Security Standards Council

INFORMATIONSNACHTRAG

Migration von SSL und frühem TLS

Version 1.1
Datum: April 2016
Autor: PCI Security Standards Council

Zusammenfassung für die Geschäftsleitung

Jetzt ist der Zeitpunkt zu migrieren.

Secure Sockets Layer (SSL) ist seit zwanzig Jahren als eines der am meisten verwendeten Verschlüsselungsprotokolle, die jemals eingeführt wurden, auf dem Markt und befindet sich auch heute noch in breiter Verwendung, obwohl verschiedene Sicherheitsrisiken in Bezug auf das Protokoll offengelegt wurden.

SSL v3.0 wurde 1999 von TLS v1.0 abgelöst und das wiederum seither von TLS v1.1 und v1.2. Heute entsprechen SSL und frühes TLS nicht mehr den Mindestsicherheitsstandards, weil es mittlerweile sicherheitstechnische Verwundbarkeiten im Protokoll gibt, für die keine Abwehrmaßnahmen bekannt sind. Es ist deshalb von allergrößter Bedeutung, dass Unternehmen sobald wie möglich auf eine sichere Alternative aufrüsten und eine Rückfallmöglichkeit auf SSL und frühes TLS sperren.

SSL/early TLS gilt seit PCI DSS v3.1 (April 2015) nicht mehr als Beispiel einer starken Kryptographie.

Was ist das Risiko?

SSL/TLS verschlüsselt einen Kanal zwischen zwei Endpunkten (beispielsweise einem Webbrowser und einem Webserver), um Datenschutz und Datensicherheit bei der Übertragung über den Kommunikationskanal zu gewährleisten. Seit der Einführung von SSL v3.0 wurden mehrere Verwundbarkeiten identifiziert, der jüngste Fall war Ende 2014, als Forscher Einzelheiten zu einer Sicherheitslücke (CVE-2014-3566) veröffentlichten, die Angreifern erlauben könnte, Daten aus sicheren Verbindungen abzuzapfen. Diese Lücke wird allgemeiner als POODLE (Padding Oracle On Downgraded Legacy Encryption) bezeichnet. Es handelt sich dabei um eine sogenannte man-in-the-middle-Angriffstechnik, die es ermöglicht, eine mit SSL v3.0 gesicherte verschlüsselte Botschaft zu entschlüsseln.

Das SSL-Protokoll (alle Versionen) lässt sich dagegen nicht schützen. Es sind keine Möglichkeiten bekannt, Sicherheitslücken wie POODLE zu schließen. SSL und frühes TLS entsprechen nicht mehr den Bedürfnissen von Unternehmen, die starke Kryptographie einsetzen, um Zahlungsdaten bei der Übertragung über öffentliche oder nichtvertrauenswürdige Kommunikationskanäle zu schützen. Außerdem haben moderne Webbrowser begonnen, SSL-Verbindungen zu verhindern, was Nutzer dieser Browser daran hindert, auf Webserver zuzugreifen, die noch nicht auf ein moderneres Protokoll zu migrieren.

Wie soll ich reagieren?

Die beste Reaktion ist, SSL komplett abzuschalten und zu einem moderneren Verschlüsselungsprotoll zu migrieren. Zum Zeitpunkt dieser Veröffentlichung ist dies mindestens TLS v1.1, allerdings wird Unternehmen dringend nahegelegt, TLS v1.2 in Betracht zu ziehen. Beachten Sie, dass nicht alle Implementierungen vonTLS v1.1 als sicher gelten – schlagen Sie in NIST SP 800-52 rev 1 zu Anleitungen zu sicheren TLS-Konfigurationen nach.

Was dies für PCI DSS bedeutet

Ab PCI DSS v3.1 sind SSL und frühes TLS keine Beispiele mehr für starke Kryptographie oder sichere Protokolle. Die direkt betroffenen PCI-DSS-Anforderungen sind:

Anforderung 2.2.3	Implementieren zusätzlicher Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden.
Anforderung 2.3	Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs mithilfe einer starken Kryptographie.
Anforderung 4.1	Verwenden von starker Kryptographie und Sicherheitsprotokollen, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen.

