öffentlich, intern und föderiert), unabhängig vom Anwendungsbereich. Zudem müssen Sie in der Lage sein, das richtige zertifikatsbasierte Vertrauensmodell für jeden Anwendungsfall zu verwenden.

- **Ad hoc:** Wahrscheinlich gibt es innerhalb der Organisation interne PKIs, aber die Fähigkeit, diese privaten CA-Zertifikate zu finden und zentral zu verwalten, ist nicht vorhanden.
- **In Entwicklung:** Das Unternehmen hat einen Überblick über seine einzelnen PKIs und hat kritische Sicherheits- oder Compliance-Probleme behoben. Die PKIs sind jedoch nach wie vor isoliert und werden getrennt verwaltet.
- **Solider Reifegrad:** Ein konsolidiertes System ermöglicht dem Unternehmen umfassende Einblicke in und das Management von öffentlichen, internen und föderierten PKIs. Das Management der internen PKIs erfolgt über eine zentralisierte Lösung und nicht über Anwendungstools. Ein leistungsstarkes CLM-System kann Active Directory-Zertifikate problemlos verwalten und so eine Microsoft-CA ersetzen. Das System kann Zertifikate von jeder öffentlichen Zertifizierungsstelle verwalten und Sie können Zertifikate leicht zwischen CAs verschieben.

Erklärung

In der Praxis haben Unternehmen meist viel mehr Zertifikate in privaten oder internen PKIs als in öffentlichen PKIs, aber diese Zahl sollte wahrscheinlich noch größer sein. Systemadministratoren verwenden manchmal öffentliche Zertifikate, insbesondere kostenlose, wenn eine Anwendung mit einer internen oder föderierten PKI sicherer wäre. Dies stellt ein Risiko dar. Wählen Sie die richtige PKI für den jeweiligen Anwendungsfall und verschaffen

Sie sich die Möglichkeit, jedes Zertifikat, unabhängig vom Typ, zu überwachen und zu kontrollieren.

Kategorie 6

Skalierbarkeit und Erweiterbarkeit

Kryptoagile Lösungen und Prozesse unterstützen das Wachstum, unternehmensweite Veränderungen im Laufe der Zeit und die Bereitschaft für PQC-Integrationen.

- **Ad hoc:** Das Zertifikatsmanagement ist fragmentiert, kann nicht skaliert werden und erfordert manuelle Eingriffe bei jedem Schritt. Das Ergebnis ist ein unzuverlässiges, reaktives System, das sich nicht ohne Weiteres weiterentwickeln kann.
- **In Entwicklung:** Die Ausstellung von Zertifikaten ist teilweise standardisiert und erfolgt über eine Mischung aus vorhandenen privaten CAs, Cloud-Diensten und öffentlichen CAs. Das Zertifikatsmanagement sowie die Entwicklung und Pflege von Integrationen sind allerdings immer noch fragmentiert.
- **Solider Reifegrad:** Die PKI wird zentral gesteuert und kann daher sowohl vor Ort als auch in einer oder mehreren Clouds betrieben werden. Sie lässt sich bei einem Anstieg von Nutzern und Rechnern skalieren und kann in viele Technologien integriert werden, wenn sich die Unternehmensinfrastruktur weiterentwickelt.

Erklärung

Unzuverlässige Integrationen verursachen häufig Probleme, die behoben werden müssen, und können neue Anforderungen und Arbeitsabläufe oft nicht unterstützen. Ausgereifte CLM-Prozesse versetzen Ihr Unternehmen in die Lage, dynamisch auf Geschäfts- und Sicherheitsanforderungen zu reagieren. Sie unterstützen die automatische Bereitstellung, die flexible Durchsetzung von Richtlinien und die nahtlose Integration in On-Premises-, Cloud- und Hybrid-Umgebungen.

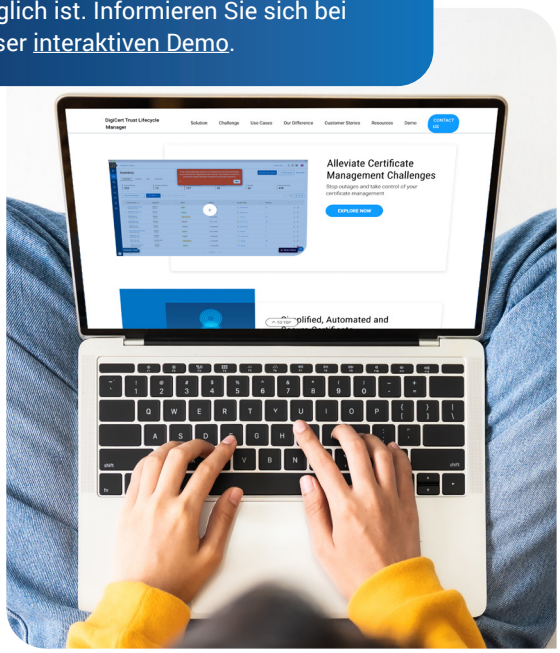
So geht es weiter

Die nächsten Schritte

Sie haben ein Gefühl für den aktuellen Reifegrad Ihrer Organisation bekommen, doch wie geht es weiter? Denken Sie daran, dass die Automatisierung selbst nicht das abschließende Ziel ist und dass es nicht darum geht, einen finalen Reifegrad zu erreichen. Wenn Sie sich auf kryptoagile Lösungen, Prozesse und Richtlinien konzentrieren, kann sich Ihr Unternehmen auch weiterhin anpassen, wenn Ihre Systeme wachsen, wenn sich Standards weiterentwickeln und wenn neue Bedrohungen auftauchen.

Mit der richtigen Lösung für das Management des Zertifikatslebenszyklus können Sie Ihre Infrastruktur zukunftssicher machen, für Compliance sorgen und das Vertrauen in ein sich schnell veränderndes digitales Ökosystem aufrechterhalten.

Sehen Sie selbst, was mit DigiCert möglich ist. Informieren Sie sich bei dieser interaktiven Demo.



Über DigiCert

DigiCert steht für mehr Sicherheit im Internet. Dieses Ziel prägt bis heute unsere gesamte Unternehmensgeschichte. Das ist der Grund, warum Personen und Unternehmen auf der ganzen Welt unseren PQC-, TLS-, PKI- und IoT-Lösungen vertrauen, unsere Zertifikate täglich millionenfach genutzt werden und warum unsere Kunden unsere Services und unseren Support so oft mit fünf Sternen bewerten. Deshalb werden wir auch weiterhin den Weg zu einer quantensicheren Zukunft ebnen, die auf digitalem Vertrauen für die reale Welt beruht. Digital Trust. Echt gemacht.