

White Paper

Gewährleistung der geschäftlichen Verfügbarkeit
und Schutz vor Datenpannen: Warum die
Verwaltung von SSL-Zertifikaten für moderne
Unternehmen von entscheidender Bedeutung ist



Gewährleistung der geschäftlichen Verfügbarkeit und Schutz vor Datenpannen: Warum die Verwaltung von SSL-Zertifikaten für moderne Unternehmen von entscheidender Bedeutung ist

Inhalt

Einführung	3
Herausforderungen bei der Verwaltung von SSL-Zertifikaten	3
Die Gefahren abgelaufener und gefälschter SSL-Zertifikate	4
Diebstahl von Kundendaten	4
Abwanderung von Kunden zur Konkurrenz	6
Erhöhte Anzahl von Anrufen beim Kundensupport	6
Zunehmende Belastung der IT-Abteilungen	6
Best Practices für die SSL-Zertifikatverwaltung	7
Zusammenfassung	8
Symantec® Certificate Intelligence Center: Zuverlässige Erkennung und Verwaltung von SSL-Zertifikaten	8

Einführung

SSL-Zertifikate gibt es seit fast 15 Jahren. Nach wie vor spielen sie für den Schutz von Daten bei ihrer Übertragung über das Internet und über andere Netzwerke eine zentrale Rolle. Ob finanzielle Online-Transaktion, E-Commerce oder Produktentwicklung – mit SSL-Zertifikaten können Benutzer rund um den Globus darauf vertrauen, dass sie sicherheitskritische Informationen weitergeben können und die Daten dabei zuverlässig vor Hackern geschützt sind.

Das Internet hat sich in den letzten 15 Jahren in schier unvorstellbarer Weise weiterentwickelt. Warum also setzen wir nach wie vor unser Vertrauen in SSL-Zertifikate? Der einfache Grund: SSL-Zertifikate sind sehr effektiv, um Daten während der Übertragung zu schützen. So würde es einigen Berechnungen zufolge beispielsweise rund sechs Milliarden Jahre dauern (d. h. rund eine Millionen mal länger als die Erde bereits existiert), eine 128-Bit-Verschlüsselung auf SSL-Zertifikaten mit einem Brute Force-Angriff zu dechiffrieren.¹ Dennoch ist die Sicherheitsbranche wachsender als je zuvor. Dies zeigt sich u. a. daran, dass viele Zertifizierungsstellen durch die schrittweise Einführung der 2048-Bit-Verschlüsselung auf ihren SSL-Zertifikaten begonnen haben, die Online-Datenkommunikation zusätzlich zu schützen.

Dennoch sind Kunden, die über SSL-geschützte Websites und Systeme Transaktionen abwickeln, nach wie vor ernsthaften Bedrohungen ausgesetzt. Eine Hauptursache dieser Gefahr: schlecht verwaltete SSL-Zertifikate. Für Unternehmen, die Hunderte von SSL-Zertifikaten unterschiedlicher Anbieter verwalten, ist es nicht immer einfach, den Überblick über die Zertifikate in ihrer Umgebung zu behalten. Verlieren sie den Überblick, können Zertifikate ablaufen und monatelang unbemerkt bleiben, so dass Website-Besucher einem Hacker-Risiko ausgesetzt sind.

Manchmal ist das erste Zeichen, dass ein SSL-Zertifikat "verloren" gegangen ist, ein Anruf von einem Kunden, der bemerkt hat, dass ein Zertifikat abgelaufen ist und jetzt wissen möchte, ob die betreffende Website sicher genug für den Online-Einkauf ist. Manchmal kann das Problem gravierender sein. Typisch sind beispielsweise Phishing-Vorfälle, die es Internetkriminellen ermöglichen, vertrauliche Kundendaten zu stehlen. Oder die Auswirkungen eines Sicherheitsverstößes bei einer Zertifizierungsstelle (Certificate Authority (CA)) sind bis in ein Unternehmen hinein zu spüren, da es aufgrund der fehlenden Übersicht über seinen SSL-Zertifikatsbestand nicht schnell genug handeln kann.