SSL und frühe Versionen von TLS dürfen nicht als Sicherheitskontrolle verwendet werden, um diese Anforderungen zu erfüllen. Zur Unterstützung von Einheiten bei der Migration weg von SSL/frühen Versionen von TLS sind die folgenden Bestimmungen enthalten:

- Neue Implementierungen dürfen SSL oder frühes TSL nicht als Sicherheitsmaßnahme einsetzen (Anweisungen zu neuen und bestehenden Implementierungen enthält der nächste Abschnitt)
- Alle Dienstanbieter müssen ab 30. Juni **2016** ein sicheres Serviceangebot vorhalten.
- Nach dem 30. Juni **2018** müssen alle Einheiten die Verwendung von SSL/frühen Versionen von TLS als Sicherheitskontrolle eingestellt haben und ausschließlich sichere Versionen des Protokolls (eine Ausnahmeregelung für bestimmte POS-POI-Terminals wird weiter unten im letzten Aufzählungspunkt beschrieben) verwenden.
- Vor dem 30. Juni 2018 müssen alle vorhandenen Implementierungen, die SSL und/oder frühe Versionen von TLS verwenden, über einen offiziellen Plan zur Risikoabschwächung und Migration verfügen.
- POS-POI-Terminals (und die SSL/TLS Abschlusspunkte, mit welchen sich diese Verbinden), bei welchen nachgewiesen werden kann, dass diese nicht anfällig für bekannte Sicherheitsrisiken von SSL und frühen Versionen von TLS sind, dürfen diese nach dem 30. Juni 2018 weiterhin als Sicherheitskontrolle verwenden.

Wird SSL/frühes TLS verwendet, gelten die Anforderung in PCI DSS Anhang A2 *„Zusätzliche PCI-DSS-Anforderungen für Unternehmen, die SSL/frühes TLS verwenden"*.

Zum Verständnis von „neuen" und „bestehenden" Implementierungen.

Implementierungen gelten als „neue Implementierungen", wenn es keine Abhängigkeit von der Verwendung der verwundbaren Protokolle gibt. Beispielsszenarien, die als „neue" Implementierungen gelten würden:

- Installation eines Systems in eine Umgebung, die bisher ausschließlich sichere Protokolle verwendet
- Installation einer Anwendung auf einem System, das bisher ausschließlich sichere Protokolle verwendet
- Bau eines neuen Systems oder Netzwerks zur Kommunikation mit anderen Systemen bzw. Netzwerken, die sichere Protokolle verwenden

Wenn eine neue Implementierung nicht die bestehende Verwendung eines verwundbaren Protokolls zu unterstützen braucht, darf sie nur mit sicheren Protokollen und starker Kryptographie implementiert und nur so konfiguriert werden, dass keine Rückfall auf das verwundbare Protokoll erlaubt ist.

Hinweis: *Neue E-Commerce-Implementierung dürfen Verbraucher-Web-Browser nicht als bestehende Infrastruktur ansehen, die es zu unterstützen gälte.*

Umgekehrt sind „bestehende" Implementierungen solche, bei denen eine Stützung auf oder Verwendung von einem oder mehreren verwundbaren Protokollen besteht. Beispielsszenarien, die als „bestehende" Implementierungen gelten würden:

- Installation eines Systems in eine Umgebung, die derzeit verwundbare Protokolle verwendet beziehungsweise unterstützen muss
- Installation einer Anwendung auf einem System, das derzeit verwundbare Protokolle verwendet beziehungsweise unterstützen muss
- Bau eines neuen Systems oder Netzwerks zur Kommunikation mit anderen Systemen bzw. Netzwerken, die derzeit verwundbare Protokolle verwenden

Es wird empfohlen, bestehende Implementierungen sofort aufzufrüsten, da fortdauernde Verwendung von SSL/frühem TLS die Umgebung in Gefahr bringen könnte.

Erstellung eines Planes zur Risikoabschwächung und Migration

Der Plan zur Risikoabschwächung und Migration ist ein von der Einheit vorbereitetes Dokument, das die Pläne zur Migration auf ein sicheres Protokoll aufführt und außerdem die Kontrollen der Einheit beschreibt, die diese zur Minderung der Risiken in Verbindung mit SSL/einer frühen Version von TLS verwendet, bis die Migration abgeschlossen ist. Der Plan zur Risikoabschwächung und Migration muss im Rahmen des PCI-DSS-Beurteilungsverfahrens einem Beurteiler vorgelegt werden.

