



# Payment Card Industry Data Security Standard (PCI DSS)

---

**Verfahren für  
Sicherheitsscans**

---

**Version 1.1**

Veröffentlichung: September 2006

## Inhaltsverzeichnis

<i>Zweck</i> .....	1
<i>Einführung</i> .....	1
<i>Umfang von PCI-Sicherheitsscans</i> .....	1
<i>Scanverfahren</i> .....	2
<i>Erfüllungsbericht</i> .....	4
<i>Lesen und Auswerten von Berichten</i> .....	4
<i>Stufe 5</i> .....	5
<i>Stufe 4</i> .....	6
<i>Stufe 3</i> .....	6
<i>Stufe 2</i> .....	6
<i>Stufe 1</i> .....	6

## Zweck

Dieses Dokument dient zur Erläuterung von Zweck und Umfang des PCI (Payment Card Industry)-Sicherheitsscans für Händler und Dienstanbieter, die sich einem PCI-Sicherheitsscan unterziehen, um ihre Konformität mit dem PCI Data Security Standard (DSS) zu überprüfen. Es wird außerdem von Approved Scanning Vendors (ASV) verwendet, um Händlern und Dienstanbietern dabei zu helfen, den Umfang des PCI-Sicherheitsscans zu ermitteln.

## Einführung

Im PCI DSS werden die Sicherheitsanforderungen für Händler und Dienstanbieter aufgeführt, die Karteninhaberdaten speichern, verarbeiten und übermitteln. Um ihre Konformität mit dem PCI DSS nachzuweisen, müssen Händler und Dienstanbieter u. U. regelmäßige PCI-Sicherheitsscans nach den Vorgaben des jeweiligen Zahlkartenunternehmens durchführen.

PCI-Sicherheitsscans werden über das Internet von einem ASV durchgeführt. PCI-Sicherheitsscans sind ein unverzichtbares Werkzeug, das in Verbindung mit einem Programm zur Beseitigung von Sicherheitsrisiken verwendet werden sollte. Mithilfe der Scans können Sicherheitsrisiken und Fehlkonfigurationen von Websites, Anwendungen und IT-Infrastrukturen mit Internet-IP-Adressen ermittelt werden.

Die Ergebnisse des Scans bieten wertvolle Informationen zur Unterstützung von effizientem Patchmanagement und anderen Sicherheitsmaßnahmen, mit denen der Schutz vor Internetangriffen erhöht werden kann.

PCI-Sicherheitsscans können für alle Händler und Dienstanbieter mit Internet-IP-Adressen verwendet werden. Selbst wenn eine Entität keine Transaktionen über das Internet anbietet, können andere Dienste den Zugriff auf Systeme über das Internet ermöglichen. Einfache Funktionen wie E-Mail und Internetzugriff für Mitarbeiter ermöglichen den Zugriff auf das Netzwerk eines Unternehmens über das Internet. Diese scheinbar unbedeutenden eingehenden und ausgehenden Internetpfade stellen häufig Schwachstellen für die Systeme von Händlern und Dienstanbietern dar und können bei unzureichender Kontrolle Karteninhaberdaten verfügbar machen.

## Umfang von PCI-Sicherheitsscans

Laut Anforderung der PCI müssen alle Internet-IP-Adressen auf Sicherheitsrisiken gescannt werden. Wenn aktive IP-Adressen gefunden werden, die ursprünglich nicht vom Kunden angegeben wurden, muss der ASV gemeinsam mit dem Kunden bestimmen, ob diese IP-Adressen im Scanumfang enthalten sein sollten. In einigen Fällen verfügen Unternehmen über zahlreiche IP-Adressen, verwenden jedoch nur wenige davon für die

Annahme und Verarbeitung von Karten. Unter diesen Umständen können ASVs Händlern und Dienst Anbietern dabei behilflich sein, den für die PCI-Konformität angemessenen Scanumfang festzulegen. Im Allgemeinen kann der Umfang des PCI-Sicherheitsscans mithilfe der folgenden Segmentierungsverfahren verringert werden:

