

엔트러스트, “IoT, 인증, 클라우드 서비스가 PKI 확산 견인차”

- ‘2020 글로벌 PKI 및 IoT 동향 보고서’ 발간
- PKI가 기업 핵심 애플리케이션 지원에 중요 역할 담당
- 한국 응답자의 96%가 “퍼블릭 클라우드 기반 애플리케이션에 PKI 사용”

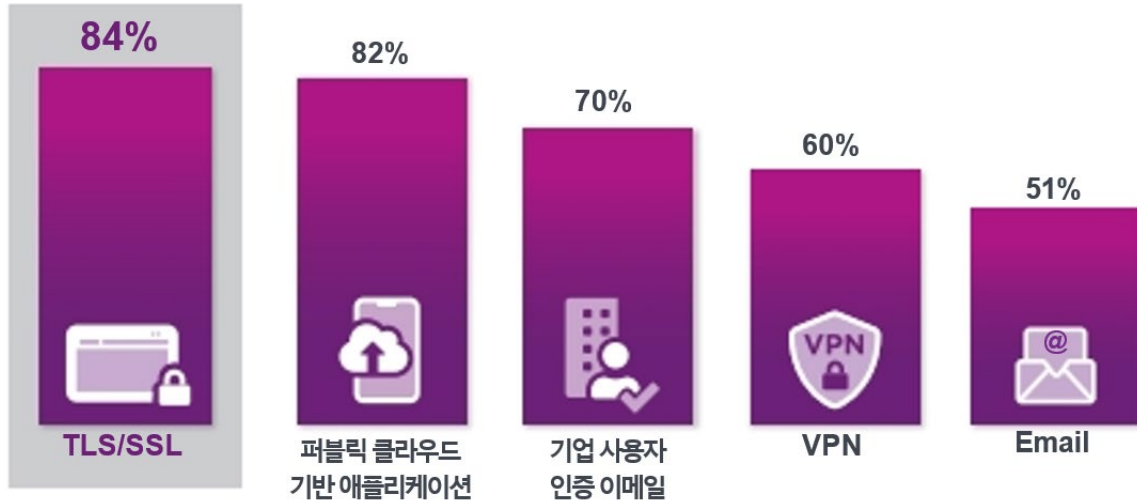
2020년 10월 14일 – 글로벌 정보보안 기업 엔트러스트(Entrust)가 ‘[2020 글로벌 PKI 및 IoT 동향 보고서](#)’를 발표했다. 보고서에 따르면 공개키기반구조(PKI) 기술 채택이 늘고 데이터 보호를 위한 기업들의 인프라 규모와 범위도 커진 것으로 나타났다. PKI는 클라우드, 모바일 기기, 본인 인증, 사물인터넷(IoT) 등 주요 디지털 이니셔티브에 강력한 보안을 제공하며 IT 인프라의 핵심으로 자리잡았다.

이번 보고서는 한국을 포함 전세계 17개 국가, 1900여명의 IT 보안 전문가 대상 설문 결과를 바탕으로 발간됐다. 조사 및 연구는 엔트러스트의 자회사 엔사이퍼 시큐리티(nCipher Security)의 후원으로 시장 조사기관 포네몬 인스티튜트(Ponemon Institute)가 진행했다.

디지털 의존도가 높아지고 사이버 공격이 정교해지면서 기업은 데이터에 대한 접근 권한 설정, 사용자·시스템·기기 인증에 PKI 기술을 활용하고 있다. 올해 PKI 기술 채택의 주요 동인으로 응답자의 47%가 IoT를 꼽았다. 지난 5년간 IoT 보안을 위해 PKI 기술을 도입한 사례는 26% 증가했다. 클라우드 기반 서비스가 PKI 도입을 이끌었다는 응답자는 44%로 나타났다.

