제106호 2015년 7월 3일

NIA

개인정보보호 주간동향

NIA 한국정보화진흥원

Contents

국내 주요뉴스

해외 주요뉴스

1 국내 주요뉴스

KIPFA, IoT 기술환경 인식조사 결과 보고서 발표 (ACROFAN)

- 한국인터넷전문가협회(KIPFA), 리서치 전문기관 이언인사이트와 인터넷 관련 분야 전문가들을 대상으로 공동조사 한 'IoT분야의 기술과 환경에 대한 인식조사' 결과 공개
- IoT 상용화 시 우려되는 점으로는 '해킹 위험(82.0%)'과 함께 '가격 부담(56.7%)', '호환성 저하(40.0%) 순으로 나타남
- 국내 IoT 기술 상용화에 있어 '개인정보보호 관련 법규'와 '전문인력 양성' 수준을 상대적으로 낮게 평가되었으며, 정보보호 및 기술표준화 정책과 인적 인프라 측면에서 전반적인 상용화 준비가 미비하다는 의견

출처

http://www.acrofan.com/ko-kr/live/news/20150630/00000032

"교사 동의 없이 일방 설치... 보육실 CCTV 훼손 무죄" (서울경제)

- 대법원 1부는 업무방해 혐의로 기소된 장모(53)씨에 대한 상고심에서 무죄인 원심을 확정
- 교사들의 반대에도 일방적으로 화장실 입구와 교사의 개인 사무공간, 교사가 개인적으로 사용하는 컴퓨터의 모니터 부분도 촬영할 수 있는 위치에 CCTV 설치
- 재판부는 "보육은 영유아의 이익을 최우선적으로 고려해 제공돼야 한다"면서도, "CCTV 설치를 통해 확보되는 영유아의 이익이 교사들이 일방적으로 CCTV 촬영대상이 되지 않을 이익에 무조건 우선한다고 단정할 수 없다"고 설명

출처

http://economy.hankooki.com/lpage/society/201506/e2015062918080593800.htm

2 해외 주요뉴스

미국 개인정보 유출 관련 규제 동향에 관한 보고서

● 개요

- 익스페리안 데이터 브리치 레솔루션(Experian Data Breach Resolution)은 최근 미국의 주 및 연방 차원에서 벌어지고 있는 개인정보유출 통지 관련 규제 동향을 분석한 보고서 발간

● 주요내용

- 익스페리안 데이터 브리치 레솔루션은「Government Focus on Cybersecurity Elevates Data Breach Legislation」제하의 보고서를 통해 기업을 대상으로 개인정보유출 제도 개선 동향을 안내하고 있음

- 개인정보 유출 관련 법률은 주(州)별, 부문별로 특화 · 세분화되는 추세에 있으며, 이와 동시에 유럽연합, 호주, 브라질 등 세계 주요국 역시 개인정보 유출 통지제도의 개선을 모색하고 있어, 글로벌 기업에게 큰 영향을 미칠 수 있다고 지적
- 개인정보 유출사고가 발생할 경우, 법률고문과 같은 외부 전문가를 활용하는 것이 필요하다고 제언

- 보고서의 핵심 내용을 요약하면 다음과 같음

① 복잡하고 일관성도 없는 주(州)의 개인정보 규제

- 콜롬비아와 푸에르토리코 지역에서 개인정보 유출 사고가 발생하면 해당 기업은 무려 49개의 일관성 없는 규제를 적용받게 됨
- 이와 더불어 주 입법부는 신원도용 위험이 있는 정보를 엄격하게 관리하기 위해 규제를 강화하고 있는 상황
- 예컨대 일리노이주는 금융 관련 신원파악 정보에 마케팅 정보와 같이 덜 민감한 정보를 포함시키는 방안을 검토하고 있음

※ 연방국가인 미국은 50개의 각 주가 해당 주의 법으로 개인정보 및 데이터 관리를 규제하고 있음. 또한 이러한 규제는 주로 산업 분야별로 각기 제정된 법률에 의하여 규제되고 있으며, 그 규제의 범위도 각 법률마다 상이함. 연방 정부 차원에서는 연방거래위원회(FCC)가 FCC의 관리·감독을 받는 법인에 대해 개인정보보호를 감독하며, 법률 위반시 이를 불공정 또는 기만적 거래행위(unfair or deceptive trade practices)로 규정하여 단속하고 있음

