FIKTIVES UNTERNEHMEN

CREDITCARD SERVICE GMBH

1. EINFÜHRUNG

Die CreditCard Service GmbH entwickelt und betreibt eine Tokenization-Lösung. Hierbei können andere Unternehmen die Speicherung von Karteninhaberdaten an die CreditCard Service GmbH auslagern. Die dafür notwendige Software wird selbst vom Unternehmen entwickelt. Auch die notwendige IT-Infrastruktur wird selbst betrieben.

Die CreditCard Service GmbH bietet eine REST-API an, die über eine verschlüsselte Verbindung von den Kunden der CreditCard Service GmbH angesprochen werden kann. Die Kunden übermitteln dem Unternehmen Karteninhaberdaten, damit sie die vollständige PAN nicht selbst speichern müssen und damit die Umsetzung einiger Anforderungen des PCI DSS vermeiden können. Sie sparen damit Kosten und es ist für sie günstiger, die Speicherung an die CreditCard Service GmbH auszulagern. Sie erhalten für jede übermittelten Datensatz einen eindeutigen Token zurück, mit diesem sie die Zahlungsdaten später wieder abrufen können.

Somit sieht das Geschäftsmodell der CreditCard Service GmbH vor, die Speicherung von Karteninhaberdaten insbesondere der vollständigen Kreditkartenummer als externe Dienstleistung am Markt anzubieten. Dafür ist eine PCI DSS Zertifizierung notwendig.

Nachfolgend werden die vorhanden technischen und organisatorischen Maßnahmen aufgelistet, die von der CreditCard Service GmbH bisher umgesetzt wurden.

2. BÜRO

Die gesamte IT-Infrastruktur befindet sich in einem getrennt gesicherten Bereich mit einem zentralen digitalen Schließsystem innerhalb des Büros. Die gesamten Büroräume werden videoüberwacht und alle Besucher werden protokolliert. Alle Bewegungsdaten werden grundsätzlich 4 Monate vorgehalten. Die restlichen Büroräume können mit einem normalen Hausschlüssel geöffnet werden.

Alle Besucher müssen sich in einem Besucherlog einschreiben und bekommen danach einen Besucherausweis. In den gesicherten IT-Raum dürfen nur Mitarbeiter und in keinem Fall externe Besucher.

3. PERSONAL

Das Unternehmen wird von einer doppelten Geschäftsführung geleitet, die sich gleichzeitig um den Vertrieb kümmert. Unter der Führungsspitze gibt es drei Teams: „Buchhaltung und Sachbearbeitung“ mit 3 Vollzeit- und einer Teilzeitkraft, das Team „Software-Entwicklung“ mit 8 internen, 2 externen Software-Entwicklern und einem Werkstudenten. Im Team „IT-Administration“ sind drei Stellen geplant, von denen aber bisher noch eine unbesetzt ist. Neben der Geschäftsführung wurde aus jedem Team ein Teamleiter berufen. Die Teamfunktion des Admin-Teams ist zurzeit nicht besetzt.

Beim Auswahlprozess für neue Mitarbeiter wird ein sauberes Führungszeugnis vorausgesetzt, um keine Straftäter einzustellen, die bereits einen Kreditkartenbetrug oder -diebstahl begangen haben.

4. SECURITY MANAGEMENT

Der Teamleiter Softwareentwicklung wurde zum IT-Sicherheitsbeauftragten berufen. Dieser hat einen umfangreichen Leitfaden und mehrere Richtlinien zur IT-Sicherheit erstellt. Es existiert zusätzlich ein Risiko Management. Es werden dabei wöchentlich aktuelle Bedrohungen mit ihren potentiellen Auswirkungen identifiziert und bewertet.

Es existieren für alle Sicherheitsanforderungen Sicherheitsrichtlinien, die jährlich aktualisiert werden. Diese beinhalten alle umgesetzten Anforderungen. Diese Richtlinien müssen von jedem Mitarbeiter erstmalig bei seiner Einstellung und dann jährlich zur Kenntnis unterschrieben werden.

