Executive Series

CIO를 위한 보안 정보

더 확실한 보안을 구현하기 위해

주요 내용:

더 확실한 보안을 구현하기 위해 주목해야 할 핵심 추세와 새로운 이슈가 세 가지 있습니다. 사회가 점점 더 지능형 시스템에 의존함에 따라서 잠재적인 취약성은 더 증가할 것입니다. 이러한 지능형 시스템은 과거 그 어느 때보다 더 많은 데이터를 생산할 것입니다. 보안이 필요한 곳이 더 많아질수록 보안 교육 및 기술에 관해 더 큰 노력을 기울여야 할 것입니다.

2012년 8월, “정의의 검”이라 불리는 집단이 샤문 바이러스를 이용해 사우디아라비아의 석유 대기업 Aramco의 워크스테이션 30,000대를 공격한 것이 자신들의 소행이라고 밝혔습니다. 샤문 바이러스는 파일을 손상시키고 컴퓨터를 고장 냈으며, Aramco의 업무는 1주일간 중단되었습니다. 샤문 바이러스나 다른 최근의 공격을 통해 CIO들은 정보 보안의 미래가 어떠한 모습일지 분명히 알 수 있게 되었을 것입니다.

이러한 악성 코드를 생성하고 이용하는 데 필요한 지식은 확산되고 발전할 것이며, 범죄자, 산업 스파이 및 테러 지원 국가에 더 강력한 무기를 제공하게 될 것입니다. 오늘날 교통량 관리, 지능형 빌딩, 로봇을 이용한 수술 등 다양한 분야에서 컴퓨터를 통해 점점 더 많은 일을 제어하고 있으며, 따라서 잠재적인 공격 대상은 매우 증가할 것입니다. IT 보안이 위험과 복잡함이 산재하는 까다로운 작업이라고 느껴지실 것입니다. 하지만 조금만 기다리십시오! IBM이 해법을 제시해 드릴 것입니다.

그동안 IBM의 “CIO가 알아야 할 보안 정보” 시리즈에서는 클라우드 컴퓨팅, 소셜 네트워크, 직원들이 회사에서 매일 사용하는 모바일 장치의 빠른 확산 등 오늘날 CIO가 직면하고 있는 중요한 위험 및 과제를 살펴보았습니다. 이러한 주제들의 교훈은 비슷했습니다. 기업들이 스마트한 정책과 우수 사례를 개발해야 한다는 것입니다. 전 직원에게, 나아가 협력 업체, 도급 업체 및 공급 협력 업체에까지 위험 인식 문화를 널리 퍼뜨려야 합니다. 이러한 계획은 각 조직의 최상위 직급에서 강력하게 지원해야 합니다. 왜냐하면, 보안은 조직의 생존이 걸린 문제이기 때문입니다.

이번 마지막 호에서는 보안의 미래를 좌우할 세 가지 과제를 살펴보겠습니다. 오늘날 IT 전문가의 영향력은 점점 커지고 있습니다. 자율 주행 자동차에서 스마트 그리드에 이르는 여러 가지 지능형 시스템의 수가 증가하여 잠재적인 공격 대상이 늘어남에 따라 취약성은 더 증가할 것입니다. 이러한 지능형 시스템은 과거 그 어느 때보다 더 많은 데이터를 생산할 것입니다. 따라서 위협에 대처하기 위해서는 더 빠른 속도로 보안 기술을 개발해야 할 것입니다.

과제 #1: 공격 대상의 증가 –

앞으로 35년 동안 전 세계 인구는 20억 명 이상 증가할 전망이며, 이는 현재의 인도와 중국의 인구수와 비슷한 수치입니다. 사람들은 대부분 도시에 거주할 것이며, 식품, 수도, 에너지, 교통 및 다양한 서비스가 필요해질 것입니다. 현재의 방식을 이용해 이 많은 사람에게 서비스를 제공하는 것은 거의 불가능할 것이며, 서비스를 계속 유지할 수 없을 것입니다. 더 저렴하고 더 지속 가능한 서비스에 대한 요구에 따라 더 지능적인 도시 환경이 개발될 것입니다. 다시 말하면, 많은 도시에서 발달된 정보 시스템을 통해 교통, 공익 시설, 보건 및 공공 안전을 모니터링 및 측정하고 최적화할 것이며, 이러한 시스템은 대부분 자동화될 것입니다. 네트워크는 확장되어 수십억 개의 센서와 작동 장치를 포함할 것이며, 그동안 예측되었던 "사물 인터넷(Internet of Things)"이 출현할 것입니다. 이러한 추세로 인해 기술 기업들은 거대한 시장의 성장을 맞이할 것입니다. 그러나 이를 위해서는 최초 설계 단계에서부터 가장 높은 수준의 보안을 갖춘 시스템이 필요합니다.

시속 100km의 속도로 고속 도로를 달리고 있는 차 안에 안전벨트와 에어백을 설치하거나, 공항에 착륙 중인 비행기에 충동 회피 시스템을 장착하려는 사람은 없을 것입니다. 이러한 상황을 피하고자 IBM에서는 소프트웨어와 시스템을 개발할 때 "설계를 통한 보안"이라는 철학을 실천하고 있으며 IBM 보안 엔지니어링 프레임워크를 이용하고 있습니다.[1] IBM 보안 엔지니어링 프레임워크는 글로벌 디지털 인프라가 최초 단계부터 보안을 유지하고 사후에 처리할 일이 없도록 보장할 수 있는 일련의 보안 엔지니어링 우수 사례입니다.

과제 #2: 대용량 데이터의 보안 –

기업과 정부는 새로운 데이터 스트림으로 시민, 직원 및 고객의 활동과 행동을 포착할 것이며, 따라서 관리하는 정보의 양은 계속하여 기하급수적으로 증가할 것입니다. IBM은 현재 250경 바이트에 달하는 데이터가 매일 생성되고 있는 것으로 추산하고 있습니다.[2] 일부 전문가는 2020년에 이르면 데이터 생산량이 4,300% 증가할 것으로 추산하고 있습니다.[3] 어떻게 하면 이러한 소중한 데이터의 보안을 유지할 수 있을까요? 어떻게 하면 데이터의 수명 주기 동안 무결성을 유지할 수 있을까요?

이를 실현하기 위한 한 가지 방법은 분석 시스템을 구축하고 구현하여 이상 상황과 위험을 더 확실히 탐지하는 것입니다. 여기에는 금융 거래 양식에서부터 개인 행동 양식의 변화에 이르는 넓은 범위의 데이터가 포함됩니다. 가장 좋은 방법은, 앞으로 접하게 될 수많은 데이터를 철저히 분석하여, 개인 정보를 침해하지 않으면서도 정보 생태계 전체의 보안을 더 확실히 유지하는 것일 것입니다. 이를 인지한 IBM은 최근 Q1 연구소를 인수하여 고객에게 최첨단 보안 정보 역량을 제공할 수 있게 되었습니다.

IBM은 현재 250경 바이트에 달하는 데이터가 매일 생성되고 있는 것으로 추산하고 있습니다.

IBM 연구소는 이러한 과제를 극복하기 위해 많은 계획을 구상하고 있습니다. 예를 들어, IBM의 스트림 컴퓨팅 제품을 이용하면 기업에서는 구조화되거나 구조화되지 않은 다수의 데이터 스트림을 실시간으로 처리할 수 있으며 이러한 데이터를 철저히 분석할 수 있습니다. 이러한 기술은 차세대 보안 정보를 이용하여 잠재적 보안 사고로 이어질 수 있는 서로 다른 점들을 연결하는 데 도움이 될 것입니다. 제퍼디 퀴즈쇼에서 우승한 왓슨 컴퓨터에 사용된 소프트웨어 아키텍처인 UIMA(Unstructured Information Management Architecture)는 페타바이트 단위의 데이터를 완벽히 처리할 수 있는 구조를 제공합니다. UIMA는 자연 언어를 포함시켜 상관관계를 검색하고 추정값을 생성합니다. 향후 버전에서는 위험이 존재하는 위치를 찾아내도록 발전될 수도 있을 것입니다.

과제 #3: 숙련된 전문가의 수요 증가 –

향후 10년간 보안 분야에는 대규모의 두뇌 집단이 유입되어야 할 것입니다. 증가하는 위협에 대처하기 위해서 정부와 기업은 새로운 세대의 보안 전문가를 육성 및 채용하여 전 세계의 중요한 정보 스트림을 구축하고 보안을 유지해야 합니다.

2011년에 Frost & Sullivan에서 발표한 보고서 "전 세계의 정보 보안 인력 연구"는 2015년경에 보안 분야의 일자리가 230만 개에서 420만 개로 증가할 것으로 추산했습니다.[4] 그렇지만 더 큰 과제는 명석한 두뇌의 바이러스 유포자와 전면전을 펼칠 수 있도록 정예 보안 전문가를 육성하여 팀을 꾸리는 것입니다. CIA의 비밀 정보 기술국의 설립자이자 책임자인 짐 고슬러 국장은 2010년에 미국 공영 라디오 인터뷰에서 최정예 기술을 가진 인재의 부족이 심각하다고 밝힌 바 있습니다. 고슬러 국장은 현재 세계 정상급 전문가 중 1,000명 정도만이 전 세계의 네트워크를 보호하기 위해 일하고 있다며, 10,000 ~ 30,000명의 인력이 필요하다고 말했습니다.[5]

각 조직은 이러한 기술적 차이를 해결하기 위해 두 가지 방법을 실행할 수 있을 것입니다. 단기적으로, 더 나은 보안 환경을 유지하기 위해 아웃소싱을 할 수 있을 것입니다. IBM은 이러한 역량에 많은 투자를 해 왔으며 전 세계 10개 지역에서 보안 활동 센터를 운영하고 있습니다. 두 번째 방법은 장기적 관점의 해결책으로 수학 및 과학 교육 발전에 특별히 많은 노력을 기울이는 것입니다. 현재 IBM 연구소는 비즈니스 관점의 사이버 보안 수요와 관련된 실용적인 의견을 공유할 수 있는 학술 커뮤니티를 위한 플랫폼을 구축하고 있습니다. IBM은 미래를 위해 필요한 커리큘럼, 기술 및 전문 지식을 구축하기 위해 일류 학술 기관 및 정부 조직과 협력을 시작했습니다. 또한, 보안 능력이 부족한 지역의 기술을 향상시키기 위한 계획을 개발하고 있습니다. 하지만, 한 세대의 보안 전문가를 육성하기 위한 이러한 노력이 성공한다고 해도, 그것은 해결책의 일부일 뿐입니다.

"전 세계의 정보 보안 인력 연구"는 2015년경에 보안 분야의 일자리가 230만 개에서 420만 개로 증가할 것으로 추산했습니다.

출처: Frost & Sullivan

소규모 그룹의 보안 전문 지식이나 최첨단 기술의 구현 만으로는 보안 분야의 미래를 보장할 수 없습니다. 각 조직과 사회가 위와 같은 세 가지 과제를 완전히 해결하기 위해 공동의 노력을 기울여야 합니다. 이러한 메시지는 상부에서 하달되어 널리 퍼져야 합니다. 현재의 과제를 해결하기 위한 유일한 방법은 위험 인식 문화를 더 널리 퍼뜨려 각 개인이 위험을 직관적으로 이해하도록 하고, 고도로 발달한 네트워크 환경에서 삶을 영위하고 비즈니스를 운영하는 데 수반되는 책임을 받아들이도록 하는 것입니다.

대화에 참여하세요

ibm.com/smarter/cai/security를 방문하면 더 많은 기사를 읽고, CIO에게 필요한 보안 정보를 더 자세히 알아보고, 다른 보안 전문가와 의견을 공유하실 수 있습니다.

저자 소개

크리스틴 러브조이(Kristin Lovejoy)는 IBM 보안 서비스 총책임자입니다. (이메일 주소: klovejoy@us.ibm.com)

조안 마틴(Joanne Martin) IT 위험 관리 부사장은 IBM CIO 사무국의 정보 보안 총책임자입니다. (이메일 주소: j1mart@us.ibm.com)

IBM Center for Applied Insights 소개

IBM Center for Applied Insights(ibm.com/smarter/cai/value)에서 새로운 사고 방식, 작업 방식 및 업무 지휘 방식을 확인하실 수 있습니다. IBM Center for Applied Insights는 실증적인 자료를 바탕으로 한 연구를 통해 실용적인 안내와 변화의 사례를 제공해 드립니다.

1 www.redbooks.ibm.com/redpieces/abstracts/redp4641.html
2 http://www-03.ibm.com/press/us/en/pressrelease/37491.wss
3 http://www.csc.com/insights/flxwd/78931-big_data_growth_just_beginning_to_explode
4 The 2011 (ISC)2 Global Information Security Workforce Study https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC%20Study_020811_MLW_Web.pdf
5 "Cyberwarrior Shortage Threatens U.S. Security", NPR.org http://www.npr.org/templates/story/story.php?storyId=128574055

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
October 2012

WGW03017USEN-00