EINER DER WELTGRÖßTEN MODEHÄNDLER ENTSCHEIDET SICH FÜR TOKENISIERUNG

Verschlüsselung ist eine effektive und sichere Methode zum Schutz von Daten, insbesondere von Daten im Ruhezustand. In hochvolumigen Echtzeit-Zahlungsumgebungen ist die Tokenisierung für viele große Einzelhändler, Banken und Kreditkartenunternehmen auf der ganzen Welt die Datenschutzmethode der Wahl, da sie einen erstklassigen Schutz mit minimalen Auswirkungen auf die Verarbeitungsgeschwindigkeit bietet. Ein bekannter Modehändler hat sich für die einfach zu implementierende Tokenisierungs-Lösung von comforte entschieden, um sein Zahlungsnetzwerk zusätzlich zu schützen und gleichzeitig das hohe Serviceniveau zu halten, das seine Kunden erwarten.

KUNDENPROFIL

In den meisten Einzelhandelsgeschäften werden bei der Verwendung einer Zahlungskarte durch einen Kunden die Transaktionsdaten in einem zentralen Computersystem gespeichert, um den Austausch von Geld für die verkauften Artikel zu erleichtern. Sofern der Einzelhändler seine Zahlungsabwicklung nicht an einen Dienstleister auslagert, ist die Speicherung der Transaktionsdaten ein normaler Geschäftsvorgang.

Dieser große Modehändler in den USA ist da keine Ausnahme. Mit fast 900 Geschäften in Nordamerika ist die Akzeptanz von Zahlungskarten seit langem ein fester Bestandteil der Kundenerfahrung: Das Unternehmen akzeptiert Zahlungen von allen großen Kartenanbietern (Visa, MasterCard, Amex und Discover) und hat seit mehr als 30 Jahren eine eigene Kreditkartenmarke.

HERAUSFORDERUNGEN

Gespeicherte Transaktionsdaten enthalten neben Zahlungskartendaten auch andere personenbezogene Informationen, die ein sehr attraktives Ziel für Hacker und andere Kriminelle darstellen, die wertvolle Daten stehlen wollen. Im Dark Web und auf anderen Untergrund-Webseiten werden gestohlene Kredit- und Debitkartendaten für hohe Geldbeträge verkauft und zum Kauf illegaler Gegenstände und für andere kriminelle Zwecke genutzt.
Aus diesem Grund versuchen Hacker ständig, in Unternehmen jeder Größe und Branche einzudringen und wertvolle Daten abzugreifen. Datenschutzverletzungen sind praktisch zum Alltag geworden, und früher oder später werden die meisten Unternehmen davon heimgesucht. Dies veranlasste das Datensicherheitsteam des Unternehmens, sofortige Maßnahmen zu ergreifen und eine zusätzliche Schutzebene einzuführen, um ähnliche und möglicherweise größere Datenschutzverletzungen in Zukunft zu verhindern. In Anbetracht der jüngsten Ereignisse wurden diese zusätzlichen Sicherheitsmaßnahmen auf Vorstandsebene ohne weiteres genehmigt.

Als Teil seines bestehenden Datensicherheitsprogramms verwendete der Einzelhändler bereits Verschlüsselung zum Schutz der Zahlungskartennummern sowie eine eindeutige interne ID-Nummer, die mit jeder Zahlungskarte verbunden ist. Eine der Herausforderungen, vor denen das Unternehmen stand, war die Ausweitung dieses Schutzes auf persönliche Daten wie Namen, Adressen, Geburtsdaten usw. seiner geschätzten Kunden. Während Zahlungskartennummern ein offensichtliches Ziel sind, suchen böswillige Akteure immer nach neuen Wegen, um aus jeder Art von Daten, auf die sie Zugriff haben, Wert zu schöpfen. Daher musste die neue Lösung einfach zu skalieren sein und den Schutz auf weitere Datenarten ausdehnen, wenn neue Situationen und veränderte Umstände dies erfordern.

Außerdem hat der Einzelhändler ein sehr hohes Transaktionsvolumen, das auf einer hybriden Cloud-Infrastruktur läuft. Das bedeutet, dass die Aktivierung der Verschlüsselung für alle Kundendaten in der komplexen Landschaft des Unternehmens eine zusätzliche Belastung für die Systeme bedeutet hätte. Verschlüsselung eignet sich hervorragend für den Schutz von Daten im Ruhezustand, doch um die Daten für Standardgeschäftsprozesse nutzen zu können, muss die Entschlüsselung in bestimmten Phasen erfolgen.

