기업 정보보안 기능 강화를 위한 정보보호관리체계에 관한 연구

박청수, 이동범, 곽진
순천향대학교 정보보호학과
e-mail: hobbang123@sch.ac.kr, dblee@sch.ac.kr, jkwak@sch.ac.kr

A Study on Information Security Management System for Security Enhancement of Enterprise

ChungSoo Park, Dongbum Lee, Jin Kwak
Department of Information Security Engineering, Soonchunhyang University

요 약

악성코드에 감염된 여러 대의 좀비 PC가 특정 사이트를 공격하는 해킹 방식인 DDoS 공격은 최근 7.7 DDoS 대란을 비롯하여, 1년도 채 되지 않아 3.3 DDoS 대란으로 이어지고 있다. DDoS 대란의 발생을 통해 사이버 보안 위협의 위험성이 점차 증가하고 있음을 확인할 수 있으며, 공격 경로를 통해 사용자 PC로 유입된 악성코드는 사용자의 자산인 PC에 저장되어 있는 정보들을 모두 삭제할 수 있어 공격으로 인해 발생하는 금전적, 정신적 피해가 점차 심각해지고 있다. 이러한 환경에서 조직 및 사용자가 보존해야 할 정보 자산의 기밀성, 무결성, 가용성을 실현하기 위하여 정보보호관리체계를 기반으로 지속적인 점검을 수행하여 조직 내의 위기관리 프로세스가 구축되어야 한다. 따라서 본 논문에서는 기업이 보유하고 있는 정보 자산이 외부로 유출되는 것을 방지하고, 악의적인 악성코드가 내부로 유입되어 조직 내부의 자산을 파괴하는 위협으로부터 보안을 제공하기 위한 정보보호관리체계에 대해서 분석하고, 기업 정보보안 기능을 강화할 수 있는 방안에 대하여 제안하고자 한다.

1. 서론

작년 7월 7.7 DDoS 대란 및 올해 3.3 DDoS 대란이 발생함에 따라 사용자가 인지하지 못한 상황에서 악성코드가 사용자의 PC에 유입되어 하드 디스크에 저장된 정보를 파괴하고 디스크에 저장된 정보를 유출하여 사회적으로 큰 이슈가 되고 있다. 사용자뿐만 아니라 기업에서도 조직원의 PC에 저장된 중요한 정보 자산들이 유출되고 조직원의 개인 정보가 거래되며, 기업 내부망으로 악성코드가 유입되어 중요 정보를 파괴하거나 유출하는 사례가 급증하고 있다. 이러한 이유로 기업들은 정보보호 보안을 강화하고 있으며, 정보유출을 통제하고 외부로부터 악성코드가 유입되지 못하도록 각종 보안시스템을 도입하고 보안 강화 프로세스를 구축하고 있다[4].

기업이 도입하고 있는 정보보호관리 프로세스 중 가장 핵심이 되는 제도가 ISMS(Information Security Management System)이다. ISMS는 조직이 보존해야 할 정보 자산의 기밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하여 지속적으로 관리하고 운영하는 체계이기 때문에 최근 기업의 정보보호 관리에 대한 표준적 모델 및 기준을 제시하여 기업의 정보보호관리체계 구축 및 운영을 촉진하고 정보보호활동에 대한 프로세스 개선을 통하여 기업의 주요 정보 자산 유출 및 피해를 사전에 예방하고 대처할 수 있도록 하고 있다. 따라서 기업에서는 ISMS 제도에 따라 컨설팅을 받아 정보보호관리 체계를 구축하고 조직원들이 준수할 수 있도록 프로세스를 정의하고 있다. 기업뿐만 아니라 전자 정부에 대한 보안이 요구됨에 따라 G-ISMS(Government-Information Security Management System)를 정부 행정기관에 도입하여 종합적인 정보보호 관리체계를 구축하고 정부 조직 및 유관 기관의 정보 자산을 체계적으로 보호하는 프로세스를 정의하고 있다.

제도 및 프로세스를 정의하는 것도 중요하지만 정보 자산을 보호하는 가장 기본적인 방안은 정보보호제품을 도입하여 내부망을 외부 악성코드로부터 보호하고 조직원 PC에 악성코드가 유입될 경우 이를 탐지하고 삭제할 수 있어야 한다. 특히 최근 이슈가 되고 있는 논리적 망분리 제품은 내부망과 외부망을 완벽히 분리하여 내부망으로 구분된 PC에서는 인터넷을 사용할 수 없도록 하고 있다.

따라서 본 논문에서는 정보보호관리 체계 및 정보보호 제품을 도입하여 기업 정보보안 기능을 강화하는 방안에 대하여 제안하고자 한다.

