IBM X-Force 2012년 동향 및 위험 보고서

CISO 보안 통찰

2012년에 발생한 보안 사건 중 다수는 상용 완제품(off-the- shelf) 툴과 기술을 이용한 광범위한 공격이었습니다. 이는 툴킷이 일반에게 널리 보급되고 인터넷에 있는 웹 애플리케이션에 많은 취약점이 존재하게 된 데 기인합니다.

- IBM X-Force 연구 개발 팀

지난 한 해, 수많은 IT 보안 사고 소식이 주요 언론의 헤드라인을 차지했습니다. 이름부터 불길한 Flame, 범플랫폼의 제로 데이(zero day) 취약점 등 새롭게 등장한 보안 위협에 대한 조언과 경고가 개인 사용자와 기업들에게 물밀듯이 밀려왔습니다. IBM® X-Force® 팀은 2012년 중간 보고서를 통해 전반기의 공격 및 보안 사고 급증 추세가 2012년 내내 계속될 것으로 예측한 바 있습니다. 이 예측은 현실로 이루어졌습니다.

데이터 손실 및 네트워크 침입 보도가 주간 뉴스 헤드라인을 차지했던 2012년은 사이버 공격이 기록적으로 발생한 해로 기억될 것입니다. 현재 모든 정부 기관과 기업의 회의실에서는 보안 대책 마련에 여념이 없습니다. 최고경영진과 임원진은 기업이 지능적인 보안 위협에 직면했음을 절감하고 있습니다. 이러한 인식과 더불어, 보안 전문성 및 전 세계의 보안 상황 파악에 대한 요구 수준도 높아졌습니다.

CISO(Chief Information Security Officer)는 클라우드 컴퓨팅을 도입하고 모바일 기기를 통합하여 전례 없이 많은 양의 데이터를 저장, 조회 및 분석하면서 조직적이고 강력한 외부 위협에 대처해야 합니다. 기본적인 방어에만 의존하던 시대는 지나갔습니다. IT 보안 팀이 정상적인 동작 패턴을 이해하고, 이상 동작을 포착하며, 실제로 피해를 입기 전에 보안 위협을 신속히 해결할 수 있으려면 거시적이고 통합적인 접근법이 필요합니다.

이 문서는 IBM X-Force 2012년 동향 및 위험 보고서의 주요 내용 중 일부를 소개하고, 기업의 경영진이 보안 태세를 강화하는 과정에서 직면하게 되는 과제와 연계하여 이를 살펴볼 것입니다. 보안 위협, 클라우드, 모바일, 소셜 미디어라는 네 가지 주요 영역이 중점적으로 조명될 것입니다.

보안 위협

2012년에는 하루가 멀다 하고 개인 정보 유출 사고 소식이 트위터 등 각종 소셜 미디어를 통해 전해졌습니다. 이메일 주소, 암호(암호화 및 일반 텍스트 형태) 심지어 주민등록번호 같은 개인 정보가 공개되는 일도 있었습니다.

2012년에 발생한 보안 사건 중 다수는 상용 완제품(off-the-shelf) 툴과 기술을 이용한 광범위한 공격이었습니다. 이는 툴킷이 일반에게 널리 보급되고 웹 애플리케이션에 많은 취약점이 존재하게 된 데 기인합니다.

전문적인 용도의 웹 브라우저 익스플로잇 킷의 보급으로 일반 사용자의 시스템에 악성 코드를 배포 및 설치하는 것이 매우 용이해졌습니다. IBM은 2012년에 Java 취약점을 주로 노리는 웹 브라우저 익스플로잇 킷의 개발과 활용이 급증했음을 확인했습니다. 이 X-Force 보고서에서는 향후 공격을 예방하는 데 유익한 전략과 조언을 상세히 제시합니다.

Java는 변함없이 주 공격 대상이 되고 있습니다. Java는 크로스 브라우저 및 크로스 플랫폼이라는 속성이 조합되어 있어 공격자에게 투자 가치를 제공하기 때문입니다. Java 익스플로잇은 안정화된 익스플로잇, 비샌드박스(unsandboxed) 코드 실행, 여러 운영 체제를 포괄하는 크로스 플랫폼적 가용성이라는 세 가지 핵심 요소를 이용합니다. 이 요소들은 2012년에 주 공격 표적이 되었으며, IBM X-Force 팀은 이러한 공격 활동이 2013년에도 계속될 것으로 예상합니다.

