경보 단계는 정상, 관심, 주의, 경계, 심각으로 나뉨.

정상

- 정상적인 활동
- 위험도가 낮은 웜, 바이러스 발생
- 위험도가 낮은 해킹 기법, 보안 취약점 발표

관심

- 웜, 바이러스, 해깅 등에 의한 피해 발생 가능성 증가
- 해외 사이버 공격 피해 확산. 국내 유입 우려
- 정보 유출 등 사이버 공격 시도 탐지
- 국내외 정치, 군사적 위기상황조성 등 사이버 안보 위해 가능성 증가

주의

- 다수 기관의 정보통신망 및 정보 시스템 장애 발생
- 다수 기관의 정보유출 등 침해사고 확산 가능성 증가
- 국내외 정치, 군사적 위기 발생 등 사이버 안보 위해 가능성 고조

경계

- 복수 ISP망 또는 기간망에 피해 발생
- 대규모 피해 확산 가능성 증대
- 정보유출 등 대규모 침해 사고 발생
- 복수 분야에서 광범위한 피해 발생 등 대규모 피해로 확대될 가능성이 높아 다수 기관의 공조 대응이 필요한 경우

심각

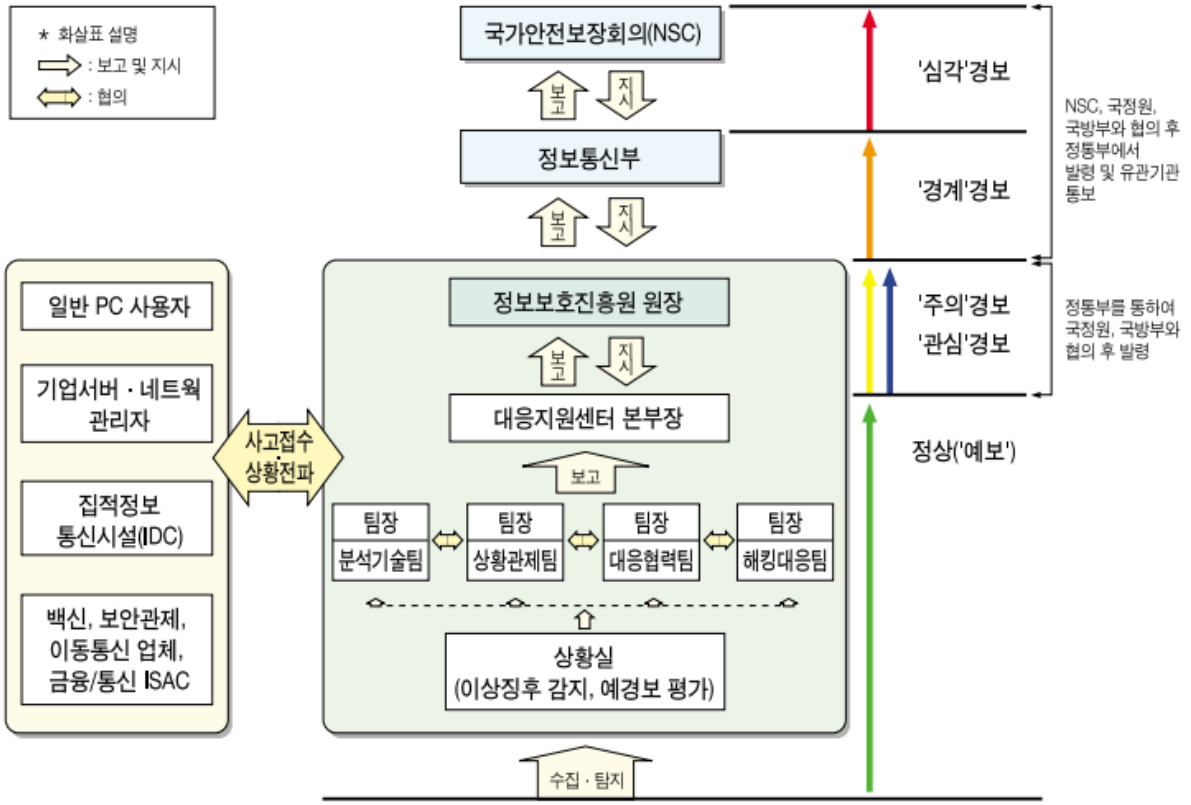
- 전국적인 네트워크 및 정보 시스템 사용 불가능
- 주요 핵심기반시설의 피해로 국민 혼란 발생
- 정보 유출 등 대규모 침해사고가 전국적으로 발생
- 국가적 차원의 평가와 조치가 필요하다고 판단되는 사고 발생

