

# Informationsnachtrag: Anwendungsprüfungen und Web-Anwendungs-Firewalls - Klärung

**Standard:** PCI Datensicherheitsstandard (PCI DSS)

**Version:** 1.2

**Datum:** Oktober 2008

**Anforderung:** 6.6

**Autor:** PCI Security Standards Council

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 6.6 des PCI Datensicherheitsstandards (DSS).

2

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 6.6  
Codeprüfungen und Anwendungs-Firewalls

## Allgemeines

PCI DSS-Anforderung 6.6 umfasst zwei Optionen, um gängige Bedrohungen für die Daten von Karteninhabern anzugehen und sicherzustellen, dass Eingaben in ausgeführten Web-Anwendungen aus unsicheren Umgebungen gründlich geprüft werden. „Ausgeführt“ bedeutet in diesem Kontext, dass die

Anwendung in einer Betriebsumgebung, einschließlich Produktions- oder Akzeptanztest-/Vorproduktionsumgebungen mit zugehörigen strengen Prozessen zur Änderungskontrolle, bereitgestellt wurde. Die Details zur Erfüllung dieser Anforderung variieren je nach der Implementierung zur Unterstützung einer Anwendung.

Forensische Analysen von Gefahren für die Daten von Karteninhabern haben gezeigt, dass häufig Web-Anwendungen

der Ausgangspunkt von Angriffen auf diese Daten sind (vor allem über SQL Injection).

Mit Anforderung 6.6 soll sichergestellt werden, dass Web-Anwendungen im öffentlichen Internet während ihrer Ausführung und bei der Annahme von Eingaben vor den gängigsten Formen von Bedrohungen

geschützt sind. Zu den Schwachstellen von Web-Anwendungen existieren zahlreiche öffentlich zugängliche Informationen. Die zu beachtenden allgemeinen Punkte sind in Anforderung 6.5 aufgeführt. (Zusätzliche Referenzmaterialien zum Test von Web-Anwendungen finden Sie im Abschnitt „Weitere Informationsquellen“.)

Der beste mehrstufige Schutz würde durch die korrekte Implementierung beider in Anforderung 6.6 aufgeführten Optionen gewährleistet werden. PCI SSC ist bewusst, dass die Kosten und die betriebliche

Komplexität der Bereitstellung beider Optionen eine Umsetzung verhindern. Es sollte jedoch möglich sein,

mindestens eine der in diesem Dokument beschriebenen Alternativen anzuwenden. Eine korrekte Implementierung kann zudem der Absicht der Anforderung entsprechen.

Dieses Dokument enthält unterstützende Informationen zur Ermittlung der besten Option. Diese kann

je nach den verwendeten Produkten, der Beschaffung oder Bereitstellung von Web-Anwendungen und anderen Faktoren in der Umgebung variieren.

## Anforderung 6.6 Option 1: Schwachstellen von Web-Anwendungen

### Sicherheitsbeurteilung

In Anbetracht der Tatsache, dass das Ziel der Anforderung 6.6 darin besteht, die Nutzung

bekannter Schwachstellen (z. B. die in Anforderung 6.5 aufgeführten) zu verhindern, können mehrere mögliche Lösungen in Betracht gezogen werden. Diese sind dynamisch und proaktiv und erfordern die spezielle

Einleitung eines manuellen oder automatischen Prozesses. Bei korrekter Implementierung können diese Alternativen

der Absicht von Anforderung 6.6 entsprechen und einen Mindestschutz vor gängigen Bedrohungen für Web-Anwendungen bieten:

1. Manuelle Bewertung der Web-Anwendungssicherheit
2. Korrekte Nutzung automatischer Tools zur Bewertung der Web-Anwendungssicherheit (Scanning)

Diese Optionen müssen so ausgelegt sein, dass das Vorhandensein von Schwachstellen in Web-Anwendungen gemäß

den Ausführungen unter „Allgemeines“ geprüft werden kann. Beachten Sie, dass bei einer Schwachstellenbewertung lediglich die

bekanntesten Schwachstellen ermittelt und gemeldet werden. Bei einem Durchdringungstest wird hingegen versucht,

Schwachstellen zu nutzen, um zu ermitteln, ob unbefugter Zugriff oder andere böswillige Aktivitäten

möglich sind.

