

과기정통부, 금융권의 연이은 해킹사고에

사이버위협 대응체계 강화

- KISC 침해대응 인력 보강 및 24시간 비상대응체계 가동
- 보호나라, C-TAS를 통한 긴급 보안정보 전파, CISO(2.8만개사) 신고 기업 대상으로 보안점검 권고
- 금융위·금융원 등과 긴밀한 협력 및 KISC 전문인력 현장 지원 체계 유지

과과학기술정보통신부(부총리 겸 장관 배경훈, 이하 '과기정통부')는 최근 발생한 금융권 해킹 사고와 관련하여 한국인터넷진흥원(이하 'KISA')과 긴급 대응 체계를 가동하고, 유사 사고의 확산을 방지하기 위한 총력 대응에 나섰다.

현재 금융권의 해킹사고에 대해서는 소관 기관인 금융위원회, 금융감독원, 금융보안원을 중심으로 조사·대응이 이루어지고 있으며, 과기정통부와 KISA는 유사 공격의 민간 분야 확산 및 추가 피해방지를 위한 사이버위협 대응을 강화하고 있다.

먼저, 금융권에서 발생한 해킹으로 인한 추가 피해 가능성에 신속하게 대응할 수 있도록 KISA 인터넷침해대응센터(KISC)의 대응체계를 강화하였다. 주요 기업의 홈페이지 등에 대한 모니터링을 강화하고 침해사고 대응인력을 보강하는 한편, 비상출동조를 상시 대기시키는 등 비상 대응체계를 가동하였다.

또한, 보호나라와 사이버위협정보 분석·공유 체계(C-TAS*) 등을 통해 사이버 위협 정보를 제공하여 각 기관·기업이 자체적인 보안조치를 강화도록 안내하였고, CISO 신고기업(약 2.8만개)을 대상으로 보안점검 권고 메일(보안공지 링크 포함)을 발송 조치하였다.(10.4)

* Cyber Threat Analysis & Sharing : 사이버 침해사고에 신속하게 대응하기 위해 악성코드, 공격자 인터넷 주소, 최신 사이버위협동향 등을 공유하는 플랫폼(약 5,900개 회원사)

※ 보호나라(www.boho.or.kr/알림마당/보안공지) "최근 사이버공격 대비 기업 보안강화 권고(10.3)"

아울러, 금융보안원이 확인한 해외 공격자 인터넷주소(IP)에 대해서는 해당 클라우드 사업자에게 관련 위협정보를 제공하여 악성행위 차단 등 필요한 조치를 취해줄 것을 요청하였다.

한편, 과기정통부(KISA)는 금융위원회 등 관계기관과 지속적으로 정보를 공유하고 있으며, 금융위원회·금융감독원 등에서 KISA 등 전문인력 지원을 요청할 경우, 즉시 현장에 투입할 수 있도록 인력과 대응체계를 사전에 준비하고 있으며, 사고 조사 과정에서도 관계기관과 긴밀하게 협력해 나갈 예정이다.

과기정통부(KISA)는 앞으로도 금융권을 포함한 민간 정보통신서비스에 대한 사이버위협 동향을 면밀하게 모니터링하고, 사이버 위협 정보의 신속한 공유와 관계기관 간 협력을 통해 유사 사고의 발생과 피해 확산을 방지하는데 총력을 다할 계획이다.

담당 부서	정보보호네트워크정책실 사이버침해조사팀	책임자	과장
		담당자	사무관 사무관
관계 기관	한국인터넷진흥원	책임자	위협대응단장
		담당자	상황관제팀장
		책임자	위협분석단장
		담당자	위협분석팀장