Hewlett Packard Enterprise

2016 년 사이버 위험 보고서

HP 보안연구소의 연례 사이버 위험 보고서는 조직이 각종 위협 환경에 대한 이해를 제고하고, 보안 위험을 최소화하는 데 도움이 될 수 있는 자원을 제공합니다. 올해 보고서는 고급 데이터 분석에서 도출한 전망을 특집으로 다루는 한편, 오픈 소스, 모바일 및 사물 인터넷을 포함하여 여러 기술에 초점을 맞추었습니다.

35%

스캔된 애플리케이션 중의 1/3 이상 (35%)에서 최소 하나 이상의 심각 또는 고위험 취약점이 드러났습니다.

약 86% 의 조사 대상 기업이 IDS 를 사용하고 있다고 응답하였습니다.

애플리케이션의 오픈 소스 컴포넌트 사용 비율이 14% 증가하였습니다.

153%

매일 10,000 개 이상의 새로운 위협이 안드로이드 플랫폼 상에서 발견되었으며, 전년 대비 153% 증가하였습니다.

80%

80% 이상의 오픈 소스 및 상용 애플리케이션에 보안 기능 취약점이 있으며, 이는 개인정보 관리에 심각한 영향을 미치고 있습니다.

95%의 새로 발견된 멜웨어 샘플과 42% 의 공격이 집중된 Windows OS 는 여전히 공격의 주 대상 플랫폼입니다.

내부 시스템 정보 유출 문제를 겪은 모바일 애플리케이션은 분실하기 쉬운 기기에 비즈니스 크리티컬 정보의 저장과 관련된 문제를 부각시키고 있습니다.

2015년에 발견된 전체 공격 샘플의 29%가 두 차례 패치 되었던 2010 Stuxnet 감염 벡터를 여전히 사용하였습니다.

29%

부수적 피해가 발생한 해

데이터 유출은 더 이상 지불 카드 정보 입수에 국한된 것이 아닙니다. **누군가의 삶을 영원히 바꿀 수 있는 정보의 입수**에 관한 문제입니다.

보안 연구를 음성화하고 있는 과도한 규제

사이버 보안에 관한 다양한 규제 안은 합법적인 보안 연구를 한층 음성화시킬 것입니다. 이러한 규제는 모두에게 도움이 되는 보안 연구를 막을 것이 아니라 장려해야 합니다.

일부분의 수정 방식에서 보다 효과적인 솔루션으로의 전환

2015 년에는 벤더들이 모든 종류의 공격을 방지하는 방어 수단의 개발에 치중하였습니다.

개인정보 보호와 보안 활동을 분리하려는 정치적인 압력

미국, 영국 등의 다수 입법자들은 기본적인 프라이버시 권리와 정당한 법 절차가 축소되어야만 보안이 가능하다고 주장하였습니다.

2015 년의 보안 패치에 관하여 아무런 교훈도 얻지 못한 업계

2015 년에 가장 많이 악용된 취약점은 벤더가 두 차례나 보안 패치를 실시한 적이 있는 이미 5년이 지난 취약점이자, 2014년에 가장 많이 악용된 취약점이었습니다.

애플리케이션의 직접 공격으로 활동을 전환한 공격자들

현재 애플리케이션은 공격자들이 민감한 기업 정보를 입수할 수 있는 가장 손쉬운 경로로 여겨지고 있습니다.

멀웨어의 수익 추구

ATM 관련 멀웨어가 더욱 보편화되면서, 사이버 범죄자들이 더 빠르게 많은 돈을 편취하고 있습니다.

보고서 전문은 다음 사이트를 참조하시기 바랍니다: www.hpe.com/software/cyberrisk