경영유의사항 등 공개안

1. 금융기관명 : 하나카드㈜

2. 조치일 : 2020. 2. 13.

3. 조치내용

대상	내용
기 관	개선사항 3건

4. 조치대상사실

가. 개선사항

(1) 스마트폰 앱 접속로그 설정 및 관리 불합리

스마트폰 앱을 통한 전자금융사기사고를 방지하기 위하여 FDS시스템을 구축하여 사기의심거래에 대해 사전 차단 또는 알림 등 모니터링을 수행하고, 위·변조 앱 실행 및 임의개조 폰 접속 등 악성행위를 방지하기 위하여 스마트폰 보안 솔루션을 도입하여 악성행위내역 로그를 수집하고 있으나,

일부 로그에 공격 의심자를 특정할 수 있는 정보를 포함하지 않았고, 공격 의심자를 포함한 로그는 FDS시스템과 연동하지 아니하여 공격 의심자에 대한 의심거래 분석 및 차단에 사용되지 않고 있으므로

위·변조 앱 실행 및 임의개조 폰 접속시 접속 단말 정보 등 공격 의심자를 특정할 수 있는 정보를 수집하여 로그에 남기고, 남겨지는 공격 의심자 정보를 FDS시스템에 연동하여 공격 의심자의 의심거래 분석 및 차단에 이용하는 등 스마트폰 앱 소비자 보호를 개선할 필요

(2) 위·변조 스마트폰 앱 유통 방지대책 불합리

스마트폰 앱은 개발 완료 후 공식 앱 배포처를 지정하여 등록하고, 외부주문업체를 통해 공식 배포처 및 블랙마켓 앱에서 위·변조 앱의 존재 여부를 주기적으로 모니터링하고 있으나

스마트폰 보안 안내 홈페이지에 하나카드의 공식 앱 배포처를 명시하지 않아 고객이 설치하는 앱의 적정성을 확인하기 어렵고, 위·변조 앱 모니터링시 주요 포털사이트 등에서 위·변조 앱을 탐지하지 않고 있으며, 외부주문업체에서 수행한 위·변조 앱 모니터링 결과를 하나카드와 주기적으로 공유하지 않고 있어 회사의 자체적인 위·변조 앱 모니터링 관리가 일부 미흡하므로

고객에게 안내하는 웹 페이지에 하나카드의 공식 앱 배포처를 명시하여 고객이 설치하는 앱의 적정성을 확인할 수 있도록 하고, 위·변조 앱 모니터링시 주요포털 사이트 등의 검색을 포함하여 위·변조 앱의 유통에 대한 탐지를 강화하며, 위·변조 앱의 모니터링 결과를 주기적으로 공유 및 보고받는 등 스마트폰 앱 모니터링을 강화할 필요

(3) 스마트폰 앱 이용자 중요정보 관리 불합리

스마트폰 앱(OOOOOO)을 통하여 본인 확인을 위한 신분증을 촬영하는 경우 이용자 개인정보(주민등록번호 등)의 유출방지대책을 마련하여야 하나,

촬영된 신분증 사진을 이용 후 즉시 삭제하지 않고 스마트폰에 저장하여 스마트폰 분실 또는 악성코드 감염시 신분증 사진이 유출될 우려가 있고,

신분증 사진을 서버에 전달하는 과정에 이용되는 암호화 키가 □□□□□에 노출되고, 고정 암호화 키를 사용함에 따라 암호화 된 데이타 획득시 신분증 사진이 복호화 될 가능성이 있으며,

신분증 정보 추출 후, 추출 정보를 확인하는 페이지에서는 이용자의 개인정보(주민등록번호 등)가 화면에 평문으로 노출됨에도 화면 캡쳐방지 등 보호대책을 미적용하여 악성코드 감염시 이용자의 개인정보가 유출 될 우려가 있으므로

촬영한 신분증 사진은 이용 후 즉시 삭제하고, 서버 전달시 사용되는 암호화 방식은 암호화된 데이터가 외부에 노출되더라도 복호화 되지 않도록 암호 알고리즘 및

키 사용 방식을 보완하는 한편, 개인정보가 노출된 화면 등 중요정보가 포함된 페이지는 화면 캡쳐방지 기능을 적용하는 등 이용자 중요정보 관리를 개선할 필요가 있음