제재내용 공개안

1. 금융기관명 : 키움예스저축은행

2. 조치일 : 2022. 6. 28.

3. 조치내용

제재대상	제재내용
기 관	기관주의, 과태료 부과(5,000만원)
임 원	주의 1명
직 원	견책 1명

4. 제재대상사실

가. 문책사항

(1) 전자금융거래 안전성 확보의무 위반

(가) 자체 보안성 심의 미수행

「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제7조 및 제36조 제1항 제1호에 의하면 금융회사는 정보통신망을 이용하여 신규 전자금융업무를 수행하는 경우 자체 보안성심의를 실시하여야 하는데도

㈜키움예스저축은행은 OOOO.O.O.(시스템 가동시점) ~ 2021.10.26.(검사종료일) 기간 중 ◇◇◇시스템에 대하여 보안취약점 노출 여부 등을 점검하기 위한 자체 보안성심의를 수행하지 않았음

(나) 공개용 웹서버 관리대책 이행 위반

「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제7조, 제17조 제1항 제1호, 제4항, 「신용정보법」 제19조제1항, 「신용정보법시행령」 제16조제1항 및 「신용정보감독규정」 제20조에 의하면 금융회사는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 하고, 공개용 웹서버를 웹 접근제어 수단으로 보호하여야 하며, 개인신용정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하여 보호해야 하는데도,

㈜키움예스저축은행은 2020.1.1.~2021.10.26.(검사대상기간) 기간 중 ◇◇◇시스템에 접속한 해외 IP에 대한 모니터링을 수행하지 않았으며*

* 금융보안원 침해사고 조사 결과 고객정보 유출 관련 해킹공격에 이용된 IP ○○개 중 ○○개가 해외 IP로 확인

OOOO.O.O. 민원인의 제보로 해킹 발생 가능성을 인지했음에도 불구하고 해외 IP 차단* 등의 대응조치를 즉각 수행하지 않았음

* 해킹 발생 가능성 인지 이후 즉각 해외IP를 차단하였다면 ○일(○○○○.○.○.~○., ○○○○.○.○.~○.)의 유출 기간 단축이 가능

OOOO.O.O. (시스템 가동시점)~2021.10.26.(검사종료일) 중 부주의로 인하여 웹서버에 대한 해킹공격을 방지할 수 있는 △△△이 정상 동작하지 않도록 운영하였으며, OOOO.O.O.에서야 새로운 웹 접근 제어수단(웹방화벽)을 설치하였음

(다) 해킹 등 방지대책 이행 위반

「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제7조, 제15조 제1항 제5호 및 제15조 제2항 제2호에 의하면 금융회사는 전산실 내 위치한 정보처리시스템을 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 하고, 정보보호시스템을 설치·운영하는 경우 최소한의 서비스번호(port)만을 적용하여야 하는데도

㈜키움예스저축은행은 OOOO.O.O.(시스템 가동시점)~OOOO.O.O.* 기간 중 전산실 내 위치한 ◇◇◇시스템을 인터넷 등 외부통신망과 물리적으로 분리하지 않았고,

* ㈜키움예스저축은행은 OOOO.O.O. 침입방지시스템에 차단 정책을 적용하여 인터넷 접속 차단

2020.1.1.~2021.10.26.(검사대상기간) 중 정보보호시스템(방화벽)을 운영하면서 인터넷에서 ◇◇◇시스템으로 일부 불필요한 서비스번호*를 통한 접속과 ◇◇◇시스템에서 인터넷으로 모든 서비스번호를 통한 접속을 허용하였음

* 웹서버를 위한 웹서비스용 서비스번호(O, O, O, O)를 WAS·DB서버에도 허용

< 관련규정 >

1.「전자금융거래법」 제21조제2항
2.「전자금융감독규정」 제7조,
제15조제1항제5호, 제2항제2호
제17조제1항제1호, 제4항
제36조제1항제1호
3.「신용정보법」 제19조제1항
4.「신용정보법시행령」 제16조제1항제1호, 제2항
5.「신용정보감독규정」 제20조 <별표3>