2012년은 데이터 유출 사고가 자주 발생했는데, 정치적 동기에서 비롯되어 은행 업계를 강타한 일련의 대규모 DDoS 공격이 연초와 연말에 일어났습니다. 은행을 대상으로 한 DDoS 공격에서 주목할 점은 고대역 데이터 센터의 웹 서버를 공격한 다음 봇넷(botnet)을 구현했다는 것입니다. 공격자는 가정용 PC를 이용하는 공격보다 더 넉넉한 대역폭으로 훨씬 오랫동안 연결 상태를 유지할 수 있었습니다.

미래 지향적인 기업은 통찰력을 활용하여 향후 일어날 수 있는 위협 및 공격과 공격자를 파악하기 위해 툴셋의 활용을 확대하고 있습니다. 이들은 DNS 트랜잭션, 비즈니스 프로세스 데이터 등에 대한 빅 데이터 애널리틱스를 통해 봇넷 감염 및 각종 네트워크 침입 사건의 이력을 관리하는 광범위하고 심층적인 지식 기반을 구축하고 있습니다. 또한, 소셜 미디어 컨텐츠를 분석함으로써 향후의 공격을 예측하고 신뢰할 수 있는 내부 구성원의 정서를 파악할 수 있습니다.

이러한 고급 보안 분석 애널리틱스는 새로운 유형의 비정형 데이터를 보안 인텔리전스 데이터베이스 내의 정형화된 보안 원격 측정 방식과 연계합니다. 빅 데이터 애널리틱스는 지능적인 보안 위협을 인식하고 대처하는 데 활용될 수 있습니다.

클라우드

XSS(cross-site scripting)는 웹 애플리케이션 취약점을 노린 공격의 주를 이루며, 지금까지 알려진 취약점의 53%에 달합니다. 이는 IBM X-Force 팀이 조사를 시작한 이래 가장 높은 비율입니다.

클라우드 기술 도입을 고려하는 기업은 애플리케이션 취약점과 관련하여 많은 고민을 하게 됩니다. 즉, 가상화에서 웹 애플리케이션, 컨텐츠 관리 시스템 및 웹 브라우저 취약점에 이르기까지 다양한 문제에 직면하게 됩니다. 이 보고서에는 취약점 리포팅과 패치 공급에 관한 조사 결과가 실려 있으며 공격에 노출되는 범위를 최소화하기 위한 방법이 수록되어 있습니다.

웹 애플리케이션은 여전히 취약점 익스플로잇의 주 대상이 되고 있습니다. 2011년에는 2,921개였던 취약점이 2012년에는 3,551개로 14% 증가했습니다. XSS는 공개적으로 확인된 웹 취약점 중 53%를 차지했는데, 이는 IBM 팀이 조사를 실시한 이래 가장 높은 비율이었습니다.

XSS 공격이 이처럼 크게 늘어난 반면 SQL 인젝션 취약점은 2011년에 비해 소폭 증가했는데, 정점을 찍었던 2010년보다는 크게 낮은 수준입니다. IBM Managed Security Services는 주로 아시아 태평양 지역에서 발생한 SQL 인젝션 기반 트래픽이 가파르고 지속적인 증가세를 보인다는 데 주목했습니다. 은행 및 금융 분야가 주요 표적이지만 모든 업종에서 경고 신호가 감지되었습니다.

클라우드 구축을 고려 중인 기업은 보안이 미비한 웹 애플리케이션을 도입하는 것이 위험에 노출되는 결과를 가져올 수 있음을 인식해야 합니다. 웹 애플리케이션을 개발할 때 그리고 프로덕션 환경에서 정기적으로 취약점 테스트를 실시함으로써 애플리케이션에 대한 보안 위협을 줄일 수 있습니다.

모바일

예측: 2014년 무렵에는 모바일 컴퓨팅 기기에 기존의 사용자 컴퓨팅 장치보다 더 강력한 보안이 구현될 것입니다. 이는 현재 식견 있는 보안 책임자들이 예상한 트렌드와 요구사항에 기초한 것입니다.

기업에 모바일 기기를 통합하는 것은 지속적인 과제로 남을 것입니다. IBM 팀은 2012년 중간 보고서에서 모바일 기기 사용에 관한 정책 및 거버넌스의 철저한 구현 없이 BYOD(Bring-Your-Own-Device) 프로그램을 도입할 경우 겪게 될 몇 가지 위험을 지적합니다. 이 보고서에서는 직원 소유의 기기에서 공적 영역과 사적 영역을 분리하려는 보안 책임자의 노력을 조명합니다. 아울러, 더 안전한 모바일 애플리케이션의 설계 및 구축을 위한 소프트웨어 개발 이니셔티브도 다루고 있습니다.

