情 報 保 護 學 會 誌
第23卷 第5號, 2013. 10

정보보호관리 패러다임 변화에 따른 주요 이슈와 미래 전략

김 정 덕*

요 약

모바일, 클라우드, BYOD 등 새로운 IT 환경으로의 변화로 인해 기존의 정보보호 접근방법의 효과성에 대해 의문이 대두되고 있다. 침입차단시스템, 안티 바이러스 등 알려진 침입패턴에 근거한 기술적 대책 중심의 접근방법으로는 복잡하고 지능화되어가는 최근의 공격에 효과적으로 대응하기에는 태생적 한계를 가지고 있다. 또한 가중되는 보안대책으로 인해 창의적인 업무 수행을 방해하고 사용자의 자율성을 감소시키는 부작용도 초래하고 있다. 따라서 새로운 환경변화에 효과적으로 대처하고 지속가능한 정보보호관리 프로그램을 수립하기 위해서는 새로운 패러다임의 도입이 필요하다고 할 수 있다. 본 고에서는 가트너에서 제시한 일련의 혁신적인 정보보호 접근방법을 소개함으로써 새로운 패러다임을 제시하고 이에 기반한 새로운 정보보호관리 프로그램 구성요소와 이의 구현을 위한 로드맵을 제시한다.

Ⅰ. 서 론

모바일, 클라우드, 소셜, 개인화 등 새로운 형태의 컴퓨팅 환경이 등장함에 따라 기존의 정보보호 접근방법으로는 한계를 나타내고 있으며 새로운 패러다임이 요구되고 있다. 이러한 컴퓨팅 환경의 변화로 인해 정보보호와 비즈니스와의 통합에 대한 요구사항이 더욱 강조되고 있으며 비즈니스를 효과적으로 지원하기 위한 정보보호관리 프로그램 구축이 필요하다[2].

국내의 정보보호관리 프로그램은 일반적으로 언급되는 5단계의 성숙도 단계에서 두 번째 단계에 해당되는 관리프로그램 개발단계에 해당된다고 할 수 있다[1]. 즉 정보보호관리 프로그램 계획 및 개발이 공식적으로 존재하지 않으며, 보안관리자 개인의 역량에 의존하여 프로그램이 개발되고 있는 상태이다. 또한 정보보안 이슈에 대한 비공식적 의사소통이 진행되고 있는 상태이다[2].

한 단계 성숙된 단계로 이전하기 위해서는 무엇보다도 비즈니스와 정보보호 활동간의 연계 및 통합이 요구되고 정보보호 거버넌스 상의 문제점을 개선해야 하며, 기존의 문제점에 대한 정확한 인식하에 새로운 시도가 필요하다고 할 수 있다.

본 논문에서는 현재 정보보호관리 패러다임의 한계점을 분석하고 향후 나아가야 할 미래상을 제시하면서 이를 위한 제반 정보보호관리 프로그램 개선 방향을 위한 로드맵을 제시하고자 한다.

Ⅱ. 정보보호관리 패러다임의 문제점

2.1 정보보호 환경의 변화

새롭게 변화하는 IT 환경은 모바일, 클라우드, 소셜, 개인화 등으로 대변할 수 있으며, 이는 IT와 비즈니스 그리고 개인 간의 관계를 변화시키고 있다. 이에 따라 공식적인 정책과 통제기반의 기존 정보보호 접근방법은 점차 그 효력을 상실하고 있다[4].

법과 규정은 점차 강화되고 있으며 이의 준수를 위한 보안대책은 제한적이고 강제적인 성격을 가질 수 밖에 없다.

기존의 정보보호관리 접근방법은 정보자산 보호의 효과성(effectiveness)을 높이기 위해서 많은 노력을 경주했다고 할 수 있다. 그러나 미래에는 정보보호의 효율성 및 생산성을 높이기 위한 노력으로 방향 전환이 될 것으로 예상된다[4].

