경영 혁신 시리즈

CIO를 위한 보안 필수 사항

기업 데이터, 개인 디바이스로의 이동 실현

주요 내용:

IBM에서는 개방성 및 리스크 관리 사이의 적절한 균형을 이루고자 지속적인 노력을 기울이고 있습니다. 또한 이러한 균형을 달성할 수 있다는 강한 믿음을 갖고 있습니다. 따라서 "전문가"와 "일반 개인"은 명백히 다르며, 직원이 이러한 차이를 이해하고 그 중요성을 인식할 수 있도록 교육하고 있습니다.

오늘날 CIO들은 그 역할을 감당하기가 그리 만만치 않습니다. 직원들이 자신의 컴퓨팅 디바이스를 업무에 사용하는 경우가 늘어나면서 CIO는 어려운 선택의 문제에 직면하고 있습니다. 결코 쉬운 일은 아니겠지만, 직원들이 자신의 디바이스에서 비즈니스를 수행할 수 있도록 안전한 방법을 찾거나, 아니면 명백하게 이를 금지해야 합니다.

이러한 추세가 개별적인 현상은 아니며, 급증하는 IT 소비에 기인하여 점차 늘고 있습니다. 오늘날 사람들은 구매한 디바이스를 직업을 비롯한 삶 전체에 도구로 애용하고 있습니다. 이러한 추세는 개인과 전문가, 활동과 정보를 "모호하게" 하는 리스크를 유발합니다. 또한 이러한 모호성 리스크는 CIO에게 중요한 문제를 제시합니다. 따라서 리스크를 최소화하면서 개방성을 제공하는 정책과 기술을 선택하고 구현해야 합니다. 여기에는 다음과 같은 어려운 문제들이 포함됩니다. 단일 디바이스에서 개인 데이터를 비즈니스 데이터와 구분하고, 이를 어떻게 보호할 것인가? 디바이스 분실 및 도난과 같은 일반적인 과제들을 어떻게 다룰 것인가? 직원이 퇴사할 경우 직원의 디바이스에 있는 데이터는 아무런 문제가 없는가?

BYOD(Bring Your Own Device)를 착수하기 전에 모든 조직은 이러한 문제를 고심하며 그 해결책을 찾아야 합니다. IBM에서는 개방성 및 리스크 관리 사이의 적절한 균형을 이루기 위해 지속적인 노력을 기울이고 있습니다. 또한 이러한 균형을 달성할 수 있다는 강한 믿음을 갖고 있습니다. "전문가"와 "일반 개인"은 명백히 다르며, 직원이 이러한 차이를 이해하고 그 중요성을 인식하도록 교육하고 있습니다.

이러한 리스크는 협업을 통해 관리할 수도 있습니다. 하지만 이미 알고 있듯이 선택의 폭이 그리 넓지 않습니다. 결국 오늘날 소비자 전자 제품에 거대한 혁신이 일어나게 되었습니다. 새로운 기계들은 전례 없는 방식으로 액세스를 실현합니다. 따라서 이러한 변화 속에서 직원들이 아이디어를 공유하고 연결하며, 새로운 기술을 습득하고, 필요한 정보를 공유하는 것은 당연한 일입니다. 가장 즐겨 사용하는 디바이스에서 비즈니스 활동을 수행할 수 있다면 동료 및 고객과 더 긴밀한 관계를 유지할 수 있을 것입니다. 오늘날과 같은 고도로 연결된 시대에 직원들은 활동적이고 책임 의식이 있는 디지털 시민이 되어야 합니다. 이는 그들이 사용하는 기술과 플랫폼을 통해 혁신이 이루어지기 때문입니다.

한 가지 중요한 단계는 정책 및 기술 관점에서 디지털 ID, 데이터 및 애플리케이션의 "개인용"과 "전문가용" 사이에 명확한 경계를 구축하는 것입니다.

