Executive Series

CIO를 위한 '보안의 핵심'

확장된 엔터프라이즈의 보안

요점:

데이터 관계의 종류가 다양해지고 그 양이 폭증함에 따라 보안에 대한 우려가 높아지고 있습니다. 위치에 상관 없이 데이터를 제어할 수 있는 정책을 수립하고 베스트 프랙티스를 구현하는 것이 관건입니다. 기업은 벤더, 제공업체, 협력업체, 인수업체 및 파트너의 정보 생태계 전체에서 보안을 유지하기 위해 적극적인 조치를 취해야 합니다.

귀사의 보안이 훌륭하게 운영되고 있다고 가정해 보겠습니다. 소프트웨어 패치를 최신 상태로 유지할 수 있는 절차를 보유하고 있고, 수 분 내에 사고에 대응할 수 있는 팀도 있습니다. 철저한 보안 의식도 전사적으로 조성되어 있습니다. 즉, 사내에서는 모든 것이 원활하게 진행되고 있습니다. 하지만 조직 외부는 어떻습니까? 혹시 급여나 직원 연금 제도를 협력업체에게 맡기고 있습니까? 이 경우 데이터가 안전하다고 확신할 수 있습니까?

전통적인 공급망에 존재하는 위험은 더 이상 간과할 수 없는 문제가 되었습니다. 아시아 지역의 홍수나 브라질의 파업으로 인해 주요 요소가 손상되면 멀리 떨어져 있는 제조업체가 마비될 수 있습니다. 기업의 광범위한 데이터 관계 또한 보안 우려의 원인이 되고 있으며, 이는 급속도로 확장되고 있습니다. 기업들이 제조, 배포 또는 마케팅을 조정함에 따라 조직 간에 데이터가 공유되며, 이 과정에서 도용, 스파이 및 기타 악의적 행위가 끼어들 수 있습니다. 실제로, 공급망을 운영하는 기업이든 서비스 공급업체를 고용하는 기업이든, 기업의 방화벽 외부에서 잠재적인 취약성이 급속하게 증가하고 있습니다.

기업은 부족한 기술력이나 불공정한 노동 행위에 대해 제공업체, 협력업체 및 벤더를 관리하는 등, 정보 생태계 전체의 보안을 유지하기 위해 적극적인 조치를 취해야 합니다. 올해 초, 세간을 떠들썩하게 했던 카드 거래 회사의 보안 침해 사건은 신용 카드 회사들에게 보안에 대한 경각심을 일깨워 주었습니다.[1] 이러한 보안 문제는 쉽사리 해결되지 않을 것으로 보입니다. PwC에서 실시한 2012 Global State of Information Security Survey에 따르면 파트너와 제공업체에 의해 보안 침해가 발생하고 있다고 답한 응답자의 수가 예전보다 늘어났습니다(2009년과 2011년 사이에 8%에서 15%로 증가). 즉, 보안 관련 문제가 증가하고 있는 것입니다.[2]

정보 생태계의 위험은 단순하게 정의할 수 없습니다. 전세계에서 수많은 사람들이 하루나 이틀 또는 수 년 동안 다양한 레벨의 데이터를 이용하고 있습니다. 직원의 주민등록번호나 의료 기록과 같이 민감한 기밀 정보에 액세스하는 사용자가 있는가 하면, 기본적인 백 오피스 서비스만 이용하는 사용자도 있습니다. 여기에서 공통되는 과제는 위치에 상관 없이 데이터를 제어할 수 있는 일련의 정책과 베스트 프랙티스를 구현하는 것입니다.

IBM은 이러한 과제를 지속적으로 관리하고 있으며 확장된 엔터프라이즈의 보안을 강화하기 위한 몇 가지 팁을 가지고 있습니다.