Unabhängig von der jeweiligen Situation droht Unternehmen, die den Überblick über ihre SSL-Zertifikate verlieren, erheblicher finanzieller Schaden und Imageverlust. Die Verwaltung von SSL-Zertifikaten im Unternehmen muss jedoch kein komplexer oder zeitaufwändiger Prozess sein.

Dieses White Paper zeigt, welche Probleme durch schlecht verwaltete SSL-Zertifikate entstehen, warum diese Probleme eine potenzielle Gefahr für Unternehmen darstellen und wie Unternehmen SSL-Zertifikate effizient überwachen können.

Herausforderungen bei der Verwaltung von SSL-Zertifikaten

Moderne Unternehmen sind komplexe Umgebungen, die oft mehrere interne Netzwerke und öffentlich zugängliche Websites umfassen. Das bedeutet, dass in einem Unternehmen zu einem beliebigen Zeitpunkt Dutzende oder sogar Hunderte verschiedene SSL-Zertifikate installiert sein können.

1. <http://www.inet2000.com/public/encryption.htm>

Neben einer großen Anzahl von SSL-Zertifikaten nutzen viele Unternehmen eine Kombination aus verschiedenen Zertifikaten unterschiedlicher Zertifizierungsstellen. Ein Unternehmen kann beispielsweise auf seiner für Kunden zugänglichen Website SSL-Zertifikate eines bekannten, vertrauenswürdigen Anbieters installieren, in seinem Intranet jedoch eine kostengünstigere Marke oder selbstsignierte Zertifikate verwenden.

Obwohl einige Zertifizierungsstellen Online-Tools für die Verwaltung ihrer eigenen Zertifikate zur Verfügung stellen, können diese Tools Zertifikate oft nicht unabhängig von der ausstellenden Zertifizierungsstelle überwachen. Anstatt die Verwaltung zu vereinfachen, wird durch die Vielzahl der Verwaltungsportale in einer Umgebung mit mehreren Zertifizierungsstellen das Problem der Nachverfolgung zahlloser SSL-Zertifikate zusätzlich erschwert. Administratoren müssen ihren Bestand an SSL-Zertifikaten über mehrere Systeme hinweg kontinuierlich überwachen und eigene Berichte zusammenstellen, um einen umfassenden Überblick über sämtliche SSL-Zertifikate im Netzwerk zu erhalten.

Hinzu kommt, dass sich in Unternehmen mit verteilten Netzwerken Sicherheitsrichtlinien von Gruppe zu Gruppe unterscheiden können. Dies bedeutet in der Praxis, dass Gruppe A die von ihr verwalteten Daten möglicherweise mit Extended Validation SSL-Zertifikaten schützt, während Gruppe B einen anderen SSL-Zertifikatstyp von einer anderen Zertifizierungsstelle verwendet. Oder in einem noch häufiger anzutreffenden Anwendungsfall benötigt Gruppe A 2048-Bit SSL-Zertifikate, Gruppe B hingegen 1024-Bit-Zertifikate. Problematische Bedingungen wie unterschiedliche Richtlinien und das Fehlen eines einheitlichen Verfahrens, um einen umfassenden Überblick über alle SSL-Zertifikate im Unternehmensnetzwerk zu erhalten, stellen ein erhöhtes Sicherheitsrisiko dar, das die Einhaltung unternehmensweiter oder gesetzlicher Richtlinien zusätzlich erschwert.

Dieses Problem wirft weitere Fragen auf, wenn die für die Verwaltung der SSL-Sicherheit zuständigen Mitarbeiter auf eine andere Position wechseln oder das Unternehmen verlassen. Wenn die zuständigen Mitarbeiter nicht rigoros dokumentieren, welche Zertifikate sie verwalten – und diese Informationen an andere Teammitglieder weiterleiten – können diese SSL-Zertifikate unbemerkt bleiben, wenn ein neues Teammitglied die Verantwortung übernimmt. Da IT-Teams in der Regel vielbeschäftigt und ihre Ressourcen häufig knapp sind, ist die manuelle Nachverfolgung von SSL-Zertifikaten nicht nur ein aufwändiger, sondern auch ein fehleranfälliger Prozess.

Alle diese Faktoren begünstigen ein Umfeld, in dem SSL-Zertifikate schnell verloren gehen oder übersehen werden. Ein solches Umfeld gefährdet den Geschäftsbetrieb des Unternehmens und lässt Sicherheitsrisiken für Kunden entstehen.

