Executive Series

CIO를 위한 보안 필수 사항

자신감을 통한 혁신 수용

IBM

매일 끊임없이 새로운 정보가 기업으로 유입되면서 최신 분석을 수행하고 스마트한 의사결정을 내리는 데 큰 도움이 되고 있습니다. 직원, 고객 및 비즈니스 파트너들은 수없이 많은 기술 속에서 과거 그 어느 때보다 더 복잡하게 연결되어 있습니다. 그러나 이와 같이 복잡하고 중복된 네트워크는위협적인 보안 문제를 일으킬 소지가 있습니다. 공격 받을 수 있는 지점이 무한대에 가까울 정도로 복잡하기가 이루 다 말할 수 없습니다. 따라서 CIO들은 점점 늘어나는 고민과 문제로 고심하고 있습니다. 오늘날 IT 자산의 연결이 폭증하는 시대에도 강력한 보안이 가능할까요? 이 질문에 쉽게 동의할 수는 있습니다. 그렇지만 프로세스와 태도에 근본적인 변화가 필요합니다. IBM은 자체적인 사내 전략을 구현했으며 21세기의 보안 인텔리전스 실현에 필요한 10가지 필수 사항을 마련했습니다.

뉴욕의 아침이 밝아오면 영업 담당 부사장이 잠자리에서 일어나 스마트폰을 통해 말레이시아 시장에 엄청난 영업기회가 있다는 사실을 확인합니다. 이 뉴스는 일련의 의사소통을 통해 전달됩니다. 아침 식사 전에 6명의 글로벌 팀원들은 텔레컨퍼런스에 참석합니다. 이들 중 한 명은 스톡홀름에서 스카이프(Skype)를 통해 연결합니다. 3명의 계약직 직원들은 휴대폰으로 접속합니다. 하루 종일 전 세계에 걸쳐 이메일이 오가고 이들 중 절반은 회사 네트워크를 통해 이루어지며, 나머지는 Gmail과 Yahoo를 통해 이루어집니다. 업무 시간이 끝나면 거래가 마감됩니다. 퇴근 시간에는 참석자 친구들 몇 명이 서로 LinkedIn을 통해 모입니다.

기업 스마트폰 사용자 중 91%가 사내 이메일에 접속하지만 3명 중 1명에게만 모바일 보안 소프트웨어가 설치되어 있습니다.

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

오늘날 관리자들이 기가바이트에 달하는 데이터와 지식을 순식간에 모은 다음 이를 활용하여 보다 빠르고 효율적인 의사결정을 내리고 있습니다. 그러나 아무리 네트워크가 강력하게 상호연결되어 있고 속도와 개방성 측면에서 우월하여 전 세계 어디서나 액세스할 수 있더라도 네트워크의 취약성은 빠질 수 없는 문제입니다. 수천 대의 디바이스와 공개 웹 기반 서비스를 통해 엄청난 양의 정보가 쏟아짐에 따라 사내 네트워크의 보안 업무는 끝없이 복잡해지고 있습니다. Kaspersky Labs의 연구에 따르면 사내 스마트폰 사용자의 91%가 사내 이메일에 접속하지만 3명 중 1명만 모바일 보안 소프트웨어를 설치하고 있습니다. 이러한 환경하에서는 범죄 조직을 포함해, 누구나 쉽게 액세스할 수 있습니다.

범죄 조직은 오늘날 인터넷 연결 PC와 모바일 디바이스를 주요 자산으로 간주하고 있습니다. 이들은 감지가 어려운 악성 코드를 디바이스에 주입하여 범죄 활동 범위를 확장합니다. 절도범들에게 기업 네트워크는 암호, 사용자 ID, 영업 비밀, 개인 정보 등 디지털 자산으로 넘쳐나는 장소입니다. 온라인 침입자들은 정부 문건부터 통신 네트워크에 이르기

까지 모든 전략적 자산을 목표로 합니다. 이들 중 일부는 비즈니스 운영의 방해를 목표로 둡니다. Gartner에 따르면 소비자 PC의 20 ~ 30%가 범죄 활동의 인프라로 사용될 수 있는 봇넷 및 악성 코드의 침입을 받은 것으로 나타났습니다. 많은 기업들이 개인 소유 디바이스의 기업 내 사용을 고려하고 있는 상황에서 감염 가능성은 매우 현실적인 문제입니다.

