기업 정보보호 이론보다 실천이 중요하다

제작 | 정보보호실천협의회

제작후원 | (주)시큐브 • (주)안철수연구소 • 어울림정보기술(주) • 인포섹(주)
• (주)에이쓰리시큐리티컨설팅 • (주)제이컴정보 • (주)잉카인터넷 • 한국CISSP협회

기업 정보보호 실천 가이드 2007

발행일 : 2007년 3월 10일
제　작 : 정보보호실천협의회
발　행 : 월간 정보보호21c
디자인 : 이지현(ggaerook@hanmail.net)
발행처 : 정보보호실천협의회
서울시 송파구 가락동 78번지
TEL.(02)4055-114 / FAX.(02)4055-619

content

01 정보보호는 '보안이 가장 중요한 투자' 라는 인식에서 시작한다

02 보안정책 수립에도 순서가 있다

03 잘나가는 기업은 정보보호 정책부터 다르다

04 정보보호, 이론보다 실천이 중요하다

부록

보안솔루션 가이드 & 침해사고 대응기관

정보보호의 시작은 보안에 대한 인식 제고이다.
보안의 중요성을 깨닫지 못한다면 아무리 잘 된 정책이 있다 해도
업무에 방해되는 귀찮고 까다로운 규정으로 인식되어
기업의 예산을 축내고 업무 효율성을 떨어뜨리는
'천덕꾸러기' 로 전락하고 만다.
정보보호를 위해서는 가장 먼저 CEO가 앞장서서
'보안이 가장 중요한 투자' 라고 인식하는 것이 필요하며,
전 임직원의 보안의식이 제고되어야 한다.

정보보호는 보안이
가장 중요한 투자라는
인식에서 시작된다

특별 기고

한국정보보호진흥원 이홍섭 원장
hslee@kisa.or.kr

“기업의 경쟁력, 이제는 정보보호관리자가 나서야 한다”

기업 정보화의 일부로만 여겨졌던 정보보호의 중요성이 나날이 강조되면서 기업내 최고보안책임자인 CSO와 최고개인정보보호책임자인 CPO제도가 도입되고 있다. CSO를 중심으로 CEO와 관리자들이 앞장서 전사적인 보안정책을 수립하고 실현해나간다면, 기업의 부가가치는 상승할 것이고, 이로 인한 ‘전략적 이익’으로 인해 21세기 치열한 글로벌 경쟁시대의 승자가 될 수 있을 것이다.

IT 강국 한국의 위기설

“한강의 기적”으로 불리우는 한국 성장의 역사가 21세기를 맞아 IT라는 새로운 화두로 다시 쓰여지고 있다. 이미 각종 매체가 발표했다시피, 한국은 초고속 기반의 정보환경을 바탕으로 IT 각 분야에서 세계적으로 손꼽히는 성과를 거두고 있다. 이 과정에서 기업은 정부의 일사불란한 IT 정책과 산업역군들의 노력을 바탕으로 IT 강국 한국號의 엔진 역할을 충실히 해왔다.

하지만 최근, 재계 일각에서 “한국 위기설”을 제기하고 있다. 1990년대 이후 우리 경제를 이끌어온 IT 산업의 경쟁력이 점차 약화되고 있으며, 이는 5~6년 후 우리나라 전체를 혼란에 빠뜨릴 수 있다는 것이 위기설의 요체다. 한국은행 역시 “지난 10년간 한국 경

제를 이끌어온 IT 산업은 국내 산업성장 동력으로서 한계에 부딪쳤다"며, 재계의 지적과 맥락을 같이했다.

CEO의 능력과 자질

우리나라는 1990년대 후반, IMF라는 절체절명의 위기를 정부, 기업, 개인 등 각 사회 주체가 합심, 단결하여 극복해냈다. 특히, 기업은 대기업간 중복투자나 무리한 차입경영 등 팽창 우선 원칙과 주먹구구식 경영을 접고, CEO를 중심으로 한 전문경영 체제로의 전환을 통해 위기일발의 상황을 돌파했다. 당시 CEO는 모험심과 도전정신으로 대표되는 "기업가 정신"을 무기로 과감한 개혁과 혁신, 선택과 집중 등 기업의 체질 개선을 시도했다. 하지만 최근의 IT 산업 위기를 돌파해야할 미래형 CEO는 기존의 CEO들의 무기였던 "기업가 정신"만으로는 부족하다. '조직이 보유한 지식을 어떻게 관리하고 통제하며 공유하느냐' 하는 문제들을 정확히 이해해야 한다. 또한, 정보획득 방법과 정보의 흐름을 통제하는 방법에 대한 지식을 갖춰야 한다. 미래기술 발전의 방향과 속도를 예측하는 식견도 갖춰야 하고 정보화시대를 살아가는 고객과 국민의 프라이버시를 보호해줄 수 있는 의지와 관련 지식도 섭렵하고 있어야 한다. 그러나 현실적인 관점에서 한 사람의 CEO가 이러한 모든 자질과 전문지식을 갖출 수 있는가에 대해서는 회의적이다. 아마 불가능할 것이다. 그래서 대기업에서는 이미 각 분야별로 전문적인 능력을 갖춘 COO(Chief of Operation Officer : 최고관리책임자), CFO(Chief of Finance Officer : 최고재무책임자), CMO(Chief of Marketing Officer : 최고마케팅책임자), CTO(Chief of Technology Officer : 최고기술책임자), CIO(Chief of Information Officer : 최고정보책임자/정보관리책임자), CKO(Chief of Knowledge Officer : 최고지식책임자) 등을 임명하고 있다.

CSO, CPO 등 정보보호관리자의 등장

기업 정보화의 일부로만 여겨졌던 정보보호의 중요성이 나날이 강조되면서 기업내 최고보안책임자인 CSO(Chief of Security Officer)와 최고개인정보보호책임자인

CPO(Chief of Privacy Offiecr) 제도가 도입되고 있다.

대표적인 글로벌 기업인 마이크로소프트사에서는 자사의 보안 향상을 위해 지난 2002년 1월 CSO를 공식적으로 임명했다. AOL Time Warner의 경우도 기업의 보안을 감독 · 조정하기 위해 2002년 초 CSO라는 직위를 만들어냈다. 이외에도 2002년을 기점으로 썬마이크로시스템즈, 오라클, HP, GE 등이 CSO 제도를 마련하였다. 한편, 국내의 경우는 2002년 초까지만 해도 대부분의 기업들이 출입관리 시스템과 같은 물리적 보안 시스템을 총무부서에서 수행하고 정보 시스템과 관련된 보안부문은 IT 부서에서 맡는 형태를 취하고 있었다. 그러나 보안의 중요성 및 그 범위가 넓어짐에 따라 LG 그룹이 2002년 6월 최초로 CSO 제도를 도입한 이후 현재는 국내 주요 기업들이 CSO를 별도로 두거나 기존 정보담당 임원의 역할을 강화해 보안수준을 한층 높이고 있다.

CSO의 역할과 필요성

기업에서 CSO를 임명하고자 할 경우, 기업이 현재 직면하고 있는 개인정보보호 및 보안규제 수준을 비롯하여 고객과 내부 직원의 규모, 고객이 원하는 보안수준 등을 고려하여야 한다. 그러나 회사 내부적으로 명문화된 보안방침이 없거나, 있더라도 그것을 제대로 실현되지 않고 있는 경우, 그리고 고객이 개인정보보호 강화를 요구했을 경우, 또 아웃소싱 계약에서 보안 이슈가 검토되지 않고 있다거나, 사내 데이터가 기밀등급에 따라 구분되지 않고 있다면, 더욱이 모든 관리자와 직원이 보안위험에 대한 심각성을 깨닫지 못하고 있는 경우라면, 이런 경우의 기업은 CSO 임명을 시급히 검토해야 할 것이다. 이는 기업 내에 CSO가 절실히 필요한 시점이라는 '경고' 이기 때문이다.

그리고 흔히들 CSO를 CIO의 하위 개념으로 생각하는 경향이 있다. 그러나 실제로 해외 선진국에서는 CSO가 IT에 국한된 보안이 아닌 전사적인 보안정책과 실현을 컨트롤하는 별도의 기능을 하며, CIO 보다 상위 개념으로 인식되고 있다. CSO는 기업보안을 위한 전사적인 보안정책 수립은 물론, 기술적인 대책과 법률적인 대응까지 총괄할 수 있어야 하기 때문이다.

먼저, CSO는 내부 직원들과 원활하게 의사소통하며 자신의 역할과 책임에 대해 정당화할 수 있어야 한다. '보안' 은 언제나 '편이성' 과 상충하는 부분이 있기 때문에 내부 직

원들이 보안에 대한 필요성과 중요성을 분명하게 인식하고 있어야 하며, 사내 보안강화가 결국은 자신이 몸담고 있는 회사에 이익이 되며, 그것이 개개인에게도 혜택이 되어 돌아올 것이라는 확신을 심어주어야 한다.

또한, 더 나은 보안체계를 구축하기 위해 기업 내부의 모든 기능과 부서에서 필요한 예산과 자원을 확보할 수 있어야 한다. 그러나 아직도 기업의 정보화 대비 정보보호 투자 예산은 턱없이 부족하고, 일부 경영자들은 아직도 '보안'이 기업경쟁력 향상을 위한 필수 요소임을 인식하지 못하고 있는 것이 현실이다. 그러므로 CEO를 비롯한 모든 임직원들에게 '보안에 대한 긴박감'을 조성하고, 보안에 대한 성과를 산술적으로 전환해냄으로써 기업 정보보호의 중요성과 이로 인한 이익을 가시적으로 보여줄 수 있는 CSO가 필요한 것이다.

기업 경쟁력에 미치는 영향

실제, 국내 기업들의 내부 정보유출 피해사례와 고객의 개인정보 유출사고로 인해 기업의 이미지에 큰 타격을 입게 되는 사례를 자주 접할 수 있는데, 이 같은 사고의 경우 그 기업이 받는 충격과 피해는 언론이나 신문지상에서 알려진 단순한 피해액의 규모를 훨씬 뛰어넘어 기업의 존폐를 좌우하기도 한다. 특히, 중소기업의 경우, 오랜 시간 연구개발한 기술자료가 유출되어 투자비용 회수와 재투자가 어렵게 되어 문을 닫게 된 경우를 쉽게 찾아볼 수 있다. 더욱이 이러한 정보유출의 경우, 대부분 내부자의 소행이기 때문에 기업 내부에 실질적이고 구체적인 보안정책과 감사체제가 확립되어 있지 않다면 막아낼 수가 없다.

그러므로 CSO를 중심으로 CEO와 관리자들이 앞장서 '보안은 조직 내 모든 사람의 책임'이란 의식을 확실하게 심어주고 전사적인 보안정책을 수립하고 실현해나간다면, 기업의 부가가치는 상승할 것이고, 이로 인한 '전략적 이익'으로 인해 21세기 치열한 글로벌 경쟁시대의 승자가 될 수 있을 것이다. 그러므로 최고경영자는 이러한 CSO의 역량이 기업의 생존과 장기적인 이익 창출은 물론, 기업의 경쟁력 제고에 막대한 영향을 미친다는 것을 확실하게 인식하고, CSO 임명을 적극적으로 추진해야 할 것이다.

01

인포섹㈜ 보안연구센터 홍진기 이사
jkhong@skinfosec.co.kr

전사적 정보보안 아키텍처 수립이 필요한 시기이다

많은 기업들이 IT 서비스와 비즈니스와의 연계성을 높이고 있어 기존의 단편적인 보안솔루션 도입이나 관련 정책, 지침에 한계를 느끼며 좀 더 체계적인 정보보안을 고민하고 있다. 기업이 제공하는 비즈니스 서비스와 정보보안이 체계적으로 연계되어 있지 않아 전사적인 관점의 정보보안 서비스가 마련되어 있지 못하기 때문이다.

정보통신기반보호법이 2001년 제정되면서 정보보안 시장은 모의해킹 진단, Perimeter Security를 위한 침입차단 시스템, 침입탐지 시스템과 같은 기본적 보안솔루션 도입 등 기술적 보안을 중심으로 활성화 되었다. 그에 따라 대리나 과장급의 실무담당자가 그 기업의 보안을 책임졌고, 활동범위와 의사결정 수준이 실무급에 머무르게 되었다. 그러나 2~3년간의 정보보안 성숙기를 거치면서 각 기업들은 비즈니스 경쟁력을 높이기 위하여 영국표준 정보보안 경영 시스템 국제인증 규격인 BS 7799(British Standard 7799)나 국제표준화 기구(ISO : International Organization for Standardization)의 정보보호 관리체계 인증인 ISO 27001 등의 정보보호 관리와 관련된 국제인증 획득을 경쟁적으로 벌이고 있다. 또한, 고객 접근성을 강화하고, 다양하게 하기 위한 차세대 시스템 구축과 같은 IT 서비스와 비즈니스와의 연계성을 높이고 있다.

그러다보니 기존의 단편적인 보안솔루션 도입이나 관련 정책, 지침들은 그 한계를 드러내고 있으며, 기업들은 좀 더 체계적인 정보보안을 고민하게 되었다.

정보보안과 관련한 기업의 주요 관심사는

- 각종 관련 법/규제에 대해 적절한 수준의 대책은 잘되어 있는가?
- 지속적으로 등장하는 신종 공격기법에 능동적 사전에 대응할 수는 방안은 없을까?
- 좀 더 효과적이고 경제적으로 보안위험을 완화할 수 있는 방법은 무엇일까?
- Time-to-Market 전략으로 인하여 시시각각 변하는 IT 서비스에 유연하게 대응할 수 있는 정보보안 방법은 무엇일까?
- 개인정보 보호, 내부정보 유출방지와 같은 동향 및 이슈에 대한 능동적인 대처 방안은 무엇이 있을까?
- 지속적으로 늘어가는 정보보안 예산과 성과에 대한 적절한 관리방안은 어떤 것일까?

가트너 그룹이 2005년에 CSO의 5가지 주요 이슈를 조사한 결과 역시 위에서 언급한 기업 정보보안 주요관심사와 크게 다르지 않다.

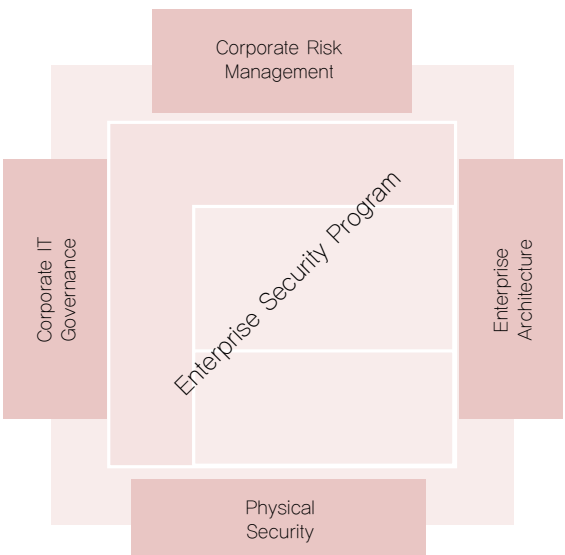
- 정보보안 조직에 대한 이슈 : 보안담당 임원은 기업 조직의 어디에 위치하고, 어떤 지휘계통 아래에서 타 조직과 어떻게 의사소통할 것인가?
- 정보보안 거버넌스에 대한 이슈 : 기업 거버넌스와 정보보안과의 관계, 정보보안 거버넌스에서 다뤄야 하는 내용은 무엇인가?
- 적절한 수준의 정보보안 예산 : 경쟁사 또는 산업군 평균과 비교하여 정보보안을 위해 소요되는 비용을 어느 정도의 수준으로 유지할 것인가?
- 정보보안 아키텍처 : 보안담당 임원의 주요 역할인 전사 정보보안 프로그램을 어떻게 관리하고, 프로그램의 핵심 구성요소인 정보보안 아키텍처를 어떻게 구성할 것인가?
- 정보보안 규정준수 : 보안담당 임원의 주요 책임인 SOX, BAZEL-II 등 상위기관 관련 규정준수에 대하여 어떻게 준비할 것인가?

CSO를 비롯한 기업의 보안담당자들이 이 같은 내용에 관심을 갖고 있다는 것은 기업이 제공하는 각종 비즈니스 서비스에 대한 정보보안의 우선순위가 높아졌다는 사실을 보

여준다. 동시에 기업이 제공하는 업무 또는 서비스와 정보보안이 체계적으로 연계되어 있지 않고, 실질적인 정보보안 최고책임자가 임원수준으로 조직되어 있지 않으며, 그로 인하여 전사적인 관점의 통합과 일관성 있는 정보보안 서비스가 마련되어 있지 못하고 있다는 현실을 드러내기도 한다.

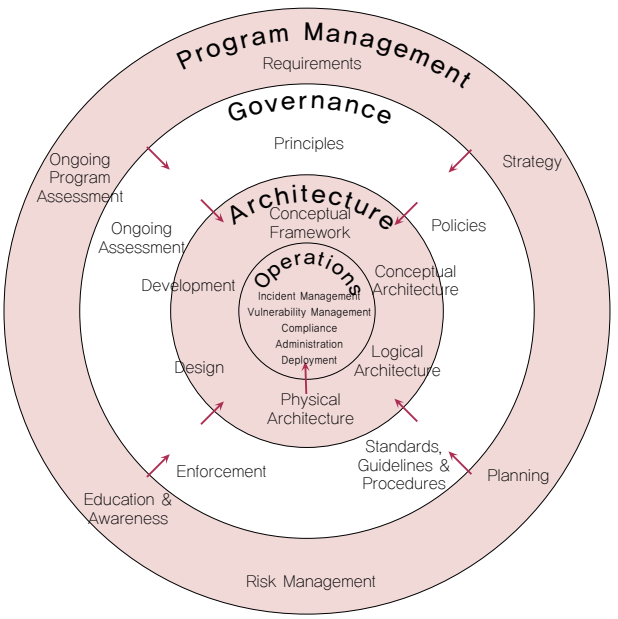
전사적인 정보보안 체계 수립을 통한 해결

가트너 그룹 등 선진사례를 통해 보면 정보보안 시스템을 구축하는 데에는 전사적인 관점에서의 정보보안 프로그램을 개발하는 것이 가장 효과적이다. BS 7799, ISO 27001, CoBIT, NIST 등과 같은 모델을 이용하여 정보보안 프로그램을 개발하는 기업도 있다. 그러나 전사적인 관점에서의 정보보안 프로그램을 위해서는 기업 비즈니스와의 연계성을 강화하고, 비즈니스 요구사항이 반영된 정보보안 전략과 원칙을 수립해야 한다. 통제정책을 마련하고, 통합 위험관리, 전사적인 아키텍처, 물리적인 보안, 통합 IT 거버넌스와 정보보안 프로그램의 상관관계를 고려해 개발해야 한다.



[그림 1] 전사적 정보보안 프로그램

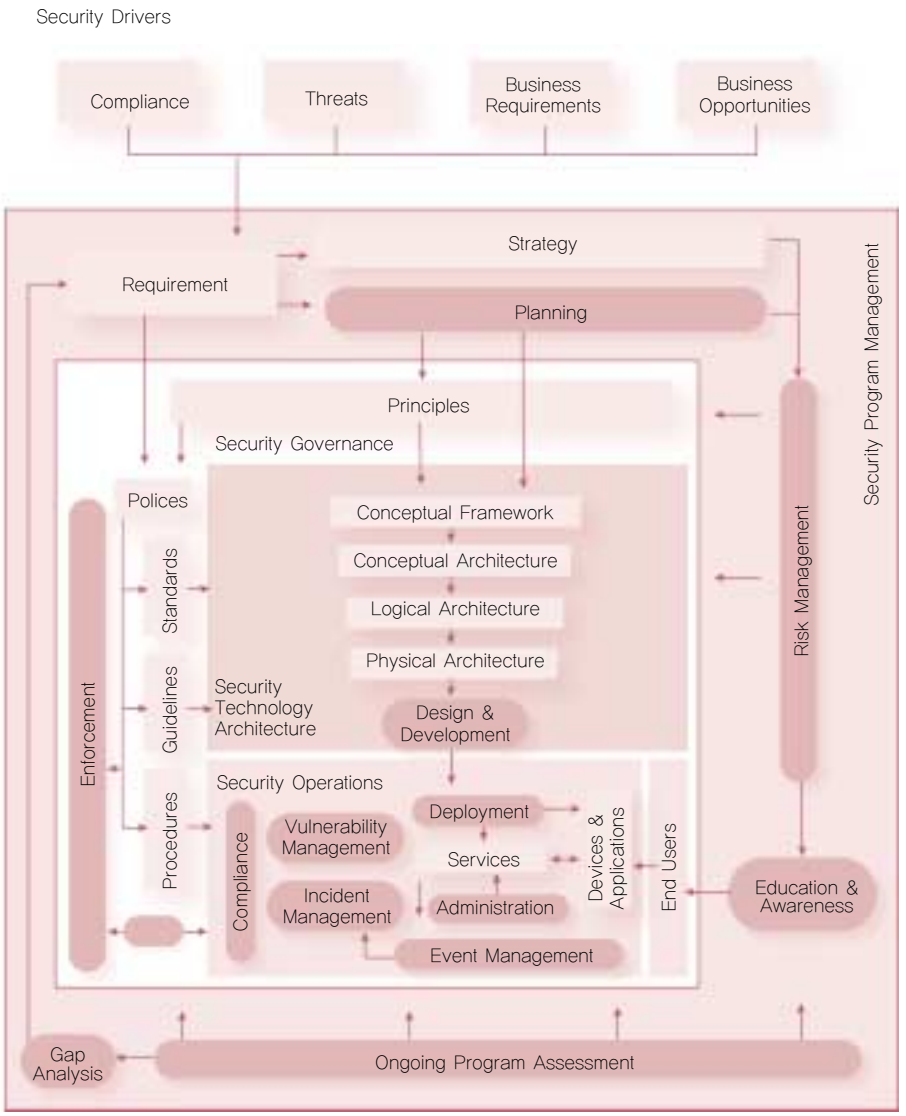
좀 더 구체적으로 전사적 관점의 보안 프로그램과 전사 정보보안 체계와의 관계를 이해하기 위해 NAC(Network Applications Consortium)에서 제시하는 전사적 관점의 정보보안 프로그램 모델을 제시한다. 〈그림 2〉에서 나타나듯이 정보보안 프로그램 전체를 포괄하는 제일 바깥쪽의 동심원인 프로그램 매니지먼트 영역의 요구사항, 전략, 계획 등의 구성요소들은 내부 동심원에 존재하는 통제, 설계, 운용영역의 구성요소와 프로세스에게 영향을 주는 관계로 구성된다. 예를 들어, 개인정보보호에 대한 새로운 요구조건이 발생하면, 통제영역의 새 법칙과 정책, 표준의 구성요소가 달라지고, 그에 따라 설계영역의 구조, 설계의 구성이 새로운 개념으로 변화된다.



[그림 2] NAC 정보보안 모델

NAC에서 제시하는 전사적 정보보안 프로그램 모델을 구조적인 면에서 좀 더 완결성을 높여 보면, 최상위의 보안 드라이버에 속하는 요구조건과 위협, 사업에 있어서의 요구사항, 사업기회 등이 정보보안 구조의 시작점이 된다. 이는 또한 전사적 정보보안 프로그램의 주된 원천이 되는 구성요소이기도 하다. 기업 내부의 요구조건은 사업영역인 사업기회와 사업상의 요구사항을 이끌어낸다. 기업 외부의 요구조건을 충족하기 위해서는 컴

플라이언스와 위험성이라는 구성요소가 정보보안을 이끌어낸다. 〈그림 3〉에서 4각형 박스로 표현된 것이 구성요소이며, 8각형 박스는 과정이다.



[그림 3] NAC 프레임 워크

Security Governance/Operations 주요 구성요소와 개발 가이드

시큐리티 거버넌스를 구성하는 주요 요소는 원칙, 정책, 표준, 가이드라인, 절차, 감사, 통제 등이 있다. 시큐리티 거버넌스를 개발할 때는 기업의 환경과 특징에 따라 부분적으로 다르지만 지표가 되는 보안원리를 식별하고 보안정책을 통해 집행권한을 부여하여 실행하는 절차를 갖는 것은 동일하다. 표준, 가이드라인, 절차를 개발하는 단계에서는 보안 전담조직 내부 뿐만 아니라 타 조직간의 역할과 책임을 정의하는 것이 매우 중요하다.

Security Governance 구성요소와 과정	Principle	• 전사적 정보보안 계획인 Planning을 Input하여 Security Technology Architecture와 전사적 정보보호 정책인 Policy의 기준이 되는 Component
	Policies	• 기업의 특수성이 반영된 Principle을 기반으로 ISO 17799:2000과 같은 표준을 이용하여 보안정책을 수립할 수 있는 Component
	Standards/ Guidelines/ Procedures	• 수립된 Policy를 기반으로 절대적으로 준수해야 하는 Standard, Best Practice로 권고되는 가이드라인. Standard와 Guideline을 달성하기 위한 방법을 기술한 Procedure로 구성된 Component
	Audit Enforcement	• 수립된 보안정책에 대한 각종 정보보안 활동의 준수여부를 검토하는 Process • Security Policy의 준수여부를 확인하는 종합적인 Process • 기술/관리적 통제들을 조합하여 수행되는 Process

[표 1] Security Governance 구성요소와 과정

보안기술 설계를 할 때 고려되어야 할 요소로 침입차단 시스템, 침입방지 시스템과 같은 기술적인 부분을 감안해야 한다. 이는 단순히 보안시스템과 네트워크, 서버, 애플리케이션, 데이터 등 레이어별로 나누거나, ITU-T X.805에 따라 Access Management, Authentication, Non-Repudiation, Data Confidentiality, Communication Security, Integrity, Availability, Privacy 등 8개의 범위로 구분할 수 있다.

구분 기준에 따라 세부적인 구성요소를 도출하고 아키텍처를 개발한다. 이때 정책과 계획에서 아키텍처 개발을 위한 정책을 반영하는 것이 중요하다. 개발순서는 Conceptual Framework, Conceptual Architecture, Logical Architecture, Physical(Implementation) Architecture의 순서를 따르는 것이 유지관리 하기에 쉽다. 동일 산업군의 경우에는 Conceptual Framework와 Conceptual Architecture가 재활

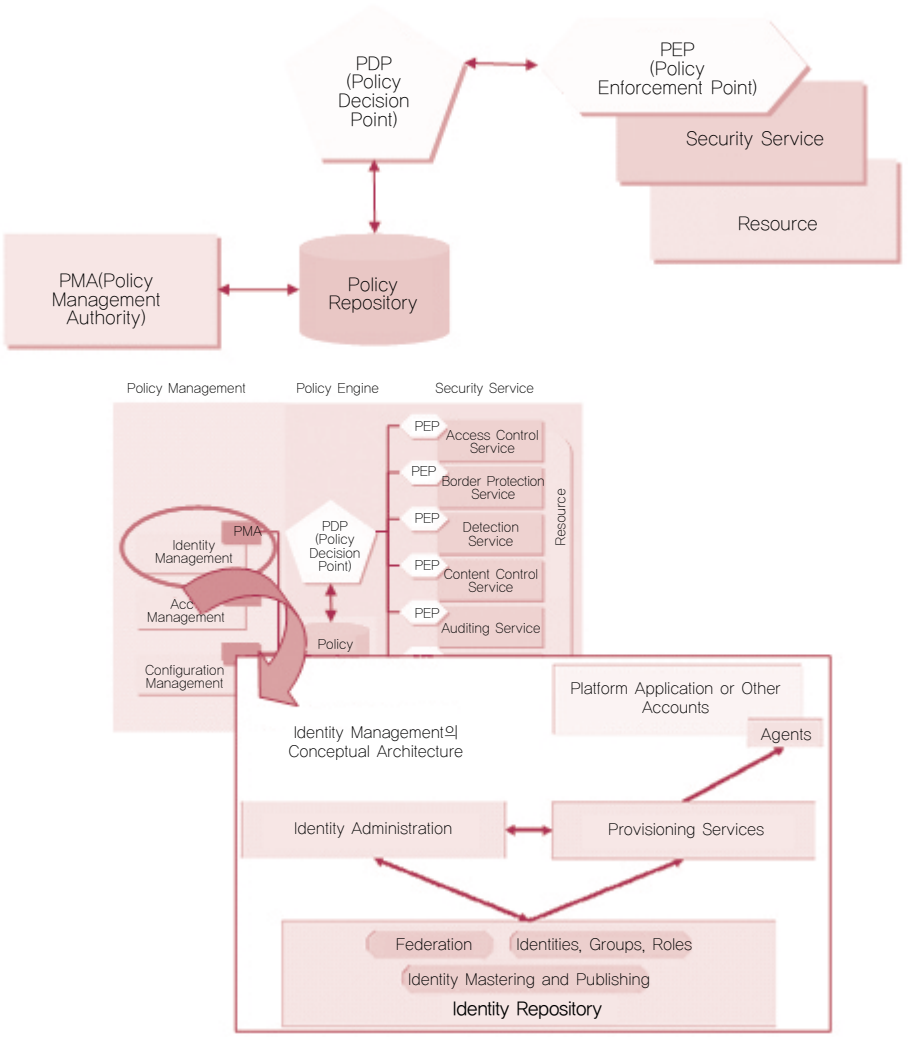
용률이 높고, Physical(Implementation) Architecture는 네트워크 구성, 하드웨어 구성 등 상황에 따라 차이를 보이는 경우가 종종 발생한다.