② 연방 차원의 규제 마련에 적극적인 의회

- 의회는 개인정보 유출 관련 규제를 국가적 표준으로 제정하고자 몇 가지 입법 활동을 시도

하고 있음

- 법안의 세부사항에 대한 합의가 이루어지지 않아 입법이 다소 지연되고 있으나, 의원들의 우선 관심사임은 확실한 상황임
- 일부 보안 관련 커뮤니티에서 개인정보 유출 통지와 관련하여 연방 차원의 규제 마련에 반대하고 있음

③ 세계 주요국의 개인정보 유출 관련 처벌 강화

- 각국의 개인정보 유출 관련 내용의 개정은 특히 글로벌 기업에 영향을 크게 미칠 것으로 보임
- 유럽연합의 경우, 모든 상업부문을 대상으로 24시간 공지를 요구하는 수준으로 개인정보 보호법을 개정하려 하고 있음
- 브라질은 지난 2월에 새로운 개인정보보호 규칙을 공개한 바 있으며, 호주도 개인정보 유출 공지 표준을 강화하는 내용으로 제도를 개선하고자 함

시사점

- 각 주별로 개인정보보호 관련 법제도를 운영하고 있는 미국은 규제 유형이 다양하고 변수가 많아 연방차원의 단일 규제 마련의 필요성이 제기되고 있는 실정
- 우리나라의 경우 최근 징벌적손해배상제도를 새로이 도입하는 등, 개인정보 유출 기업에 대한 제재를 강화하고 있음
- 실질적인 개인정보 보호를 위하여 제도 간 상호운용성을 검토하고, 해당 규제가 일관성 있게 시행되고 있는지에 대해 점검하는 등 선진적인 법제도 정비를 위한 노력이 필요

출처

http://money.cnn.com/news/newsfeeds/articles/prnewswire/LA39438.htm

http://www.experian.com/assets/data-breach/white-papers/experian-data-breach-legislative-white-paper-2015.pdf

WEDI, 의료 관련 사이버 공격에 대한 대응 전략 초안 보고서

● 개요

- 미국의 전자정보 교환을 위한 워크그룹(Workgroup for Electronic Interchange; 이하 'WEDI')은 의료기관이 직면하고 있는 사이버 공격에 대한 방어를 위해, 이에 대한 대응 전략에 대한 초안 보고서 발표

● 주요내용

- WEDI의 의장이자 CEO인 Devin Jopp은 의료영역에 있어서의 주파수 범위 및 사이버 공격의 정교함이 지속적으로 성장하고 있으며, 더 이상 사이버 공격의 위험성은 IT에 국한되는 문제가 아니라는 점을 성명을 통해 밝힘
  - WEDI의 리포트에 따르면 2010년부터 2014년까지 약 3,700만 건의 의료기록이 데이터 침해로 인해 노출되었으며, 2015년 1분기에는 99,000,000개의 의료기록이 노출되었음
  - 미국의 전 대통령 빌 클린턴 또한 '올해 미국 건강 보험 계획'에 대한 기조연설을 통하여 의료 영역에 있어서의 주요 기술 과제로 사이버 보안을 선정하는 등 의료영역에 있어서의 건강 데이터가 침해 또는 유출될 경우 그 피해가 심각할 수 있다고 설명한 바 있음
  - Fierce Health IT 보고서에 따르면, 현재 의료 관련 조직들은 사이버 위협의 대안과 방안 마련을 위한 조직적인 준비를 하고 있으나, 대부분의 병원은 여전히 이 문제에 대한 프로그램에도 불구하고 어려움을 겪고 있는 실정임. 이에 따라 구체적 전략 대응 방안 수립의 필요성이 제기됨

- 본 보고서에서는 의료영역에서의 사이버 보안과 관련하여 세 가지 주요사항에 대하여 설시하고 있음
  - ① 사이버 공격과 방어의 수명 주기에 대한 분석 ② 사이버 공격의 유형에 대한 분석 ③ 사이버 공격 예방의 문화 구축
  - 사이버 공격 예방의 문화를 구축하기 위해 본 보고서는 사이버 공격의 유형을 분석하고 이에 대한 지속적인 모니터링을 통하여, 이에 대응하기 위한 방법으로 유기적인 단계를 제시
  - 보안 아키텍처는 이러한 공격행위에 대하여 단계별로 신속하고 정확하게 방어하고 대응해야 함

- 사이버 공격으로부터의 실질적 대응을 위해 기존의 '네트워크 레벨' 뿐만 아니라 실제 피해가 발생하고 있는 '엔드포인트 영역'에 까지 광범위한 대응의 전략을 구체화하고자 함.

