Kaspersky® Endpoint Security

# PCI DSS v3.2 Mapping

PCI DSS 3.2 regelt verschiedene technische Sicherheitsanforderungen und Einstellungen für Systeme, die Kreditkartendaten verarbeiten. In den Unterpunkten 1.4, 2.4a, 3.4.1, 5.1, 5.1.1, 5.2, 5.3, 6.1, 6.2 des PCI DSS v3.2 sind strenge Regeln für Virenschutzprogramme auf Endpoints aufgeführt, die Daten von Kreditkartenkunden verarbeiten. Es ist gängige Praxis, wenn auch keine offizielle Regel, dass die Funktionen der Geräte- und Programmkontrolle beim Software-Audit nach PCI DSS berücksichtigt werden.

## 1.4

**ANFORDERUNGEN VON PCI DSS:**

Installation persönlicher Firewall-Software oder Software mit vergleichbarer Funktionalität auf allen tragbaren Computern, die außerhalb des Netzwerks eine Verbindung mit dem Internet herstellen und die auch für den Zugriff auf das CDE verwendet werden. Für Firewall- (oder gleichwertige) Konfigurationen gilt:

- Konkrete Konfigurationseinstellungen werden definiert.
- Die persönliche Firewall (oder gleichwertige Funktionalität) wird aktiv ausgeführt.
- Die persönliche Firewall (oder gleichwertige Funktionalität) kann nicht von den Benutzern der tragbaren Computer geändert werden.

**TESTVERFAHREN:**

**1.4.a** Überprüfen Sie Richtlinien und Konfigurationsstandards auf folgende Punkte:

- Persönliche Firewall-Software oder vergleichbare Funktionalität wird für alle tragbaren Computer benötigt, die außerhalb des Netzwerks eine Verbindung mit dem Internet herstellen und die auch für den Zugriff auf das CDE verwendet werden.
- Für die persönliche Firewall (oder vergleichbare Funktionalität) werden konkrete Konfigurationseinstellungen definiert.
- Die persönliche Firewall (oder gleichwertige Funktionalität) ist so konfiguriert, dass sie aktiv ausgeführt wird.
- Die persönliche Firewall (oder gleichwertige Funktionalität) ist so konfiguriert, dass sie nicht von den Benutzern der tragbaren Computer geändert werden kann.

**1.4.b** Untersuchen Sie eine Auswahl von Firmengeräten auf folgende Punkte:

- Die persönliche Firewall (oder gleichwertige Funktionalität) ist gemäß den unternehmensspezifischen Konfigurationseinstellungen installiert und konfiguriert.
- Die persönliche Firewall (oder gleichwertige Funktionalität) wird aktiv ausgeführt.
- Die persönliche Firewall (oder gleichwertige Funktionalität) kann nicht von den Benutzern der tragbaren Computer geändert werden.

**TIPP:**

Tragbare Computer, die von außerhalb der Unternehmens-Firewall eine Internetverbindung herstellen können, sind anfälliger für Internetbedrohungen. Die Verwendung von Firewall-Funktionen (z. B. persönliche Firewall-Software oder -Hardware) schützt Geräte vor Angriffen aus dem Internet, die ein Gerät nutzen könnten, um nach der erneuten Verbindung des Geräts mit dem Netzwerk auf die Systeme und Daten des Unternehmens zuzugreifen.

Die genauen Firewall-Konfigurationseinstellungen werden durch das Unternehmen festgelegt.

# 2.4a

**ANFORDERUNGEN VON PCI DSS**

Ein Inventar der Systemkomponenten führen, die für PCI DSS infrage kommen.

**TESTVERFAHREN**

**2.4.a** Überprüfen des Systeminventars, um sicherzustellen, dass eine Liste von Hardware- und Softwarekomponenten geführt wird, die eine Beschreibung der Funktion/Verwendung für jede Komponente enthält.

**TIPP**

Durch das Führen einer aktuellen Liste aller Systemkomponenten kann ein Unternehmen den Bereich für die Implementierung von PCI-DSS-Steuerungen präzise und effizient definieren. Ohne Inventarisierung könnten einige Systemkomponenten vergessen werden und versehentlich von den Konfigurationsstandards des Unternehmens ausgeschlossen werden.