Security Technology Architecture의 주요 구성요소	Conceptual Framework	Security Policy 기반의 정보보안 서비스에 대한 상위 레벨의 개념적 기술 프레임워크
	Conceptual Architecture	Conceptual Framework를 좀 더 세분화하고 의사결정을 관리하기 위한 개념적 틀
	Logical Architecture	Conceptual Architecture에서 정의된 주요 Component들과 Service들에 대한 구성과 관계를 기술
	Physical Architecture	Implementation Architecture와 같은 의미로 쓰이며, 앞에서 설계된 Logical architecture가 실제 환경

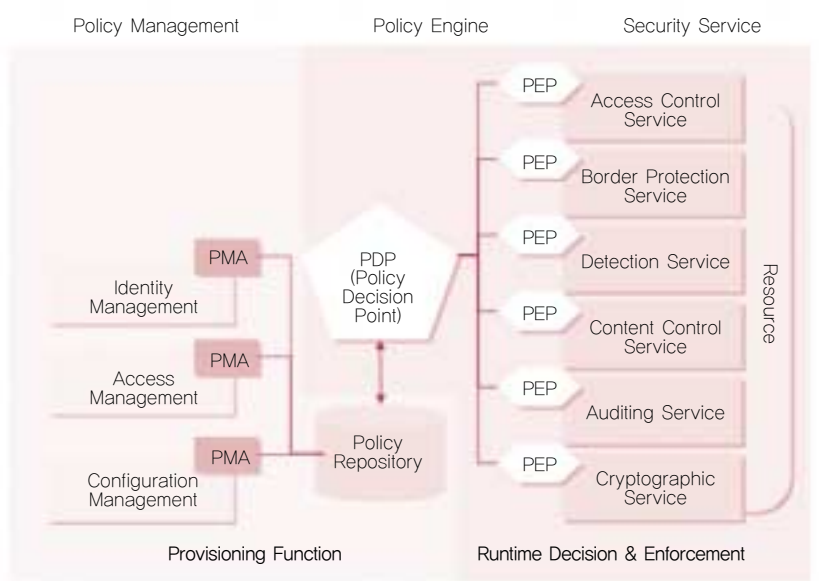
[표 2] Security Technology Architecture의 주요 구성요소

Conceptual Framework와 Conceptual Architecture는 전사적인 정보보안 정책을 Policy Repository에 저장함으로써 정보보안 정책개발과 의사결정에 참조되도록 개념적인 프레임워크를 개발한 것이다. 위에서 언급된 Conceptual Framework에서 PMA를 세분화하여 Identity Management, Access Management, Configuration Management와 같은 세부 아키텍처를 도출하고 PEP를 세분화하여 Policy Management와 Access Control, Border Protection, Detection 등과 같은 세부 아키텍처를 도출하여 세분화된 Architecture를 보면 〈그림 4〉와 같다. Conceptual Architecture에서 도출된 Identity Management, Access Management, Configuration Management 중에서 Identity Management에 대한 Conceptual Architecture를 설계하면 〈그림 5〉와 같이 나타낼 수 있다. 도출된 Identity Management Component의 Conceptual Architecture를 기반으로 서비스에 필요한 세부 구성요소들과 그 관계를 도출하기 위한 Logical Architecture의 구성은 〈그림 6〉과 같이 나타낼 수 있다. Identity Management의 Logical Architecture에서 세부적으로 도출된 구성요소들과 그 관계를 통하여 실제 환경에 적용하기 위한 Physical Architecture의 예는 〈그림 7〉과 같다. Identity Management이외에 Conceptual Architecture에서 도출된 Access Management와 같은 기타 다른 Architecture들도 위

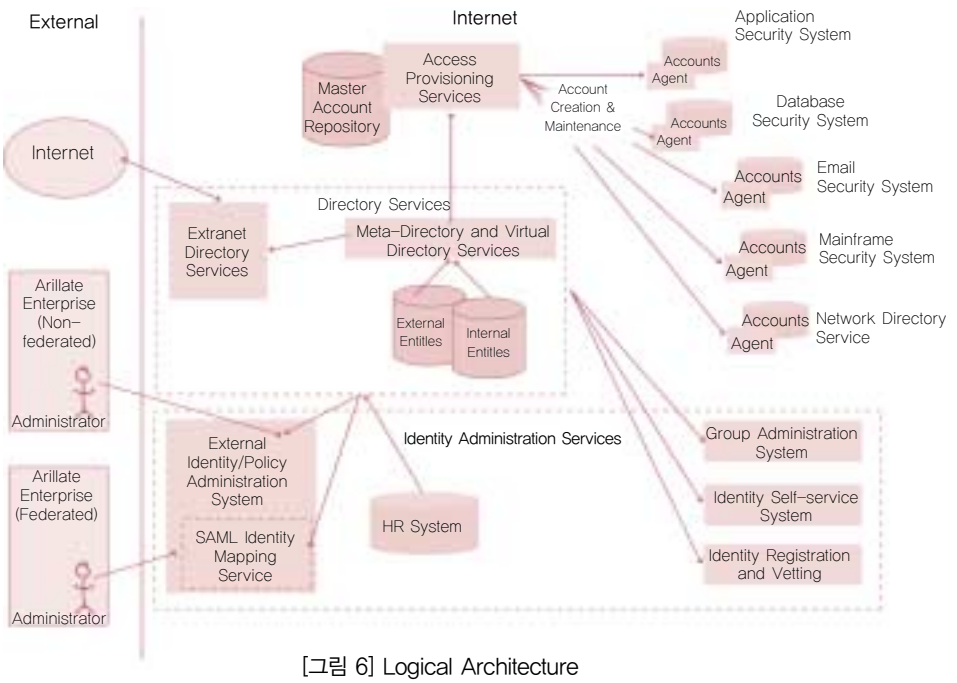
와 같은 방법으로 Conceptual Architecture, Logical Architecture, Physical Architecture를 설계하면 된다.



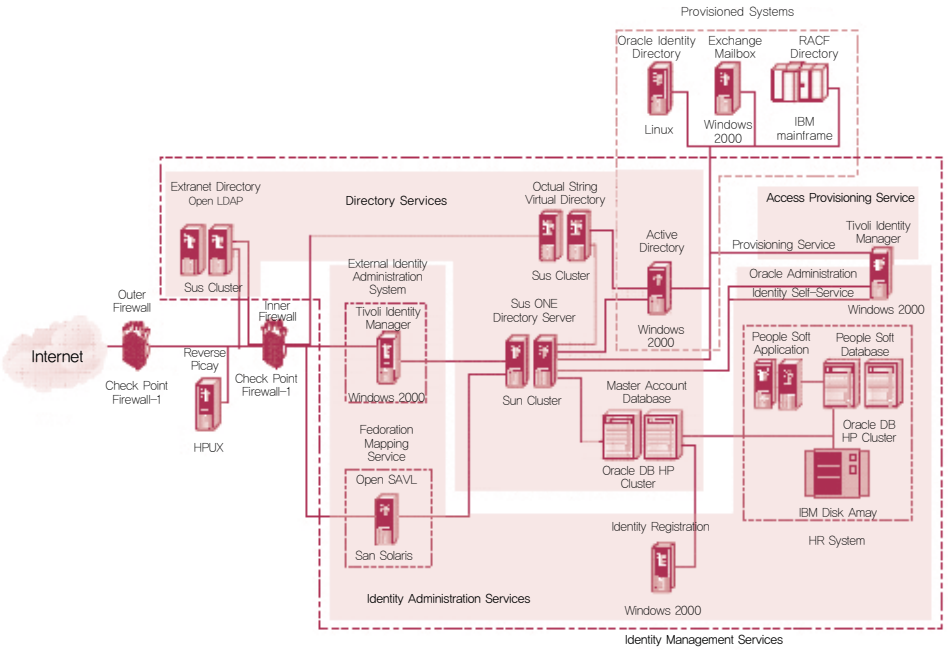
[그림 4] Conceptual Framework/ Conceptual Architecture



[그림 5] Identity Management에 대한 Conceptual Architecture



[그림 6] Logical Architecture



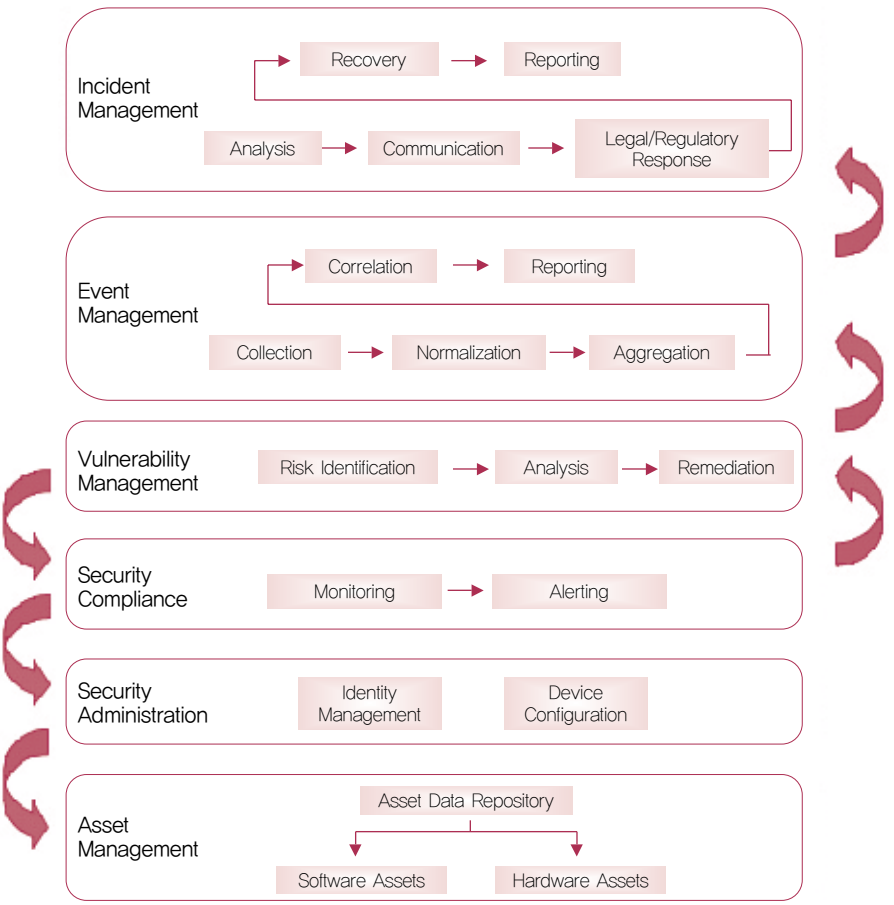
[그림 7] Physical(Implement) Architecture

Security Operations Architecture는 두 개 유형의 Process로 분류할 수 있다. 하나는, Administration, Compliance Vulnerability management Process와 같은 정보보안 정책에 따라 기술요소들을 확인하고 적절한 보호역할을 제공하는데 필요한 프로세스이다. 다른 하나는 Administration, Event, Incident Management Processes와 같은 정보보안 정책을 집행하기 위해 필요한 프로세스들이다. 두 유형의 근본은 Asset Management이다.

6개의 Process와 Component로 구성된 Security Operations Architecture는 Asset Management를 기반으로 다른 구성요소를 지원하며, 이 Component의 하드웨어와 소프트웨어 등 모든 정보자산의 정보는 계약갱신 활동, 소프트웨어 라이센스 준수 감사 활동, 소요비용 절감활동 등에 활용된다.

Security Administration Component는 Identity Management와 Device Configuration으로 구성되어 정보자산의 안전한 접근관리와 시스템이나 장비의 정보에

대한 무결성을 확보하기 위해 필요한 기술요소와 Best Practice를 계획하고 조정하고 구현하는 역할을 담당한다. 각 Component들은 〈그림 8〉과 같이 세부 Component와 Process들로 구성되며 각 Management 아키텍처들과 관계를 갖고 있다.



[그림 8] Security Operations Architecture

최근 정보보안 사고대응에 대한 요구사항이 높아짐에 따라 Security Operation Architecture를 구성하는 대부분의 Component와 Process들은 자동화 도구를 도입하고 있으므로 Security Technical Architecture를 구성하는 Component들과 연계성을 충분히 고려해야 한다.

Vulnerability Management의 경우, 기존의 단편적인 진단기능 만을 자동화한 솔루션에서 3-Tier 아키텍처를 가지고 분산형태로 정보자산의 취약점을 진단하고 통합분석하며 진단 히스토리까지 관리하는 자동화된 솔루션이 등장하고 있으며, Asset Management, Event Management의 경우, 최근 ITSM 구축을 추진하는 기업이 많아짐에 따라 ITSM을 통해 구축되는 CMDB(Change Management Data Base)와 연계를 고려하는 경우도 나타나고 있다. 조직구성이 전국적으로 분산된 대형기업의 경우, 각종 준수규정들을 데이터베이스화 하고 프로그래밍하여 Compliance Management를 통합관리 하는 사례도 종종 있다.

최근 주요 대표적인 기업이나 기관들의 경우, 크래커로부터 금전적인 지불을 요구하는 공개적 위협을 받는 경우도 있고, IT의 특성상 이미 웹사이트를 긁어갔는데도 모르고 있다가 나중에서야 홍커(중국 해커)에게 노출 되었었음을 알게 되는 경우도 있다. 또한, 개정된 전자정부거래법에 대하여 나름대로 바쁘게 준비는 했지만 어딘지 모르게 만족스럽지 못한 막연한 불안감을 갖고 있는 기업도 있을 것이다. 이러한 내 · 외부의 각종 정보보안 이슈들에 대하여 전사적으로 이미 준비가 되어 있는 기업이나 기관이라면, 좀 더 느긋하게 해외 정보보안의 동향은 어떠한지도 살펴볼 수 있는 여유를 가질 수 있을 것으로 보인다.

Security Operations Architecture의 주요 구성요소	Asset Management	Security Operations Architecture에서 가장 기본이 되며, H/W, S/W의 목록을 관리하는 콤포넌트와 프로세스
	Administration	각종 보안사고로부터 정보자산을 안전하게 관리하는 프로세스
	Compliance	적용된 기술요소가 조직내 정책 · 지침 · 절차 · 아키텍처에 준수하도록 관리하는 프로세스
	Vulnerability Management	인프라 구성요소의 위험요소를 식별하고 취약점을 평가하여 적절한 대책을 적용하는 프로세스
	Event Management	운영환경을 구성하는 각종 장비에서 생성되는 보안관련 이벤트를 Day-to-Day로 관리하는 프로세스
	Incident Management	정보보안 정책에 위배되는 이벤트 등에 대해 대응 · 관리하는 프로세스

[표 3] Security Operations Architecture의 주요 구성요소

02

㈜에이쓰리시큐리티컨설팅 박세현 책임컨설턴트
shpark@a3sc.co.kr

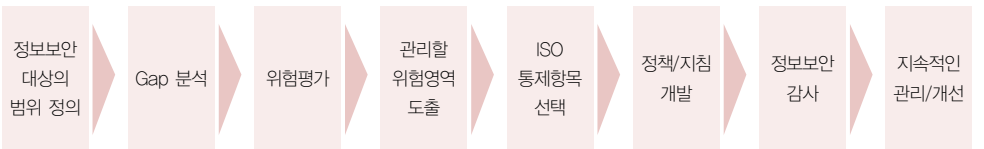
왜 국제 보안표준 체계를 구축해야 하는가

정보보안의 국제표준 인증은 회사의 보안통제 수준을 점검하고, 임직원의 정보보안 마인드를 제고하며, 회사의 대외 이미지와 신뢰성을 강화할 수 있다. 또한, 국제표준 인증을 받았다는 것은 정보보안 관리체계 개선 프로세스가 비로소 시작된 것이라고 볼 수 있다. 보안사고와 정보유출 사고가 급증하고 있는 상황에서 정형화된 보안 프로세스를 구축하고, 이를 통하여 보안사고 및 정보유출 사고를 사전에 예방하여 기업 경쟁력을 강화하는 것은 선택의 문제가 아닌 필수적인 활동이다.

정보보안도 국제표준에 부합한 프로세스를 구축하는 것이 필요하다. 글로벌 비즈니스 시대에 기업의 정보보안 통제(Control)와 프로세스를 국제표준에 맞게 구축하여 정보보안 활동을 하고 기업의 소중한 정보자산을 보호하는 것은 글로벌 경쟁력의 필수 요소로 자리 잡고 있다.

국제 보안표준은 영국 표준인 BS 7799에서 시작하였다. BS 7799는 2005년 10월 ISO27001 국제 표준으로 전환되었으며 현재 국내외 많은 기관과 기업이 ISO 27001 인증을 획득하기 위해 준비하고 있다. 우리나라에서는 LG전자, 삼성전자, 포스코, 우리은행, 서울시청, 특허청 등 40여개 기관 및 기업이 국제 보안표준 인증을 획득하였다. 해외에서는 Sony, British Telecom 등의 기업이 인증을 획득하였다. ISO 27001 국제 보안표준은 정보보안 관리체계(ISMS : Information Security Management System)를 수

립하고 지속적으로 개선하는 프로세스를 구축하도록 요구하고 있다. 이는 ISO 9000, ISO 14000에서 요구하는 개선 프로세스와 동일하다. 개선 프로세스를 지속적으로 하기 위해서는 PDCA(Plan-Do-Check-Act) 체계를 구축하고, 단발성 보안통제 보다 계속 발생하는 보안 취약점을 제거하고 정보보안 관리체계의 보안성을 강화하는 것을 목적으로 한다.



[그림 1] ISO 27001 정보보안 관리체계 수립 과정

ISO 27001 인증획득 과정 통해 본 국제 보안표준 인증 필요성

㈜에이쓰리시큐리티컨설팅이 ISO 27001 국제 보안표준에 따라 정보보안 관리체계를 구축한 A사의 사례를 통해 국제 보안표준 인증의 필요성을 살펴보겠다. A사는 IT관련 연구소이며 신기술 제품정보와 같은 각종 연구개발정보를 보유하고 있다. A사는 ISO 27001 인증을 획득하여 회사의 보안통제 수준을 점검하고, 인증을 획득하는 과정에서 임직원의 정보보안 마인드를 제고하며, 회사의 대외 이미지와 신뢰성을 강화하고자 하였다.

[그림 2] ISO 27001 인증 컨설팅 수행절차

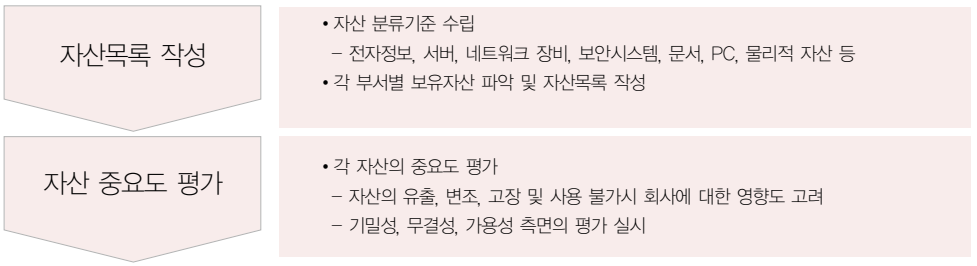
ISO 27001 인증 획득 컨설팅의 첫 번째 과정은 인증을 획득할 범위를 정의하는 것이다. ISMS 구축범위와 컨설팅 수행범위를 결정하는 것을 말한다. 일반적으로 정보보안관

리 체계를 구축하는 범위는 회사의 중요한 비즈니스 또는 업무 프로세스에 대하여 우선적으로 수립한다. 정보보안 관리체계를 구축하기 위해서는 적지 않은 노력이 필요하고, 임직원의 보안 마인드 강화가 필요하다. 따라서 작은 영역에서 시작해서 점차 확대하여 회사 전체에 적용하는 것이 바람직하다. 예를 들어 은행 등 금융권은 인터넷 뱅킹 시스템, e-Business 업무 프로세스 등과 같은 영역에서 우선 인증을 획득하는 것이 일반적이다. 회사의 핵심 영역에 대하여 보안체계를 우선적으로 강화하여 비용대비 효과를 극대화하기 위한 전략이다.

A사는 인증획득 범위를 사업장 전체로 정의하였다. A사는 물리적으로 여러 곳에 사업장을 갖고 있었으며, 수십개의 부서와 수천명의 임직원으로 구성되어 있었다. 인증범위가 넓을수록 경영층의 적극적인 지원과 임직원의 참여가 필요했기 때문에 A사의 프로젝트 전담인력과 컨설턴트로 TFT를 구성한 후 다음 단계인 자산분석을 시작하였다.

자산분석은 정보보안 관리체계를 구축할 영역에 포함된 모든 자산을 파악하여 목록을 작성하고, 파악된 자산이 회사에서 차지하는 중요도를 평가하는 과정이다. 이러한 자산분석 과정은 회사의 많은 자산 중 중요한 핵심자산을 파악하고, 추후에 보호대책을 집중하기 위한 것이다. TFT는 A사의 자산을 파악하기 위하여 자산 분류기준을 작성하였다. 자산 분류기준은 A사의 자산보유 현황과 업무환경을 고려하여 수립하였다. 예를 들어 A사의 경우, 연구개발 정보와 함께 개발중인 제품의 디자인 또한 중요한 정보였다. 따라서 프로젝트 Task는 제품에 포함된 디자인 정보도 회사의 자산으로 자산분류 기준에 포함하였다. 이와 같이 회사의 자산을 분류하기 위해서는 해당 회사의 환경을 분석하고, 회사의 자산환경을 반영하는 분류기준을 수립해야 한다. 이 외에도 서버, 네트워크 장비, 보안시스템, 물리적 장비(UPS, 항온항습기 등) 등이 포함된다.

TFT는 수립된 자산분류 기준에 따라 자산조사를 시작하였다. 수십개의 부서에서 보유하고 있는 자산에 대한 조사는 많은 시간이 소요되었으며, 각 부서의 적극적인 참여가 이뤄지지 않는다면 불가능한 작업이다. 이렇게 작성된 자산목록은 각 부서에서 지속적으로 유지 관리해야 하도록 되어 있다. A사의 각 부서에서 파악된 자산은 회사에서 차지하는 중요도에 대한 평가로 실시되었다. 이러한 자산의 중요도 평가는 각 자산의 소유자에 의하여 진행되었다. 자산에 대한 중요도 평가는 회사의 많은 자산 중에서 보호해야 할 핵심자산을 찾아내기 위한 과정이었다.



[그림 3] 자산분석 수행 절차

A사의 자산을 파악하고, 각 자산의 중요도를 파악한 후 취약점 분석을 시작하였다. 취약점 분석은 파악된 자산에 존재하는 취약점을 찾아내는 과정이다. 자산 유형별로 다양한 취약점이 존재할 수 있으며, 이러한 취약점을 관리적, 물리적, 기술적 측면에서 분석하였다.

관리적, 물리적 취약점 분석은 ISO 27001에서 요구하는 11개 영역 133개 통제항목과 A사의 보안통제 현황 사이의 Gap 분석작업이었다. 이를 통하여 보안정책, 보안조직, 보

[그림 4] 관리적, 물리적 취약점 분석

[그림 5] 기술적 취약점 분석

안사고 관리, 인적 보안, 물리적 보안구역 등에 대한 취약점을 발견할 수 있다. 기술적 취약점 분석은 서버, 네트워크 장비, 보안시스템(침입차단 시스템, 침입방지 시스템 등) 등에 대한 점검과 모의해킹을 실시하여 A사 자산의 기술적 취약점을 찾아내었다.

다음 단계는 위험평가로, 파악된 자산의 중요도와 취약점 분석단계에서 파악된 자산의 취약점(위협 포함) 정도를 종합하여 자산의 보안 위험을 산정하는 과정이다. 서버에 취약점이 많다고 해서 보안위험이 높은 것은 아니다. 서버에 많은 취약점이 있지만 서버에 중요한 정보가 하나도 존재하지 않는다면 많은 비용을 들여서 보안솔루션을 설치하고 보안을 강화하는 것보다, 중요한 정보를 포함한 서버에 대하여 우선적으로 보안을 강화하는 것이 필요하다.

다음은 정보보안 대책을 수립하는 것으로, 산출된 위험중에서 높은 위험을 선별하고 이러한 위험을 감소시키기 위한 보호대책을 정의하는 단계이다. 정보보안 대책은 즉시 조치할 수 있는 Hot-Fix와 단기 및 중·장기 대책으로 구분한다. 정보보안 대책의 이행일정, 비용계획 등을 포함한 정보보안 마스터플랜을 작성하였다. 정보보안 관리체계는 지속적으로 개선하는 프로세스를 구축하는 작업이다. 수립된 체계를 이행하고 지속적으로 개선하기 위해서는 적절한 정책 및 지침과 절차가 필요하다. TFT는 기존에 수립된 A사의 정보보안 정책, 지침, 절차를 분석하고 ISO 27001 표준 체계를 반영한 신규 정보보안 정책, 지침, 절차를 수립하였다.

인증을 지원하는 절차를 시작하는 단계에서는 TFT에서 수립한 정보보안 대책과 이를 증명하기 위한 기록을 만들어야 한다. 정보보안 정책, 지침, 절차에 따라 임직원은 각종 보안활동을 수행하며, A사는 이러한 내용을 인증기관의 심사원에게 증명해야 한다. A사는 수립된 정보보안 관리체계를 운영하면서 관련 기록을 관리하고, 인증준비를 실시하였다. 또한, 임직원의 보안 마인드 강화를 위하여 보안담당자 교육, 전자메일, 게시판 등을 통한 인식제고 홍보 활동을 실시하였으며, 각 부서에 대한 보안점검을 병행하였다.

ISO 27001 인증심사는 문서심사와 본심사로 이뤄지며, 두 단계의 심사를 통과하면 인증을 획득하고 인증서를 받는다. 컨설팅사는 A사가 성공적으로 인증획득을 완료할 수 있도록 임직원 보안교육, 각종 문서 작성 등을 지원하였으며, 이러한 과정을 통하여 A사는 인증기관으로부터 인증심사를 받고 성공적으로 인증을 획득하였다.

구 분	내 용
정보보안 정책서	• 조직의 보안통제 목적, 목표, 내용 등을 정의 • 세부 지침, 절차 수립 필요
정보보안 관리체계 범위 정의서	• 정보보안 관리체계 구축 범위를 기술
위험평가 방법론	• 위험평가를 수행한 방법을 기술
위험평가 보고서	• 위험평가 결과를 기술
위험조치 계획서	• 산출된 위험을 관리하기 위한 계획을 기술
통제효과성 측정 지표	• 보안통제의 효과성을 측정하기 위한 지표 및 절차 기술
적용성 보고서	• 통제 선택 사유, 현 보안통제 현황 등 기술

[표 1] ISO 27001 문서와 요구사항

성공적인 정보보안 관리체계 구축요건

국제표준 인증획득을 위해서도 그렇지만, 궁극적으로 성공적인 정보보안 관리체계를 구축하고 이행하기 위해서는 우선 경영층의 적극적인 의지와 지원이 기본이 되어야 한다. 보안담당자들이 정보보안의 중요성을 인식하고, 적극적인 활동을 하고자 하여도 경영층이 이해하지 못하면 보안활동을 업무의 효율성을 방해하는 요소로만 인식할 수 있다. 경영층이 이러한 생각을 갖고 있을 때 정보보안 관리체계는 효과적으로 구축, 운영될 수 없다. 따라서 경영층의 적극적인 의지와 지원이 뒷받침되어야만 정보보안 관리체계는 실질적인 효과를 발휘할 수 있다. 경영층의 의지만큼 중요한 것이 임직원의 보안의식이다. 구축된 보안체계에 따라 행동해야 하는 임직원이 보안활동에 대하여 저항감을 갖고 있다면 형식적인 보안활동에 머무를 뿐이고, 보안통제는 무너질 수밖에 없다. 이를 위해서는 정보보안 관리체계의 지속적인 개선활동이 필요하다. 국제표준 인증은 지속적인 개선 프로세스가 시작되었다는 것을 의미하므로, 표준에 따른 개선활동이 이어져야 한다.

03

인포섹㈜ 전략컨설팅 조희석 팀장
hscho@skinfosec.co.kr

효과적인 개인정보 보호를 위해 고객정보관리 프로세스 개선이 필요하다

IT 기술의 발전으로 인한 개인정보 유출 피해가 심각한 상황에 이르고 있다. 정부와 각 기관이 이와 관련한 각종 규제정책을 발표하고 있지만, 개인정보 유출사고는 날이 갈수록 늘고 있다. 기업도 각종 보안솔루션을 도입하면서 개인정보를 보호하고 있지만, 지능화 되는 침해사고를 예방하지 못한다. 효과적인 개인정보 보호를 위해서는 고객정보관리 프로세스의 개선이 필요하다.

몇 년 전 까지만 해도 우리사회에서 개인정보 보호는 관심밖의 일이었다. 정부와 시민단체, 언론에서 꾸준히 개인정보 유출에 따른 심각성을 공론화하면서 개인정보 보호와 관련된 각종 법률과 제도가 만들어졌다. 하지만 개인정보 유출 사고는 날이 갈수록 늘어나고 있으며, 이로 인한 피해규모는 심각한 수준에 이르고 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률에서는 개인정보를 '생존하는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(당해 정보만으로 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)' 라고 정의하고 있다. 이에 따른 개인정보 유형은 일반정보와 가족정보, 교육정보, 병역정보, 부동산정보, 동산정보, 소득정보, 기타수익정보, 신용정보, 법적정보, 의료정보, 신체정보 등으로 구

분할 수 있다. 개인정보의 오남용과 부적절한 누출은 개인에 대한 편견, 명예훼손, 경제적인 손실, 신용 저하, 범죄 악용 등을 초래할 수 있다.

단 계	침해 유형
정보의 수집 단계	• 동의없는 개인정보의 수집 및 수집시 고지사항의 불이행 • 동의 및 고지 없는 개인정보 주체 외로부터 수집 • 법정 대리인의 동의없는 개인정보의 수집 • 서비스 이용과 관련없는 과도한 개인정보의 수집 • 해킹 등 불법 수단에 의하여 개인정보의 수집 • 기망에 의한 개인정보의 수집
정보의 저장 및 관리	• 조직 내부 취급자에 의하여 개인정보의 유출/훼손/변경 • 외부인의 불법적 접근에 의한 개인정보 유출/훼손/변경 • 사업자의 인식부족과 과실 등으로 인한 개인정보의 공개 • 기술/관리 조치 미비로 인한 개인정보 유출 • 개인정보와 관련하여 고객의 크레임에 대한 불응 또는 미조치
이용 및 제공	• 동의없는 개인정보의 무단 제공 및 공유 • 당초 수집시에 고지한 이용목적을 넘어서는 개인정보의 이용 • 타인의 개인정보를 무단으로 이용하는 경우
정보 파기	• 수집 및 목적 달성 후 개인정보의 미파기 • 개인정보 삭제 요구의 불응

[표 1] 정보의 생명주기에 따라 분류한 개인정보 침해유형

개인정보 유출이 일어나는 이유

엔씨소프트의 온라인 게임 리니지 명의도용 사건에 대해 법원은 2006년 "재산상 손해가 없더라도 개인정보 유출만으로 정신적 고통을 당했으므로 위자료를 지급하라"고 판결하였다. 이 사건은 개인정보 보호에 대한 기업의 경각심을 다시한번 일깨우는 계기가 되었다. 각 기업은 개인정보 보호 강화를 위한 다각적인 노력을 시작하였으며, 정부와 관계기관은 관련 법률과 규제정책을 마련하였다. 그러나 대량의 개인정보 침해사고는 여전히 빈번하게 발생하고 있다.

우리나라의 경우, 대량의 개인정보 유출사고가 일어나는 이유로 주민등록번호 체계를 지적하기도 한다. 단일번호를 통한 인증체계인 주민등록번호는 공공기관 뿐 아니라 민간

부문에서도 광범위하게 사용되고 있다. 한번 유출되면 그 피해가 오랫동안 반복적으로 일어날 가능성이 높다는 것이다. 다른 나라에서 사용되는 사회보장번호는 번호 자체에 생년월일이나 성별 등 식별 가능한 정보가 담겨있지 않으며, 본인이 원할 경우 변경할 수 있다. 주민등록번호는 신원확인 뿐 아니라 법적 권리 행사, 재산권 행사 및 금융활동 등 개인에게 결정적인 일에 사용되고 있어 주민등록번호 유출은 피해자를 사회생활에서 한 순간 도태시킬 수 있는 엄청난 파괴력을 갖고 있다.

