CSC

Die SSL-Landschaft

Einblicke in das Zertifikatsmanagement für einen grundlegenden Transformationsprozess

Zusammenfassung: Die SSL-Landschaft verändert sich – und ein fragmentiertes Management kann Unternehmen teuer zu stehen kommen

Angesichts der bevorstehenden Verkürzung der Lebenszyklen von SSL-Zertifikaten (Secure Sockets Layer) können es sich Unternehmen nicht leisten, den Übergang zur Zertifikatsautomatisierung zu verzögern. Genauso wenig können sie es sich leisten, die Sicherheit ihrer Domains durch fragmentiertes SSL-Management zu gefährden.

Die Domainsicherheit befindet sich in einer entscheidenden Umbruchphase – einer Phase, die Unternehmen beim Schutz ihrer Online-Marken und digitalen Identitäten weit zurückwerfen könnte. Vor allem die Abschaffung der WHOIS-E-Mail-Validierung zu Beginn dieses Jahres und die bevorstehende Verkürzung der Zertifikatslaufzeiten sowie der Wiederverwendungszeiträume der Domain Control Validation (DCV) ab März 2026 werden erhebliche Veränderungen in der Arbeitsweise von Unternehmen zur Folge haben.

Bis 2029 werden die Lebenszyklen von SSL- und TLS-Zertifikaten von 367 Tagen auf nur noch 47 Tage verkürzt. Das bedeutet, dass Unternehmen, die bisher etwa ein Jahr Zeit hatten, um ein Zertifikat zu erneuern, dies nun fast achtmal pro Jahr tun müssen. Darüber hinaus werden die DCV-Wiederverwendungszeiträume bis 2029 von 367 Tagen auf nur noch 10 Tage verkürzt.

Diese Änderungen erfolgen zu einer Zeit, in der kostengünstige, leicht zu beschaffende DV-Zertifikate den Markt dominieren.

Cyberkriminelle nutzen diese günstigen oder kostenlosen Zertifikate, um ihren betrügerischen Websites den Anschein von Authentizität zu verleihen, wenn sie sich als Markenhersteller unter Verwendung der gleichen Zertifikatstypen ausgeben. So können sie Kunden dazu verleiten, auf Links zu klicken, um deren Daten zu kompromittieren.

Gleichzeitig legen einige Unternehmen mehr Wert auf Sicherheit: Unser jährlicher „Bericht zur Domainsicherheit“ hat jedoch gezeigt, dass ein Großteil der Unternehmen nach wie vor erhebliche Domainsicherheitsrisiken aufweist. Unsere Untersuchung ergab, dass mehr als zwei Drittel aller Global-2000-Unternehmen weniger als die Hälfte der empfohlenen Sicherheitsmaßnahmen implementiert haben.

Für diesen Bericht über die SSL-Landschaft haben wir Nutzungstrends und -muster für mehr als 802.000 digitale Zertifikate analysiert, die mit 2,4 Millionen Domains verknüpft sind, um zu verstehen, wie Unternehmen SSL-Zertifikate überwachen und wie sich dies auf die Integritätssicherheit dieser Domains auswirkt. Bei unseren Recherchen und persönlichen Interaktionen mit Unternehmensleitern haben wir festgestellt, dass Unternehmen die Umsetzung einer strategischen Antwort auf die verkürzten SSL-Zertifikatslebenszyklen und DCV-Wiederverwendungszeiträume ignorieren oder verzögern. Dieser Bericht bietet einen detaillierten Blick auf diese Problematik – sowie die notwendigen Schritte, um sie zu umgehen.

Zu viele Marken entscheiden sich für einfacher zu beschaffende Zertifikate

Ein SSL-Zertifikat authentifiziert die Legitimität und Sicherheit einer Online-Marke, indem es die Anmeldeinformationen des Zertifikats validiert und die Verbindung zwischen dem Server einer Website und dem Browser eines Benutzers verschlüsselt.

