PCI 카드 보안 표준

Payment Card Industry(PCI)

Data Security Standard

보안 스캐닝 절차

Version 1.1

Release: 2006. 09.

목 차

목적

본 문서는 가맹점 (merchants) 들과 서비스 제공업체들이 PCI 데이터 보안 표준(이하 PCI DSS) 요건을 준수하고 있음을 점검받기 위해 수행되는 PCI 보안 스캔의 목적과 범위를 설명한 문서이다. 승인된 스캐닝 벤더들 (Approved Scanning Vendors – 이하 ASV)은 가맹점(merchant) 들과 서비스 제공업체가 PCI 보안 스캔 범위를 선정시 본 문서를 참조하여 선정할 수 잇도록 지원한다.

개요

PCI DSS 는 카드소유자 정보의 저장, 처리 및 전송을 담당하는 가맹점 및 서비스 제공업체들의 보안 요건에 관한 세부 사항을 기술한 문서이다. PCI DSS 의 요건 준수를 위하여 가맹점 및 서비스 제공업체는 각 지불카드 회사에 의해 정해진 규정대로 주기적으로 PCI 보안 스캔을 실행한다.

PCI 보안 스캔은 ASV 들이 인터넷 상에서 수행하는 스캐닝이다. PCI 보안 스캔은 취약점 관리 프로그램과 함께 필수적인 중요한 툴이다. 스캔을 통해 취약점과 웹사이트의 구성 오류, 어플리케이션, 인터넷에서 사용되는 IP 프로토콜 주소를 포함하는 IT 구성 등을 파악할 수 있다.

스캔 결과는 효율적인 패치 관리 및 인터넷 해킹에 대비한 보안 개선에 관한 정보를 제공한다.

PCI 보안 스캔은 공인 IP 주소를 사용하는 모든 가맹점 및 서비스 제공업체에 적용될 수 있다. 웹 상에서의 거래를 제공하지 않는 업체라 하더라도, 다른 서비스를 통하여 업체의 시스템이 인터넷에 접속할 수 있다. 이메일 및 직원의 인터넷 사용 등 간단한 기능을 통해서도 인터넷 상에서 회사 네트워크로 접근이 가능하다. 이러한 작은 경로를 통하여 가맹점 및 서비스 제공업체 시스템에 대한 접근이 가능하며 시스템이 적절하게 관리되지 않을 경우 카드 소유자 정보가 노출될 수 있다.

PCI 보안 스캔의 범위

PCI 는 모든 외부 개방용 IP 주소를 대상으로 취약점 스캔 실시를 요구한다. 처음 고객이 제공하지 않은 IP 주스들 중에 active IP 주소를 발견시, 해당 IP 주소를 스캐닝 범위에 포함시킬 여부를 고객들이 결정할 수 있도록 ASV 는 조원을 해 주어야 한다. 회사는 수많은, 가용한 IP 주소를 보유하고 있으나 카드 승인이나 카드 처리를 위해서는 단지 소수의 IP 만을 사용하고 있는 경우가 있다. 이러한 경우, ASV 는 가맹점과 서비스 제공업체가 PCI 기준에

맞게 적절한 스캐닝 범위를 선정하도록 도와 줄 수 있다. 일반적으로 PCI 보안 스캔의 범위를 줄이는 데 있어서 다음과 같은 방법이 사용된다.

1) 카드소유자 정보를 다루는 세그먼트와 그 외의 세그먼트 간의 물리적인 세그먼트 제공

2) "카드소유자 정보를 취급하는 네트워크/세그먼트 및 그 외의 네트워크/세그먼트 간에 트래픽을 금지하는 곳에 적절히 논리적 세그먼트 제공

ASV 에게 전문가적 도움을 받는다 하더라도 PCI 보안 스캔의 범위를 정하는 최종 책임은 가맹점이나 서비스 제공업체들에게 있다. 스캔 범위에서 제외된 IP 주소나 다른 구성요소들을 통해 계좌정보들을 취급시, 가맹점이나 서비스 제공업체에게 책임이 있는 것이다.

스캔 절차

PCI 보안 스캔 요건 준수를 위해, 가맹점과 서비스 제공업체는 아래의 절차에 따라서 웹사이트 및 공인 IP 주소와 연계된 IT infrastructure 를 스캔한다:

1. PCI 보안 규정 협회 (PCI Security Standards Council) 이 승인하는 ASV 들 중에서 수행업체를 선정하여 ASV 가 모든 스캔을 수행해야 한다.

   ASV 들은 "승인된 ASV 의 기술적·운영상의 요구사항" 절차에 따라 스캔을 수행해야 한다. 이러한 절차에 [고객의 환경의 정상적 운영에 영향을 미쳐서는 안되며 ASV 는 고객 환경에 침투하거나 변경을 해서는 안 된다] 라는 사항이 언급되어 있다.