개인정보 유출의 가장 큰 이유는 IT 기술의 발전이다. 컴퓨터 용량의 급속한 증가와 데이터베이스 기술의 발전은 과거에는 상상하기도 힘들었던 대용량의 정보를 저장하고, 처리할 수 있게 만들었다. IT 기술의 발전은 수집된 개인정보를 가공해 개인의 취향을 분석하고, 판매 수요를 예측하며, 이탈 예상고객을 가려내는 등 영업적으로 매우 유용하게 사용될 수 있다. 많은 기업들이 이를 활용하여 기업 이익을 극대화 하고 있다. 이 기술은 최근 이익을 추구하는 기업뿐만 아니라 정부기관, 의료기관, 교육기관 등으로 확대되어 국민의 사생활은 모두 디지털 정보화 되어 있다고 할 수 있다. 개인정보를 저장하고 있는 정보시스템에 불법적 접근을 통한 불법 정보유출의 피해는 커질 수밖에 없는 실정이다.

개인정보가 디지털화 되어 있다고 해도 공공의 목적으로만 사용한다면 개인정보 유출 피해를 걱정할 이유가 없다. 그러나 많은 기업들이 이익 극대화를 위해 개인정보를 무작위로 사용하였으며, 심지어 다른 목적으로 판매하는 등의 비윤리적인 행동까지 보이면서 개인의 피해를 심화시켰다. 여기에는 기업의 최고경영자의 무관심도 큰 영향을 미쳤다. 기업 보안담당자의 대부분은 경영자의 관심 부족을 정보보호 강화에 있어 가장 어려운 점으로 꼽고 있다. 여전히 많은 기업에서 보안담당자와 개인정보보호 담당자가 하는 일이 경영층에 보고되지 않고 있는 실정이다. 실제로 보안책임자의 29%만이 CEO 또는 이사회에 개인정보보호와 관련된 사항을 보고하는 것으로 나타났다.

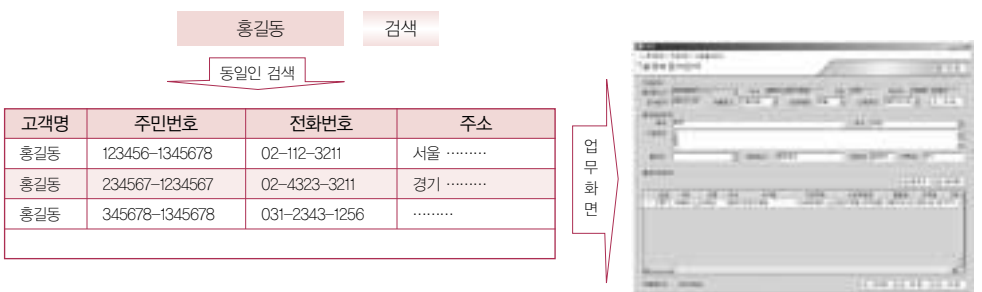
프로세스 개선을 통한 보안체계 강화

개인정보 보호기술(Privacy Enhancing Technology)은 크게 웹을 기반으로 하는 익명성 제공기술과 에이전트 기술, 네트워크 기반시설로 구분할 수 있다. 웹 기반의 익명성 제공기술은 정보와 소유자간의 관계나 송수신자간의 관계를 비밀로 하여 사용자의 정보

를 보호하는 기술이다. 에이전트 기술은 사용자가 파악하기 쉽지 않은 인터넷 상의 정보 유출에 대해 사용자를 대신하여 통제해주는 역할을 하는 에이전트를 사용하는 기술이다. 쿠키 매니저(Cookie Manager), 애드 브로커(Ad Blocker), 스파이웨어 필터(Spyware Filter) 등의 기술이 있다.

가장 빈번하게 일어나는 개인정보 침해사고는 네트워크 환경에서 정보를 전달할 때 중간에서 가로채거나, 수정하거나, 단순히 그 데이터를 열람하는 행동이다. 이를 막기 위해서는 프록시, 방화벽, IDS 등을 이용할 수 있다. 현재 개발중인 기술로 PISA(Privacy Incorporated Software Agent)와 W3C의 P3P(Platform for Privacy Preferences) 등이 있다.

이 중 네트워크 기술을 제외한 대부분의 기술은 개인사용자가 네트워크 상에서 스스로의 정보를 보호하려는 것에 집중되고 있어 개인정보를 다루는 기업이 내부자 또는 악의적인 외부자에 의해 대량의 정보가 유출되는 사고에 대한 방법을 제시하지 못하고 있다. 이같은 한계를 해결하기 위해 기업의 보안담당자나 개인정보보호 담당자는 보안솔루션을 대안으로 내세운다. 보안솔루션을 도입한다는 것 자체가 나쁘다는 것은 아니지만, 고객정보보호를 위해 각 기업에 맞는 솔루션을 찾기가 어렵고, 높은 효과를 기대하기도 어렵다. 확실한 보안효과를 노리기 위해서는 보안솔루션과 함께 프로세스 개선이 필수적이다.



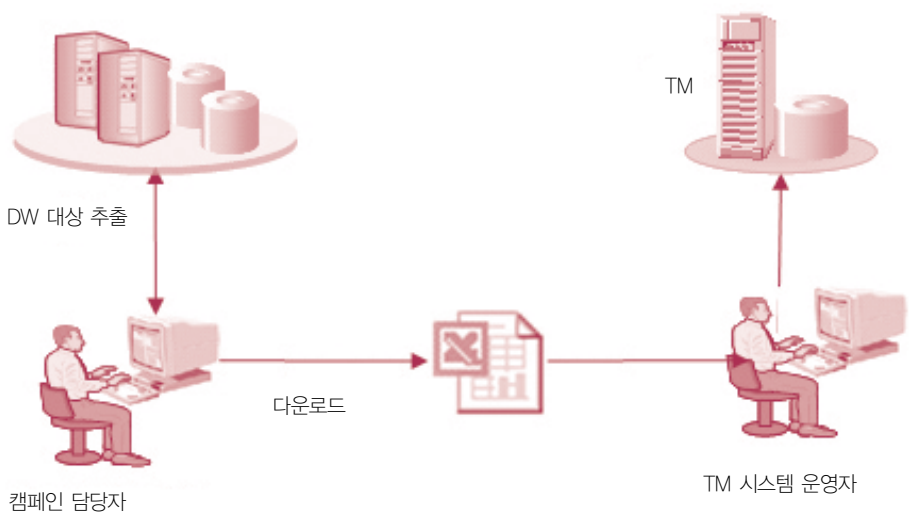
[그림 1] 고객조회 방법 수정으로 개인정보 보호

현재 개인정보 보호를 위해 기업들이 가장 많이 사용하는 고객조회 방법은 〈그림 1〉과 같이 동명의 개인을 전부 조회하고 사용자가 개인의 속성자료를 확인한 후, 속성이 일

치하는 고객을 선택하여 원하는 업무화면으로 이동하는 것이다. 1000만 명 이상의 고객 정보를 보유하고 있는 기업이 많은 우리나라 현실에서 이러한 시스템은 경제 활동을 하는 모든 사람들의 정보를 사용자가 이름 하나만으로 조회할 수 있다는 문제점을 안고 있다. 국민 대다수의 개인정보를 간단하게 조회할 수 있어 사용자에 의한 개인정보 오남용 가능성이 크다.

이러한 경우 조회키로 입력되는 값을 변경하는 방법을 제안한다. 조회방법을 변경하는 문제는 기술적인 영향보다는 시스템을 사용하는 사람들에게 많은 영향을 미치고 업무 프로세스의 변경이 필요하기 때문에 시스템 사용자와 충분한 협의를 거쳐 선정해야 한다. 조회키의 변경은 기업 특성에 따라 다르겠지만 시스템 사용자가 임의로 추측하여 입력하기 힘든 값일수록 좋다. 고객을 식별하기 위해 기업이 임의로 만들어 사용하는 고객번호가 가장 좋으며, 불가피할 경우, 주민등록번호나 기타의 값을 사용할 수 있다.

고객정보를 취급하는 시스템 중에는 TM(Telemarketing), DM(Direct Mail) 등 대상자를 추출하고 이를 수행하는 경우가 있다. 〈그림 2〉와 같이 캠페인 담당자가 TM을 위해



[그림 2] 고객정보가 여러 경로를 거쳐 전달되는 경우

DW(Data Warehouse)에서 고객정보를 추출해 엑셀로 다운받아 이를 다시 TM 시스템 운영자에게 전달해주고 이를 TM 시스템에 입력하는 경우, 고객정보가 여러 경로를 거쳐 전달돼 유출 가능성이 커진다. 이런 때에는 TM 대상으로 추출된 고객정보는 관련자에게 다운로드 되지 않고 바로 TM 시스템으로 전송되어야 한다. 추출된 데이터의 정확성 여부는 얼마든지 화면상에서도 확인 가능하며 이는 개인정보보호 담당자가 캠페인 담당자를 설득하여 해당 프로세스 및 시스템을 변경시켜야 한다.

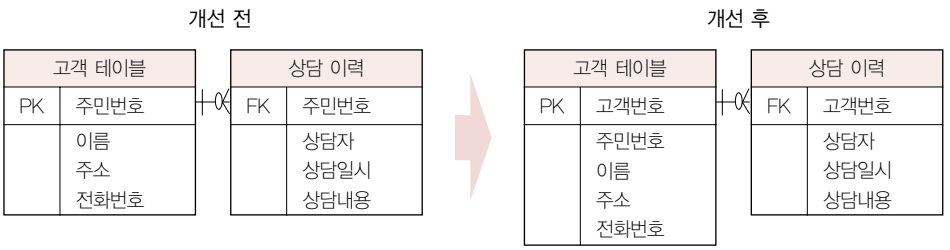
고객이 콜센터 등으로 전화를 걸어 일정한 요구를 할 때 본인확인을 위해 개인정보 등을 물어봐야 하는 경우가 있다. 이런 경우, 상담원이 임의로 고객의 모든 정보를 조회할 수 있어 개인정보 유출의 위험을 갖고 있다. 이같은 프로세스는 고객의 본인확인 답변은 IVR(Interactive Voice Response)을 통해 상담원을 거치지 않고 시스템에 전달되어 시스템이 본인 여부를 판단하게 한 후 상담원이 고객정보를 조회하고 업무처리를 할 수 있도록 변경되어야 한다.

시스템 개발과정에서 개인정보보호에 대한 충분한 고려가 없을 경우, 예전의 관습대로 무심코 모든 개인정보를 나열해 고객정보를 취급하는 시스템의 사용자 화면에 업무와 무관한 개인정보들이 노출되는 일이 발생한다. 시스템 관리자는 모든 화면에 대해 시스템을 사용하는 사용자와 불필요한 개인정보 노출이 있는지 검토하고 수정하여야 한다.

시스템 개발과정에서의 보안 강화

시스템을 운영하면서 발생하는 보안문제를 수정하기 위해 드는 비용은 개발과정에 미리 보안 요구사항을 반영하여 구현하는 것보다 20배 이상의 비용이 소요된다고 한다. 이 때문에 개발과정에서의 보안이 강조되고 있으며, 프로세스 개선도 개발과정에서 더불어 이루어진다면 금상첨화라 할 수 있다.

이외에도 개인정보 보호를 위해 기술적으로 고려해야 할 요소가 많이 있는데, 그 중 개인정보를 저장하고 있는 데이터베이스 관리 시스템(DBMS : Database Management System)은 고객정보를 그대로 갖고 있으므로 설계단계에서 중요하게 고려되어야 할 요소이다.



[그림 3] 고객 DB 시스템 개발에서의 보안

DBMS 설계시 가장 중요한 것은 개인식별 정보를 최소화해야 한다는 것이다. 〈그림 3〉은 개인을 식별할 수 있는 정보인 주민등록번호가 개인을 특정할 필요가 없는 상담 이력 테이블에 사용되는 경우의 개선책을 설명한 것이다. 주민등록번호 등 개인식별이 가능한 정보는 개선후 처럼 '고객번호' 라는 가공의 PK를 사용해 상담 이력 테이블에 개인을 식별할 수 있는 고객정보를 보유하지 않은 상태로 설계해야 한다.

주민등록번호는 유출시 큰 피해를 입을 수 있기 때문에 많은 기업에서도 이를 암호화하기 위한 노력을 하고 있으나 시스템의 성능문제를 동반하기 때문에 쉽지 않다. 주민등록번호 대신 주민등록번호가 포함하고 있는 생년월일, 성별을 별도의 컬럼으로 설계한다면, 암호화된 주민등록번호를 호출하는 횟수를 현저히 줄일 수 있어 성능문제를 크게 개선할 수 있다. DB 서버가 기존의 시스템과 직접적인 트러스트 관계를 맺고 직접 접속을 허용한다면 DB 서버로 접근할 수 있는 경로가 많아진다. 이럴 경우, 보안 취약점을 이용한 침투의 위험이 커지므로, 인터페이스를 단일화하고 규격화해야 한다.

고객정보를 취급하는 시스템의 개발 및 운영자가 고객정보 테이블에 대한 접근을 통제하는 것은 쉽지 않기 때문에 개발 및 운영자에게 테이블을 접근할 수 있는 권한을 부여한다. 그러나 DBMS에서 제공하는 View를 적절히 활용하면 고객정보를 보유하고 있는 테이블에 대한 접근을 차단하면서 효율적인 시스템 개발과 운영이 가능하다.

04

어울림정보기술㈜ 기술연구소 김형률 소장
whatisit@oullim.co.kr

네트워크 보안의 대세 통합보안관리(UTM)

보안시스템의 발달로 인해 보안솔루션이 다양해지면서 이를 관리 · 운용하는 인력과 비용의 증가가 수반되었다. 이에 따라 기업과 기관은 보안솔루션을 좀 더 효율적으로 운용할 수 있는 통합솔루션을 요구하게 되었다. 앞으로 보안시장은 통합보안이 주류를 이룰 것이며, 국내 솔루션도 세계시장에 선보인 해외 제품들을 뛰어 넘을 준비가 끝났다고 보인다.

보안시장의 태동기인 1990년대 말부터 여러 보안회사들은 네트워크 보안을 위해서 방화벽, 가상사설망(VPN), 침입탐지 시스템(IDS), 침입방지 시스템(IPS), 안티 바이러스, 안티 스팸, 메일 보안 및 웹 보안 등 다양한 보안솔루션들을 선보여 왔다. 이러한 보안솔루션들은 각 기업과 기관의 정보보호 시스템을 네트워크 상의 다양한 침해와 공격으로부터 보호해왔다.

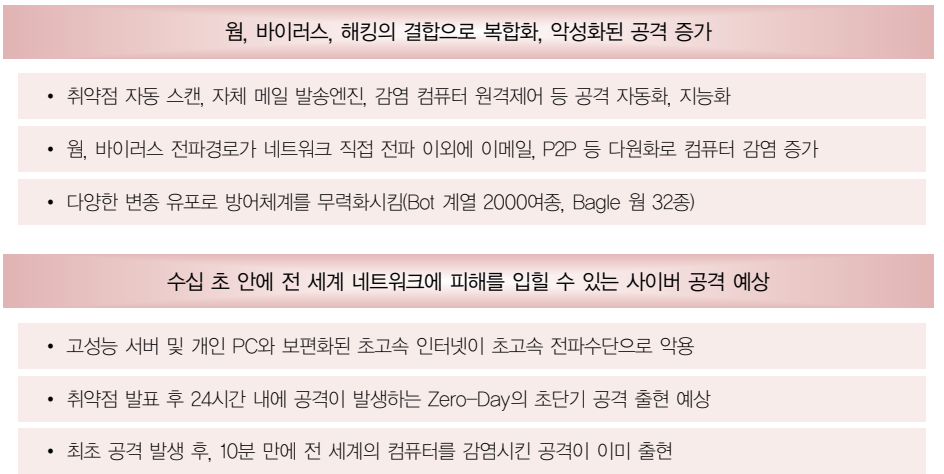
보안시스템들이 시간이 지나면서 다양한 솔루션으로 늘어나게 되었으며, 결국 〈그림 1〉과 같이 네트워크의 변화와 증가로 인해 운용해야 하는 보안시스템들의 양적 증가로 이어졌다. 이 때문에 운용 · 관리하는 업무가 증가되고, 보안관리 인력이 늘어나며, 더 많은 비용이 소요되었다. 많은 기업과 기관이 이 문제를 해결하고 더 효율적으로 운용할 수 있는 통합보안솔루션을 요구하게 되었다.

[그림 1] 보안솔루션의 증가 요인

기술적인 측면에서도 초기 보안시장은 세부적인 단위의 보안제품으로 분화하는 과정을 거치면서 다양한 보안솔루션이 출현되었다. 최근 몇 년간 출시된 보안솔루션은 통합 운영되었을 때 다양한 위협으로부터 종합적인 보호가 가능하다는 개념이 나오면서 통합 보안관리(UTM : Unified Threat Management) 솔루션이 등장하였다.

정보화의 역현상으로 발생된 공격기법들은 단순한 수작업으로부터 시작해서 대량이나 자동 반복을 목적으로 하는 자동화 도구 또는 대리자(Agent)를 활용하는 형태로 변화되어 왔다. 하나의 시스템을 탈취, 마비, 오동작시키는 방법에서 서비스 가용성 자체를 위협하는 유해한 트래픽의 폭증과 대리 또는 매개 시스템(Agent)을 통한 분산공격 형태로 변화되어 왔다. 최근에는 예전보다 더 광범위한 피해가 발생하고 있지만, 피해대상자를 미리 예측할 수 없다는 문제점이 높아졌다. 보안위협과 그로 인한 피해의 규모가 점차 증가하고 있으며, 이에 대한 예방과 상황 발생시 신속한 대응 및 조치가 최선의 방법으로 제기되었다.

2000년 이후의 보안 이슈에 대한 양상을 살펴보면 공격 패러다임의 변화로 인적인 노력과 시간 투입만으로는 문제를 해결할 수 없는 상태이다. 전 세계 네트워크가 연결되어 있는 상황에서 어디서나 이를 교란할 수 있는 사이버 공격이 가능하기 때문에 보다 강력한 보안방법이 필요하다.



[그림 2] 공격 패러다임의 변화

UTM 제품의 개념과 주요 기능

UTM 제품은 방화벽, IPSec 또는 SSL 가상사설망(VPN), 침입방지 시스템(IPS) 등의 주요 보안기능을 갖추고 있다. 컨텐츠 보안(Contents Filtering) 기능에 해당되는 안티 바이러스와 안티 스팸, 실시간 메신저 보안, P2P 보안기능 등이 포함되어 있으며, 최근 많은 관심을 받고 있는 웹 방화벽과 NAC 기능도 포함되어 안전한 정보시스템 운영을 위해서 보호해주는 범위의 확대가 지속적으로 늘어나고 있다. 이들을 관리하기 위한 사용자 관리 및 사용 환경관리, 보안정책 관리, 로그 관리 및 정보제공, 그리고 패치 관리 등의 관리기능이 포함되어 다양한 보안기능에 대해서도 일관성을 가지고 보다 편하게 관리할 수 있는 기능을 제시해주고 있다.

UTM 솔루션을 제공하는 국내외 벤더는 그 태생에 따라 몇 가지 유형으로 나뉜다. 방화벽 제품으로부터 출발하여 이 기능을 기반으로 다른 주요 보안기능들이 포함되면서 발전된 유형이 있고, IDS 제품으로 출발하여 다른 주요 보안기능들이 포함되면서 UTM으로 발전된 유형, 네트워크 장비로부터 출발하여 보안기능들이 추가되면서 UTM으로 진화된 유형이다.

방화벽이나 IDS 제품으로부터 출발한 UTM 솔루션은 기존의 보안전문회사들의 제품들로 처음부터 보안 기능성을 기반으로 발전되어온 제품이다. 성능을 기반으로 발전된 네트워크 장비 기반의 제품은 네트워크 장비회사의 제품으로 보안전문회사의 제품에 비해서 성능은 우월한 편이나, 보안 측면의 기능성은 덜 다양하다. 보안전문회사의 UTM 솔루션은 다양하고 강력하며, 기본에 충실한 보안 기능을 탑재하고 있는 반면, 네트워크 장비회사들의 UTM 솔루션은 보안기능의 다양성 측면 보다는 L2~L4 스위치 기능이 포함된 고성능 UTM 솔루션에 초점이 맞추어져 있다.

네트워크 장비의 보안시장 전이 추세에 따라 보안전문회사의 UTM 솔루션도 영향을 받아 이미 Load Balancing 기능이 내장된 제품이 제공되고 있다. 성능 측면에서도 고성능 플랫폼이 채택된 제품이 출시되고 있으며, 스위치와 같은 기능도 UTM 솔루션에서 지원하는 기능 중 하나가 되고 있어 네트워크 장비 기반의 UTM 장비가 제공하고 있는 특화된 우위 요소도 점차 반감되고 있다.

방화벽 기반의 UTM 솔루션을 제공하는 회사는 어울림정보기술, 시큐아이닷컴, 퓨쳐시스템즈가 있다. 전형적인 방화벽/VPN 전문회사들로, 여기에 다른 보안기능과 모듈이 추가 탑재되어 양질의 고기능 고성능 제품화를 추구한다. IDS/IPS 기반 UTM 솔루션을 제공하는 회사는 윈스테크넷, 포티넷이 있으며, IDS/IPS의 탐지능력에 초점을 두고 용이한 사용성 측면에서 다른 보안기능들을 추가 탑재하여 제공하는 측면의 제품이 출시되고 있다. 네트워크 장비 기반의 UTM 솔루션을 제공하는 회사는 삼성 네트웍스, 시스코시스템즈, 주니퍼 네트웍스 등이 있으며, 고성능 스위치 기반에 탑재되는 보안 모듈이 점차 다양화하고 있다.

OSI 7 계층별 차단기술

보안솔루션 동작의 가장 기본 원리는 네트워크를 사용하기 위해 정해진 OSI 7 계층별로 보안위협이 존재한다는 것이다. 이러한 위협으로부터 시스템을 안전하게 사용하기 위해 각 계층별로 이들을 차단하는 기술이 적용된다.

각 계층별 분석내용을 살펴보면, 주요 보안솔루션이 제공하는 기능에 따라 각각의 패킷들에 대하여 계층별로 Mac 주소, IP 주소, 포트 및 패킷 내용을 분석하여 해당 패킷이

구 분	차단기능	세부 내용
Layer 5~7	Contents Filtering 방식	7계층을 통해서 전달되는 모든 패킷을 분석해 유해한 텍스트/이미지/동영상 등을 필터링함
	Proxy 방식	프록시 서버에 원하는 사이트만 접속할 수 있는 방화벽 기능과 캐시 기능을 제공함
Layer 4	Port 차단방식	4계층에서 특정 포트를 차단하는 방식으로 P2P나 메신저, 웹하드 같은 경우 Well Known Port(1~1024) 이후의 TCP/UDP 포트를 사용하는데, 그에 해당되는 Port를 지정된 정책에 의거하여 차단함
Layer 3	URL 차단방식	네트워크에 Tapping, Capture된 패킷을 분석하여 사용자가 어떤 URL과 패킷을 사용하는지 파악한 후 연결을 허용하거나 차단(웹에서 유용)
	IP 차단방식	3계층에서 Capture된 패킷을 분석하여 접속하려는 IP가 유해 사이트인지 여부를 판단하여 차단함

[표 1] 보안솔루션의 OSI 7 계층별 차단기술

차단대상인지 아닌지 판별하고, 차단대상인 경우에 차단하도록 하는 방식으로 동작되고 있다.

주요 보안솔루션들은 Layer 3~7에 해당되는 내용에 따른 차단기능을 통해서 보안기능을 수행하고 있는데, Layer 3로 갈수록 단순한 처리만으로도 차단할 수 있어서 높은 성능을 유지할 수 있으며, Layer 7으로 갈수록 복잡한 판단에 의해서 차단처리를 하기 때문에 3계층 쪽에 의한 차단성능에 비해서 상대적으로 성능이 낮다.

UTM의 경우에는 Layer 3에서 7까지의 차단기능을 모두 포함하는 방향으로 발전해 왔기 때문에, 전체 계층을 대상으로 하는 다양한 기능을 복합적으로 사용할 경우 낮은 쪽 성능에 맞춰지게 되며, 이는 효율성 측면에서 성능 이슈를 발생시킬 수 있다. 다시말해 Layer 3~4에 해당되는 차단기능을 주로 사용하여 상대적으로 높은 성능을 내어주는 방화벽에 비해, Layer 5~7에 해당되는 차단기능을 주로 사용하는 VPN, IPS, Contents Filtering 기능들은 방화벽에 비해서 낮은 성능이 나오고 있으며, 이러한 성능 특성을 갖는 보안기능들이 하나의 어플라이언스에 탑재되어 한꺼번에 운용될 수도 있다. UTM에 대한 도입을 고려할 경우 기능뿐만 아니라 성능도 중요하게 고려해야 한다는 지적이다.

UTM의 성능

2004년 IDC에서 UTM은 통합적으로 위협을 관리하는 어플라이언스 제품으로 중소기업 시장에서 지속적인 인기를 끌 것이며, 특히 2007년이 되었을 때에는 모든 보안솔루션의 80%가 전용 어플라이언스 제품으로 공급될 것이라는 보고서를 내놓았다. 다수의 보안솔루션이 하나의 어플라이언스에 담겨져 있으며, 그 중 상대적으로 성능이 낮은 보안기능이 같이 탑재되면 그만큼 처리에 대한 부담이 따르고 그러다 보면 고속의 성능을 제공하는데 한계가 있을 것이라는 판단때문에 UTM이 중대형 시장보다 중소기업 시장에 적합할 것이라는 예측이다. 그러나 UTM 제품은 생각보다 더 빠르게 발전하였다. 국내 보안전문회사에서 발표되는 제품을 살펴보면, 2006년 말을 기점으로 UTM이 중소기업 시장만을 위한 제품이 아니라는 것을 입증하고 있다. 2004년에 미처 예측하지 못했던 고속의 성능을 자랑하는 UTM 제품이 등장하고 있으며, 2007년 상반기에는 거의 대다수의 국내 보안전문회사들이 3~5G 또는 10G급의 고성능 UTM 제품을 출시하거나 보유할 전망이다.

주목해야 할 점은 예전에는 ASIC 방식의 제품이 CPU 방식 보다 고성능과 저가격을 무기로 시장을 공략해 왔는데, 네트워크의 대용량화 추세에 따라 ASIC 방식의 제품만으로는 대용량화된 망을 보호할 수 없다는 점이다. 결국, 고성능 시장을 대비하여 NPU를 기반으로 하는 제품들이 주류를 이루게 될 것이다. 또한, NPU 자체가 고성능 네트워크 장비를 위한 용도로도 활용되고 있기 때문에 이를 채택한 플랫폼을 이용하는 UTM 솔루션은 고성능 네트워크 기능을 기본적으로 활용할 수 있다는 장점을 보유하게 된다. 그러나 NPU 기반의 제품은 국내에서 최근 몇 년간 개발된 제품이 있었으나 펌웨어의 기능과 최적화 여부가 까다로워 성공하지 못했다. 이들에 대한 기술력 확보가 결국 제품의 우위성을 달성하는 밑거름이 되고 있으며, 이를 확보한 벤더가 보다 더 우수한 제품을 선보이게 될 것으로 예상된다.

2004년부터 단독형 보안솔루션을 글로벌 시장에 출시해온 해외의 유명 벤더들 역시 UTM에 대한 준비를 해왔다. 2006년 중반 미국에서 진행된 NetWorld Interop 전시회에서도 방화벽, VPN, IPS 등 기존에 주류를 이루어왔던 단독형 주요 네트워크 보안솔루

구 분	특 징	장단점
Multi CPU	다수의 CPU로 병렬 처리하도록 구성	• 다수 CPU를 사용하기 때문에 중급 정도의 성능 제공 • CPU 사용 숫자 증가에 따라서 제품의 크기가 커지고, 일반적으로 양산된 마더보드를 사용할 수 없기 때문에 비용이 높은 편임
Multi Core CPU 적용	최신의 Multi core CPU를 적용함 현재 4 Core까지 가능	• 양산된 마더보드를 선택적으로 사용할 수 있기 때문에 Multi CPU 방식의 경우보다 비용이 저렴하고, 단일 CPU 보다 높은 성능이 가능함 • NPU에 비해 고성능을 낼 수 없음
ASIC 적용	전용 ASIC을 통해서 CPU에 비해 상대적으로 처리가 빠르도록 구성	• CPU 보다 빠르기는 하나 NPU에 비해서 성능이 떨어짐 • 양산시 가격이 낮음 • CPU 기반의 제품보다 몇 배의 고성능이 가능함
NPU 적용	CPU에 비해 상대적으로 처리가 빠른 Network Processor로 처리하도록 구성 현재 16 Core까지 가능	• 시스템 하드웨어 자체를 직접 설계 · 생산해야 하고, NPU 관련 Firmware 개발이 수반되기 때문에 CPU 기반으로 개발하는 경우보다 어렵고, 개발 지연 또는 실패 가능성도 존재함

※향후 CPU 기반 제품의 경에는 Multi Core, Multi CPU 혼합 방식으로 발전할 것으로 예상됨

[표 2] UTM 성능 한계를 극복하기 위한 기술

션들 대신 UTM 제품과 NPU를 기반으로 하는 고성능 제품들, 최신 제품으로는 웹 방화벽과 NAC 제품 등 특화된 보안장비들이 선보였다. 이는 향후 이러한 유형의 제품들이 시장을 주도할 것이라는 것을 시사한다. 주니퍼 네트웍스나 시스코 시스템즈와 같은 세계적인 장비 벤더 역시 방화벽 모듈을 탑재한 장비들을 선보여 기존 네트워크 장비들 역시 UTM 영역으로 넘어오고 있음을 보여주었다. 이 때문에 2006년을 기점으로 전 세계적으로 단독형 보안제품은 퇴조하고, UTM으로 대체하고 있는 것으로 전망되고 있다. 국내에서는 이미 NPU를 탑재한 고성능 플랫폼에 기존 UTM 기능 외에 웹 방화벽과 NAC 기능이 탑재된 일체형 제품들이 준비되고 있어 이제는 국내 솔루션도 세계시장에 선보인 해외 제품들을 뛰어 넘을 준비가 끝났다고 보인다.

UTM의 활용성 제고

네트워크가 고속화 되고, IPv6 체계가 도입되면서 기존 네트워크 환경에는 많은 변화가 일어날 것이다. 이에 따라 기업들은 기존에 도입되어 운영하고 있는 많은 보안솔루션을 향후 몇 년에 걸쳐서 대대적으로 교체하거나 신규 도입할 것으로 예상된다. 최근 몇 년간 UTM 솔루션들은 진화를 거듭하며, 진화과정은 네트워크 환경변화에 맞추고 있다.

