2024년 의료환경에서의 정보보안 키워드 10

- **생성형 AI 보안, CPO 지정 의무화, 「개인정보 보호법」 위반 과징금 제도 변경, 의료기관 ISMS-P 인증, 의료분야 공급망 공격, 다중 인증, 업무망과 인터넷망 분리, 원격의료 보안, 업무연속성과 회복탄력성, Never Trust & Always Verify**

병원정보보안협회는 올해의 의료환경에서 정보보안 키워드를 선정하여 발표하였다. 정보보안 키워드 선정은 2023년 12월 11일부터 2023년 12월 31일까지 협회 회원을 대상으로 키워드를 공모하였고, 트렌드와 중요도를 반영한 올해의 키워드 10개를 최종 선정하였다. 병원정보보안협회에서 선정한 올해의 정보보안 키워드는 다음과 같다.

1. 생성형 AI 보안

Chat GPT로 대표되는 생성형 AI 기술의 발전은 다양한 분야의 혁신을 가져왔지만 보안에 대한 전문지식 없이도 손쉽게 악성코드를 제작하거나 음성 위·변조 등 사회공학적 방법을 이용한 다양한 사이버 공격에 악용될 가능성이 커졌음을 의미한다. 잘못된 정보, AI 모델 악용, 데이터 유출 등은 생성형 AI 기술의 오용은 개인정보 보호를 위협할 뿐 아니라 사회적 혼란을 조장하고 악용될 수 있어 사이버 범죄와 다양한 보안 위협이 야기될 것으로 전망된다.

이에 따라 기업의 기밀정보 또는 개인정보 등 민감한 정보의 입력을 금지하고 생성물에 대한 정확성, 윤리성, 적합성 등에 대한 검증 및 생성형 AI를 악용한 사이버 범죄에 적극 대응할 수 있는 관련 보안 기술의 필요성이 중요해지고 있다.

2. CPO 지정 의무화

올해 3월 15일부터 상급종합병원에 CPO(Chief Privacy Officer, 개인정보 보호책임자) 지정이 의무화된다. 의료기관이 보유한 민감하고 중요한 개인정보 및 의료정보 보호의 중요성이 강조되고 상황에서 CPO에게 요구되는 자격요건을 도입해 CPO의 전문성과 독립성을 갖추게 하여 의료기관의 개인정보 보호 수준이 한층 강화되는 계기가 될 수 있을 것으로 전망된다.

개인정보보호위원회에서는 올해 초 상급종합병원 CPO 지정을 위한 가이드라인을 만들고 의료기관에 배포할 예정이다.

3. 「개인정보 보호법」 위반 과징금 제도 변경

작년 9월 15일 「개인정보 보호법」이 전면 개정되면서 법규 위반 시 과징금 제도가 변경되었다. 과징금 상한액을 위반행위와 관련된 전체 매출액을 기준으로 하여 최대 3%로 산정하도록 변경하였다. 이러한 위반 행위는 발생할 수 있으며, 제재 시 천문학적인 비용을 납부할 수 있기 때문에 이에 대한 대응책 마련이 시급하다. 개인정보보호 배상책임보험 가입 등을 통해 이를 대비하는 것이 필요하고 과징금 부과 시 이의 신청 등 적극적인 대응을 통해 금액을 경감하는 것이 중요하다.

4. 의료기관 ISMS-P 인증

의료기관에서의 ISMS-P 인증(정보보호 및 개인정보보호 관리체계 인증)이 본격화될 전망이다. 작년 8월 국립암센터는 주요 빅데이터 운영시스템인 임상연구데이터웨어하우스(Clinical Research Data Warehous)와 가명정보 결합전문시스템에 대해 ISMS-P 인증을 획득했다.

또한 분당서울대학교병원은 작년 10월 국내 최초로 EMR을 포함한 병원정보시스템 전체에 대하여 ISMS-P 인증 심사를 받았으며 발견된 결함사항을 조치하고 인증위원회의 최종 판정을 기다리고 있다.

이처럼 의료기관에서의 ISMS-P 인증 요구가 계속됨에 따라 작년 12월 개인정보보호위원회, KISA, KAIT와 분당서울대학교병원, 서울대학교병원, 삼성서울병원, 연세의료원, 국립암센터 등이 함께 의료기관의 ISMS-P 인증범위 설정 등에 대한 논의를 가졌다. 올해는 의료기관의 ISMS-P 인증 획득이 본격화될 전망이다.

