보안성 향상을 위한 PCI DSS

작성자 : 김재벌
E-mail : ostoneo@gmail.com

PCI DSS 란?

최근 보안 업계의 핫한 키워드 중에 하나는 클라우드와 핀테크 일 것이다.
클라우드와 핀테크가 이슈가 되면서 업계에서 함께 대두되는 용어가 있는데, 바로 PCI DSS 다.
최근에는 대부분의 정부가 법적 규제를 통해 통제하므로 기업들은 적절한 보안대책을 강구하여야 한다.
법이나 제도권하에서의 보안은 다소 딱딱한 주제일 수 있다. 그러나, 최근 시스템들은 이러한 컴플라이언스 요소를 반영하여 보안성을 강화 하고 있으므로 이에 대해서 알아보는 것도 중요하다고 할 것이다.

그 첫 번째로 PCI DSS에 대해서 알아보고자 한다.

보안에 관심이 있다면 PCI DSS에 대해서 한번쯤은 들어봤을 수도 있지만, 여전히 PCI DSS 는 생소한 분들이 많다.

PCI DSS '란 무엇인가?

신용 카드 회사의 홈페이지를 보면 **PCI DSS (Payment Card Industry Data Security Standard)** 는 가맹점 결제 대행 사업자가 취급하는 카드 회원의 신용 카드 정보 및 거래 정보를 안전하게 보호하기 위해 JCB, 아메리칸 익스프레스, Discover, MasterCard, VISA의 국제 결제 브랜드 5 개사가 공동으로 책정 한 신용 업계 글로벌 보안 기준 이라고 언급되어 있다.

그렇다면 이러한 PCI DSS는 비단 신용카드 정보를 취급하는 곳에만 관계가 있다고 생각할 수 있다.

이 PCI DSS 사실 정보 보안에 대한 구체적인 구현을 요구하고 있는 것으로, "네트워크 및 애플리케이션 침투 테스트의 횟수와 실시시기」「패치 릴리스 후 1 개월 이내에 신청」「몇 번의 잘못된 로그온 시도 한 경우 잠금 ""클라이언트 PC에 개인 방화벽 설치 '등 구체적인 시책을 정량적으로 제시되어 있으며, **미국에서는 신용 카드 정보와 무관 한 기업이나 조직이 PCI DSS를 기준으로 채택하고 있다.**

PCI DSS 개발 과정

신용 카드 회사는 PCI DSS가 개발되기 이전부터 신용 카드 정보와 결제 정보를 보호하기 위해 자신들 만의 기준을 책정했다.
예를 들어 VISA나 마스터 카드도 별도의 기준을 가지고 있다.
이러한 각 회사의 의도는 결국 카드 소유자의 데이터를 저장, 처리, 전송할 때 최소한의 보안수준을 만족시키는 것이었다.

따라서 여러 카드를 취급하는 가맹점은 여러 기준을 만족시켜야 하므로 기준을 공통화함으로써 비용과 시간을 아낄 수 있게 된다.
이러한 이유로 주요 신용 카드 회사가 연계하여 등장한 것이 PCI DSS다.

PCI DSS는 2004 년 12 월에 제정되어 2006 년 9 월 현재 v1.1 버전업 되면서 발전하였고, 또한 동시에 PCI SSC (PCI 보안 표준 협의회)가 PCI DSS의 유지, 관리, 보급 활동을 목적으로 설립되었으며, 현재는 3.1.1 이다.

PCI DSS 준수여부 진단은 1. **문진표에 의한 자기 진단** 2. **취약성 스캐닝 테스트** 3. **방문 조사** 통해 심사 하고 있다.

해외의 경우 신용 카드 회사는 가맹점이 프로그램에 참여하지 않으면 벌금을 부과하거나 구체적인 조치를 취하도록 요구하는 경우도 있다.

마스터 카드의 홈페이지를 보면 "과거에 카드 거래 정보의 유출이 발생한 적이 있는 모든 가맹점」은 매년 방문 조사와 분기별 취약점 스캐닝 테스트를 의무화하고 있음을 알 수 있다.

국내사례는 아니지만 실제로 일본 기업의 인터넷 쇼핑 사이트에서 카드 회원 데이터 유출 사고가 발생했을 때 사고 대응 후 신용 카드 회사에서 PCI DSS 준수를 카드 취급 재개의 조건으로 걸었다는 사례가 있다.