앞으로 보안솔루션의 대체 또는 신규 도입을 고려할 경우, 대다수의 보안시스템 운영자들은 그 기능성과 관리 편리성, 비용과 관리노력의 절감 측면에서 단독형 보안제품 보다는 UTM을 선택할 가능성이 높다. 이를 효과적으로 선택하기 위해서는 단순히 기능만을 고려하거나 성능만을 봐서는 안된다. 모든 요소에 대해 경쟁력 있는 최적의 조합으로 이루어진 솔루션을 선택해야 한다.

UTM 솔루션은 센터급의 대규모 제품으로부터 내부 네트워크 보호를 위한 소규모 제품까지 그 선택의 폭이 넓어지고 있기 때문에, 어떤 기능을 주로 사용할 것이며 어떤 영역까지 보호하게 될지, 그에 대한 보안정책을 잘 수립하고 각 제품들을 요소에 잘 배치하여 보다 높은 보안 효율성을 얻을 수 있도록 고려해야 한다.

중요한 것은 보다 좋은 UTM 솔루션을 선택하는 지혜도 필요하지만, 이를 효과적으로 운용하기 위한 보안관리 정책에 대한 고려와 관리체계, 숙련된 인력, 그리고 최적의 투자 등이 수반되어야 100%에 가까운 보안이 가능하다. 만일, 하나라도 간과할 경우에는 아무리 좋은 솔루션을 도입하여 운용하더라도 보안성의 효과를 얻기 힘들 수 있다는 점을 인식해야 한다.

05

한국코카콜라보틀링 보안 · 부정행위 담당 이진규 과장
jin.kyu.lee@kor.ccamatil.com

보안투자로 얻을 수 있는 산술적 이익, ROSI

일반적으로 규모가 작은 기업에서는 보안활동이 미비하거나 보안업무에 대한 전문적 지식이 없는 인사담당자가 그 임무를 겸임하면서 보안 리스크가 발생하는 경우가 많다. 그러나 많은 기업들이 이를 인식하면서도 보안업무를 전담할 수 있는 보안담당자를 고용하고 별도의 자원을 투입하지 못하고 있다. 여기에는 보안업무가 투자이익을 남기지 못한다는 인식이 자리잡고 있다.

'회사'는 그 본질상 필연적으로 '이익'을 추구하고 발생시켜야 그 존재가치를 인정받는 조직이기 때문에 회사규모나 수익구조 등의 이유로 '돈이 되지 않는' 보안활동에 회사의 자원을 투입할 이유를 찾지 못하는 것이다. 또한, 보안업무가 회사의 주요 업무로 확고히 자리를 잡고 있다 하더라도 경기가 불황일 때에나 전략적 이유로 회사가 감원을 고려할 때에 제1순위로 항상 보안부서가 꼽히는 이유도 여기에 있다.

일례로, 기능이 기존제품에 비해 향상된 생산설비를 구매해 동일한 작업시간에 생산량이 기존대비 10%가 향상되는 경우 이로 인한 매출 및 이익증가는 쉽게 계산이 가능하다. 그렇기에 쉽게 수치화된 자료를 제시함으로써 투자를 위한 근거로 삼을 수 있는 것이다. 그러나 보안에 대한 투자문제는 이와 사뭇 다르다. 가령 정보보호 수준 향상을 위해 새로운 패치 시스템을 도입할 필요가 있을 경우, CEO는 CIO 또는 CSO에게 다음과 같은

질문을 하게 된다. "새로운 패치 프로그램을 도입해 시스템이 안정되고, 바이러스에 걸릴 가능성이 줄어들며, 직원들의 임의적인 소프트웨어 사용이 제한되는 것이 과연 얼마만큼의 이익이 있는지 '수치화' 할 수 있는가?"

이러한 CEO의 질문에는 아래와 같은 원인이 밑바탕에 있다.

- 회사의 주가는 점차 엄격한 감시체계 하에 놓이게 된다.
- 회사이익의 증가에 대한 요구가 점차 거세지고 있다.
- 업무책임이 '회사' 에서 '개인' 에게로 이양되고 있다.
- 규모가 크지 않은 회사의 경우, 보안활동에 투자할 인력 및 자산을 확보하기 어렵다.
- 자동화된 보안설비에 대한 맹신이 커져가고 있다.

이와 같은 CEO의 질문은 보안부서(정보보안 및 물리적 보안부서 공통으로)가 자원에 대한 투자를 회사에 요구할 때마다 항상 부딪히게 되는 난관이며, 회사 정책결정자의 보안에 대한 인식이 얼마나 이진법적인 상태로 정체되어 있는지 알 수 있는 한 예가 된다. 다시 말해 '평소 보안 리스크에 대해 미리 대비할 필요가 없다(0)거나 위협이 발생했을 경우에 대처하면 된다(1)' 는 0 아니면 1이라는 식이다.

보안투자로 얻을 수 있는 산술적 이익 산출방법

위와 같은 이유로 보안담당자 및 학계 교수와 관련분야 연구원들을 중심으로 '보안활동에 대한 투자로 얻을 수 있는 산술적 이익(ROSI : Return on Security Investment)에 대해 1990년대 중 · 후반부터 연구를 지속해오고 있으며, 현재는 기존의 투자수익률(ROI : Return on Investment)의 하위개념을 벗어나 Cost Of Investment vs Survivability에 대한 매핑(Mapping) 작업에 이은 투자 최적점 찾기에 이르기까지 활발히 연구가 진행되고 있다.

일반적으로 투자한 자산에 대한 이익을 산출하는 방식을 ROI라 하는데, 투자한 자산에 대한 이득의 비율, 즉 ROI = Return or Profit/Capital Invested or Cost로 정의한다. 그렇기에 일정한 기간 중에 ROI를 높이기 위해서는 ①비용이나 투자를 최소화하거나 ②이익을 최대화하거나 ③Return이 발생하는 시간을 최소화하면 된다. ROI는 투자결정의 신뢰성과 프로젝트의 경제성을 증명하는 효과적인 도구로써, NPV, IRR, PP 등

과 같은 순 유형효과(Net Tangible Benefits)의 핵심지표 가운데 하나로 명쾌하게 이해되기 때문에 매우 많이 사용되는 개념이다.

CEO의 입장에서 보안활동에 대한 투자를 고려할 때에 수치화된 Return을 생각해 내기란 쉬운 일이 아니다. 무인경비에 대한 설비투자 및 인적자원 고용, 그리고 사이버 공간에서의 끊임없는 침입을 막기 위한 방화벽 설치에 드는 시스템 구축비용 등 'Return이 보이지 않는 곳' 인 경우 발등에 불이 떨어지지 않는 이상 산더미처럼 쌓여있는 각종 투자기회를 마다하고, 보안부문에 투자하고 싶어하는 CEO는 없다 해도 과언은 아닐 것이다. 그렇기에 ROI와 같이 명쾌하게 투자에 대한 이익을 수치화해 보여줄 수 있다면 보안활동에 대한 더 많은 투자를 유치함으로써 보안수준의 극적인 향상을 이루어내는 것이 가능하기에 보안담당자들은 보안투자에 대한 이익을 명확한 수치로 보여주고자 노력하고 있으며, 이로 인해 ROSI의 개념이 더욱 중요해지고 있는 것이다.

ROSI를 산출하는 방식

ROSI는 산출하는 방식이 연구를 담당하는 주체마다 다소 차이가 있지만, ROI와 유사한 방식으로 ROSI = (Reduction in Risk Exposure)/(Investment in Countermeasures) [ROSI = 위험에의 노출 경감/대응방안에 대한 투자]로 정의하는 것이 일반적이다. Risk Exposure는 Risk Avoidance(위험 회피)와 Risk Mitigation(위험 경감)의 두 가지 개념의 결합으로 이해되며, 전자는 사건발생의 가능성을 경감시키는 것이며, 후자는 기왕에 발생한 사건의 영향을 경감하는 것이다. 이를 공식으로 설명하면 다음과 같다.

Risk Avoidance means Min : f(x) = P(Occurrence)
Risk Mitigation means Min : f(y) = Consequence of Occurrence
Risk Exposure = f(x) · f(y)

ROI와 마찬가지로 ROSI를 증가시키는 방법으로는 ①운영손실(Operational Losses) 최소화 ②투자 최소화 ③ROI를 적용 가능한 분야에는 Positive Return을 최대

화 ④Return 발생시기를 가속하는 등의 방법이 있다.

그러나 이러한 ROSI의 개념설명에 있어 가장 큰 문제점으로 대두되는 것은 ①Risk로 인해 잃게 될 가치를 수치화 하는 것과 ②손실의 가능성을 수치화하는 것이다. 이러한 것을 수치화하기 위해서는 기존 기업들에서 어떠한 보안위기가 있었으며, 이로 인한 손실액은 어느 정도가 되는지 체계적으로 정리된 자료를 확보해 이를 데이터베이스화하고, 이렇게 구축된 DB에서 각종 변수들 간의 상관관계를 확인하는 작업을 수행해야 하기 때문에 기업들의 협조가 필수적이라 할 수 있다.

그러나 기업 이미지 실추와 이에 따른 주가하락 등에 대한 우려때문에 이러한 작업에 적극 협조할 필요성을 느끼지 못하는 기업이 대부분이므로 실증이 어렵다는 문제가 꾸준히 제기되고 있다(그러나 모든 ROSI가 명확하지 않은 것은 아니다. 때로 ROSI가 명확한 경우도 있다. 이를테면 회사 리스크에 대한 보험(Corporate Insurance)의 경우, 비용(Cost)이 발생하는 것을 예방 · 보전하는 방식으로 직접적인 Return이 발생하기도 한다).

Idaho University의 연구

이러한 단점을 해소하고자 여러 연구기관에서 실험을 통한 시뮬레이션을 이용해 이를 실증적인 데이터로 삼고자 하는 시도가 있었는데, 대표적으로 Idaho 대학에서 개발한 ROSI 공식1)을 살펴보면 다음과 같다.

(R-E) + T = ALE(Annual Loss Expectancy)

T : 침입감지 툴(The cost of intrusion detection tool)

E : 침입감지 툴로 인해 침입을 예방함으로써 얻어진 이익금액(The dollar savings gained by stopping any number of intrusions through the introduction of an intrusion detection tool)

R : 침입으로부터 회복하는 데 발생하는 비용(The cost per year to recover from any number of intrusions)

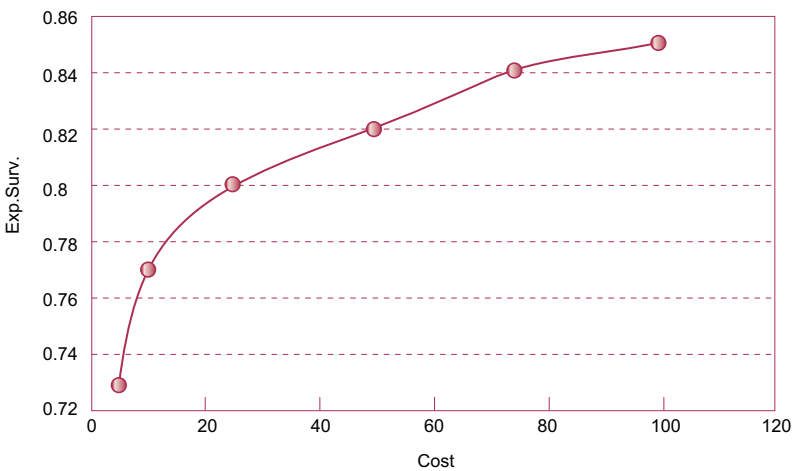
R-(ALE) = ROSI

Idaho 대학에서는 위와 같은 모델을 증명하기 위해 침입감지 시스템(Hummer로 명명)을 구축하고, 실제 종종 행해지는 각종 침입방식을 이용해 실험에서 사용된 방식으로 발생하는 비용이 가설에서 설정한 비용과 일치하는지를 확인했고, 그 결과 성공을 거두었다. 그 실험결과의 예를 들면 4만 달러의 가격이 나가며, 85% 정도 침입감지 효과가 있던 시스템이 10만 달러의 보안위험에 기인한 손해가 예상되는 네트워크에서 4만5000 달러의 순 ROI를 발생시켰던 것이다.

그러나 Idaho 대학의 이러한 노력에도 다음과 같은 비판이 따랐다. ①실제 이론을 뒷받침할만한 데이터 부재 ②이론을 뒷받침하기 위한 추정(Assumption)이 너무 많았다. 이를테면 투자와 더불어 위험상황이 단순감소(Monotonically decreasing) 한다든지 위험상황은 투자에 대한 수확 체감의 법칙을 따른다던지 또는 ROSI는 투자가 존재하는 모든 범위에서 항상 양의 값을 가진다는 등의 추정이 바로 그것이다.

CMU & CERT의 실증적 증명

이에 MIT와 더불어 세계 컴퓨터 공학을 이끌어가고 있는 카네기멜론 대학(Carnegie Mellon University)에서는 CERT(Computer Emergency Response Team : 컴퓨터 해



[그림 1] ROSI의 수확체감의 법칙

킹사고가 빈발함에 따라 컴퓨터 통신망을 해커로부터 보호하기 위해 결성된 정보보안 전문가 그룹, 국내에도 CERT가 존재하며 미국의 경우 CMU에 의해 운영됨)와 연합해 'A Simulation Model for Managing Survivability of Networked Information Systems(네트워크 시스템의 생존성에 대한 시뮬레이션 모델)' 이라는 보고서를 내놓았다. 이 연구보고서의 가장 중요한 점은 실제 데이터를 이용해 보안에의 투자 이유를 설명한 것도 있지만, Idaho 대학 연구에서 비판받았던 이론의 추정 가운데 하나인 ROSI의 수확체감의 법칙을 아래 그래프와 같이 보여주었다는 데 있다.

위 그래프가 시사하는 또 한 가지 가능성은 경제학에 있어 수요/공급 그래프와 마찬가지로 기업의 투자가능성에 대한 그래프도 매핑 작업이 가능하다면 보안 투자의 최적점을 찾을 수 있어 얼마만큼 투자해야 어느 정도의 보안수준(Expected Survivability)을 유지할 수 있는가를 예측할 수 있다는 점이다.

[그림 2] 보안투자에 대한 개념을 실제 데이터화 하는 논리 〈FIST Conference Oct. 2003〉

이상으로 ROSI의 개념 및 각 모델의 장단점에 대해 알아봤다. ROSI라는 개념이 아직까지는 ROI처럼 확고하게 투자의 Index로 자리잡았다고 할 수는 없지만, 보안전문가들이 보안활동에 대한 투자의 Selling Point로 삼을 수 있을 정도로 발전해왔으며, 앞으로 데이터베이스가 축적돼 실질적인 데이터에 기인한 공식과 데이터가 확보된다면 기업들의 보안에 대한 충분한 투자를 이끌어낼 수 있으리라 생각한다.

이제는 단순히 보안에 투자하면 안전하다는 식의 이진법적 사고로는 더 이상 보안에 대한 투자를 이끌어내기 힘들다. 위에서 언급한 대로 CEO라는 기업의 정책결정권자는 단순히 투입대비 산출비율뿐 아니라 주주를 설득하고, 산업에서의 파이를 키워가며, 개인에게 이양되는 책임에 대한 관리부담까지 떠안아야 하기 때문이다.

06

BAT코리아 Security Record Management 이은희 과장
annie_lee@bat.com

기록물 관리, 회사의 막대한 손해도 막는다

문서는 회사 비즈니스에 꼭 필요한 정보이기 때문에 관리가 제대로 되지 않으면 자원의 비효율적인 사용에서부터 회사에 막대한 손실을 초래하는 원인이 될 수도 있다. 체계적인 기록물 관리를 위해서는 관리목적에 적합한 정책수립과 연중계획 수립, 업무담당자 교육과 상시업무 지원, 정기적인 점검, 경영진의 중요성 인식과 강조가 지속적으로 요구된다.

'구슬이 서 말이라도 꿰어야 보배' 라는 말은 회사의 문서관리에도 해당되는 격언이다. 매일 회사에 있는 상당 시간을 책상에 앉아 문서작업을 한다. 회사 비즈니스에 꼭 필요하다고 생각하는 정보를 생성해내지만 제대로 관리가 되지 않는다면? 적게는 자원의 비효율적 사용에서부터 크게는 회사에 막대한 손실을 초래하는 원인이 될 수 있다. 몇 가지 극단적인 경우를 통해서 Best Practice를 도출해내고자 한다.

Worst Practice 1

나문서 라는 사람은 열심히 작업한 결과물을 'My document' 에 보관하고, 출력물은 파일링 해 본인의 책상서랍에 넣어두고 필요할 때마다 꺼내 보곤 한다. 5년 동안 A사에서 일을 한 후 B회사로 급하게 이직하게 돼 인수인계를 제대로 해주지 못한 채 거의 몸만

빠져 나오다시피 했다. 나문서 씨의 후임으로 온 나몰라 씨는 책상서랍에 가득 들어있는 전임자의 서류들을 보고 뭔가 중요한 것일 듯 해 버리지는 못하고 상자에 넣어 외부창고로 보내기로 한다. 'My document' 에 쌓여 있는 문서들은 하나하나 열어 보는데 석 달은 걸릴 것 같아서 아예 손도 못 대고 있다. 오늘 나몰라 씨는 나문서 씨가 만들었던 비슷한 문서들을 만드느라 바쁘다.

Worst Practice 2

전반기 영업실적이 좋아서 주가가 상한가를 달리던 A사는 전반기 영업 순익의 절반을 떼어갈 수도 있는 소송에 휘말리게 됐다. 그런데 10년 전에 작성됐던 증거문서만 있으면 소송에서 이길 수 있는 상황이다. 10년 동안 회사는 이전도 했고 담당 업무를 했던 사람들도 여러 번 바뀌었다. 더군다나 회사를 이전하면서 2년 이상 된 문서는 모두 상자에 넣어 외부창고로 보내고 왔다. 그러나 10년 전 문서를 반드시 찾아야만 한다.

Worst Practice 3

못버려 씨는 10년 동안 한 회사에서 일했다. 그는 일단 한번 파일링 한 문서를 절대로 버리지 않는다. 언제 어떤 일 때문에 필요할지 모를 일 아닌가? 그래서 그의 Mail Box도 10GB가 넘는다. 파일도 이제 더 이상 보관할 장소가 없어서 오늘 총무과에 새로운 캐비닛을 신청했지만 사무실에 놓을 장소도 마땅치 않아 고민이다.

위와 같은 경우는 주변에서 쉽게 찾아 볼 수 있다. 하지만 앞선 사례는 효율적 Records Management(기록물 관리)의 개념과 목적만 정확하게 알고 있다고 해도 피할 수 있는 경우이기도 하다. 그렇다면 Records Management란 무엇이고, 왜, 그리고 어떻게 Records Management를 해야 하는가? Records Management란 조직에서 영업활동을 하는 동안 생성하거나 받은 Records의 생성, 복사, 유포, 파일링, 회수, 보관, 폐기를 관리하는 시스템이다. Records는 장소나 물리적인 형태에 관계없이 영업활동을 하는 과정에서 생성하거나 받은 자료로 종이문서나 전자문서뿐만 아니라 CD, 오디오, 비디오, 테이프, 녹취자료, 사진, 책, 지도 및 기타 형태의 자료도 모두 포함한다. 모든 비즈니스 목적으로 생성되어 보관하고 있는 Records의 소유권은 회사가 가지고 있다.

"Who owns the records?"

"Who owns the records?"

매달 있는 교육 시작에 앞서 항상 묻는 질문이다. 놀랍게도 절반 이상의 직원들이 명쾌하게 답을 못하거나 아니면 'Records를 만든 사람' 이라고 대답한다. 소유권의 문제가 확실해지면 회사문서의 생성부터 폐기까지 어떻게 관리해야 하는지에 대한 답이 명확해진다. 만약에 회사 Records의 소유권에 대한 인식이 정확하지 않다면 회사의 문서는 제대로 관리되지 않은 채 위와 같은 Worst Practice만 반복될 것이다. Records는 생성자가 누구인가를 떠나서 가치를 돈으로 환산할 수 없는 회사의 자산이므로 그에 맞게 관리돼야 하고 보호돼야 한다. Records는 가치있는 정보이며 중요한 영업자산으로서 법, 세금, 감사의 의무를 이행하기 위한 회사정책 및 정당한 영업활동에 대한 증거로 필요하며, 영업활동 관리를 위해서 필수적이다.

회사는 Records를 통해

- 영업활동을 효율적이고, 투명하고, 바르게 할 수 있다.
- 일관되고, 정당한 서비스를 제공할 수 있다.
- 인사이동 및 퇴직시 관리 및 행정의 지속성과 생산성을 유지할 수 있다.
- 영업활동의 효율성을 제고할 수 있다.
- 기록 및 감사활동을 포함한 법적 · 규율적 의무를 준수한다.
- 영업활동의 증거부족이나 증거발견과 관련된 위험을 관리해 소송시 최대한 보호받을 수 있다.
- 조직의 이해와 직원, 고객, 현재 및 미래의 주주들의 권리를 최대한 보호할 수 있다.
- 현재와 미래의 연구개발 활동 및 성과뿐만 아니라 역사적인 연구에 대해서 문서화할 수 있다.
- 회사의 정체성을 확립하고, 역사적 기록을 보존할 수 있다.

성공적인 Records Management는 사람들의 습관을 바꾸는 것이기 때문에 끊임없는 트레이닝과 전사적인 노력이 중요하다. 체계적인 Records Management를 위해서는

- 관리목적에 적합한 정책(Policy) 수립

- 정책에 따른 연중계획 수립 및 시행
- 업무담당자 임명, 교육 및 상시업무 지원
- 직원의식 고취
- 정기적인 점검
- 경영진의 중요성 인식 및 강조가 지속적으로 요구된다.

또한, 아무리 완벽한 정책과 시스템을 갖추고 있다고 할지라도 사람들을 움직이기 위해서는 단순화, 훈련, 강화가 절실히 요구된다.

- 단순화 : 필요한 정책이라 해도 복잡하면 아무도 따라할 엄두를 내지 못할 것이다. 관리의 효율성을 위해서는 명확하고 간결한 지침이 필요하다.
- 훈련 : 하고 싶어도 무엇을 어떻게 해야 하는지 알 수 없다면 아무리 외쳐도 메아리 없는 공허한 울림이 될 것이다. 계속되는 직원의 이동과 새로운 직원들을 대상으로 정규적으로 Training을 운영하는 것 또한 중요한 요소이다.
- 강화 : 실제 정책대로 시행되고 있는지 훈련받은 대로 하루 업무에서 이루어지고 있는지를 확인하고 명확한 지침을 주는 것은 업무담당자로서 대단한 인내와 추진력이 요구되지만 결코 간과할 수 없는 부분이다.

이런 노력들을 통해서 효율적으로 관리가 된다면, 나문서 씨가 5년 동안 만들었던 귀중한 자료들은 외부창고에서 썩어가는 대신 나몰라 씨가 유용하게 사용할 수 있을 것이고, 소송에 휘말린 A사는 10년 전 자료 덕분에 위기에서 벗어날 수 있을 것이다.

07

이네트렉스 기술지원팀 최성훈 과장
hope@enetrex.com

컴퓨터를 안전하게 잘(?) 버리는 다섯가지 방법

정보보호를 중시하면서도 우리가 일상적으로 간과하는 부분은 컴퓨터를 아무 조치없이 폐기처분한다는 것이다. 컴퓨터에는 각종 중요한 정보들이 저장되어 있는데, 이를 삭제하지 않고 폐기해 심각한 피해를 입게 되는 경우를 찾아볼 수 있다. 그러므로 컴퓨터를 안전하게 잘(?) 버리는 다섯가지 방법을 알아보자.

이제 우리 일상은 컴퓨터 없이 단 하루도 살 수 없는 시대가 되어버렸다. 그것이 회사든 가정이든 말이다. 하지만 여기에서 우리가 한가지 잊고 있는 것이 있다. 컴퓨터가 중요해지면서 그 안에는 각종 중요한 정보들이 저장되고 있다. 그리고 더욱 중요한 것은 우리는 그런 컴퓨터를 아무런 조치없이 폐기처분하고 있다는 점이다.

컴퓨터의 본체에 저장되어 있는 개인정보나 기업의 중요정보를 삭제하지 않고 폐기함으로 인한 심각한 피해들이 속출하고 있다. '개인정보 유출실태 보고서'에 의하면 조사대상의 30%에 이르는 중고 하드디스크에서 총 1349명분의 개인정보가 발견된 것으로 나타났고, 보험회사에서 중고로 매각한 컴퓨터에서는 수백 개에 달하는 개인정보가 발견됐으며, 버려진 컴퓨터에서 얻은 760명의 개인정보(신용카드번호)를 이용해 거액을 챙긴 범인이 경찰에 체포되는 등 지속적인 피해가 발생하고 있다.

현재 개인정보 및 기업의 정보유출로 인한 피해는 갈수록 늘어나고 있다. 하지만 이렇듯 막대한 피해에 비해 개인이나 기업의 정보유출에 대한 관심과 투자는 미비하다고 볼 수 있다. 이제 보안체계의 중요한 타깃은 외부에서 내부로의 침입을 방지하는 것뿐만 아니라 내부자에 의한 정보유출과 기업이나 개인의 폐기되는 PC를 통한 정보를 차단하는데 초점이 맞추어져야 한다. 실제로 이에 따른 관련 보안제품의 수요도 늘어나고 있다. 이러한 보안제품을 설치했을 경우, 기업의 중요정보 유출을 직접적으로 방지할 수 있기 때문에 정보유출로 인한 막대한 피해를 사전에 예방할 수 있다.

한가지 예로 은행이나 증권사 등에서의 정보유출로 인한 피해가 점차 증가하고 있는 것은 어제 오늘만의 이야기가 아니다. 또한, 기업에서 매각이나 기증형식으로 처리되는 컴퓨터에서 정보를 빼내 악용하는 사례들도 점차 증가하고 있다. 이러한 문제점 때문에 콘텐츠 차단이나 모니터링 저장매체를 삭제하는 제품의 수요가 늘어나고 있으며, DB 보안도 점차 강화되는 추세다.

다섯가지 폐기방식

가정이나 기업에서 버려지고, 폐기되는 컴퓨터 본체를 정보유출 없이 손쉽게 폐기할 수 있는 방법은 없을까? 기존의 폐기방법은 개인의 경우 중고 컴퓨터를 전문적으로 매입하거나 회수하는 업체들에 대부분 의존하고 있으며, 기업의 경우 사내 사원들에게 저렴한 가격으로 매각하는 방식이나 복지기관 등에 기증 또는 완전 폐기 등에 의한 방법으로 처리되고 있다. 하지만 이런 방법들은 폐기나 기증하는 컴퓨터 본체내의 HDD 정보를 어떠한 방식으로 처리했느냐에 따라 정보유출의 가능성이 제기될 수 있다. 만일, 폐기나 기증되는 본체의 HDD 정보를 아무런 조치없이 처리했을 경우 사용하던 HDD의 내용에 따라 막대한 정보유출 피해를 입을 수 있기 때문이다.

이에 기업이나 공공기관에 최대한 적합한 방법으로 정보유출로 인한 피해를 최소화하는데 도움이 될 수 있는 다섯가지 방법을 제시한다.

1. Overwriting(겹쳐 쓰기) 방식

S/W를 이용해 폐기될 HDD 내에 데이터를 겹쳐 쓰게 해 원래의 데이터를 찾을 수 없

게 한다. 저장매체에 대해 난수나 0, 1로 겹쳐 쓰는 방식으로, 클라이언트의 수가 작을 경우 처리비용이 저렴하고, 재활용이 가능하며, 일반 복구 S/W로는 데이터 복구가 불가능하다는 장점이 있다. 그러나 보안규정상 최소 3회 이상을 반복해야 해 작업시간이 길어진다. 그리고 HDD 자체 불량이나 Bad Sector, OS 상의 제약을 받는다.

2. Low Level Format 방식

각 HDD 제조업체에서 제공하는 S/W를 이용해 데이터를 삭제하는 방식이다. 그러나 Format 후 급격한 성능저하와 HDD 고장시 사용이 불가능하고 Overwriting 방식과 동일하게 시간이 오래 걸려, 최근에는 겹쳐쓰기 프로그램으로 대체하고 있다.

3. 파기방식

망치 등을 이용해 물리적인 힘으로 분쇄해 HDD의 원형이 불가능하게 파기하는 방식이다. 작업자가 HDD 파기시 위험에 노출되며, 완전하게 파기되지 않은 조각에 대해 복구가 가능하다는 단점이 있다.

4. 소각방식

HDD를 소각하거나 용광로에서 소각하는 방식이며, 소각시 발생하는 유해물질로 인해 해외에서는 환경청에서 승인된 소각로에서만 소각하도록 승인돼 있다. 국내에서는 몇몇 공공기관과 군부대에서만 시행되고 있을 정도로 시행하기가 까다롭다.

5. 소자(Degaussing) 방식

자력을 이용해 HDD내 영구모터의 자력소거와 미디어에 보자력을 상쇄시켜주는 방식으로, 초기 투자비용이 많이 들지만 OS나 소프트웨어적으로 처리가 불가능한(HDD Bad sector, 인식불능 HDD) 방법도 처리가 가능하며, 짧은 시간에 대량의 HDD를 폐기할 수 있다.

기업이나 공공기관은 이와 같은 방식으로 HDD를 폐기해야만 내부의 중요 정보유출을 방지하고 피해를 최소화할 수 있다. 실정에 맞는 방법을 잘 선택해 재활용을 하고자

저장자료 / 저장매체	공개자료	중요자료	비밀자료(대외비)
플로피 디스크	A	A	A
광디스크(CD/DVD)	A	A	A
하드 디스크(HDD)	C	A, B 중 선택	A, B 중 선택
자기 테이프	A, B 중 선택	A, B 중 선택	A

A : 소각, 파쇄, 용해　B : 전용장비(소자장비) 이용 저장자료 삭제
C : 완전 Format 3회 실행(난수나 0, 1 로 저장)　D : 완전 Format 1회 실행(난수로 저장)

[표 1] 중요 정보(주민번호, 금융정보, 회계자료, 대외비) 저장매체별 삭제방법

할 때는 Overwriting 방법으로 데이터를 삭제한 후에 매각이나 기증해야만 되며, 완전 폐기를 위해서는 파기, 소각, 소자방식을 이용해야만 한다. 하지만 소각 및 파기는 위험부담이 많고 처리하기도 까다롭기 때문에 초기 투자비용이 요구되더라도 소자방식이 제일 안전한 방법이라 할 수 있다. 더불어 소자방식은 백업용 테이프 등의 재사용이 가능하다. 최근 들어서는 백업 테이프, CD, DVD 매체에 대한 폐기의 중요성도 부각되고 있기 때문에 중요 정보에 따라서는 소자방식 처리 후, 파기(분쇄)의 방법을 병행하는 것도 좋다.

