



금융회사 IT 보안강화 종합대책

최 원 선임연구원

- 금감원은 6월 23일에 금융회사 경영진의 IT 보안 관련 인식전환과 IT 보안조직의 실질적 역량 강화 등에 중점을 둔 'IT 보안강화 종합대책'을 발표함.
 - 금감원은 현대캐피탈 고객정보유출(4월 7일)과 농협 전산장애(4월 12일) 등 IT 보완 관련 사고가 연이어 발생함에 따라 금융회사 IT 보안강화 T/F를 구성하여 개선작업을 추진하였으며, 서면 및 현장점검 결과를 토대로 근원적 종합대책을 마련함.
- IT 보안 관련 CEO에 대한 책임부여와 정보보호최고책임자(CISO) 지정 의무화 등의 책임관리시스템을 구축하고, 사고 시 제재수준도 강화함.
 - CEO에게 연간 IT 보안계획을 직접 승인하고 이행여부를 확인하도록 책임을 부여하고, 임원의 성과평가와도 연계하도록 유도함.
 - 정보보호최고책임자 지정을 의무화하고 정보보호최고책임자의 업무범위와 자격요건 등을 명시하는 전자금융거래법령 개정을 추진 중임.
 - IT 보완사고 관련 위반행위에 대해 대상별 제재기준을 별도로 마련하여 엄중한 제재조치를 취하며, 현행 IT 부문 실태평가 대상에서 일부 금융회사가 제외되어 있는 문제점을 개선하기 위하여 실태평가대상 범위도 확대함.
 - 전자금융거래법에 침해행위 금지의무와 처벌조항을 신설하고, 사고보고 범위와 절차 등을 명시하며, 해킹사고의 경우에도 금융회사 등이 손해배상 책임을 지도록 규정함.
- IT 보안 인프라 개선 및 내부통제 강화 등 기술적 보안관리를 강화함으로써 해킹 등 침해사고 발생 가능성을 최소화함.
 - 금융회사의 인터넷망과 업무망 분리를 단계적으로 유도하고, 시스템운영실에선 전용단말기 사용만을 허용하는 등 시스템 접속통제와 계정관리도 강화할 계획임.

- 금융회사의 IT 업무에 대한 외주계약 시 자체 IT 보안 전담조직으로 하여금 외주업체 보안관리를 철저히 하도록 하고, 외부위탁 시에는 IT 개발과 운영에 대한 내·외부 감리 실시를 유도함.
 - 불가피하게 발생한 침해사고에 대해서는 신속한 위기대응 및 재해복구 체계를 사전에 구축하여 피해 확산을 차단할 수 있도록 조치함.
 - 사이버테러에 대응하기 위하여 금융 ISAC* 참가대상에 중소 금융회사를 추가하는 한편, 해킹 정보에 대한 실시간 공유를 위해 ‘금융회사 IT 보안 지식공유센터’ 운영을 추진함.
 - 금융분야 사이버테러 대응훈련을 실제 복구 중심의 실질적 재해복구훈련으로 강화함.
- * 금융 ISAC(Information Sharing & Analysis Center)란 금융기관의 정보통신기반시설에 대한 각종 침해사고를 사전에 예방하기 위해 설립된 금융권 정보보호 전담조직임.

(금융회사 IT 보안강화 종합대책 마련, 금감원, 6/23)