PCI DSS의 12가지 요구 사항

PCI DSS는 카드 회원 데이터를 취급하는 시스템을 다른 시스템과 분리하라는 메시지가 네트워크를 분리하고 적절하게 관리하기 위해 6 개의 "컨트롤의 목적 '과 네트워크 아키텍처, 소프트웨어 디자인, 보안 관리, 정책, 절차 등에 관한 기준이 "**12가지 요구 사항"** 으로 규정되어 있다 .

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

- **Ⅰ 안전한 네트워크 구축 및 유지**
  - **요구 사항 1** : 카드 회원 데이터를 보호하기 위해 방화벽을 도입, 최적의 설정을 유지
  - **요구 사항 2** : 시스템 암호 및 기타 보안 매개 변수에 벤더가 제공하는 기본값을 사용하지 않는 것

- **Ⅱ 카드 회원 데이터 보호**
  - **요구 사항 3** : 저장된 카드 회원 데이터를 안전하게 보호
  - **요구 사항 4** : 퍼블릭 네트워크에서 카드 회원 데이터를 보낼 때 암호화

- **Ⅲ 취약점 관리 프로그램의 정비**
  - **요구 사항 5** : 안티 바이러스 소프트웨어를 이용하여 정기적으로 갱신
  - **요구 사항 6** : 안전한 시스템과 어플리케이션을 개발, 유지 보수

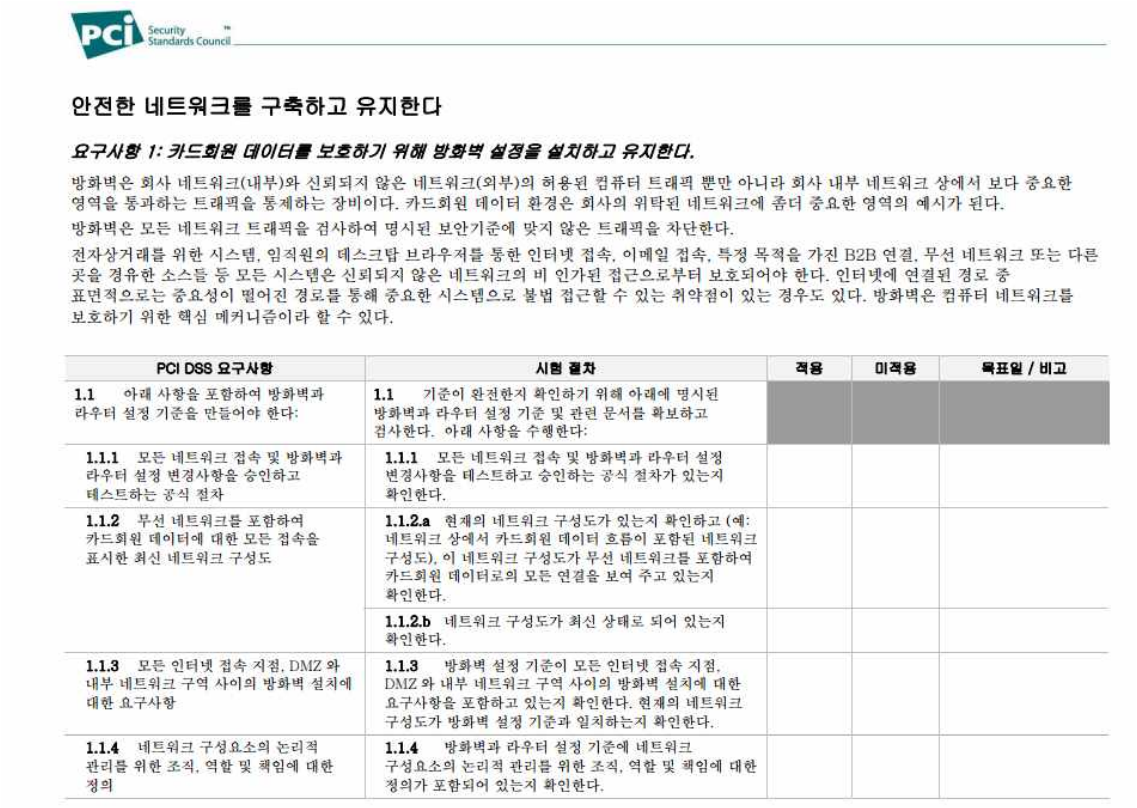
- **Ⅳ 강력한 액세스 제어 기법의 도입**
  - **요구 사항 7** : 카드 회원 데이터에 대한 접근을 업무상 필요한 범위 내로 제한
  - **요구 사항 8** : 컴퓨터에 액세스하는 사용자마다 개별 ID를 할당
  - **요구 사항 9** : 카드 회원 데이터에 대한 물리적 액세스를 제한