08

Magnus Ahlberg Managing Director, Pointsec Mobile Technologies
magnus.ahlberg@pointsec.com

위험천만한(?) 이동식 저장매체, 손쉬운 대처방법 다섯가지

이동식 저장매체가 인기를 얻게 되면서 보안상의 문제점과 위험도도 증가하고 있다. USB를 분실하거나 악의적인 직원에 의해 유실되면, 회사정보와 개인의 신상정보가 모두 빠져나갈 수 있다. USB 등 이동식 저장매체를 안전하기 사용하기 위해 회사는 보안정책을 사용하며, 직원대상의 교육을 실시하고 감사와 대응책을 마련해야 한다.

이동식 저장매체는 사용상의 편리함과 저렴한 가격으로 인해 어디에서든 쉽게 찾아볼 수 있는 장비가 됐다. 그로 인해 이동식 저장매체는 그 사용량이 갈수록 늘어날 것으로 보인다. 하지만 이렇듯 편리한 이동식 저장매체가 엄청난 위험성을 갖고 있다는 것을 많은 사람들은 인식하지 못하고 있는 듯 보인다. 여기서는 이동매체의 장단점과 이와 관련된 보안상의 위험을 감소시키기 위해 보안 및 IT 관리자들이 취할 수 있는 조치에 대해 생각해 보기로 한다.

필자는 어느 날 USB 메모리 스틱이 필요해 인터넷 쇼핑을 통해 구입하기로 마음먹었다. 인터넷을 뒤적인지 얼마 되지도 않아 엄청나게 싼 가격(수백 파운드)에 4GB의 USB 메모리 스틱을 구입할 수 있음을 알게 됐다. 이것은 곧 4GB의 정보를 한 손에 넣을 수 있

[그림 1] 20MB 정도의 정보쯤은 다른 사람이 마음만 먹는다면 쉽게 가져나갈 수 있다.
(그림제공 : Pointsec Mobile Technologies)

음을 의미하는 것이다. 대용량, 휴대성 및 간편성으로 이동매체는 오늘날 우리 주변에서 가장 인기있는 저장매체가 됐다. 이렇듯 폭발적인 인기를 얻고 있는 저장매체는 가격도 저렴해져 이제는 대형 컴퓨터 쇼룸에 가면 선물로 공짜 메모리 스틱을 받을 수 있을 정도가 됐다.

여러분이 필자와 같다면, 작은 메모리 스틱이나 콤팩트 플래시 카드, 그리고 디지털 카메라에 사용되는 메모리 카드가 갖는 장점이 매우 매력적이라고 느낄 것이다. 이런 장점은 장시간의 여행이나 사무실에서 오래 떨어져 있을 때 더 이상 휴대용 컴퓨터를 들고 다닐 필요가 없다는 것을 의미한다. 그냥 열쇠고리에 USB 메모리를 달아 놓으면 그 무겁고 불편한 노트북 컴퓨터를 들고 다닐 필요없이 필요한 모든 서류들을 갖고 다닐 수 있기 때문이다. 이동매체 장치는 우리가 일하는 방식에 '편리함'을 부여해줬을 뿐만 아니라

즐거움까지 더해준 환상적인 장치다.

그렇다면 이에 따른 단점은 존재하지 않는 것일까? 이동매체가 인기를 얻게 되면서 더욱 많은 사람들이 회사의 정보를 저장하기 위해 이런 매체를 작업 현장에서 사용하게 됐다. 서류, 데이터베이스, 그래픽, 음악, 심지어는 영화와 비디오까지도 이 장치에 저장해 사용하고 있는 것이다. 그러나 이동매체와 관련된 보안상의 문제점이나 위험도도 증가하고 있다는 것은 불행한 사실이다.

만약, 당신이 중요한 회사서류를 다운로드 받아 USB 장치에 저장해뒀다고 가정해보자. 어느 날 그것을 사용하기 위해 가방을 뒤져봤지만, 불행하게도 USB는 온데 간데 사라졌다. USB 장치를 분실한 것이다. 당신의 USB를 주운 사람이 안의 내용을 읽어본 후 흥미가 없다고 한다면 불행 중 다행이겠지만 만약 그 정보가 범죄자나 기자 또는 경쟁사에게 입수되게 되는 경우에는 어떤 일이 일어날지는 상상할 수 없다. 더욱 치명적인 경우는 당신의 은행구좌가 텅 비게 되거나 당신의 신상정보를 도둑맞게 되는 것이다. 이런 일들은 실제로 발생하고 있으며, 믿을 수 없을 정도로 많은 사람들에게 치명적인 상처를 남기고 있다.

IT 관리자들이 당신의 회사조직 안에서 이동매체 사용을 통제할 수 없다면 그것은 당신 회사의 지적재산과 다른 민감한 회사정보를 마음대로 다운로드 받도록 대문을 활짝 열어놓고 있는 것과 다름없다. 정보손실이 비즈니스에 끼치는 해악은 단순히 재정적이거나 또는 영업에 관련된 것만은 아니다. 즉, 이제는 이동매체로 누출된 정보에 대한 법적인 책임도 고려해야 한다는 것이다. 만약, 불만을 가진 종업원이 고객정보를 누설하는 경우, 회사의 심각한 명예훼손을 불러일으킬 수 있을 뿐만 아니라 고객이 제기하는 명예훼손 소송에 휘말릴 수도 있다는 것을 의미한다.

손쉬운 대처방법 다섯가지

이동매체는 크기가 작고, 쉽게 은닉할 수 있으며, 사용이 간편하기 때문에 어느 조직에게나 보안상 심각한 위협요소가 될 수 있다. 이러한 이동매체가 가진 효용성과 그 안에 내재된 위험요소간의 균형을 이룰 수 있는 몇 가지 방법을 제시하고자 한다.

• 보안정책

이동매체는 장난감이 아니다. 따라서 먼저회사입장에서 이것을 어떻게 관리할 지를 결정해야 한다. 하지만 모든 이동매체의 사용을 금지한다는 것은 순진한 생각이 될 것이다. 이유는 이동매체가 실생활과 기업 비즈니스에 너무나도 폭넓게 사용되고 있기 때문이다. 따라서 이동매체의 사용을 용인하되 이동매체를 보안정책 대상에 포함시키고, 모든 직원들이 이 정책에 동의한다는 각서를 쓰게 하는 것이 첫 번째 방법이 될 수 있다. 또한, 직원들에게 이러한 정책이 지켜지지 않을시 취할 조치에 대해서도 충분히 설명할 필요가 있다.

• 교육 실시

종업원들에게 보안의 개념과 의미에 대해 알려줘야 한다. 그리고 왜 이런 특정한 통제들이 필요할 수밖에 없는지를 설명해야 한다. 여러가지 통제규칙을 단순히 강압적으로 부과하면 안된다. 그들에게 이를 충분히 설명하지 못한다면 종업원들은 이러한 통제규칙을 무시하게 될 것이다.

• 암호화

이동식 데이터를 보호하는 장치의 사용을 검토한다. IT 부서에 의해 이동식 매체에 대한 강제적인 암호화 기법이 가능하다. 이러한 보호장치는 자동으로 USB 장치나 다른 이동매체에 다운로드 되는 모든 정보에 암호를 부여하게 된다. 그리고 패스워드를 갖고 있는 사용자에게만 접근이 허용된다.

• 통제

이동매체나 실행 파일을 통제할 수 있는 대책을 수립해 어떤 장치들이 시스템에 연결 가능하고, 어떤 실행 파일들만이 실행 가능한지 충분히 파악하고, 통제할 수 있어야 한다.

• 감사와 대응책

누가 이동매체를 사용하고 있는지를 파악하기 위해 정기적으로 감사를 실시하도록 한다. 오늘날의 복잡한 디지털 세계에서는 보안에 관한 어떤 것도 완벽히 보장되지 않는다. 그러나 이러한 몇 가지 간단한 조치들만으로도 위험을 상당부분 줄일 수 있으며, 이동매체를 통해 전달되고 있는 정보들의 안전을 위해 당신이 할 수 있는 모든 적절한 조치를 취하고 있음을 증명해 보일 수 있다.

09

한국정보보호진흥원 불법스팸대응센터
www.spamcop.or.kr

스팸메일에서 자유로워지자

스팸메일은 이용자의 정신적인 피해를 일으키며, 필요한 정보 수신을 방해하고, 메일서버의 과부하를 초래할 뿐 아니라 업무효율을 떨어뜨려 생산성을 악화시킨다. 스팸으로 인한 근로손실 비용은 전세계적으로 5억 달러가 넘는 것으로 추정되고 있을 만큼 스팸메일로 인한 피해는 심각한 수준이다.

스팸메일이란, 이메일이나 휴대폰 등 정보통신서비스를 이용하는 이용자의 단말기로 일방적으로 전송되는 영리목적의 광고성 정보를 말한다. 본인이 원하지 않음에도 불구하고 일방적으로 전송되는 메시지 때문에 이용자의 정신적인 피해를 일으키며, 필요한 정보 수신을 방해하고, 메일서버의 과부하를 초래한다.

현재 전 세계적으로 발생하는 스팸메일은 전체 이메일의 50~80%에 이르는 것으로 나타났다. 한국정보보호진흥원이 2006년 상반기 스팸 수신량을 조사한 결과, 1인당 하루 평균 받는 스팸메일은 5.4통이었으며, 대출 관련한 스팸이 전체의 50%를 차지하고, 성인물 스팸은 8.7%를 차지했다.

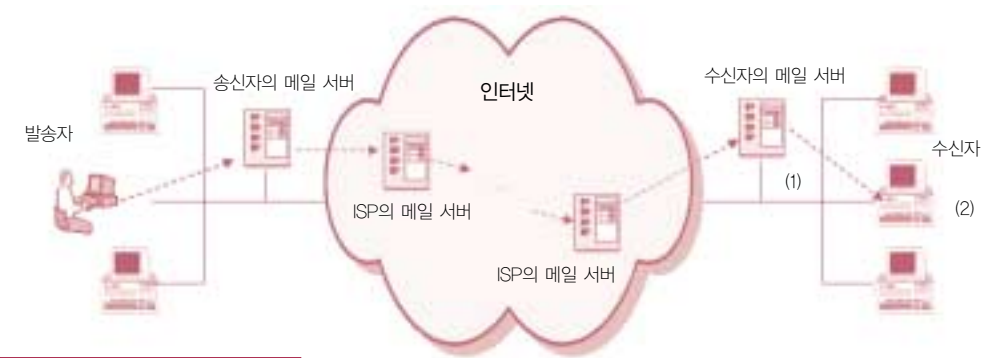
한국정보보호진흥원의 2005년 정보보호 실태조사 결과 스팸으로 인한 가장 큰 피해는 수신자가 성가시고 짜증나는 기분을 느낀다는 것이다. 전체 응답자의 21.3%가 이같은

정신적인 피해를 호소했으며, 다음은 바이러스 감염과 개인정보 유출을 들었다(18.2%, 22.1%).

스팸은 정신적인 피해 뿐 아니라 사회 · 경제적인 피해를 갖고 오는 것으로 조사되고 있다. 스팸 필터링에 근무시간이 낭비되고, 스팸으로 인해 발생하는 문제를 해결하기 위해 추가적인 자원이 투여되기 때문이다. 스팸메일 차단 솔루션 업체인 지란지교소프트가 2006년 2500명 규모의 사업체를 대상으로 조사한 결과, 스팸으로 인한 근로손실 비용은 연간 약 6억원 정도라고 추정했으며, 미국의 전문시장조사 기관인 Ferris Research사는 2005년 스팸으로 인한 전세계의 피해액은 5억 달러가 넘는다고 추정하였다.

스팸 피해를 줄이기 위해서는 다양한 인증과 필터링 기능을 이용한 스팸메일 차단 솔루션을 활용하는 것이 가장 효과적인 방법이다. 웹메일 서비스 업체는 이를 이용해 사용자에게 도착하는 스팸메일을 줄이고 있지만, 자체 메일계정을 발급하고 관리하는 기업이나 기관은 상대적으로 스팸메일의 피해에 대한 문제인식이 부족해 해당 솔루션을 도입한 곳이 많지 않으며, 솔루션 도입 계획조차 없는 곳이 대다수인 것으로 나타나고 있다.

스팸차단 솔루션의 활용방법



- 서버용 : (1)단계에 설치
- 클라이언트용 : (2)단계에 설치

[그림 1] 스팸차단 솔루션 기능도

스팸메일 차단 솔루션은 서버용과 클라이언트용으로 나뉘며, 서버용은 메일전송 1단계에, 클라이언트용은 수신자가 메일을 받기 전인 2단계에 설치된다. 기업 등에서 자체

적으로 메일전용 프로그램을 이용할 경우, 회사 메일 서버에 설치할 때는 서버용으로, 이용자 PC에 설치할 때는 클라이언트용을 구입해 사용한다.

현재 국내에서 판매되고 있는 스팸메일 차단 솔루션의 스팸 감축효과는 80~90% 이상이며, 오탐지율은 0.01~1% 정도인 것으로 나타나고 있다. 미국의 시장전문기관인 Frerris Research사의 조사결과에 의하면 스팸 솔루션을 설치했을 때 스팸 취급비용은 개별 PC에 설치하는 솔루션은 217달러, 서버 솔루션은 132달러인 것으로 나타난다. 서버기반 솔루션이 설치와 관리비용이 가장 적게 소요되지만, 직원수가 적은 사업체는 PC 기반 솔루션이 더 효과적이다. 스팸 솔루션이 없어 직접 삭제하는 데에는 718달러가 드는 것으로 나타난다. 스팸 차단 솔루션을 도입할 때는 이용자 수가 많은 큰 규모의 기업이나 기관, 학교 등에서는 솔루션 패키지를 구입하는 것이 좋고, 이용자 수가 적은 중소기업은 임대하는 방법을 사용할 수 있다.

스팸메일 방지기술

스팸메일을 방지하는 기술은 발송과 수신의 단계에서 차단하는 방법이 있다. 발송단계에서의 차단은 인증과 발송비용 부과, 발송량 제한, 유동 IP 이용자의 25번 포트 차단 등의 방법이 있다. 이중 인증 시스템은 특정 IP 주소의 이메일이 참인지 거짓인지 구분하여 알려주는 것으로 위조된 이메일을 구분하기 위해 여러 가지 방법이 고안되고 있다. SMTP 인증방식은 이용자 계정과 암호를 이용하는 것으로, SASL(Simple Authentication and Security Layer) 기반을 이용하여 이용자 암호가 네트워크로 전송되는 것을 방지하거나 질의-응답(Challenge-Response System)을 통해 클라이언트에게 비밀번호와 해당 질의의 해시값을 보낸다.

SPF(Sender Policy Framework)와 SIDF(Sender ID Framework)는 해당 도메인에서 발송 서버로 정식 등록되었는지 확인하고, 확인되지 않은 메일을 스팸메일로 간주하는 강력한 방식이다. SPF는 이메일 주소와 발송서버가 일치하지 않는 이메일을 차단하며, SIDF는 SPF 인증기능에 발송자 인증기능을 추가한 것이다. 도메인과 서버 수준에서 인증을 받는 DKIM(Domain Keys Identified Mail)은 발송자 도메인을 공개키 방식으로 서명하고, 수신 서버에서 확인해 메시지 전송과 발송과정에서의 위 · 변조를 원천적으로 방

지할 수 있는 기술이다. PKI(Public Key Infrastructure)와 PGP(Pretty Good Privacy)는 공개키 방식의 이메일을 암호화해 전자서명 하는 방식이다. PKI는 중앙집중식 인증서 관리를 통해 메시지의 전송과정 및 발송과정의 위·변조를 방지 할 수 있는 기술이며, PGP는 이메일 이용자간의 공개키 교환을 통해 동일한 효과를 얻을 수 있는 기술이다.

개념적으로 스팸문제를 해결하기 위한 가장 간단한 방법은 전통적인 우편물처럼 각 이메일마다 발송 대가의 지불을 요구하는 것이다. 이메일 총량에 대한 발송비용을 부과하는 방법 외에도 메시지를 발송하는데 소요되는 시간에 대해 비용을 부과하는 방식도 사용되고 있다. 수신 서버측에서 화이트리스트와 블랙리스트를 관리하며, 화이트리스트에 들어있지 않은 이용자가 발송한 메일은 발송자를 확인한 후 메일을 발송하도록 했다.

좀비 PC로부터 발송되는 스팸을 줄이기 위해 유동 IP의 25번 포트를 차단하는 방식은 외국의 많은 ISP가 사용한다. 포트 25번을 차단하면 발송자는 ISP 메일 서버를 이용해 메일을 발송하는데, 이는 ISP가 구현한 스팸방지 대응방법에 통제된다. 이 방법은 네트워크에 진입하는 스팸을 현저하게 줄일 수 있다. 또한, 스팸메일이 기본적으로 대량의 광고메일을 발송하는 것이라는 점에서 발송량을 제한하는 방법도 일부 쓰이고 있다.

수신단계에서 스팸을 방지하기 위해 발송자의 신뢰도를 평가하는 시스템은 전통적인 스팸대응 해결방법중 하나이다. 발송하는 측의 이메일 서버가 과거에 갖고 있던 신뢰도에 근거해 스팸인지 아닌지 결정한다. 화이트리스트를 허용하는 방법과 블랙리스트를 차단하는 방법이 기본적으로 쓰인다. 필터링은 가장 구현이 쉽고 이용자가 스팸으로 간주하는 수준을 직접 결정할 수 있어 가장 많이 쓰인다. 그러나 스패머가 철자를 틀리게 하거나 다른 언어로 표기해 발송하면 스팸을 걸러낼 수 없다는 한계를 갖고 있다. 발송 단계에서 발송량을 제한하는 것과 마찬가지로 수신량을 제한하는 방법도 스팸방지에 많이 쓰이는 방식이다. 신뢰도평가 시스템과 함께 사용되며, 이메일 스팸을 감소할 수 있다. 그러나 시급하고 중요한 메일이 불필요하게 지연될 수 있다는 단점도 갖고 있다.

이 외에도 이메일 주소를 홈페이지에서 자동 수집하지 못하도록 여러 형태로 변형하는 방법이 있으며, 존재하지 않는 이메일 주소에 대해 수신자 없음 확인메일을 회신하지 않도록 설정하는 기술, 회원가입 단계에서 사람의 육안으로만 식별이 가능한 왜곡된 이미지를 제시하여 제한시간 내에 입력하도록 하는 웹메일 자동등록 차단기술도 많이 쓰이고 있다.

'스팸'의 어원

스팸은 햄과 다진 돼지고기를 섞어 조리한 통조림 식품으로 1937년 미국 호멜식품이 처음 선 보인 뒤, 전쟁과 함께 미군이 가는 곳을 따라 성장해 나갔다. 지금 스팸의 의미는 그 뜻이 확장되어 이메일이나 휴대폰 등을 이용해 대량의 광고를 보내는 행위, 또는 광고 자체를 스팸이라고 일컫고 있다.

스팸이 '대량광고'라는 뜻을 갖게 된 것은 스팸을 처음 출시한 호멜식품이 홍보효과를 높이기 위해 엄청난 양의 광고를 뿌리기 시작하면서 부터이다. 막대한 자금을 투자한 호멜식품은 스팸을 성공시키기 위해 광고와 홍보에 열을 냈으며, 사람들은 어디에 가도 스팸 광고를 접하게 되었다. 이때부터 '광고 공해'라는 사회적인 문제가 시작되어 공중파 드라마에서도 이를 풍자한 장면을 연출하기도 했다.

드라마에서는 한 부부가 식당에 가서 주문을 하려고 종업원에게 어떤 메뉴가 있는지 물어본다. 종업원은 "달걀과 스팸이 있습니다. 베이컨과 스팸도 있고, 소시지와 스팸도 있습니다. 스팸 달걀 스팸 베이컨도 있고, 스팸 소시지, 스팸 감자, 스팸 토마토도 있습니다. 스팸 스팸 스팸…."

10

(주)정보보호기술 보안컨설턴트 이성구
(주)화이트웨이 보안관리자 김훈

미래사회를 위한 준비, 정보보호전문가

기업은 보안시스템을 구축하기 위해 막대한 예산을 들이기보다는 이미 갖추어진 인프라스트럭처를 효율적으로 활용하기를 원한다. 이 때문에 현재의 보안구조를 보다 총체적인 안목에서 분석하고 효과적인 비용관리와 솔루션을 제공할 수 있는 보안전문가의 역할이 중요해지고 있다.

IT 시장에서 핵심이 될 키워드를 꼽으라고 한다면 '정보보호'가 매우 높은 순위에 오를 것이다. 사이버 세상이 방대해지면서 점점 더 다양한 경로로 정보가 유출되며, 이로 인한 사회 · 경제적인 피해가 늘어나고 있기 때문이다.

1990년대 이전 까지만 해도 '해커'나 '크래커'는 미래사회를 그린 SF 영화에서나 볼 수 있는 존재였다. 그러나 2000년대에 접어들면서 전 세계의 네트워크망이 5년마다 10배씩 빨라지고, 네트워크에 위해를 가하는 공격자들의 공격양상은 그 보다 수 십 배 이상 빠른 속도로 변화하고 있다. 심지어 정보가 다른 곳으로 빠져나가고 있다는 사실조차 알아채지 못한 채 정보를 도둑맞는 경우도 비일비재하게 일어나고 있다. 이는 개인이나 기업 뿐만 아니라 정부와 국가조직 전반에서도 심심치 않게 발생하고 있다. 정부조직도 IT에 대한 의존도가 높아지면서 네트워크의 발달과 함께 정보보호가 중요해지고 있다. 이

제 보안은 기업과 정부조직의 생존과 직접적인 관계에 있다고 해도 과언이 아니다.

그러나 여전히 우리 사회에서 보안은 일단 어떤 사건이 터지면, 그제서야 대응책을 마련하고 피해확산을 막는 '사후 약방문' 수준에 머무르고 있다. 〈Information Week〉 등의 정보보호 연구결과를 보면, 보안사고는 급증하고 있지만 보안에 높은 우선순위를 두는 기업은 극히 소수에 불과하다. 대다수의 기업들이 보안을 위한 인프라스트럭처에 대해 충분히 투자했다고 생각하고 있으므로 기업은 보안시스템을 구축하기 위해 막대한 예산을 들이기보다는 이미 갖추어진 인프라스트럭처를 보다 효율적으로 활용하기를 원한다.

그러나 네트워크에 대한 공격은 1분, 1초가 멀다 하고 새로운 방식을 쏟아내고 있다. 공격자들은 더욱 정교하고 복잡하고 다양한 방식으로 시스템의 취약점을 노리고 있어 아무리 잘 갖추어진 보안시스템도 100% 안심할 수 있는 것은 없다. 이 때문에 현재의 보안구조를 보다 총체적인 안목에서 분석하고, 효과적인 비용관리와 솔루션을 제공할 수 있는 보안전문가의 역할이 무엇보다 중요하다. 정보보호전문가가 디지털 시대의 필수인력으로 꼽히는 시대가 온 것이다.

정보보호전문가의 역할

정보보호전문가란 해킹과 바이러스, 개인 · 기업의 정보유출 등에 대응해 보안과 유지를 전문적으로 담당하며 관련 정보를 제공하는 사람을 말한다. 정보기술의 발달과 함께 더욱 교묘해지고 지능화되는 공격유형을 분석하고 탐지해 예방책을 마련하는 정보보호전문가는 모든 분야에서 반드시 필요한 전문직업으로 자리잡고 있다. 이같은 추세를 반영하듯 최근 언론에 발표된 '2010년 유망직종'에 정보보호전문가가 들었으며, 향후 10년 뒤 소득수준과 사회적 위상이 가장 높아질 직업에도 정보보호전문가가 꼽혔다.

정보보호에 대한 관심이 높아졌다 해도 기업이나 정부가 막대한 비용을 들여 보안시스템을 구축하려 하지는 않는다. 이왕이면 기존에 구축된 시스템을 최대한 활용하며, 제한된 예산 안에서 완벽한 보안이 이뤄지기를 원하고 있다. 이 때문에 보안담당자는 탄탄한 이론과 함께 다양한 실무능력이 요구된다.

정보보호는 단순히 방화벽이나 IDS, IPS에만 국한된 것이 아니다. 모든 불법적인 침입과 침해에 대응하기 위해 시스템, 네트워크 보안시스템을 구축할 수 있어야 한다. 이를

위해 필요한 제반 영역을 설계하는 것은 물론, 인프라 구축, 차후 관리까지 정보보호관리자의 역할에 포함된다. 나아가 시스템을 운용하면서 이를 보호하기 위한 컨설팅 역할도 정보보호 관리자의 몫이다. 따라서 현장에서 필요로 하는 정보보호전문가는 IT에 대한 기본지식은 물론이고, 정보보호에 대한 전문지식과 해당 조직의 업무에 대한 폭넓은 이해가 필수요건이다. 어떤 시스템을 어떻게 보호할 것인지 보안에 대한 전반적인 틀을 잡고, 필요한 인프라를 구축하며, 실제 업무에서는 어떻게 적용시킬 것인지 방법을 강구해 내는 것이 정보보호전문가가 해야 할 일이다.

우리나라의 경우, 보안전문가의 숫자는 수요에 비해 절대적으로 부족한 상황이다. 이론과 실무를 겸한 전문가는 더욱 적어 정보보호 산업은 아웃소싱을 중심으로 이루어지고 있는 실정이다. IT 강국이라 자부하는 우리나라에 보안전문가가 적다는 것은 그만큼 보안에 대한 인식이 낮다는 것을 보여준다. 그동안 보안이 산업의 발전과 개발에 있어 불편한 장애물로 인식되어 언제나 뒷전으로 밀려났기 때문이다. 전 세계적으로 보안에 대한 중요성이 커지고 있는 만큼 우리나라도 IT 강국에서 '보안강국' 으로 거듭나기 위해 정보보호전문가가 중요한 시점이 되었다.

정보보호전문가의 필수 요건

정보보호전문가가 되기 위해 가장 필요한 것은 두말할 필요도 없이 관련 자격증을 취득하는 것이다. '진료는 의사에게 약은 약사에게' 라는 말은 전문적인 자격증을 가진 사람에게 필요한 서비스를 받으라는 것이다. 자동차 정비를 받을 때는 자동차 정비 자격증을 가진 사람에게 가게 되고, 빵을 살 때는 제과 · 제빵 자격증을 가진 사람이 만든 제품을 사게 된다. 세탁소에 세탁물을 맡길 때도 '세탁 기능사' 라는 자격증을 가진 사람이 운영하는 세탁소에 먼저 눈길이 가게 된다. 자격증이라는 것은 해당 분야에 대한 전문적인 자격을 갖춘 사람이라는 것을 증명해주는 것이기 때문이다. 정보보호전문가 역시 마찬가지이다. 스스로가 자동차 정비전문가라고 자부하며 다년간의 실무 경험을 자랑한다 해도 자동차 정비 1급 자격증을 가진 사람과 같은 대우를 받지 못하는 것이 현실인 것처럼, 정보보호 분야에서 다년간의 경력을 갖췄다 해도 전문 자격증을 갖고 있지 않으면 그 사람의 능력을 인정받기가 쉽지 않다.

자격증만 갖고 있다고 해서 전문적인 능력을 인정받는 것도 아니다. 자격증에도 희소가치가 있다. 자격증 소지자가 많지 않았을 때는 '부르는 것이 몸값' 이 될 수 있으나 너도 나도 자격을 취득하게 되면 자격증 외에 또 다른 무언가가 있어야 해당 분야에서 인정을 받을 수 있다. 몇 년 전, '전망있는 전문자격증' 이라는 타이틀이 붙었던 마이크로소프트의 MCSE(Microsoft Certified System Engineer)나, 시스코의 CCNA(CISCO Certified Network Associate)는 'IT의 국민자격증' 으로 불릴 만큼 많은 합격자를 배출했다. 두 자격증 모두 외국에서는 대단히 높은 인정을 받고 있으나 우리나라에서는 그만한 가치를 인정받지 못하고 있는 것은 이러한 이유 때문이다.

현재 국제적인 정보보안 자격증으로 인정받고 있는 것은 정보시스템 보안전문가(CISSP : Certified Information System Security)와 국제공인 정보시스템 감사사(CISA : Certified Information Systems Auditor)를 들 수 있다.

CISSP는 1989년 정보보호 전문가 자격증 개발에 관심있는 국제단체들이 컨소시엄을 형성하여 설립한 국제정보보호 자격증 컨소시엄((ISC)^2 : International Information Systems Security Certification Consortium)에서 도입한 것이다. 특정 벤더에 종속되지 않으면서 광범위한 보안 주체를 10개의 CBK 도메인으로 정리해 보안 전문자격을 인증한다. CISA는 정보시스템감사통제협회(ISACA : Information Systems Audit and Control Association)에서 실시에서 실시하고 있으며, 정보 시스템의 지배, 통제, 보안, 감사 분야의 공인 전문 자격증이다.

ISACA에서 실시하는 또 다른 보안 자격 인증 프로그램인 CISM(Certified Information Security Manager)은 2003년 처음 도입한 후 가장 주목받는 자격증으로 떠오르고 있다. CISM은 정보보안 관리 책임자를 위한 자격증으로, 효과적인 정보보안과 컨설팅 서비스 제공에 요구되는 경력과 지식을 국제적으로 보증한다.

우리나라에서 공인되는 자격증은 한국정보보호진흥원(KISA)과 한국정보통신대학교(ICU)가 공동으로 주관해 실시하는 정보보호전문가(SIS : Specialist for Information Security)가 있다. SIS는 정보보호와 보안관련 분야의 지식과 정보보호가 요구되는 다양한 분야에서의 업무수행 능력을 평가한다.

정보보호 자격증 취득의 이점

네트워크에 대한 공격으로 인한 피해가 막대해지면서 기업 경영진 사이에는 정보보호가 사업비용이 아니라 사업을 가능하게 하는 수단이라는 인식이 빠르게 확산되고 있다. 정보보호가 그 어느 때 보다 중요한 시점에 이르면서 보안시장은 가파르게 성장하고 있어 정보보호전문가에 대한 수요도 매우 커지고 있다. 이에 따라 정보보호전문가에 대한 폭발적인 수요는 앞으로도 꾸준히 계속될 것으로 전망된다.

정보보호 관련 자격증을 취득하게 되면, 현재의 직업에 보안전문가로서의 자격을 부여받아 노동시장에서 보다 높은 경쟁 우위를 가질 수 있다. 이는 보다 넓고 다양한 고용기회와 급여 인상을 위한 토대를 제공받을 수 있으며, 보다 높은 사회적인 지위를 보장받을 수 있다는 말이기도 하다. 자격증을 취득하고, 실무경력을 쌓아 보안전문가로서 인정을 받으면, 개인적인 이익 외에도 정보보호를 통해 국가 및 기업의 경쟁력을 강화한다는 사회적인 보람도 찾을 수 있다. 공격유형을 미리 예측하고 이미 갖추어진 보안 인프라로 효과적으로 막는다면, 공격을 막지 못해 발생하는 사회적인 비용을 줄일 수 있다.