2. PCI DSS 요구사항 11.2 에 따라 분기별로 스캔을 해야 한다.

3. Web site 나 IT Infrastructure 을 스캔하기 전에, 가맹점과 서비스 제공업체들은 반드시 다음 사항을 지켜야 한다.

   - 모든 공개 IP 주소 및 IP 주소 범위 (IP address ranges) 목록을 ASV 에게 제공한다.
   - 도메인 기반 가상 호스팅 (Domain-based virtual hosting) 이 사용되고 있으면 스캔되어야 할 모든 도메인 목록을 ASV 에게 제공한다.

4. 고객이 제공한 IP 주소 범위 (IP address range)를 사용하여, ASV 는 네트워크 스캔을 수행하여 IP 주소와 서비스의 active 여부를 결정해야 한다.

5. 가맹점 및 서비스 제공업체는 ASV 와 함께 모든 Active IP 주소 가능하다면 도메인도) 및 장비에 대해 주기적으로 스캔을 해야 한다. (정기적 스캔을 위해 밴더와 계약을 체결해야 한다.

6. ASV 는 침입차단시스템 또는 외부 라우터 (트래픽 필터에 사용되고 있다면) 등의 모든 필터링 장비들을 스캔해야 한다. 침입차단시스템이나 라우터가 DMZ 구성을 위해 사용되고 있으면 해당 장비들도 취약점을 파악하기 위해 스캔을 수행해야 한다.

7. ASV 는 반드시 모든 웹 사이트를 스캔해야 한다.

   웹서버를 통해 인터넷 사용자들이 웹 페이지를 보고 웹 가맹점과 상호 작용한다. 인터넷으로부터 이러한 서버에 대한 폭넓은 접근이 가능하므로, 취약점 스캔은 매우 중요하다.

8. ASV 는 모든 어플리케이션 서버를 스캔해야 한다.

   어플리케이션 서버는 웹 서버와 백엔드 데이터베이스 (Back-end database) 및 레거시 시스템 (Legacy system)을 연계하는 인터페이스 역할을 수행한다. 예를 들어, 카드고객이 가맹점 또는 서비스 제공업체와 카드 번호를 공유할 경우, 어플리케이션 서버는 안전한 네트워크 내외부로 데이터를 전달하는 기능을 수행한다. 해커들은 이러한 서버들의 취약점을 악용하여 해킹 스크립을 통해 신용카드 데이터 저장 가능성이 높은 내부 데이터베이스에 대한 접근을 시도한다.

9. ASV 는 DNS 서버들 (Domain Name Servers – DNS) 을 스캔해야 한다.

   DNS 서버는 도메인명을 IP 주소로 변환함으로써 인터넷 주소를 결정한다. 가맹점과 서비스 제공 업체는 자체 DNS 서버를 사용하거나 인터넷 서비스 제공업체 (Internet Service Provider (ISP))의 DNS 서비스를 사용하는 경우가 있다. DNS 서버가 취약할 경우, 해커들은 가맹점 또는 서비스 제공업체 웹 페이지를 스푸핑 (Spoof)하여 신용카드 정보를 수집할 수 있다.

10. ASV 는 메일 서버들을 스캔해야 한다.

    메일 서버는 주로 DMZ 내에 존재하며 해커의 공격에 취약할 수 있다. 메일 서버들은 전체 웹 사이트 보안을 유지하는 데 중요한 요소이다.

11. ASV 는 가상 호스트들 (Virtual Host)을 스캔해야 한다.

단일 서버가 한 개 이상의 웹 사이트를 호스팅하는 공유된 호스팅 환경(Shared hosting environment) 은 일반적인 관행이다. 이러한 경우에, 가맹점들이 이 서버를 호스팅 회사의 다른 고객들과 공유하게 되고 가맹점의 웹 사이트가 이 호스팅 서버의 다른 웹 사이트들을 통해 위험에 노출될 수도 있다.

웹 사이트를 호스팅받고 있는 모든 가맹점들은 반드시 호스팅 제공자에게 요청하여 모든 공인 IP 범위를 스캔하여, PCI 요구사항 준수를 입증해야 한다.

12. ASV 는 반드시 무선 랜(wireless LANs-WLANs) 의 무선 AP (wireless access points) 를 스캔해야 한다.

    무선랜 사용으로 인해 새로운 데이터 보안 위험이 발생 가능하므로 이를 파악하여 위험을 줄여야 할 필요성이 있다. 가맹점들, 프로세서, 게이트웨이, 서비스 제공업체 및 기타 관련 업체는 그들의 인터넷에 연결되어 있는 무선 요소를 반드시 스캔하여 잠재적인 취약점과 구성 오류를 파악해야 한다.