- Physische Trennung zwischen dem Segment zur Verarbeitung von Karteninhaberdaten und anderen Segmenten
- Angemessene logische Segmentierung zur Unterbindung des Datenverkehrs zwischen dem Segment bzw. Netzwerk zur Verarbeitung von Karteninhaberdaten und anderen Netzwerken oder Segmenten

Letztendlich sind Händler und Dienstanbieter für die Definition des Umfangs ihres PCI-Sicherheitsscans verantwortlich, können jedoch ASVs zurate ziehen. Kommt es zu einer Sicherheitsgefährdung von Kontodaten über eine IP-Adresse oder Komponente, die nicht im Scanumfang eingeschlossen war, trägt der Händler oder Dienstanbieter die Verantwortung.

## Scanverfahren

Um den Anforderungen für PCI-Sicherheitsscans zu entsprechen, müssen Händler und Dienstanbieter Websites oder IT-Infrastrukturen, die Internet-IP-Adressen enthalten, mithilfe der folgenden Verfahren scannen lassen:

1. Alle Scans sind von einem Approved Scanning Vendor (ASV) durchzuführen, der aus der Liste der zugelassenen ASVs des PCI Security Standards Council ausgewählt wird.

ASVs müssen Scans in Übereinstimmung mit den Prozeduren der technischen und betrieblichen Anforderungen für Approved Scanning Vendors („Technical and Operational Requirements for Approved Scanning Vendors, ASVs“) durchführen. Diese Prozeduren schreiben vor, dass der Scan keine Auswirkungen auf den normalen Betrieb der Kundenumgebung haben darf und der ASV die Kundenumgebung auf keinen Fall penetrieren oder ändern sollte.
2. Nach Anforderung 11.2 des PCI DSS sind vierteljährliche Scans durchzuführen.
3. Vor dem Scannen der Website und IT-Infrastruktur müssen Händler und Dienstanbieter dem ASV Folgendes bereitstellen:
  - eine Liste aller Internet-IP-Adressen bzw. IP-Adressbereiche
  - bei Verwendung von virtuellem, domänenbasiertem Hosting eine Liste aller zu scannenden Domänen
4. Der ASV muss anhand des vom Kunden bereitgestellten IP-Adressbereichs eine Netzwerksuche durchführen, um die aktiven IP-Adressen und Dienste zu ermitteln.

5. Zwischen dem Händler bzw. Dienstanbieter und dem ASV sind regelmäßige Scans aller aktiven IP-Adressen (oder ggf. Domänen) und Geräte vertraglich zu vereinbaren.
6. Der ASV muss alle Filtervorrichtungen scannen, z. B. Firewalls oder externe Router (sofern zur Datenverkehrsfilterung verwendet). Wenn eine Firewall oder ein Router zur Erstellung einer entmilitarisierten Zone (Demilitarized Zone, DMZ) verwendet wird, sind diese Vorrichtungen auf Sicherheitsrisiken zu scannen.
7. Der ASV muss alle Webserver scannen.

Mithilfe von Webservern können Internetbenutzer Webseiten aufrufen und mit Webhändlern interagieren. Da diese Server vollständig über das öffentliche Internet zugänglich sind, ist ein Scannen auf Sicherheitslücken von größter Wichtigkeit.
8. Der ASV muss ggf. die Anwendungsserver scannen.

Anwendungsserver dienen als Schnittstelle zwischen dem Webserver und den Back-End-Datenbanken und -Legacy-Systemen. Wenn Karteninhaber beispielsweise Kontonummern mit Händlern oder Dienstanbietern austauschen, stellt der Anwendungsserver die Funktionalität für den Transport der Daten über das sichere Netzwerk bereit. Die Sicherheitslücken dieser Server und ihrer Skripts werden von Hackern ausgenutzt, um sich Zugang zu internen Datenbanken zu verschaffen, in denen möglicherweise Kreditkartendaten gespeichert sind.

Einige Websitekonfigurationen schließen keine Anwendungsserver ein. Stattdessen ist der Webserver selbst so konfiguriert, dass er gleichzeitig als Anwendungsserver dient.
9. Der ASV muss DNS (Domain Name Service)-Server scannen.

