**Best of Best 11**

**사례에서 어떠한 법규를 위반 했는 지와 사유작성하기**

**허원식 멘토님 과제 #1 번**

**Best of Best 11기**

**보안제품 개발 희망 정경재**

**제출날짜:2022-07-10**

* 사례 1. DMZ 구간에 고객 정보 저장  
  **위반 법규**  
  **1. 전자금융감독규정  
  제 17조(홈페이지 등 공개용 웹서버 관리대책)**  
  4. DMZ구간 내에 이용자 정보 등 주요정보를 저장 및 관리하지 아니할 것(다만 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화 하여 저장-관리하여야 한다)  
  **2. 개인정보의 안전성 확보조치 기준  
  [시행 2017.7.26.][행정안전부고시 제2017-1호, 2017.7.26. 타법개정]  
  제 7조 3항**  
  개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.  
  **위반 사유**  
  전자 금융감독규정과 개인정보의 안전성 확보조치 기준에서 DMZ의 구간에 고객의 정보를 저장하면 안되지만 만약 저장한다면 암호화를 해 저장을 했어야 한다고 했으나 하지만 그러한 조치가 없었기에 법규들을 위반했다.
* 사례 2. 보안운영 단말기 인터넷 접속  
  **위반 법규  
  1. (개인정보보호위원회)개인정보의 안전성 확보조치 기준  
  제 6조(접근통제)**  
  ③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.   
  **2. 전자금융감독규정  
  [시행 2016.10.5.][금융위원회 제 2016-37호, 2016. 10. 5., 일부개정]  
  제 12조(단말기 보호대책)**  
  3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것.  
  **위반 사유**첫번째로 개인정보의 안전성 확보조치 기준에 의거해서 개인정보가 인터넷을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 단말기에 접근 통제를 해야 했으나 그러한 조치를 취하지 않았다.  
  두번째로는 전자금융감독규정에 단말기 보호 대책에 의해 인터넷 접속이 가능한 중요 단말기를 지정하지 않고 인터넷을 접속했기에 위반사유에 해당한다.
* 사례 3. 전산원장 변경 결제 시 개발자> 팀장> 임원  
  **위반 법규  
  1. 전자금융감독규정  
  [시행 2015. 3. 18.][금융위원회고시 제 2015-7호, 2015. 3. 18., 일부개정]  
  제27조(전산원장 통제)**   
  ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용하여야 한다.  
  ② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.  
  ③ 금융회사 또는 전자금융업자는 대차대조표 등 중요 자료의 계상액과 각종 보조부·거래기록·전산원장파일의 계상액에 대한 상호일치 여부를 전산시스템을 통하여 주기적으로 확인하여야 한다.  <개정 2013. 12. 3.>  
  ④ 금융회사 또는 전자금융업자는 제3항에 따른 확인 결과 불일치가 발견된 때에는 그 원인 및 조치 내용을 전산자료의 형태로 5년간 보존하여야 한다.  <개정 2013. 12. 3.>  
  ⑤ 금융회사 또는 전자금융업자는 이용자 중요원장에 직접 접근하여 중요원장을 조회·수정·삭제·삽입하는 경우에는 작업자 및 작업내용 등을 기록하여 5년간 보존하여야 한다.  <개정 2013. 12. 3.>  
    
  **제28조(거래통제 등)**   
  ① 금융회사 또는 전자금융업자는 사고위험도가 높은 거래에 대하여는 책임자 승인거래로 처리토록 하는 등 전산시스템에 의한 이중확인이 가능하도록 하여야 한다.  <개정 2013. 12. 3.>  
  ② 금융회사 또는 전자금융업자는 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 해야 한다.  <개정 2013. 12. 3.>  
  **위반 사유**전자금융감독규정에 의해서 전산원장의 변경을 위해선 별도의 변경절차를 수립해야 했지만 그러한 것이 없었다는 점과 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제 3자 확인 등이 포함되지 않았다.
* 사례 4. 전자금융 거래 약관 변경 2주 전 이용자에게 통지  
  **위반 법규**  
  **1. 전자금융거래법  
  제24조(약관의 명시와 변경통지 등)**   
  ③ 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 변경되는 약관의 시행일 1월 전에 금융위원회가 정하는 방법에 따라 이를 게시하고 이용자에게 알려야 한다. 다만, 법령의 개정으로 인하여 긴급하게 약관을 변경하는 때에는 금융위원회가 정하는 방법에 따라 이를 즉시 게시하고 이용자에게 알려야 한다. <개정 2008. 2. 29., 2013. 5. 22.>  
  ④ 이용자는 제3항의 규정에 따른 약관의 변경내용이 게시되거나 통지된 후부터 변경되는 약관의 시행일 전의 영업일까지 전자금융거래의 계약을 해지할 수 있다. 전단의 기간 안에 이용자가 약관의 변경내용에 대하여 이의를 제기하지 아니하는 경우에는 약관의 변경을 승인한 것으로 본다.  
  **위반 사유**전자금융거래법 제 24조에 의거하여 약관을 변경할 때는 변경된 약관이 시행되기 1달전에 금융위원회가 정하는 방법에 따라 게시하고 이용자에게 알려줬어야 하지만 그러한 절차가 없었다.  
  따라서 이러한 약관을 위반할 경우 사용자는 시행일전의 영업일까지 약관을 해지할 수 있다,
* 사례 5. 공개용 웹서버에 gcc 사용  
  **위반 법규  
  1. 전자금융감독규정  
  제17조(홈페이지 등 공개용 웹서버 관리대책)**3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험ㆍ개발 도구 등의 사용을 제한할 것 **위반 사유**전자금융감독규정에 의거해 공개용 웹서버애는 서비스를 제외한 나머지 기능을 사용하지 말아야함에도 불구하고 gcc 컴파일러를 사용했으므로 해당 법규를 위반했다고 볼 수 있다.  
  따라서 웹서비스의 테스트나 개발은 테스트 서버에서 진행해야 한다.