2. 정보보호관리체계

기업은 조직이 가지고 있는 정보 자산을 보호하기 위하여, 정보보호관리체계 수립·운영을 위한 5단계 관리과정(정보보호정책수립, 정보보호관리체계 범위설정, 위험관리,

구현, 사후관리), 문서화, 정보보호대책에 대하여 조직의 특성 및 환경에 부합되도록 적절하게 수립·구현하여, 체계적으로 관리·유지하고 이행하는지를 평가하는 제도를 도입하고 있다[5]. 체계적인 관리가 되고 있는 기업은 인증을 부여받을 수 있으며, 관리가 되지 않는 기업은 컨설팅을 통해 관리 체계를 구축해야 한다.

2.1 정보보호관리체계 인증

정보보호관리체계(ISMS) 인증 제도는 2001년 (구)정보통신부가 '정보통신망이용촉진및정보보호등에관한법률'을 개정하여 공표함으로써 제47조에 근거를 두고 추진하였다. 즉 정보보호관리체계(ISMS)란 조직이 보존해야 할 정보자산의 기밀성·무결성·가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하여 지속적으로 관리하고 운영하는 체계를 말한다[6]. 이러한 인증 제도를 통하여 단편적이고 일회적이었던 조직의 정보보호활동을 체계적이고 지속적인 관리가 가능하게 함으로써 전사적으로 균형 잡힌 정보보호활동을 할 수 있게 된다. 특히 기업의 정보보호관리에 대한 표준적 모델 및 기준을 제시하여 기업의 정보보호관리체계 구축·운영을 촉진하고 정보보호 활동에 대한 프로세스 개선을 통하여 기업의 주요 정보자산 유출 및 피해를 사전에 예방하고 대처할 수 있도록 하는 데 목적을 두고 있다[3].

정보보호관리체계를 구축하기 위해서는 정보보호관리체계 범위를 결정하고 해당 범위 내의 정보 자산을 식별 및 분류하여 목록을 작성해야 한다. 목록 작성은 기존의 자산관리체계를 활용하는 것이 효율적이며, 크게 유형 자산과 무형 자산으로 분류될 수 있다. 자산을 식별했을 경우 자산의 유출, 위·변조, 사용·미사용에 따라 업무에 미치는 영향도를 고려하여 기밀성, 무결성, 가용성을 기반으로 자산 가치를 평가한다.

자산 정보가 유출 또는 외부에 공개되었을 경우 미치는 업무 영향도가 클 경우 기밀성 측면의 가치가 높이 평가되며, 자산 정보가 위·변조 되었을 경우 미치는 업무 영향도가 클 경우 무결성 측면의 가치가 높이 평가되며, 정보자산의 사용·미사용으로 미치는 업무 영향도가 클 경우 가용성 측면의 가치가 높아진다.

<표 1> ISMS 인증 절차

인증 절차	내용
준비 단계	정보보호관리체계 구축, 인증신청, 사전심사, 계약, 수수료 납부 등 인증을 준비하는 단계
심사 단계	심사팀을 구성하여 서면심사 및 기술 심사를 수행하고, 그 심사결과로 발견된 결함사항을 신청기관이 보완조치(보완조치기간 : 1개월)하여 확인하는 단계
인증 단계	심사팀의 인증심사결과를 인증위원회가 심의·의결하여 인증서를 교부하는 단계
사후관리 단계	인증 취득기관이 정보보호관리체계를 지속적으로 운영·유지하는 지를 점검

이러한 절차를 통해 평가된 자산 정보의 가치가 높을수록 정보보호관리체계 인증을 필요로 하게 된다. 그 절차는 인증 취득을 원하는 기업이 인증심사를 신청하고 평가 받으며, 인증서를 발급받기까지는 약 3개월의 시간이 소요되고 4단계로 진행된다. 사후관리 단계까지 통과했을 경우 인증서가 발급되며 기업의 정보보호관리 제도가 검증되었음이 보증 받는다.

2.2 전자정부 정보보호관리체계 인증

전자정부 정보보호관리체계(G-ISMS) 인증은 기관이 수립하고 구축한 종합적인 정보보호관리체계(ISMS)를 제3자가 객관적으로 심사하여 인증을 부여하는 제도이다[8]. 정부 행정기관 등의 조직 및 서비스의 특성에 적합하게 수립된 종합적인 정보보호 관리체계를 의미한다. G-ISMS 인증체계는 역할과 책임에 따라 [표 2]와 같이 정책기관, 인증위원회, 인증기관, 신청기관으로 구분한다. 정책기관과 인증위원회는 행정안전부가, 인증기관의 역할은 한국인터넷진흥원이 수행하고 있다.

