

Informationsnachtrag: Durchdringungstest

Standard: Datensicherheitsstandard (DSS)

Version: 1.2

Datum: März 2008

Anforderung: 11.3

Autor: PCI Security Standards Council

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 11.3 des PCI Datensicherheitsstandards (DSS).

2

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 11.3
Durchdringungstest

Allgemeines

PCI DSS-Anforderung 11.3 befasst sich mit Durchdringungstests, die sich von der in PCI DSS-Anforderung 11.2 geforderten Bewertung der externen und internen Sicherheit unterscheiden.

Bei einer Schwachstellenbewertung werden lediglich die bekannten Schwachstellen identifiziert und gemeldet. Bei einem

Durchdringungstest wird hingegen versucht, Schwachstellen zu nutzen, um zu ermitteln, ob unbefugter

Zugriff oder andere böswillige Aktivitäten möglich sind. Der Durchdringungstest muss die Netzwerk-

und Anwendungsebene umfassen sowie Steuerelemente und Prozesse rund um die Netzwerke und

Anwendungen berücksichtigen. Der Test muss von außerhalb des Netzwerks versuchen, in das Netzwerk einzudringen (externer

Test) und er muss innerhalb des Netzwerks durchgeführt werden.

Wer führt den Durchdringungstest durch?

PCI DSS setzt nicht voraus, dass ein QSA oder ASV den Durchdringungstest durchführt. Er kann entweder von einer qualifizierten internen Ressource oder durch qualifizierte Dritte erfolgen.

Werden interne

Ressourcen zur Durchführung von Durchdringungstests verwendet, muss es sich um erfahrene Tester handeln. Die Personen, die den Durchdringungstest durchführen, dürfen nicht mit dem Management der getesteten Umgebung betraut sein. Der

Firewall-Administrator darf beispielsweise nicht den Durchdringungstest für die Firewall durchführen.

Berichte und Dokumentation

Es wird empfohlen, die Methoden und Ergebnisse des Durchdringungstests zu dokumentieren. PCI SSC definiert keine Berichtsanforderungen an Durchdringungstests, aber die Ergebnisse sollten dokumentiert werden, damit ermittelte Probleme näher untersucht werden können und ein Anhaltspunkt

für die Prüfung im Rahmen der PCI DSS-Bewertung vorhanden ist.

Umfang

Der Umfang des Durchdringungstests beinhaltet die Datenumgebung des Karteninhabers sowie alle damit verbundenen Systeme und

Netzwerke. Ist eine Netzwerksegmentierung vorhanden, die die Datenumgebung des Karteninhabers

von anderen Systemen isoliert, und wurde diese Segmentierung

im Rahmen der PCI DSS-Bewertung geprüft, kann der Umfang des Durchdringungstests auf die Datenumgebung des Karteninhabers begrenzt werden.

Häufigkeit

Der Durchdringungstest sollte mindestens einmal pro Jahr und immer dann erfolgen, wenn die Infrastruktur oder Anwendung erheblich aktualisiert oder verändert wurde (z. B. nach der Installation neuer Systemkomponenten bzw. nach dem Hinzufügen eines Subnetzwerks oder eines Webservers). Die Notwendigkeit des Tests ergibt sich aus der Konfiguration einer vorgegebenen Umgebung und kann daher nicht von PCI SSC definiert werden. Sofern die Aktualisierung/Änderung die Daten des Karteninhabers beeinflusst oder den Zugriff auf diese Daten ermöglicht, ist die Notwendigkeit eines Tests gegeben. Die Notwendigkeit in einem hochgradig segmentierten Netzwerk, in dem die Daten des Karteninhabers klar von anderen Daten und Funktionen getrennt sind, unterscheidet sich stark von der Notwendigkeit in einem einfachen Netzwerk, in dem alle Personen und Geräte möglicherweise auf die Daten des Karteninhabers zugreifen können. Als Sicherheits-„Best Practice“ hat sich bewährt, dass alle Aktualisierungen und Änderungen einen Durchdringungstest durchlaufen müssen, um sicherzustellen, dass die angenommenen Sicherheitsmaßnahmen auch nach der Aktualisierung/Änderung effizient funktionieren.

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 11.3 des PCI Datensicherheitsstandards (DSS).