Nachfolgend Anweisungen und Beispiele von Angaben, die im Plan zur Risikoabschwächung und Migration niederzulegen sind:

- Beschreibung, wie verwundbare Protokolle verwendet werden, darunter:
    - Die Art der Umgebung, in der die Protokolle verwendet werden - z.B. die Art des Zahlungskanals und der Funktionen, für die die Protokolle verwendet werden
    - Die Art der übertragenen Daten - z.B. Elemente von Kartenkontodaten, Verwaltungsverbindungen usw.
    - Anzahl und Arten von Systemen, die die Protokolle verwenden bzw. unterstützen - z.B. POS-POI-Terminals, Zahlungsswitches usw.
- Ergebnisse der Risikobewertung und vorhandene Kontrollen zur Risikominderung;
    - Unternehmen sollten das Risiko für ihre Umgebung untersucht und dokumentiert und Kontrollen zur Risikominderung eingerichtet haben, um das Risiko abzudämpfen helfen, bis die verwundbaren Protokolle vollständig entfernt werden können.
- Beschreibung der Prozesse, die implementiert sind, um neue Verwundbarkeiten von verwundbaren Protokollen zu überwachen und zu entdecken:
    - Unternehmen haben von sich aus tätig zu werden und über neue Verwundbarkeiten auf dem laufenden zu bleiben. Werden neue Verwundbarkeiten veröffentlicht, muss das Unternehmen jeweils das Risiko einschätzen, das sie für seine Umgebung darstellen, und ermitteln, ob zusätzliche Kontrollen zur Risikominderung implementiert werden müssen, bis die Migration abgeschlossen ist.
- Beschreibung der Verfahren zur Änderungskontrolle, die implementiert wurden, um zu gewährleisten, dass SSL/eine frühe Version von TLS nicht in neuen Umgebungen implementiert wird;
    - Verwendet ein Unternehmen derzeit keine verwundbaren Protokolle und muss es auch keine Unterstützung dafür leisten, besteht kein Grund, dass es diese Protokolle in seiner Umgebung einrichtet. Zu den Verfahren zur Überwachung des Wandels (change control processes) gehört auch die Einschätzung der Auswirkung des Wandels, um sicherzustellen, dass der Wandel keine neue Sicherheitsschwäche in die Umgebung einträgt.
- Überblick über den Migrationsprojektplan, einschließlich einem Termin für den Abschluss der Migration spätestens zum 30. Juni 2018:
    - Dokumentation zur Migrationsplanung einschließlich der Bestimmung, welche Systeme/Umgebungen migriert werden und wann, sowie eines Zieldatums bis zu dem die Migration insgesamt abzuschließen ist. Das Zieldatum für die Migration insgesamt muss am oder vor dem 30. Juni 2018 liegen.

Häufig gestellte Fragen (FAQs)

Was sind Kontrollen zur Risikoabschwächung?

Bei Umgebungen, die derzeit verwundbare Protokolle verwenden, hilft die Implementierung und fortgesetzte Verwendung von Kontrollen zur Risikoabschwächung, die verwundbare Umgebung zu schützen, bis die Migration zu einer sicheren Alternative abgeschlossen ist.

Folgende Kontrollen können bei der Risikoabschwächung helfen:

- Minimieren der Angriffsfläche soweit wie möglich durch Konsolidieren von Funktionen, die verwundbare Protokolle verwenden, auf weniger Systeme, und Verringern der Zahl der Systeme, die die Protokolle unterstützen.
- Entfernung oder Sperrung der Verwendung von Webbrowsern, JavaScript und sicherheitsrelevanten Sitzungscookies, wo sie nicht benötigt werden.
- Erkennen und Abweisen von Anfragen zur Herunterstufung auf eine niedrigere Protokollversion, um die Anzahl von Kommunikationen zu verringern, die die verwundbaren Protokolle verwenden.
- Einschränkung der Verwendung der verwundbaren Protokolle auf bestimmte Einheiten, beispielsweise durch Konfiguration von Firewalls zur Erlaubnis von SSL/frühem TLS ausschließlich auf bekannte IP-Adressen (bzw. Geschäftspartner, die die Nutzung der Protokolle benötigen) und Abweisung dieses Verkehrs für alle anderen IP-Adressen.
- Erweiterung der Erkennungs-/Präventionsfähigkeiten durch Ausdehnung der Abdeckung von Systemen zur Verhinderung des Eindringens, Aktualisieren von Signaturen und Abweisung von Netzwerkverkehr, der auf böswilliges Verhalten hindeutet.

- Aktives Beobachten auf verdächtige Aktivität - beispielsweise Erkennen von ungewöhnlicher Zunahme bei Anfragen für den Rückfall auf verwundbare Protokolle - und Ergreifen entsprechender Gegenmaßnahmen.

