IBM X-Force 2011 상반기 동향 및 리스크 보고서

CIO 보안 우선 순위

"세상은 더욱 더 긴밀하게 연결되고, 지능적이며 도구화되고 있습니다. 이러한 혁신은 우리의 효율성을 증가시키고 세계적인 규모로 즉시 연결시켜주는 한편, 서로 연결된 세상의 위험 역시 보다 정교해지고 통제하기가 어려워지고 있습니다."

— IBM X-Force 보안 연구소

보안 침해 사건이 2011년에는 지속적으로 발생하고, 연일 새롭게 보고되어, 올해를 "보안 침해의 해(The Year of the Security Breach)"로 규정하게 되었습니다. 이러한 보안 침해는 그 빈도에서 놀랄 만한 것일 뿐만 아니라 침해 대상이 된 기업의 운영에도 상당한 피해를 입힌 것으로 추정되고 있습니다. 환경은 변화하고 있습니다: 클라우드와 모빌리티, 소셜 비즈니스, 대규모 데이터 등의 등장에 따라 비즈니스 인프라의 경계가 확대되거나 경계 자체가 없어지고 있는 반면에, 광범위하게 정보를 수집하고 신중하며, 참을성 있고 장기적인 계획 하에서 공격이 이루어지고 있다는 증거가 발견되는 등 공격은 더욱 더 정교해지고 있습니다. 보안 관련 논의가 이제는 기술적인 테두리에서 벗어나 이사회에서 다루어질 만큼 공격의 영향이 더욱 더 커지고 있습니다.

주요관심대상을보면다음과같습니다:

- 공격자가 주로 선호하는 공격 방법은 SQL 인젝션이며 비밀번호와 데이터베이스, 마이크로소프트 윈도우 폴더/드라이브 공유에 대한 무차별 대입 공격을 시도합니다. 개방형 서비스인 인터넷을 스캐닝하고 이를 토대로 침투하게 됩니다.
- 주요 취약점들은 이미 2010년에 보고된 총 취약점을 넘어섰으며, 중요한 엔터프라이즈급 소프트웨어 제품에 영향을 끼치는 중대한 원격 코드 실행 문제와 대부분 연관되어 있습니다.
- 도큐먼트 리더와 멀티미디어 플레이어에서의 취약점이 대폭 증가하고 있습니다. 공격자들은 브라우저에 상관없이 소비자들이 구동하는 소프트웨어에 초점을 맞추고 있으며, 이를 특별히 이용 도구로 삼아 그 피해가 최고치를 기록할 정도입니다.
- Futune 500 기업과 인기 있는 웹 사이트 등 678곳 중 40%가 클라이언트 측면의 자바스크립트 취약점을 내포하고 있는 것으로 나타났습니다.

X-Force 위협 분석(Threat Analysis) 서비스는 진화하는 위협 상황에 적극적으로 대응할 수 있도록 IT 담당자들에게 최신 위협 요인과 이용 가능한 보호 수단, 업계의 전반적인 경향을 알려주는 맞춤형 데일리 서비스로 이용할 수 있습니다.

역설적이게도, 인터넷을 보호하기 위한 수많은 해결책들이 등장해 많은 취약점들과 공격 수치가 비약적으로 개선되고 있는 것으로 나타났습니다.

- 러스턱 봇넷(Rustock botnet) 이후 스팸의 양은 2011년에 지속적으로 줄어들고 있습니다.
- 2011년 상반기, 스패머들은 전통적인 이메일 피싱에 종식을 선언했습니다. 주간별로 피싱이 이루어진 스팸의 비율을 살펴본 결과 매주 0.01% 이하인 것으로 조사되었습니다.
- 지난 수년 동안 알려진 보안 취약점 중 절반 가량이 웹 애플리케이션 취약점이었습니다. 올해 그 수치는 37%로 낮아졌는데, 특히 SQL 인젝션 취약점의 양이 대폭 줄어들었습니다.
- 브라우저 마켓플레이스가 확산되고 경쟁이 치열한 가운데에서도 높고 중요한 브라우저의 취약점 역시 지속적으로 감소하고 있습니다.

이에 따라, 일부에서는 승리한 것으로 보이지만 싸움이 결코 끝난 것은 아닙니다. 공격자들은 새로운 대상을 찾아 이동하고 있을 뿐이며 그러한 새로운 공격 대상 중의 하나가 바로 스마트폰입니다. 통합 운영 체제가 결합된 스마트폰의 보급이 확산됨에 따라, 공격자들은 스마트폰에 대한 공격 개시를 위한 준비 태세에 돌입해 있습니다. IBM X-Force® 보안 연구소는 모바일 운영 체제의 취약점을 목표로 한 공격이 2010년에 비해 두 배 이상 늘어날 것으로 예상하고 있습니다.