3

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 11.3 Durchdringungstest

Vorbereitung

Für einen Durchdringungstest stehen zahlreiche Methoden zur Verfügung. Zunächst muss entschieden werden, über welche Kenntnisse zum zu testenden System der Tester verfügt. Ein Test ohne Vorkenntnisse wird als „Black Box-Test“ bezeichnet, bei dem der Tester zunächst die Position der Systeme ermitteln muss, bevor er fortfahren kann. Ein Test mit expliziten Kenntnissen wird als „White Box-Test“ bezeichnet.

Wird festgestellt, dass der Tester von Vorkenntnissen profitiert, gelten einige andere PCI DSS-Anforderungen, auf deren Grundlage verwendbare Informationen ermittelt werden. Zu diesen PCI DSS-Elementen zählen:

- Ein Netzwerkdiagramm (1.1.2)
- Ergebnisse einer QSA-Prüfung oder ein Selbstbeurteilungs-Fragebogen (SBF)
- Vierteljährliche Tests auf WLAN-Zugriffspunkte (11.1)
- Ergebnisse vierteljährlicher externer und interner Schwachstellenprüfungen (11.2)
- Ergebnisse des letzten Durchdringungstests (11.3)
- Jährliche Identifikation von Bedrohungen und Schwachstellen, die zu einer Risikobewertung führen (12.1.2)
- Jährliche Prüfungen der Sicherheitsrichtlinien (durch die Aktualisierung von Richtlinien lassen sich ggf. neue Risiken in einem Unternehmen ermitteln) (12.1.3)

Die Dokumentation aus den zuvor genannten Punkten muss evaluiert werden. Bedrohungen und Schwachstellen, die im Rahmen der normalen Bewertungsprozesse ermittelt wurden, müssen berücksichtigt werden.

Methoden

Nach der Evaluierung von Bedrohungen und Schwachstellen müssen Sie den Test entwickeln, um die in der Umgebung ermittelten Risiken einschätzen zu können. Der Durchdringungstest muss der Komplexität und Größe des Unternehmens angemessen sein. Alle Positionen von Karteninhaberdaten,

alle Schlüsselanwendungen, in denen diese Daten gespeichert, verarbeitet oder übertragen werden, alle wichtigen Netzwerkverbindungen und alle wichtigen Zugriffspunkte müssen berücksichtigt werden. Der Durchdringungstest muss versuchen,

Schwachstellen in der Datenumgebung des Karteninhabers auszunutzen und auf Netzwerk- sowie auf Anwendungsebene einzudringen. Das Ziel des Durchdringungstests ist zu klären, ob der unbefugte Zugriff auf wichtige Systeme und Dateien möglich ist. Ist der Zugriff möglich, muss die Schwachstelle beseitigt und der Test wiederholt werden, bis kein unbefugter Zugriff oder andere böswillige Aktivitäten mehr möglich sind.

Komponenten

Berücksichtigen Sie diese Techniken für Durchdringungs- und andere Tests in folgenden Methoden: Social Engineering und Nutzung bekannter Schwachstellen, Zugriffskontrolle für Systeme und Dateien, Web-orientierte Anwendungen, individuelle Anwendungen

und Wireless-Verbindungen.

Dieses Dokument enthält ergänzende Informationen. Diese Informationen ersetzen nicht die Bestimmungen der Anforderung 11.3 des PCI Datensicherheitsstandards (DSS).

4

Informationsnachtrag: Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderung 11.3 Durchdringungstest

Wichtige Aspekte

Im Hinblick auf die PCI-Konformität sollten Tests auf Schwachstellen oder Fehlkonfigurationen, die zu DoS-Angriffen auf die Ressourcenverfügbarkeit (Netzwerk/Server) führen können, vom Tester nicht berücksichtigt werden, da diese Schwachstellen die Karteninhaberdaten nicht gefährden.

Teilen Sie allen betroffenen Parteien im Unternehmen den zeitlichen Ablauf und den Umfang des Durchdringungstests mit.

Führen Sie die Tests gemäß der zentralen Unternehmensprozesse durch. Hierzu zählen Änderungskontrolle, Business Continuity und Disaster Recovery.

Führen Sie den Durchdringungstest in einem überwachten Wartungsfenster durch.

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.