핵심은 리스크를 관리하면서 이러한 혜택을 누리는 것입니다. 또한 적절한 정책 및 기술적 제어의 구현 없이 개인용 디바이스를 허용하면 위험을 초래할 것은 분명합니다. 예를 들어, Gartner에서는 2013년까지 BYOD 정책을 도입한 조직의 80%가 네트워크 내부에서 봇네트 위험이 2배에 달할 것으로 예측하고 있습니다. 모바일 장치가 원격에서 비즈니스를 수행하므로 기존에 영역으로 사용되었던 경계를 넘어 기업 네트워크가 확장됩니다. 따라서 보안이 가장 중요합니다. 여기서 중요한 한 가지 단계는 정책 및 기술 관점에서 디지털 ID, 데이터 및 애플리케이션의 "개인용"과 "전문가용" 사이에 명확한 경계를 구축하는 것입니다. 또한 조직의 각 구성원은 이러한 경계와 엔터프라이즈 보안이 왜 중요한지를 이해해야 합니다.

이를 위해 널리 흩어져 있는 계약 근로자들부터 CEO에 이르기까지 폭넓은 교육을 위한 노력을 강화해야 합니다.

IBM의 경험에 비추어 볼 때 BYOD 프로그램 시작 시 고려해야 할 5가지 단계가 있습니다. BYOD의 목표는 개인 활동과 데이터를 논리적으로 구분하면서 디바이스에서 기업 데이터와 애플리케이션을 완벽히 보호함으로써 BYOD 사용의 타당성을 구축하기 위함입니다. 또한 직원은 리스크를 이해할 뿐만 아니라 솔루션에 참여해야 합니다. 여기에는 디바이스 장치 등록에서 디바이스 분실에 따른 문제 해결 및 신속한 보고에 이르는 모든 것이 포함됩니다.

BYOD 정책을 도입한 조직의

80%가 2013년까지 네트워크

내부에서 봇네트 위험이 2배에 달할 것입니다.

출처: http://www.sans.org/reading_room/analysts_program/ForeScoutmobile-security.pdf

이 모든 것에는 심도 있는 전반적인 인식 즉, 진정한 리스크 인식의 문화가 필요합니다. 이러한 문화는 고위 관리자의 지원이 있을 경우에만 가능합니다. 모바일 세계에서 기업의 중요한 보안을 강화하기 위한 권장사항 몇 가지를 아래와 같이 제시합니다.

개인 소유 디바이스 사용을 허용하기 위한 팁

1. 규칙의 제정 및 적용 확대

조직의 고위 리더와 협업하면서 CISO(최고 정보 보안 책임자)와 함께 CIO는 데이터에 대한 액세스, 소비, 분산 및 비즈니스 용도에 적합한 디바이스 선택 방법에 대한 지침을 주는 일련의 원칙을 개발하고 게시해야 합니다. 리스크의 인식 및 이해와 함께 향후 진행 방향에 대한 동의가 고위 관리자들 사이에서 필요합니다. 새로운 기술이 기업에

도입되면서 이러한 지침의 원칙은 보안 정책과 거버넌스 면에서 각 직원에게 요구되는 사항에 적용될 것입니다.

2. 모든 디바이스 등록

기업은 하드웨어, 소프트웨어 및 관련 ID 등 기업 데이터를 취급하거나, 기업 네트워크에서 비즈니스를 수행하는 모든 디바이스의 완전한 인벤토리를 보유해야 합니다. 여기에는 예외가 있을 수 없습니다. 예외는 불확실성을, 그리고 불확실성은 리스크를 초래하기 때문입니다. 리스크가 있을 경우, 알 수 없거나 등록되지 않은 디바이스를 기업 네트워크에 연결해서는 안됩니다. 또한 직원이 개인 디바이스를 비즈니스용으로 사용하는 유연성을 높이기 위해 디바이스를 사용할 경우 시작 단계에서 디바이스를 등록해야 합니다.