DNS-Server lösen Internetadressen durch Übersetzung von Domännennamen in IP-Adressen auf. Händler oder Dienstanbieter können einen eigenen DNS-Server oder einen von ihrem Internetdienstanbieter (Internet Service Provider, ISP) angebotenen DNS-Dienst verwenden. Wenn die DNS-Server Sicherheitsrisiken aufweisen, können Hacker durch Spoofing über die Websites der Händler oder Dienstanbieter an Kreditkartendaten gelangen.
10. Der ASV muss Mailserver scannen.

Mailserver befinden sich in der Regel in der DMZ und können für Hackerangriffe anfällig sein. Sie spielen für die Aufrechterhaltung der allgemeinen Websitesicherheit eine entscheidende Rolle.
11. Der ASV muss virtuelle Hosts scannen.

In einer gemeinsamen Hostingumgebung ist es allgemein üblich, dass ein einzelner Server mehrere Websites hostet. In diesem Fall nutzt der Händler den Server gemeinsam mit den anderen Kunden des

Hostingunternehmens. Dies kann zur Ausnutzung der Website des Händlers durch andere Websites auf dem Server des Hosts führen.

Alle Händler mit gehosteten Websites müssen ihren Hostinganbieter anweisen, den gesamten Internet-IP-Adressbereich zu scannen und dessen Konformität nachzuweisen, während die Händler selbst die eigenen Domänen scannen müssen.

12. Der ASV muss drahtlose Zugriffspunkte in drahtlosen LANs (WLANs) scannen.

Die Verwendung von WLANs führt zu Datensicherheitsrisiken, die identifiziert und verringert werden müssen. Händler, Prozessoren, Gateways, Dienstanbieter und andere Entitäten müssen mit dem Internet verbundene drahtlose Komponenten scannen, um potenzielle Sicherheitsrisiken und Fehlkonfigurationen zu ermitteln.

13. Das Intrusion Detection System/Intrusion Prevention System (IDS/IPS) muss entsprechend konfiguriert werden, um die Ursprungs-IP-Adresse des ASV zu akzeptieren. Wenn dies nicht möglich ist, sollte der Scan von einem Standort aus durchgeführt werden, der eine Beeinträchtigung durch das IDS/IPS verhindert.

## Erfüllungsbericht

Händler und Dienstanbieter müssen die Anforderungen zur Erstellung von Erfüllungsberichten der einzelnen Zahlungskartenunternehmen befolgen, um sicherzustellen, dass diese den Konformitätsstatus der jeweiligen Entität bestätigen. Während alle Scanberichte ein einheitliches Format aufweisen müssen, sind die Ergebnisse gemäß den Anforderungen der einzelnen Zahlungskartenunternehmen einzureichen. Setzen Sie sich mit der Händlerbank in Verbindung oder überprüfen Sie die regionalen Websites der einzelnen Zahlungskartenunternehmen, um festzustellen, an wen die Ergebnisse gesendet werden sollen.

## Lesen und Auswerten von Berichten

Der vom ASV erstellte Bericht basiert auf den Ergebnissen des Netzwerkscans.

Der Scanbericht enthält eine Beschreibung der Art der Sicherheitslücke bzw. des Sicherheitsrisikos, eine Diagnose der damit verbundenen Probleme und Anleitungen zur Behebung bzw. Beseitigung der isolierten Sicherheitsrisiken. Den im Scanprozess ermittelten Sicherheitsrisiken wird im Bericht eine Bewertung zugewiesen.

Der ASV kann Berichte zu Sicherheitsrisiken individuell gestalten. Hohe Risiken werden jedoch auf einheitliche Weise gemeldet, um eine faire und

konsistente Konformitätsbewertung zu gewährleisten. Wenden Sie sich zur Auswertung Ihres Scanberichts an Ihren Anbieter.

Tabelle 1 gibt Aufschluss darüber, wie eine konforme Netzwerk-Scanlösung Sicherheitsrisiken kategorisieren kann. Sie zeigt außerdem die Sicherheitslücken und -risiken mit hohen Risikostufen.