시대에 따라 유망한 직군과 직종이 새로 생겨나고 퇴색되기도 하지만 정보보호 전문가는 시간이 지날수록 더욱 더 가치를 인정받는 직업이 될 것이다. 그 시대를 준비하기 위해 정보보호 자격증에 대한 필요성은 더욱 강조될 것으로 예상된다.

보안 자격증 소개

CISSP_ 특정 벤더에 종속되지 않은 체계적인 보안인증 프로그램

CISSP(Certified Information Systems Security Professional)는 국제공인정보시스템 보안전문가의 약칭으로, 정보보호전문가 개발에 관심있는 국제 조직들이 1989년에 컨소시엄을 형성하여 설립한 (ISC)²(International Information Systems Security Certification Consortium)가 발급, 관리하는 국제정보 시스템 보안전문가 자격증이다.

CISSP는 특정 벤더에 종속되지 않으며, 광범위한 보안 주체를 10개의 CBK 도메인으로 정리한 체계적인 보안인증 프로그램으로, 각종 언론의 조사결과에서도 10대 유망 IT 자격

증 가운데 하나로 선정되고 있다.

CISSP 자격을 얻기 위해서는 자격시험과 일정 기간의 실무경험이 있어야 하며, 자격 취득 후에도 CPE 자격을 유지하기 위해 교육을 받아야 한다. CISSP 자격시험은 한글과 영어, 일본어 중 하나를 선택할 수 있으며, 총 250문제를 6시간 안에 풀어야 한다. 시험과목은

- 접근제어 시스템 및 방법론(Access Control Systems and Methodology)
- 응용 및 시스템 개발 보안(Applications and Systems Development Security)
- 사업연속계획 및 비상복구계획(Business Continuity Planning(BCP) and Disaster Recovery Planning(DRP))
- 암호학(Cryptography)
- 법, 수사 및 윤리(Law, Investigation and Ethics)
- 운영보안(Operations Security)
- 물리적 보안(Physical Security)
- 보안구조 및 모델(Security Architecture and Models)
- 보안관리(Security Management Practices)
- 통신 및 네트워크 보안(Telecommunications and Network Security) 등이다.

자격시험 통과 외에 (ISC)²에서 지정하는 10개 도메인 중 하나 이상의 도메인에서 4년 이상의 실무 경력이 필요하다. (ISC)²가 지정한 도메인은 시험과목에 제시된 것과 같다. 학사학위를 갖고 있으면 1년의 경력을 대체할 수 있다. 자격시험에 합격할 때를 기준으로 자격요건을 갖추지 못한 경우, 합격 후 5년 내에 요건을 충족해야 하며, 요건이 충족될 때까지 매년 35달러의 지연금을 지불해야 한다.

CISSP 자격을 얻은 후에도 (ISC)²의 윤리강령을 준수해야 하며, 매 3년 마다 최소 120학점을 이수해야 하는 CPE(Continuous Professional Education) 요구조건을 충족시켜야 한다.

SIS_ 정보통신부 고시 기술인력 자격

한국정보보호진흥원(KISA)과 한국정보통신대학교(ICU)가 공동으로 주관해 실시하고 있는 국가공인 자격증인 정보보호전문가(SIS : Specialist for Information Security)는 정보보호와 보안정책을 수립, 구축하는데 필요한 업무를 수행한다. SIS 자격소지자가 진출한 분

야는 정보보호 전문업체를 비롯해 보안시스템 개발업체, 전자상거래 및 보안전문 컨설팅 업체, 정부기관, 일반기업, 연구소, 인터넷 쇼핑몰, 금융권 등 사회 전 분야에 걸쳐 있다.

SIS 자격 취득자는 KISA, 기무사, 한국전력공사 등의 정보보호 관련 종사자를 채용할 때 우대받을 수 있으며, 학점은행을 통해 SIS 1급은 24학점, 2급은 12학점을 인정받을 수 있다.

정보보호 전문가 2급 자격시험은 응시자격에 제한이 없지만, 1급 시험은 관련직무에서 3년 이상의 경력을 갖고 있어야 한다. 2급 자격을 얻고 관련 직무에서 2년 이상 경력을 가진 사람도 1급 시험에 응시할 수 있다. 4년제 대학교를 졸업했거나 졸업예정자로서 정보보호 관련과목을 12학점 이상 이수한 사람도 1급 시험 응시자격을 얻는다. 해당과목은 시스템 / 네트워크 / 애플리케이션 / 정보보호 일반분야이다.

시험은 시스템 보안 / 네트워크 보안 / 어플리케이션 보안 / 정보보호론 등 4개 과목으로 이루어지며, 1차 필기시험과 2차 실기시험으로 나누어 진행된다. 2차 실기시험은 실무능력검증을 위해 단답형, 서술형과 함께 실무형 시험이 병행된다. 합격기준은 필기시험의 경우, 과목별 40% 이상 과목평균 60% 이상 취득해야 하며, 2차 실기시험은 유형별 40% 이상, 전체평균 60% 이상 점수를 얻어야 한다. 1차 필기시험에 합격한 사람은 3회까지 2차 실기시험에 응시할 수 있다.

CISA_ 정보시스템 지배/통제/보안/감사 공인 전문자격증

CISA(Certified Information Systems Auditor)는 미국에 국제본부를 두고 있는 정보시스템 감사통제협회(ISACA : Information Systems Audit and Control Association)가 1981년 도입한 정보 시스템의 지배, 통제, 보안, 감사분야의 공인 전문자격증이다.

미국과 유럽에서는 CISA를 정보시스템 감사전문가로 인정해 공인회계사(CPA)와 같은 수준의 위상으로 인정하고 있으며, 우리나라에서도 최근 CISA에 대한 인지도가 높아져 회계법인이나 IT 컨설팅 업체에서는 CISA를 입사시 갖춰야 할 자격요건으로 제시하고 있기도 하다. 현재 우리나라에서 CISA가 진출해 있는 영역은 금융계나 일반 회사의 감리부서는 물론이고, 감사원, 금융감독원, 국방관련 부서, 한국정보보호진흥원, 정보사회진흥원 등 정부부처와 공공기관, 회계법인, IT 전문업체, 컨설팅 전문업체, 산업계, 학계, 금융계, 언론계 등 사회 전반의 폭넓은 분야이다.

CISA 자격시험은 감사 프로세스 / IT 거버넌스 / 시스템 및 인프라 생명주기 / IT 서비스

의 제공 및 지원 / 정보자산의 보호 / 비즈니스의 연속성 및 재난 복구로 구성되며, 시험 출제 유형은 지식사항과 실무 관련사항, 포괄적인 개념으로 나뉜다. 관련사항에서는 개별적인 경험이 세계적인 환경과 일치하지 않을 수도 있으므로 다양한 분야의 경험이 필수적이다. 시험은 매년 6월과 12월 둘째 주 토요일에 실시되며, 한국어를 포함한 세계 11개 언어로 실시된다.

CISA 자격시험을 통과한 후에도 ISACA의 직무윤리 규정(Code of Professional Ethics)을 준수해야 하고, 5년 이상의 실무경력이 있어야 자격을 인정받을 수 있으며, 자격 취득 후 매년 교육을 수료해 CPE 요건을 충족시켜야 한다.

CISA에서 인정하는 실무 경험은

- 경영 전략과 조직 관리
- 정보시스템 기반 기술(Information Systems Infrastructure)
- 정보시스템 보안(Information Systems Security) 및 위험 관리
- 정보시스템 개발 및 프로젝트 관리
- BPR과 전자상거래

등이다.

실무경력 중 1년 이상의 정보 시스템 운영, 프로그래밍 경력 또는 회계감사 정보 시스템 감사 · 통제 · 보안경력 1년으로 인정되며, 전문대학 졸업자는 1년, 학사학위를 취득한 사람은 2년의 경력을 인정받는다.

CISM_ 정보보안 관리책임자를 위한 자격증

CISM(Certified Information Security Manager)은 CISA를 주관하고 있는 ISACA에서 정보보안 관리자와 정보보안 관리책임자를 위해 개발한 자격증이다. CISA가 정보기술 보증(IT Assurance) 영역을 커버한다면, CISM은 정보보안 영역을 커버한다고 볼 수 있다.

CISM은 정보보안 관리업무의 세계적인 표준을 조화시키는 역할을 하며, 효과적인 정보보안과 컨설팅 서비스 제공에 요구되는 경력과 지식을 국제적으로 보증할 수 있어 전망이 매우 높다. CISM이 진출한 영역은 컨설팅 업체를 비롯한 IT 관련 업계와 회계법인, IT 감사업체, 정보보안 관련 연구소, 일반 기업체와 금융기관 등이다.

CISM이 처음 실시된 2003년에는 일정한 자격요건을 갖춘 사람에게 자격시험을 면제해

주는 그랜드파더링(Grandfathering) 제도가 실시되기도 했다. 당시 대학교수와 IT 컨설팅 업체 등의 전문가들이 이 제도로 CISM 자격을 취득했지만, 자격요건이 까다로워 시험에 응시하는 사람이 해마다 큰 폭으로 늘었다.

CISM 시험은 CISA와 같은 6월과 12월에 실시되며, 시험영역은

- 정보보안 지배(Information Security Governance)
- 위험 관리(Risk Management)
- 정보보안 프로그램 관리(Information Security Program Management)
- 정보보안 관리(Information Security Management)
- 대응 관리(Response Management)

이다.

4지선다형 객관식 200문항으로 이뤄져 있지만, 현장에서 필요로 하는 지식과 경험을 근거로 하는 내용이 많아 결코 쉽지는 않다. CISM이 관리자를 위한 시험인 만큼 관련분야의 경험을 중요시 하기 때문이다. CISM은 아직 한국어 시험이 실시되고 있지 않고 있기 때문에 영어 · 일어 · 스페인어 3개 언어 중 하나로 응시해야 해 외국어 실력도 갖추고 있어야 한다.

CISM 자격 취득을 위해서는 시험합격 외에도 5년 이상의 정보보안 관련 경험이 있어야 한다. 단, CISA나 CISSP 자격을 취득한 사람이나 정보보안 관련 대학원을 수료한 사람은 2년의 경력을 대체할 수 있다. 정보시스템 운영경력이나 일반보안관리 경력, 혹은 GIAC(SANS Global Information Assurance Certification), MCSE(Microsoft Certified Systems Engineer), CompTIA Security+, Disaster Recovery, CBCPI(Institute Certified Business Continuity Professiona), ESL IT Security Manager 등의 자격을 취득한 사람은 1년의 경력을 대체할 수 있다.

CISM 자격을 얻은 후도 3년간 최소 120학점(매년 최소 20학점)의 CPE를 충족시켜야 자격을 유지할 수 있다.

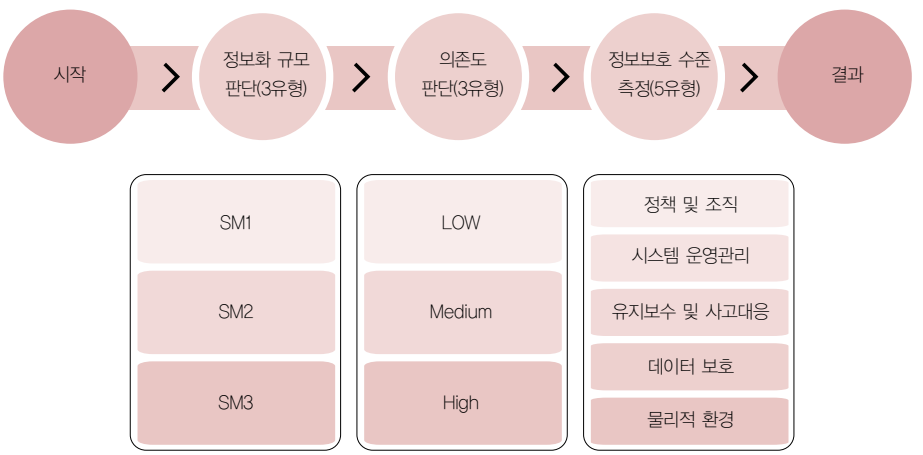
보안정책을 만든다고 해서 보안 솔루션만
잔뜩 들여놓을 수는 없는 일이다.
우리 조직에 필요한 정보보호 수준을 파악하고,
정보보호 정책 구현을 위한 지침과 표준, 절차를 정한 후,
이를 전담할 담당자와 필요한 교육, 솔루션을 구비하면서
단계적이고 체계적으로 진행해야 한다.

보안정책 수립에도 순서가 있다

01

한국정보보호진흥원 IT기반기획팀
www.kisa.or.kr

기업 정보보호 자가측정 리스트



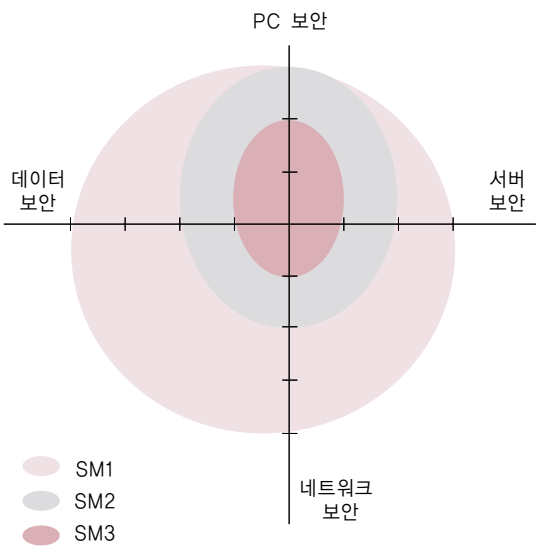
[그림 1] 정보보호 수준 자가측정 절차

대기업의 경우, 경영진의 보안의식이 높아지면서 정보보호에 대한 대책과 전략은 일정한 수준에 올라있는 것으로 보인다. 그러나 중소기업의 보안은 여전히 사각지대에 머무르고 있다. 보안이 중요하다는 것은 누구나 인식하고 있지만, 보안에 소요되는 예산이나 인력을 마련하는 것이 쉽지 않은 일이다. 그보다 더 큰 문제는 어디에서부터 어떻게 보안체계를 수립해야 하는지 모른다는 것이다.

보안정책 마련이 어렵다고 미리 포기하지 말고 한국정보보호진흥원에서 제공하는 무료 온라인 '정보보호 수준 자가측정 서비스'를 통해 회사의 정보보호 수준을 진단해 보자. 이 서비스는 한국정보보호진흥원 홈페이지(www.kisa.or.kr)에 접속해 회원으로 가입하면 이용할 수 있다. 기업의 정보보호 수준과 미흡한 부분의 대책에 대한 결과를 막대그래프 등으로 알아보기 쉽게 보여준다. 설문에는 30분 정도 소요되며, 기업의 전산 시스템에 대해 잘 알고 있는 CEO나 정보시스템 담당자가 작성하는 것이 좋다.

서비스는 첫 단계로 기업의 정보화 규모를 진단해 SM1/SM2/SM3의 세가지 유형으로 분류한다.

SM1(Small & Mediu) 유형은 고객관리와 사내업무 등을 단순 PC 중심으로 처리하는 기업을 말한다. SM2는 인사, 재무, 공정관리 등 업무를 내부 네트워크 기반으로 처리하는 기업이며, SM3는 B2B, B2C 등 외부 네트워크와 연결해 전자거래를 하는 기업을 말한다. 일반적으로 정보화 유형이 SM1에서 SM3으로 이동하게 되면 지켜야 할 정보자산의 규모가 커지게 되고, 그에 따라 요구되는 정보보호 수준도 높아지게 된다.



[그림 2] 기업 유형별 정보보호 요구수준

다음단계에서는 정보화 유형에 따른 정보화 의존도를 판단한다. 정보화 자산의 민감성, 정보보호 재난이 발생했을 때 기업에 미치는 영향과 사외 시스템에 대한 의존도 등에 따라 요구되는 정보보호 목표수준을 평가한다. 정보시스템 의존도는 Low, Medium, High의 3 수준으로 나뉜다. 그 후 기업에 구축된 정보보호 수준을 정책과 조직, 시스템 운영관리, 유지보수 및 사고대응, 데이터보호, 물리적 환경 등 5가지 분야에 대해 측정한다. 이 단계에서 각 분야별 정보보호 조치상태와 목표수준 대비 미흡한 부분을 찾을 수 있다.

마지막은 수준측정 결과를 확인하는 단계이다. 3단계 설문내용을 토대로 막대, 방사형 그래프 등을 활용해 자사의 정보보호 수준을 한 눈에 알아볼 수 있는 결과보고서를 받을 수 있고, 분야별 정보보호 대책방안을 중소기업 정보보호 가이드라인 등을 통해 제시받을 수 있다.

중소기업 정보보호 수준 자가측정 서비스 설문 항목

구성도 평가

1. 귀사의 연간 총 매출액은 얼마입니까?

① 10억원 미만

② 10억원 ~ 50억원 미만

③ 50억원 ~ 100억원 미만

④ 100억원 ~ 300억원 미만

⑤ 300억원 이상

2. 귀사에 현재 재직중인 직원은 총 몇 명입니까?

① 1명 ~ 9명

② 10명 ~ 19명

③ 20명 ~ 49명

④ 50명 ~ 99명

⑤ 100명 ~ 299명

⑥ 300명 이상

3. 귀사에서 PC를 사용하는 직원은 총 몇 명입니까?

① 1명 ~ 9명

② 10명 ~ 19명

③ 20명 ~ 49명

④ 50명 ~ 99명

⑤ 100명 ~ 299명

⑥ 300명 이상

4. 국내 또는 국외에서 운영되고 있는 지점(지사)이 있습니까?

① 없다

② 국내 1지점(지사) 또는 국외 1지점(지사)

③ 국내 1지점(지사)와 국외 1지점(지사)

④ 국내 여러 지점과 국외 1지점 또는 국내 1지점과 국외 여러 지점

⑤ 국내 여러 지점과 국외 여러 지점

5. 정보시스템 구축 및 관리 등의 업무를 전문적으로 수행하는 인력이 몇 명 있습니까?

① 없음

② 1명 ~ 9명

③ 10명 ~ 19명

④ 20명 ~ 29명

⑤ 30명 ~ 39명

⑥ 40명 이상

6. 귀사는 총 몇 대의 PC를 사용하고 있습니까?(노트북 포함)

① 1대 ~ 5대

② 6대 ~ 10대

③ 11대 ~ 15대

④ 16대 ~ 19대

⑤ 20대 이상

7. 귀사의 주요 업무는 다음의 업종분류 중 어느 것에 속합니까?

① 정보서비스, ISP, 금융 및 보험, 통신, 방송

② 전력, 가스, 운수

③ 제조

④ 도소매

⑤ 건설, 부동산 및 임대

⑥ 농림, 수산, 임업, 광업

⑦ 그 외(복지, 기타 서비스업 등)

8. 귀사의 정보시스템(PC, 서버, 네트워크 등)을 활용한 업무환경은 어떻습니까?

① LAN 환경의 내부 네트워크 기반으로 인사, 재무 등의 단위업무 처리

② 독립적 PC 환경에서 고객관리 및 사내 업무 등이 PC 중심으로 처리

8-1. 네트워크를 통해 기업내 관련 업무를 수행하는 분야는 어느 분야입니까?

① 사내 네트워크 중심으로, 그룹웨어 및 단위업무 처리 등에 사용됨

② 외부 네트워크와 연결되어 전자거래 등을 하는 분야(B2B, B2C 등)

9. 귀사에서는 총 몇 대의 네트워크 장비(라우터, 허브, 스위치 등)를 사용하고 있습니까?

① 없음

② 1대

③ 2대 ~ 3대

④ 4대 ~ 5대

⑤ 6대 이상

10. 귀사에서는 총 몇 대의 서버(파일, 메일, 웹, DB 서버 등)를 운영하고 있습니까?

① 없음

② 1대 ~ 4대

③ 5대 ~ 9대

④ 10대 ~ 19대

⑤ 20대 이상

의존도 평가 : 컴퓨터 시스템에 대한 의존도

1. 하드웨어 컴퓨터 시스템(PC, 서버 등)에 장애가 발생하였을 경우, 정상적인 업무운영에 어느 정도의 차질을 가져옵니까?

① 전혀 영향을 미치지 않음(0%)

② 약간 영향을 미침(25%)

③ 보통 영향을 미침(50%)

④ 많은 영향을 미침(75%)

⑤ 매우 많은 영향을 미침(100%)

2. 소프트웨어 시스템(그룹웨어, ERP 등 보유 소프트웨어)에 장애가 발생하였을 경우, 정상적인 업무운영에 어느 정도의 차질을 가져옵니까?

① 전혀 영향을 미치지 않음(0%)

② 약간 영향을 미침(25%)

③ 보통 영향을 미침(50%)

④ 많은 영향을 미침(75%)

⑤ 매우 많은 영향을 미침(100%)

3. 온라인으로 금융거래 및 업무자료 교환 등의 어느 정도 자주 발생합니까?

① 2주에 1회 미만으로 발생

② 2주에 1회 정도 발생

③ 주 1회 정도 발생

④ 매일 1건 정도 발생

⑤ 매일 수차례 발생

4. 기업 업무에 정보시스템(PC, 서버, 네트워크 등)이 어느 정도 활용됩니까?

① 거의 활용하지 않음(0%)

② 필요에 따라 간헐적으로 활용(25%)

③ 일부 사내 업무에 활용(50%)

④ 상당부분 사내 업무의 매우 높게 활용(75%)

⑤ 모든 업무가 정보시스템을 활용(100%)

5. 귀사에서 정보시스템을 사용하는 주요 목적은 무엇입니까?

① 인터넷 웹 검색 등을 통한 자료 혹은 정보수집

② 소프트웨어를 이용한 문서작성 및 편집

③ 그룹웨어 등을 전자결재

④ 온라인 금융거래 등 전자상거래

⑤ ③+④

6. 귀사에서는 정보시스템에 대한 유지/관리가 어느 정도 이루어지고 있습니까?

① 유지/관리를 실시하지 않음

② 사고 발생시에만 실시

③ 부정기적으로 실시

④ 연 1~2회 이상 정기적으로 실시

⑤ 분기당 1회 이상 정기적으로 실시

의존도 평가 : 보안사고에 따른 의존도

1. 시스템 고장 및 해킹/바이러스 등으로 인하여 귀사의 정보시스템이 비정상적으로 작동하거나 외부인터넷 연결이 중단될 경우 귀사의 수익에 어느 정도 영향이 있습니까?

① 전혀 영향을 미치지 않음(0%)

② 약간 영향을 미침(25%)

③ 보통 영향을 미침(50%)

④ 많은 영향을 미침(75%)

⑤ 매우 많은 영향을 미침(100%)

2. 시스템 고장 및 해킹, 바이러스 등으로 인하여 귀사의 정보시스템이 비정상적으로 작동할 경우, 이를 복구하는 동안 정상업무에 어느 정도 영향을 미치게 됩니까?

① 전혀 영향을 미치지 않음(0%)

② 약간 영향을 미침(25%)

③ 보통 영향을 미침(50%)

④ 많은 영향을 미침(75%)

⑤ 매우 많은 영향을 미침(100%)

3. 최근 1년 동안 몇 건의 보안사고가 발생하였습니까?

① 없음

② 1 ~ 4건

③ 5건 ~ 9건

④ 10건 ~ 19건

⑤ 20건 이상

4. 보안사고로 인하여 귀사가 보유하고 있는 고객정보 및 기밀정보 유출시 귀사의 신인도에 미치는 영향은 어느 정도입니까?

① 전혀 영향을 미치지 않음(0%)

② 약간 영향을 미침(25%)

③ 보통 영향을 미침(50%)

④ 많은 영향을 미침(75%)

⑤ 매우 많은 영향을 미침(100%)

5. 귀사에서는 총 몇 건의 고객(개인) 주요정보를 보유하고 있습니까?

① 100건 미만

② 100건 ~ 500건 미만

③ 500건 ~ 1000건 미만

④ 1000건 ~ 2000건 미만

⑤ 2000건 이상

6. 귀사에서는 총 몇 건의 타기업(협력업체 포함) 주요정보를 보유하고 있습니까?

① 없음

② 1건 ~ 9건

③ 10건 ~ 49건

④ 50건 ~ 99건

⑤ 100건 이상

의존도 평가 : 기업 구성요소에 대한 의존도

1. 귀사에서는 전산시스템 구축 및 운영관리를 위하여 외부업체에 아웃소싱하고 있습니까?

① 아웃소싱하지 않음(0%)

② 특정 부분만 아웃소싱하고 있음(25%)

③ 일정 부분을 아웃소싱하고 있음(50%)

④ 대부분을 아웃소싱하고 있음(75%)

⑤ 모든 부분을 아웃소싱하고 있음(100%)

2. 정보시스템(서버, 네트워크 등)은 외부의 장애에 어느 정도 영향을 받습니까?

① 사내 정보시스템은 외부 정보시스템과 전혀 관계없이 작동함(0%)

② 사내 정보시스템은 외부 정보시스템과 필요에 따라 연관이 있음(25%)

③ 외부 정보시스템 장애 발생시 일부 IT 업무에 영향이 있음(50%)

④ 외부 정보시스템 장애 발생시 상당 IT 업무에 영향이 있음(75%)

⑤ 외부 정보시스템 장애 발생시 모든 IT 업무가 진행되지 않음(100%)

3. 귀사에서는 전자 기밀자료를 어느 정도 보유 및 관리하고 있습니까?

① 기밀자료를 전자자료로 보관하지 않음(0%)

② 소량의 기밀자료만 전산화 되어있음(25%)

③ 일부 기밀자료가 전산화 되어있음(50%)

④ 다량의 기밀자료가 전산화 되어있음(75%)

⑤ 모든 기밀자료는 전산화 되어있음(100%)

4. 귀사의 정보가 정보침해사고로 유출될 경우, 귀사 혹은 국가의 사회, 경제기반에 주는 영향력은 어느 정도 입니까?(주관적)

① 영향을 미치지 않음(0%)

② 거의 영향을 미치지 않음(25%)

③ 일정수준 영향을 미침(50%)

④ 상당한 영향을 미침(75%)

⑤ 매우 큰 영향을 미침(100%)

5. 정보화 대비 정보보호 투자수준은 어느 정도입니까? (정보보호지출액/정보화지출액X100)

① 1% 미만

② 1% 이상 ~ 3% 미만

③ 3% 이상 ~ 5% 미만

④ 5% 이상 ~ 10% 미만

⑤ 10% 이상

보안수준 평가 : 정책 및 조직

1. 각종 보안사고 예방 및 대응을 위한 정보보호 정책 또는 규정이 수립되어 있습니까?

① 정책 또는 규정이 수립되어 이행되고 있음

② 정책 또는 규정은 없으나 지침이 존재하여 필요시 수행됨

③ 정책 또는 규정이 수립 되어 있지 않음

1-1. 사내외 인력이 정보보호 정책과 규정을 이해하고 준수하도록 권고하고 있습니까?

① 주기적으로 정보보호 정책 및 규정을 공지함

② 필요에 따라 정보보호 정책 및 규정을 공지함

③ 정보보호 정책 및 규정을 따로 공지하지 않음

2. 귀사 내 정보보호 업무를 수행하는 개념의 부서가 존재합니까?

① 정보보호를 수행하는 담당조직이 존재함

② 필요에 따라 소집함

③ 정보보호 업무를 수행하는 부서가 없음

2-1. 정보보호 부서 내 해당 업무가 명확히 구분되어 업무를 수행하고 있습니까?

① 정보보호 부서 내 업무분담이 이루어지고 있음

② 필요시마다 업무분담을 수행하고 있음

③ 업무분담을 수행하고 있지 않음

3. 귀사 내 자산(인력, 시설, 매체, 정보)에 대해 중요도별로 분류하여 관리되고 있습니까?

① 모든 자산에 대해 중요도를 구분하여 관리되고 있음

② 기업내 대외비 정보 및 매체에 대해서만 구분하고 있음

③ 중요도를 분류하지 않고 있음

3-1. 귀사 내 자산관리를 위한 책임자를 지정하고 있습니까?

① 모든 자산에 대하여 책임자를 지정하여 관리함

② 중요 정보 및 매체에 대해서만 관리자를 지정하여 관리함

③ 자산관리를 담당하는 관리자가 지정되어있지 않음

4. 귀사 내 업무수행을 위하여 아웃소싱을 수행하고 있습니까?

① 예

② 아니오

4-1. 귀사 내 업무를 외부업체에 아웃소싱 수행시, 외부 인력 및 업체에 대한 관리규정이 있습니까?

① 아웃소싱 인력에 대한 관리규정이 수립되어 있음

② 특별한 관리규정은 없으나 아웃소싱 인력에 대한 관리를 수행

③ 아웃소싱 인력에 대한 관리규정이 수립되어 있지 않음

5. 귀사 내 인력 또는 아웃소싱 인력을 대상으로 보안사고 예방 및 대응의 정보보호 교육을 수행하고 있습니까?

① 사내외 모든 인력에 대한 정기적인 정보보호 교육을 수행함

② 사내 특정 업무 인력에 대해서만 비정기적인 교육 수행함

③ 정보보호 교육을 수행하지 않음

6. 귀사 내 · 외의 현직인력 및 퇴직인력에 대한 보안관리를 수행하고 있습니까?

① 모든 인력에 대한 개인 정보 보호 및 업무수행에 대한 관리를 수행

② 기업 내 주요 업무를 수행하는 인력에 대한 관리를 수행

③ 특별한 인력관리가 마련되어 있지 않음

보안수준 평가 : 시스템 운영관리

7. 귀사 내 서버를 보유하고 있습니까?

① 예

② 아니오

7-1. 귀사 내 서버의 예제 응용프로그램을 제거하였습니까?

① 불필요한 예제 응용 프로그램을 모두 제거하였음

② 중요 서버의 불필요한 예제 응용 프로그램만을 모두 제거하였음

③ 예제 응용 프로그램을 제거하지 않음

8. 네트워크로 연결된 개인 PC 및 서버에 대해 제3자에 의해 접근이 이루어지지 않도록 사용자별 권한을 설정하고 있습니까?

① 네트워크 공유설정 정책에 따라 사용자 권한을 설정하여 운영

② 개인이 필요시 접근권한을 설정하여 운영

③ 네트워크 접근에 대한 접근통제가 없음

9. PC 및 서버에 불필요한 공유폴더를 제거하고, 사용자 권한설정을 수행하고 있습니까?

① 모든 시스템에 불필요한 공유폴더 제거 및 사용자 권한설정을 수행함

② 중요 시스템(기밀문서, 회계정보 등을 관리)의 공유폴더만 관리

③ 공유폴더 관리를 수행하고 있지 않음

10. 네트워크 보안을 위한 정보보호 제품(침입탐지 시스템, 침입차단 시스템, Viruswall 등)을 설치하여 운영하고 있습니까?

① 모든 시스템에 설치하여 운영하고 있음

② 중요 시스템에만 설치하여 운영하고 있음

③ 보안제품을 설치 및 운영하지 않음

10-1. 담당자가 정보보호 제품의 보안기능을 이해하고 활용하는 정도는 어떻습니까?