* 중앙대학교 정보시스템학과 교수(jdkimsac@cau.ac.kr)

현재의 컴퓨팅 및 비즈니스 환경변화를 기반으로 미래의 정보보호 환경을 예측하는 것은 매우 어려운 일이면서 중요한 일이다. 현재 발생하고 있는 환경변화를 요약하면 다음과 같은 세 가지 주요 메가트랜드로 구분할 수 있을 것이다. 첫째, APT 등 기존의 전통적인 보안접근방법으로는 해결하기 어려운 위협들이 지속적으로 나타나고 있으며, 이로 인한 보안사고는 향후 계속해서 나타날 것이다. 둘째, 대부분의 경우, 새로운 공격은 금전적 목적으로 시스템 또는 개인을 대상으로 기밀정보를 유출하고자 할 것이다. 중요 시스템 중단이나 비즈니스 업무중단을 통해 재무적 손실을 목표로 하고 있다. 셋째, 클라우드 서비스, BYOD 등의 최근 추세로 인해 IT 부서는 사용자 디바이스나 서비스를 직접 소유/제공하지 않게 되고 이로 인해 통제능력이 상당부분 감소될 것이다[5].

이러한 메가트랜드는 다음과 같은 두 가지 기존 정보보호 전략의 한계를 보여주고 있으며 새로운 패러다임으로의 변화를 요구하고 있다.

2.2 예방적 대책 위주의 정보보호 한계

지난 수십 년 간 정보보호에 대한 많은 노력에도 불구하고 정보보호 사고는 계속해서 발생하고 있으며 미래에도 이러한 증가 추세는 멈추지 않을 것으로 예상된다. 이 현상은 현재의 예방적 보안 접근방법으로는 다양하고 지능화되는 APT공격을 예방하기에는 한계가 있다는 점을 대변하고 있다. 즉 침입차단시스템, IPS, 악성코드 백신 시스템 등에 대한 투자 및 노력은 미래에도 필요하기는 하나, 모든 공격을 예방하기는 어렵다. 따라서 앞으로는 정보보호에 대한 투자는 신속 대응 및 대응역량을 높이는 데 사용되어야 할 필요가 있다.

침입패턴에 기반한 공격탐지기법으로는 새로운 침입을 탐지하기 어려우며, 따라서 악의성 의도를 의미할 수 있는 비 정상 행위를 식별할 수 있는 광범위한 모니터링이 필요하다. 즉, 정밀하고, 전반적이며, 상황인식에 기반한 위협 모니터링 구축이라는 방향으로 정보보호 노력이 집중될 필요가 있다[8].

2.3 기술적 대책 위주의 정보보호의 한계

앞으로는 기술적 대책 중심의 보안 접근방법으로는 새로운 환경변화에 적절히 대응하기 어렵다. 즉, 기술적 보안대책으로 인한 비즈니스 또는 IT 생산성과 유연성에 부정적인 영향을 최소화하기 위해서도 더 이상의 기술적 보안대책을 추가 실행하기도 어렵다. 또한 인가된 사용자/관리자에 의한 의도적인 손실 또는 비의도적인 피해로부터 정보를 보호하기 위해서는 기술적 대책만으로는 한계가 있다.

특히 SNS 등으로 인한 데이터의 폭발적 증가와 함께 클라우드와 같이 IT 서비스 전달 방식이 다양해지고 복잡해짐에 따라 전통적 기술 중심의 대책으로는 더 이상 효과를 내기 어려운 상황이다.

III. 미래 정보보호관리의 주요 이슈

3.1 지속적 모니터링

예방적 대책의 한계를 극복하기 위해서는 지속적이고 포괄적인 모니터링이 필요하다. 그러나 구체적으로 무엇을 모니터할 것인가라는 질문에 답하기 위해서는 예상 시나리오에 따라 달라질 수 밖에 없다. 침입공격이 기업이나 조직을 대상으로 할 경우에는 모니터링은 응용, DB, 파일 시스템, 콘텐츠 관리 시스템 등 전사적 시스템에 대한 접근을 모니터링 해야 할 것이다. 사용자의 접근 패턴을 기반으로 비정상적 행위, 즉 접근빈도, 다운로드 정보의 규모, 접근대상 정보의 유형, 접근요청 기기나 접근시점 등과 같은 접근 상황정보 등을 기반으로 침입을 식별해 낼 수 있어야 한다. 특히 클라우드를 통해 정보와 IT서비스를 사용할 경우, 클라우드 접근에 대한 비정상행위 탐지를 수행하는 서비스가 추가로 요구된다고 할 수 있다.