3. 공용 도구

등록 프로세스 중에 각 디바이스마다 관리 기능을 탑재합니다. 이러한 기술은 기술 팀이 구성 및 보안 설정을 관리하도록 하며, 데이터를 효과적으로 분리합니다. 또한 비밀번호 보호 및 자동 잠금을 포함해야 하며, 디바이스 분실 또는 도난 시 원격 삭제(remote-wipe)가 가능해야 합니다. 물론 바이러스 방지도 중요한 보안 제어 기능에 포함됩니다. 암호화 사용을 고려할 수도 있습니다. 1년간 약 330개 조직에서 86,000개의 랩탑 컴퓨터 분실이 발생하는 것으로 추정되고 있습니다.[1] 분실 또는 도난 당한 랩탑 하드 디스크가 암호화되어 있으면 도난 및 무단 액세스로부터 모든 데이터를 보호할 수 있습니다.

4. Wi-Fi 감시

Wi-Fi 네트워크는 모든 곳에 있지만, 모든 공공 Wi-Fi를 신뢰할 수 있는 것은 아닙니다. 따라서 Wi-Fi 네트워크 사용 시 주의하며, 보안되지 않은 네트워크에서 민감한 데이터를 전송하지 않도록 직원을 교육해야 합니다. 또한 Bluetooth의 자동 발견과 VPN 소프트웨어의 스캐닝 및 구현을 비활성화시켜 암호화된 채널을 통해 기업 데이터와 자원에 연결하도록 독려해야 합니다.

5. 분실 보고

직원은 개인용 휴대 전화 또는 태블릿에서 업무를 수행할 때 이를 가족 구성원에게 주거나 분실할 경우, 비즈니스에 영향을 줄 수 있음을 반드시 이해해야 합니다. 그리고 기업 비즈니스를 정확하고 최신 상태로 유지하는 데 사용되는 시스템의 기업 인벤토리를 보유하는 것이 중요합니다.

[1] "수십 달러의 랩탑 부실 문제: 미국 조직의 벤치마크 연구", Ponemon Institute, 2010년 9월 30일(http://newsroom. intel.com/servlet/JiveServlet/download/1544-8-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf)

더 나아가 대규모 정책의 일환으로 기업은 개인 소유 디바이스에 대한 특정 사고 대응 정책을 마련해야 합니다. 개인 소유 디바이스에 기업 데이터가 있으므로 기업 소유 기기와 마찬가지로 주의 깊게 관리해야 합니다.

CIO를 위한 보안 필수 사항

혁신과 리스크 제어 사이의 균형을 이루기 위한 IBM의 접근 방식에는 수행해야 할 일련의 필수 과정이 있습니다. 이러한 과정을 수행하면 고도로 연결된 시대에서 보안 인텔리전스를 획득할 수 있습니다.

BYOD 및 이동성을 어떻게 사용할 것인가?

편의성과 책임 사이의 균형

대화 참여

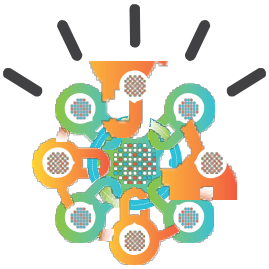
추가 기사 또는 CIO를 위한 보안 필수 사항에 대한 자세한 내용을 알고 싶거나 보안 전문가와 의견을 공유하길 원하시면 **www.ibm.com/smarter/cai/security**에 가입하십시오.

저자 정보

Kristin Lovejoy는 IBM CIO Office의 IT Risk 부문 VP입니다. 문의는 **klovejoy@us.ibm.com**으로 메일을 보낼 수 있습니다.

IBM Center for Applied Insights 정보

IBM Center for Applied Insights는 고객을 위한 새로운 가치의 과정을 논의하기 위해 심도 있는 컨텐츠와 분석 전문 지식을 통합합니다. 또한 조직의 활동을 추진하기 위한 실용적인 지침과 함께 자산과 도구를 구축하고 연구를 수행합니다.



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

Produced in the United States of America
February 2012

WGW03003-USEN-00