| 산업통상자원부 http://www.motie.go.kr | 보도참고자료 | 평창 |
|---|---|---|

**배포 즉시** 보도하여 주시기 바랍니다.

| 배포일시 | 2017. 5. 16.(화) | 담당부서 | 정보보호담당관실 |
|---|---|---|---|
| 담당과장 | 장근무 과장(044-203-5590) | 담 당 자 | 김용완 서기관(044-203-5591) |

# 랜섬웨어 확산에 따른 공공기관 사이버 대응현황 점검

□ 산업통상자원부는 **랜섬웨어 공격의 전 세계적 확산**과 관련하여 **5.16일 정만기 1차관 주재**하에 **41개 전 산하 공공기관의 사이버 대응현황을 점검**하였음

* 회의개요 : 5.16(화) 10:30분 엘타워, 정만기 1차관 주재, 41개 공공기관 부기관장 참석

○ 동 회의에서 정만기 차관은 현재 **산업부 및 산하 공공기관에 대한 랜섬웨어 피해는 없으나**, 변종의 출현 및 새로운 유형의 공격 가능성이 상존하는 만큼 각 기관별로 **사이버 대응태세를 더욱 강화**하도록 요청하였음

* 워너크라이(WannaCry)라 불리는 금번 렌섬웨어는 MS사 윈도우 OS의 취약점을 공격하여 자기복제를 통해 네트워크로 전파가 가능한 악성코드임

□ 산업부는 지난 4월 중순 **미국 국가안보국(NSA) 해킹 툴의 유출 보도** 이후, **동 유형의 공격 가능성에 대비**하여 **지난 4월 16일 대응방안*을 마련**하고 **전 산하기관에 탐지룰을 배포**하는 등 **적극 대응**하여 왔음

* 윈도우 방화벽 포트차단, 개인PC 보안설정 강화, 윈도우 OS 보안 업데이트 등

○ 이번 랜섬웨어 공격의 확산으로 **국가 사이버 위기 경보가 5.14(일) 18:00부로 관심단계에서 '주의'로 격상**된 바, 산업부는 **국정원, 한국인터넷진흥원 등과도 공조를 강화**하고,

○ 향후에도 **한전, 한수원, 발전 5사 등 11개 정보통신기반시설 보유기관***은 **3중의 보안관제 시스템**(국정원-산업부 사이버안전센터- 11개 자체 관제센터)을 통해 **긴밀히 협조하고 유사시 대응체계**를 더욱 강화할 계획임

* 한전, 한수원, 발전5사, 가스공사, 지역난방공사, 전력거래소, 한전기술

**< 첨부 > 공공기관 회의 참여기관 현황**

**첨 부** 공공기관 회의 참여기관 현황(41개 기관)

| 구분 | 기관명 | 구분 | 기관명 |
|---|---|---|---|
| 1 | 한국전력공사 | 22 | 한국에너지공단 |
| 2 | 한국가스공사 | 23 | 한국가스안전공사 |
| 3 | 한국석유공사 | 24 | 한국광해관리공단 |
| 4 | 한국광물자원공사 | 25 | 한국디자인진흥원 |
| 5 | 한국지역난방공사 | 26 | 한국산업기술진흥원 |
| 6 | 한국수력원자력 | 27 | 한국산업기술평가관리원 |
| 7 | 한국중부발전 | 28 | 한국산업단지공단 |
| 8 | 한국서부발전 | 29 | 한국석유관리원 |
| 9 | 한국동서발전 | 30 | 한국세라믹기술원 |
| 10 | 한국남부발전 | 31 | 한국에너지기술평가원 |
| 11 | 한국남동발전 | 32 | 한전원자력연료 |
| 12 | 대한석탄공사 | 33 | 강원랜드 |
| 13 | 한국전력기술 | 34 | 한국산업기술시험원 |
| 14 | 한전KPS | 35 | 한국로봇산업진흥원 |
| 15 | 한전KDN | 36 | 전략물자관리원 |
| 16 | 한국가스기술공사 | 37 | 한일산업기술협력재단 |
| 17 | 한국무역보험공사 | 38 | 한국원자력문화재단 |
| 18 | 한국원자력환경공단 | 39 | 한국스마트그리드사업단 |
| 19 | 한국전력거래소 | 40 | 의료법인 한전의료재단 한일병원 |
| 20 | 한국전기안전공사 | 41 | 한국전력 국제원자력대학원대학교 |
| 21 | 대한무역투자진흥공사 | | |

try of Trade,
try and Energy