이러한 방안으로서 크게 세 가지 전략 방안을 제시하고 있음

- 첫째로, 네트워크 연결 전에 위협을 완화하는 등 운영 체제 및 서버와 엔드 포인트에서의 맬웨어 방지, 웹 필터링, 안티 바이러스 소프트웨어 업데이트 및 취약성, 감염의 위험을 줄이기 위한 패치 등의 기초적인 통제 및 관리
- 둘째로, 모든 사이버 공격에 대한 완벽한 사전 대응방안의 한계를 인식하고, 사이버 공격 시에 신속하고 정확하게 이를 인지하고, 보안 직원에게 통보할 수 있는 대응 체계 구축과 범위를 식별, 이를 통해 다른 보안의 적용 지점을 구체화함으로써 부수적인 피해의 예방
- 셋째로, 모든 네트워크 침해 위협에 대한 반응을 요구. 새로운 위협을 감지하고 테스트 할 수 있는 샌드 박스(Sandbox: 네트워크 영역에서의 지능형 위협에 대한 대응 솔루션의 하나를 지칭) 제품의 배포뿐만 아니라, 조직의 내포 네트워크 방화벽의 구축 및 재침해 방지

▪ **참고: Workgroup for Electronic Data Interchange: Perspectives on Cybersecurity in Healthcare (June 2015) 보고서**

- 본 보고서는 Ⅰ. Introduction (소개), Ⅱ. Purpose of Primer (초안의 목적), Ⅲ. The Life Cycle of Cyber Attack and Defense (사이버 위협과 방어의 주기), IV. The Anatomy of an Attack (사이버 위협의 유형 분석), Ⅴ. Building a Culture of Prevention (예방의 문화 구축)의 내용으로 이루어짐
- 이 보고서의 목적은 과거와는 다르게 발전하고 있는 의료산업과 이에 수반하여 진행되고 있는 병원 기록의 전자정보화에 맞추어 발생되고 있는 사이버 위협의 증대와 피해를 예방하고자함
- 의료정보의 판매는 $20(신용정보는 $2)에 이르는 등 건강데이터는 금전적 가치를 지니므로 공격대상이 되기 쉬움. 이에 대한 예방과 방안 마련이 필요함
- 또한 본 보고서는 사이버 위협과 방어의 주기에 대한 분석의 내용을 담고 있음. 위협 주기에 따른 이에 대한 방어의 대응방안을 통하여 효율적이고 실제적인 가이드라인 마련
- 사이버 위협의 대표적 유형으로써 본 보고서는,

  ① 정찰[1] ② 무기화・공격화[2] ③ 침투, 침해[3] ④ 장악 및 관리[4] ⑤ 내부 정찰[5] ⑥ 유지 및 지속 등의 유형별 단계를 통하여, 사이버 위협의 특성 및 유형분석의 예를 제시하고 있음

1) 네트워크 정찰 및 취약부분에 대한 파악

2) 악성 코드의 설계 및 네트워크에로의 침투

3) 사전의 정찰 및 악성 코드의 설계를 통하여 네트워크 내부로의 침투. 사전 정찰 및 설계를 통하여 공격 대상의 유형에 맞는 적절한 형태의 침입 방법을 수행 (피싱, 멀웨어 등의 Delivery)

4) 시스템이 감지 할 수 없거나 혹은 통제하기 어려운 다양한 침입을 통하여 이를 관리 (SSL, TOR, ICMP or DNS)

5) 관리자의 계정 및 권한 등에 접근하고 지속적인 정보를 얻기 위한 시스템 내부로의 위협

<The Life Cycle of Cyber Attack and Defense>

● 시사점

- 의료시장이 커지고 의료 전자기록을 이용한 서비스가 제공되면서, 의료 전자정보를 이용하는 사례가 증가되고 있음. 그러나 한편으로 이러한 의료 전자정보에 대한 관리, 사이버 위협으로부터의 보안·대응방안의 마련 논의는 부족한 실정임
- 해외뿐만 아니라 국내에서도, 의료정보에 대한 사이버 위협으로부터의 대응은 기존의 개인정보에 대한 사이버 위협의 유형 및 관점 하에서 논의되고 있음. 의료영역의 특성과 유형을 반영하여 의료정보 침해에 대한 대응방안 마련을 위한 노력이 필요함

● 출처

http://www.fiercehealthit.com/story/wedi-cybersecurity-report-illustrates-health-care-security-challenges/2015-06-22

http://www.wedi.org/docs/test/cyber-security-primer.pdf?sfvrsn=0