금융위원회
의결 제2022-184호

1. 조치대상자의 인적사항

제재대상	내용(회사명, 성명 등)
기 관	㈜ 키움예스저축은행

2. 조치내용

○ 「전자금융거래법」 제21조 제2항에 따라 '전자금융거래 안전성 확보의무 위반'에 대하여 ㈜ 키움예스저축은행에 과태료 50백만원 부과 조치

* 과태료 부과 사전통지 후 의견제출 기한내 자진납부시 「질서위반행위규제법」 제18조에 따라 부과금액의 20%를 감경

3. 조치이유

가. 지적사항

1. 자체 보안성 심의 미수행

○ 금융회사는 정보통신망을 이용하여 신규 전자금융업무를 수행하는 경우 자체 보안성심의를 실시하여야 하는데도,

- ㈜키움예스저축은행은 20××.×.×. ~ 20××.×.×. 기간 중 ■■■■■시스템에 대하여 보안취약점 노출 여부 등을 점검하기 위한 자체 보안성심의를 수행하지 않았음

2. 공개용 웹서버 관리대책 이행 위반

○ 금융회사는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 하고, 공개용 웹서버를 웹 접근제어 수단으로 보호하여야 하며, 개인신용정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하여 보호해야 하는데도,

- ㈜키움예스저축은행은 20××.×.×.~20××.×.×. 기간 중 ××××× 시스템에 접속한 ◇◇ ◇◇에 대한 모니터링을 수행하지 않았고,

- 20××.×.×. 민원인의 제보로 해킹 발생 가능성을 인지했음에도 불구하고 ◇◇ ◇◇ 차단 등의 대응조치를 즉각 수행하지 않았으며,

- 20××.×.×.~20××.×.×. 기간 중 부주의로 인하여 웹서버에 대한 해킹공격을 방지할 수 있는 ▲▲▲▲시스템이 정상 동작하지 않도록 운영하였으며, 20××.×.×.에서야 새로운 △△△△을 설치하였음

3. 해킹 등 방지대책 이행 위반

○ 금융회사는 전산실 내 위치한 정보처리시스템을 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 하고, 정보보호시스템을 설치·운영하는 경우 최소한의 서비스번호(port)만을 적용하여야 하는데도,

- ㈜키움예스저축은행은 20××.×.×.~20××.×.×. 기간 중 전산실 내 위치한 ××××××시스템을 인터넷 등 외부통신망과 물리적으로 분리하지 않았고,

- 20××.×.×.~20××.×.×. 기간 중 정보보호시스템(■■■)을 운영하면서 인터넷에서 ××××× 시스템으로 일부 불필요한 서비스번호를 통한 접속과 ××××× 시스템에서 인터넷으로 모든 서비스번호를 통한 접속을 허용하였음

나. 근거법규

○ 「전자금융거래법」 제21조 제2항, 제51조제1항제1호
○ 「전자금융감독규정」 제7조
제15조제1항제5호, 제2항제2호
제17조제1항제1호, 제4항
제36조제1항제1호