CT-Monitor für essendi xc – mit Sicherheit einfach

Das Versenden von vertraulichen Nachrichten über E-Mails oder Social Media Plattformen, Online Banking sowie das Einkaufen über das Internet zählen zu den Diensten, die von einer großen Anzahl an Menschen täglich genutzt werden. Dabei sind Anwender darauf angewiesen, dass niemand unberechtigten Zugriff auf ihre persönlichen Daten nehmen kann. Deshalb werden diese Daten über diverse Sicherheitsmaßnahmen und kryptographische Verfahren verschlüsselt übermittelt.

Digitale Zertifikate für mehr Sicherheit

Neben der Datenverschlüsselung ist aber auch von Bedeutung, ob sensible Daten wirklich an den vorgesehenen Kommunikationspartner übermittelt werden. Der Identitätsnachweis des Empfängers erfolgt deshalb über digitale Zertifikate. Diese enthalten den öffentlichen Schlüssel des Kommunikationspartners und weitere Informationen, die seine Identität beweisen. Digitale Zertifikate werden von speziellen Zertifizierungsstellen ausgestellt, die mit ihrer Signatur die Korrektheit der Angaben garantieren. Zertifikate besitzen eine bestimmte Gültigkeitsdauer und müssen nach deren Ablauf erneuert werden. Werden sie fälschlicherweise ausgestellt, können sie gesperrt werden. Stetig wachsende Sicherheitsanforderungen resultieren in immer kürzer werdenden Laufzeiten.

Gefälschte Zertifikate können für ein Unternehmen einen erheblichen finanziellen oder Imageschaden verursachen. Über sie ist beispielsweise ein unberechtigter Zugang zu Unternehmens- oder Kundendaten, sowie das Betreiben von Phishing-Seiten möglich. Phishing-Seiten sind gefälschte Webseiten, die der originalen Unternehmenswebseite ähneln und Nutzer dazu verleiten sollen, sensible Daten wie Passwörter oder Zahlungsinformationen preiszugeben.

Auch können sie dazu verwendet werden, um sogenannte Man-In-The-Middle-Attacken auszuführen, bei denen ein Angreifer sich zwischen die Kommunikation von Client und Server schaltet und beiden Kommunikationspartnern vorgibt, der jeweils andere zu sein.

Zertifizierungsstellen als Vertrauensanker

Zertifizierungsstellen sind daher die Vertrauensanker für die verschlüsselte Kommunikation im Internet. Über das Ausstellen digitaler Zertifikate bestätigen sie die Identität von Personen oder Organisationen. Ein Großteil der verschlüsselten Kommunikation im Internet beruht also auf digitalen Zertifikaten und dem Vertrauen in die ausstellende Zertifizierungsstelle (CA). Das funktioniert aber nur so lange, wie sie keine Zertifikate mit falschen Informationen ausstellt, keine Fehler bei der Ausstellung der Zertifikate macht oder unbemerkt von Angreifern dafür verwendet werden kann, um gefälschte Zertifikate auszustellen. Wird einer dieser Punkte nicht gewährleistet, ist die gesamte sichere Kommunikation im Internet gefährdet. Leider war die fehlerfreie Arbeit von Zertifizierungsstellen in der Vergangenheit nicht immer gegeben. Um die

Kommunikation über das Internet weiterhin sicher gestalten zu können, musste eine Lösung geschaffen werden.

Certificate Transparency Standard für mehr Transparenz
Aufgrund ihres besonderen Stellenwerts für die vertrauliche Kommunikation im Internet ist es daher notwendig, die Arbeit der Zertifizierungsstellen überwachen zu können. Genau dafür wurde der **Certificate Transparency Standard** entwickelt, der mittels öffentlicher Verzeichnisse über ausgestellte Zertifikate in Form von CT-Logs versucht, die Arbeit der Zertifizierungsstellen transparenter zu gestalten.

Da bei den Sicherheitsvorfällen immer wieder Domains von beliebten und daher häufig genutzten Diensten betroffen waren, trieben diese die Entwicklung des Certificate Transparency Standards voran. Der Standard sieht vor, dass alle von Zertifizierungsstellen ausgestellten Zertifikate in öffentlich einsehbare Verzeichnisse eingetragen werden. Dadurch wird eine Echtzeitüberwachung der von CAs ausgestellten Zertifikate ermöglicht. Durch diese Echtzeitüberwachung sollen fälschlich ausgestellte Zertifikate oder Abwicklungsfehler in Zertifizierungsstellen schneller erkannt und Gegenmaßnahmen schneller eingeleitet werden können.