5. WEITERBILDUNGSMAßNAHMEN

Es sind keine expliziten externen Weiterbildungsmaßnahmen vorgeschrieben. Es findet nur On-the-job-Training stat. Allerdings erhalten die IT-Anwender eine IT-Schulung (bei der Einstellung und danach jährlich), dass z.B. sichere Passwörter zu verwenden sind und wie man sichere Passwörter erstellen kann. Bei dieser Gelegenheit wird auf sicherheitsrelevante Aspekte im Allgemeinen eingegangen.

6. PATCH MANAGEMENT

Es werden stets am ersten Werktag eines Monats überall Sicherheitsupdates eingespielt. Die korrekte Funktional aller Updates wird innerhalb eines von Produktion und Entwicklung getrenntem Testsystem nachvollzogen.

7. SOFTWARE-ENTWICKLUNG

Die Software zur Verarbeitung und Speicherung der Karteninformationen wird selbst entwickelt. Es existiert ein eigener Leitfaden zur sicheren Softwareentwicklung. Dieser enthält folgende Anforderungen an die Software bzw. an die Entwickler:

- Schutz gegen SQL Injections und Cross Site Scripting

- Validierung aller Eingabedaten-Parameter, die von extern kommen

- Keine Produktionsdaten in Test & Entwicklung

- Durchführung von stichprobenhaften Code Reviews

- Es dürfen keine Testdaten in Produktion gelangen

Um etwas Fortbildung zu ermöglichen, dürfen Entwickler gemeinsam den German OWASP Day besuchen.

8. SERVER-INFRASTRUKTUR

Es existieren zwei Standleitungen nach außen und jede Hardware wurde redundant ausgelegt. Es werden keine virtualisierten Server verwendet und jede Server erfüllt nur einen expliziten Zweck.

Die Netzwerkarchitektur wurde segmentiert und durch Firewalls maximal restriktiv getrennt. Die Webserver befinden sich dabei im gleichen Segment (DMZ) wie die Datenbanken, um aus Performancegründen den Traffic nicht über eine Firewall leiten zu müssen. Die Desktopcomputer befinden sich netzwerktechnisch in einem gesonderten DMZ-Segment. Von außen darf auf die beiden DMZ-Segmente zugegriffen werden. Ausgehende Verbindungen sind auch nur aus der DMZ erlaubt. In weiteren Segmenten stehen interne Dienste wie z.B. der Logserver. Diese Netzsegmente sind nicht von außen erreichbar und können auch nicht nach außen kommunizieren.

Die gesamte Systemlandschaft ist in einem jeweils aktuellen Diagramm festgehalten und vollständig dokumentiert, inklusive der restriktiven Berechtigungsstruktur.

Auf den Servers läuft als Betriebssystem Red Hat Enterprise Linux. Sie werden anhand der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik gehärtet. Es ist auf allen Systemen nur die jeweils notwendige Software installiert; zusätzlich sind überall noch C++-Compiler installiert, um bei Bedarf Software übersetzen zu können. Jede andere nicht notwendige Software wurde entfernt. Es werden grundsätzlich keine unsicheren Protokolle wie z.B. FTP verwendet.

Vor den Webanwendungen steht eine zentrale Web Application Firewall, die Warnmeldungen per E-Mail an die Administratoren verschickt. Die WAF nutzt das Core Rule Set von OWASP und läuft nicht im Enforcing-Modus.

Alle Server und Dienste erhalten eine genaue Zeitangabe von mehreren externen NTP-Servern, die von vertrauenswürdigen Non-Profit-Organisationen zur Verfügung gestellt werden. Eine eventuelle Manipulation der Zeiteinstellungen würde durch ein zentrales Monitoring-System identifiziert und alarmiert werden.