G-ISMS 인증을 취득했을 경우 침해사고에 대한 능동적인 예방체계 구축을 통해 전자정부 서비스에 대한 피해를 최소화 할 수 있으며, 종합적인(관리·기술·물리) 정보보호 대책을 수립하여 개인 및 국가 정보 유출을 사전에 예방할 수 있다[2]. 또한 정보보호관련 법적 요구사항에 대하여 체계적으로 대응하고, 지속적인 정보보호 관리를 통하여 새로운 보안위협에 대하여 효과적으로 대응할 수 있다. 이에 따라 정부 및 행정기관에서는 G-ISMS 도입에 대한 요구가 점차 증가하고 있다.

2.3 개인정보보호 관리체계 인증

개인정보 유출 사고 증가로 개인정보 침해 관련 사고가 급증함에 따라 개인정보보호 노력을 객관적으로 증빙할 수 있는 인증 제도에 대한 요구가 증가하게 되었다. 이에 따라 기업이 고객의 개인정보보호를 체계적·지속적으로 수행하기 위해 필요한 일련의 보호 조치를 개인정보보호 관리체계(PIMS: Personal Information Management System)로 정의하였다[7].

<표 2> G-ISMS 구성 조직

수행 기관	업무
정책기관 (행정안전부)	G-ISMS 인증 제도의 수립, 인증기관의 지정 및 감독, 인증위원회 구성 및 관리, 인증심사원 임명, 인증관련 예산의 확보 및 출연, 그 밖의 인증에 필요한 정책의 수립 등 수행
인증위원회	인증기관에서 제출한 인증심사결과보고서의 심의·승인, 인증기관 자격 심의·인정, 인증심사원 자격 심의·인정, 기타 행정안전부 장관이 위임한 업무를 수행
인증기관 (KISA)	G-ISMS 인증심사, 인증서 발급 및 관리, 인증심사원 교육, 인증상담 및 기술자문, 그 밖의 인증업무에 필요한 연구사업 등을 수행
신청기관	G-ISMS 인증을 신청한 기관

PIMS는 기업이 개인 사용자의 정보보안을 위하여 도입하는 제도로 기업이 사용자의 개인 정보를 유출하지 않기 위해 수립하고 있는 관리 체계이다. PIMS 도입을 통해 기업에서 개인정보를 다루는 과정에 대한 평가 받을 수 있으며, 평가를 통과할 경우 안전하게 개인정보를 취급하고 있음을 보증 받을 수 있다.

3. 정보보호제품

기업은 기업의 정보 자산을 보호하고 조직원 및 사용자의 개인 정보의 유출을 방지하기 위하여 다양한 정보보호 관리체계를 도입하여 기업 정보보안 기능을 강화하고 있다[1]. 이러한 정보보호관리체계가 실제로 구축되기 위해서는 조직원 및 사용자 측면의 보안부터 내부망 전체의 보안을 제공할 수 있는 정보보호제품이 도입되어야 한다.

3.1 백신 제품군

과거에는 보안 사고를 통해 자신을 과시하는데 목적을 둔 보안 위협이 대부분이었으나, 최근에는 금전적 이득을 취하는 공격이 날로 증가하고 있다. 이로 인해 악성코드 제작 툴 등을 이용한 대량의 악성코드가 유포되고 있으며, 악성코드도 복잡해지고 은폐기능이 고도화되고 있다. 기업의 경우 1대의 PC가 악성코드에 감염될 경우 네트워크를 통하여 전사적으로 전파되어 대규모 피해를 일으킬 수 있어 해킹 예방에 대한 요구가 급증하고 있다. 이러한 요구를 만족하는 가장 기본적인 보호 조치가 백신이다. 백신은 기업이나 개인 사용자 모두에게 기본적으로 설치해야 될 제품군으로 외부로부터 유입된 악성코드를 탐지하고 삭제할 뿐만 아니라 실시간으로 감염 여부를 알려주기 때문에 기본적으로 조직원 및 사용자 모두가 설치해야 한다. 특히 DDoS 대란이 발생했을 경우에도 좀비 PC를 생성하는 악성코드들을 탐지하고 분석하는 역할을 하였으며, 분석된 내용을 기반으로 백신 개발 업체에서 전용 백신을 배포하여 좀비 PC를 치료하는데 중요한 역할을 하였다. 또한 최근 개발되는 백신은 악성코드 탐지 및 치료뿐만 아니라 웹 보안, 메일 보안, USB 드라이브 검사 등 다양한 기능을 제공하고 있어 정보 유출 및 악성코드 유입으로부터 보호하고 있다. 웹 보안 기능을 통해서 유해 사이트에 대한 접근을 차단하며, 유해 사이트로부터 파일 다운로드를 차단한다. 메일 보안 기능을 통해서는 메일을 통해 내부로 유입하는 악성코드를 차단하며, USB 드라이브를 검사하는 기능을 통해서 매체를 통해 악성코드가 전파되는 것을 방지하고 있어 정보보안에 큰 역할을 하고 있다.

