TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

Einhaltung der PCI-DSS-Anforderungen mit G DATA

G DATA Software AG | Dezember 2017

Einführung

Die Entwicklungen im Bereich Informationstechnologie haben massive Auswirkungen auf den Geschäftsbetrieb. Digitale Arbeitsplätze, vernetzte Point-of-Sale-Terminals und zentrale Kundendatenbanken bieten spürbare Verbesserungen für Konzerne, KMUs und ihre Kunden, wie z. B. eine hohe Effizienz und niedrige Kosten. Aber die Digitalisierung birgt auch Risiken. Obwohl vernetzte Geräte innovative Funktionalitäten ermöglichen, bieten sie Kriminellen auch die Chance, unerlaubten Zugriff auf interne Daten zu bekommen. Datendiebstahl wirkt sich unmittelbar auf die Kunden und den Geschäftsbetrieb aus und kann zu erheblichen finanziellen Schäden führen.

Um die Risiken von digitalen Abläufen rund um die Verarbeitung von Kreditkartendaten zu stemmen, haben die großen Kreditkartenherausgeber den Payment Card Industry Security Standards Council gegründet und eine Richtlinie für den Umgang mit Kreditkartendaten entwickelt. Alle Unternehmen, die Kreditkartendaten verarbeiten, müssen die Anforderungen des Payment Card Industry Data Security Standards (PCI DSS) einhalten und haften im Fall eines Datenverlusts. G DATA Lösungen unterstützen Unternehmen, die Kreditkartendaten schützen und die PCI-DSS-Anforderungen einhalten wollen. Dieses Whitepaper erklärt die Grundsätze des PCI-DSS-Standards und zeigt, wie Sie mit Hilfe von G DATA Lösungen den PCI-DSS-Anforderungen gerecht werden können.

1. PCI DSS

Die PCI-DSS-Richtlinie wurde in 2004 erstellt, indem die Gründer des PCI Security Standards Councils ihre bestehenden Datensicherheitsrichtlinien zusammenführten. Das Ziel ist der Schutz der Kontodaten von Kreditkarteninhabern. Der Standard definiert explizit ein minimales Anforderungsniveau: Unternehmen dürfen zusätzliche Maßnahmen implementieren um den Datenschutz weiter zu verbessern. Der Standard ersetzt keine Gesetze oder Vorschriften; die Anforderungen wurden zusätzlich zu den gesetzlichen Regelungen definiert.

1.1. Anwendungsbereich

Jedes Unternehmen, das Kreditkartendaten verarbeitet, ist von den Anforderungen des PCI-DSS-Standards betroffen. Zuerst müssen Unternehmen wissen, welche Datentypen vom Standard betroffen sind. PCI-DSS unterscheidet zwischen zwei Datentypen: Karteninhaberdaten und vertraulichen Authentifizierungsdaten. Karteninhaberdaten umfassen die Kreditkartennummer, den Namen des Kreditkarteninhabers, den Servicecode und das Ablaufdatum und dürfen gespeichert werden. Vertrauliche Authentifizierungsdaten dürfen dagegen nur verarbeitet aber nie gespeichert werden. Beide Datentypen unterliegen den PCI-DSS-Anforderungen.

Zweitens sollten Unternehmen alle Systeme, die Karteninhaberdaten verarbeiten (können) und deshalb dem PCI-DSS-Standard unterliegen, auflisten. Die Anforderungen treffen auf alle Systeme zu, die sich in der Karteninhaberdatenumgebung (Cardholder Data Environment, CDE) befinden oder mit dieser verbunden sind. Als Beispiele nennt der Standard Server (z. B. Web- oder Mail-Server), Netzwerkkomponenten wie Firewalls und Access-Points, Anwendungen und jede andere

Copyright © 2017 G DATA Software AG

Komponente und jedes andere Gerät, das mit der CDE verbunden ist. In der Praxis betrifft das oft die ganze IT-Infrastruktur von Unternehmen, die Kreditkartendaten verarbeiten. Damit unterliegt auch die ganze Infrastruktur den PCI-DSS-Anforderungen. Alternativ kann man die CDE verkleinern, indem man eine Netzwerksegmentierung implementiert und so den Teil des Netzwerks, in dem Karteninhaberdaten verarbeitet werden, vom Rest des Netzwerks trennt. Insbesondere beim Einsatz von WLAN-Netzwerkinfrastruktur kann die Struktur des Netzwerks einen starken Einfluss auf die Einhaltung der PCI-DSS-Anforderungen haben. Das muss beim Netzwerkentwurf entsprechend berücksichtigt werden.

Falls Karteninhaberdaten mit einem oder mehreren externen Dienstleistern ausgetauscht werden, trifft der PCI-DSS-Standard auch auf diese zu. Dies kann z. B. der Fall sein, wenn die Zahlungsabwicklung über einen externen Dienstleister läuft oder die Verwaltung von Unternehmenshardware oder –Software an einen Dienstleister übergeben wurde (z. B. Cloud-Provider).