Die Gefahren abgelaufener und gefälschter SSL-Zertifikate

Ein abgelaufenes oder gefälschtes SSL-Zertifikat in einer Netzwerkumgebung kann gravierende Folgen haben. Schon ein einziges abgelaufenes oder gefälschtes Zertifikat kann das Unternehmen – oder noch schlimmer dessen Kunden – für Angriffe durch Internetbetrüger anfällig machen. Dies sind nur einige Beispiele für mögliche Konsequenzen abgelaufener und gefälschter SSL-Zertifikate.

Diebstahl von Kundendaten

Dank jahrelanger Schlagzeilen zum Thema Sicherheitsverstöße und Aufklärungskampagnen von Verbraucherschützern und Unternehmen erkennt die breite Öffentlichkeit Identitätsdiebstahl heute mehr denn je als eine ernstzunehmende Bedrohung. Laut einer

jüngsten Studie sind 64 Prozent der amerikanischen Bürger sehr/äußerst besorgt, dass Hacker ihre Identität ausspionieren könnten – 31 Prozent gaben an, äußerst besorgt zu sein.²

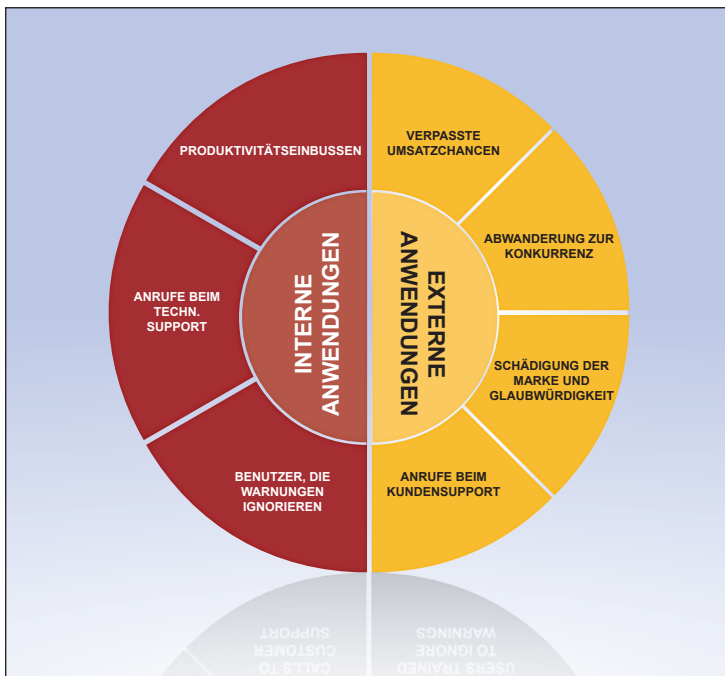
Eine Hauptsorge gilt dabei dem Phishing. Bei einem Phishing-Angriff tarnt sich ein Hacker als legitimes Unternehmen und richtet eine gefälschte Website ein, die der echten Website ähnelt oder praktisch mit ihr identisch ist. Der Angriff erfolgt über eine Sicherheitslücke, die entsteht, wenn der Authentifizierungsprozess des Unternehmens infolge fehlender oder abgelaufener SSL-Zertifikate nicht mehr stattfindet. Arglose Kunden geben dann vertrauliche Informationen wie Kreditkartennummern oder andere sicherheitskritische Daten auf der Website ein. Die Phishing-Website leitet Daten direkt an den Hacker weiter, der diese Daten wiederum an andere Kriminelle verkauft.

Selbst ein relativ begrenzter Phishing-Vorfall oder Sicherheitsverstoß kann diese Ängste zusätzlich schüren und das Unternehmen ernsthaft gefährden.

Über diese unmittelbaren Verluste hinaus können Phishing-Angriffe und Datenpannen auch dem Image des Unternehmens schaden und dazu führen, dass sowohl bestehende Kunden als auch Interessenten die Vertrauenswürdigkeit des betreffenden Unternehmens in Frage stellen. Nach Meinung von Experten kann es bis zu sechs Monate dauern, um nach einem Sicherheitsverstoß den Verkauf und das Vertrauen in das Netzwerk des Unternehmens zu stabilisieren³ – und selbst dann lässt sich der Imageschaden nicht immer komplett rückgängig machen.