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 6.6 des PCI Datensicherheitsstandards (DSS).

3

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 6.6  
Codeprüfungen und Anwendungs-Firewalls

Bewertungen können durch eine qualifizierte interne Ressource oder durch Dritte erfolgen.

In allen Fällen muss die betreffende Person über die entsprechenden Fähigkeiten und Erfahrungen verfügen, um

die Web-Anwendung zu verstehen. Außerdem ist ein gewisses Know-how zur Evaluierung der Schwachstellen und zum Verständnis der

Ergebnisse erforderlich. Personen, die automatische Tools verwenden, müssen über die erforderlichen Kenntnisse und das Wissen verfügen, um

die Tools und die Testumgebung korrekt zu konfigurieren und die Ergebnisse zu evaluieren.

Werden interne Ressourcen verwendet, dürfen diese nicht mit dem

Management der zu testenden Anwendung betraut sein. So darf z. B. das Entwicklungsteam der Web-Anwendung nicht die abschließende Sicherheitsbewertung durchführen.

Bei korrekter Durchführung kann eine Bewertung der Web-Anwendungssicherheit den gleichen (oder besseren) Schutz wie eine Web-Anwendungs-Firewall bieten, wenn

Schwachstellen

gefunden und korrigiert werden, bevor die Anwendung dem öffentlichen Internet ausgesetzt wird.

Im Rahmen der Bewertung können ein manueller Prozess oder spezielle Tools genutzt werden, um

eine Web-Anwendung bei ihrer Ausführung auf das Vorhandensein bekannter Schwachstellen und Defekte zu prüfen. Dieser Ansatz

umfasst die Erstellung und Übermittlung böswilliger oder vom Standard abweichender Eingaben an die Anwendung, mit denen ein

Angriff simuliert wird. Die Reaktionen hierauf werden auf Anzeichen dafür geprüft, ob die Anwendung unzureichend gegen bestimmte Angriffe geschützt ist.

Die Bewertung einer Anwendung in einer Produktionsumgebung bietet die besten Testergebnisse, da diese Umgebung am anfälligsten für Angriffe ist. Eine Durchführung dieser

Bewertungen in einem Produktionssystem kann jedoch ein inakzeptables Betriebsrisiko darstellen.

Die Bewertungen können in den SDLC (Software Development Life Cycle) aufgenommen und vor der Bereitstellung der Anwendung in der Produktionsumgebung durchgeführt werden, wenn

strenge Richtlinien und Verfahren zur Änderungskontrolle sicherstellen, dass die ausgeführte Anwendung, die

in der Akzeptanztest-/Vorproduktionsumgebung bewertet wird, sich nicht von der in der Produktionsumgebung bereitgestellten unterscheiden kann.  
Der SDLC muss gemäß Anforderung 6.3 durchgängige Informationssicherheit umfassen. Prozesse zur Änderungskontrolle müssen sicherstellen, dass Softwareentwickler nicht in der Lage sind, den Bewertungsschritt zu umgehen und die neue Software direkt in der Produktionsumgebung bereitzustellen.  
Prozesse zur Änderungskontrolle müssen außerdem die Korrektur und das erneute Testen von Schwachstellen vor der Implementierung umfassen.  
Während die abschließende Freigabe der Bewertung durch eine unabhängige interne Organisation erfolgen muss, wird empfohlen, dass den Softwareentwicklern Tools zur Integration in die Entwicklungsumgebung zur Verfügung gestellt werden, sofern dies praktikabel ist.  
Dadurch können Schwachstellen so früh wie möglich im Entwicklungsprozess erkannt und korrigiert werden.  
Prüfen Sie unbedingt, ob diese Tools Tests der gängigen Web-Anwendungsschwachstellen vornehmen können, bevor sie diese gemäß Anforderung 6.6 einsetzen.  
Außerdem müssen sich im Hinblick auf neue und zukünftige Bedrohungen neue Analyseregeln in die Tools integrieren lassen. Personen, die Bewertungen vornehmen, müssen sich fortlaufend über Branchenentwicklungen informieren, um sicherzustellen, dass ihre Evaluierungs- oder Testkenntnisse neue Schwachstellen berücksichtigen.