Es wird ein Tool verwendet, um die Prüfsummen von Binär- und Konfigurationsdateien sowie Logdateien auf den IT Systemen zu überwachen.

Es existiert ein IDS-System (Intrustion Detection System) am Übergang zwischen WAN und lokalem Netz. Dieses analysiert und überwacht den kompletten eingehenden und ausgehenden Datenverkehr. Es versendet E-Mails an die IT-Administration, falls es eine Auffälligkeit feststellt. Die Signaturdatenbank vom IDS wird täglich aktualisiert.

9. USER MANAGEMENT & PASSWÖRTER

Die Berechtigungen für die Nutzer werden von der IT-Administration definiert und vergeben. Diese versuchen im Allgemeinen so wenige Berechtigungen wie möglich zu erlauben. Jeder Nutzer erhält seinen eigenen eindeutigen Benutzernamen. Gruppenpasswörter werden von der IT-Administration nicht angelegt. Scheiden Mitarbeiter aus, werden je nach Auslastung 1-2 Wochen später die Zugänge gesperrt.

Die Nutzer sind per Policy angehalten nur sichere Passwörter zu verwenden, d.h. in diesem Fall mindestens 12 Zeichen lang. Die Nutzer müssen zwingend per Systemvorgabe alle 3 Monate ihr Passwort ändern. Ein neues Passwort darf nicht identisch sein mit den letzten 10 vorherigen Passwörtern. Alle Passwörter werden ausschließlich mit kryptographisch starken Hashverfahren gesichert abgelegt. Sollten Nutzer ein Passwort vergessen haben, müssen sie sich an die IT-Administration wenden.

Die IT-Systeme sind so eingestellt, dass sie nach 4 falschen Login-Versuchen einen Account für 1 Stunde sperren. Inaktive User werden überall automatisch nach 90 Tagen gesperrt. Alle IT-Systeme beenden die Nutzer-Session automatisch, wenn nach 120 Minuten keine weitere Interaktion vorgenommen wurde.

10. IT-ADMINISTRATION

Die Administratoren greifen auf die Systeme per SSH mit digitalen Schlüsseln als root zu. Die Anmeldung mit Passwörtern ist technisch unterbunden. Die Anmeldedaten werden an einen zentralen Logserver übermittelt. Nur Administratoren dürfen Änderungen an den Systemen und Deployments vornehmen; alle anderen verfügen nicht über die dafür notwendigen Berechtigungen.

Auf die Datenbanksysteme dürfen folglich auch nur die Administratoren zugreifen. Alle Aktivitäten dort werden von der Datenbank protokolliert.

11. ÜBERTRAGUNGS-VERSCHLÜSSELUNG

Zur Datenübertragung wird SSLv3 und TLS1.0 eingesetzt. Alle Karteninhaberdaten werden damit verschlüsselt über öffentliche Netzwerke übertragen.

12. SPEICHERUNG DER KARTENINHABERDATEN

Alle Karteninhaberdaten werden AES verschlüsselt mit 256bit im Modus CBC und danach in einer Datenbank gespeichert. Der Schlüssel liegt mit einem Passwort geschützt auf den Webserver. Innerhalb der Software wurde von den Entwicklern das geheime Passwort gespeichert. Der Schlüssel wird fest alle 2 Jahre ausgetauscht und alles wird re-verschlüsselt. Es werden keine Daten gelöscht, sondern maximal in der Datenbank diese als "nicht zur Verwendung freigegeben" markiert.

Es werden nie sensitive Authentifizierungsdaten wie z.B. die Prüfsumme gespeichert. Die CreditCard Service GmbH erhält nur folgende Daten von ihren Kunden zur Speicherung: Name, PAN, und das Ablaufdatum der Karte. Der Karteninhabername und Ablaufdatum wird im Klartext gespeichert. Die PAN wird zusätzlich zur Verschlüsselung auch als Hash zur eindeutigen Identifizierung des Datensatzes gespeichert. Es wird aus Gründen der Kompatibilität der Algorithmus MD5 verwendet.