13. ASV 의 IP 주소를 허용하도록 침입차단시스템 및 침입방지시스템의 설정을 변경한다. 이것이 불가능하다면, 침입차단시스템 및 침입방지시스템의 인터페이스에 영향을 주지 않는 장소에서 스캔을 해야 한다.

요건 준수 사항 보고

가맹점 및 서비스 제공업체는 각각의 카드 회사의 준수 보고 요건에 따라 요건 준수 보고를 하여 각각의 카드 회사가 요건 준수 사항을 알 수 있도록 한다. 스캔 결과 보고서는 공통된 형식에 따라야 하나 스캔 결과는 각각의 카드 회사의 요건에 맞게 제출되어야 한다. 매입 은행 (acquiring bank) 에게 연락하거나 또는 각각의 카드 회사의 웹사이트를 참조하여 보고서를 제출할 대상을 결정한다.

보고서 읽기 및 이해하기

ASV 는 네트워크 스캔의 결과에 근거하여 보고서를 작성한다.

스캔 결과 보고서에 취약점 또는 위험의 유형, 관련 이슈 진단 사항, 취약점의 수정 및 패치 방법에 대한 가이드 내용을 기술한다. 또한 스캔을 통해 발견된 취약점을 등급으로 분류하여 보고서에 포함시킨다.

ASV 는 각각의 취약점 결과 보고 방식을 갖고 있을 수 있으나, 공정하고 일관된 준거성 Rating 을 보장하기 위해서 높은 수준의 위험을 일관성 있게 보고해야 한다. 스캔 결과 보고서를 검토하여 결과 내용을 이해할 수 있도록 벤더와 상의하도록 한다.

표 1 은 네트워크 스캔 솔루션이 취약점과 취약점 유형 및 높은 수준의 위험 유형을 분류하는 방법을 기술한 것이다..

보안 요건 준수를 위하여 스캔 결과에 높은 등급의 취약점을 나타내지 않는다. 스캔 결과 보고서에는 PCI DSS 를 위반하는 특징 및 구성요소들을 나타내는 어떠한 취약점들에 대해서 기술하지 않는다 만약 포함되어 있다면, ASV 는 고객과 상의하여 PCI DSS 위반사항 유무를 결정해야 한다. (사실 PCI DSS 위반 사항이 보고된 것은 요구 사항을 충족하지 않는다는 것을 의미한다.)

높은 등급의 취약점은 3,4,5 단계로 나타나 있다.

표 1 취약점 단계

단계	등급	설명
5	Urgent (긴급한 사항)	트로이 목마 (Trojan Horse), 파일 읽기 및 쓰기 취약점, 원격 명령 실행
4	Critical (치명적인 사항)	트로이 목마 잠재 가능성 있음, 파일 읽기 취약점
3	High (높음)	제한적인 읽기 취약점, 디렉토리 브라우징(Directory browsing), 서비스 거부 (Denial of service (DoS))
2	Medium (중간)	해커에 의해 민감한 구성정보 획득 가능성 있음
1	Low (낮음)	구성정보 상에 해커에 의해 획득될 수 있는 정보.

5 등급

5 등급 취약점은 원격 침입자에게 원격 루트 또는 원격 관리 기능을 제공한다. 5 등급 취약점을 통해 해커가 호스트 전체를 침입 (compromise) 할 수 있다. 5 등급 취약점은 원격 해커들에게 전체 파일 시스템을 읽고 쓸 수 있는 기능, 루트나 관리자에 의한 원격 명령어 실행 등을 제공하는 취약점을 포함한다. 백도어나 트로이 목마 역시 5 등급 취약점으로 분류된다.

4 등급

4 등급 취약점은 침입자에게 원격 사용자 기능은 제공하지만 원격 관리 또는 루트 사용자 기능은 제공하지 않는다. 4 단계 취약점은 해커들에게 파일 시스템으로의 부분적인 접근을 할 수 있게 해 준다. (예를 들어 완전한 쓰기 접근(full write access)은 없지만 완전한 읽기 접근(full read access)은 가능). 민감도가 높은 정보를 유출시키는 취약점도 4 단계 취약점으로 분류된다.

3 등급

3 등급 취약점은 해커들에게 보안 셋팅을 포함하여 호스트에 저장된 특정한 정보에 접근할 수 있도록 한다. 이러한 취약점으로 인해 침입자가 호스트 오용 (misuse)을 일으킬 수 있다. 3 등급 취약점의 예로 파일 내용의 부분적 공개, 호스트의 특정 파일에 대한 접근, 디렉토리 브라우징(directory browsing), 필터링 규칙과 보안 메커니즘의 노출, 서비스 거부 공격에 쉽게 노출, 메일 릴레이 같은 서비스의 무허가 사용 등이 있다.

2 등급

2 등급 취약점은 정확한 서비스 버전 등 호스트로부터 일부 민감한 정보를 유출시킨다. 이러한 정보를 가지고 해커들은 호스트 공격에 대해 조사할 수 있다.

1 등급

1 등급 취약점은 공개 포트 (open port) 와 같은 정보를 노출시킨다.