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 6.6 des PCI Datensicherheitsstandards (DSS).

4

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 6.6 Codeprüfungen und Anwendungs-Firewalls

## **Anforderung 6.6 Option 2: Web-Anwendungs-Firewalls**

Eine Web-Anwendungs-Firewall (WAF) stellt einen Punkt zur Durchsetzung von Sicherheitsrichtlinien zwischen einer Web-Anwendung und dem Client-Endpunkt dar. Diese Funktionalität kann in Software oder Hardware implementiert, in einem Appliance-Gerät oder in einem typischen Server mit einem gängigen Betriebssystem ausgeführt werden. Es kann sich um ein eigenständiges Gerät oder um ein in andere Netzwerkkomponenten integriertes System handeln.  
Typische Netzwerk-Firewalls werden am Netzwerkrand oder zwischen Netzwerksegmenten (Zonen) implementiert und stellen die erste Verteidigungslinie gegen zahlreiche Arten von Angriffen dar. Sie müssen jedoch zulassen, dass Mitteilungen jene Anwendungen erreichen, die von einem Unternehmen für das öffentliche Internet definiert wurden. Netzwerk-Firewalls verfügen in der Regel nicht über die Möglichkeit, jene Teile einer IP-Mitteilung (IP-Pakete) zu prüfen, zu evaluieren und zu verarbeiten, die von Web-Anwendungen verwendet werden. Daher empfangen öffentliche Anwendungen häufig ungeprüfte Daten. Aus diesem Grund wird ein neuer, logischer Sicherheitsbereich geschaffen (die Web-Anwendung selbst). Sicherheits-„Best Practices“ rufen beim Wechsel von einem unsicheren in einen sicheren Bereich die zu prüfenden Mitteilungen auf. Web-Anwendungen sind zahlreichen bekannten Angriffsarten ausgesetzt. Wie wir alle wissen, sind die Anwendungen nicht immer darauf ausgelegt, diesen Angriffen standzuhalten. Dieses Risiko wird durch die Verfügbarkeit der Anwendungen für alle Personen mit einer Internet-Verbindung weiter vergrößert.  
Die Struktur der IP-Pakete entspricht einem Stufenmodell. Hierbei enthält jede Ebene definierte Informationen, die von bestimmten Netzwerkknoten oder Komponenten (physisch oder

softwarebasiert) für den Informationsfluss durch das Internet/Intranet geprüft werden. Die Ebene mit den Inhalten, die von der Anwendung verarbeitet werden, wird als „Anwendungsebene“ bezeichnet.

WAFs prüfen den Inhalt der Anwendungsebene eines IP-Pakets sowie den Inhalt weiterer Ebenen, die für einen Angriff auf eine Web-Anwendung verwendet werden könnten. Beachten

Sie jedoch, dass Anforderung 6.6 nicht auf die Einführung redundanter Kontrollen abzielt. Inhalte von IP-Paketen, die von Netzwerk-Firewalls, Proxys oder anderen Komponenten angemessen geprüft werden (d. h. durch geeignete Schutzmaßnahmen), müssen von einer WAF nicht erneut geprüft werden.

WAF-Technologie wird zunehmend in Lösungen integriert, die auch andere Funktionen wie Paketfilterung, Proxying, SSL-Terminierung, Lastausgleich, Objektpufferung usw. enthalten. Diese Geräte werden verschiedentlich als „Firewalls“, „Anwendungs-Gateways“, „Anwendungs-Bereitstellungssystem“, „Sicherer Proxy“ o. ä. bezeichnet. Sie müssen die Möglichkeiten der Datenprüfung dieser Produkte kennen, um ermitteln zu können, ob das betreffende Produkt den Absichten von Anforderung 6.6 entspricht.