이에 대해 어떻게 대응하시겠습니까? 이러한 새롭고 보다 복잡해진 환경에서, IBM X-Force 보안 연구소는 여러분들의 네트워크를 다음을 주의해서 관리하고 있는지 확인해 보시기를 적극 권장드립니다:

1. 정기적으로 외부 및 내부 보안 감사 실행
2. 엔드 포인트 제어
3. 중요한 시스템과 정보에 대한 분리 운영
4. 네트워크 보호
5. 웹 애플리케이션 감사
6. 피싱 및 스피어 피싱에 대한 최종 사용자 교육
7. 취약한 비밀번호 검색
8. 모든 프로젝트 계획에 보안을 통합
9. 비즈니스 파트너의 정책 검사
10. 견고한 사고 대응 계획 수립

상세 정보는 보고서 전문에서 제공됩니다

IBM X-Force 보안 연구소는 SQL Slammer가 사라진 주요 원인이 보안 전문가 집단의 노력(혹은 악의적인 집단의 포기)였다고 판단하고 있습니다. 상세 내용은 보고서 전문을 참고하시기 바랍니다.

IBM X-Force 연구소와 IBM 보안 협업 소개

IBM Security는 광범위한 보안 역량을 제공하는 여러 브랜드를 대표합니다.

- IBM X-Force 보안 연구소는 해커들이 사용하는 최신 공격 동향을 분석하고 있으며 고객을 보호하기 위한 기술 개발을 위해 IBM 내부의 다른 그룹들과 함께 그러한 풍부한 데이터를 활용하고 있습니다.
- IBM X-Force 연구소는 광범위한 컴퓨터 보안 위협과 취약점을 파악하고 분석하며 모니터링하고 기록합니다.
- IBM 보안 관제 서비스는 엔드포인트와 서버(웹 서버 포함), 범용 네트워크 인프라와 관련된 위협을 모니터링하고 있습니다.
- IBM 보안 관제 서비스는 웹이나 이메일, 인스턴트 메시징 등을 통해 제공된 악용 사례를 추적합니다.
- IBM 보안 전문가 서비스는 효과적인 정보 보안 솔루션을 개발할 수 있도록 종합적이며 전사적인 보안 평가와 설계, 도입 서비스를 제공합니다.
- IBM의 콘텐츠 보안 팀은 크롤링(crawling)과 독립적인 발견, IBM 보안 관제 서비스가 제공하는 데이터를 통해 웹을 철저하게 탐색하고 범주화합니다.
- IBM은 IBM Rational® 서비스 팀이 지난 수년 동안 수행한 보안 테스트로부터 도출된 실제 취약점 데이터를 수집해 왔습니다. 이러한 데이터는 IBM Rational AppScan®을 통해 이루어진 애플리케이션 보안 평가와 수동으로 진행된 보안 테스트 및 인증을 결합한 것입니다. 설계와 코드, 생산을 통한 요구 사항을 토대로, IBM Rational AppScan은 애플리케이션의 수명 주기 전반에 걸쳐 종합적으로 애플리케이션의 취약점을 관리합니다.
- IBM 클라우드 보안 서비스는 고객들이 비용을 절감하고 서비스 전송을 향상하며 보안을 강화할 수 있게 해 주는 호스트형(hosted) 가입 모델을 통해 보안 소프트웨어 기능을 사용할 수 있도록 해 줍니다.
- 신원 확인 및 접근 관리 솔루션은 신원 확인 관리와 접근 관리, 사용자의 준수 여부 감사 기능을 제공합니다. 이러한 솔루션은 사용자 관리와 인증, 접근, 감사 정책, 사용자 서비스의 프로비저닝을 중앙에서 자동으로 관리할 수 있도록 해 줍니다.
- IBM 데이터와 정보 보안 솔루션은 기업 전반적으로 정보 수명 주기 보안에 대응할 수 있도록 통합 가능한 데이터 보호와 접근 관리 기능을 제공합니다.

자세한 정보

2011 X-Force 동향 및 리스크 보고서에 관한 자세한 정보는, ibm.com/kr/security를 방문하십시오.

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
September 2011

135-700
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080
U.S. Patent No. 7,093,239

이 문서는 IBM에서 "IBM X-Force 2011 Mid-year Trend and Risk Report" 의 요약본입니다. 전체 문서는 다음 사이트를 참고하시기 바랍니다. http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03009USEN&attachment=WGL03009USEN.PDF

WGE03015-USEN-00