1.2. Beurteilungsverfahren

Unternehmen, die sich im Geltungsbereich des PCI-DSS-Standards bewegen, müssen regelmäßig eine PCI-DSS-Beurteilung durchführen um ihre Konformität nachzuweisen. Die Untersuchungsparameter hängen vom Händlerniveau und Kreditkartenanbieter ab. Zum Beispiel: Ein Visa-Händler auf Niveau 4 (verarbeitet weniger als 20.000 Visa-Transaktionen pro Jahr) muss mindestens eine Konformitätsbescheinigung (Attestation of Compliance, AOC) abgeben und jährlich einen Selbstbewertungsfragebogen (Self-Assessment Questionnaire, SAQ) ausfüllen, um seine PCI-DSS-Konformität sicherzustellen. Größere Unternehmen müssen eine ausführlichere Dokumentation bereitstellen: Visa-Händler auf Niveau 1 (mehr als 6 Millionen Visa-Transaktionen) müssen, zusätzlich zum AOC-Formular, von einem zertifizierten Sicherheitsprüfer (Qualified Security Assessor, QSA) oder einem internen Prüfer einen Konformitätsbericht (Report on Compliance, ROC) erstellen lassen. Die Händlerniveaus unterscheiden sich je nach Kreditkartenanbieter, aber die AOC- und SAQ-Voraussetzungen sind allgemein gültig. Externe Dienstleister müssen auch ihre PCI-DSS-Konformität nachweisen, indem sie selbst eine Beurteilung ausführen, entweder jährlich oder nur auf Nachfrage von Kunden.

1.3. Struktur

Der Standard enthält sechs allgemeine Kategorien mit insgesamt zwölf Anforderungen, wobei jede Anforderung eine bestimmte Menge an individuellen Maßnahmen einschließt:

- Erstellung und Wartung sicherer Netzwerke und Systeme
    1. Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
    2. Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden
- Schutz von Karteninhaberdaten
    3. Schutz gespeicherter Karteninhaberdaten

Copyright © 2017 G DATA Software AG

4. Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze

- Unterhaltung eines Anfälligkeits-Managementprogramms
    5. Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen
    6. Entwicklung und Wartung sicherer Systeme und Anwendungen
- Implementierung starker Zugriffskontrollmaßnahmen
    7. Beschränkung des Zugriffs auf Karteninhaberdaten je nach betrieblichem Informationsbedarf
    8. Zugriff auf Systemkomponenten identifizieren und authentifizieren
    9. Physischen Zugriff auf Karteninhaberdaten beschränken
- Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken
    10. Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
    11. Regelmäßiges Testen der Sicherheitssysteme und -prozesse
- Befolgung einer Informationssicherheitsrichtlinie
    12. Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal

Jede Anforderung weist eine weitere Unterteilung in Unteranforderungen oder –maßnahmen auf, die von technischen Konfigurationsempfehlungen bis zu Richtlinien und Workflowimplementierungen reichen. Für jede Maßnahme bietet der Standard zusätzliche Informationen sowie Testabläufe, mit denen die Konformität nachgewiesen werden kann.

2. Einhaltung der PCI-DSS-Anforderungen mit G DATA

Die G DATA Businesslösungen unterstützen Unternehmen bei der fortwährenden Einhaltung der PCI-DSS-Anforderungen durch die Unterstützung von spezifischen Workflows und Richtlinien sowie die Implementierung von technischen Maßnahmen. Die Anforderungen einzuhalten ist keine Momentaufnahme, sondern ein Prozess: Änderungen an der Infrastruktur oder im Personalbestand können den Status beeinflussen. Mit Hilfe der Software von G DATA können Administratoren die initiale Einhaltung sicherstellen und den Status überwachen.

Die jeweiligen PCI-Maßnahmen stellen eine Mischung aus technischen Maßnahmen und Entscheidungen auf Verwaltungsebene dar. Nicht alle Maßnahmen können sinnvoll von Sicherheitssoftware unterstützt werden. Dieses Whitepaper beschreibt deshalb nur die Teile des PCI-DSS-Standards, bei denen G DATA unterstützen kann. Um den kompletten PCI-DSS-Standard einzuhalten und geeignete Maßnahmen zu implementieren, empfehlen wir, einen spezialisierten PCI-DSS-Berater zu beauftragen.

Anforderung 1: Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten

Die G DATA Client Security Business, Endpoint Protection Business und Managed Endpoint Security enthalten eine Firewall, die beim Sichern von Netzwerk-Endpoints behilflich ist (Anforderung 1.4). Die Firewall kann so konfiguriert werden, dass der Verkehr zur CDE auf das notwendige Minimum

Copyright © 2017 G DATA Software AG

eingeschränkt wird (Anforderung 1.2). Die Firewall schützt sowohl Desktops als auch Laptops, mit flexiblen Regeln für Geräte, die sowohl innerhalb als auch außerhalb des Firmennetzwerks verwendet werden. G DATA Lösungen können auch in einem DMZ-Szenario eingesetzt werden (Anforderung 1.3). Die Produktdokumentation bietet einen klaren Überblick über die Port- und Protokolleinstellungen, die für den Einsatz von G DATA Lösungen notwendig sind (Anforderung 1.1).

Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden

Für die Konfiguration der G DATA Lösungen steht ein umfangreiches Dashboard zur Verfügung. Mit Hilfe des Dashboards können Administratoren die Schutzeinstellungen schnell ihren Anforderungen entsprechend konfigurieren (Anforderung 2.1). Die klar gruppierten und dokumentierten Konfigurationsmodule bieten eine schnelle Übersicht mit Informationen, die Administratoren für die Überwachung von Sicherheitsrichtlinien und betrieblichen Verfahren brauchen (Anforderung 2.5). Die Lösungen unterstützen die Entwicklung von Konfigurationsstandards, indem sie verschiedenen Bereitstellungsszenarien sowie die Konfiguration von Maschinen auf Basis von Gruppeneinstellungen unterstützen (Anforderung 2.2). Durch die Integration mit bestehenden Active-Directory-Diensten sowie das ausführliche Hardware- und Softwareverzeichnis sind Administratoren immer über Komponenten, die möglicherweise in den Anwendungsbereich von PCI DSS fallen, informiert (Anforderung 2.4).

Anforderung 5: Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen

G DATA Lösungen bieten Endpoint-Schutz für eine umfangreiche Gruppe an Betriebssystemen an, inklusive Windows, Mac, Linux, Android und iOS (Anforderung 5.1). Administratoren können regelmäßige Updates und periodische Scans konfigurieren und Protokolle über eine leicht verständliche Konsole einsehen (Anforderung 5.2). Standardmäßig können Schutzkomponenten nicht von Endbenutzern deaktiviert werden. Sicherheitseinstellungen können nur auf dem Endpoint selbst konfiguriert werden, falls ein Administrator dies explizit erlaubt (Anforderung 5.3). Die Administrationskonsole bietet eine Übersicht von Einstellungen und Aufträgen und erleichtert so die Dokumentation von Sicherheitsrichtlinien und betrieblichen Verfahren. Darüber hinaus können Administratoren mit dem ReportManager-Modul maßgeschneiderte Berichte über den Security-Status und die Konfiguration erstellen (Anforderung 5.4).

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Die sechste Anforderung betrifft technische Schutzmaßnahmen und Richtlinien mit denen verhindert wird, dass Angreifer über Sicherheitslücken Systemzugriff erhalten können. Mit Hilfe von Beratungsdienstleistungen der G DATA Advanced Analytics GmbH kann ein Prozess für das Identifizieren von Sicherheitsschwachstellen etabliert werden (Anforderung 6.1). Mit dem Modul

Copyright © 2017 G DATA Software AG

Patch Management können Administratoren das Testen und Verteilen von Patches automatisieren, um bekannte Sicherheitslücken schnell und effizient zu schließen (Anforderung 6.2).

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach betrieblichem Informationsbedarf

Mit Hilfe des PolicyManager-Moduls der G DATA Endpoint Protection Business und Managed Endpoint Security können Administratoren umfassende Richtlinien und technische Maßnahmen für Zugangskontrolle umsetzen. Zum Beispiel: Mit der Applikationskontrolle kann Zugriff auf bestimmte Anwendungen auf eine Gruppe von Mitarbeitern, die den Zugriff für ihre Aufgaben brauchen, beschränkt werden (Anforderungen 7.1 und 7.2). Das integrierte Dashboard der G DATA Lösungen unterstützt die Dokumentation von Maßnahmen der Zugriffskontrolle.

Anforderung 8: Zugriff auf Systemkomponenten identifizieren und authentifizieren

Die Benutzerverwaltung der G DATA Lösungen basiert sich auf Windows-Logindaten, was eine feingranulare, kennwortbasierte Verwaltung erlaubt (Anforderungen 8.1 und 8.2). Alternativ kann auch ein integriertes Authentifizierungssystem verwendet werden.

Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten

Die Überwachung von Ereignissen in der Infrastruktur wird vom Modul G DATA Network Monitoring ermöglicht. Das Network Monitoring überwacht eine Vielzahl an Statistiken über Infrastrukturkomponenten, wie z. B. CPU-Last, Netzwerkverkehr oder aufgehängte Prozesse, um Administratoren bei der Identifikation von verdächtigen Aktivitäten zu unterstützen (Anforderung 10.6). Die Komponenten der Endpoint-Schutzschichten bieten ausführliche Protokolle, die für eine sofortige Analyse bereitstehen (Anforderung 10.7).

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

Ähnlich wie beim Aufdecken von verdächtigen Aktivitäten kann das Network Monitoring auch eingesetzt werden um SNMP-Monitoring-Maßnahmen umzusetzen, um so die Netzwerkinfrastruktur zu überwachen (Anforderungen 11.1 und 11.4). Weitere Tests, wie z. B. Schwachstellenscans oder Penetrationstests können bei der G DATA Advanced Analytics GmbH beauftragt werden (Anforderungen 11.2 und 11.3). Es ist ebenfalls möglich Änderungen an Einstellungen der G DATA Lösungen nachzuverfolgen (Anforderung 11.5).

Dieses Paper ersetzt keine professionelle juristische Beratung.

Copyright © 2017 G DATA Software AG