PCI DSS 3.2 COMPLIANCE-CHECKLISTE

SCHUTZ DER DATEN VON KARTENINHABERN

DSS-Anforderung 3

Schützen Sie gespeicherte Karteninhaberdaten

DO:

- ☐ Implementieren Sie dokumentierte Richtlinien zur Datenaufbewahrung und Entsorgung sowie zur Minimierung der erfassten Daten sowie für die Dauer der Aufbewahrung. (3.1)
- ☐ Befragen Sie Ihre Mitarbeiter um sich zu versichern, ob die Richtlinien eingehalten werden. Stellen Sie sicher, dass vierteljährlich wirksam werdende Prozesse dafür sorgen die Karteninhaberdaten zu entfernen, die die Aufbewahrungsfristen überschritten haben. (3.1.b)
- ☐ Stellen Sie sicher, dass die gespeicherten und übertragenen Daten nicht lesbar sind. (3.4, 4.1)
- ☐ Verschlüsseln Sie Kartendaten und schützen Sie die zugehörigen Schlüssel. (3.5)
- ☐ Maskieren Sie die PAN-Daten, wenn diese angezeigt werden müssen (siehe oben) und verwenden Sie dabei möglichst wenige Zeichen (weniger als die ersten 6 und maximal die letzten 4). (3.3)
- ☐ Erstellen Sie ein Flussdiagramm zu den Daten der Karteninhaber und zwar für alle Datenflüsse innerhalb Ihrer Firma. (1.1.3)
- ☐ Verwenden Sie ein Tool zum Auffinden von Daten, um falsch abgespeicherte sensible Daten in der betreffenden Umgebung aufzuspüren.

DON'T:

- ☐ Speichern Sie keine sensiblen Authentifizierungsdaten nach der Authentifizierung. (3.2)
  - o **Ausnahme:** Ihre Organisation ist selbst Aussteller und verfügt über die entsprechende geschäftliche Legitimation.
- ☐ Speicherung maskierter PAN-Daten.
  - o **Lösung:** Verwenden Sie Verschlüsselung.

DSS-Anforderung 4

Verschlüsselte Übertragung von Karteninhaberdaten über offene, öffentliche Netzwerke

DO:

- ☐ Überprüfen Sie, wohin die Daten der Karteninhaber geschickt werden, und stellen Sie sicher, dass Ihre Richtlinien bei der Übermittlung nicht verletzt und ausschließlich vertrauenswürdige Schlüssel oder Zertifikate verwendet werden. (4.1)
- ☐ Wählen Sie eine Reihe an ein- und ausgehenden Übertragungen aus und überprüfen Sie inwieweit die Kryptografie während der Übermittlung gewährleistet ist. (4.1.c)

DON'T:

- ☐ Schicken Sie keine PANs über Kommunikationskanäle, die für End-User gedacht sind, wie E-Mail, SMS oder IM. (4.2)
- ☐ Verwenden Sie keine Technologien, die SSL/ oder frühe TLS-Versionen verwenden (Version 1.0 oder früher)
- ☐ Migrieren Sie keine Daten von Karteninhabern auf Systeme, die SSL/oder frühe TLS-Versionen verwenden. (Version 1.0 oder früher)

SCHUTZ VOR EXTERNEN BEDROHUNGEN

DSS-Anforderung 1

Installieren Sie eine Firewall-Konfiguration, die Karteninhaberinformationen schützt und erhalten Sie diese Konfiguration aufrecht

DO:

- ☐ Installieren Sie eine Firewall an jedem mit dem Internet verbundenen Punkt (auf jedem Gerät) sowie zwischen allen demilitarisierten Zonen (DMZ) und der internen Netzwerkzone. (1.1.4, 1.4)
- ☐ Konfigurieren Sie Ihre Firewalls mit einer Beschreibung der Gruppen, die für Netzwerkkomponenten verantwortlich sind und entsprechend den jeweiligen geschäftlichen Erfordernissen für alle Dienste/Protokolle/Anschlüsse innerhalb der Konfiguration. (1.1.5, 1.1.6)
- ☐ Überprüfen Sie die Firewall- und Router-Konfigurationen mindestens alle sechs Monate, und stellen Sie sicher, dass jeder andere, nicht-konfigurierte Datenverkehr (eingehend und ausgehend) blockiert wird. (1.1.7, 1.2.1)
- ☐ Konfigurieren Sie die Router so, dass es keine Verbindung zwischen den nicht vertrauenswürdigen Teilen des Netzwerks und dem Zugriff auf Informationen von Karteninhabern gibt. (1.2, 1.3)
- ☐ Weisen Sie jemandem konkret die Verantwortung zu, die Firewall-Protokolle täglich zu prüfen.

DON'T:

- ☐ Speichern Sie keine Informationen von Karteninhabern in der DMZ oder nicht vertrauenswürdigen Netzwerken.
  - o **Lösung:** Erstellen Sie eine sichere interne Netzwerkzone. (1.3.6)

DSS-Anforderung 2

Verwenden Sie keine standardmäßigen Voreinstellungen für Systempasswörter und andere Sicherheitsparameter

DO:

- ☐ Identifizieren Sie einen für die Systemkomponenten zuständigen Systemadministrator. (2.2.4)
- ☐ Pflegen Sie eine Bestandsliste aller im Rahmen von PCI DSS verwendeten Systemkomponenten. (2.4)
- ☐ Dokumentieren Sie Richtlinien zur Änderung von voreingestellten Passwörtern, geben Sie Wireless-Einstellungen vor und entfernen Sie voreingestellte Konten bevor Sie ein weiteres System in Ihrem Netzwerk installieren. (2.1, 2.1.1, 2.5)
- ☐ Dokumentieren Sie Konfigurationsstandards für Systemkomponenten, die sich mit Sicherheitsschwachstellen befassen, beschränken Sie den Service-/Protokoll-Zugriff rein auf den Bedarfsfall und folgen Sie gehärteten Standards. (2.2, 2.2.2)

DON'T:

- ☐ Verzichten Sie darauf unterschiedliche Funktionen auf einem einzigen Server umzusetzen, da das zu Berechtigungskonflikten führen kann. (2.2.1)
- ☐ Gehen Sie nicht davon aus, dass Anbieter einen Antiviren-Scan durchführen.
    - o **Anforderung:** Es liegt in Ihrer Verantwortung sicherzustellen, dass Anbietertechnologien auf dem aktuellen Stand sind und regelmäßig geprüft werden.

DSS-Anforderung 5

Schützen Sie sämtliche Systeme vor Malware und aktualisieren Sie Antiviren-Software und -Programme regelmäßig

DO:

- ☐ Aktualisieren Sie die Antiviren-Software regelmäßig auf häufig betroffenen Systemen und finden Sie heraus, ob weitere Systeme gefährdet/zusätzliche Antiviren-Programme erforderlich sind. (5.1, 5.1.1, 5.1.2)
- ☐ Automatisieren Sie Antiviren-Scans und pflegen Sie die Antiviren-Audit-Protokolle für die betreffenden Systeme. (5.2)
- ☐ Stellen Sie sicher, dass ausschließlich Administratoren Antiviren-Systeme verändern oder deaktivieren können. (5.3)
- ☐ Dokumentieren Sie Methoden zum Schutz vor Malware. (5.4)

DON'T:

- ☐ Warten Sie mit der Identifizierung von Malware nicht, bis die verursachten Schäden offensichtlich werden.
  - o **Lösung:** Installieren Sie eine Software, die Verhaltensanomalien erkennt und die zuständigen Mitarbeiter bei Abweichungen benachrichtigt.

DSS-Anforderung 6

Entwickeln und Pflegen von sicheren Systemen und Applikationen

DO:

- ☐ Definieren Sie einen Prozess, um sich permanent zu aktuellen Sicherheitsschwachstellen auf dem Laufenden zu halten, Risiken einschätzen und den Bedrohungslevel definieren zu können. (6.1)
- ☐ Installieren Sie vom Hersteller bereitgestellte Sicherheits-Patches. (6.2.a)
- ☐ Dokumentieren Sie die Auswirkungen, Befugnisse und Bevollmächtigte, Funktionalitätsprüfungen sowie die Back-Out-Verfahren zur Änderungskontrolle. (6.4.5)
- ☐ Verwenden Sie nur strikte Entwicklungsprozesse und sichere Codierungsrichtlinien (gemäß der DSS-Definition) bei der betriebsinternen Entwicklung von Software. (6.3)

DON'T:

- ☐ Warten Sie nicht länger als einen Monat, um die vom Hersteller bereitgestellten Sicherheits-Patches für eine als kritisch identifizierte Risikoebene zu installieren. (6.2.b)
- ☐ Testen Sie betriebsinterne Software nicht in Ihrer Produktionsumgebung, verwenden Sie während den Tests keine Produktionsdaten und hinterlassen Sie keine Test-Konten/IDs nach der Softwarefreigabe. (6.3.1, 6.4.1, 6.4.3)

SCHUTZ VOR DER INTERNEN BEDROHUNGEN

DSS-Anforderung 7

Zugriff auf Karteninhaberinformationen gemäß geschäftlicher Erfordernisse einschränken

DO:

- ☐ Erstellen Sie eine Liste der Rollen mit Zugriff auf die CDE, einschließlich einer Definition aller Rollen, der jeweiligen Privilegienebene und der Berechtigungen, die alle Rollen benötigen, um korrekt zu funktionieren. (7.1, 7.3)
- ☐ Erarbeiten Sie eine Richtlinie auf der Basis der minimalen Rechtevergabe, und zwar für alle Mitarbeiter sowie eine Standard-Einstellung für „alle ablehnen“ (deny-all) für alle Einstellungen, die Zugriffskontrollen betreffen. (7.1.2, 7.2.3)
- ☐ Holen Sie sich eine dokumentierte Genehmigung der Bevollmächtigten für alle zu vergebenden Privilegien oder Änderungen der Privilegien innerhalb der CDE. (7.1.4)

DON’T:

- ☐ Vergeben Sie keine übermäßigen Berechtigungen (sozusagen „für alle Fälle“) für eine Rolle.
  - o **Lösung:** Verwenden Sie ein Modell der minimalen Rechtevergabe, in dem Berechtigungen nur erteilt werden, wenn sie geschäftlich erforderlich sind.
  - o **Lösung:** Gewähren Sie den Zugriff nur für genau den Zeitraum, für den er tatsächlich benötigt wird.

DSS-Anforderung 8

Identifizieren und Authentifizieren des Zugriffs auf Systemkomponenten

DO:

- ☐ Definieren und dokumentieren Sie Verfahren zur Benutzeridentifizierung und -authentifizierung für alle Systemkomponenten. (8.1, 8.4)
- ☐ Weisen Sie sämtlichen Benutzern einmalige IDs zu, testen Sie diese Privilegienkontrollen und beseitigen Sie den Zugriff von inaktiven/deaktivierten Benutzern. (8.1.1, 8.1.2, 8.1.3, 8.1.4)
- ☐ Überwachen Sie alle Konten, die von Anbietern und anderen Dritten verwendet werden, und deaktivieren Sie diese Konten, wenn sie nicht länger gebraucht werden. (8.1.5)
- ☐ Sperren Sie Benutzer-IDs nach sechs fehlgeschlagenen Zugriffsversuchen für 30 Minuten. (8.1.6, 8.1.7)
- ☐ Folgen Sie den Best-Practice-Empfehlungen der DSS für das Einrichten von Passwörtern, einschließlich des Erstellens starker Passwörter, dem Verschlüsseln von Zugangsdaten, der ID-Prüfung vor dem Zurücksetzen und einem Pflicht-Reset alle 90 Tage. (8.2.1, 8.2.2, 8.2.3, 8.2.4)
- ☐ Integrieren Sie eine Mehrfaktor-Authentifizierung für jeden Admin-Zugriff ohne Konsole sowie den Remote-Zugriff auf die CDE. (8.3)