X-Force 팀은 *이러한 보안 제어를 통해 2014년이면 모바일 기기가 기존의 데스크탑 장치보다 더 안전한 환경이 될 것*으로 전망합니다. IBM은 최근 글로벌 기술 전망(Global Technology Outlook) 트렌드 연구 조사에서 이와 같이 과감한 예측을 내놓았습니다. 허황된 의견처럼 들릴 수도 있으나, 이는 현재 식견 있는 보안 책임자들이 예상한 트렌드와 요구사항에 기초한 것입니다.

X-Force 팀이 확인한 바에 따르면, BYOD를 도입하면서 가상화 데스크탑 솔루션을 활용하여 업무용 애플리케이션 및 데이터를 개인 소유 기기에 저장된 나머지 데이터로부터 분리하여 제어하는 기업은 소수에 불과합니다. 기업들은 어떠한 형태로든 모바일 기기에서 공적 영역과 사적 영역을 분리하는 정책을 구현해야 합니다.

기업의 브랜드 평판에 모바일 앱이 중요해지면서, 각종 애플리케이션 보안 프랙티스(예: 보안 기준 확립을 위한 취약점 테스트)를 제도화할 필요성도 커졌습니다. 모바일 앱 개발 업무가 회사 전반에 분산되어 있거나 아웃소싱을 통해 이루어지는 경우라면 특히 그러합니다. 많은 기업들이 SSDLC(Secure Software Development Life Cycle) 프로세스의 구현에 적극적으로 투자하고 있습니다. SSDLC는 오늘날의 모바일 애플리케이션 개발에도 활용되고 있습니다. 기업은 보안을 프로세스의 일부로 간주하고 보안 사고를 사전에 대비해야 합니다.

모바일 상호작용의 방식이 다양해지고 혁신적인 협업 기술이 빠르게 도입됨에 따라, 이전에는 중요도가 높지 않았던 새로운 차원의 보안을 구현해야 하게 되었습니다. 모바일 상호작용이 일어나는 환경의 요소, 가령 온사이트/오프사이트, 시간, 사용자 액세스 수준 등은 상호작용의 리스크 프로필을 정의하는 데 중요한 역할을 합니다. 이러한 동적 속성을 뒷받침하려면 데이터 및 서비스에 대한 탄력적인 권한 제어와 액세스 방식이 필요합니다. 현재의 보안 환경을 강화하고 보안 베스트 프랙티스를 강조함으로써 향후 사용자의 상호작용을 효과적으로 지원할 수 있습니다.

모바일 보안은 기기 관리 및 보호, 액세스 보안, 애플리케이션 방어를 포함합니다. 새로운 보안 위협에 대처하고 위험한 행동을 파악하려면 이와 같은 핵심 보안 기능이 꼭 필요합니다. 보안 인식 제고 및 툴 강화가 기기 보안의 표준으로 자리잡음에 따라 기업은 종합적인 관점에서 모바일 상호작용의 다른 접점까지 보호해야 합니다. 여기에는 액세스 제어, 보안 연결, 애플리케이션 보안 등이 포함됩니다. 이를 통해 CISO는 최적의 보안 투자 효과를 누리고 기기 보안 툴과 솔루션이 최상의 조합인지 평가하여 기업의 운영 요구사항을 만족시킬 수 있습니다.

소셜 미디어

소셜 미디어는 새로운 연결 방식을 통해 우리의 삶의 사적 영역과 공적 영역을 모두 바꿔 놓았습니다. 개인 정보의 지속적인 가용성이 실현됨에 따라, 공격자는 즉시 데이터에 액세스하여 공격 활동을 전개할 수 있게 되었습니다.

스팸 관련 설문 조사에 따르면 피싱 공격이 전체 중 가장 큰 비중을 차지하고 있었으며, 개인 정보 이용이 용이해지면서 스피어 피싱 공격이 활성화되고 있었습니다. 이 보고서에는 피싱 기법, 봇넷 명령과 제어 기능, 소셜 미디어 연결에 관한 조사 결과가 수록되어 있습니다.

2012년에 스팸량은 여전히 고른 분포를 보였습니다. 2012년 가을에 배포된 스팸 중 인도의 스팸이 20% 이상을 차지하였고 미국, 베트남, 페루 및 스페인이 그 뒤를 이었습니다. 기업 인프라를 구성하는 보안 인텔리전스 계층은 이 정보를 이용하여 의심스러운 출처/목적지의 비정상적 트래픽 패턴을 밝혀 보안 사고 가능성을 판단할 수 있어야 합니다.