- **Ⅴ 정기적 인 네트워크 모니터링 및 테스트**
  - **요구 사항 10** : 네트워크 자원과 카드 회원 데이터에 대한 모든 접근을 추적하고 모니터링
  - **요구 사항 11** : 보안 시스템 및 관리 절차를 정기적으로 테스트

- **Ⅵ 정보 보안 정책의 점검**
  - **요구 사항 12** : 정보 보안 정책 점검

요구 사항은 더욱 상세하게 세부항목에 규정되어 있다.
규정의 내용은 카드 회원 데이터 보호를 목적으로 하고 있기 때문에, **ISO / IEC27001 등 일반 기준보다 구체적인 정량적으로 표현 된다.**

구체적으로 이미지하기 쉬운 PCI DSS 요구 사항



PCI Security Standards Council

안전한 네트워크를 구축하고 유지한다

요구사항 1: 카드회원 데이터를 보호하기 위해 방화벽 설정을 설치하고 유지한다.

방화벽은 회사 네트워크(내부)와 신뢰되지 않은 네트워크(외부)의 허용된 컴퓨터 트래픽 뿐만 아니라 회사 내부 네트워크 상에서 보다 중요한 영역을 통과하는 트래픽을 통제하는 장비이다. 카드회원 데이터 환경은 회사의 위탁된 네트워크에 좀더 중요한 영역의 예시가 된다.

방화벽은 모든 네트워크 트래픽을 검사하여 명시된 보안기준에 맞지 않은 트래픽을 차단한다.

전자상거래를 위한 시스템, 임직원의 데스크탑 브라우저를 통한 인터넷 접속, 이메일 접속, 특정 목적을 가진 B2B 연결, 무선 네트워크 또는 다른 곳을 경유한 소스들 등 모든 시스템은 신뢰되지 않은 네트워크의 비 인가된 접근으로부터 보호되어야 한다. 인터넷에 연결된 경로 중 표면적으로는 중요성이 떨어진 경로를 통해 중요한 시스템으로 불법 접근할 수 있는 취약점이 있는 경우도 있다. 방화벽은 컴퓨터 네트워크를 보호하기 위한 핵심 메커니즘이라 할 수 있다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
1.1 아래 사항을 포함하여 방화벽과 라우터 설정 기준을 만들어야 한다:	**1.1** 기준이 완전한지 확인하기 위해 아래에 명시된 방화벽과 라우터 설정 기준 및 관련 문서를 확보하고 검사한다. 아래 사항을 수행한다:			
1.1.1 모든 네트워크 접속 및 방화벽과 라우터 설정 변경사항을 승인하고 테스트하는 공식 절차	**1.1.1** 모든 네트워크 접속 및 방화벽과 라우터 설정 변경사항을 테스트하고 승인하는 공식 절차가 있는지 확인한다.			
1.1.2 무선 네트워크를 포함하여 카드회원 데이터에 대한 모든 접속을 표시한 최신 네트워크 구성도	**1.1.2.a** 현재의 네트워크 구성도가 있는지 확인하고 (예: 네트워크 상에서 카드회원 데이터 흐름이 포함된 네트워크 구성도), 이 네트워크 구성도가 무선 네트워크를 포함하여 카드회원 데이터로의 모든 연결을 보여 주고 있는지 확인한다.			
	1.1.2.b 네트워크 구성도가 최신 상태로 되어 있는지 확인한다.			
1.1.3 모든 인터넷 접속 지점, DMZ 와 내부 네트워크 구역 사이의 방화벽 설치에 대한 요구사항	**1.1.3** 방화벽 설정 기준이 모든 인터넷 접속 지점, DMZ 와 내부 네트워크 구역 사이의 방화벽 설치에 대한 요구사항을 포함하고 있는지 확인한다. 현재의 네트워크 구성도가 방화벽 설정 기준과 일치하는지 확인한다.			
1.1.4 네트워크 구성요소의 논리적 관리를 위한 조직, 역할 및 책임에 대한 정의	**1.1.4** 방화벽과 라우터 설정 기준에 네트워크 구성요소의 논리적 관리를 위한 조직, 역할 및 책임에 대한 정의가 포함되어 있는지 확인한다.			