DON'T:

- ☐ Verwenden Sie niemals das gleiche Passwort für mehrere Konten oder Geräte – sobald dieses Passwort kompromittiert ist, sind alle diese Konten/Geräte gefährdet.
- ☐ Teilen Sie keine IDs oder Authentifizierungsmethoden innerhalb der CDE. (8.5)

DSS-Anforderung 9

Beschränken des physischen Zugriffs auf Karteninhaberinformationen

DO: (sofern zutreffend)

- ☐ Dokumentieren Sie Prozesse für den physikalischen Zugriff auf CDE-Systeme. Erstellen Sie eine Liste aller Geräte, um den Zugriff auf die Rollen zu beschränken, die den Zugriff wirklich benötigen, und überwachen Sie alle Zugriffe mit Autorisierungs-Token. (9.1.1a, 9.1.1b, 9.2, 9.3, 9.9.1)
- ☐ Erstellen Sie eine Besucherautorisierung und Zugriffskontrollen, die sicherstellen, dass Besucher in allen Zugriffsbereichen bezüglich der CDE identifiziert, dokumentiert und überwacht werden. (9.4)
- ☐ Definieren Sie strikte Kontrollen für physische Medien innerhalb der Firma/der Organisation und verfolgen Sie ebenfalls nach, wenn diese Medien sich außerhalb des Unternehmens bewegen. Stellen Sie sicher, dass zerstörte Medien nicht wiederhergestellt werden können. (9.5, 9.6, 9.8)
- ☐ Schulen Sie die Aufmerksamkeit der Mitarbeiter um Externe zu identifizieren, die einen physikalischen Zugriff anfordern und um verdächtiges Verhalten zu identifizieren/zu melden. (9.9.2, 9.9.3)

SCHUTZ VOR ZU VIEL SELBSTZUFRIEDENHEIT

DSS-Anforderung 10

Nachverfolgen und Überwachen des Zugriffs auf Netzwerkressourcen und Karteninhaberinformationen

DO:

- ☐ Implementieren Sie Audit-Trails für alle Systeme, Meldungen bei verdächtigen Aktivitäten und einen Reaktionsplan, wenn Anomalien auftreten. (10.1, 10.2, 10.6.2.b)
- ☐ Verfolgen Sie alle Admin-Aktionen, Login-Versuche, Kontoänderungen und Unterbrechungen mittels des Audit-Trails nach. (10.2.3, 10.2.4, 10.2.5, 10.2.6)
- ☐ Stellen Sie sicher, dass das Audit-Protokoll die Benutzer-ID, Event-Art, Datum und Uhrzeit, Event-Erfolg oder -misserfolg, Ursprung des Events sowie die betroffenen Ressourcen erfasst. (10.3)
- ☐ Heben Sie alle Audit-Protokolle für mindestens ein Jahr auf, wobei die letzten drei Monate zur Auswertung verfügbar sein müssen. (10.7)
- ☐ Verhindern Sie die Manipulation von Audit-Trails und verwenden Sie Software zur Benachrichtigung bei Protokolländerungen. (10.5)
- ☐ Etablieren Sie einen Prozess zur täglichen Prüfung der CHD-Systemprotokolle sowie einen Prozess um Systemkomponenten zu überprüfen - basierend auf den Ergebnissen Ihrer Risikobewertung. (10.6.1, 10.6.2)

DON'T:

- ☐ Vergeben Sie keine Zugriffsrechte auf Protokolle ohne die entsprechende Legitimation für die Rolle. (10.5.1)
- ☐ Überprüfen Sie die täglichen Audit-Trails nicht manuell – das nimmt unnötig viel Zeit in Anspruch.
- ☐ Speichern Sie keine Audit-Protokolle für nach außen gerichtete Technologien auf diesen Maschinen – sie können kompromittiert werden. (10.5.4)