KURZ & BÜNDIG

- Datenschutz über PANs hinaus auf personenbezogene Daten ausgedehnt
- Hohes Sicherheitsniveau wie bei der Verschlüsselung, aber jetzt mit geringerer Belastung der IT-Ressourcen
- Beschleunigte PCI-Audits durch Herausnahme sensibler Daten aus dem Geltungsbereich
- Keine Verwaltung von Verschlüsselungsschlüsseln für tokenisierte Daten mehr erforderlich
- Tokenisierung konnte leicht in bestehende Datensicherheitssysteme implementiert werden
- Skalierbare Datenschutz-Tools erleichtern die Einhaltung übergreifender gesetzlicher Vorschriften

SCHREIBEN SIE IHRE EIGENE ERFOLGS-GESCHICHTE MIT COMFORTE

Mit mehr als 20 Jahren Erfahrung in der Datenschutz auf wirklich geschäftskritischen Systemen ist comforte der perfekte Partner für Unternehmen, die ihr wertvollstes Gut schützen wollen: Daten. comforte's Data Protection Suite, SecurDPS, wurde von Grund auf entwickelt, um die Datensicherheit in einer Welt zu gewährleisten, die von digitalen Geschäftsinnovationen, mündigen Kunden und ständigen technologischen Umwälzungen geprägt ist.

Wir sind für Ihren Erfolgda. Wir bieten Ihnen unser Fachwissen, eine innovative Technologie-Lösung und lokalen Support. Um mehr zu erfahren, sprechen Sie noch heute mit Ihrem comforte-Vertreter und besuchen Sie : **www.comforte.com.**

> *Wir waren begeistert von der Zusammenarbeit mit comforte bei der Erweiterung unserer Datensicherungssysteme. Das engagierte Team von Fachleuten hat sich wirklich die Zeit genommen, unsere Anforderungen vollständig zu verstehen und war immer bereit, die Extrameile zu gehen, um dieses Projekt erfolgreich zu machen. Ihre kontinuierliche Unterstützung wird auch in Zukunft von unschätzbarem Wert sein.*
>
> *– CISO bei einem großen Modehändler*

Ver- und Entschlüsselungsvorgänge beanspruchen zusätzliche Rechenleistung und können die Transaktionsgeschwindigkeit und -leistung beeinträchtigen. In Spitzenzeiten, wenn Kunden ihre Geschäfte besuchen, kann das Transaktionsvolumen von allen POS-Geräten in den Geschäften und den Online-Transaktionen zusammengenommen über 800 Transaktionen pro Sekunde erreichen. Das Letzte, was dieser Einzelhändler wollte, war eine Verlangsamung der Autorisierung von Zahlungen an seinem Point of Sale, da dies seinen weltweit anerkannten Kundenservice beeinträchtigen könnte.

Ver- und Entschlüsselung bedeuten auch Mehraufwand für den IT-Betrieb, insbesondere für die Verwaltung der Verschlüsselungsschlüssel. Wie bei der Verschlüsselungsverarbeitung üblich, müssen die Verschlüsselungsschlüssel in regelmäßigen Abständen aktualisiert und ausgetauscht werden (auch als "rotierende Schlüssel" bezeichnet), um die Möglichkeit einer Datengefährdung bei Verlust oder Diebstahl der Schlüssel zu verringern. Der Einzelhändler rechnet damit, dass sein Volumen von Jahr zu Jahr zunimmt; daher war es folgerichtig, dass auch die Betriebs- und Schlüsselverwaltungsfunktionen wachsen. Um diesen Aufwand ins rechte Licht zu rücken: Angesichts des Jahresvolumens dieses Einzelhändlers war die jährliche Rotation der Verschlüsselungsschlüssel auf einer Milliarde Zahlungskarten keine Aufgabe, die man fortsetzen wollte.

LÖSUNG

Tokenisierung

Der Einzelhändler entschied sich für Tokenisierung, um sensible Daten im gesamten Unternehmen zu schützen. Bei der Tokenisierung werden sensible Datenelemente durch einen Ersatzwert ohne auswertbaren Wert ersetzt, der auch als Token bezeichnet wird. Sie unterscheidet sich von der klassischen Verschlüsselung dadurch, dass sie keine Verschlüsselungsschlüssel oder Schlüsselverwaltung erfordert. Dies macht die Tokenisierung zu einer idealen Datenschutzmethode für wachsende Unternehmen mit hohem Transaktionsvolumen, da ohne Schlüsselverwaltung ein geringeres Risiko der Offenlegung sensibler Daten und geringere betriebliche Auswirkungen bestehen. Außerdem muss keine Verschlüsselungsverwaltung geplant und mit Ressourcen ausgestattet werden.