SSL-Zertifikate haben zwei Schlüsselfunktionen:

- **Sicherheit:** Die Verschlüsselung gewährleistet den Schutz von Anmeldeinformationen, Kreditkartennummern und anderen sensiblen Daten.
- **Vertrauen:** Nutzer vertrauen darauf, dass eine Website mit einem Zertifikat im Besitz einer seriösen Organisation ist, die die Website betreibt, und dass die Datenübertragung gesichert ist. Das Authentifizierungsniveau variiert mit den Validierungsebenen eines Zertifikats.

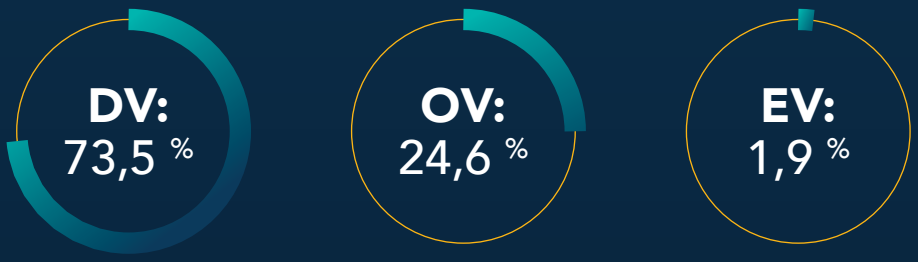
Laut unserer Untersuchung ist dieser ideale Zustand von Sicherheit und Vertrauen jedoch eher die Ausnahme als die Norm, da die große Mehrheit der Online-Marken Zertifikatsarten wählt, die einfacher zu beschaffen sind, um den Arbeitsaufwand zu verringern und die Geschwindigkeit zu erhöhen.

Es gibt drei Stufen der SSL-Zertifikatsvalidierung:

- **Domain-Validierung (DV).** Dies sind die kostengünstigsten und am schnellsten zu erhaltenden Zertifikate. Ein DV-Zertifikat prüft nur, ob der Käufer des Zertifikats den Domainnamen kontrolliert. Jeder Domainnamen-Registrant kann ein SSL-Zertifikat erhalten, unabhängig davon, wie er den Domainnamen verwenden möchte.
- **Organisationsvalidierung (OV).** Die OV erfüllt die gleichen Aufgaben wie die DV, wobei bestimmte Details über die Organisation authentifiziert werden, wie z. B. die Bescheinigung über die Unternehmensregistrierung.
- **Erweiterte Validierung (EV).** Die EV ist das gründlichste und sorgfältigste Zertifikat, das durch eine gründliche Überprüfung der rechtlichen, physischen und betrieblichen Existenz der Organisation ergänzt wird.

In unserer Untersuchung stellten wir fest, dass DVs drei Viertel (73,5 %) der Zertifikate und OVs fast ein Viertel (24,6 %) ausmachen. EVs machen weniger als 2 Prozent (1,9 %) aus.

Anteil der Zertifikatsarten:



Es überrascht nicht, dass DV-Zertifikate am beliebtesten sind, da sie einfacher und schneller zu erwerben sind. Wenn Unternehmen auf Anbieter zurückgreifen, die diese kostengünstigen Zertifikate anbieten, können Cyberkriminelle dieselben Zertifikate von denselben Anbietern nutzen, um ihre betrügerischen Websites zu legitimieren und das Vertrauen der Nutzer durch das zusätzliche Hypertext Transfer Protocol Secure (HTTPS) zu gewinnen. Die Betrüger sind inzwischen viel raffinierter als früher, als gefälschte Websites noch Tipp- und Grammatikfehler enthielten. Böswillige Akteure sind äußerst geschickt in ihrer Tarnung, und der einfache Zugang zu DV-Zertifikaten erleichtert es ihnen, sich als legitimes Unternehmen auszugeben.

In der Vergangenheit wurde auf Websites, die EV-Zertifikate verwendeten, ein grüner Balken angezeigt, der die Besucher darüber informierte, dass die Website durch eine sorgfältig überprüfte Organisation gesichert ist. Der grüne Balken wird von den gängigen Browsern nicht mehr unterstützt, weshalb die Verbreitung von EV-Zertifikaten zurückgegangen ist.