Außerdem sollten Unternehmen sicherstellen, dass alle geltenden PCI-DSS-Anforderungen ebenfalls erfüllt sind, darunter:

- Von sich aus über neue Verwundbarkeiten informiert bleiben, beispielsweise Mitteilungsdienste zu Verwundbarkeiten oder Besuch von Supportsites von Lieferanten, um aktualisierte Nachrichten zu neuen Verwundbarkeiten zu erhalten, sowie sie sich ergeben.
- Anwenden der Herstellerinformationen für die sichere Konfiguration der Technik.

Welche Migrationsoptionen gibt es unter anderem?

Beispiele zusätzlicher kryptographischer Maßnahmen, die implementiert und als Sicherheitskontrolle für den Ersatz von SSL/frühem TLS verwendet werden können, sind unter anderem:

- Aktualisieren auf eine laufende, sichere Version von TLS, die sicher implementiert und so konfiguriert ist, dass sie den Rückfall auf SSL oder frühes TLS nicht zulässt.
- Verschlüsselung von Daten mit starker Kryptographie vor dem Versand über SSL/frühes TLS (beispielsweise Verwendung von Verschlüsselung auf der Feld- oder Anwendungsebene bei der Verschlüsselung der Daten vor der Übertragung)
- Einrichten einer stark verschlüsselten Sitzung (z.B. einen IPsec-Tunnel) und erst danach Versand der Daten über SSL innerhalb des sicheren Tunnels

Zusätzlich kann die Verwendung der Zwei-Faktor-Authentifizierung mit den obigen Maßnahmen verbunden werden, um die Authentifizierung sicherzustellen.

Die Wahl einer alternativen kryptographischen Kontrolle wird von den technischen und wirtschaftlichen Erfordernissen der jeweiligen Umgebung abhängen.

Was gilt für Kleinhändlerumgebungen?

Die Probleme mit SSL/frühem TLS betreffen alle Arten von Unternehmen, also auch kleine Händler. Es kommt entscheidend darauf an, dass auch kleine Händler die nötigen Schritte ergreifen, um SSL/frühes TSL aus ihrer Kundendatenumgebung zu entfernen, um sicherzustellen, dass ihre Kundendaten geschützt sind.

Was die POI-Umgebung angeht, wird empfohlen, dass kleine Händler sich an ihren Terminallieferanten bzw. ihren Acquirer (Geschäftsbank) wenden, um herauszufinden, ob ihre POS-POI-Terminals von den SSL-Verwundbarkeiten betroffen sind.

Was andere Umgebungen angeht - z. B. virtueller Zahlungsterminals, Server im Backoffice usw., sollten kleine Händler prüfen, ob SSL/frühes TLS verwendet wird und wo es implementiert ist, und dann ermitteln, ob ein Upgrade sofort geschehen kann, oder ob es betriebswirtschaftliche Gründe gibt, das Upgrade erst später durchzuführen (jedoch spätestens zum 30. Juni 2018).

Zu den Dingen, die Sie in Ihrer Umgebung in Betracht ziehen sollten, gehören die folgenden:

- Prüfen Sie, welche Webbrowserversion Sie verwenden - ältere Versionen nutzen SSL/frühes TLS, so dass Sie womöglich auf einen neueren Browser aktualisieren müssen
- Prüfen Sie die Konfiguration Ihrer Firewall, ob SSL abgewiesen werden kann
- Stellen Sie sicher, dass alle Anwendungs- und Systempatches auf dem neuesten Stand sind
- Überprüfen und überwachen Sie Ihre Systeme, um verdächtige Aktivität zu entdecken, die womöglich auf ein Sicherheitsproblem hindeutet

Außerdem müssen Sie, wenn Sie Ihre Migration zu einer sicheren Alternative planen, einen Plan zur Risikoabschwächung und Migration erstellen.

Was sollten Händler mit POI-Terminals tun, die SSL/frühes TLS unterstützen?

POI können weiterhin SSL/eine frühe Version von TLS verwenden, wenn nachgewiesen werden kann, dass der POI nicht anfällig für aktuell bekannte Schwachstellen ist. Bei SSL handelt es sich jedoch um veraltete Technologie und kann daher in Zukunft von weiteren Sicherheitsrisiken betroffen sein; es wird daher dringend empfohlen, dass POI-Umgebungen so schnell wie möglich auf sichere Protokolle aktualisiert werden. Neue Implementierungen von POIs sollten dringend die Unterstützung und Verwendung von TLS 1.2 oder höher in Betracht ziehen. Wenn SSL/eine frühe Version von TLS in der Umgebung nicht benötigt werden, sollte die Verwendung dieser Versionen und ein Fallback deaktiviert werden.