Die steigenden Kosten von Datenpannen

Während sich der Imageverlust eines Unternehmens kaum exakt beziffern lässt, sprechen die Zahlen für die wirtschaftlichen Folgen einer Datenpanne eine klare Sprache. Laut einer kürzlich durchgeführten Studie in den USA belaufen sich die Kosten eines Datenverstoßes pro Sicherheitsvorfall auf 7,2 Millionen USD oder gut 214 USD pro kompromittiertem Datensatz⁴ – Zahlen, die den Prognosen zufolge weiter wachsen werden.



Die Folgen unerwartet abgelaufener SSL-Zertifikate und ignoriertener Browser-Warnungen

2. "Identity theft fears weigh on Americans", Tim Greene, Network World, 12/4/2010

3. "Sony Data Breach Exposes Users to Years of Identity-Theft Risk", Cliff Edwards und Michael Riley, BusinessWeek.com, 3/5/11

4. "Cost of a data breach climbs higher", Ponemon Institute, ponemon.org, 8/3/11

Abwanderung von Kunden zur Konkurrenz

Ein weiterer Risikofaktor für Unternehmen sind abgelaufene SSL-Zertifikate. Ein abgelaufenes SSL-Zertifikat kann auf andere Weise zu Umsatzausfällen führen. In erster Linie gehört hierzu ganz einfach ein Rückgang des Besucheraufkommens, wenn Kunden Warnmeldungen zum Ablauf von SSL-Zertifikaten sehen und die Website des Unternehmens verlassen, um Produkte und Services auf Websites mit sicheren SSL-Zertifikaten zu kaufen.

Kunden wissen vielleicht nicht in allen Einzelheiten, wie eine Verschlüsselung mit öffentlichem Schlüssel funktioniert. Doch sichtbare Zeichen der SSL-Sicherheit – wie etwa ein SSL Trust-Siegel oder die grüne Extended Validation-Adressleiste – erhöhen die Wahrscheinlichkeit, dass sie ihre Transaktion auf einer bestimmten Website abwickeln.⁵ Wenn SSL-Zertifikate auf E-Commerce- oder anderen öffentlich zugänglichen Websites ablaufen, verlieren Unternehmen das Vertrauen der Kunden und damit letztlich ihre Umsätze.

Erhöhte Anzahl von Anrufen beim Kundensupport

Viele Unternehmen verfügen heute über Web-Tools, automatisierte Telefonmenüs und andere Selbstbedienungsoptionen, die es für Kunden noch einfacher machen, die Informationen zu finden, die sie suchen. Wenn Kunden, die eine Website besuchen, jedoch Bedenken hinsichtlich der Sicherheit ihrer privaten Daten haben, brechen sie ihre Transaktion (wie oben beschrieben) ab oder wenden sich an den Kundensupport.

Die durchschnittlichen Kosten pro Supportanruf variieren erheblich von Branche zu Branche – eine Tatsache ist jedoch unbestritten: Die Kosten für zusätzliche Supportanrufe summieren sich mit der Zeit. Zusätzliche Supportanrufe binden nicht nur finanzielle Ressourcen, sie belasten auch zusätzlich das Contact Center und verhindern, dass Supportmitarbeiter andere strategisch wichtigere Kundenanrufe abwickeln können.

Die hohen Kosten und der zusätzliche Arbeitsaufwand für Kundenanfragen lassen sich durch Aufrechterhaltung eines hohen Sicherheitsstandards, der gültige SSL-Zertifikate einschließt, leicht vermeiden.

Zunehmende Belastung der IT-Abteilungen

Ähnlich wie Kunden, die sich an den Kundensupport wenden, wenn sie sich über die Sicherheit einer Website nicht im Klaren sind, wenden sich auch Mitarbeiter innerhalb des Unternehmens, die Warnmeldungen im Zusammenhang mit abgelaufenen SSL-Zertifikaten im Intranet oder auf anderen internen Websites sehen, häufig an IT-Mitarbeiter, um das Problem zu lösen. Dies kann für bereits stark geforderte IT-Abteilungen eine erhebliche zusätzliche Belastung bedeuten.