개인에 대한 공격 시나리오에서 효과적인 모니터링 및 탐지를 위해서는 개인의 ID와 역할에 따라 단말기에서의 활동을 모니터링 할 수 있는 기능을 제공해야 할 것이다. 이미 관련 모니터링 및 포렌식 도구들이 존재하며, 향후 단말기 보안 플랫폼을 제공하는 업체에서 이러한 모니터링 기능을 제공할 것으로 예상된다.

효과적이며 지속적인 모니터링을 위해서는 모니터링 정보 분석의 정확성을 높이기 위해서는 상황정보를 추가적으로 사용할 필요가 있으며, 모니터링 정보를 저장할 수 있는 대용량의 저장장치를 준비할 필요가 있다.

2013년 7월, 미국 DHS 주도하에 미 정부기관에서의

지속적 모니터링을 위한 노력으로 향후 5년간 60억불을 투자하여 지속적 진단 및 대응 프로그램(Continuous Diagnostic and Mitigation Program) 구축 사업을 개시함으로써, 사이버 보안위험을 실시간으로 식별 및 평가하고 그 결과를 실시간으로 자동 업데이트해서 대시보드 형태로 보여줄 수 있는 시스템을 정부기관에 구축하기로 하였다[6]. 구체적으로는 하드웨어 자산관리, 소프트웨어 자산관리, 구성관리, 취약점 관리 등 네 가지 시스템을 구축함으로써 연방, 주, 지방정부기관의 IT 취약점에 대한 모니터링 및 대응조치를 하고자 한다. 또한 미국 공공기관에 클라우드 서비스 보안 인증체계인 FedRAMP에서는 잠정 인증을 받은 서비스 제공업체에게 그들의 클라우드 서비스에 대한 지속적 모니터링을 지시하고 이를 평가할 계획으로 있다[7].

효과적인 보안사고 대응과 피해의 확산과 재발 방지를 위해서는 보안사고와 관련된 정보분석과 더불어 정보공유가 병행되어야 할 것이다. 최근 위협/취약점에 대한 분석 및 공유 서비스 등 security intelligence 서비스가 최근 주목을 받고 있다. 이와 병행해서 공격자 정보에 대한 분석 및 공유 서비스도 제공될 필요가 있다.

3.2 인간 중심의 정보보호

인간 중심의 정보보호 전략은 개인의 권한과 이와 관련된 책임을 강조하며 신뢰를 기반으로 하는 한편, 제한적이고 예방적 성격의 보안대책을 가급적 최소화하고자 하는 접근방법이다. 즉 기존의 정보보호 방식이 기술적 대책과 보안정책을 기반으로 개인 사용자에 대한 신뢰 영역을 축소시켰다면, 인간 중심 보안전략은 자발성, 소통, 탐구 등을 통한 개인 사용자의 신뢰 영역을 가능한 한 확장하고자 하는 방식이다[3].

인간 중심 보안을 위한 주요 전제조건은 개인 사용자들이 기술 및 응용시스템의 사용에 관해 적절한 위험기반 의사결정을 할 수 있는 능력과 환경이 보장되어야 한다는 점이다. 따라서 이 접근방법을 구현하기 위해서는 아래와 같은 세 가지 요소를 고려해야 할 것이다[2].

첫째, 개인 사용자의 권한과 책임이 명확하게 정의되어야 하고 이는 인센티브와 제재조치와 연계되어야 한다. 가능하면 이러한 권한과 책임은 문서화되어야 하며 모든 구성원의 동의하에 규약 또는 협정으로 공식화되어야 한다.

둘째, 개인 사용자의 책임과 자발성을 유도할 수 있는 교육 프로그램이 필요하고 이것이 조직문화 형성까지 연결될 수 있도록 해야 한다. 사용자의 책임성에 관해 단순히 인식 수준에만 머무는 것이 아니라, 행동으로 나타나게 할 수 있도록 교육 프로그램이 설계되어야 한다. 이러한 면에서 전통적인 인식제고 및 훈련 프로그램과는 구별된다.