# 3.4.1

**ANFORDERUNGEN VON PCI DSS**

Bei Verwendung von Festplattenverschlüsselung (anstelle einer Datenbankverschlüsselung auf Datei- oder Spaltenebene) muss der logische Zugriff separat und unabhängig von nativen Authentifizierungs- und Zugriffssteuerungsmechanismen des Betriebssystems verwaltet werden (z. B. durch den Verzicht auf lokale Benutzerkontodatenbanken oder allgemeine Anmeldedaten im Netzwerk). Entschlüsselungsschlüssel dürfen nicht mit Benutzerkonten verknüpft sein.

**TESTVERFAHREN**

**3.4.1.a** Wird Festplattenverschlüsselung verwendet, überprüfen Sie die Konfiguration, und achten Sie auf den Authentifizierungsprozess, um sicherzustellen, dass der logische Zugriff auf verschlüsselte Dateisysteme über einen vom Authentifizierungsmechanismus des nativen Betriebssystems getrennten Mechanismus erfolgt (z. B. keine lokalen Benutzerkontodatenbanken oder allgemeinen Anmeldedaten des Netzwerks).

**3.4.1.b** Beobachten Sie Abläufe, und befragen Sie Mitarbeiter, um sicherzustellen, dass kryptografische Schlüssel sicher aufbewahrt werden (z. B. auf Wechselmedien, die durch strenge Zugriffssteuerung ausreichend geschützt sind).

**3.4.1.c** Überprüfen Sie die Konfigurationen und Abläufe, um sicherzustellen, dass Karteninhaberdaten auf Wechseldatenträgern immer verschlüsselt gespeichert werden.

**TIPP**

Ziel dieser Anforderung ist es, Verschlüsselung auf Datenträgerebene zum vollständigen Schutz von Karteninhaberdaten in die Unternehmenskultur zu integrieren. Die Verschlüsselung auf Datenträgerebene verschlüsselt die gesamte Festplatte/Partition auf einem Computer und entschlüsselt die Informationen automatisch, wenn ein autorisierter Benutzer sie anfordert. Viele Festplatten-Verschlüsselungslösungen fangen Lese-/Schreibvorgänge des Betriebssystems ab und führen die entsprechenden kryptografischen Transformationen durch, ohne dass der Benutzer beim Systemstart oder zu Beginn einer Sitzung ein Passwort oder eine Passphrase eingeben muss. Anhand dieser Merkmale der Verschlüsselung auf Festplattenebene kann die Methode diese Anforderung nicht erfüllen, wenn:

- dieselbe Benutzerkontoauthentifizierung wie das Betriebssystem verwendet wird oder
- ein Schlüssel verwendet wird, der mit der lokalen Benutzerkontodatenbank des Systems oder allgemeinen Netzwerk-Anmeldedaten verknüpft ist oder daraus abgeleitet wurde.

Vollständige Datenträgerverschlüsselung hilft, Daten im Falle des physischen Verlustes einer Festplatte zu schützen und kann daher für tragbare Geräte geeignet sein, auf denen Karteninhaberdaten gespeichert werden.

# 5.1

ANFORDERUNGEN VON PCI DSS: Auf allen Systemen, die am häufigsten von schädlicher Software betroffen sind (insbesondere PCs und Server), muss eine Antiviren-Software installiert werden.

TESTVERFAHREN: Eine Stichprobe an Systemkomponenten aller Betriebssysteme, die am häufigsten von schädlicher Software betroffen sind, dahingehend überprüfen, dass eine Antiviren-Software installiert und Antiviren-Technologie vorhanden ist.

TIPP: Der Strom an Angriffen, die auf weit verbreiteten Exploits basieren (sogenannte „Zero Day-Angriffe", bei welchen eine zuvor unbekannte Sicherheitslücke genutzt wird) und auf Systeme abzielen, die ansonsten gut geschützt sind, steigt kontinuierlich an. Wenn keine Antiviren-Lösung vorhanden ist, die zudem regelmäßig aktualisiert wird, können diese neuen Formen von schädlicher Software Systeme angreifen, Netzwerke deaktivieren oder Daten kompromittieren.