① 정보보호 제품의 모든 보안기능을 이해하고 활용함

② 정보보호 제품의 일부 보안기능을 이해하고 활용함

③ 정보보호 제품의 기본 설치기능으로 활용함

11. 개인 PC 및 서버의 사용자 계정에 대한 암호 변경이 정기적으로 이루어지고 있습니까?

① 정기적(월 1회 이상)으로 암호를 변경함

② 비정기적으로 관리자의 지시에 의해 변경

③ 암호관리를 수행하지 않음

12. 웹브라우저의 보안 수준에 대한 권고를 이행하고 있는가?

① 모든 시스템의 웹브라우저에 보통이상의 보안수준 지정을 권고함

② 중요 시스템에 대해서만 권고함

③ 보안수준 권고를 이행하지 않음

12-1. 악의적인 ActiveX 컨트롤 차단을 권고 및 수행하고 있습니까?

① 기업 내 모든 사용자가 악의적인 ActiveX 컨트롤 차단을 수행함

② 중요 시스템에 대해서만 관리자에 의해 수행함

③ 악의적인 ActiveX 컨트롤에 대한 차단을 권고하지 않음

13. 허가된 소프트웨어를 설치하고 소프트웨어 설치시 충분한 테스트를 수행하고 있습니까?

① 모든 소프트웨어는 허가를 받아 설치하고 테스트를 수행해야 함

② 중요 소프트웨어에 대해서만 허가를 받아 설치하고 테스트를 수행함

③ 허가 및 테스트 수행없이 소프트웨어를 설치하고 있음

13-1. 정기적으로 허가된 소프트웨어 사용을 점검하고 있습니까?

① 정기적(월 1회)으로 수행

② 비정기적으로 수행

③ 점검을 하지 않음

14. 서버 및 개인 PC에 대해 실시간 바이러스를 점검하는 소프트웨어를 설치하여 운영하고 있습니까?

① 모든 시스템에 설치하여 운영함

② 중요 시스템에 대해서만 설치하여 운영함

③ 설치하지 않음

14-1. 수신 파일 및 이메일에 대한 바이러스를 점검하고 있습니까?

① 모든 수신 파일 및 이메일에 대하여 반드시 점검하도록 함

② 필요시 점검하도록 권고하고 있음

③ 점검을 수행하지 않음

15. 운영체제에 대한 정기적인 보안 업데이트를 수행하고 있습니까?

① 모든 시스템에 대한 보안 업데이트를 수행함

② 중요 시스템에 대해서만 보안 업데이트를 수행함

③ 정기적인 업데이트를 수행하지 않음

16. 책상을 비울 경우, 화면보호기 및 스크린 잠금을 사용하고 있습니까?

① 모든 시스템에 대하여 화면보호기 및 스크린 잠금을 사용함

② 중요 시스템에 대해서만 수행됨

③ 화면보호기 및 스크린 잠금을 사용하지 않음

17. 스팸메일에 관하여 차단 및 수신 제한을 수행하고 미리보기 화면이 설정되지 않도록 하고 있습니까?

① 모든 메일에 대하여 스팸메일 차단 및 점검을 수행함

② 중요 메일에 대해서 스팸메일 차단 및 점검을 수행함

③ 점검을 수행하지 않음

18. 귀사 내 무선 랜을 설치하고 사용하고 있습니까?

① 예

② 아니오

18-1. 귀사에서는 무선 랜 사용시, 무선 랜(AP, 단말기 등)에 대한 접근정책이 수립되고 접속자에 대한 인증을 수행하고 있습니까?

① 무선 랜 보안정책에 따라 인증을 수행함

② 접근정책이 수립되어 있지 않으나, 필요에 따라 인증을 수행함

③ 접근정책이 수립되어 있지 않으며, 인증을 수행하지 않음

19. 귀사에서는 전자결재 또는 전자상거래를 수행하고 있습니까?

① 예

② 아니오

19-1. 전자결재 및 전자상거래시 전송되는 정보에 대한 보안정책이 수립되어 있습니까?

① 전자결재 관련 보안정책과 지침이 수립되어 운영됨

② 보안정책은 없으나, 간단한 지침 등이 존재하여 필요시 적용

③ 전자결재 관련 보안정책이 수립되어 있지 않음

19-2. 전자결재 및 전자상거래시 전송되는 정보에 대해 암호화를 수행하고 있습니까?

① 모든 정보(일반 전자결재 서류 포함)에 대해 암호화를 수행

② 중요 정보(회계관련, 기밀자료 등)에 대해서만 암호화를 수행

③ 수행하지 않음

20. 이벤트 및 로그관리를 정기적 혹은 비정기적으로 수행하고 있습니까?

① 모든 개인 PC 및 서버, 보안장비에 대한 운영 로그를 관리 수행

② 중요 서버 및 보안장비에 대해 필요한 로그만을 관리

③ 로그관리 수행하지 않음

21. 서버 및 응용 소프트웨어, 보안장비 등의 시스템에 대한 주기적인 패치를 수행하고 있습니까?

① 정기적(주 1회 이상, 보안권고 발생시)으로 패치를 수행

② 보안권고 발생시 필요에 따라 패치를 수행

③ 패치를 수행하지 않음

21-1. 각종 바이러스 및 해킹으로부터 시스템을 보호하기 위한 취약성 점검을 수행하고 있습니까?

① 주기적(분기 1회 이상)으로 취약점 점검을 수행하고 있음

② 관리자의 필요에 따라 취약점 점검을 수행하고 있음

③ 취약점 점검을 수행하지 않음

보안수준 평가 : 유지보수 및 사고대응

22. 귀사 내 유지보수 대책 및 관리를 위한 규정을 수립하고 있습니까?

① 정기적인 유지보수를 위한 규정을 수립하고 권고하고 있음

② 필요 사항 발생시 규정을 유지보수하고 있음

③ 유지보수 대책이 없음

22-1. 유지보수 관리에 대해 기록하고 관리하고 있습니까?

① 유지보수 시기, 내용, 담당자 등 전반적인 부분을 기록함

② 유지보수 관리에 대한 변경사항만을 기록함

③ 유지보수 관리에 대해 기록하지 않음

23. 침해사고 예방 및 발생시 대응을 위한 대책 및 절차를 수립하고 있습니까?

① 비상연락체계와 대응절차가 존재하고 훈련을 실시함

② 대책 및 절차는 있으나, 훈련을 실시하지 않음

③ 침해사고 대책이 수립되어 있지 않음

23-1. 침해사고 발생 후 사고대응에 대한 기록을 관리하고 있습니까?

① 사고분석과 대응내용을 절차에 따라 기록함

② 사고대응에 대한 간단한 메모만을 기록함

③ 사고대응에 대해 기록하지 않음

24. 보안사고 발생시 업무연속성 지원대책 및 절차를 수립하고 있습니까?

① 업무연속성 지원대책과 절차를 수립하여 운영함

② 지원대책은 있으나, 구체적인 절차에 따라 운영하지 못함

③ 업무연속성 계획이 수립되어 있지 않음

보안수준 평가 : 데이터 보호

25. 귀사 내 데이터를 분류하고 관리하고 있습니까?

① 모든 데이터에 대한 분류를 수행하고 책임자에 의해 관리되고 있음

② 중요 데이터(기술개발, 회계자료 등)에 대한 분류만이 수행되고 있음

③ 데이터 분류를 수행하고 있지 않음

26. 데이터 백업을 수행하고 있습니까?

① 데이터 백업에 대한 규정에 따라 수행하고 있음

② 규정은 있으나, 수행하고 있지 못함

③ 백업을 수행하지 않음

26-1. 데이터 백업 기간 및 방법을 지정하고 있습니까?

① 데이터 백업 기간 및 방법이 지정되어 있음

② 지정되어 있지 않으나 관리자 임의로 수행하고 있음

③ 특별한 백업 기간 및 방법을 지정하고 있지 않음

27. 보안사고 발생시, 업무가 연속될 수 있도록 시스템의 대체장비를 가지고 있습니까?

① 모든 시스템에 대해 즉각 활용할 수 있는 대체장비를 보유하고 있음

② 중요 시스템에 대해서만 대체장비를 보유하고 있음

③ 대체장비를 보유하고 있지 않음

보안수준 평가 : 물리적 환경

28. 귀사 내 중요 정보를 보관한 장소 또는 사무실에 대한 물리적 시설을 보호하기 위해 출입통제 장치 및 시건장치를 사용하고 있습니까?

① 모든 기업내 장소에 대해 출입통제 장치 및 시건장치를 하고 있다.

② 특정 장소(서버실, 회의실, 중요 문서관리 등)에 대해 수행하고 있음

③ 특별한 출입통제 장치 및 시건장치가 없음

28-1. 물리적 시설에 대한 출입통제 기록이 작성되고 관리되고 있는가?

① 사무실 및 주요 장소에 대해 출입기록이 작성 및 관리되고 있음

② 주요 물리적 시설에 대해서만 출입기록을 작성하고 있음

③ 출입통제 내역을 기록하지 않음

29. 귀사 내 중요 정보를 저장한 매체에 대해 분류 및 라벨링, 폐기방법 등에 대한 사내 규정이 수립되어 있습니까?

① 중요도에 따라 저장매체의 분류 및 라벨링 규칙이 수립, 수행됨

② 명확한 규정은 없지만 중요도에 따라 라벨링을 수행하고 있음

③ 저장매체에 대한 분류 및 라벨링 규칙이 수립되어 있지 않음

29-1. 중요 매체(문서류, CD 등)의 폐기 및 사용일지를 작성, 관리하고 있습니까?

① 중요 매체 사용 여부 및 폐기일자 및 사유, 사용자 등을 기록, 관리함

② 관리일지가 명확한 형식없이 개인별로 작성하여 관리함

③ 매체에 대한 관리일지를 작성하지 않음

30. 귀사 내 소방장치(화재경보 센서, 소화기), 누수장치 및 UPS 등이 설치되어 있습니까?

① 소방장치(화재경보 센서, 소화기 등), 누수장치 및 UPS 등이 설치

② 소방장치(화재경보 센서, 소화기 등)만 설치되어 있음

③ 관련 장치를 설치하지 않음

30-1. 귀사 내 시설 및 장비(소방장치, 경보기, 조명, 온도 등 각종 장비)에 대한 책임부여 및 점검일지를 작성하고 있습니까?

① 책임자를 부여하여 관리하고 정기적으로 점검일지를 작성하고 있음

② 특정 책임자없이 사내인력으로 관리하며 점검일지는 작성하지 않음

③ 시설 및 장비에 대한 책임부여 및 점검일지를 작성하지 않음

중소기업 정보보호수준 자가측정 서비스 이용방법

1 한국정보보호진흥원 홈페이지(www.kisa.or.kr)에 접속한다.

2 홈페이지 우측 상단에 있는 로그인 버튼을 클릭하여 홈페이지에 회원가입을 한다.
※이전 측정결과와 비교하여 보안수준을 판단하기 위하여 회원가입을 해야 한다.

회원가입시, 아래의 박스에 체크를 하고 기업정보 입력해야 함.

□ 정보보호산업지원센터(LAB실, 회의실, 교육실), 중소기업 정보보호수준 자가측정도구를 이용하실 분은 왼쪽을 체크하여 주시고 아래 소속단체 정보를 반드시 입력하여 주시기 바랍니다.

3 로그인 후, 홈페이지 좌측 하단에 있는 '중소기업 정보보호수준 자가측정도구' 배너를 클릭한다.

4 웹페이지 하단의 'GO!'를 눌러 진단 웹페이로 이동한다.

자가측정 웹페이지로 이동 GO!

5 좌측 메뉴의 '측정하기'를 눌러 측정을 시작한다.

- 도구설명
- 측정하기
- 사용자 매뉴얼
- 이전 측정결과 보기

02

(주)인젠 컨설팅사업본부 김민수 본부장
mink@inzen.com

기업 보안정책 수립시 체크리스트

구 분	점검 항목	점검 내용
보안정책 및 조직	정보보호 정책서 작성 및 보유	정보보호 정책을 구현하기 위한 지침, 표준, 절차 등이 구현돼 있어야 함
	정보보호 정책 배포 및 교육	승인된 정책 및 지침이 모든 임직원에게 적절히 공표되고 교육돼 있어야 함
	정보보호 정책 검토	정보보호 정책은 정기적으로(혹은 중대한 변화가 발생할 경우) 검토하고 업데이트 돼야 함
	정보보호담당자	정보보호 활동을 계획, 실행, 검토하는 정보보호 담당부서 또는 담당자가 별도로 존재해야 함
	정보보호담당자 자격	정보보호관리자 또는 담당자는 충분한 보안기술을 보유하거나 보안관련 전문 자격증(CISA, CISSP 등)을 보유하고 있어야 함
	외부 전문가의 활동	주기적으로 외부 보안전문가에 의한 정보시스템 보안취약점 진단 및 이에 대한 평가를 받고 있어야 함
	정보보호에 관한 독립적 검토	정보보호의 통제목적/통제방안/정책/절차/처리 등 정보보호 관리와 이행에 대해 조직은 정기적으로 혹은 정보보호 구현에 중대한 변화가 발생할 경우 독립적(외부전문가 또는 내부 통제부서 등)으로 검토해야 함
	외부위탁 계약시 보안 요구사항	외부위탁 계약시 정보시스템/네트워크/인력/사무환경 등을 관리통제하기 위한 보안 요구사항을 계약서 상에 명시해야 함
	외부위탁 보안관리	외부 위탁업체 관리책임자로부터 보안관리 상황에 대해 주기적으로 보고받고, 수시점검 및 필요시 감사를 수행하고 있어야 함
	외부자 보안관리	정보시스템 및 관련 시설에 대한 제3자 또는 외부인의 접근을 통제해야 함

인적 보안	적격심사	직원 채용시, 신원/업무능력/교육정도/경력 등에 대한 적격심사가 이뤄져야 하며, 직원이 용역회사를 통하여 충원되는 경우, 용역회사의 계약서에 적격심사에 따른 책임사항이 명문화돼 있어야 함
	비밀유지 서약서	직원 최초 고용계약시, 비밀유지 서약서에 서명을 해야 함(임시직원이나 제3자에게 정보시스템에 대한 접근권한을 부여할 경우, 비밀유지에 관련된 사항이 계약서에 포함돼 있으며, 이에 대한 비밀유지 서약서를 받아야 함)
	정보보호 인지/교육/훈련	조직의 모든 직원들과 계약자, 제3자들은 적절한 인지훈련과 함께 업무기능과 관련된 조직의 정책과 절차에 대한 주기적인 업데이트를 받아야 함
	훈련 절차	보안위반 경험이 있는 직원들에 대한 정식 훈련절차가 있어야 함
	자산의 반환	직원/계약자/제3자는 그들의 고용/계약/협약의 종료와 함께 그들이 가지고 있던 조직의 모든 자산을 반환해야 함
	자산권리의 삭제	정보와 정보처리설비에 대한 모든 직원/계약자/제3자의 접근 권한은 그들의 고용/계약/협약의 종료 혹은 변경시 적절하게 삭제돼야 함
물리적 환경 보안	물리적 보안경계	정보와 정보처리 설비가 포함돼 있는 구역을 보호하기 위해 보안경계(벽/카드 출입구/인력배치 등)가 설치되어야 함
	물리적 출입통제	보안구역은 오직 허가받은 직원만 출입할 수 있도록 적절한 출입통제 수단에 의해 보호되어야 함
	외부적 환경적 위협에 대한 보호	화재, 홍수, 지진, 폭발, 폭동 그리고 기타 자연 재해나 인재에 의한 피해로부터의 물리적 보호방안이 설계되고 적용되어야 함
	보안구역 내 작업	보안구역 내 작업에 대한 물리적 보호와 가이드라인이 설계되고 적용되어야 함
	일반 접근/배송/하역 구역	배송 및 하역 구역과 비인가자가 접근할 수 있는 접근지점 통제, 허가받지 않은 접근을 방지하기 위해 정보처리 설비로부터 격리돼야 함
	장비설치 및 보호	장비는 환경적 위협, 위험요소, 비인가 접근을 감소시키기 위해 보호돼야 함
	케이블 보안	데이터와 정보 서비스를 지원하는 전력 및 통신 케이블은 차단 혹은 손상으로부터 보호돼야 함
	장비 유지보수	장비는 지속적인 가용성과 무결성을 보장하기 위해 올바르게 유지 · 보수돼야 함
	구역 외에서의 장비보안	장비가 조직내 구역밖에서 운영되고 있을 경우에도 조직내와 동일한 수준으로 보안위험을 대비해야 함
	사무실 보호	책상 위에 중요한 자료를 방치한 채로 오랜 시간 자리를 비우지 않도록 하는 정책이 있으며 준수되고 있는가? 컴퓨터에 중요한 화면을 띄워 놓고 이석하지 않도록 하는가?

정보시스템 운영	안전한 장비 폐기 및 재사용	중요 데이터나 정품 소프트웨어는 장비내의 매체가 폐기되기 전에 저장된 정보가 완전히 삭제되고 이에 대한 확인 및 점검이 수행돼야 함
	운영절차 문서화	운영지침 및 절차는 문서화돼 있으며, 다음과 같은 내용을 포함하고 있어야 함 – 정보처리 및 취급 요구사항 – 오류 및 예외사항 처리지침 – 예기치 않은 운영적 · 기술적 문제 발생시 비상연락망 – 시스템 문제 발생시 시스템 재동작 및 복구절차, 시스템 모니터링 방안
	직무분리	운영인력에 대한 책임과 직무분리가 정의돼 있어야 하며, 개발자와 운영자간, 혹은 운영자들간의 직무분리가 어려운 경우는 이에 대한 보완대책이 있어야 함
	개발/테스트/운영설비의 분리	개발 및 테스트 시스템이 운영 시스템이 분리되어 있어야 하며, 운영환경으로의 소프트웨어 이행은 통제된 절차에 의해 허가된 방식으로 이뤄지고 문서화되며 승인돼야 함
	네트워크 운영대책	네트워크 분리/접근권한 통제/책임 및 직무분리/원격접속 설비관리 등의 내용을 포함한 네트워크 운영절차 및 보안정책이 수립되고 이행돼야 함
	인터넷 접속관리	인터넷 연결시 네트워크 구성정책, 이메일/인터넷 사이트의 접속, 소프트웨어 다운로드 및 전송 등의 사용자 접속정책 등과 같은 인터넷 접속에 대한 정책이 수립돼 있어야 함
	침입차단 시스템 운영	인터넷의 연결은 침입차단 시스템에 의해 보호되고, 침입차단 시스템 등 보호장비를 우회한 인터넷 접속을 금지하고 있으며, 침입차단 시스템에는 최소한의 서비스만 적용하고 업무목적 이외의 기능 및 프로그램을 제거해야 함
	원격 운영관리	네트워크를 통해서 시스템을 운영하는 경우 시스템 관리는 특정 터미널을 통해서만 수행할 수 있도록 제한해야 함. 인터넷 등 외부망을 통해 내부 시스템을 관리하는 것을 금지하고, 부득이하게 허용할 경우, 강력한 사용자 인증, 암호 및 접근통제 기능을 설정해야 함
	이동매체의 관리	USB 메모리, 이동형 HDD, 기타 모바일 장비의 메모리장치 등 이동식 매체사용 금지. 필수불가결한 장비는 승인을 받고 통제해야 함
	매체의 폐기	매체 폐기절차가 수립되어 있어야 하며, 주요정보를 저장한 매체가 재사용될 경우, 데이터는 재사용되기 전에 완전히 지워져야 함
	자산목록	정보자산(하드웨어, 소프트웨어, 통신/네트워크, 데이터, 직원, 물리적 시설 등)은 조사돼 있어야 하고, 모든 주요 자산목록은 정리되고 유지돼야 함
	자산소유권	중요한 정보자산마다 소유자, 관리자, 사용자가 확인되고 관련 통제 유지를 위한 책임소재가 명시돼 있어야 함
	자산 라벨링과 처리	정보자산 분류기준에 따라 정보자산에 보안등급이 일관성 있게 부여돼 있으며, 물리적, 전자적 표시가 부착돼 있어야 함

정보시스템 운영	운영환경 이행보안	운영 프로그램의 수정권한이 적절하게 통제되고 있는가? 운영 시스템에는 실행 코드만 존재하는가? 시험이 성공적으로 완료되고 사용자가 최종 인수를 승인한 후에만 실행 코드가 수행되는가?
	시험 데이터의 보안	시험 데이터가 운영 데이터에 준하여 보호하고 통제되는가? 운영환경에 적용하는 접근통제 절차를 시험환경에도 적용하는가? 운영 데이터가 시험환경으로 복사될 경우, 인가절차를 수립하여 이에 따라 수행하고 있는가? 시험완료 후 운영 데이터를 시험 시스템에서 삭제하는가?
	소스 프로그램의 접근보안	소스 프로그램은 실제 운영환경에 보관하지 않는 것을 원칙으로 하고 있는가? 소스 프로그램과 목적, 프로그램간의 버전관리가 일관성 있게 수행되는가? 소스 프로그램 관리자가 운영시스템별로 지정되는가? 소스 프로그램에 대한 접근통제 절차를 수립하고 이행하는가?
	시스템 문서화 보안	시스템 운영문서는 허가받지 않은 접근으로부터 보호돼야 함 보안절차, 운영매뉴얼, 운영기록 등의 시스템 문서의 목록이 작성되어 있고, 이에 대한 사용/복사 등의 접근내역이 관리되어야 함
외부연계	정보교환 정책 및 절차	공식적인 교환 정책, 절차, 통제는 모든 형태의 통신시설의 사용을 통한 정보의 교환을 적절하게 보호하고 있어야 함
	교환 협약	조직내 혹은 외부 기관과 정보 및 소프트웨어 교환을 위한 협약이 수립돼야함
	이동 중인 물리적 매체	정보를 포함하고 있는 매체는 조직의 물리적 경계를 넘어서는 이동중에 허가받지 않은 접근/오용/손상으로부터 보호하고 있어야 함
	전자상거래	전자 금융거래에 대해 인증 시스템을 통해 거래 당사자의 신원을 확인하고, 거래당사자를 제외한 열람이 불가능하도록 암호화해야 함
	온라인 트랜잭션	온라인 트랜잭션에 포함된 정보는 불완전한 전송, 잘못된 라우팅, 허가받지 않은 메시지 변경 및 노출, 메시지 복사, 재전송 등을 예방해야 함
	공개 서버 관리	공개 서버는 내부망과 분리하여 설치되며, 침입차단 시스템 등에 의해 보호되는 등의 네트워크 보호대책이 수립되고 운영돼야 함
	네트워크 서비스 사용 정책	사용자들은 특별히 사용이 허가된 서비스들에 대한 접근만 할 수 있어야 함
	외부 연결을 위한 사용자 인증	원격 사용자에 의한 접근을 통제하기 위한 적절한 인증방법이 사용돼야 함
	원격 운영관리	네트워크를 통해서 시스템을 운영하는 경우, 시스템 관리는 특정 터미널을 통해서만 수행할 수 있도록 제한되는가? 인터넷 등 외부망을 통해 내부 시스템을 관리하는 것을 금지하고, 부득이하게 허용할 경우 강력한 사용자 인증, 암호 및 접근통제 기능을 설정하는가?

보안운영	네트워크 상에서의 분리	정보서비스, 사용자, 정보시스템 등의 그룹들은 네트워크 상에서 서로 분리돼야 함
	네트워크 연결 통제	조직의 경계를 넘나드는 공유 네트워크의 경우, 네트워크에 연결하는 사용자들의 권한은 접근통제 정책과 업무 애플리케이션의 요구사항 등에 따라 제한돼야 함
	사용자 확인 및 인증	모든 사용자들은 각자 개인 용도의 유일한 ID를 가지고 있어야 하며, 사용자 신분을 입증할 수 있도록 적절한 인증기술이 마련돼야 함
	패스워드 관리 시스템	패스워드 관리 시스템은 상호작용해야 하며 안전한 패스워드를 보장해야 함
	세션 타임아웃	비활성화 세션은 허용된 비활성화 시간이 지나면 닫혀야 함
	연결시간의 제한	매우 중요한 애플리케이션에 대한 연결시간 제한이 사용돼야 함
	정보접근 제한	정보 및 응용프로그램 기능의 접근이 접근통제 정책에 따라 제한되고 있어야 함
	민감한 시스템 분리	민감한 정보를 처리하는 시스템은 전용의 또는 분리된 컴퓨팅 환경에서 수행돼야 함
	모바일 컴퓨팅 및 통신	이동 컴퓨터 보안에 대한 다음과 같은 정책이 수립되어야 함 – 이동 컴퓨터의 사용 – 물리적 보호/접근제어/암호화/백업/바이러스 정책 – 내부 네트워크와의 연결 이동 컴퓨터로 부터 공공망을 통해 내부 네트워크 접속시 적절한 인식/인증/접근통제 대책(VPN 등 포함)이 수립돼 있어야 함
	원격작업	원격작업을 통해 내부 시스템 접근시 관련 식별/인증/접근통제 대책이 수립돼야 하고, 재택 근무의 물리적 보안환경이 구축돼야 함
	보안 요구사항 분석 및 명세	신규 정보시스템 혹은 현존하는 정보시스템의 향상안에 대한 업무 요구사항 문서는 보안통제를 위한 요구사항들을 서술하고 있어야 함
	정보보안 이벤트 보고	정보보안 이벤트는 가능한 신속히 적절한 관리 채널을 통해 보고돼야 함
	보안 취약점 보고	정보시스템과 서비스를 사용하는 모든 직원과 계약자, 제3자는 시스템이나 서비스에서 관찰되거나 의심되는 어떠한 보안 취약점이라도 알리고 보고할 수 있는 대응체계가 구축돼야 함
	책임과 절차	경영진의 책임과 절차는 정보보안 사고에 대하여 신속하고 효과적이며 질서정연하게 대응할 수 있도록 수립돼야 함
	정보보안 사고로부터의 습득	정보보안 사건의 형태와 범위, 비용 등을 정량화하고 모니터할 수 있는 메커니즘이 존재해야 함
	증거 수집	정보보안 사고 후 사람 및 조직에 대한 대응 조치는 민형사상 법적 조치를 포함하기 때문에 증거가 수집, · 유지되고, 관할 사법권 규정대로 증거에 관한 규칙에 따르도록 제공돼야 함

보안운영	적용 가능한 법률 확인	모든 관련 법령, 규정, 계약상 요구조건, 이러한 요구조건들을 만족시키기 위한 조직의 접근방법 등이 명확하게 정의되고, 문서화되고, 각각의 정보시스템과 조직에 대해 항상 갱신, 유지돼야 함
	정보처리 설비의 오용 예방	사용자들이 허가받지 않은 목적을 위한 정보처리 설비 사용을 금지해야 함
	기술적 준수 검사	정보시스템들은 보안이행 표준을 준수하기 위하여 정기적으로 검사돼야 함
	정보시스템 감사 통제	감사 요구사항과 운영 시스템들에 대한 검사를 포함하는 활동은 신중하게 계획되고 업무 프로세스에 대한 중단 위험을 최소화할 수 있어야 함
	보안감사 계획 및 이행	정보보호 감사에 대한 정책 및 공식적인 계획이 수립돼 있고 계획에는 대상, 범위, 주기, 방법, 절차, 감사자, 감사도구 등이 포함돼 있어야 함. 정보보호 감사조직이 적절하게 구성돼 있고, 정보보호 감사인력에 대한 자격요건이 정의돼 있으며, 감사인력이 독립성 및 전문성을 보유하고 있어야 함 정보보호 감사는 정기적으로 수행되어야 함
	감사결과 및 사후관리	감사결과에 따라 감사보고서가 작성돼 있으며, 감사결론을 위한 증거가 충분히 뒷받침돼야 함 감사결과를 경영진에게 보고하는 보고 프로세스가 존재하며 이에 따라 적정한 책임자에게 보고가 이루어지고 있어야 함 감사결과에 따른 지적사항이 이행되도록 사후관리가 이루어지고 있어야 함
	감사 로깅	활동, 예외, 정보보안 이벤트 등을 기록하는 감사 로그가 생성돼야 하며 향후 발생하는 조사활동과 접근통제 모니터링에 활용 가능하도록 정해진 기간 동안 보관돼야 함
	시스템 사용 모니터링	정보처리 설비의 사용을 모니터링하는 절차가 수립돼야 하며 모니터링 활동의 결과는 정기적으로 검토되어야 함
	로그 정보 보호	로깅 시설과 로그 정보는 무단변조 허가받지 않은 접근으로부터 보호돼야 함
	관리자와 운영자 로그	시스템 관리자와 시스템 운영자의 활동은 로깅돼야 함
	실패 로그	실패 항목은 로깅/분석돼야 하고 이에 대한 적절한 대응이 이뤄져야 함
	사용자 등록	공식적인 사용자 등록/해지를 위한 계정관리 절차를 수행하고 있는가? 사용자는 유일한 식별자를 가지고 그룹명은 적절한 명명규칙을 따르고 있는가? 사용자 계정생성 및 권한부여 절차가 한 사람이 모두 수행하지 못하도록 적절히 직무분장돼 있으며, 사용자 권한변경의 기록을 별도로 검토하고 있는가?
	특권 관리	시스템 관리자/DBA와 같은 특별권한 할당/사용이 통제되는가?
	사용자 패스워드 관리	사용자 패스워드 관리절차가 존재하고 이에 따라 이행되고 있는가? – 안전한 패스워드 사용기준/초기 패스워드 할당 후의 변경/패스워드의 암호화/패스워드의 재발급 등
	사용자 접근권한 검토	접근통제 정책 및 절차에 의해 결정된 접근권한을 적절히 반영한 접근통제 방법이 있고 이를 적절히 운영하고 있는가?

03

(주)시큐브 정보보호기술 전임연구원 이진명
(주)안철수연구소 컨설팅서비스 사업부 이현수 전임 컨설턴트

네트워크 관리자 체크리스트

구 분	점검 항목	점검 내용
관리규정 점검	정보보호 관리규정 제정 및 준수	• 보안조직의 구성, 자산의 분류 및 통제, 인적 보안 지침, 사용자 교육 지침, 정보보안 사고 대응절차 등 정보보호정책 및 지침을 마련해 전 직원과 공유하고 보안감사 활동의 수행하는가?
	정보보호 전담조직(정보보호책임자 등) 구성 및 운영	• 정보보호 전담조직을 구성해 최고 경영진 직속의 형태로 운영하는가? • CSO를 별도로 두고 정보보안을 위해 외부기관과 협조체계를 구성하는가?
	정보보호교육 실시	• 임직원을 대상으로 정보보호에 대한 교육을 실시하는가? • 정보보호 전담인력은 전문 교육을 주기적으로 받는가?
제품 점검	정보보호제품 구축현황 및 운영	• 정보보호 시스템을 구축하고 운영사항을 정기적으로 모니터링하며 최신 패치를 유지하도록 관리하는가?
	서버 및 PC 등의 백업 및 패치	• 중요한 서버에 대해 주기적인 백업을 실시하는가? • 서버, DB 및 네트워크 장비 및 시스템에 대한 최신 패치를 정기적으로 설치하는가? • 주요 서버에 대한 로그 관리(기록 및 분석)를 수행하는가?
Network 점검	불법적인 네트워크 접근 및 경로에 대한 감시 · 통제	• 정보시스템에 대한 보안 취약성을 정기적으로 점검하고 외부에서 내부로의 네트워크 접근을 통제하기 위한 DMZ를 구성했는가? • 네트워크 트래픽 모니터링을 위한 도구를 마련하여 보안에 활용하고 네트워크 흐름을 통제하기 위한 절차나 방안을 수립해 시행하고 있는가?

