IBM Center for Applied Insights

SecurityIntelligence

경영진 시리즈

CIO를 위한 보안 필수 요소

확신을 기반으로 혁신 추진

IBM

매일같이 새로운 정보들이 기업으로 흘러 들어와 첨단 분석과 스마트한 의사결정이 이루어집니다. 직원, 고객 및 계약 당사자들은 갖가지 기술을 통해 모두 그 어느 때보다 긴밀히 연결되어 있습니다. 하지만 이렇게 널리 확산되고 겹겹이 중복된 네트워크로 인해 보안에 관한 문제를 해결하기는 힘에 부칩니다. 복잡성은 현기증이 날 지경이고 공격을 받을 수 있는 지점에는 제한이 없습니다. CIO는 절망적인 상황에서 고군분투를 벌이는 와중에 다음과 같은 의문이 듭니다. 이토록 복잡하게 얽히고 설켜 있는 환경에서 강력한 보안이 가능하긴 한 것일까? 정답은 "예" 입니다. 하지만 이를 위해서는 프로세스와 사고방식에 근본적인 변화가 필요합니다. IBM은 자체적인 사내 전략을 구현하였으며 21세기의 보안 인텔리전스 실현을 위한 10가지 필수 요건을 정립했습니다.

New York의 해가 떠오르자 마자 영업 담당 부사장은 침대에서 일어나 스마트폰을 통해 Malaysia에 대형 입찰 기회가 있다는 사실을 확인합니다. 이 소식은 곧 일파만파로 퍼져나갑니다. 아침식사를 하기도 전에 글로벌 팀의 여섯 멤버는 화상 회의를 진행하고 그 중 한 명은 Stockholm에서 Skype 연결을 통해 참여합니다. 세 명의 계약 당사자들이 휴대폰을 통해 3자 통화를 합니다. 그 날 하루 동안 전자 메일이 전 세계를 돌아 전송되며 그 중 절반은 회사 네트워크를 사용하고 나머지는 Gmail과 Yahoo를 거쳐갑니다. New York에서 저녁이 되면 계약이 완료됩니다. 그 후 몇 시간 내에 참가자 중 일부는 LinkedIn에서 친구가 됩니다.

91%

의 업무용 스마트폰 사용자가 회사 전자 메일에 연결하지만 규정에 따라 모바일 보안 소프트웨어를 설치해야 하는 사용자는 그 중 1/3에 불과합니다.

출처: Kaspersky Labs
http://usa.kaspersky.com/sites/usa.kaspersky.com/files/Enterprise%20Mobile%20Survey.pdf

오늘날 관리자들이 지적 능력과 대량의 데이터를 즉시 수집하고 이를 활용하여 정보에 기반한 현명한 의사결정을 신속히 내릴 수 있다는 것은 잘 알려진 사실입니다. 하지만 이것은 상호 연결된 네트워크의 힘, 즉 속도, 개방성, 그리고 세계 어디에서나 손쉬운 액세스로부터 기인하며, 이로 인해 무수한 취약성 또한 발생합니다. 또한 수천 개의 장치와 수십여 가지 공용 웹 기반 서비스에서 쏟아지는 정보 덕분에 기업에서 네트워크의 보안을 유지하는 작업은 계속 복잡해지기만 합니다. Kaspersky Lab의 연구 보고서에 따르면 91%의 업무용 스마트폰 사용자가 회사 이메일에 연결하지만 규정에 따라 모바일 보안 소프트웨어를 설치해야 하는 사용자는 그 중 1/3에 불과합니다. 이러한 환경에서는 누구나 쉽게 접근이 가능하며, 범죄 조직도 그 중 하나로 종종 포함됩니다.

범죄 조직은 인터넷에 연결된 PC와 모바일 장치를 범죄를 위한 주요 자산으로 간주합니다. 이들은 감지가 어려운 악성 소프트웨어에 장치를 감염시키는 수법으로 운영 기반을 확대해 나갑니다. 절도범에게 있어 기업 네트워크는 비밀번호, 사용자 ID, 비즈니스 기밀 및 개인 정보와 같은 디지털 보물로 넘쳐나는 보고입니다. 디지털 침입자는 또한 정부 부처에서 통신 네트워크에 이르는 전략적 자산을 목표로 합니다.

일부는 비즈니스 운영을 혼란에 빠뜨립니다. Gartner에서 추정한 바에 따르면 소비자 PC의 20 – 30%가 범죄 행위의 인프라로 사용될 수 있는 봇넷 및 악성 소프트웨어에 의해 위험에 처한 경험이 있다고 합니다. 개인 소유 기기의 업무용 사용을 허용할지 여부를 고려 중인 기업이 늘어나면서 감염 가능성이 매우 현실적인 우려로 다가옵니다.

20 –30%

의 개인 PC는 악성 소프트웨어를 호스트하거나 범죄를 저지르는데에 일부 시간이 사용되고 있습니다.

출처: http://www.computerweekly.com/opinion/CW-Security-Think-Tank-How-to-prevent-security-breaches-from-personal-devices-in-the-workplace

컴퓨터가 단 한대만 감염되어도 심각한 손상을 일으킬 수 있습니다. 현재까지 가장 인상적인 예 중 하나는 산업용 소프트웨어와 장비에 심각한 손상을 주도록 제작된 매우 정교한 웜인 Stuxnet입니다. 2009년 봄, 이 웜은 대부분 이란에 위치한 시스템을 통해 확산되기 시작했습니다. 누군가의 감염된 썸드라이브(Thumb Drive)를 통해 이 웜이 유입되었습니다. Siemens 소프트웨어 프로그램을 실행하는 시스템을 타겟으로 개발된 이 웜은 수많은 산업 시스템에 큰 피해를 입혔습니다.

기업 보안 책임자가 배워야 할 교훈은 명확합니다. 웜이 이란 또는 다른 곳에서 강력하게 보호되는 산업을 뚫고 들어올 수 있다면 전 세계를 돌아다니는 Twitter, Facebook, 문자 메시지 및 Skype를 사용하는 전문 인력에게서 틈을 발견하는 것은 식은 죽 먹기일 것입니다. 더욱이, 웜이 산업 장비를 무력화할 수 있다면 다른 종류의 악성 소프트웨어는 공급망을 차단하고 트래픽을 변경하고 전력망을 손상시키는 등 각종 재난을 불러올 수 있지 않을까요?

이렇게 늘어나는 문제에 대응하려면 기업에 **새로운 유형의 보안 리더**가 필요합니다. 기업은 무수한 기술 위협뿐만 아니라 전략적 문제에도 적절히 대응해야 합니다. 폭넓게 공유해야 하는 정보는 무엇일까요? 중요 정보에 대한 액세스 권한을 누구에게 부여해야 하고 이를 어떻게 보호해야 할까요? 기술 문제에 전략적 문제가 더해지면 매우 복잡해집니다. 또한 복잡한 만큼 일일이 솔루션으로 대응하고 싶은 유혹이 들긴 하지만 미래를 내다보는 경영진은 그러한 방식으로는 방어가 불가능하고 경제적 여유가 없으며 궁극적으로 성과가 없다는 것을 깨닫습니다.

유일한 해답은 기업 운영 방식을 근본적으로 바꾸는 것입니다. 기술 담당자와 이들의 시스템에서부터 기업 내의 모든 직원, 그리고 비즈니스를 함께하는 모든 사람까지 **기업 보안의 사명을 확대**하는 것에서 시작합니다. 모든 사람이 침해 가능성을 안고 있으며, 모든 사람이 또한 해결책이 되어야 합니다. 성공은 결국 강력하고 지속적인 인식, 즉 **위험 인식 문화**에 달려 있습니다.

위험 인식 문화는 최신 기술만으로는 부족하며 모범 사례 및 그 이상으로 확장이 필요합니다. 이것은 보안에 대한 실용적 접근법에 따라 기업의 각 레벨에서 모든 의사결정 및 절차가 진행되는 새로운 사고방식을 의미합니다. 최고 경영자에서부터 하계 인턴 사원에 이르기까지 모두가 정보를 처리하는 방식을 바꾸어야 합니다. 이러한 문화 안에서는 데이터에 대한 안전한 처리가 안전 벨트를 조이거나 안전한 장소에 성냥을 쌓아두는 것과 같이 간단하고 자연스러워집니다.

이는 보안에 대한 실용적 접근법에 따라 기업의 각 레벨에서 모든 의사결정 및 절차가 진행되는 새로운 사고방식을 의미합니다.

더 이상 결정을 미룰 수 없습니다. 기업의 보안은 커다란 변화를 향해 빠른 속도로 달려가고 있습니다. 해당 요소에 대해 생각해 보십시오. 범죄 집단에서는 전문가가 아마추어를 점령해 왔습니다. 이로 인해 위험은 더 커집니다. 동시에, 기업에서는 광범위하게 분산된 운영, 마케팅, 영업 및 고객 서비스에 대한 광범위한 분산을 통해 효율성을 확보했지만 이는 취약성을 곱절로 증가시킵니다.
현재는 회사의 전체 비즈니스가 디지털로 관리되기 때문에 침입이 발생할 경우 그 결과는 기업 전체를 뒤흔들 수 있습니다. 요약하면, 절도범들은 매우 노련하고, 수많은 디지털 관문과 창으로 살며시 들어오며, 그 안에는 매우 귀중한 것이 숨겨져 있습니다.

비록 이후 대가는 매우 값지지만 보안으로 가는 길은 어렵고 혼란스러울 수 있습니다. 오늘날 보안 제품과 서비스가 시장에 넘쳐남에도 불구하고 고객들은 최근 보안 위험이나 준수 규정에 관한 각종 뉴스들을 접하면서 좌절하고 있습니다. 많은 사람들이 어디서부터 시작해야 할지 또는 무엇을 믿어야 할지에 대한 확신이 없으며 종종 보안 및 준수를 측정이 불가능한 가치에의 투자, 불확실한 ROI 및 도로의 과속 방지턱 정도로 여깁니다. 이러한 오해로 인해 의사결정을 망설이거나 최악의 경우 두려움 때문에 혁신을 포기하게 됩니다.

기업을 보호하는 일이 엄청난 작업이며 결코 완전하지 않다는 사실을 부정할 수는 없습니다. 문화를 바꾸는 일은 더욱 어렵습니다. 하지만 이는 반드시 필요한 작업입니다. 강력한 보안은 비즈니스의 존속을 위한 비용이며 실현가능한 것 입니다.

IBM은 필요한 혁신과 위험 통제의 필요성 사이에 균형을 유지하는 방법을 찾기 위해 끊임없이 노력 중입니다. IBM의 포괄적인 대응 방법에는 기술, 프로세스, 정책 과제가 포함되어 있으며 10가지 필수 실행 요소로 구성되어 있습니다. 다음 몇 개월 동안 당사에서는 이에 대한 자세한 내용을 소개하는 백서를 연재할 예정입니다. 다음은 이에 대한 간략한 소개입니다.

필수 보안 요소

1. 위험 인식 문화 형성

가장 기본이 되는 아이디어입니다. 의심스러운 첨부파일을 클릭하거나 스마트폰에 보안 패치를 설치하지 않는 경우 누구나 회사 네트워크를 감염시킬 수 있습니다. 안전한 기업을 만드려는데에 모두가 참여해야 합니다. 위험 인식 문화는 위험과 목표를 설정하고 이를 널리 퍼뜨림으로써 형성됩니다. 하지만 문화 자체의 변화가 중요합니다. 부모가 휴대폰으로 통화하는 사이 어린아이가 도로로 뛰어드는 것을 목격하는 경우 많은 사람이 경험하는 반사적인 반응(예: 공포)을 떠올려 봅시다. 회사 전체적으로 동료가 보안에 관해 부주의할 경우 이렇게 즉각적으로 반응하는 분위기가 형성되어야 합니다. 물론, 경영진은 위에서부터 이러한 변화가 이루어지도록 강력히 추진하는 동시에 진행 상황을 추적할 수 있는 도구를 구현해야 합니다.

2. 사고 관리 및 대응

Brazil과 Pittsburgh에서 두 건의 유사한 보안 사고가 발생했다고 가정해 보겠습니다. 이 둘은 서로 연관이 있을지도 모릅니다. 하지만 이들을 연결하는 보안 인텔리전스가 없다면 사고 발생 가능성을 알려줄 지도 모르는 중요한 패턴을 놓칠 수 있습니다. 지능형 분석 및 자동화된 대응 기능을 구현하려는 전사적인 노력이 반드시 필요합니다. 자동화되고 통일된 시스템을 구현하면 기업의 운영을 모니터링하고 신속히 대응할 수 있습니다.

3. 워크플레이스 보호

사이버 범죄자는 취약한 곳이 없는지 지속적으로 조사합니다. 각 워크스테이션, 랩톱 또는 스마트폰은 악의적인 공격을 위한 진입점이 될 수 있습니다. 각 장치의 설정을 개인 또는 자율적인 그룹에 미뤄두어서는 안 됩니다. 모든 장치를 중앙에서 관리 및 규제해야 합니다. 기업에서 데이터의 이동 경로를 각 경로의 자체 위험 프로파일에 따라 분류하고 경로 내의 사용자간에만 데이터가 이동되도록 제한해야 합니다. 직원을 보호한다는 것은 혼란을 극복하고 이를 확신으로 바꾸는 것을 의미합니다.

4. 설계 단계에서 보안 적용

자동차 회사가 안전벨트나 에어백 없이 차량을 생산한 다음 나중에 위험한 상황이나 사고가 생긴 뒤에 부품을 갈아끼운다고 상상해 보십시오. 이는 무의미한 동시에 엄청난 비용만 소요되는 행위입니다. 마찬가지로, 정보 시스템에서의 최대 취약점 및 비용의 낭비는 서비스를 먼저 구현하고 나서 보안을 나중에 추가하는 데서 발생합니다. 유일한 해결책은 처음부터 보안을 구현하고 준수 여부 추적을 위해 정기적으로 자동 테스트를 수행하는 것뿐입니다. 이 방법으로 비용도 절감할 수 있습니다. 애플리케이션 안에 보안 기능을 구현하는 데는 60달러만 추가하면 되지만 이 기능을 나중에 추가하려면 최고 100배나 비싼 6천 달러까지도 소요될 수 있습니다.

5. 최신 상태로 유지

이 문제는 항상 발생합니다. 사람들은 익숙하고 편안하다는 이유로 이전 버전의 소프트웨어에 집착합니다. 하지만 버전이 뒤섞인 소프트웨어의 업데이트 상태를 관리하기란 불가능에 가깝습니다. 또한 소프트웨어 기업에서 이전 프로그램용 패치 제공을 중단하기도 합니다. 사이버 범죄자도 이 사실을 너무나 잘 알고 있습니다. 안전한 시스템이라면 관리자가 실행 중인 모든 프로그램을 추적하고 해당 프로그램이 최신 버전이라는 확신을 가지며 업데이트 및 패치가 릴리스되면 바로 이를 설치할 수 있는 포괄적 시스템을 보유해야 합니다.

6. 네트워크 액세스 제어

도시에서 범죄가 발생한 경우를 가정해 보겠습니다. 시내의 모든 차량이 라디오 태그를 휴대하고 제한된 간선도로만을 따라 이동하며 각 차선에 센서가 설치되어 있다면 경찰의 수사가 훨씬 수월해질 것입니다.

이는 데이터도 마찬가지입니다. 모니터링되는 액세스 포인트를 통해 데이터의 채널이 등록된 기업에서는 훨씬 간단하게 악성 소프트웨어를 발견하고 고립시킬 수 있습니다.

7. 클라우드에서의 보안

클라우드 컴퓨팅은 막대한 효율성을 제공합니다. 하지만 위험도 따를 수 있습니다. 특정 IT 서비스를 클라우드로 마이그레이션 중인 기업의 경우 여러 문제로 어려움을 겪게 되며 이러한 문제 중에는 사기꾼도 포함될 수 있습니다. 그런 면에서, 클라우드는 일정 비율의 고객이 무서운 전염병을 보유한 채 투숙 중인 호텔과 같습니다. 이러한 환경을 극복하려면 투숙객은 자신을 남들로부터 격리하고 가능한 위협을 모니터링할 수 있는 도구와 절차를 가지고 있어야 합니다.

8. 이웃 감시

시스템에 액세스해야 하는 계약자가 있습니다. 해당 계약자에게 시스템의 정확한 비밀번호를 어떻게 알리시겠습니까? 메모장에 비밀번호를 남겨둘까요? 메신저로 알려주시겠습니까? 그러한 방법은 위험합니다. 기업의 보안 문화는 회사 밖으로까지 확대되어야 하며 계약 당사자와 공급업체간에도 모범 관행을 정립해야 합니다. 이는 이삼십 년 전의 품질 관리 추진 절차와 유사합니다. 논리는 동일합니다. 우수한 품질과 마찬가지로 보안도 에코시스템 전체에 주입되어야 합니다. 한 기업에서 부주의가 가져오는 악영향이 사회 전체를 혼란에 빠뜨릴 수 있습니다.

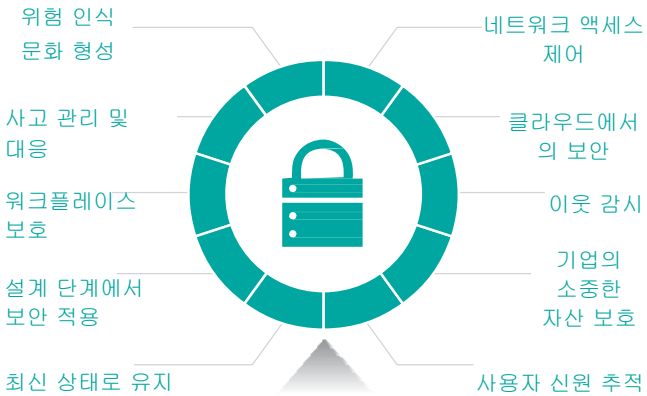
9. 기업의 소중한 자산 보호

회사에 보관된 자료들 중 어딘가에 아마도 과학 및 기술 데이터이거나 인수 합병 관련 문서일 수도 있고 고객의 비공개 재무 정보와 같은 매우 소중한 보물이 섞여 있을 것입니다. 각 기업은 특별한 취급을 필요로 하는 중요 데이터에 대한 인벤토리를 작성해야 합니다. 기업의 생존이 걸린 것처럼 우선 항목 각각을 보호, 추적 및 암호화해야 합니다. 이는 결코 과장된 표현이 아니며, 실제로 사활이 달려있는 경우도 있습니다.

10. 사용자 신원 추적

계약자가 전일 근무자로 채용됩니다. 6개월 후 승진을 합니다. 1년 후 경쟁업체에서 해당 계약자를 전격 스카우트합니다. 시간이 지나면서 시스템은 해당 사용자를 어떻게 취급할까요? 처음에는 데이터에 대한 제한적인 액세스 권한을 부여한 다음 점차 권한을 확대해 나가고 최종적으로 삭제해야 합니다. 이것이 ID 수명 주기 관리입니다. 이 수명 주기는 매우 중요합니다. 이를 올바르게 관리하지 않는 기업은 앞이 보이지 않는 것과 같으며 침입에 취약해질 수 있습니다. 이 위험을 해결하려면 사용자를 식별하고 권한을 관리하고 퇴사 시 즉시 권한을 취소하는 정교한 시스템을 구현해야 합니다.

어떻게 하면 확신을 가지고 혁신을 추진할 수 있을까요?



위험 관리와 혁신 실현의 균형 유지

대화에 참여

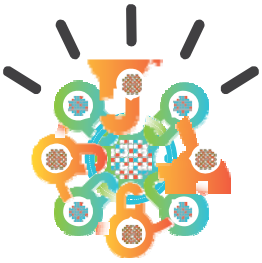
다른 기사를 읽거나 자세한 내용을 알아보거나 귀하의 의견을 다른 보안 리더와 공유하려면 **ibm.com/smarter/cai/security**를 방문하십시오.

저자 소개

Kristin Lovejoy는 IBM CIO Office의 IT 위험 부문 부사장입니다. 연락처: **klovejoy@us.ibm.com**.

IBM Center for Applied Insights 소개

IBM Center for Applied Insights는 심도 있는 컨텐츠와 분석 전문성을 통합하여 고객이 새로운 가치 실현 과정을 계획할 수 있도록 지원합니다. 조직에서 실천할 수 있는 실용적인 지침을 사용하여 연구를 수행하고 자산을 구축합니다.



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

Produced in the United States of America
January 2012

CIE03116-USEN-00