1. 처음부터 모든 관계에 보안을 구축합니다. 확실한 제어를 구현하는 유일한 방법은 모든 관계에서 처음부터 보안 정책을 설계하는 것입니다. 즉, 데이터 교환이 이루어지는 관계에서 모든 엔티티에 대해 명확한 보안 기준과 절차를 설정해야 합니다. 조직은 파트너, 협력업체, 제공업체 및 벤더와 협력하여 데이터 처리와 정보 보호 현황을 파악해야 합니다.

2. 클라우드를 감시합니다. 데이터 관리를 클라우드 컴퓨팅 센터로 외주 처리하는 기업이 늘어나고 있습니다. 이 현상은 특히 SaaS(Software as a Service)를 제공하는 기업 사이에 널리 퍼져 있습니다. 따라서, 이제 파트너의 제공업체의 보안에도 관심을 기울여야 합니다. 이들이 비즈니스를 안전하게 운영하고 있으며 집과 데이터 센터에서 데이터와 관련된 법률을 준수하고 있음을 확신할 수 있어야 합니다. 또한, 귀사의 명시적 동의 없이는 다른 클라우드 공급업체로 이동하지 못하도록 해야 합니다.

3. 사소한 부분에도 주의를 기울입니다. 일반적으로, 민감한 데이터를 페타바이트 단위로 처리하는 은행이나 보험 회사와 같은 대형 파트너에게 관심이 집중되기 마련입니다. 이러한 회사들은 철저한 감사의 대상이 되며, 대부분은 수년간 까다로운 산업 규제를 준수해야 합니다. 하지만 포털 애플리케이션 또는 마케팅 캠페인 계약을 체결한 작은 신생 기업에서도 위험은 발생합니다. 이러한 소기업들은 한 가지 아이디어나 서비스만을 제공하기 위한 목적으로 설립되기 때문에 보안에 투입할 자원이 충분하지 않습니다. 또한, 클라우드에서 애플리케이션을 실행하는 경우가 많아 문제가 발생할 소지도 많습니다. 활용할 수 있는 자원이 한정되어 있다 하더라도, 이러한 소기업들 역시 기본적인 보안 요구 사항을 따라야 합니다.

보안의 범위 확장

1. 처음부터 모든 관계에 보안을 **구축**합니다.
2. 사전 조사부터 통합에 이르기까지 M&A의 모든 과정에 적용할 수 있는 확실한 절차를 **개발**합니다.
3. 규모에 상관 없이, 파트너의 제공업체에 대해 시야를 **넓힙니다**.
4. 불변하는 것은 없음을 **염두에** 둡니다.

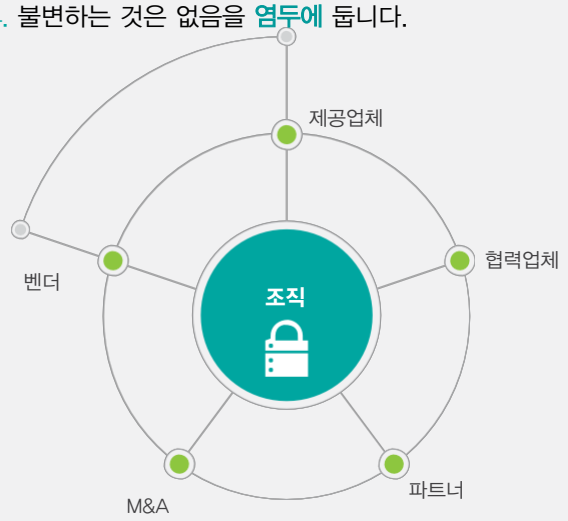

그림 1

4. M&A를 위한 확실한 절차를 개발합니다. 인수합병이 진행되는 동안에는 취약성이 더 높아집니다. 기업의 인수 뉴스가 발표되면 곧바로 트위터를 통해 소식이 전파되며, 인수 대상 회사는 해커와 도난범들의 염탐과 공격의 대상이 될 수 있습니다. 이러한 공격자들에게는 M&A가 매우 좋은 기회입니다. 이들은 새 목표물의 방어벽을 뚫고 들어가 인수 회사에 자신을 암시하는 표시나 맬웨어를 남겨두려 합니다.