Beachten Sie, dass die Konformität allein durch die Implementierung eines Produkts mit den hier beschriebenen Fähigkeiten nicht sichergestellt wird. Die korrekte Positionierung, Konfiguration, Administration und Überwachung ist ebenfalls ein wichtiger Aspekt einer konformen Lösung. Die Implementierung einer WAF ist eine

Option zur Erfüllung der Anforderung 6.6 und macht einen sicheren Softwareentwicklungsprozess (Anforderung 6.3) nicht überflüssig.

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 6.6 des PCI Datensicherheitsstandards (DSS).

5

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 6.6 Codeprüfungen und Anwendungs-Firewalls

## **Empfohlene Fähigkeiten**

Die Firewall einer Web-Anwendung sollte zu Folgendem in der Lage sein:

- Erfüllen aller betreffenden PCI DSS-Anforderungen zu Systemkomponenten in der Datenumgebung des Karteninhabers.
- Angemessene Reaktion (definiert durch geltende Richtlinien oder Regeln) auf Bedrohungen für die relevanten

Schwachstellen, mindestens gemäß OWASP Top Ten und/oder PCI DSS-Anforderung 6.5.

- Prüfen der Web-Anwendungseingaben und Reaktion (Freigabe, Blockierung und/oder Alarmierung) auf Basis

aktiver Richtlinien oder Regeln mit entsprechender Protokollierung der Maßnahmen.

- Verhindern von Datenlecks, d. h. die Fähigkeit zur Prüfung der Ausgaben von Web-Anwendungen

und zur Reaktion (Freigabe, Blockierung, Maskierung und/oder Alarmierung) je nach aktiven Richtlinien

oder Regeln mit entsprechender Protokollierung der Maßnahmen.

- Durchsetzen positiver und negativer Sicherheitsmodelle. Das positive Modell („Weiße Liste“) definiert akzeptables, zulässiges Verhalten, Eingaben, Datenbereiche usw. und weist alles andere ab. Das negative Modell („Schwarze Liste“) definiert, was NICHT zulässig ist.

Meldungen, die diesen Signaturen entsprechen, werden blockiert. Datenverkehr, der diesen Signaturen nicht entspricht, wird weitergeleitet.

- Prüfen von Web-Seiten-Inhalten, wie z. B. Hypertext Markup Language (HTML), Dynamic HTML (DHTML) und Cascading Style Sheets (CSS) sowie der zugrunde liegenden Protokolle, die Inhalte transportieren: Hypertext Transport Protocol (HTTP) und Hypertext Transport Protocol über SSL (HTTPS). (Neben

SSL umfasst HTTPS auch das Hypertext Transport Protocol über TLS.)

Prüfen der Meldungen von Web-Diensten, wenn diese Kontakt mit dem öffentlichen Internet haben. Hierzu zählt in der Regel das Simple Object Access Protocol (SOAP) und eXtensible Markup Language (XML), dokument- und RPC-orientierte Modelle sowie HTTP.

Prüfen aller Protokolle (proprietär oder standardisiert) bzw. Datenkonstrukte (proprietär oder standardisiert), die für die Übertragung von Daten zu oder von einer Web-Anwendung verwendet werden, sowie von Protokollen oder Daten, die ansonsten an keiner anderen Stelle geprüft werden.

*Hinweis: Proprietäre Protokolle stellen aktuelle Web-Anwendungs-Firewall-Produkte vor Herausforderungen, die eventuell individuelle Änderungen erforderlich machen. Entsprechen die Meldungen einer Anwendung*

*nicht den Standardprotokollen und Datenkonstrukten, kann die Prüfung der Daten durch eine Web-Anwendungs-Firewall u. U. nicht sinnvoll sein. In diesen Fällen ist die Implementierung der Schwachstellenbewertung von Anforderung 6.6 ggf. die bessere Wahl.*

Abwehren von Bedrohungen für die WAF selbst.