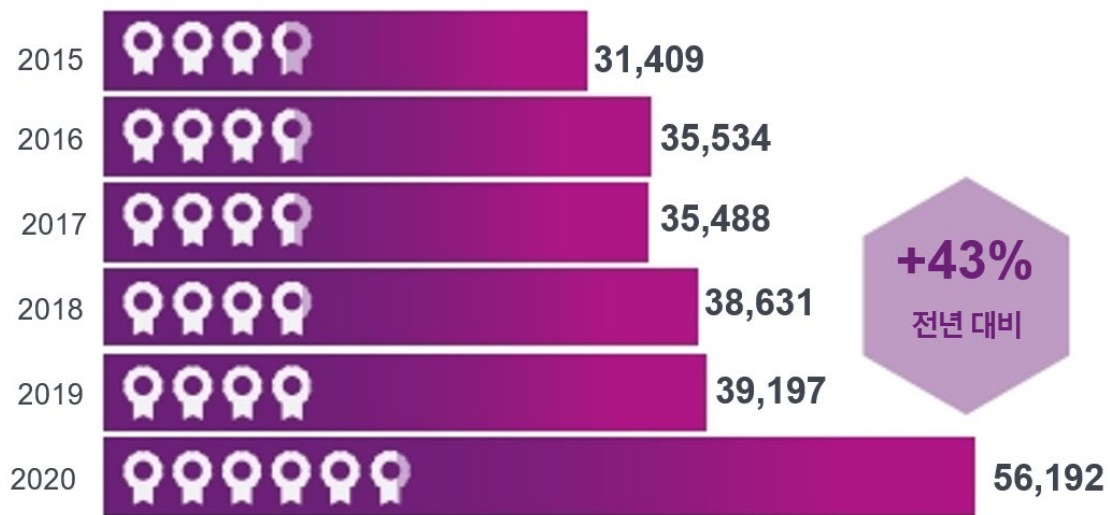
클라우드·인증 분야에서 PKI 이용 급증

PKI는 일반 사용자용 웹사이트 및 서비스의 TLS/SSL 인증에 가장 많이 사용됐다(응답자의 84%). 퍼블릭 클라우드 기반 애플리케이션은 82%로 전년 대비 27% 증가하며 가장 높은 연간 성장률을 보였다. 한국은 특히 퍼블릭 클라우드 기반 애플리케이션에 PKI를 사용한 비율이 96%로 매우 높았다. 기업 사용자 인증은 70%로 전년 대비 19% 늘었다.



▲PKI 기술이 활용되는 주요 분야

기업이 관리해야 하는 인증서 평균 개수는 5만 6192개로 전년 3만 9197개 대비 43% 늘었다. 이는 인증서 유효기간을 줄이는 추세와 클라우드 및 기업 사용자 인증 용도가 급격히 증가한 데 따른 것으로 분석된다.



▲기업이 관리해야 하는 인증서 평균 개수

PKI 기술의 당면과제로 응답자 52%가 PKI 보안 역량 결여를 들었으며(전년 대비 16% 증가) 사이버 보안에 대한 전문 지식, 보안 및 운영 모범사례를 기반으로 기업 맞춤형 로드맵을 만들

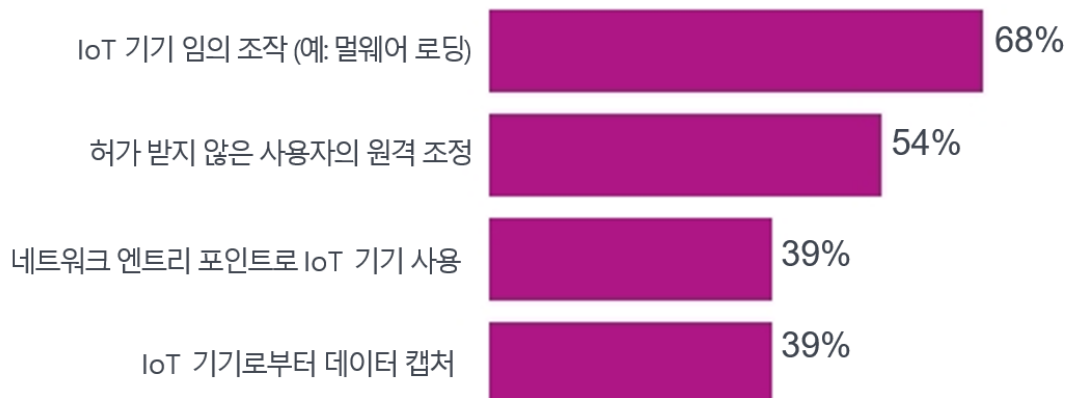
PKI 전문 인력의 필요성이 제기됐다. 기존(legacy) 애플리케이션을 변경할 수 있는 역량 부족(51%), 기존 PKI 로 신규 애플리케이션을 지원할 수 없다는 점(51%)도 꼽혔다.