# 5.1.1

ANFORDERUNGEN VON PCI DSS: Das Virenschutzprogramm muss alle bekannten Arten von schädlicher Software erkennen, entfernen und vor diesen schützen können.

TESTVERFAHREN: Die Dokumentation des Lieferanten ist zu überprüfen und die Virenschutzkonfiguration dahingehend zu prüfen, ob das Antiviren-Programm alle bekannten Typen von schädlicher Software erkennt, alle bekannten Typen von schädlicher Software entfernt und vor allen bekannten Typen von schädlicher Software schützt.

TIPP: Es ist wichtig, dass der Schutz für ALLE Arten und Formen von schädlicher Software gilt.

# 5.2

ANFORDERUNGEN VON PCI DSS: Alle Virenschutzmechanismen müssen auf dem neuesten Stand sein, es müssen regelmäßig Scans durchgeführt und Audit-Logs generiert werden, die in Übereinstimmung mit Anforderung 10.1 des PCI DSS aufbewahrt werden müssen.

TESTVERFAHREN:

**5.2.a** Richtlinien und Prozesse dahingehend überprüfen, dass die Antiviren-Software und die Definitionen stets auf dem neuesten Stand sein müssen.

**5.2.b** Die Virenschutzkonfiguration inklusive Masterinstallation der Software dahingehend überprüfen, dass die Virenschutzmechanismen zur Durchführung von automatischen Updates und regelmäßigen Scans konfiguriert sind.

5.2.c Eine Stichprobe an Systemkomponenten aller Betriebssysteme, die am häufigsten von schädlicher Software betroffen sind, dahingehend überprüfen, dass die Antiviren-Software und die Definitionen auf dem neuesten Stand sind und regelmäßig Scans durchgeführt werden.

**5.2.d** Die Virenschutzkonfiguration inklusive Masterinstallation der Software und eine Stichprobe an Systemkomponenten dahingehend überprüfen, dass die Log-Generierung der Antiviren-Software aktiviert ist und die Protokolle in Übereinstimmung mit Anforderung 10.1 des PCI DSS aufbewahrt werden.

TIPP: Auch die besten Antiviren-Lösungen sind weniger effektiv, wenn sie nicht gewartet und mithilfe aktueller Sicherheits-Updates, Signaturdateien oder Malware-Schutzmechanismen auf dem aktuellen Stand gehalten werden. Anhand der Audit-Logs können die Aktivitäten von Viren und Malware überwacht und Maßnahmen zum Schutz vor Malware ausgeführt werden. Es ist absolut erforderlich, dass die Antimalware-Lösung zur Generierung von Audit-Logs konfiguriert wird und diese Logs in Übereinstimmung mit Anforderung 10 verwaltet werden.

# 5.3

ANFORDERUNGEN VON PCI DSS:

Es muss sichergestellt sein, dass die Virenschutzmechanismen aktiv ausgeführt werden und vom Benutzer nicht deaktiviert oder verändert werden können, wenn dies nicht explizit durch das Management von Fall zu Fall für eine begrenzte Zeit genehmigt wurde.

TESTVERFAHREN:

**5.3.a** Die Virenschutz-Konfiguration inklusive Masterinstallation der Software und eine Stichprobe an Systemkomponenten dahingehend überprüfen, dass die Antiviren-Software aktiv ausgeführt wird.

**5.3.b** Die Virenschutz-Konfiguration inklusive Masterinstallation der Software und eine Stichprobe an Systemkomponenten dahingehend überprüfen, dass die Antiviren-Software vom Benutzer nicht deaktiviert oder geändert werden kann.

**5.3.c** Verantwortliches Personal befragen und Prozesse beobachten, um zu überprüfen, dass die Antiviren-Software nicht deaktiviert oder durch den Benutzer verändert werden kann, wenn dies nicht explizit durch das Management von Fall zu Fall für eine begrenzte Zeit genehmigt wurde.

TIPP:

Ein Virenschutzprogramm, das kontinuierlich ausgeführt wird und nicht verändert werden kann, bietet den besten Schutz vor Malware.