Unterstützung von SSL- und/oder TLS-Terminierung oder Positionierung in einer Weise, dass verschlüsselte

Übertragungen vor der Prüfung durch die WAF entschlüsselt werden. Verschlüsselte Datenströme können nicht geprüft werden, sofern SSL nicht vor der Prüf-Engine deaktiviert wird.

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 6.6 des PCI Datensicherheitsstandards (DSS).

6

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 6.6 Codeprüfungen und Anwendungs-Firewalls

## **Weitere empfohlene Fähigkeiten für bestimmte Umgebungen**

Verhindern und/oder Erkennen von Manipulationen an Sitzungs-Tokens, z. B. durch Verschlüsseln

von Sitzungs-Cookies, verborgene Formularfelder oder Datenelemente, die zum Erhalt des Sitzungsstatus dienen.

Automatisches Empfangen und Anwenden dynamischer Signaturaktualisierungen von einem Anbieter oder

einer anderen Quelle. Ist diese Fähigkeit nicht vorhanden, müssen Verfahren zur Verfügung stehen,

die für häufige Aktualisierungen von WAF-Signaturen oder anderen Konfigurationseinstellungen sorgen.

Falsches Öffnen (ein fehlerhaftes Gerät lässt nicht geprüften Datenverkehr durch) oder falsches Schließen (ein fehlerhaftes Gerät blockiert den Datenverkehr), je nach aktiver Richtlinie.

*Hinweis: Das Zulassen einer falschen WAF-Öffnung muss sorgfältig geprüft werden, da nicht geschützte Web-Anwendungen dem öffentlichen Internet ausgesetzt sind. Ein Umgehungsmodus,*

*bei dem keine Modifikationen am weitergeleiteten Datenverkehr möglich sind, kann unter bestimmten Umständen sinnvoll sein. (Auch bei falscher Öffnung fügen einige WAFs Verfolgungskopfzeilen hinzu, bereinigen HTML-Code, den sie als risikoreich ansehen oder führen andere Aktionen aus. Dies kann die Fehlerbehebung beeinträchtigen.)*

In bestimmten Umgebungen muss die WAF Secure Sockets Layer (SSL) Client-Zertifikate und Proxying Client-Authentifizierung über Zertifikate unterstützen. Viele moderne

Web-Anwendungen verwenden Client SSL-Zertifikate zur Identifikation von Anwendern. Ohne diese

Unterstützung können diese Anwendungen nicht hinter einer Web-Anwendungs-Firewall betrieben werden.

Viele moderne Anwendungs-Firewalls lassen sich in das Lightweight Directory Access Protocol (LDAP) oder andere Anwenderverzeichnisse integrieren und können sogar die erste

Authentifizierung für die zugrunde liegende Anwendung übernehmen.

Einige E-Commerce-Anwendungen erfordern ggf. die Unterstützung der Speicherung von FIPS-Hardwareschlüsseln. Ist

dies in Ihrer Umgebung der Fall, stellen Sie sicher, dass der WAF-Anbieter diese Anforderung in einem seiner Systeme unterstützt. Beachten Sie, dass dieses Merkmal die Kosten der Lösung ggf. erheblich steigert.

## **Weitere Aspekte**

Während WAFs Schutz vor zahlreichen Bedrohungen bieten können, bringen Sie auch technische

Probleme für eine Infrastruktur mit sich. Achten Sie auf die folgenden Probleme, die eine erfolgreiche Bereitstellung verhindern können:

Sites, die auf ungewöhnlichen Kopfzeilen, URLs oder Cookies basieren, erfordern ggf. eine spezielle Anpassung.

WAFs setzen häufig Maximalgrößen für diese Komponenten durch. Darüber hinaus filtern die gesuchten Signaturen ggf. bestimmte Zeichenfolgen, die als gefährlich wahrgenommen werden,

aber tatsächlich für eine bestimmte Anwendung vollkommen in Ordnung sind.