PKI 도입·관리에 대해 응답자는 명확한 업무 권한이 없고, 역량 및 자원 부족 같은 조직적 문제로 어려움을 겪고 있다고 답했다. PKI 도입은 일부 국가에서 온프레미스(on-premise)보다 서비스 형태가 선호되며 다각화된 것으로 나타났다.

응답자는 PKI 의 변화와 불확실성을 가져오는 주요 요인으로 IoT(52%), 외부 규정 및 표준(49%)을 들었다. 응답자의 24%는 규제 환경이 PKI 기술을 적용한 애플리케이션 도입을 더욱 필요로 한다고 답했다.

보안, 모범사례와 관행의 큰 괴리

향후 2년 간 IoT 기기의 41%가 계정 및 권한 확인을 위해 디지털 인증서에 의존할 것으로 예상된다. 하지만 IoT 기기, 플랫폼, 데이터 저장소(repository)를 위한 암호화는 33% 증가에 그쳐 민감 데이터에 대한 잠재적 취약점이 될 수 있다. IoT 보안 위협으로 응답자들은 악성코드 또는 기타 공격을 통한 IoT 기기 임의 조작(68%), 허가 받지 않은 사용자의 원격 조정(54%)을 꼽았으며, 패치 배포나 IoT 기기 업데이트 같은 악성코드 차단 방식으로는 통제 실효성이 없다고 답했다.



▲주요 IoT 보안 위협

미국 국립표준기술연구소(NIST)는 인증기관(CA)용 암호화 모듈, 주요 복구 서버, OCSP(Online Certificate Status Protocol) 응답에 대해 FIPS 140-2 레벨 3 또는 그 이상의 인증을 권고한다. 응답자 39%가 하드웨어 보안 모듈(HSM)의 주된 사용처가 루트·발급·정책 인증기관을 위한 PKI 보안 유지라고 답했지만 HSM을 OCSP 설치에 사용하는 응답자는 12%에 불과했다. 이는 모범사례와 관행의 큰 괴리를 보여준다.

래리 포네몬(Larry Ponemon) 포네몬 인스티튜트 창업자는 “PKI는 소스, 무결성을 증명하기 위한 디지털 서명 트랜잭션과 애플리케이션부터 스마트폰, 게임 콘솔, 신분증, 대중교통 발권, 모바일 बैं킹에 이르기까지 기업과 일반 사용자 모두에 보안을 제공한다”며 “클라우드 기반 애플리케이션 및 기업 사용자 인증에 PKI 사용이 가파르게 증가하는 것은 PKI가 기업 핵심 애플리케이션 지원에 중요 역할을 하고 있음을 입증한다”고 밝혔다.

존 그림(John Grimm) 엔트러스트 디지털 솔루션 전략 부문 부사장은 “엔트러스트는 전통적인 PKI 도입 모델과 방식을 바꾸는 새로운 시장 수요에 대응하기 위해 노력하고 있다”며 “기업은 IoT 같은 새로운 영역에서 보안 위협에 대응할 펌웨어 인증 등 보안 매커니즘 구축에 어려움을 겪고 있다. 이번 연구 결과는 인증서 자동관리, 유연한 PKI 도입, HSM 등 모범사례에 기반한 강력한 보안의 필요성을 보여준다”고 말했다.

2020 글로벌 PKI 및 IoT 동향 보고서 전문은 [웹사이트](#)에서 무료로 다운로드 받을 수 있다.

###

엔트러스트(Entrust)

엔트러스트는 인증, 결제, 데이터 보호를 지원하면서 전세계 정보 보안을 위해 노력하고 있다. 오늘날 그 어느 때보다 많은 사람들이 인터넷에서 국경을 넘나들고, 물건을 구매하고, 전자정부 서비스에 접속하고, 기업 네트워크에 접근하는 데 끊임 없고 안전한 환경을 경험하기를 원한다. 이를 위해 엔트러스트는 다양한 디지털 보안과 신원 인증 솔루션을 제공한다. 엔트러스트는 2500 명이 넘는 직원, 글로벌 파트너 네트워크, 고객사와 함께 전세계 150 여 국가에서 세계 최고의 신뢰받는(entrust) 기업들을 지원한다. 자세한 내용은 웹사이트(www.entrust.com)에서 확인할 수 있다.

[보도자료]



문의

홍보대행사 KPR	정광진 이사	river@kpr.co.kr	3406-2252	010-7608-5107
	박수진 차장	susan@kpr.co.kr	3406-2265	010-9801-5077
	김성준 대리	simon@kpr.co.kr	3406 2221	010-6712-8312