Mithilfe von richtlinienbasierten Kontrollen auf allen Systemen wird sichergestellt, dass der Malware-Schutz nicht verändert oder deaktiviert werden kann. So wird verhindert, dass Schwachstellen im System von schädlicher Software ausgenutzt werden.

Eventuell müssen für den Zeitraum, in welchem der Virenschutz nicht aktiv ist, weitere Sicherheitsmaßnahmen ergriffen werden (zum Beispiel Trennung des ungeschützten Systems vom Internet und Durchführung eines vollständigen Scans nach der Reaktivierung des Virenschutzes).

# 6.1

ANFORDERUNGEN VON PCI DSS:

Einen Prozess zur Identifizierung von Sicherheitsschwachstellen erstellen, bei dem seriöse externe Quellen für Informationen über Sicherheitsschwachstellen verwendet werden und eine Risiko-Rangliste (z. B. „hoch", „mittel" oder „niedrig") für neu erkannte Sicherheitsschwachstellen erstellt wird.

TESTVERFAHREN:

**6.1.a** Richtlinien und Verfahren überprüfen, um sicherzustellen, dass Prozesse für Folgendes definiert sind:

- Identifizierung neuer Sicherheitslücken
- Zuordnung einer Risiko-Rangliste für Schwachstellen, einschließlich der Identifizierung aller „risikoreichen" und „kritischen" Sicherheitslücken
- Nutzung seriöser externer Quellen zum Bezug von Informationen über Sicherheitslücken

**6.1.b** Personal befragen und Prozesse beobachten, um Folgendes sicherzustellen:

- Neue Sicherheitslücken werden erkannt.
- Schwachstellen werden einer Risiko-Rangliste zugeordnet, einschließlich der Identifizierung aller „risikoreichen" und „kritischen" Sicherheitslücken.
- Prozesse zur Identifizierung neuer Sicherheitslücken umfassen die Verwendung seriöser externer Quellen für Informationen über Sicherheitslücken.

TIPP:

Ziel dieser Anforderung ist, dass Unternehmen über neue Schwachstellen, die sich auf ihre Umgebung auswirken können, auf dem Laufenden gehalten werden.

Informationsquellen für Sicherheitslücken sollten vertrauenswürdig sein. Dazu gehören oft Hersteller-Websites, branchenspezifische News Groups, Mailinglisten oder RSS-Feeds.

Sobald ein Unternehmen eine Schwachstelle erkennt, die sich auf seine Umgebung auswirken könnte, muss das durch die Schwachstelle verursachte Risiko bewertet und klassifiziert werden. Das Unternehmen muss daher über eine Methode verfügen, um Schwachstellen kontinuierlich zu bewerten und ihnen Risikoklassifizierungen zuzuordnen. Dies wird nicht durch einen ASV- oder internen Schwachstellen-Scan erreicht, sondern erfordert, dass Informationen zu Schwachstellen aktiv von Quellen aus der Branche bezogen werden.

Die Einstufung der Risiken (z. B. als „hoch", „mittel" oder „niedrig") ermöglicht Unternehmen, die größten Risikofaktoren schneller zu identifizieren, zu priorisieren, zu eliminieren und so die Wahrscheinlichkeit zu verringern, dass die Schwachstellen mit dem höchsten Risiko ausgenutzt werden.

# 6.2

ANFORDERUNGEN VON PCI DSS:

Alle Systemkomponenten und Software müssen vor bekannten Sicherheitslücken geschützt werden, indem die vom Hersteller bereitgestellten Sicherheitspatches installiert werden. Sicherheitspatches müssen innerhalb eines Monats nach Veröffentlichung installiert werden.

**Hinweis:** Kritische Sicherheitspatches müssen gemäß der Risikoeinstufung in Anforderung 6.1 identifiziert werden.

TESTVERFAHREN:

**6.2.a** Richtlinien und Prozesse zur Installation von Sicherheitspatches dahingehend überprüfen, dass Prozesse zur Installation der vom Hersteller bereitgestellten kritischen Sicherheitspatches innerhalb von einem Monat nach der Veröffentlichung und alle weiteren vom Hersteller bereitgestellten Sicherheitspatches innerhalb eines angemessenen Zeitrahmens (zum Beispiel innerhalb von drei Monaten) definiert sind.