Bei der Durchsicht von Implementierung von POI-Terminals, die SSL/frühes TLS verwenden sollten Beurteiler die unterstützende Dokumentation ebenfalls durchsehen (beispielsweise vom POI-Lieferanten bereitgestellte Dokumentation, Konfigurationsdetails zum System/Netzwerk usw.) um zu ermitteln, ob die Implementierung für bekannte Sicherheitsrisiken anfällig ist.

Sollte die POS-POI-Umgebung anfällig für bekannte Sicherheitsrisiken sein, ist sofort mit der Planung zur Migration auf eine sichere Alternative zu beginnen.

Hinweis: Die Ausnahmeregelung für POS-POI-Umgebungen, die derzeit nicht anfällig für bekannte Sicherheitsrisiken sind, basiert auf aktuellen, bekannten Risiken. Sollten sich neue Schwachstellen ergeben, für die POI-Umgebungen anfällig sind, müssen diese aktualisiert werden.

Warum sind POS-POI-Umgebungen weniger verwundbar?

PCI DSS bietet eine Regelung, wonach SSL und frühes TLS auf Point-of-Sale-(POS) und Point-of-Interaction-(POI)-Geräten und ihren Abschlusspunkten weiter verwendet werden dürfen. Dies liegt daran, dass die Verwundbarkeiten, die zum Zeitpunkt dieser Veröffentlichung bekannt sind, im allgemeinen in diesen Umgebungen schwerer auszunutzen sind.

Beispiel: Manche der derzeitigen SSL-Verwundbarkeiten werden von einem Angreifer ausgenutzt, der die Client-Server-Kommunikation abfängt und die Nachrichten an den Client manipuliert. Ziel des Angreifers ist es, den Client dahingehend irrezuführen, dass er weitere Daten sendet, die der Angreifer nutzen kann, um die Sitzung zu missbrauchen. POS-POI-Geräte mit den folgenden Merkmalen sind im allgemeinen widerstandsfähiger gegen diese Art von Verwundbarkeit:

- Das Gerät unterstützt keine mehrfachen Verbindungen auf der Client-Seite (was die POODLE-Schwachstelle ermöglicht)
- Das Zahlungsprotokoll gehorcht ISO 20022 (Universal Financial Industry Message Scheme)/ISO 8583-1:2003 (Financial Transaction Card Originated Messages – Interchange Message Specifications) oder einem gleichwertigen Standard, der die Datenmenge begrenzt, die durch „replay attacks" offengelegt werden kann.
- Das Gerät verwendet keine Webbrowsersoftware, JavaScript oder sicherheitsbezogene Sitzungscookies.

Hinweis: Diese Merkmale sollen lediglich als Beispiel dienen. Jede Implementierung ist unabhängig zu überprüfen, um das Ausmaß ihrer Verwundbarkeit zu bestimmen.

Es kommt darauf an im Sinn zu behalten, dass sich Schwachstellen weiterentwickeln. Organisationen müssen deshalb vorbereite sein, auf neue Bedrohungen zu reagieren. Alle Organisationen, die SSL beziehungsweise frühes TLS verwenden, sollten planen, so bald wie möglich auf ein starkes kryptographisches Protokoll aufzurüsten.

Jede übergangsweise Verwendung von SSL/frühem TLS in POS-POI-Umgebungen muss mit aktuellen Patches versehen sein, auch ist sicherzustellen, dass nur die notwendigen Erweiterungen aktiviert sind.

Was bedeutet dies für Zahlungsabwickler, die POI-Umgebungen unterstützen?

Das Problem mit SSL/frühem TLS betriff Unternehmen aller Arten einschließlich Zahlungsabwickler, Zahlungsgateways sowie sonstigen Unternehmen, die Zahlungsabwicklungsdienste anbieten. Diese Unternehmen müssen ihren Einsatz von SSL/frühem TLS überprüfen und in gleicher Weise Migrationen planen wie andere Unternehmen.

Zahlungsabwickelnde Unternehmen POI-Terminierungspunkten müssen überprüfen, dass die POI-Kommunikation nicht verwundbar ist (wie oben im Abschnitt „Warum POS-POI-Umgebungen weniger verwundbar sind"), wenn sie weiter SSL/frühes TLS verwenden wollen.