Diese Daten werfen folgende Fragen auf: Haben die IT-Abteilungen eine klare Strategie dafür, welches Zertifikat für welche Art von Web-Asset erworben wird? Oder erwerben sie lediglich DV-Zertifikate, weil sie „einfach und schnell“ sind?

Mehrere Anbieter verursachen mehrere Risikopunkte

Anzahl der Anbieter	% untersuchte Unternehmen
1	22,4 %
2	18,5 %
3	16,6 %
4	15,8 %
5	12,2 %
6	7,4 %
7	4,1 %
8	1,9 %
9	1,0 %
10 oder mehr	0,3 %

Unsere Untersuchung zeigt, dass fast **60 % der Unternehmen** drei oder mehr Zertifikatsanbieter nutzen, wobei ein Unternehmen sogar 13 Anbieter hatte.

Aus der obigen Tabelle geht hervor, dass die große Mehrheit der Unternehmen mehrere Zertifikatsanbieter nutzt.

Tatsächlich nutzen etwa 60 % der Unternehmen drei oder mehr Anbieter, was aus Managementperspektive zu erheblichen Problemen führen kann. Die Folge sind möglicherweise ein uneinheitlicher Ansatz und fragmentierte, kontraproduktive Prozesse, deren Auswirkungen sich mit dem Übergang zu kürzeren Lebenszyklen und DCV-Wiederverwendungszeiträumen exponentiell bemerkbar machen werden.

Die Konsolidierung bei einem einzigen Anbieter macht die Erneuerung von Zertifikaten – und die Behebung von Problemen – wesentlich schneller und effizienter. Wenn ein SSL-bezogenes Problem auftritt, wenden sich die Mitglieder des Sicherheitsteams zur Lösung des Problems einfach an eine Anlaufstelle, wenn sie mit einem einzigen Anbieter arbeiten.

Darüber hinaus reduziert die Zusammenarbeit mit einem einzigen Anbieter das Risiko. Anstatt mehrere Verlängerungsfristen über verschiedene Anbieter hinweg zu jonglieren, sorgt ein zuverlässiger Anbieter für rechtzeitige Verlängerungsbenachrichtigungen. Der Umgang mit mehreren Anbietern führt möglicherweise auch zu Einbußen hinsichtlich der Kosteneffizienz, die durch die Zusammenarbeit mit einem einzigen Zertifikatsanbieter erzielt werden kann.

Führende Anbieter bieten keinen Support der Enterprise-Klasse

Die drei führenden Zertifikatsanbieter:

Let's Encrypt, Google® und Amazon®

Zusammen: 66 % aller analysierten Zertifikate

Diese drei Anbieter stellen die Mehrheit der DV-Zertifikate (89 %), die von den untersuchten Unternehmen genutzt werden. Ihre kostengünstigen Angebote sprechen einerseits Unternehmen an, die ihre Kosten senken wollen, andererseits sind diese Anbieter eine Hauptquelle für Zertifikate für betrügerische Domains, die das Enforcement-Team von CSC aus dem Verkehr gezogen hat. Diese für legitime Unternehmen attraktive Zugänglichkeit ist auch böswilligen Akteuren verfügbar.

Die führenden Zertifikatsanbieter für betrügerische Domains, die von CSC ausgeschaltet wurden:

Google | Let's Encrypt | Cloudflare® | Amazon

Auf der Suche nach Kosteneinsparungen und Geschwindigkeit entscheiden sich Unternehmen für diese Privatkunden-Anbieter. Diese Anbieter können jedoch nicht den Support der Enterprise-Klasse bieten, den Unternehmen benötigen, um sich auf die bevorstehenden Änderungen in der SSL-Branche vorzubereiten. Dieser kurzsichtige Ansatz verursacht auch unnötige Komplikationen in Bezug auf die engeren Zertifikatserneuerungszyklen.