M&A 진행 중의 보안 절차는 3단계로 이루어집니다. 첫 번째 단계는 사전 조사입니다. 이전의 보안 침해 및 공격의 잔재가 인수 대상 회사에 남아 있습니까? 만일 그렇다면 인수의 실현 가능성에 대해 다시 생각해 보아야 하며, 최소한 취약성을 해결할 수 있도록 포괄적인 노력을 기울여야 합니다. 두 번째 단계는 발표 후 발생할 수 있는 공격에 대비한 방어벽을 쌓는 것입니다. 기업은 법이 허용하는 한도

내에서 인수업체와 긴밀하게 협조하여 방어를 강화해야 합니다. 세 번째 단계는 6개월 또는 1년 후 인수 대상 회사의 네트워크가 통합되었을 때 모든 부분이 인수 회사의 보안 수준과 같아질 수 있도록 소프트웨어, 교육 및 베스트 프랙티스를 활용하여 보안을 강화하는 것입니다.

파트너와 제공업체에 의해 보안 침해가 발생하고 있다고 답한 응답자의 수가 2009년과 2011년 사이에

8%에서 15%로

증가하였습니다.[2]

출처: PwC

5. 불변하는 것은 없음을 염두에 둡니다. 보안의 변경은 비즈니스에 매우 큰 영향을 미칩니다. 한 제공업체의 보안 위반으로 인해 공급망 전체의 수정과 조정이 불가피해질 수 있습니다. 전세계에서 제정되는 새로운 데이터 법률로 인해 새로운 준수 요구 사항이 발생되고 있습니다. 이를 자세히 살펴보지 않으면, 한 국가에서 오늘은 여러분의 데이터가 법률을 준수하고 있다고 해도 당장 내일 보안을 위반하게 될 수도 있습니다.

오늘날 비즈니스의 기반이 되고 있는 데이터 스트림이 증가하고 있는 것처럼, 보안 문제도 지속적으로 증가할 것입니다. 이러한 상황에 대처하려면 모든 조직에서 일류의 보안 팀을 가동하여 확장된 엔터프라이즈 전체를 모니터링해야 합니다. 이렇게 되면 작업 부하가 높아지고 업무가 많아질 것입니다. 하지만 오늘날처럼 고도로 연결된 세상에서 비즈니스를 수행하려면 데이터가 어디에 있든 효과적으로 제어할 수 있어야 합니다.

IBM과의 대화에 참여하기

다른 기사를 읽고 싶거나, CIO를 위한 보안의 핵심에 대해 더 자세히 알고 싶거나, 자신의 생각을 다른 보안 리더들과 공유하고 싶다면 ibm.com/smarter/cai/security에 참여하십시오.

필자 소개

Kristin Lovejoy는 IBM의 Office of the CIO에 속한 IT 위험 부문의 부사장입니다. 연락처는 klovejoy@us.ibm.com입니다.

IBM Center for Applied Insights 소개

IBM Center for Applied Insights(ibm.com/smarter/cai/value)에서는 새로운 사고 및 업무 방식과 조직을 이끄는 혁신적인 방법을 소개합니다. 이 센터에서는 증거에 기반한 연구 조사를 통해 기업 리더들에게 실용적인 지침과 혁신 사례를 제공합니다.

[1] "Global Payments Data Breach Exposes Card Payments Vulnerability", Forbes, 2012년 4월 3일, http://www.forbes.com/sites/greatspeculations/2012/04/03/global- payments-data-breach-exposes-card-payments-vulnerability/

2 "Eye of the storm-Key findings from the 2012 Global State of Information Security Survey", PwC, http://www.pwc.com/jg/en/media-article/2012-global-state-of- information-security-survey.jhtml

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

Produced in the United States of America
September 2012

WGW03015USEN-00