Automatisierte Prüfung der CT-Logs
Diese Verzeichnisse liegen in Form von sogenannten CT-Logs vor. Ein CT-Log ist ein Netzwerk-Service, der ein kryptographisch gesichertes und öffentlich zugängliches Verzeichnis ausgestellter Zertifikate zur Verfügung stellt. Der CT Standard sieht vor, dass alle von einer CA ausgestellten Zertifikate einen Eintrag in einem CT-Log erhalten. Die Einträge können ausschließlich zu einem Log hinzugefügt und später nicht mehr gelöscht oder bearbeitet werden (Append-Only). Das korrekte Verhalten eines Logs kann durch kryptographische Beweise nachgewiesen werden. Die CT-Logs werden typischerweise von CAs, Internet Service Providern (ISP) oder anderen Interessensparteien betrieben. Jedes Log besitzt eine standardisierte Schnittstelle, über die Zertifikate hinzugefügt, Einträge abgefragt und kryptographische Beweise durchgeführt werden können. Die Fälschung von Zertifikaten wird durch die CT-Logs selbst nicht erkannt oder verhindert. Die Logs sind lediglich eine Datenbasis, um eine solche Prüfung durchzuführen.

Monitor
Die Prüfung, ob ein gefälschtes Zertifikat ausgestellt wurde, wird von den Monitoren übernommen. Sie rufen in gewissen Zeitabständen neue Einträge der existierenden CT-Logs ab und prüfen die darin enthaltenen Informationen. Ein solcher Monitor kann beispielsweise von Unternehmen oder Domain-Besitzern betrieben werden, um zu erkennen, ob ein gefälschtes Zertifikat für ihre Domain ausgestellt wurde. Üblicherweise wird der Monitor in Form eines Subscription-Services angeboten, bei dem Domainbesitzer ihren Domainnamen und ihre Kontaktadresse hinterlegen und vom Monitor benachrichtigt werden, wenn ein Zertifikat für ihre Domain ausgestellt wurde.

Auditor
Damit die CT-Logs einen Mehrwert für die Sicherheit im Internet bieten können, muss deren korrektes Verhalten überprüft werden. Diese Aufgabe wird von dem Auditor übernommen, der entweder ein eigenständiger Dienst, Teil eines Monitors oder Bestandteil eines Browsers sein kann. Er prüft beispielsweise die Konsistenz eines Logs und stellt somit sicher, dass alle Zertifikate, die im Log enthalten sein sollten, auch tatsächlich vorhanden sind.

essendi xc – Zertifikatemanagement the easy way
Um die Verwaltung von digitalen Zertifikaten und die damit verbundenen Prozesse in einem Unternehmen zu erleichtern, wurde der Zertifikatemanager essendi xc entwickelt. Er stellt im zentralen Dashboard eine Übersicht über alle in einem Unternehmen befindlichen Zertifikate zur Verfügung. Er enthält ebenfalls Informationen zum Management von Zertifikaten, wie beispielsweise das Ablaufdatum oder den Installationsort des jeweiligen Zertifikats.

Für den initialen Import der Zertifikate in den xc wird ein Netzwerksscan angeboten, der automatisch im Netzwerk befindliche Zertifikate aufspürt. Kernbestandteil der Anwendung ist die Überwachungsfunktion, die den Benutzer rechtzeitig vor dem Ablauf von Zertifikaten warnt und das Risikomanagement erleichtert. Die Verwaltungsaufgaben wie Beantragung, Auslieferung oder Erneuerung von Zertifikaten können über den xc weitgehend automatisiert erfolgen. Die Beantragung von Zertifikaten wird über vordefinierte Zertifikatsprofile vereinfacht. In Profilen werden unternehmensinterne Konventionen festgelegt, sodass Zertifikate für verschiedene Anwendungsbereiche schneller beantragt werden können und das versehentliche Ausstellen von falschen Zertifikaten verhindert wird. Die im Profil eingegebenen Daten werden dann vom xc an die CA gesendet.

Um die Zertifikateverwaltung noch sicherer und komfortabler zu gestalten, wurde die bisherige Funktionalität der Zertifikatsüberwachung des essendi xc um einen CT-Monitor erweitert. Die von CT-Logs bereitgestellten Daten werden periodisch abgefragt und geprüft, ob ein Eintrag für ein gefälschtes Zertifikat einer Domain des xc-Nutzers erstellt wurde. Wird ein solcher Eintrag gefunden, erhält der xc-Nutzer eine Alert-Nachricht.
Durch die Monitoring-Komponente bietet der xc dem Nutzer zukünftig nicht mehr nur Informationen über den Zertifikatsbestand des Unternehmens, sondern überwacht die Zertifikatsausstellung sämtlicher CAs, um Informationen zu Zertifikaten zu liefern, die die Domains des Unternehmens bzw. das Unternehmen selbst betreffen.

essendi xc mit CT Logs Monitor – einfach und sicher
Während es vor der Einführung des Certificate Transparency Standards praktisch unmöglich zu bemerken war, ob ein gefälschtes Zertifikat für die Domain eines Nutzers ausgestellt wurde, können mit Hilfe der CT-Logs sogenannte Monitore die Domainbesitzer benachrichtigen, wenn Zertifikate für ihre Domain ausgestellt werden. Hierfür werden alle neuen Einträge in allen CT-Logs periodisch abgerufen und geprüft. Somit können gefälschte Zertifikate zeitnah entdeckt und revoziert werden, bevor sie möglicherweise großen Schaden anrichten.