Die PAN wird in keiner Anwendung vollständig angezeigt und nur wieder entschlüsselt, wenn der der Kunde diese PAN mit dem dazugehörigen Token anfordert.

Es existieren keine externen Medien oder Backups mit Kartendaten. Kartendaten auf andere Speichermedien zu übertragen ist per Policy verboten. Defekte Datenträger mit Karteninhaberdaten werden mit Gewalt (Vorschlaghammer) vernichtet und als Elektroschrott entsorgt.

13. DESKTOP-COMPUTER

Die Desktop-Computer sind nach Best Practice gesichert: Es sind stets aktuelle Virenscanner installiert, Personal Firewalls und die Benutzer besitzen keine Administrationsrechte. Die Virenscanner erkennen auch andere Schadsoftware und aktualisieren sich selbstständig täglich. Bei allen Vorgängen produzieren sie Loginformationen.

14. WIFI

Es existiert kein WIFI-Netz, dieses ist per Richtlinie verboten worden. Es werden keine Prüfungen durchgeführt, ob dieses auch eingehalten wird.

15. EXTERNE DIENSTLEISTER

Die CreditCard Service GmbH hat Dienstleistungsverträge mit einem Reinigungsunternehmen für ihre Büroräume und einem Vertrag mit einem Steuerberater für Jahresabschlüsse und Lohnabrechnung abgeschlossen. Zusätzlich wurde eine externe Kraft als Datenschutzbeauftragter berufen.

16. INCIDENT RESPONSE

Es existiert ein formales Incident Response Team, bestehend aus der Geschäftsführung. In der Praxis werden mögliche Incidents ausschließlich von der IT-Administration identifiziert und behandelt. Es existiert keine formalisierte Vorgehensweise im Incident-Fall, weil nach Erfahrung der CreditCard Service GmbH hier maximale Flexibilität erforderlich ist. Formal überwacht die IT-Administration 24/7 alle IT-Systeme und soll auf Incidents zeitnah und angemessen reagieren.

17. CHANGE MANAGEMENT

Alle Änderungen an der entwickelten Software und an IT-Systemen unterliegen einem Change Management. Alle Änderungen müssen vorab getestet und abgenommen werden. Alle eventuellen Default-Settings müssen auf sichere Einstellungen korrigiert werden. Bei jedem Change muss klar definiert werden, welche Auswirkungen dieser hat. Zusätzlich ist festzuhalten, wie man bei Fehlern wieder zu einem funktionierenden Zustand kommen kann.

Ein nachträglicher Review von Systemen oder Netzwerkkomponenten findet nicht statt.

18. SECURITY TESTING

Die IT-Infrastruktur wird monatlich mit dem Schwachstellen-Scanner Nessus auf Sicherheitslücken untersucht. Einmal im Quartal wird ein externer „PCI Scan“ von einem sehr günstigen Anbieter aus Indien durchgeführt, der nach Abschluss des kurzen Scans ein PDF-Zertifikat ausstellt.

Grundsätzlich werden alle Anwendungen und IT-Systeme einmal im Jahr einem Penetrationstest unterzogen. Dieser orientiert sich an den OWASP-Empfehlungen und wird mit einem Pentesting-Tool von einem Softwareentwickler ausgeführt, der zum CEH zertifiziert wurde. Hierbei werden die Pentests so oft wiederholt, bis keine Findings mehr offen sind. Diese Tests werden von extern und intern ausgeführt. Bei größeren Änderungen, die eine signifikante Auswirkung auf die Sicherheit haben könnte, wird zusätzlich ein Pentest durchgeführt.

19. ZIELSTELLUNG

Die CreditCard Service GmbH strebt die PCI DSS Zertifizierung an. Im vorliegenden Dokument wurden alle sicherheitsrelevanten Details bemerkt. Führe nun die CreditCard Service GmbH erfolgreich zum ersten PCI DSS Audit.