경보 발령 과정

소속기관, 산하기관, 지방자치단체 등은 이상징후, 전산망 장애, 사이버 공격 징후 등이 포착되면 상급기관에 상황 조치결과를 통보. 상급기관은 조치사항을 종합, 국가사이버안보센터에 통보. 보고를 받은 측에서 다른 기관과 협의 후 경보 발령.

아래는 한국인터넷진흥원이 발생한 [민간사이버안전매뉴얼]에서 발췌한 그림.

(4) 민간분야 경보발령 체계



경보 발령 후 전파 방법

웹, 이메일, 핸드폰 문자 / 팩스 / 보도기관, ISP 등을 이용한 경보 현황 안내가 이루어짐.

경보 단계 상향 및 하향 변경

경보 단계는 웜, 바이러스, 해킹 등 침해사고의 진행상황에 따라 변경될 수 있음. 상향 변경의 경우 현재보다 상황이 악화되어 사이버 공격의 피해 또는 피해 가능성이 커질 때 변경됨. 하향 변경은 현재보다 상황이 호전되어 사이버 공격의 피해 또는 피해 가능성이 줄어들었을 때 변경됨.

경보 단계별 대응 요령

아래는 한국인터넷진흥원이 발생한 [민간사이버안전매뉴얼]에서 발췌한 그림.

[표 2-2-1] 경보 단계별 대응 요령

		경보			
단계	정 상 (Green)	관 심 (Blue)	주 의 (Yellow)	경 계 (Orange)	심각 (Red)
대응요령	• 서버 네트워크, 보안장비 및 보안정책 등 점검 • 보안 패치(운영 체제, 응용 SW) • 바이러스 월 업데이트 • 침입차단시스템 및 침입 탐지 시스템 모니터링 • 서비스 포트 모니터링 • 웜 · 바이러스 취약점 동향 파악	• 기업내부 직원 및 서비스 관련 고객에게 "관심" 경보 전파 • 백신프로그램 및 바이러스 월 업데이트 • 해당 S/W 취약점 보안패치 • 기업 내부 서비스에 지장을 주지 않는 해당 포트 차단 권고 • 침해사고대응팀 비상연락망 비상 점검 ※ "정상" 단계대응 요령 포함	• 기업내부 직원 및 서비스 관련 고객에게 "주의" 경보 전파 • 백신프로그램 · 바이러스 월 업데이트 및 점검 • 해당 S/W 보안 패치 • 기업 내부 서비스에 지장을 주지 않는 해당포트 차단 • 모든 서버 및 관리용 시스템 이상 유무 점검 ※ "관심" 단계대응 요령 포함	• 기업내부 직원 및 서비스 관련 고객에게 "경계" 경보 전파 • 언론보도 주시 • 모든 서버 및 관리 시스템 지속적 점검 • 기업내 PC사용 최소화 권고 • 침해사고대응팀 비상연락망 비상 점검 ※ "주의" 단계 대응 요령 포함	• 기업내부 직원 및 서비스 관련 고객에게 "심각" 경보 전파 • 언론보도 주시 • 전체 네트워크 24시간 모니터링 및 해당 포트 차단 • 감염된 시스템 LAN에서 분리 • 침해사고대응팀 비상연락망 비상 점검 ※ "경계" 단계 대응 요령 포함