셋째, 위험기반의 모니터링 대책들이 구현되어 사용자의 예외적 행동을 모니터하고 교정활동을 수행할 수 있도록 해야 한다. 따라서 보안탐지 기능(DLP, SIEM, DAM 등)을 통해 보다 투명성을 보장해야 한다. 모니터링과 이에 따른 분석(security intelligence) 역량은 인간 중심 보안구현을 위한 기본 조건이라고 할 수 있다.

이 접근방법의 성공요인은 사용자들의 권한-책임 서약에 대한 위반사항을 다루는 방법과 속도에 있다고 할 수 있다. 위반사항에 대해서는 우선적으로 즉각적인 반응과 더불어 교정활동을 위한 피드백을 제공해주어야 한다. 만일 교정활동이 효과적이 못하다면, 위반자의 권한을 제한하는 등 추가적인 제재행위가 고려되어야 한다.

모니터링에 대한 잠재적인 부정적인 영향을 최소화시키기 위해서는 긍정적 행위를 장려하고 인정하는 추가적인 인센티브를 제공할 필요도 있다.

IV. 미래 전략과 고려사항

본 고에서는 기존의 전통적인 정보보호 접근방법에 대한 한계를 지적하고 새로운 패러다임과 관련 이슈를 제시하였다. 기존의 알려진 침입패턴에 근거해 침입을 탐지하거나 차단하는 기술적 대책으로는 복잡하고 지능화되는 APT 공격에 대처하기에는 제한이 있다. 이러한 예방적 성격의 기술적 대책은 보안사고가 증가함에 따라 계속적으로 추가되고 있으며 이의 구축과 운영에 따른 비용부담뿐만 아니라 업무/IT 생산성 및 유연성에도 제한을 가하고 있다.

따라서 새로운 정보보호 접근방법으로 지속적이고 광범위한인 모니터링 체계 구축과 보안정보 분석과 공유에 기초한 스마트한 보안, 개인 사용자의 권한과 책임을 강조하여 자발적인 노력을 유도하는 인간 중심의 보안접근방법을 제시하였다. 특히 인간 중심의 보안접근방법은 새로운 패러다임으로서 지속적 모니터링과 보안

정보 분석 및 공유에 기반을 두어야 하고, 긍정적 보안 문화 형성을 위한 변화관리 계획 수립이 매우 중요하다고 할 수 있다[3].

따라서 미래 전략으로는 우선적으로 지속적이고 광범위한 모니터링 체계를 구축하고, 모니터링 결과의 분석 및 공유체계를 통해 보다 위험에 근거한 의사결정을 내릴 수 있도록 해야 할 것이다. 이후 점차적으로 조직의 보안문화의 변화를 도모하면서 인간 중심의 보안 접근방법을 실행하는 등 단계적 접근을 고려하여야 할 것이다.

참고문헌

[1] KISA, 정보보호관리 등급기준 및 ISMS 인증기준 개발, 2011. 11.

[2] Gartner, Prevention is Futile in 2020: Protect Information via Pervasive Monitoring and Collective Intelligence, 2013. 5.

[3] Gartner, People-Centric Security Challenges Require Careful Planning, 2013. 3.

[4] Gartner, Maverick Research: Kill Off Security Controls to Reduce Risk, 2012.9.

[5] Gartner, ITScore for Information Security, 2010. 9.

[6] Department of Homeland Security, Continous Diagnostics and Mitigation, www.dhs,gov/CSM

[7] FedRAMP Office, FedRAMP Continuous Monitoring Strategy & Guide, v.1.1, 2012. 7.

[8] NIST SP 800-137, Information Security Continuous Monitoring for FIS and Organizations, 2011.9.

〈著者紹介〉

김 정 덕 (Jungduk Kim)
종신회원

1979년: 연세대학교 정치외교학과, 학사
1981년: 연세대학교 경제학대학원, 석사
1986년: Univ. of S. Carolina, MBA
1990년: Texas A&M University, Ph. D. in MIS
1991~1993년: 한국전산원, 선임연구원
1995년~현재: 중앙대학교, 교수
<관심분야> 정보보호관리 및 거버넌스, 시스템감사, 정보시스템의 전략적 응용