Erhaltung des Formats

Eine weitere wichtige Anforderung war, dass sensible Daten, wenn sie geschützt werden, im gleichen Format bleiben sollten, damit der Einzelhändler sie im gesamten Unternehmen weiterverwenden und die gleichen Resultate bekommen kann. Bei der Tokenisierung wird beispielsweise eine 16-stellige Kreditkartennummer durch einen 16-stelligen Token ersetzt, der für die Verarbeitung einer Zahlung verwendet werden kann, ohne dass die ursprüngliche 16-stellige Nummer in irgendeinem Schritt offengelegt werden muss. Das gleiche Prinzip lässt sich auf andere sensible Daten wie Namen, Geburtsdaten, Telefonnummern usw. anwenden. Auf diese Weise kann der Einzelhändler die Verwendbarkeit der Daten während des gesamten Lebenszyklus jedes Kunden in seinen Anwendungen und Diensten aufrechterhalten und eine zusätzliche Sicherheitsebene schaffen, um Vorfälle der Datenpreisgabe und Datenschutzverletzungen zu verhindern.

Proof of Concept

Der Einzelhändler führte ein Proof-of-Concept-Projekt (PoC) mit der Tokenisierungslösung von comforte durch und war mit den Ergebnissen sehr zufrieden, da alle Anforderungen in Bezug auf Geschwindigkeit, Sicherheit und Formaterhaltung erfüllt werden konnten. .

> *Wir haben es zu unserer Aufgabe gemacht, Lösungen zum Schutz der Daten anzubieten, die Unternehmen von ihren Kunden anvertraut wurden. Wir freuen uns sehr, diese Mission fortzusetzen, indem wir die Tokenisierung in Arsenal der Informationssicherheit dieses großen Einzelhändlers aufnehmen und dabei helfen, die Daten seiner treuen Kunden zu schützen.*
>
> *– Michael Deissner, CEO der comforte AG*

VORTEILE

Die Tokenisierung ist vom PCI Security Standards Council als wirksamer Ansatz zum Schutz der Karteninhaberdaten anerkannt. Die neue Tokenisierung hat es dem Einzelhändler ermöglicht, die PCI DSS Vorschriften weiterhin einzuhalten, jetzt aber zu wesentlich geringeren Kosten.

Reduzierung des PCI-Auditumfangs

Die Umstellung auf Tokenisierung als Datenschutzmethode brachte zwei zusätzliche Vorteile mit sich. Erstens kann der Einzelhändler den Umfang der Sicherheitsprüfungen, denen er sich jedes Jahr unterziehen muss, reduzieren. Normalerweise müssen bei den Sicherheitsaudits zur Einhaltung der PCI DSS Vorschriften alle Systeme überprüft werden, die die ursprünglichen Daten der Karteninhaber enthalten. Da bei der Tokenisierung die Originaldaten durch einen Token ersetzt werden, können die meisten Systeme aus dem Umfang der Sicherheitsprüfung herausgenommen werden, da die Originaldaten nicht mehr existieren. Tatsächlich konnten ganze Geschäfte aus dem Geltungsbereich herausgenommen werden, was den Zeit- und Kostenaufwand für die Prüfungen erheblich reduzierte.

Übergreifende Einhaltung von Vorschriften

Darüber hinaus ist der Einzelhändler durch die Tokenisierung in der Lage, auf andere Datenschutzgesetze zu reagieren, die die Verarbeitung personenbezogener Daten (PII) betreffen. In den USA hat jeder Bundesstaat Datenschutzgesetze zum Schutz von Kundendaten erlassen oder wird dies in Kürze tun. Je nachdem, wie der Einzelhändler die personenbezogenen Daten seiner Kunden verwendet, kann er in Zukunft weiteren Datenschutzgesetzen mit unterschiedlichen Anforderungen unterliegen. Durch die Tokenisierung werden sensible Daten durch Token ersetzt, und wenn es neue Datenschutzgesetze gibt, die der Einzelhändler in Zukunft einhalten muss, ist die Ausweitung des Schutzes auf zusätzliche Daten nur eine Frage eines API-Aufrufs.