소비자 PC의 20 ~ 30%는 악성 코드 호스팅 및 시간제 기반의 범죄 용도로 사용되고 있습니다.

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

한 대의 컴퓨터가 감염되어도 심각한 손실로 이어질 수 있습니다. 최근 산업용 소프트웨어 및 장치 손상을 위해 매우 정교하게 만들어진 웜 바이러스 Stuxnet 사례가 있었습니다. 2009년 봄 이란 대부분의 지역에 시스템을 통해 웜 바이러스가 퍼지기 시작했습니다. 누군가 오염된 USB 드라이브로 전염시킨 것으로 보였습니다. Siemens 소프트웨어 프로그램을 실행하는 시스템을 대상으로 개발된 이 웜 바이러스는 수많은 산업용 시스템을 손상시켰습니다.

기업 보안 리더가 얻은 교훈은 확실합니다. 웜이 철통 보안으로 이루어진 이란과 기타 지역을 감염시킬 수 있다면 Twitter, Facebook 및 Skype 역시 안전하다고는 말할 수 없을 것입니다. 뿐만 아니라, 웜 바이러스로 산업용 장치를 무력화시킬 수 있다면 다른 웜 바이러스로 공급망을 차단하고, 트래픽을 조작하고 전력 시설을 손상시키는 행위 등도 가능합니다.

이렇게 증가하는 도전 과제에 대처하려면 **새로운 보안 리더**가 필요합니다. 당연히 수없이 많은 기술적인 위협 요소와 전략적인 문제에 대처할 수 있어야 합니다. 그렇다면 어떤 정보를 폭넓게 공유해야 할까요? 특정 정보에 액세스해야 하는 주체는 누구이며 이러한 정보를 어떻게 보호해야 할까요? 이와 함께 기술 및 전략적 도전 과제는 점점 더 복잡해지고 있습니다. 해결방안이 조금 더 복잡해도 대처할 수 있다는 유혹을 극복하지 못하고 통찰력을 잃은 경영진들은 이러한 방법을 지지하지도, 실행하지도 못한 채 결국에는 아무런 성과도 얻지 못합니다.

유일한 방법은 근본 단계에서 기업의 운영 방식을 바꾸는 것입니다. 이러한 변화는 기술 담당자 및 사내 시스템에서부터 기업 내 모든 직원들과 회사와 거래하는 모든 사람들에 이르는 모든 대상으로 **기업 보안의 사명을 확장**하는 것에서 출발합니다. 이것은 단지 시작에 불과합니다. 직원들 누구나 잠재적 침투에 노출된 존재이므로 각자가 하나의 솔루션을 대표해야 합니다. 결국 성공은 **리스크 인식 문화**라는 탄탄하고 일관된 규정에 달려 있습니다.

리스크 인식 문화는 더 최신의 기술을 요구하고 성공 사례 이상으로 확장합니다. 또한 보안에 대한 실용적 접근법으로 기업 내 모든 의사결정 및 모든 레벨의 절차를 안내하는 새로운 사고 방식을 나타냅니다. 이 것은 C 레벨 경영진부터 인턴에 이르기까지 모든 임직원들이 정보를 처리하는 방식을 새롭게 제시합니다. 이 문화에서 데이터 보안 절차는 안전 벨트를 매거나 성냥을 안전한 장소에 보관하는 것과 같은 차선책이 됩니다.

이 문화는 보안에 대한 실용적 접근법으로 기업 내 모든 의사결정 및 모든 레벨의 절차를 안내하는 새로운 사고 방식을 나타냅니다.