요구 사항 I, 안전한 네트워크 구축 및 유지 " **카드 회원 데이터를 보호하기 위해 방화벽을 도입하여 최적의 설정을 유지** " 의 내용을 보면

- **1.1** 아래 사항을 포함한 방화벽과 라우터의 설정 기준을 확립한다.
- **1.2** 신뢰할 수 없는 네트워크와 카드회워 데이터 환경의 모든 시스템 구성 요소 사이에 접속을 제한하는 방화벽설정을 적용한다.

등으로 항목이 있고 아래와 같이 세부적으로

- **1.1.1** 모든 외부 네트워크 연결 및 방화벽 설정 변경을 승인 테스트 하기 위한 공식적인 절차.
- **1.1.2** 무선 네트워크를 포함하여 카드 회원 데이터에 대한 모든 연결을 보여주는 최신 네트워크 구성도

- **1.1.3** 모든 인터넷 접속 및 DMZ와 내부 네트워크 영역 사이에 방화벽 설치에 대한 요구

등등 으로 보다 세분화 되어 있다.

보다 상세하고 구체적으로 설정되어 있고 구체적으로 정량적으로 표시되어 있다.

PCI DSS 활용 방안

카드 회원 데이터를 사내 시스템에서 취급하는 기업은 PCI DSS 요구 사항을 충족하도록 시스템 구현 업무를 구현할 수 있으며, 이를 통해 최소한 확보해야 할 보안 수준을 달성 수 있다. 그리고, 이 요구 사항은 **구체적이며 정량적이기 때문에 보다 쉽게 이해하고 적용하기 용이하다.**

그러나, PCI DSS가 아무리 좋다고 해도 시간, 비용, 인적자원에는 한계가 있기 때문에, 수백개의 항목에 이르는 요구 사항을 한꺼번에 구현하는 것이 어렵다는 것은 분명하다.

따라서 , 관련 항목중에 우선순위를 설정하고 이를 바탕으로 효율적으로 계획을 세워 적용하는 것이 좋을 것이다.

현재 미국 등에서는 신용 카드 업무와 무관한 기업이나 조직도 PCI DSS를 기준으로 적용하는 등 PCI DSS가 확산되고 있으나 , 아직 국내에서 PCI DSS는 카드사를 중심으로 제한적으로 사용되고 있다.

그러나, 향후 PCI DSS를 활용하는 움직임은 더욱 가속화 해 나갈 것으로 예상된다.

신용 카드 데이터를 다루는 유무에 구애받지 않고, 현재 운영 중인 시스템과 운영 관리 수준을 확인하는데 참고한다면 좋을 것이다.

아울러 , 이러한 PCI DSS 컨설팅을 지원하는 업체와 솔루션이 시장에 나와 있다 있으므로 이를 검토해 보는 것도 좋은 대안이 되리라 생각한다.

오라클 솔라리스 11에는 이미 PCI DSS 3.0 기능이 탑재되어 있어 몇 개의 명령을 통해 이러한 요구를 충족시킬 수 있다.

솔라리스 11은 compliance 패키지를 설치하고 이에 대한 평가를 수행할 수 있다.

1) 패키지의 설치

```
#pkg install compliance
```

2)평가를 생성한다.

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
# compliance -p Recommended -a recommended
```

해당 명령의 결과로 /var/share/compliance/assessments/recommended 디렉토리에 recommeded.html , recommended.txt , recommneded.xml 파일이 생성되어 진다.

3) 사용자 정의 보고서 생성

```
# compliance report -s -pass,fail,notselected
```

참고 : https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf