사이버 위협 증가에 따른 보안강화 권고

2025-03-11

□ 개요
◯ 최근 크리덴셜 스터핑 공격을 통한 개인정보 유출사고가 발생하고, 국제 해커그룹의 국내 기업·기관 대상 디도스 공격으로 인한 서비스 장애 등 피해 발생 우려
- 각 기관 및 기업의 보안 담당자들이 사이버 공격 피해에 대비하여 사전 보안점검 및 대비 필요

□ 주요 사고 사례
◯ 국내 정부기관·이동통신사 대상 디도스 공격 예고 및 수행
◯ 국내 유통업체 및 구인구직 플랫폼 대상 크리덴셜 스터핑 공격을 통한 개인정보 유출

□ 보안 권고 사항
◯ 기업, 기관의 주요 시스템에 대한 보안 모니터링 및 보안강화 실시
- 시스템 및 보안장비의 안정적인 운영 현황 및 적절한 보안정책 적용 여부 확인
- 외부 스캐닝 공격에 대비한 자사 시스템의 불필요한 인터넷 노출 여부를 확인하고 접근 차단
- 취약점(인프라, OS 및 S/W 등) 존재 여부 점검 및 보안패치
- 랜섬웨어 등 공격에 대비하여 중요 데이터 백업 현황 점검
- 디도스 공격에 대비하여 KISA 및 통신사 등에서 제공하는 사전 방어서비스 이용 권고

◯ 해킹메일 예방
- 송신자 주소를 정확히 확인하고 모르는 이메일 및 첨부파일은 열람 금지
- 이메일 첨부파일 중 출처가 불분명한 파일 다운로드 자제
- 이메일 본문내 클릭을 유도하는 링크는 일단 의심하고 연결된 웹사이트 주소가 정상적인지 반드시 확인

◯ 피싱·스미싱 예방
- 문자 수신 시 출처가 불분명한 사이트 주소는 클릭을 자제하고 바로 삭제
- 의심되는 사이트 주소의 경우 정상 사이트와의 일치여부를 확인하여 피해 예방
- 휴대폰번호, 아이디, 비밀번호 등 개인정보는 신뢰된 사이트에만 입력하고 인증번호의 경우 모바일 결제로 연계될 수 있으므로 한 번 더 확인

◯ PC 및 스마트폰 보안 강화
- 운영체제 및 자주 사용하는 문서 프로그램(hwp, doc 등)에 대해 최신 업데이트 수행
- 바이러스 백신 업데이트 및 수시 검사

□ 침해사고 신고 및 지원
◯ 침해사고 및 특이사항 발생시 KISA에 신고·정보공유

- '개인성보보호 포털' 홈페이지(privacy.go.kr) → 개인성보 유출 신고

◯ 디도스 공격 사전 대비 및 공격 발생 시 디도스 방어서비스 이용
※ 영세·중소기업은 한국인터넷진흥원에서 무료로 제공하는 디도스 방어서비스 (antiddos@krcert.or.kr, 02-405-4769) 신청
※ 그 외 기관·기업은 통신사 등 민간 디도스 공격 방어 서비스 활용을 통한 사전 예방 및 대응

□ 기타 문의사항
◯ 한국인터넷진흥원 인터넷침해대응센터 종합상황실(02-405-4911)

□ 작성 : 위협대응단 상황관제팀

이전 글 목록으로 다음 글

나주본원) 58324 전라남도 나주시 진흥길 9 한국인터넷진흥원
서울청사) 05717 서울시 송파구 중대로 135 (가락동) IT벤처타워
대표번호 : 1433-25(수신자 요금 부담) [해킹 · 스팸개인정보침해 상담 118]