이것은 지연을 위한 의사결정이 아닙니다. 기업 보안은 빠른 속도로 전환하고 있습니다. 그 요인을 생각해 보시기 바랍니다. 범죄 세계에서 전문가들은 아마추어들을 제쳤습니다. 이것은 기업에 가해지는 위협을 촉진합니다. 동시에 기업은 경영, 마케팅, 영업 및 고객 서비스에 대한 데이터를 온라인으로 널리 활용하여 생산성을 극대화하고 임직원들에게 "권한을 부여"했습니다. 이것은 네트워크의 취약성을 부추깁니다. 오늘날 기업 비즈니스의 총체적 제어가 온라인으로 가능해지면서 온라인 침입의 결과는 기업 전체를 뒤흔들고 있습니다. 요약하면 범죄자들의 기술은 날로 발전하고 있어 이들이 온라인을 통해 침입할 수 있는 통로는 수없이 많으며 임의로 코드를 조작하는 것은 일도 아닙니다.

이렇게 위험성은 높지만 보안에 대한 해결책은 너무나 어렵고 혼란스럽습니다. 오늘날 시장에는 보안 제품 및 서비스가 부족하지는 않지만 고객들은 종종 업계가 제공하는 보안 제품에 대해 주저 없이 실망을 토로합니다. 이들 제품은 구입 후 얼마 되지 않아 취약성을 야기하고 최신 보안 위험 또는 컴플라이언스 준수 여부에 대한 적합성을 모색해야 하기 때문입니다. 많은 기업들은 어디서 시작할 것인지, 무엇을 신뢰할 것인지 잘 모르는데다 보안 및 컴플라이언스를 계량 불가능한 가치, 믿을 수 없는 ROI 및 진로를 방해하는 장애물로 가득한 일종의 투자로 인식합니다. 이러한 혼란은 종종 의사 결정의 포기로 인해 혁신에 반대되는 역행으로 이어집니다.

기업 보안은 엄청난 임무지만 절대로 완료할 수 없는 사안이라는 것은 부인할 수 없는 사실입니다. 뿐만 아니라, 문화를 바꾸는 것도 쉬운 일은 아닙니다. 그러나 반드시 해야 하는 일입니다. 강력한 보안은 비즈니스를 그대로 유지하기 위해 필요한 것으로, 이를 실현하는 길은 그리 멀리 있지 않습니다.

IBM은 필요한 혁신과 리스크 관리 에 대한 요구를 조화시키기 위해 꾸준히 노력하고 있습니다. 기업의 포괄적 대응력은 기술, 프로세스 및 정책적 기준을 포함합니다. 여기에는 10가지 필수 절차가 필요합니다. 몇 개월 후에는 일련의 백서를 통해 더 자세한 내용을 설명드릴 예정입니다. 지금은 간단히 요약 내용만 소개하겠습니다.

보안 필수 사항

1. 리스크 인식 문화 구축

이 아이디어는 매우 기본적인 내용을 바탕으로 합니다. 개개인 누구나 의심스러운 첨부 파일을 클릭하거나 스마트폰에 보안 패치를 설치하지 않음으로써 기업 시스템을 감염시킬 수 있습니다. 따라서 안전한 기업을 만들기 위한 노력은 직원 모두가 참여해야 합니다. 리스크 인식 문화를 수립하려면 리스크 및 목표 설정과 이를 기업 전역에 전파해야 합니다. 그러나 중요한 변화는 문화적 측면에 있습니다. 아이는 도로에 뛰어들고 있는데 부모는 휴대 전화로 수다를 떨고 있는 모습을 상상한다면 무감각한 반응을 통해 얼마나 무서운 결과가 초래되는지 알 수 있습니다. 동료가 보안에 대해 부주의하면 기업에서도 이와 동일한 일이 벌어집니다. 경영진은 물론 이러한 변화를 하향식으로 추진해야 하지만 진행 상황을 추적하기 위한 방안도 필요합니다.

2. 사건 및 대응 관리

브라질과 피츠버그에서 각각 2건의 사건이 발생했다고 가정해 보겠습니다. 이들 사건은 연관되었을 수 있습니다. 그러나 두 사건 간의 연관성을 찾는 데 필요한 보안 인텔리전스가 없다면 잠재적 사건을 암시할 수 있는 중요한 패턴을 누구도 알아채지 못할 것입니다. 지능형 분석 및 자동 대응 기능을 구현하기 위한 전사적 노력이 절실히 필요합니다. 자동화된 통합 시스템을 구축하면 기업이 자사 운영을 모니터링하고 사건에 신속히 대처할 수 있습니다.

3. 업무 공간 보호

사이버 범죄는 취약점이 지속적으로 존재하고 있음을 입증합니다. 각 워크스테이션, 노트북 또는 스마트폰은 악성 해커들이 침투할 수 있는 잠재적 경로입니다. 각 디바이스의 설정을 개인 또는 자치 부서에 그대로 맡겨둔 채 방치해서는 안됩니다. 이러한 설정은 모두 중앙 관리 및 규제를 통해 운영해야 합니다. 기업 전역에 걸쳐 오가는 데이터는 분류를 통해 각각에 고유한 리스크 프로파일이 지정되고 사용자 경로에 따라 하나씩 경로를 파악할 수 있어야 합니다. 직원 보안이란 혼란을 막고 자신감으로 무장하는 것입니다.

4. 보안 설계

자동차 회사가 자동차 제조 과정에서 안전 벨트 또는 에어백을 넣지 않고 나중에 추가한다면 위험 또는 사고로 이어질 수 있습니다. 그것은 무의미하고 막대한 비용이 드는 일이 될 수 있습니다. 비용 낭비와 동일한 차원에서 정보 시스템의 가장 큰 취약점 중 하나는 서비스를 먼저 구축하고 나서 보안을 나중에 추가하는 것에서 발생합니다. 유일한 해결 방법은 보안을 처음부터 구축한 다음 정기적인 자동 테스트를 실행하여 준수 여부를 추적하는 것입니다. 이것은 비용 절감과도 직결됩니다. 애플리케이션에 보안 기능을 구축하기 위해 60달러가 더 든다면 나중에 추가할 경우 비용은 이보다 100배에 달하는 6천달러가 될 수 있습니다.

5. 정리된 상태로 유지

이것은 항상 일어나는 일입니다. 사용자들은 익숙하다는 이유로 업그레이드 없이 지금 쓰고 있는 소프트웨어 버전을 고집합니다. 그러나 소프트웨어 업데이트 관리가 엉망이 되면 다음 버전으로 업그레이드가 불가능할 수 있습니다. 또한 어떤 소프트웨어 회사는 종종 이번 버전 프로그램에 대한 패치 제공을 중단하는 경우도 있습니다. 사이버 범죄자들은 이런 사실을 너무 잘 알고 있습니다. 보안 시스템에서 관리자들은 실행 중인 모든 프로그램을 추적하여 최신 버전임을 자신있게 식별하고 버전별 업데이트 및 패치를 설치하기 위한 포괄적 시스템을 올바른 위치에 배치할 수 있습니다.

6. 네트워크 액세스 제어

도시에서 발생하는 범죄를 생각해 보시기 바랍니다. 자동차에 고유의 무선 태그를 달고 센서를 단 채 주요 도로만 달린다면 치안 유지는 더욱 쉬워질 것입니다. 데이터의 경우도 마찬가지입니다. 모니터링되는 액세스 지점을 통해 등록된 데이터를 전송하는 기업은 악성 코드의 위치를 파악하고 격리하는 것이 훨씬 쉬울 것입니다.