② 사고 발생 시 대응 요령

=> 최근 공격 사례(4가지) 기반으로

공격 유형, 공격 탐지 방법, 대응방법 정리

1. 이력서 사칭한 'LockBit 3.0' 랜섬웨어

https://www.boannews.com/media/view.asp?idx=111762&page=1&kind=1

랜섬웨어와 정보탈취 악성코드를 포함한 메일이 기업을 대상으로 해 이력서를 사칭. 첨부파일을 확인하면 한글 파일, 엑셀 파일 아이콘으로 위장한 실행 파일 2개와 이미지 파일 하나가 2번 압축되어 있음. 피해자가 실행파일을 실행하면 악성행위를 수행. 랜섬웨어는 파일을 암호화. 악성코

드는 사용자의 시스템 정보, 브라우저 정보를 수집해서 C&C 서버로 전송.

- 공격 유형: 랜섬웨어, 스파이웨어
- 공격 탐지 방법: 첨부파일은 압축되어 있어서 다운로드 시점에 탐지는 어려울 거 같음. 악성코드는 C&C 서버로 피해자의 정보를 전달하기 때문에 그 패킷을 탐지할 수 있음.
- 대응 방법: 파일이나 url이 첨부된 메일은 의심하기. 실행 전 확장자 확인. 허용된 서버 외로는 개인정보를 반출하지 못하도록 차단.

2. 북 해커조직 APT37, 만능 기능 '돌핀' 백도어로 남한 정찰

https://www.boannews.com/media/view.asp?idx=112200&page=1&kind=1

돌핀은 백도어로 이동식 장치 모니터링, 주요 파일 반출, 키로깅 등 스파이 기능을 수행. C&C 통신을 위해 구글 드라이브 악용. 돌핀은 공격자가 원하는 공격 대상에게 수동 구축되어 감염된 시스템의 드라이브에서 파일을 검색, 구글 드라이브를 통해 파일을 반출.

- 공격 유형: 스파이웨어
- 공격 탐지 방법: 돌핀은 수동 구축되기 때문에 그에 대한 로그가 남을 것. 설치 로그를 통해 탐지. 파일을 검색하고 파일을 외부로 반출하기 때문에, 구글 드라이브에 접근한 로그를 통해서 탐지.
- 대응 방법: 유출하는 구글 드라이브는 공격자의 구글 드라이버일 것으로 예상됨. 허용된 서버 외로는 개인정보를 반출하지 못하도록 차단.

3. 러시아 지지하는 해킹 단체, 미국 공항 웹사이트 15개 마비시켜

https://www.boannews.com/media/view.asp?idx=110553&page=2&kind=1

미국 주요 공항이 운영하는 웹사이트를 디도스 공격. 수시간 동안 사이트 접속 불가. 항공 운영 자체에는 문제가 없었음.

- 공격 유형: 디도스
- 공격 탐지 방법: 동일하거나 비슷한 패킷이 동시다발로 들어올 때, 그 양이 일정 시간 내 공격 인정 횟수를 넘는지 확인.
- 대응 방법: 동일하거나 비슷한 패턴의 패킷이 과도하게 전송될 경우 해당 ip는 차단.

4. 국내 1위 가상자산 거래소 '업비트' 사칭해 카카오톡 계정정보 노린다

https://www.boannews.com/media/view.asp?idx=106095&page=4&kind=1

업비트를 사칭한 피싱 메일을 발송하여 첨부된 링크를 클릭하면 실제 업비트 사이트와 유사한 가짜 사이트로 넘어가는 공격. 로그인을 위해 카카오톡 로그인을 유도. 피해자가 개인정보를 입력하면 해당 아이디와 비밀번호는 피해자의 ip와 함께 공격자에게 전송됨.

- 공격 유형: 피싱 사이트를 통한 정보 탈취
- 공격 탐지 방법: 사용자의 로그인 정보가 공격자의 서버로 전송될 테니 그 패킷을 탐지.
- 대응 방법: 스팸 메일 차단할 수 있도록 메일 필터 사용하기.