Inhalte, die von HTML-/HTTP-RFCs abweichen oder auf andere Art „ungewöhnlich“ sind, können ebenfalls blockiert werden, wenn die Standardfilter nicht angepasst werden. Hierzu zählen

übergroße Datei-Uploads und Inhalte in

Fremdsprachen.

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 6.6 des PCI Datensicherheitsstandards (DSS).

7

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 6.6 Codeprüfungen und Anwendungs-Firewalls

DHTML, Asynchronous JavaScript and XML (AJAX) und andere dynamische Technologien erfordern ggf. spezielle Anpassungen, Tests und Optimierungen. Diese Anwendungen gehen u. U. davon aus, dass sie auf eine Art auf eine Website zugreifen können, die

von einer WAF als böswillig angesehen wird.

Anwendungen, die Informationen über die zugrunde liegende Netzwerksitzung (z. B. die IP-Adresse des Clients) benötigen, müssen ggf. angepasst werden, wenn die WAF als umgekehrter

Proxy funktioniert. Diese WAFs platzieren generell clientseitige Informationen in einem HTTP-Header,

den vorhandene Anwendungen u. U. nicht erwarten.

## **Wichtige Aspekte**

Die in diesem Dokument beschriebenen Bewertungen von Anwendungsschwachstellen müssen

vor der Implementierung der Anwendung in der Produktion durchgeführt werden.

Werden eine falsche WAF-Öffnung oder ein Umgebungsmodus in Betracht gezogen, müssen vor der Implementierung spezifische Verfahren

und Kriterien zur Definition dieser Modi mit einem höheren Risiko eingerichtet werden. Web-Anwendungen sind in diesen Modi

nicht geschützt. Lange Anwendungszeiträume werden nicht empfohlen.

Die Auswirkungen von Änderungen an der Web-Anwendungs-Firewall müssen hinsichtlich der möglichen

Folgen für relevante Web-Anwendungen und umgekehrt geprüft werden.

- Teilen Sie allen betroffenen Parteien im Unternehmen den zeitlichen Ablauf und den Umfang der Änderungen an der Produktions-Web-Anwendungs-Firewall mit.
- Beachten Sie alle Richtlinien und Verfahren, einschließlich Änderungskontrolle, Business Continuity und Disaster Recovery.
- Änderungen an der Produktionsumgebung müssen in einem überwachten Wartungsfenster erfolgen.

## **Weitere Informationsquellen**

Diese Liste dient als Einstieg für weitere Informationen zur Sicherheit von Web-Anwendungen.

- OWASP Top Ten
- OWASP Countermeasures Reference
- OWASP Application Security FAQ
- Build Security In (Dept. of Homeland Security, National Cyber Security Division)
- Web Application Vulnerability Scanners (National Institute of Standards and Technology)
- Web Application Firewall Evaluation Criteria (Web Application Security Consortium)

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 6.6 des PCI Datensicherheitsstandards (DSS).

8

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS) Anforderung 6.6 Codeprüfungen und Anwendungs-Firewalls

## **Informationen zum PCI Security Standards Council**

Das PCI Security Standards Council hat sich die Verbesserung der Sicherheit von Kundenkonten durch Förderung des Wissens und der Kenntnisse zum PCI Datensicherheitsstandard und zu anderen

Standards, die die Sicherheit von Zahlungsdaten erhöhen, zum Ziel gesetzt.

Das PCI Security Standards Council wurde von den großen Kreditkartenunternehmen

American Express, Discover Financial Services, JCB International, MasterCard

Worldwide und Visa Inc. gegründet. Es soll ein transparentes Forum schaffen, in dem alle

Teilnehmer

aktiv an der fortlaufenden Entwicklung, Erweiterung und Nutzung des

PCI Datensicherheitsstandards (DSS), der PIN Entry Device (PED)-Sicherheitsanforderungen und des

Payment Application Datensicherheitsstandards (PA-DSS) beteiligt sind. Händler, Banken, Verarbeitungsunternehmen und

Point-of-Sale-Anbieter werden ermutigt, als Unternehmen teilzunehmen.