7. 클라우드 보안
클라우드 컴퓨팅은 엄청난 효율성을 약속하지만 리스크를 야기할 수 있습니다. 기업이 특정 IT 서비스를 클라우드 컴퓨팅으로 이전할 경우 다른 서비스와 맞붙어 있어나 신용사기에 노출될 수 있습니다. 이러한 맥락에서 클라우드는 흑사병에 걸린 일정 비율의 고객이 호텔에 있는 경우와 같다고 볼 수 있습니다. 이러한 상황을 해결하기 위해 손님들은 서로를 격리하고 가능한 위협 요소를 모니터링할 수 있는 툴과 절차를 가지고 있어야 합니다.

8. 주변 감시
계약직 직원이 시스템 액세스를 필요로 한다고 가정하겠습니다. 암호를 어떻게 전달하겠습니까? 메모장에 남기시겠습니까? 문자 메시지로 발송하겠습니까? 이러한 임시 방편은 위험을 초래합니다. 기업의 보안 문화는 기업 장벽을 넘어서 계약직 직원과 공급업체와 함께 성공 사례를 구축할 수 있어야 합니다. 이는 이전의 품질 관리 노력을 위한 프로세스와 유사한 것입니다. 또한 우수한 보안은 기업 생태계 전체에 적용되어야 합니다. 한 기업의 감당할 수 없는 부주의가 사회 전체를 망칠 수도 있습니다.

9. 핵심 기업 자산 보호
기업 자산 내 어딘가 존재하는 보물은 아마도 과학적 기술적 데이터이거나 가능성 있는 M&A에 대한 특정 문서, 또는 고객의 비공개 재무 정보가 될 수 있습니다. 각 기업은 인벤토리 관리 단계에서중요한 데이터는 특별히 다루어야 합니다. 각 항목은 우선순위별로 기업의 생사를 걸고 보호, 추적 및 암호화를 거쳐야 합니다. 실제로 기업의 생사가 달린 경우도 있습니다.

10. 사용자 추적
고용주가 정규 직원을 채용한다고 가정하겠습니다. 6개월이 지나고 승진을 하였습니다. 1년 후 경쟁사에서 그 직원을 채용했습니다. 이 시스템은 이후 해당 직원을 어떤 방식으로 다루어야 할까요? 이 직원의 데이터 액세스를 제한해야 하지만 마지막으로 회사를 떠나기 전까지는 사용할 수 있는 길을 열어주어야 합니다. 이것이 ID 라이프사이클 관리로 기업에 필수 요소입니다. 이를 제대로 관리하지 못하는 기업은 어둠에 갇혀 침입자 공격에 취약할 수 밖에 없습니다. 이러한 리스크는 이와 같은 시스템 구축을 통해 직원을 확인하고, 승인 사항을 관리하고 해고가 이루어지는 즉시 취소하여 해결할 수 있습니다.

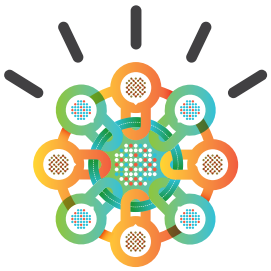
혁신을 자신있게 수용하는 방법은 다음과 같습니다.

리스크 관리와 혁신 활용 사이의 균형

토론 참여
추가 기사를 읽거나, 자세한 사항 확인 또는 다른 보안 리더들과 의견 나누려면 다음 사이트를 방문하시기 바랍니다. ibm.com/smarter/cai/security.

필자 소개
Kristin Lovejoy는 IBM의 IT 담당 부사장 겸 CIO입니다. 연락처는 klovejoy@us.ibm.com입니다.

IBM Center for Applied Insights
IBM Center for Applied Insights는 심층적 내용과 분석 전문 지식을 통합하여 고객을 위한 새로운 가치 창출을 유도하고 있습니다. IBM Center는 기업이 실행으로 옮길 수 있는 실질적 가이드를 통해 연구 수행 및 자산 및 툴을 구축합니다.



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

Produced in the United States of America
2012년 1월

CIE03116-KRKO-00