

침해사고(랜섬웨어 감염 등) 예방 대책

<진료정보침해대응센터>

[업무용 PC 등 정보시스템 보안조치]

- ❶ 병원 내 PC OS(윈도우즈 등) 최신 보안패치 적용 및 유지관리
- ❷ PC OS의 기본 계정 삭제(administrator 등) 및 비밀번호 복잡도 설정* 권고

※ 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성([개인정보위원회개인정보의 기술적·관리적 보호조치 기준])

- ❸ 데이터베이스(MS-SQL)가 외부에서 접속 불가하도록 조치 필요

※ 외부에서 접속 가능한 데이터베이스의 포트(1433 등)를 이용하여 내부 침투 및 감염사례 빈번히 발생

☞ (접속차단) 외부에 DB 서비스 포트 개방 시 침투 시도 공격에 노출되므로 접속 차단 필요

☞ (DB계정) DB 계정을 별도로 생성하고 비밀번호 복잡도 설정

☞ (최신버전) 최신 패치 적용 및 최신 버전으로 데이터베이스 업그레이드 권고

- ❹ 공유 폴더 사용 자제(랜섬웨어의 병원내 확산에 활용됨)

- ❺ 원격접속 SW(RDP, 팀뷰어, 애니데스크 등)를 이용한 원격 유지보수 등의 업무를 지양하고 병원에 현장 방문하여 업무 처리 권고

※ 원격접속 업무 후, 랜섬웨어 감염사례 빈번히 발생

☞ (사용제한) 평시 원격접속 설정 비활성화 권고, 원격제어 SW 사용 자제 (불가피할 경우 일시적으로 허용 후 차단 등 사후 관리 철저)

☞ (접속계정) 원격 접속 계정을 별도로 생성하고 비밀번호 복잡도

설정

* 윈도우 기본 사용자 계정(Administrator, GUEST 등)으로 원격접속 허용 금지

⑥ 진료정보에 대한 백업 조치 필요

☞ (분리보관) 백업 후, PC(서버)와 분리하여 보관 필요

* (참고) 사이버 공격 대응을 위한 중소기업 정보시스템 백업 지침(TTAKO-120340)

⑦ 병원 내 PC에 백신 SW 설치 및 정기적 업데이트 적용

※ 백신 및 안티랜섬웨어 SW 도입 권고

⑧ 병원 내 주요 업무용 PC에서 인터넷, 이메일 열람, USB 사용 등 자제

※ 인터넷, 이메일, USB 저장매체를 통한 랜섬웨어 감염사례 다수

[보안장비 및 네트워크 보안조치]

⑨ 보안장비(방화벽 등) 도입 및 불필요한 서비스 포트 차단 등 권고

☞ 업무적으로 외부 개방이 불가피한 ·포트 외 불필요한 포트 차단 권고

* SMB(TCP 135, 445), RDP(TCP 3389), FTP(TCP 21), TELNET(TCP 23),
DB 서비스 포트(1433, 1434) 포트 등

⑩ 유·무선 공유기 사용 시 기본 비밀번호 변경 및 복잡도 설정, 공유기가 제공하는 보안기능 활성화