국가·공공기관 DDoS 대응강화 안내

<'26.03.13(금), 의료정보보호센터>

□ 개요

○ 최근 중동상황 악화로 인해 사이버 위협이 증가하고 있어, 우리나라 대상으로도 사이버 공격이 발생할 가능성이 있는 상황

- 3.4 이후 사이버 성전을 선동하는 촉구문이 온라인(X·다크웹 등)에 유포

○ 이에 따라 DDoS 공격 발생 가능성에 사전 대비하는 차원에서 DDoS 대응강화 방안을 업무에 참조하시기 바랍니다.

□ 조치 및 당부사항

○ 기관에 DDoS 공격 발생시, 아래와 같이 조치단계를 참고하여 대응하시기 바라며, 과거 친러 해킹그룹 DDoS 공격시에는 해외IP를 차단하는 방법이 가장 효과적이었음

구분	지원주체	상세 내용
① 자체방어장비 차단	기관	• 불필요한 서비스포트(UDP,·ICMP 등) 사전 차단 • 장비내 최신 방어정책(Pattern 등) 사전 적용 • 평소 서비스수준 학습 통한 탐지 임계치(Threshold 등) 설정 최적화 • 암호화 공격 방어 위한 암호통신(SSL) 가시화 및 방어장비 연계
② 통신사 방어시스템 적용	통신사	• 통신사 방어시스템(클린존) 가입 운영시 통신사 방어서비스 적용 • 해외서비스 계획이 없다면, 통신사 관문국에서 해외IP 전량 차단

○ DDoS 공격 관련 유해IP 정보

43.128.64.0/19	43.129.160.0/19	43.130.128.0/17	43.131.0.0/18
43.132.128.0/17	43.133.160.0/19	43.133.192.0/19	43.134.128.0/17
43.135.128.0/18	43.153.0.0/18	43.153.64.0/19	43.154.128.0/17
43.156.0.0/18	43.157.0.0/17	43.159.128.0/17	43.163.128.0/17
43.166.128.0/17	43.167.160.0/19	43.167.192.0/18	43.173.118.0/23
43.173.120.0/21	43.173.164.0/24	43.173.167.0/24	43.173.172.0/22
43.173.176.0/21			

□ 기타 사항

○ 이상징후 발견시 의료정보보호센터로 신고하여 주시기 바랍니다.

○ (연락처) 의료정보보호센터

- email: cert@hisac.or.kr
- Tel: 02-6360-6280