긴급공지 랜섬웨어 관련 사례 2023.11.22

1. 랜섬웨어 감염으로 인한 피해 발생이 보고되어 안내 드립니다.

- OO병원에서 랜섬웨어 감염 발생.
- 진료마비 및 의무기록 조회 불가 발생.
- 해커 집단으로부터 암호키 비용으로 비트코인 요구 받음.
- 비트코인을 지불한 후 암호키를 받아서 복구함.
- 병원 승인 없이 접속 가능한 원격접속 프로그램의 해킹으로 랜섬웨어 감염 의심되고 있음.

2. ㈜비트컴퓨터에서는 랜섬웨어 관련 공지를 통해 수 차례 보안에 관해 권고를 드린 바 있습니다.

3. ㈜비트컴퓨터에서는 병원의 명시적 승인이 있어야만 원격 접속이 가능한 방식을 이용하고 있습니다.

[상담원 번호 (02)번을 클릭해 주세요] 와 같이 병원의 승인이 있어야 원격 접속이 가능한 방식 입니다.

4. 보안을 위한 권고사항

- EMR에 접속하는 모든 협력업체(PACS, CRM, 동의서 관리업체 등)에 병원의 승인없이 접속 할 수 있는 원격 접속 프로그램의 사용금지를 요구 하시기 바랍니다. (사용금지 요구는 공문을 통해 명시적으로 수행 하시기를 권고 드립니다.)
- EMR업무용 PC의 개인용도 사용을 금지 하셔야 하며 USB포트 사용 또한 필수PC 외에는 사용불가 조치 하시기를 권고 드립니다.
- 개인 E-Mail을 EMR업무용 PC에서 열어 보는 것 또한 적정 보안교육 이수자 외에는 금지 하시기를 권고 드립니다.
- 원내 보안담당자를 선임하시어 필요한 교육을 이수 하시고 적용 하시기를 권고 드립니다.
- 적정 보안교육은 아래의 사이트 등 여러 종류가 있으니 참고하시기 바랍니다.
  https://bitcampus.com/lecture/?seq=89
  https://bitcampus.com/lecture/?seq=631

5. 감염 발생시에 대한 대비책 권고

- 보안을 위한 권고사항을 엄수 하는 것은 감염의 확률을 낮추는 것일 뿐 100%방어하는 것이 아님을 인지 하셔야 합니다.

- 원내 백업 점검 담당자를 선임하시기 바랍니다.
- 선임된 담당자는 백업정책 및 백업 경로 등을 문서상으로 인지/관리하셔야 합니다.
- 선임된 담당자는 1일 1회 이상 백업의 정상 여부를 확인하셔야 합니다.
- 백업된 파일은 NAS 장비 또는 외장하드 등 원내 EMR 망과 분리하여 보관되어야 합니다.
- 백업파일로 복구가 진행될 경우 백업시점부터 복구시점 까지의 Data는 손실됨을 인지하셔야 합니다.

6. 상기 권고를 유념하시어 큰 피해를 예방하시기를 다시 한번 당부 드립니다.

감사합니다.