In anderen Fällen werden diese Ablaufwarnungen von Mitarbeitern möglicherweise komplett ignoriert, so dass die betroffenen Ressourcen ungeschützt Angriffen ausgesetzt sind. Dieses Verhalten wirkt sich zudem negativ auf die Einhaltung unternehmensinterner Sicherheitsstandards aus, da es den Eindruck erweckt, dass Mitarbeiter interne Sicherheitsmaßnahmen einfach ignorieren können.

Beide Szenarien lassen sich jedoch durch Aufrechterhaltung eines hohen Sicherheitsstandards auf der Basis von SSL-Zertifikaten vermeiden.

5. <http://www.verisign.de/ssl/symantec-certificate-intelligence-center/index.html>

Best Practices für die SSL-Zertifikatverwaltung

Glücklicherweise gibt es Dienste, die eine einfache Erkennung und Verwaltung von SSL-Zertifikaten im gesamten Unternehmen ermöglichen. Einige Lösungen geben vor, die SSL-Verwaltung zu vereinfachen, selbst wenn sie keine Möglichkeit bieten, Zertifikate unabhängig von der Zertifizierungsstelle zu erkennen. Andere Lösungen bieten möglicherweise eine Scanfunktion für mehrere Zertifizierungsstellen, besitzen jedoch keine intuitive, einfach zu navigierende Benutzeroberfläche.

Damit Sie die beste Lösung für Ihre Anforderungen finden, enthält die nachstehende Liste wichtige Funktionen, auf die Sie achten sollten, ganz gleich, welche Lösung Sie in Erwägung ziehen:

- **Funktion zum automatischen Scannen Ihrer Umgebung:** Obwohl es theoretisch möglich ist, Netzwerke manuell zu überwachen, wäre ein solches Verfahren ganz einfach zu zeitaufwändig und würde zu viele Mitarbeiterressourcen binden, um in einer großen komplexen Unternehmensumgebung wirklich praktikabel zu sein. Achten Sie darauf, einen Service auszuwählen, mit dem Ihr Team automatische Scans durchführen kann, die SSL-Zertifikate von jedem Anbieter erkennen.
- **Benutzerfreundliche Oberfläche:** Informationen, die nicht unmittelbar zugänglich oder schwer zu lesen sind, sind nur von geringem Wert. Suchen Sie deshalb gezielt nach einem Tool mit einem einfach zu navigierenden Dashboard, das Daten auf einen Blick verständlich abbildet.
- **Delegierungsfunktionen:** In einer typischen Unternehmensumgebung sind meistens mehrere Mitarbeiter mit der Sicherheitsverwaltung beauftragt. Daher ist es wichtig, eine Zertifikatserkennungslösung zu finden, die es Administratoren ermöglicht, unterschiedliche Zugriffsrechte zuzuweisen und Aufgaben an unterschiedliche Mitarbeiter im Netzwerk zu delegieren.
- **Warnmeldungen und Berichterstellung:** Ein abgelaufenes SSL-Zertifikat gefährdet Daten. Einen Service zu finden, der Warnmeldungen sendet, bevor ein Zertifikat abläuft, ist deshalb von entscheidender Bedeutung. Die Möglichkeit, einfach zu lesende und zu verstehende Berichte zu erstellen, ist eine weitere wichtige Anforderung. Erweiterte Berichterstellungsfunktionen liefern nicht nur einen genauen und umfassenden Überblick über die im Netzwerk vorhandenen Zertifikate, sondern ermöglichen es Ihrem Team zudem, wichtige Informationen effektiver an andere Mitarbeiter – beispielsweise Führungskräfte – weiterzuleiten.
- **Flexibilität und Skalierbarkeit:** Unternehmensnetzwerke sind dynamische, sich ständig wandelnde Umgebungen. Das bedeutet, dass ein Zertifikatserkennungsdienst konfigurierbare Parameter enthalten sollte, wie etwa Scandauer, welche IP-Adressen zu scannen sind und andere. Zusätzlich muss der Dienst skalierbar sein, um künftiges Wachstum mitzutragen.
- **Aktualität:** Um effektiv zu sein, müssen Netzwerkscans schnell ausgeführt werden. Wenn ein netzwerkweiter Scan zu viel Zeit beansprucht, ändert sich der Status einzelner SSL-Zertifikate möglicherweise, bevor der Scan vollständig abgeschlossen ist. Dadurch ergibt sich ein ungenaues Bild vom SSL-Zertifikatsbestand.