**6.2.b** Für eine Stichprobe an Systemkomponenten und verwandter Software die Liste der installierten Sicherheitspatches auf den einzelnen Systemen mit der aktuellen Liste der Sicherheitspatches des Herstellers vergleichen und sicherstellen, dass die kritischen Sicherheitspatches des Herstellers innerhalb eines Monats nach Veröffentlichung und alle weiteren vom Hersteller bereitgestellten Sicherheitspatches innerhalb eines angemessenen Zeitraums (zum Beispiel innerhalb von drei Monaten) installiert werden.

TIPP:

Der Strom an Angriffen, die auf weit verbreiteten Exploits basieren (sogenannte „Zero Day-Angriffe", bei welchen eine zuvor unbekannte Sicherheitslücke genutzt wird) und auf Systeme abzielen, die ansonsten gut geschützt sind, steigt kontinuierlich an. Wenn auf geschäftskritischen Systemen die neuesten Patches nicht unmittelbar implementiert werden, können diese Exploits von Kriminellen genutzt werden, um ein System anzugreifen, zu deaktivieren oder Zugriff auf vertrauliche Daten zu erhalten.

Durch Priorisierung der Patches für kritische Infrastrukturen wird sichergestellt, dass Systeme und Geräte mit hoher Priorität vor Sicherheitslücken geschützt sind, sobald ein Patch veröffentlicht wird. Die Patchinstallationen sollten so priorisiert werden, dass Sicherheitspatches für kritische oder gefährdete Systeme innerhalb von 30 Tagen und andere Patches für Lücken mit geringerem Risiko innerhalb von 2 bis 3 Monaten installiert werden.

Diese Anforderung gilt für alle für die installierte Software bereitgestellten Patches.

## MEHR EFFIZIENZ – INTEGRIERTES MANAGEMENT

Mit Kaspersky Endpoint Security for Business erhalten Ihre Sicherheitsteams umfassende Transparenz und Kontrolle über jeden einzelnen Endpoint.

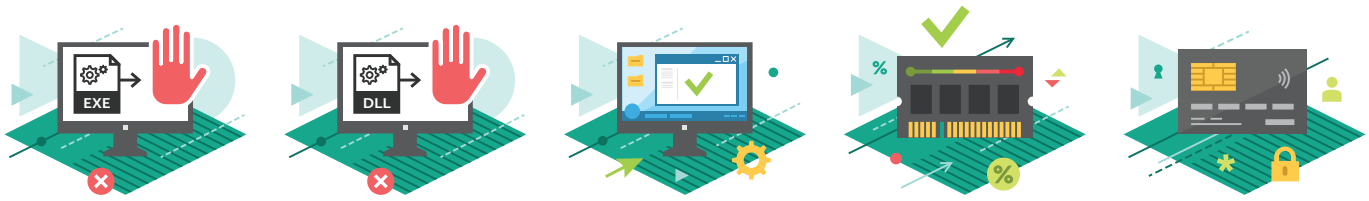
Die Lösung ist hoch skalierbar und bietet Zugriff auf Bestandslisten, Lizenzierung, Remote-Troubleshooting und Netzwerkkontrollen, die alle über eine Konsole zugänglich sind, das Kaspersky Security Center.

## INSTANDHALTUNG UND SUPPORT

Wir sind in mehr als 200 Ländern mit 34 Niederlassungen weltweit tätig und bieten exzellenten Support – rund um die Uhr an jedem Tag im Jahr. Dieses Engagement spiegelt sich in unseren speziellen Maintenance-Service-Agreement (MSA)-Support-Paketen wider.

Unsere professionellen Serviceteams sind immer in Bereitschaft und stellen sicher, dass Sie aus Ihrer Kaspersky-IT- und OT-Security-Lösung stets das Maximum herausholen.

Kontaktieren Sie das Kaspersky Lab Enterprise Sales Team, um mehr über die effektive Sicherung Ihrer Endpoints zu erfahren.




Informationen zur Internetsicherheit: **de.securelist.com**
Informationen zu Partnern in Ihrer Nähe finden Sie hier:
**www.kaspersky.de/partners**

**www.kaspersky.de**
**#truecybersecurity**