Wenn ein Zahlungsabwicklungsunternehmen mehrfache Zahlungskanäle – beispielsweise POI und E-Commerce-Transaktionen – über denselben Terminierungspunkt unterstützt, muss es sicherstellen, dass alle verwundbaren Kanäle bis 30 · Juni 2018 auf eine sichere Alternative migriert werden. Wenn die POI-Umgebung als nicht verwundbar eingeschätzt wird, kommen für das Unternehmen die folgenden Optionen in Betracht:

- POI-Kanäle auf eine sichere Alternative migrieren, so dass sowohl POI- als auch E-Commerce-Transaktionen weiterhin denselben Terminierungspunkt verwenden können.
- Wenn POI-Kanäle nicht migriert werden, können getrennte Terminierungspunkte beziehungsweise -schnittstellen verwendet werden, um den POI-Verkehr, der SSL/frühes TLS verwendet, von dem E-Commerce-Verkehr zu trennen, der auf eine sichere Alternative migriert wurde.

Was gilt für E-Commerce-Umgebungen?

Das Wesen von webbasierten Umgebung bringt es mit sich, dass E-Commerce-Implementierung die höchste Gefährdung aufweisen und daher unmittelbar von den bekannten Verwundbarkeiten in SSL/frühem TLS bedroht sind.

Deshalb dürfen neue E-Commerce-Website kein SSL/frühes TLS verwenden oder unterstützen.

E-Commerce-Umgebungen, die derzeit Kunden unterstützen müssen, die SSL/frühes TLS verwenden, müssen sobald wie möglich mit der Migration beginnen und alle Migrationen bis 30. Juni 2018 abschließen. Kann eine Migration nicht sofort erfolgen, muss die Begründung dafür im Rahmen des Plans zur Risikoabschwächung und Migration dokumentiert werden.

Bis zum Abschluss der Migration wird empfohlen, die Zahl der Server, die SSL/frühes TLS verwenden, so gering wie möglich zu halten. Die Verringerung der Zahl verwundbarer Systeme verringert die mögliche Exposition gegenüber Schwachstellen und kann auch helfen, Kontrollen zur Risikoabschwächung erleichtern, etwa verstärkte Beobachtung von verdächtigem Verkehr.

Wir ermutigen E-Commerce-Händler außerdem dazu, ihre Kunden anzuhalten, ihre Webbrowser zu aktualisieren, damit sie sichere Protokolle unterstützen.

Wo sollte der Migrationsprozess beginnen?

Nachfolgend einige empfohlene Schritte, die Unternehmen helfen, ihre Migration zu einer sicheren Alternative zu planen:

1. Alle Systemkomponenten und Datenflüsse identifizieren, die sich auf die verwundbaren Protokolle stützen beziehungsweise sie unterstützen.
2. Für jede Systemkomponente oder Datenfluss bestimmen, welches geschäftliche beziehungsweise technische Bedürfnis besteht, das verwundbare Protokoll zu verwenden
3. Sofort alle Instanzen verwundbarer Protokolle entfernen oder sperren, für die es keine geschäftliche oder technische Rechtfertigung gibt
4. Technik identifizieren, die die verwundbaren Protokolle ersetzen kann, und sichere Konfigurationen dokumentieren, die implementiert werden sollen.
5. Einen Migrationsprojektplan aufsetzen, der Schritte und Termine für Updates beschreibt
6. Kontrollen zur Risikoabschwächung einrichten, um die Anfälligkeit gegen bekannte Schwachstellen zu verringern, bis die verwundbaren Protokolle aus der Umgebung entfernt sind
7. Migrationen durchführen und Change-Control-Verfahren befolgen, um sicherzustellen, dass Systemaktualisierungen getestet und autorisiert sind
8. Systemkonfigurationsstandards aktualisieren, wenn die Migrationen auf die neuen Protokolle abgeschlossen sind

Kann SSL/frühes TLS in einer Umgebung verbleiben, wenn es nicht als Sicherheitskontrolle verwendet wird?

Ja, diese Protokolle können in einem System in Gebrauch bleiben, solange SSL/frühes TLS nicht als Sicherheitskontrolle verwendet wird.

Außerdem sind gemäß PCI-DSS-Anforderung 11.2 alle SSL/TLS-Verwundbarkeiten mit einer Bewertung von CVSS 4 oder höher auf einem ASV-Scan oder auf dem internen Verwundbarkeitsscan des Unternehmens als „hoch" eingestuft werden, innerhalb des vorgeschriebenen Zeitraumes (z. B. vierteljährlich bei ASV-Scans) zu beheben. Befolgen Sie definierte Prozesse zum Umgang mit Verwundbarkeit, um zu dokumentieren, wie SSL/TLS-Verwundbarkeiten behoben wurden – beispielsweise, wo das Protokoll nur für POI-Kommunikation verwendet wird, das nicht für Schwachstellen anfällig ist, oder wo es vorhanden ist, aber nicht als Sicherheitskontrolle eingesetzt wird (z. B. nicht zum Schutz der Vertraulichkeit der Kommunikation dient).