Ein solcher CT-Monitor wurde von essendi it entwickelt, um die Funktionalität des Zertifikatemanagers essendi xc zu erweitern. Die CT-Monitoring-Komponente besteht dabei aus zwei eigenständigen Anwendungen zum Abrufen und Prüfen der Log-Einträge.

Die klare Trennung zwischen Abruf und dem Prüfen der Einträge stellt sicher, dass der Zertifikatemanager essendi xc nicht direkt mit einer Komponente kommuniziert, die mit dem Internet verbunden ist. Die aus den beiden Teilkomponenten aufgebaute CT-Monitoring-Anwendung wird über eine Schnittstelle mit dem Zertifikatemanager xc verbunden. Über sie erhält der CT-Monitor die Liste an Domains, die er überwachen soll und kann Nachrichten an das Postfach eines festgelegten xc-Nutzers senden, falls ein Eintrag für eine dieser Domains gefunden wird.

Die Nachrichten werden unterschieden in Info- und Warnmeldungen, da auch Einträge für regulär vom Nutzer beantragte Zertifikate vom Certstream-Server abgerufen werden. Die Unterscheidung zwischen Info- und Warnmeldung erfolgt dabei über CAA-Records, die bei einem DNS Server abgefragt werden können und festlegen, welche Zertifizierungsstellen für eine Domain Zertifikate ausstellen dürfen. Bei der Prüfung der Logeinträge wird vom CT-Monitor der Aussteller mit der Liste an berechtigten Zertifizierungsstellen verglichen. Ist der Aussteller im Record vorhanden, wird eine Infomeldung versendet. Andernfalls erhält der Nutzer eine Warnmeldung.

Fazit

Durch Integration der CT-Monitoring-Komponente ist es zukünftig erstmals automatisch möglich, gefälschte Zertifikate für eine Nutzer-Domain zu entdecken, die nicht über den xc beantragt wurden. Zusätzlich werden die Einträge für gefälschte Zertifikate zeitnah entdeckt und können somit gesperrt werden, bevor sie Schaden anrichten. Mit diesen Funktionen bietet der CT-Monitor einen Mehrwert für die IT-Sicherheit und das Risikomanagement eines Unternehmens. Je schneller gefälschte Zertifikate entdeckt werden, desto schneller können Gegenmaßnahmen eingeleitet werden. Der CT-Monitor sendet aber nicht nur Alert-Meldungen aufgrund gefälschter Zertifikate, sondern zusätzlich Informationen, wenn vom Nutzer beantragte Zertifikate in den CT-Logs eingetragen wurden. Damit erhöht die Komponente die Aufmerksamkeit für den Certificate Transparency Standard und die Transparenz des Beantragungsvorganges eines Zertifikats.

Hier essendi xc unverbindlich in einer Live-Demo kennenlernen.

essendi it ist ein Softwarehaus mit Standorten in Schwäbisch Hall und München. Wir entwickeln moderne IT-Lösungen auf aktuellem technologischem und sicherheitstechnischem Niveau. Dabei sind wir spezialisiert auf IT-Sicherheit und Zertifikatemanagement.

Unser Unternehmen blickt auf zwei Jahrzehnte Erfahrung in der IT-Branche zurück und konnte sich seit seiner Gründung im Jahr 2000 erfolgreich am Markt etablieren.

Wir glauben daran, dass wir mit unseren maßgeschneiderten Softwarelösungen und IT-Dienstleistungen Ihre Firmenabläufe vereinfachen und miteinander verbinden können.
Zu unserer Firmenphilosophie zählt es, über den Entwicklerhorizont hinwegzublicken und uns in den praktischen Alltag der Kunden hineinzuversetzen. Damit dies gelingt, arbeiten wir untereinander und mit Ihnen eng zusammen und kommunizieren ehrlich und offen.

essendi it GmbH
Dolanallee 19
74523 Schwäbisch Hall

essendi it GmbH
Max-Planck-Str. 2
85609 Aschheim bei München

Telefon: +49 89 944 697-71
www.essendi.de
info@essendi.de