5. 의료분야 공급망 공격

최근의 사이버 공격은 피해가 해킹 당한 조직에만 국한되지 않고 그 조직과 관련 있는 모든 것들에 영향을 끼치고 있다. 그렇게 때문에 강조되는 것이 바로 공급망 보안으로 복잡한 공급망의 한 지점만 침투하면 공급망에 연결된 모든 조직을 공격할 수 있고 대규모 피해를 야기할 수 있다.

최근 국내 다수의 침해 사고 사례에서 EMR, PACS 등 의료정보시스템의 취약점을 이용한 공급망 공격이 보고되고 있으며, 의료분야에서의 사이버 공격은 의료정보 유출, 결제 정보 손실 등이 발생하여 진료 중단 및 환자 피해로 이어질 수 있으므로 이에 대한 대응이 강조되고 있다.

6. 다중 인증

다중 인증(MFA, Multi Factor Authentication)이란 정보 자원에 대한 접근 권한을 부여받기 위해 적어도 두 가지 이상의 확인 요소를 제공해야 하는 인증 방법이다. 의료분야에서는 의료정보시스템을 중심으로 ID와 패스워드를 입력하는 전통적인 지식 기반 인증 방식을 사용하였으나 사용자 인증에 대한 다양한 문제가 발생하여 새로운 인증 체계가 요구되고 있다. 특히 ID 공유로 나타나는 오남용과 보안 취약점을 해결하기 위한 FIDO(Fast Identity Online) 등이 해결책으로 떠오르고 있다.

7. 업무망과 인터넷망 분리

업무망과 인터넷망 분리는 랜섬웨어, 해킹 등으로부터 내부 시스템을 보호하고 개인정보 유출을 근본적으로 해결할 수 있는 가장 효과적인 방법으로 알려져 있다. 「개인정보 보호법」에서는 외부에서 개인정보처리시스템에 접속할 수 있고 100만 이상 개인정보를 보유하는 경우 망분리를 하도록 되어 있다. 이전까지 의료정보시스템은 내부에서만 접속할 수 있는 폐쇄적인 환경에서 운영되었으나, 최근 모바일 시스템, 재택근무 등으로 인하여 외부에서 의료정보시스템에 접속을 허용하는 방향으로 변화하고 있다. 이에 따라 많은 병원들이 망분리를 도입 추진 중이거나 검토하고 있다.

8. 원격의료 보안

코로나19의 유행 이후 전 세계는 비대면 사회로 급속히 전환되었고, 의료 분야 역시 많은 영향을

받아 우리나라에서도 원격의료에 대한 논의가 본격화되고 있다. 정부는 코로나19 상황에서 한시적으로 원격진료를 허용하고 있어 향후 이에 대한 구체적인 논의가 필요할 전망이다.

의료정보는 환자의 생명과 직접적으로 연결되기 때문에 무엇보다 신뢰성 보장이 필수적이라 할 수 있다. 원격의료를 위해서는 사용자 인증, 민감정보의 유출 방지, 의료사고 발생 시 책임소재 등이 명확히 규정되어야 한다.

9. 업무연속성과 회복탄력성

2022년 카카오 서비스 중단 사고, 2023년 정부 행정전산망 네트워크 장애로 인하여 정부와 기업의 신뢰도 하락과 대국민 서비스의 불편함으로 인해 사회 전 분야에 대한 재난에 대한 대비 및 복구의 중요성이 강조되고 있다. 특히 의료환경에서는 재난 발생 시 회복탄력성을 강화하여 재난을 견디고 의료서비스를 계속할 수 있는 업무연속성에 대한 요구가 높아지고 있다. 특히 EMR 도입 후 병원의 모든 프로세스가 IT에 의존적인 상황에서 IT 서비스의 안정적인 운영은 병원의 업무연속성과 회복탄력성을 확보하는데 필수적이라 할 수 있다. 2024년은 작년과 마찬가지로 의료기관의 업무연속성과 회복탄력성을 점검하고 보완하는 한 해가 될 것이다.

10. Never Trust & Always Verify

최근 병원의 정보 환경은 모바일 솔루션의 확산, 클라우드 의료정보시스템 도입, 코로나로 인한 재택근무 등으로 인하여 내·외부 네트워크 경계가 허물어지게 되었다. 기존의 경계 보안에서는 병원 내부망은 기본적으로 신뢰하고 외부는 믿지 않는 방식으로 운영되었지만, 내·외부 네트워크 경계가 모호해지면서 전통적인 경계 보안의 한계를 극복하기 위한 새로운 보안 모델이 필요하게 되었다. 의료기관이 사이버 공격의 대표적인 표적이 되고 있는 상황에서 민감한 의료정보를 안전하게 보호하는 것은 의료 IT 보안의 새로운 도전 과제가 되고 있으며 제로 트러스트가 이에 대한 해결책으로 떠오르고 있다.