Unternehmen können es sich nicht leisten, die Vorbereitungen für die 47-Tage-Fenster zu ignorieren oder zu verzögern. Denn wenn sie bis zur letzten Minute warten, sehen sie sich mit einer unglaublich komplexen und disruptiven Umstellung konfrontiert. Unter Umständen sind sie nicht in der Lage, die kürzeren Intervalle von Zertifikatserneuerungen und DCVs zu bewältigen. Verpasste Erneuerungen könnten ganze Domains und Anwendungen und damit auch den Geschäftsbetrieb zum Erliegen bringen.

Wenn sie vorausschauend planen und die Unterstützung eines SSL-Zertifikatsanbieters der Enterprise-Klasse in Anspruch nehmen, können sie unberechenbare und kostspielige Szenarien vermeiden. Ein etablierter Partner verfügt über eine proaktive und effektive Zertifikatsstrategie und liefert Automatisierungstools, die zeitaufwendige, manuelle Prozesse ersetzen und sicherstellen, dass es nie zu Ablaufausfällen kommt. Mit solchen Tools kann ein Agent im Rahmen eines automatisierten Verlängerungsprozesses ein Zertifikat vollständig anfordern, empfangen und installieren.

Die Integration der Automatisierungstools in die Systeme nimmt jedoch Zeit in Anspruch. Es ist nicht einfach möglich, auf fertige Produkte zurückzugreifen und diese zu implementieren, da es dabei einige Feinheiten zu beachten gibt. Beispielsweise sind vorhandene Systemkomponenten möglicherweise nicht mit den Tools kompatibel, sodass Unternehmen sie ersetzen müssen. Deshalb führt das Ignorieren oder Zurückstellen der kürzeren Erneuerungszyklen zu vermeidbarem – und kostspieligem – Chaos.

Drei Schritte zur optimalen Automatisierung

Um Ausfälle aufgrund abgelaufener Zertifikate zu vermeiden, erkennen Unternehmen zunehmend, dass sie SSL-Zertifikate ohne Automatisierung nicht verwalten können. Bislang wurde dies manuell versucht, indem ausstehende Ablaufdaten mit Tabellenkalkulationen verfolgt und die aktuellen jährlichen Erneuerungstermine verwaltet wurden. Diese Situation wird sich jedoch ändern, und hier kommt die Automatisierung ins Spiel.

Wie bereits erwähnt, ist eine automatisierte Integration keine einfache Aufgabe. Mehrere Zertifikatsanbieter und Versäumnisse führen bis dahin zu Engpässen und Unübersichtlichkeit. Um effektiv am Ball zu bleiben, empfehlen wir die folgenden Schritte:

Prozesse standardisieren und dokumentieren.

Teammitglieder kommen und gehen. Die Dinge ändern sich. Unabhängig davon erfordert das Zertifikatsmanagement standardisierte Praktiken, die im Laufe der Zeit konsistent bleiben. Bevor Sie mit der automatisierten Integration fortfahren, sollten Sie diese Verfahren entwickeln und dokumentieren, damit aktuelle und zukünftige Teammitglieder sie befolgen können. Berücksichtigen Sie dabei auch Probleme, die aufgetreten sind, damit die Teammitglieder wissen, welche Probleme es gab und wie sie gelöst wurden.

Bilden Sie sich und Ihre Teams weiter.

Es gibt viele Komponenten der Automatisierung, die man verstehen muss, bevor man sie einsetzt. Die Zusammenarbeit mit einem einzigen, bewährten Zertifikatsanbieter ist für den Lernprozess sehr hilfreich, da dieser Anbieter sich mit diesen Komponenten gut auskennt und Kunden entsprechend schulen kann.