Gelten die Migrationstermine auch, wenn sich aus der Verwendung von SSL/frühem TLS keine Gefahr für Karteninhaberdaten ergibt?

Ja, der Termin für die Migration weg von SSL/frühem TLS ist unabhängig von der Zahl der Bedrohungen von Zahlungskartendaten, die sich in der Zukunft ergeben kann oder auch nicht. Die PCI-DSS-Anforderungen sollen helfen, durch einen Ansatz der Verteidigung in der Tiefe Bedrohungen von Karteninhaberdaten verhindern zu helfen. Die Veröffentlichung von möglichen Datenlecks abwarten, ehe man Schritte unternimmt, die eigenen Daten zu sichern, ist kein wirkungsvoller Ansatz in der Sicherheit und wird in den PCI DSS auch nicht unterstützt.

Wie beeinflusst die Anwesenheit von SSL die ASV-Scanergebnisse?

SSL v3.0 und frühes TLS enthalten eine Anzahl von Verwundbarkeiten, wovon sich einige derzeit in einem Wert von 4,3 im CVSS (Common Vulnerability Scoring System) niederschlagen. Dem CVSS liegt die NVD (National Vulnerability Database) zugrunde und ist das Bewertungssystem, das ASVs zu verwenden haben. Verwundbarkeiten mit mittlerem oder hohem Risiko (d.h. Verwundbarkeiten mit einem CVSS von 4,0 oder mehr) müssen behoben und die betroffenen Systeme nach der Behebung neu gescannt werden, um zu zeigen, dass das Problem gelöst wurde.

Allerdings gibt es für manche dieser Verwundbarkeiten keine Möglichkeit, sie zu beheben, weshalb die empfohlene Strategie zur Risikoabschwächung die Migrierung auf eine sichere Alternative zum nächstmöglichen Zeitpunkt ist. Soweit ein Unternehmen nicht in der Lage ist, sofort auf eine sichere Alternative zu migrieren, sollte es mit seinem ASV zusammenarbeiten, um sein jeweiliges Szenario wie folgt zu dokumentieren:

- *Vor dem 30. Juni 2018:* Unternehmen, die ihre Migration noch nicht abgeschlossen haben, sollten dem ASV schriftlich bestätigen, dass sie einen Plan zur Risikoabschwächung und zur Migration in Kraft gesetzt haben und daran arbeiten, ihre Migration zum vorgeschriebenen Termin abzuschließen. Der ASV sollte dfen Empfang dieser Bestätigung als Ausnahme unter „Ausnahmen, falsche Positive oder ausgleichende Kontrollen" in der Zusammenfassung des ASV-Scanreports. Der ASV kann für diesen Scanbestandteil oder Host ein „bestanden"-Ergebnis verleihen, sofern der Host alle einschlägigen Scananforderungen erfüllt.
- *Nach dem 30. Juni 2018:* Unternehmen, die die Migration weg von SSL/frühem TLS noch nicht abgeschlossen haben, befolgen das Verfahren zur Begegnung von Verwundbarkeiten mithilfe von ausgleichenden Kontrollen, um sicherzustellen, dass das betroffene System nicht für die jeweiligen Verwundbarkeiten anfällig ist. Beispielsweise Fälle, in denen SSL/frühes TLS vorhanden ist, aber nicht als Sicherheitskontrolle eingesetzt wird (z. B. nicht zum Schutz der Vertraulichkeit der Kommunikation dient).

Unternehmen mit POS-POI-Terminals beziehungsweise Terminierungspunkten, die als nicht anfällig für die jeweiligen Verwundbarkeiten bestätigt sind, sind womöglich berechtigt, für diese Systeme eine verringerte NVD-Bewertung zu erhalten. In diesem Szenario muss der ASV (zusätzlich zu allen anderen erforderlichen Berichtselementen) die folgenden Informationen entsprechend dem ASV-Programmführer bereitstellen:

- Die NVD-Bewertung der Verwundbarkeit
- Die Bewertung der Verwundbarkeit durch den ASV
- Warum der ASV mit der NVD-Bewertung nicht einverstanden ist

Beispielsweise könnte der ASV feststellen, dass eine bestimmte Verwundbarkeit in einer bestimmten POS-POI-Umgebung schwerer ausnutzen ist als entsprechend der Definition im allgemeinen NVD-Bewertungssystem. Der ASV kann dann dieses Element für die fraglichen Systeme im Bewertungssystem in Bezug auf die jeweilige Verwundbarkeit neu einstufen.