DSS-Anforderung 11

Regelmäßige Überprüfung der Sicherheitssysteme und Prozesse

DO:

- ☐ Dokumentieren Sie alle autorisierten drahtlosen Zugriffspunkte gemäß den geschäftlichen Erfordernissen. (11.1.1)
- ☐ Implementieren Sie Prozesse um autorisierte und nicht autorisierte drahtlose Zugangspunkte auf vierteljährlicher Basis zu testen und um gemäß den Ergebnissen reagieren zu können. (11.1, 11.1.2)
- ☐ Führen Sie interne (mit qualifiziertem Personal) und externe (mit zugelassenen Scanning-Anbietern) Schwachstellen-Scans durch. Diese Scans sollten vierteljährlich oder bei jeder relevanten Netzwerkänderung durchgeführt werden. Alle identifizierten Schwachstellen müssen korrigiert und ein erneuter Scan durchgeführt werden. (11.2)
- ☐ Führen Sie jährlich interne und externe Penetrationtests (mit qualifiziertem Personal oder mit Hilfe von Dritten) durch. Alle ermittelten Risiken müssen Sie beheben und anschließend einen erneuten Test durchführen. (11.3)
- ☐ Verwenden Sie ein Tool, das jede Änderung sofort erkennt, die zuständigen Mitarbeiter bei jeder unbefugt vorgenommenen Änderung an kritischen Systemen informiert und mindestens einmal pro Woche einen Dateiabgleich durchführt. (11.5)
- ☐ Dokumentieren Sie einen Prozess wie Sie auf Änderungsmeldungen reagieren. (11.5.1, 11.6)

DON'T:

- ☐ Verlassen Sie sich bei den Tests nicht auf das Minimum.
    - o **Lösung:** Führen Sie Prüfungen häufiger durch als es vorgeschrieben ist. So sind Sie in der Lage frühzeitig auf Bedrohungen zu reagieren, sogar bevor es zu Datenschutzvorfällen kommt.

DSS-Anforderung 12

Pflegen Sie eine Richtlinie, die sich mit der Informationssicherheit für alle Mitarbeiter befasst

DO:

- ☐ Veröffentlichen Sie eine jährlich geprüfte Sicherheitsrichtlinie, die alle CDE-kritischen Geräte und Dienste dokumentiert, den angemessenen Zugriff definiert (Rolle, Verwendung des Zugriffs und Standort) und die einen Prozess zur Risikoeinschätzung implementiert. (12.1, 12.2, 12.3, 12.4)
- ☐ Führen Sie jährlich Sicherheitsschulungen für alle Mitarbeiter durch, die auf die CDE zugreifen. (12.6)
- ☐ Weisen Sie Rollenverantwortungen zu, um Verfahren zu dokumentieren, Sicherheitsmeldungen zu analysieren, Konten zu verwalten und den Zugriff auf alle Daten zu überwachen. (12.5)
- ☐ Erstellen Sie eine Dokumentation der Serviceanbieter, einschließlich einer Liste der angebotenen Dienste, der Due-Diligence der Auswahl (inklusive Risikobewertung), einer Bestätigung des Serviceproviders zur Annahme der CHD-Verantwortlichkeit und einen Prozess um PCI DSS-Compliance durch die Anbieter zu gewährleisten. (12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5)
- ☐ Erstellen Sie einen jährlich zu überprüfenden Reaktionsplan bei auftretenden Systemverstößen. In diesem Plan sollten enthalten sein: die Aufgaben aller Rollen, spezielle Maßnahmen bei verschiedenen Bedrohungsarten/entsprechende Benachrichtigungen, die Behandlung kritischer Systeme und Backups sowie rechtliche Anforderungen an das Reporting und im Hinblick auf die Benachrichtigung der jeweiligen Kreditkartenanbieter. (12.10)