Der Alleinanbieter kann Kunden beispielsweise dabei helfen, zu entscheiden, ob sie eine „umfangreiche Automatisierungslösung“ erwerben oder einen kostengünstigeren und weniger ambitionierten Weg einschlagen möchten. Es gibt IT-Tools – einige davon Open Source, andere mit Anwendungsprogrammierschnittstellen (APIs) entwickelt –, die sich als Alternativen zu einer umfassenden Lösung etabliert haben. Ein hochqualifizierter Anbieter ermöglicht es Kunden, fundierte Entscheidungen über das weitere Vorgehen zu treffen.

Alles einbeziehen.

Zuweilen lassen Teams bei einer automatisierten Integrationsinitiative etwas außer Acht. Das ist ein Fehler. Unvollständige Ansätze hinterlassen unweigerlich eklatante Lücken, die eine erfolgreiche Integration erschweren. Beziehen Sie daher den gesamten Workflow ein.

Fazit

Zertifikate sind allgegenwärtig, und Unternehmen können ohne sie nicht auskommen. Es genügt schon eine Popup-Warnung „Unsichere Website“, und Kunden wechseln zur Konkurrenz. Dennoch haben die meisten Unternehmen keinen genauen Überblick über ihren Zertifikatsbestand. Angesichts der geplanten Branchenveränderungen sind Unternehmen gezwungen, Automatisierungsmaßnahmen zu ergreifen, und müssen sich darauf vorbereiten.

Die Verkürzung der Lebenszyklen und der Wiederverwendungszeiträume für DCV lässt eine perfekte Cyber-Katastrophe befürchten – Unternehmen, die die Planung der Zertifikatserneuerung hinauszögern, werden bei der Umstellung mit höheren Kosten und Risiken konfrontiert sein. Die Entscheidung für eine Konsolidierung – mit einem einzigen, bewährten Partner für Zertifikatslösungen – ermöglicht eine reibungslosere und sicherere Umstellung, die durch Automatisierung noch optimiert wird.

Erfahren Sie mehr über die flexiblen Lösungen von CSC für die Verwaltung digitaler Zertifikate, die auf Unternehmen mit unterschiedlichen Anforderungen zugeschnitten sind.

Sprechen Sie mit uns

+49 (0) 611 7120090 0 | cscdbs.com/de

Über CSC

CSC ist der vertrauenswürdige Anbieter von Sicherheit und Threat Intelligence der Wahl für Unternehmen im Forbes Global 2000 und für die 100 Best Global Brands (Interbrand®) mit Schwerpunkten in den Bereichen Domain-Sicherheit und -Management sowie digitalem Markenschutz und Betrugssicherung. Angesichts der erheblichen Investitionen, die globale Unternehmen in ihre Sicherheitsposition tätigen, kann unsere Plattform DomainSec℠ ihnen helfen, bestehende Versäumnisse in puncto Cybersicherheit zu verstehen und ihre digitalen Online-Vermögenswerte und -Marken zu schützen. Durch den Einsatz der firmeneigenen Technologie von CSC können Unternehmen ihren Sicherheitsstatus verbessern, um sich vor Cyberbedrohungen zu schützen, die auf ihre Online-Vermögenswerte und den Ruf ihrer Marke abzielen. So können sie verheerende Umsatzeinbußen vermeiden. CSC bietet darüber hinaus Online-Markenschutz – eine Kombination aus Online-Markenüberwachung und Durchsetzungsmaßnahmen – einschließlich einer mehrdimensionalen Übersicht über verschiedene Bedrohungen außerhalb der Firewall, die bestimmte Domains ins Visier nehmen. Unsere Lösungen werden ergänzt durch Betrugspräventionsdienste, die Phishing bereits in der Frühphase des Angriffs bekämpfen. CSC hat seinen Hauptsitz seit 1899 in Wilmington, Delaware, USA, und verfügt über Niederlassungen in den Vereinigten Staaten, Kanada, Europa und im asiatisch-pazifischen Raum. CSC ist ein globales Unternehmen und kann überall dort tätig sein, wo unsere Kunden sind. Dies erreichen wir, indem wir in jedem Geschäftsbereich, den wir bedienen, Experten beschäftigen. Besuchen Sie cscdbs.com/de.

DBS02132026