국가정보원
산업기밀보호센터

사이버 기술유출 이슈레터 <세 번째 이야기....>

海外發 해킹에 의한 기술유출 대응 강화 당부

- 코로나 장기화·재택근무 활성화에 따라 海外發 해킹을 통한 기술 탈취 시도건수가 증가하고 있고 피해사례도 발생하고 있는 상황입니다.

  * ▲ MS익스체인지 취약점(3월) ▲ VPN 취약점(4~6월) ▲코로나 기술 관련 해킹시도 감지(7월)

- 최근 발생한 해킹사고들의 경우 VPN 취약점, 악성메일 배포 등의 방법으로 내부망 점거 후 우리의 소중한 기술을 탈취하는 것으로 확인되어 각별한 주의가 요구됩니다.

- 이에, 기업들은 아래와 같은 보안사항을 점검하고 조치하시기 바랍니다.

보안점검 사항

① VPN 보안 강화하기

⇒ ▲기본 계정(Default) 삭제 ▲패스워드 변경 ▲VPN 취약점(펄스시큐어 등) 패치여부 점검 ▲이중인증 권고(SMS/OTP 등)

② 해킹 이메일 대응 강화하기

⇒ ▲모르는 발신자 메일은 읽지 않기 ▲아이디/패스워드 입력 금지 ▲거래처·지인 메일이더라도 발신자가 정확한지 점검 후 유선으로 추가 확인

* 예 : √@daum.net(정상), @deum.com(비정상) , √mail.kkk.kr(정상), mail.kkk-h.kr(비정상)

③ 웹서버 점검하기 (KISA 중소기업 무료지원 서비스 활용 권고)

⇒ ▲홈페이지에 악성코드 삽입 여부 점검(문의처 : 02-405-5617) ▲홈페이지 취약점 점검(문의처 : 02-405-5665)

기술 개발은 **10년**, 유출은 **1초**

산업스파이 신고는 111
해킹을 통한 기술유출 신고도 111
한국인터넷진흥원 사이버민원센터 : 국번없이 118