Nur wenn ein Scan keine hohen Sicherheitsrisiken nachweist, gelten die Anforderungen als erfüllt. Der Scanbericht darf keine Sicherheitsrisiken enthalten, die auf Features oder Konfigurationen hinweisen, die gegen den PCI DSS verstoßen. Wenn solche Sicherheitsrisiken vorhanden sind, muss der ASV gemeinsam mit dem Kunden feststellen, ob es sich dabei tatsächlich um Verstöße gegen den PCI DSS handelt, und somit als Scanergebnis eine Nichterfüllung der Anforderungen des PCI DSS angeben.

Hohe Sicherheitsrisiken werden mit Stufe 3, 4 oder 5 klassifiziert.

<b>Stufe</b>	<b>Schweregrad</b>	<b>Beschreibung</b>
5	<b>Dringend</b>	Trojanische Pferde, unerlaubter Lese- und Schreibzugriff auf Dateien, Remoteausführung von Befehlen
4	<b>Kritisch</b>	Potenzielle Trojanische Pferde, unerlaubter Lesezugriff auf Dateien
3	<b>Hoch</b>	Beschränkter unerlaubter Lesezugriff, Durchsuchen von Verzeichnissen, DoS (Denial of Service)
2	<b>Mittel</b>	Vertrauliche Konfigurationsinformationen können von Hackern abgerufen werden
1	<b>Niedrig</b>	Informationen können bei der Konfiguration von Hackern abgerufen werden

Tabelle 1 – Stufen von Sicherheitsrisiken

## Stufe 5

Sicherheitsrisiken der Stufe 5 ermöglichen Angreifern von außen den Remotezugriff mit root- oder Administratorberechtigungen. Bei Sicherheitsrisiken dieser Stufe können Hacker den gesamten Host gefährden. Sicherheitsrisiken der 5. Stufe schließen Schwachstellen ein, über die sich Hacker vollständigen Lese-/Schreibzugriff auf das Dateisystem verschaffen und von außen root- oder Administratorbefehle ausführen können. Auch Backdoors und Trojanische Pferde fallen unter diese Kategorie.

## **Stufe 4**

Sicherheitsrisiken der Stufe 5 ermöglichen Eindringlingen den Remotezugriff, allerdings nur mit Benutzer- und nicht mit Administrator- oder root-Berechtigungen. Durch Sicherheitsrisiken der Stufe 4 erhalten Hacker teilweisen Zugriff auf Dateisysteme (z. B. vollen Lesezugriff, aber keinen vollen Schreibzugriff). Sicherheitsrisiken, durch die streng vertrauliche Informationen verfügbar gemacht werden, gelten als Sicherheitsrisiken der Stufe 4.

## **Stufe 3**

Bei Sicherheitsrisiken der Stufe 3 erhalten Hacker Zugriff auf bestimmte, auf dem Host gespeicherte Informationen, einschließlich Sicherheitseinstellungen. Diese Sicherheitsrisikostufe kann zu Missbrauch des Hosts durch Eindringlinge führen. Beispiele für Sicherheitsrisiken der Stufe 3 sind die teilweise Offenlegung von Dateiinhalten, der Zugriff auf bestimmte Dateien auf dem Host, das Durchsuchen von Verzeichnissen, die Offenlegung von Filterregeln und Sicherheitsmechanismen, die Verwundbarkeit durch Denial of Service (DoS)-Angriffe und die nicht autorisierte Verwendung von Diensten, z. B. der Weiterleitung von E-Mails.

## **Stufe 2**

Bei Sicherheitsrisiken der Stufe 2 werden einige vertrauliche Informationen vom Host verfügbar gemacht, z. B. die genauen Versionen von Diensten. Anhand dieser Informationen können Hacker potenzielle Angriffe auf den Host untersuchen.

## **Stufe 1**

Bei Sicherheitsrisiken der Stufe 1 werden Informationen, z. B. offene Anschlüsse, verfügbar gemacht.