3.2 방화벽 제품군

방화벽은 기업이나 조직에서 정보보안을 위하여 필수적으로 도입해야 되는 가장 대표적인 정보보호시스템 이다. 외부망에서 내부망으로 패킷이 유입될 때 방화벽 정책에 따라 허용·차단 등의 정책을 패킷에 명령하여 내부로 유입되어도 되는 패킷인지 판단하는 시스템이다. 또한 내부망에서 외부망으로 전송하는 패킷에 대해서도 검사하여 허용된 패킷만 외부로 유출 가능하도록 하는 시스템이다.

블랙 리스트와 화이트 리스트 기반의 필터링 기능으로 패킷을 허용·차단하고 기본적으로 제공하는 NAT 기능을 통해 유연한 망 호환성을 제공하고 있다.

방화벽은 네트워크 보안 제품 중 하나로 악성코드를 탐지하는 침입방지시스템(IPS: Intrusion Prevention System), 네트워크에 대한 접근 통제 기능을 제공하는 네트워크접근제어시스템(NAC: Network Access Control), 인터넷망을 전용선과 동일한 안전성을 제공하는 사설망으로 사용하는 가상사설망(VPN: Virtual Private Network) 등의 기능이 접목되어 통합보안시스템(UTM: Unified Threat Management)으로 운영되기도 한다.

3.3 논리적 망분리 제품군

정부기관 및 기업의 해킹 등 사이버 공격이 증가함에 따라 내부의 정보 유출을 막기 위해 업무망과 인터넷망을 분리하여 운영하고자 하는 요구가 증가하고 있다. 이러한 요구는 PC 2대를 사용하여 물리적으로 망을 분리하는 환경을 조성하게 되었다. 하지만 물리적 망분리를 구축했을 경우 조직원 수만큼의 PC가 더 필요하고 망을 다시 구축해야 하기 때문에 설비비용에 대한 문제가 제기되었다. 이러한 요구들을 만족하기 위하여 1대의 PC에서 업무망과 인터넷망을 분리하는 논리적 망분리 제품이 개발되었다.

논리적 망분리 제품에 기반이 되는 기술이 가상화 기술이다. 가상화란 하나의 물리적인 하드웨어를 다수의 가상 하드웨어로 구분하여 각각의 가상 하드웨어에 사용자가 필요한 어플리케이션 및 운영체제를 설치하여 사용하는 기술이다. 여러대의 물리적인 시스템으로 운영하던 환경에서 1대의 물리적인 시스템의 다수의 가상 머신이 운영되는 환경으로 변경되어 하드웨어 사용률을 최적화 할 수 있다. 효율성뿐만 아니라 가상 환경에서만 인터넷이 가능하도록 기능이 제공되고 있어 인터넷망을 통하여 악성코드가 유입되더라도 악성코드는 가상화 환경에만 존재하는 것이며, 하드 디스크, 메모리, 네트워크가 모두 분리되어 있기 때문에 내부망으로 악성코드가 유입될 수 없다. 또한 내부망의 기업 정보도 인터넷이 연결되지 않는 로컬 영역에서만 업무가 가능하기 때문에 기업 정보의 유출이 발생하지 않으며, 유출 경로를 추적할 수 있기 때문에 논리적 망분리 제품에 대한 요구가 증가하고 있다.

4. 기업 정보보안 기능 강화 방안 및 결론

기업의 정보 자산의 가치가 점차 높아짐에 따라 기업 정보를 보호하고 기업의 정보통신 인프라를 강화하는 방안이 강구되고 있다. 기업 정보보안 기능을 강화하기 위해서는 아래와 같이 정보보호관리체계에 따라 프로세스를 수립하여 관리하고 유지하는 것이 중요하다.

