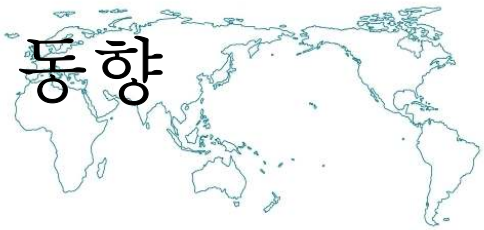
해외 ICT 표준화 동향



2014. 2

3rd Week

목차

한국정보통신기술협회
Telecommunications Technology Association

▷ 본 자료의 게시처 : TTA 홈페이지 > 자료마당 > TTA간행물 > 표준화 이슈 및 해외 동향

1 CardLinx™, 카드사기 방지 카멜레온 표준 초안 발표

- 보도날짜 : 2014. 2. 10
- 출 처 : pymnts.com
- 사 이 트 : http://www.pymnts.com/news/businesswire-feed/2014/february/10/cardlinx-trade-task-force-chaired-by-deem-releases-draft-standard-for-fraud-prevention-20140210005174

■ Deem이 의장으로 있는 CardLinx Association의 태스크포스는 CLO 구매 반환 시 발생하는 사기를 사전에 방지하기 위한 새로운 CardLinx™ 카멜레온 표준 초안 프로토콜을 완성, 발표함

– 고객이 지불 카드를 사용하면 자동으로 할인을 해주는 CLO는 일반적으로 종이 쿠폰, 프로모션 코드 및 종이 바우처보다 훨씬 더 안전하며 사기 리스크를 제한함

– 초안은 현재 회원들의 코멘트에 열려있음

■ CardLinx™ 카멜레온 표준은 상거래 보안이 점점 더 중요해지는 현 시점에서 카드와 관련된 거래에 중요한 역할을 담당 할 것

– 업자의 오용을 방지하여 카드연계 산업을 강화할 것

– 리베이트와 자동 리버설이 필요한 시점을 알려줄 것

– 실시간으로 사기 패턴 및 사기꾼 탐지를 가능하게 할 데이터보고 요구조건을 수립함

■ Deem 외 태스크포스에 참여하는 다른 회사들로 MasterCard, Living Social, CardLytics 및 ValPak/Cox Target Media가 있음

2 Verizon 리포트: 많은 단체가 여전히 PCI 준수에 미달

- 보도날짜 : 2014. 2. 11
- 출 처 : Dark Reading
- 사 이 트 : http://www.darkreading.com/attacks-breaches/verizon-report-many-organizations-still/240166049/

■ Verizon의 새로운 리포트는 기업들이 지불카드산업 데이터보안 표준(PCI DSS)의 준수 정도를 개선하고 있으나 감사 결과 여전히 요구사항에 대체로 못 미치는 것으로 나타난다고 밝힘

– 연구는 신용 카드 거래를 다루는 모든 조직에 대한 가이드라인 세트인 PCI DSS를 반드시 준수해야 하는 기업의 실제 경험을 살펴봄

■ 2014 Verizon PCI 컴플라이언스 리포트에 따르면, 2013년 연간 기준 평가 때 전체 기관의 82% 이상이 PCI 표준을 최소 80% 준수했음

– 2012년에는 단 32%였음

■ 기업들이 초기 준수를 달성하는데 가장 분투하는 분야로 보안 테스트(23.8%), 보안 모니터링과 데이터 손상의 효과적으로 감지 및 대응(17%), 민감한 저장 데이터 보호(55.6%) 등이 있었음

■ 준수의 문제는 기술이나 표준의 결함이 이슈가 아니라, 지속적인 구현에 있다고 Verizon은 언급함

– “우리는 PCI 준수에 365일 내내 초점을 맞출 필요가 있음을 인식하지 못하고 평가를 그저 하나의 연례행사로 생각하는 기관들을 계속해서 봐오고 있다.”고 로돌프 시모네티 Verizon Enterprise Solutions의 PCI 실행 전무이사는 말함

3 오바마 정부, 사이버보안 프레임워크 출범

- 보도날짜 : 2014. 2. 12
- 출 처 : 백악관
- 사 이 트 : http://www.whitehouse.gov/the-press-office/2014/02/12

■ 오바마 행정부는 주요 인프라 사회의 기관들의 사이버보안을 향상시키기 위한 자발적인 가이드를 개발하기 위해 일 년 동안 민간 부문이 주도한 노력의 결과인 사이버보안 프레임워크의 출범을 발표함

– 프레임워크는 오바마 대통령이 2013 신년 국정연설에서 발표한 “주요 인프라의 사이버보안 개선” 행정 명령의 핵심 결과물임

– 미 상무부의 국립표준기술연구소(NIST)가 자발적인 사이버보안 프레임워크로의 인풋을 통합했음

– 이 프레임워크의 개발을 통해 산업계와 정부는 공공-민간 협력 모델 내 핵심 인프라의 보안 및 탄력을 강화하고 있음

■ 프레임워크의 각 요소들(프레임워크 코어, 프로파일 및 계층)은 비즈니스 드라이버와 사이버보안 활동 간 연결을 강화하며 사이버보안 활동에서 발생할 수 있는 개인정보 및 시민의 자유에 관한 지침을 제공함

– 프레임워크 코어는 주요 인프라 부문에 걸친 사이버보안 활동 및 정보 레퍼런스의 집합임. 사이버보안 활동은 식별, 보호, 탐지, 대응, 복구의 다섯 기능으로 분류됨

– 프로파일은 비즈니스 요구사항, 리스크 허용범위 및 자금과 사이버보안 활동이 상응할 수 있도록 도와줌

– 계층은 조직에 사이버 리스크 관리에 대한 접근 방식과 프로세스에 대한 메커니즘을 제공함. 부분(1단계)에서 적응(4단계)에 이르는 계층은 리스크 관리의 엄격한 정도를 설명함

■ 프레임워크의 채택은 자발적이나 미 국토안전부(DHS)는 사이버보안 프레임워크의 인식 및 사용을 증가시키기 위한 공공-민간 파트너십으로서 주요 인프라 사이버 커뮤니티(C3) 자발적 프로그램을 수립함