Zusammenfassung

SSL-Zertifikate sind für den Schutz von Daten während der Übertragung unverzichtbar. Trotz ihrer Stärke und Zuverlässigkeit bietet die SSL-Sicherheit jedoch keinen hundertprozentigen Schutz vor Angriffen – dafür gibt es jedoch nur einen Grund: schlecht verwaltete SSL-Zertifikate.

In Unternehmensumgebungen mit mehreren Zertifikaten und unterschiedlichen Zertifizierungsstellen ist ein umfassender Überblick über die SSL-Sicherheit unentbehrlich. Die Kenntnis des Status jedes einzelnen Zertifikats auf allen Websites und in allen Netzwerken ist nicht nur ein Mittel zur Kostenkontrolle im Kundenservice, sondern auch eine Möglichkeit, die Mitarbeiter der SSL-Verwaltung zu entlasten, damit sich vielbeschäftigte IT-Teams wieder verstärkt auf andere geschäftskritische Aufgaben konzentrieren können.

Eine strikte SSL-Verwaltung kann darüber hinaus noch viel gravierendere Probleme verhindern, wie etwa Phishing-Vorfälle oder andere Datenpannen, deren Behebung nicht nur hohe Kosten verursachen, sondern langfristig auch den Ruf Ihres Unternehmens schädigen können.

Symantec® Certificate Intelligence Center: Zuverlässige Erkennung und Verwaltung von Zertifikaten

Symantec Certificate Intelligence Center hilft Administratoren, SSL-Zertifikate effektiver zu erkennen und zu verwalten. Symantec Certificate Intelligence Center ermöglicht eine detaillierte Zertifikaterfassung und bietet umfassende Verwaltungsfunktionen, die es einfach machen, den Überblick über SSL-Zertifikate zu behalten.

Symantec Certificate Intelligence Center verfügt über eine intuitive Oberfläche, mit der Administratoren automatische Scans einrichten können, die Zertifikate jeder Zertifizierungsstelle schnell erkennen. Benutzer können zudem Warnmeldungen einrichten, um SSL-Manager zu informieren, bevor Zertifikate ablaufen.



Das einfach zu navigierende Dashboard von Symantec Certificate Intelligence Center

Als einfach zu skalierende Lösung hält Symantec Certificate Intelligence Center mit schnellen Netzwerkänderungen im Rahmen sich ändernder und wachsender Unternehmensanforderungen problemlos Schritt. Erweiterte Funktionen im Bereich der Berichterstellung geben einen umfassenden, leicht verständlichen Überblick über die SSL-Sicherheit, der schnell und einfach im Unternehmen weitergegeben werden kann.

Weitere Informationen dazu, wie Sie mit Symantec Certificate Intelligence Center die Erkennung und Verwaltung von SSL-Zertifikaten vereinfachen können, finden Sie auf folgender Website:

<http://www.verisign.de/ssl/symantec-certificate-intelligence-center/index.html>

Weitere Informationen

Besuchen Sie unsere Website

<http://www.verisign.de>

Um mit einem Produktspezialisten zu sprechen:

0800 128 1000 (kostenlos aus DE) oder

0800 208899 (kostenlos aus AT)

+41 26 429 7726

Über Symantec

Symantec ist einer der weltweit führenden Anbieter auf dem Gebiet der Informationssicherheit, Datenspeicherung und der Systemverwaltung und bietet Unternehmen sowie Privatkunden Lösungen zur Absicherung und Verwaltung ihrer Daten. Das Unternehmen hat seinen Hauptsitz in Mountain View, Kalifornien, und vertreibt seine Produkte in 40 Ländern. Weitere Informationen finden Sie unter www.symantec.de.

Symantec Deutschland GmbH

Wappenhalle

Konrad-Zuse-Platz 2-5

D-81829 München



VeriSign
Authentifizierungsdienst