<표 3> ISMS 인증 심사 기준

통제분야	내용
관리 과정	1. 정보보호 정책 수립 2. 관리체계 범위 설정 3. 위험관리 4. 구현 5. 사후관리
문서화	1. 문서요건 2. 문서의 통제 3. 운영기록의 통제
정보보호대책	1. 정보보호 대책 2. 정보보호 조직 3. 외부자 보안 4. 정보자산 분류 5. 정보보호 교육 및 훈련 6. 인적 보안 7. 물리적 보안 8. 시스템개발 보안 9. 암호 통제 10. 접근 통제 11. 운영 관리 12. 전자거래 보안 13. 보안사고 관리 14. 검토, 모니터링 및 감사 15. 업무 연속성 관리

정보보호관리체계(ISMS) 인증심사 기준은 필수사항인 '관리과정 14개 통제항목', '문서화 요구사항 3개 통제항목', 선택사항인 '정보보호관리 통제항목 120개 항목' 등 총 137개로 구성되어 있다. 인증 신청기업은 관리과정과 문서화 요구사항인 17개 항목은 반드시 이행하여야 하며, 선택사항인 정보보호대책을 위한 정보보호관리 통제항목은 120개 중에서 해당되는 항목을 선택하면 된다. 이렇게 선택된 심사기준의 요구사항을 충족하고 기업에 정보보호제품을 도입한다면 기업 정보보안 기능을 강화할 수 있을 것으로 사료된다.

4.1 정보보호 정책 수립 및 관리

정보보호관리체계는 ① 정보보호정책 수립, ② 정보보호관리체계 범위 설정, ③ 위험관리, ④ 구현, ⑤ 사후관리 등 5단계의 과정을 거쳐 수립·운영된다. 새로운 위협요소 및 취약성 발견 등 지속적으로 변화하는 IT 및 인터넷 환경에서 내부 주요 정보자산을 효과적으로 보호하고 관리하기 위해서는 주기적인 위험분석을 통한 지속적인 사후관리가 필요하다. 이 과정은 일회성 단계가 아니라, 지속적으로 유지 관리되어야 하는 순환 주기의 형태를 가진다. 특히 사후관리를 통해 실질적으로 운영되고 있는 정보보호관리체계의 적합성을 판단하고 부족한 부분에 대한 갱신이 이루어져야 한다. [표 3]에서 이러한 관리과정의 순환적 절차를 보여준다. 정보보호 관리과정 5단계에 대한 심사기준은 총 14개 통제항목으로 구성되어 있으며, 각 단계에서 통제항목을 만족하도록 정보보호 정책을 수립하고 관리되어야 한다.

<표 4> 문서관리 요구사항

요구사항	내용
문서요건	정보보호관리체계와 관련된 문서는 기업의 모든 임직원 및 관련자들이 쉽게 이용할 수 있도록, 해당 기업의 규모 및 운영 환경, 기능 등을 고려하여 문서화해야 함
문서의 통제	작성된 문서는 문서의 발생 타당성 승인, 갱신, 배포, 폐기 등의 통제를 위한 절차를 수립하여야 함
운영기록의 통제	정보보호관리체계를 효율적으로 운영하기 위해서 운영기록을 확인, 유지보수, 보존, 폐기하는 문서화된 절차를 수립하고 유지·관리하여야 함

4.2 문서화 및 문서 관리

정보보호관리체계 수립 및 운영의 근거는 정책, 지침, 절차 등을 수립하고, 문서화하여 관리되어야 한다. 이러한 문서 관리에 대한 요구사항을 인증심사 기준에서 [표 4]와 같이 3개 항목으로 제시하고 있으며, 이러한 통제항목을 만족할 수 있도록 필요한 정보에 대한 문서화가 반드시 이행되어야 한다.

4.3 정보보호 대책 마련

정보보호관리체계는 정보보호에 관련된 위험을 통제하기 위한 대책을 수립하고 관리하는 체계라고 할 수 있으며, 인증심사 기준에 대해서는 15개 분야로 구분하여 총 120개 통제항목을 제시하고 있어 이를 만족할 수 있는 대책을 마련해야 한다.

참고문헌

[1] Carey, Mark. "Enterprise Risk Management: How To Jumpstart Your Implementation Efforts." International Risk Management Institute, 2005

[2] Corporate Governance Task Force. "Information Security Governance: A Call to Action." National Cyber Security Partnership, 2004.04

[3] ISO(International Standard organization), ISO 27001, 2005.10

[4] John Sherwood, Andrew Clark and David Lynas. "Enterprise Security Architecture: A Business -Driven Approach", CPM Books 2005.

[5] Westby, Jody. "Information Security: Responsibilities of Boards of Directors and Senior Management." Testimony before the House Committee on Government Reform: Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, September 22, 2004.

[6] 한국인터넷진흥원, ISMS(정보보호관리체계), 2008.05

[7] 한국인터넷진흥원, PIMS(개인정보보호관리체계), 2010.11

[8] 행정안전부, G-ISMS(전자정부정보보호관리체계), 2009.12