공격자들은 소셜 미디어 사이트에 쉽게 액세스하여 공격의 계획 및 실행에 이용할 개인 정보를 입수할 수 있습니다. 실제로, 10대 인기 웹사이트를 비롯하여 가장 널리 이용되는 웹 사이트 100만 개 중 48%가 소셜 네트워크 링크를 포함하고 있습니다. 이는 기밀 정보의 공유를 통제해야 하는 기업에게 새로운 과제를 던져 줍니다.

공격은 더욱 지능화되고 있으며, 속임수에 넘어가 웹사이트를 방문하거나 감염된 이메일을 열어봤다가 피해를 입는 이용자가 늘어나고 있습니다. 광범위한 표적을 노리는 피싱 사기와 좀 더 특화된 스피어 피싱은 적법한 것처럼 보이는 고도의 사회 공학적 이메일 메시지를 통해 일반 사용자를 공격합니다. 이를테면 은행의 경고 메시지, 택배업체의 이메일 등으로 위장하여 고객이 안심하고 열어보게 만드는 수법이 효과를 발휘하고 있습니다.

공격자가 특정 기업을 하나의 독립체가 아닌, 여러 개인의 집합체로 보고 공격을 행하는 경우도 있습니다. 이 경우, 기업의 인프라나 애플리케이션이 아닌 특정 개인을 표적으로 삼습니다. 이 표적은 기업 소속의 직원이자, 360도 전방위적 접근이 가능한 인물이기도 합니다. 즉, 직원의 개인적 활동 및 사생활이 기업을 공격하는 데 이용될 수 있습니다.

여러 사례에서 보았듯이, 직원의 사생활 정보는 해커와 사이버 범죄자에게 금광과도 같습니다. 집요한 공격자는 몇 달에 걸쳐 생일, 기념일 및 각종 중요한 날짜는 물론 출신 학교, 클럽 멤버십 등의 개인적 관계와 직업적 관계까지 파헤치고 이를 악용합니다. 각 기업은 직원을 위한 종합적인 소셜 미디어 이용 지침을 마련하여 사적이거나 업무적인 글을 게시하는 데 따른 이점과 위험성을 주지시켜야 합니다.

요약

CISO는 전 세계 보안 환경의 취약점 및 공격 양상에 관한 지식 기반을 강화함으로써 날로 급증하는 공격에 대처해야 합니다.

기업의 클라우드 컴퓨팅 도입, 모바일 기기 통합 및 빅 데이터 이용이 늘어나는 상황에서, 거시적이고 통합적인 IT 보안 방식만이 효과를 발휘할 수 있습니다. 이를 통해 정상적인 동작 패턴을 이해하고 이상 징후를 포착하며 실제 피해가 발생하기 전에 보안 위협을 신속히 해소할 수 있습니다.

IBM X-Force 2012년 동향 및 위험 보고서 전문을 다운로드하여 현재는 물론 미래의 보안 위협에 대처할 실용적 전략을 개발하는 데 유익한 정보를 얻으십시오.

IBM X-Force 정보

IBM X-Force 연구 개발 팀은 세계 최고의 민간 보안 연구 개발 조직 중 하나입니다. 이 팀의 보안 전문가들은 6만여 개의 컴퓨터 보안 취약점을 수록한 데이터베이스, 글로벌 웹 크롤러, 다국적 스팸 컬렉터를 비롯한 각종 소스로부터 확보한 데이터를 모니터링하고 분석합니다. 뿐만 아니라 130여 개국 4,000여 개 고객사를 위해 매일 130억 건의 보안 이벤트를 실시간으로 모니터링합니다. 세계 각처에 위치한 IBM 보안 운영 센터가 이 업무를 수행합니다.

IBM X-Force 연구 개발 팀은 연 2회 IBM X-Force 동향 및 위험 보고서를 발행합니다. 이 보고서는 고객, 다른 보안 연구자와 일반인이 최신 보안 리스크를 더 잘 이해하고 새로운 보안 위협에 대비하도록 돕는 데 목적이 있습니다. 여기서는 소프트웨어 취약점, 공개적인 익스플로잇, 악성 코드, 스팸, 피싱, 웹 기반 보안 위협, 일반적인 사이버 범죄 행위 등 오늘날 보안 전문가의 최대 과제가 심도 깊게 다뤄집니다.

추가 정보

IBM 보안 팀에 관한 자세한 사항은 ibm.com/security를 참조하십시오.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2013

본 문서는 IBM이 발행한 "IBM X-Force 2012 동향 및 위험 보고서"의 요약본입니다. 전체 보고서는 다음 사이트를 참고하시기 바랍니다.
http://ibm.co/xforce12

Please Recycle

WGE03020-USEN-00