Will ein ASV diese Art von Anpassungen vornehmen, muss er die jeweiligfe Umgebung des Kunden, seine System und Kontrollen berücksichtigend und diese Art von Anpassungen nicht einfach aufgrund allgemeiner Trends oder Annahmen vornehmen. Scankunden sollten mit ihrem ASV darin zusamenarbeiten, ein Verständnis von ihrer Umgebung zu gewinnen, da ansonsten der ASV nicht in der Lage sein wird zu beurteilen, ob eine CVSS-Bewertung geändert werden darf.

ASV haben bei diesen Zugeständnissen die gebotene Sorgfalt und Vorsicht anzuwenden und sicherzustellen, dass es eine ausreichende Grundlage für die Änderung der CVSS-Bewertung gibt. Alle Änderungen dieser Art müssen nach dem im ASV-Programmführer definierten Verfahren folgen.

Alle ASV-Scanberichte sind gemäß den Verfahren im ASV-Programmführer zu erstellen.

Heißt das, Unternehmen mit einem Plan zur Risikoabschwächung und Migration brauchen Verwundbarkeiten in SSL/frühem TLS nicht zu patchen?

Nein, die Migrationszieltermine sind keine Grund, das Patchen von Verwundbarkeiten zu verzögern. Neue Bedrohungen und Risiken müssen auch weiterhin gemäß den einschlägigen PCI-DSS-Anforderungen, etwa 6.1, 6.2 und 11.2 bekämpft werden, auch müssen Unternehmen Verwundbarkeiten behandeln, wo ein Sicherheitupdate, Fix oder einen Patch verfügbar ist.

Was ist die Auswirkung auf Dienstleistungen, die sowohl sichere Protokolle unterstützen (z.B. TLS v.12) als auch unsichere (z.B. SSL/frühes TLS)?

Viele Dienstantbieter (beispielsweise Anbieter von gemeinsamem Hosting) stellen Plattformen und Dienste für eine breite Kundenbasis, wozu Unternehmen gehören können, die PCI-DSS-Anforderungen erfüllen müssen ebenso wie solche, die dies nicht tun. Dienstanbieter, die das CDE eines Kunden unterstützen, können entweder belegen, dass sie im Aufrag des Kunden die betreffende Anforderung erfüllen, oder dass sie ihren Kunden Dienstoptionen zur Nutzung anbieten, die PCI-DSS-Anforderungen erfüllen. Der Dienstanbieter sollte seinen Kunden klar zu verstehen geben, welche Sicherheitsprotokolle er anbietet, wie die verschiedenen Optionen zu konfigurieren sind und wie sich die Verwendung von Konfigurationen auswirkt, die als unsicher gelten.

Beispielsweise kann ein Webhostinganbieter eine gehostete Webplattform für Händler anbieten, die TLS v1.2 unterstützt, aber auch schwächere Protokolle. Um die Kunden bei der PCI-DSS-Compliance zu unterstützen, muss der Hostinganbieter ihnen klare Anweisungen geben, wie sie ihre Dienstnutzung so konfigurieren, dass er nur TLS v1.2 ohne Rückfall auf SSL/frühes TLS verwendet. Auf Kundenseite muss ein Händler, der diese Plattform im Rahmen seiner PCI-DSS-Implementierung verwendet, sicherstellen, dass die Konfigurationsoptionen, die er verwendet, TLS v1.2 ohne Rückfall auf SSL/frühes TLS nutzen.

Die Anwesenheit von schwächeren Protokollen in einer gemischten Hostingumgebung kann zu einem Fehlschlag beim ASV-Scan führen. Tritt dies auf, sollten Dienstanbieter und ASV das Verfahren „Ausnahmen, falsche Positive und ausgleichende Kontrollen" befolgten, um zu dokumentieren, wie das Risiko behandelt wurde – beispielsweise, in dem sie bestätigen, dass der Dienstanbieter SSL/frühes TLS nicht als Sicherheitskontrolle verwendet, und dass sichere Konfigurationsoptionen für den Kundenbetrieb gestellt werden, die keinen Rückfall auf schwächere Protokolle erlauben. Der ASV kann für diesen Scanbestandteil oder Host ein „bestanden"-Ergebnis verleihen, sofern der Host alle einschlägigen Scananforderungen erfüllt.