보안 점검	사용자 보안대책	• 중요 서버의 패스워드를 정기적으로 변경하는가? • 내부 사용자 PC 보안을 위한 정보보호 가이드를 제정해 운영하는가? – 부팅 및 화면보호 – 파일 공유 비밀번호 설정 – 안티바이러스 및 복구솔루션 설치 – PC 방화벽 설치 – 중요 자료 백업 – PC의 취약점 패치 등
	CPU 점유율 확인	• 장비의 CPU 점유율이 높지는 않는가?
	Public SNMP Community	• Snmp Community가 Public으로 돼 있지 않은가?
	MRTG 그래프 확인	• SNMP를 이용해 트래픽 그래프를 정기적으로 생성해 확인하는가?
	QOS 설정 여부	• QOS 설정은 추가 할 것이 없는가?
	Netbios 필터	• Netbios 패킷을 차단하고 있는가?
	펌 웨어 업그레이드	• 장비의 보안취약점에 대한 최신 패치가 적용돼 있는가?
	로그인 내역확인	• 모르는 접근이 있지는 않는가?
	로그 용량 확인	• 로그 용량이 지나치게 크지 않는가?
	저장공간 확인	• 로그의 저장공간은 충분한가?
사고 예방	주요 데이터 보호대책	• 주요 데이터 암호화 등의 보안대책과 중요 정보의 저장매체에 대한 폐기 절차를 수립, 시행하는가?
	해킹, 침해사고 등에 대한 정보 획득	• 해킹 및 침해 사고가 발생하는 즉시 통고받을 수 있는 정보 획득 채널을 확보하고 국내외 해킹 및 보안사고에 대한 주기적인 모니터링을 수행하는가?
	침해사고 해결방안 및 후속 조치	• 침해사고 발생에 대처하기 위한 긴급연락체계를 구축하고, 사고처리가 종결된 후 이에 대한 정밀한 분석과 재발 방지를 위해 IT 아웃소싱 구현방법 및 사례연구 방지대책을 수립하는가?

04

인포섹(주) 기술팀 이준희 과장
joonhlee@skinfosec.co.kr

웹 방화벽 체크리스트

구 분	점검 항목	점검 내용
성능 점검	웹 방화벽 성능 점검	장비 기본성능 측정
		HTTP 처리 능력
	보호기능 점검	사용자 요청 검사/서버 컨텐츠 보호기능/학습기능/서버정보 위장
취약점 점검	XSS 취약점	세션 정보 노출 또는 임의 명령 실행
	SQL Injection 취약점	악의적인 쿼리 또는 시스템 실행
	디렉토리 인덱싱	디렉토리 정보 파악 및 서버 정보 획득
	쿠키 스니핑/조작 가능성	쿠키 조작을 통한 권한상승 또는 데이터 조작
	백업 파일	하드코딩된 정보의 노출 또는 시스템 정보 노출
	디폴트 페이지	취약한 초기 디폴트 취약점에 의한 정보 노출
	에러페이지 미비(404, 500)	서버 시스템 정보노출 및 에러 정보 획득
	서버 설정 취약점(http method)	서버 설정 오류를 이용한 권한 획득
	버퍼 오버플로우 취약점	권한 획득 및 예외 상황 발생
	웹 서버 정보 노출 취약점	http header 를 통한 서버 정보 획득
	파일 업로드	파일 업로드 ACTION URL 정보

취약점 점검	파일 다운로드	파일 다운로드 절대 경로 정보
	사용자 개인정보 노출 취약점	개인정보가 노출되는 페이지
	파라미터 변조 취약점	연속되거나 추측 가능한 파라미터 Value 조작에 의한 정보 요청
	주석 정보 노출 취약점	취약한 주석이 노출되고 있는 특정 페이지
	URL 강제 접속	시작, 진입, 최종 URL 설정
	취약한 패스워드	회원가입, 비밀번호 변경 기능의 URL 및 파라미터 정보
	관리자 페이지 IP 접근제어 설정	IP 접근제어 설정을 위한 디렉토리 정보
	인증 우회	취약한 인증방식으로 상황에 따른 정보
	히든필드 점검	Hidden Field Value가 유지돼야 하는 페이지(전, 후)
	DOS 공격 취약점	특정 IP에 대한 과다 요청 제어
	과다 요청 취약점	알려진 웜바이러스 시그니처 탐지
관리기능 점검	접근기록	접근기록이 남는가? 지원 로그 포맷의 종류는? Log 서버로의 전송이 가능한가? (전송 방식 지원)
	차단 로그 이해의 편의성	로그 형식은 이해하기 쉽게 정리되었는가? 세밀한 로그 보기가 가능한가? 조건별로 검색이 가능한가?
	로그 유지	최대 보존기간 설정이 가능한가? 로그는 자동 백업이 될 수 있는가?
	보고서	필요시 보고서 생성이 가능한가? 필터링에 의해 필요한 보고서만 작성이 가능한가? 다양한 형식(Word, Excel등)을 지원하는가?
	정책관리	예외처리 기능이 존재하는가? Application별 다른 정책설정이 가능한가? 사용자정의 정책 작성이 가능한가? 탐지, 방어정책 혼용이 가능한가? 정책 Roll-Back 기능을 사용할 수 있나?
	학습기능	신뢰 호스트만 학습 가능한가? 보안정책 변경 내용을 기록할 수 있나? 자동 학습기능이 지원되는가?
	기타	UI 자체의 보안 UI는 어떤 방식으로 구현되었는가? 별도의 관리용 인터페이스를 제공하는가?

05

(주)시큐브 정보보호기술연구소 전임연구원 이진명
hubgo@secuve.com

웹 관리자 체크리스트

구 분	점검 항목	점검 내용
웹 서비스 점검	웹 서버 실행 권한	Web 서버가 Nobody 권한으로 실행되고 있는가?
	CGI 보안	취약한 cgi 프로그램은 존재하지 않는가?
	관리자 페이지 인증	관리자 웹 페이지는 인증으로 보호되는가?
Upload/Image 디렉토리 취약점	웹 페이지 존재여부	웹 페이지가 올라와 있는가?
	업로드 파일 비교	업로드 하지 않은 파일이 존재하는가?
	업로드 퍼미션	업로드 한 파일에 실행권한이 부여된 것은 없는가?
패치 적용	웹 서버 보안 패치	웹 서버의 최신 보안 패치는 적용돼 있는가?
	게시판 보안 패치	게시판에 사용된 보안 취약 언어는 없는가?
	WAS 보안 패치	WAS의 최신 보안 패치가 적용되어 있는가?
로그 분석	로그 통계확인	특정 IP에서만 많은 접속이 있는가?
	로그 용량 확인	로그 용량이 지나치게 크지 않은가?
	저장공간 확인	로그의 저장공간은 충분한가?

06

(주)시큐브 정보보호기술연구소 전임연구원 이진명
hubgo@secuve.com

서버보안 관리자 체크리스트

구 분	점검 항목	점검 내용
사용자계정 정책	보안상 취약한 계정	패스워드가 없는 계정, 특별 계정들은 없는가? 서비스되고 있지 않은 ftp, uucp 계정을 유지하고 있는가?
	루트 권한의 유저 존재 여부	/etc/passwd 에서 UID가 0인 유저가 존재하는가? /etc/passwd 에서 GID가 0인 유저가 존재하는가?
	Default Vender Accounts 관련	/etc/passwd에서 보았을 때, Default vender Accounts인 sys, bin 등에 shell이 부여되어 있는가?
	C2 Level 적용 여부	/etc/passwd 파일에서 유저들의 패스워드 항목이 암호화 되어 있고, /etc/shadow 파일이 존재하는가?
	Password 취약성	패스워드는 최소 6자 이상으로 설정되어 있는가? 추측하기 쉬운 패스워드로, Crack에 취약한 패스워드가 존재하는가?
Tcp/Wrapper	/etc/hosts.deny	파일 내용을 "ALL:ALL"로 구성, 불필요한 모든 서버로부터의 접근거부를 하는가?
	/etc/hosts.allow	꼭 필요한 Administrator 또는 Manager에게만 접근권한을 주도록 되어있는가? /etc/hosts.allow Permission이 600인가?
/etc/inetd.conf	파일 Permission	Permission이 600인가?
	'r' command 사용 여부	Shell, login, exec를 #으로 remark하였는가?

/etc/inetd.conf	rpc daemon 사용 여부	sadmin, ttdb, cmsd 등의 보안에 취약한 rpc daemon들을 #으로 remark 하였는가?
	Tftp 사용 여부	Tftp(Trivial FTP)가 #으로 remark되었는가?
	DoS 공격에 취약한 서비스 사용여부	echo, discard, daytime, chargen가 #으로 Remark되었는가?
	기타 불필요 서비스 사용 여부	불필요한 서비스가 Remark되었는가?
ftp 설정상태	Version	보안에 취약한 Version은 아닌가?
	TCP/Wrapper적용	TCP/Wrapper에 의해 원격으로 부터의 FTP 접속을 제한했는가?
	ftp user	ftp 유저의 홈디렉토리가 루트 소유인가? Anonymous ftp 서비스가 제공되지는 않는가? ftp account의 login shell이 /bin/false인가? /etc/ftpusers 안에 root, bin, uucp, ingress, daemon, news, nobody, ftp, anonymous 등의 vendor가 지원하는 Default User들을 등록했는가?
System Trust 관계	/etc/hosts	불필요한 시스템이 포함되어 있지 않은가?
시스템 Start-up 관련 파일 접근권한	/etc/rc*	Perm : 755 이하
	/etc/init.d	Perm : 755 이하
기타 보안관련 설정상태	Patch 상태	Patchdiag를 이용, 최신 보안 패치 적용 여부 점검
불필요한 파일 존재 여부	보안상 취약하거나 의심스러운 루트 권한의 suid bit가 설정된 파일이 없는가?	Setuid bit가 설정된 파일의 조사
불필요한 NFS의 사용 여부	불필요하거나 민감한 directory가 외부로 mount가 가능하지 않은가?	showmount-e
해킹 흔적이 존재하는가?	로그 파일 분석	messages/sulog/lastlog/xferlog/lastcomm

사내 PC 관리담당자가 점검해야 할 체크리스트

1	중요 서버의 데이터에 대해 정기적인 백업 시스템을 갖춘다.
2	모든 클라이언트 시스템에 백신 및 PC 보안제품을 설치한다.
3	파일서버, 메일서버, 그룹웨어 서버에도 모두 보안솔루션을 설치하여 관리한다.
4	보안솔루션을 모두 최소 1주일에 한 번 이상 정기적으로 엔진 업데이트한다.
5	사내 악성 프로그램 유입 및 전파시 신속한 감염 시스템 파악을 위해 시스템에 고정 IP를 부여하여 관리한다.
6	방화벽 설정을 통해 불필요한 포트는 모두 막는다.
7	사내 보안지침 문서를 구비한다.
8	사내 보안지침을 위반하여 회사에 피해를 입혔을 경우에 대한 인사조치 사항 등을 사내 보안 지침 문서에 명기한다.
9	전 직원을 대상으로 정기적인 보안교육을 실시한다.
10	정기적으로 사내 보안감사를 실시한다.
11	정기적으로 보안관련 사이트를 방문하여 최근 보안정보를 확인한다.
12	보안 취약점 발표시 패치 적용에 대한 공지를 그 날 안에 클라이언트에게 전달하고, 클라이언트의 패치 적용 여부가 관리자에게 전달되도록 시스템을 구축한다.
13	새로운 보안문제 발생시 직원들이 적절히 대응할 수 있도록 대응지침이 신속하게 전달되는 체계를 갖춘다.
14	외부에서 반입되는 시스템에도 사내 보안지침을 적용한다.
15	연휴 때는 사용하지 않는 모든 시스템의 전원을 끈다.

07

인포섹㈜ 보안연구센터 홍진기 이사
jkhong@skinfosec.co.kr

PC 보안 체크리스트

보안정책은 엔드 포인트 보안으로 끝난다고 해도 좋을 만큼 사용자의 PC 관리는 보안시스템에서 매우 중요한 요소가 되고 있다. PC 보안은 기업 전체 시스템 보호를 위해서도 중요하지만, PC를 이용하는 개인의 피해를 예방할 수 있어 중요하다. 자신의 정보를 보호하고, 더불어 회사 시스템을 보호하기 위해 지켜야 할 기본적인 수칙을 알아본다.

어느 날 갑자기 신용카드 연체 통보가 날아왔다. 은행 잔고를 확인하니 '0' 이었다. 휴대폰의 스팸성 문자메시지도 부쩍 늘었다.

스팸메일 한 번 잘못 클릭하면 이런 피해를 입게 될 수 있다. 거래처를 가장한 스팸메일을 잘못 열었다가 개인정보를 빼내는 웜에 감염되어 윈도우 업데이트나 바이러스 백신 검사를 해보지 않았던 PC에 들어있는 정보가 줄줄이 새어나가 은행 통장의 잔고는 '0' 이 되고 복제 휴대폰으로 인한 피해를 비롯하여,대출관련 전화를 비롯한 온갖 스팸 문자메시지에 시달리게 된다. 이런 피해사례를 들으면 PC의 인터넷을 끊어버리고 싶은 생각이 들게 마련이다. 또한, 시중 은행 인터넷 뱅킹을 가장한 피싱사이트에서부터 은행이나 게임 사이트의 온라인 거래를 통해 개인정보가 빠져나가기도 한다. PC 관리를 잘 한다고 자부하는 사람들도 피해에서 자유롭지 못하다. 스패머들은 어떻게든 보안 취약점을 찾아

내기 마련이다.

정보보호는 기업에만 한정된 것이 아니다. 개인의 사생활과 재산보호를 위해 개인정보보호에도 관심을 기울여야 한다. 가장 취약하기 쉬운 개인 PC의 정보보호는 어떻게 할까. 전문가들이 제안하는 'PC 안전하게 관리하는 방법'을 참고해 PC 안전성을 점검해보자.

개인 정보보호 체크리스트

1. 윈도우 운영체계는 최신 보안 패치를 모두 적용한다.
2. 인터넷 로그인 계정의 패스워드를 자주 변경하고, 영문/숫자/특수문자 조합으로 6자리 이상으로 설정한다. 로그인 ID와 패스워드를 동일하게 설정하지 않는다.
3. 해킹, 바이러스, 스파이웨어 등을 종합적으로 막아주는 V3 같은 통합보안 제품을 하나 정도는 설치해둔다. 설치 후 항상 최신 버전의 엔진으로 유지하고 부팅 후 보안제품이 자동 업데이트되도록 하고, 시스템 감시기능이 항상 작동하도록 설정한다.
4. 웹 서핑시 '보안경고' 창이 뜰 경우에는 신뢰할 수 있는 기관의 서명이 있는 경우에만 프로그램 설치에 동의하는 '예'를 클릭한다. 잘 모르는 프로그램을 설치하겠다는 경고가 나오면 '예' '아니오' 중 어느 것도 선택하지 말고 창을 닫는다.
5. 이메일 확인시 발신인이 불분명하거나 수상한 첨부 파일이 있는 것은 모두 삭제한다.
6. 메신저 프로그램 사용시 메시지를 통해 URL이나 파일이 첨부되어 올 경우에는 메시지를 보낸 이가 직접 보낸 것이 맞는지를 먼저 확인하고 실행한다.
7. P2P 프로그램 사용시 파일을 다운로드할 때에는 반드시 보안제품으로 검사한 후 사용한다.
8. 정품 소프트웨어를 사용한다. 인터넷을 통해 불법 소프트웨어를 다운로드해 설치하는 경우, 이를 통해 악성 코드가 설치될 가능성이 높다.
9. 중요한 자료를 주기적으로 백업해 만일의 상황에 정보를 잃는 일에 대비한다.

온라인 금융 및 게임 사용시 개인정보 유출 예방 수칙

1. 온라인 게임 계정 정보를 외부에 공개하지 않는다. 특히, 게임 관리자 또는 업체를

사칭하는 사람에게 게임 계정을 알려주지 말아야 한다. 게임 운영자는 사용자에게 계정 정보 등의 개인 정보를 요구하지 않는다.

2. 온라인 게임에 접속할 때는 일정한 장소에서 한다. 게임방 등과 같이 불특정 다수가 컴퓨터를 사용하는 장소에서 계정 정보 유출 등의 문제가 많이 발생하므로 가능한 한 일정한 장소에서 게임을 하는 것이 좋다.
3. 온라인 게임 해킹 툴을 사용하지 말아야 한다. 인터넷에서 구할 수 있는 온라인 게임 해킹 툴을 통해 악성코드에 감염될 수 있으며, 이를 통해 계정정보 등이 외부로 유출될 수 있다.
4. 의심스런 웹사이트에 정보를 입력하지 말아야 한다. 온라인 게임 관련 홈페이지로 위장한 가짜 홈페이지를 통해 계정정보 등이 유출되는 사고가 발생하고 있다. 의심스런 웹사이트에는 정보를 입력하지 말고 해당 게임 업체로 문의해 확인한다.
5. 금융거래를 공공장소에서 하지 말아야 한다.
6. 금융 거래용 공인인증서는 USB 같은 별도 저장매체에 저장한다.

피싱 사이트와 정상 사이트 구분하기

1. 정상적인 인터넷 뱅킹 사이트는 공인인증서 비밀번호, 계좌비밀번호, 보안카드 비밀번호 등 개인정보를 여러 창에 걸쳐 입력하게 돼 있지만, 피싱 사이트는 한 화면에서 동시에 입력하도록 돼 있다.
2. 이체거래 때 정상 사이트는 화면상에 자신의 출금계좌번호를 선택하게 돼 있지만, 피싱 사이트는 이용자가 직접 입력하도록 돼 있다.
3. 정상 사이트는 로그인 절차(ID 및 패스워드 또는 공인인증서 입력)를 거쳐야 인터넷 뱅킹 화면이 나타나는 반면, 피싱 사이트는 화면 상의 주소창에 은행주소만 치면 바로 화면이 나타난다.
4. 정상 사이트는 보안카드 비밀번호 2자리를 2회만 입력하도록 요구하나, 피싱 사이트는 그 이상의 자릿수 및 횟수를 입력하도록 요구한다.
5. 정상 사이트는 공인인증서 비밀번호 입력시 별도의 인증서 선택창이 뜨지만, 피싱 사이트는 화면에서 직접 입력하게 돼 있다.

분 류	점검 항목
윈도우	• 최신의 서비스 팩과 핫픽스가 설치돼 있다. • 새로운 Windows Update는 최소한 한 달 주기로 업데이트 한다. • 로그인 암호는 8자리 이상 영문과 숫자 혼용으로 이용한다. • 로그인 암호는 최소 한 달에 한 번 변경한다. • CMOS 패스워드를 설정했다. • 화면보호기 암호를 설정했다. • 공유 폴더 이용시 패스워드를 설정했다. • 관리 공유 폴더를 제거했다. • Windows 방화벽 기능을 설정하여 사용하고 있다.
파일	• NTFS를 사용하여 사용자별로 접근을 제한하고 있다. • 중요 데이터는 원격지에 백업돼 있다. • 필요한 경우 파일을 암호화하여 저장하고 있다.
애플리케이션	• 인터넷 옵션의 보안설정을 보통 이상으로 설정했다. • ActiveX 관련 설정을 올바르게 설정했다. • 자동 완성기능을 사용하지 않도록 설정했다. • '개인 정보' 탭의 보안수준을 '보통 이상으로 설정했다. • 웹메일의 경우, 보안접속 기능을 사용하여 로그인한다. • 아웃룩 익스프레스에서 '사용할 IE' 의 보안영역을 '제한된 사이트 영역' 으로 설정했다. • 바이러스 확산 방지를 위한 수칙을 알고 있으며 지키고 있다. • 백신을 이용하여 첨부파일을 매번 검사하고 있다. • 메신저 사용중 알 수 없는 곳에서의 파일 수신을 한 적이 없다. • P2P 사용시 환경설정을 재설정한다. • 실시간 감시/자동 업데이트/E-mail 감시기능을 설정해 사용하고 있다.
안티바이러스	• PC용 방화벽을 설치해 사용하고 있다. • 아웃룩 등 메일 클라이언트 프로그램 사용시 미리보기 기능을 사용하지 않는다.
메일	• 메일 클라이언트 프로그램의 기능을 활용해 '광고' 등 기본적인 필터링을 설정하고 있다. • 발송자가 불분명한 곳에서 온 메일을 열지 않고 삭제한다. • 발송자가 불분명한 곳에서 온 메일의 첨부 파일을 열지 않고 삭제한다. • 발송자가 불분명한 곳에서 온 광고메일을 통해 물건을 구매하지 않는다. • 인터넷 상에서 신뢰할 만한 사이트가 아닌 곳에 자신의 이메일 주소를 남기지 않는다. • 원하지 않는 광고 메일에 대해 수신거부 의사를 전달하지 않는다. • 원하지 않는 휴대폰 문자광고에 대해 해당 이동통신 서비스 회사에 차단을 요청한다. • 인터넷 사이트 이용시 광고 프로그램 설치에 동의하지 않는다. • 불법 스팸메일에 대해 불법스팸대응센터(www.spamcop.or.kr)에 신고한다.

정보통신부가 매년 말 실시하는
기업 정보보호 대상을 수상한 기업에는 공통점이 있다.
사업 확장과 함께 글로벌화에 성공하면서
정보보호 정책을 강화했다는 것이다.
성장가도를 달리고 있는 기업들이
정보호호에 눈을 돌린 이유는 무엇일까?
2006년 정보호호 대상 수상기업의
사례를 통해 그 이유를 알아본다.

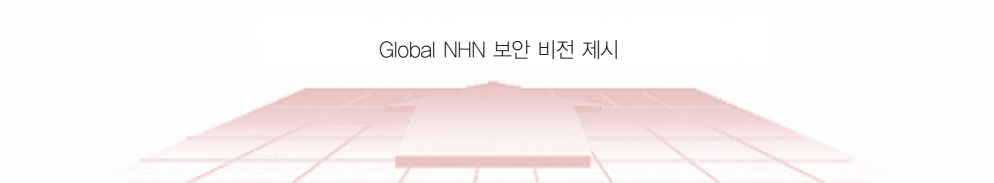
잘 나가는 기업은 정보보호 정책부터 다르다

01

NHN 보안실 나윤성
skyhawk@nhncorp.com

글로벌 NHN의 효율적인 정보보호 방법론

2006 정보보호 대상을 수상한 NHN은 통일된 보안체계를 확립하고, 지속적인 변화로 보안 프로세스를 확립해 기업 정보보호에 앞장서 왔다. 이를 위해 NHN은 보안 정책 · 지침 프로세스 'NGSS'를 제시하고, 전 직원을 대상으로 '시큐리티 및 프라이버시 더블 세븐 원칙'을 교육하고 있다.



[그림 1] Global NHN 보안 비전

NHN㈜은 내부 조직의 급속한 변화 · 확대와 함께 일본, 중국, 미국 등 해외 진출을 통한 사업의 글로벌화를 진행하고 있다. 이에 따라 웜, 바이러스, 해킹, 명의도용, 전자문서 변조 등 각종 보안사고 위협, 고성장에 대한 위험을 조기에 파악하거나 관리할 수 있는 국제수준의 위험관리 체계가 필요하게 되었다. 'Global NHN'을 위한 필수요건인 보안정책 수립을 위해 NHN은

- 통일된 보안체계 수립
- 지속적인 변화 관리
- 보안 프로세스 확립

등을 제시하고 있다. 이를 통해 대내 · 외 각종 위협과 취약성 및 자산에 대한 조화로운 관리체계에 정보보안 프로세스를 적용하고 있다.

위험관리 보안 표준, NGSS로 안전한 서비스 제공

글로벌 보안 비전 달성을 위해 NHN은 보안정책과 지침을 마련하고 위험관리 조직을 강화하며, 프로세스 및 기술보안 체계를 설계하여 위험관리 시스템과 프로세스를 구축하고 있다. 이를 위해 NHN은 'NGSS(NHN Global Security Standard)'라는 위험관리를 위한 보안정책과 지침, 프로세스 표준을 수립하고 공표하였다. NGSS는 NHN 고객들에게 안전하고 신뢰할 수 있는 서비스를 제공한다는 목표 아래 정보보안 위험관리와 조기정보 체계를 갖추고, 개인정보 침해 모니터링 시스템을 설계 운영하였다.

[그림 2] Global NHN의 보안 위험관리 체계

또한, 조직적인 보안관리 체계와 함께 직원들의 보안의식 강화를 위해 '시큐리티 및 프라이버시 더블 세븐 원칙을 만들어 교육하고 있다. 이 원칙의 주요 내용은

- 새로운 사이버 공격 패턴을 탐지하고 독창적인 분석 및 증명을 바탕으로 위협에 대응
- 모든 시스템과 서비스 비밀번호에 대한 무단도용 및 오남용 차단 · 억제
- 바이러스 유포나 해킹 등 불법적인 행동 예방
- 콜센터 등 업무처리담당자 단말기(PC)에 대한 철저한 보안
- 네티즌의 지적재산권 보호 및 존중
- 개인정보 열람시 네티즌 사전동의 확보
- 업무담당자의 업무 외 목적으로 개인정보 수집금지
- 모든 정보이용 로그는 법적 테두리 내에서 네티즌의 요구시 공개
- 어린이들이 보안 및 프라이버시 프로그램을 통해 친구들과 안전하게 교류

NHN은 정보보안 강화를 위해 거시적인 관점과 미시적인 관점을 동시에 가져가고 있다. 거시적인 관점에서의 보안은 정책과 지침을 수립하고 내 · 외부 조직 간의 보안 프로세스 흐름상의 미비한 점과 취약점을 파악하여 원활하고 안전한 시스템을 구축하는 것이다. 미시적인 관점에서의 접근법은 개발 프로세스 중 테스트, Q&A 단계에서 애플리케이션 코드상의 취약점을 발견하고, 시스템 구축시 보안성을 고려하여 기획하는 등 기술적인 관점을 말한다.

조직이 커지고 사업영역이 전 세계로 확대되면서 고정된 시점이 아닌, 보다 유연하게 위험을 파악할 수 있는 넓은 시야가 보안관리자에게 요구되고 있다. 이를 위해 보안조직을 강화하여, 효과적으로 역할을 분담하고 보안운영 중 일부는 아웃소싱을 통해 위험을 분담하고 있다.

정보보안 강화 위해 변화관리 마스터플랜 설계

NHN은 정보보안 강화라는 목표를 위해 변화관리 마스터플랜을 설계했다. 특히, 한게임 개인 정보보호 부문 ISO 27001 인증 취득과 네이버 개인 정보보호 부문 ISO

27001 인증 획득을 목표로 추진하고 있다.

포털사이트의 정보보안 체계는 사람들의 삶과 매우 밀접한 관계에 있다. 보안위협은 갈수록 지능화되고 정교해지고 있으며, 사용자 데스크탑과 개인정보 모바일 영역까지 보안의 영역이 넓어지고 일반화되고 있다. 글로벌 포털을 지향하는 NHN은 네이버 툴바의 무료 악성 코드 치료 서비스와 패치 배포, 관리 서비스를 비롯하여 한게임 이용자들이 안전한 게임 문화를 형성하고 이용할 수 있는 방안을 제시하는 등을 통해 안전한 포털문화를 만들고 있다. 또한, 정보통신부와 산업자원부, 경찰청 등 정부기관, 한국정보보호진흥원, CONCERT 등 다양한 외부 기관과 연계해 정보보안 서비스를 실시하고 있다.

보안은 어느 한 조직, 어느 한 담당자의 몫이 아닌 모든 회사와 모든 사용자, 정보를 취급하는 모든 담당자들에게 요구되고 있는 상황이다. 이를 위해 정보보호를 바라보는 시각이 바뀌어야 하고, 새로운 문화를 형성하기 위한 노력이 요구된다.

정보보안 문화 형성	전사적 정보보안 비전 선포 필요	• 리더십을 보유한 경영층의 후원 • 워크숍을 통한 정보보안 비전 선포
	변화관리 추진 조직 구성	• 서비스 보안팀이 주도하는 변화관리 프로젝트 TFT 구성
	전 임직원 공감대 형성	• 생활보안 캠페인 실시 • 보안 워크숍 실시 • 사내 게시판 활용 • 각종 이벤트 시상제 실시
	보안교육 실시	• 정보보안 관리체계 방법론 이전 • 임직원 수준별 보안교육 실시
	보안 인식제고 수준향상을 위한 전략적 제도 및 프로그램 필요	• 보안포털을 통한 인식변화 및 피드백이 가능하도록 프로그램 개발 • 프로세스 KPI(변화결과 측정) 도출 및 지표화
	제도 및 프로그램에 대한 효용성 평가 필요	• 제도/프로그램 계획시 KPI 도출 • 인사와 연계한 보안평가 실시

[표 1] 전사 변화관리 마스터플랜

"네티즌 교육으로 개인정보보호 강화"

NHN 임채호 보안실장(chlim@nhncorp.com)

■ NHN이 정보보호 정책에 중점을 두게 된 계기는 무엇인가?

우리나라를 대표하는 포털사이트인 NHN은 해외 진출을 통한 사업의 글로벌화를 진행하고 있다. 이 과정에서 각종 보안위협에 대처할 수 있는 국제수준의 위험관리 체계가 필요하게 되었다. 이 때문에 NHN은 통일된 보안체계를 만들고, 지속적인 변화관리를 통해 보안 프로세스를 확립한다는 계획을 세우고, 대내 · 외 각종 위협과 취약성에 대한 정보보안 프로세스를 적용했다.

■ NHN에서 실시하는 정보보호 관련 정책은 어떤 것이 있나?

NHN 보안실에서 1년 여 동안 각 부서와 인터뷰, 설문조사, 협의 등을 통해 산재해 있는 보안 관련 정책과 지침을 취합하여 'NGSS'라는 정보보호 정책 및 지침 체계를 수립하고, 2007년 1월 주요 경영진의 승인을 통해 공표했다. 올해를 원년으로 NGSS와 관련된 프로세스, 체크리스트를 바탕으로 전사적으로 보안교육, 캠페인을 진행하고 있다.

■ 직원들의 보안교육은 어떻게 실시하고 있나?

직원들의 보안의식 강화를 위해 '시큐리티 및 프라이버시 더블 세븐 원칙'을 만들어 교육하고 있다. 주요 내용은 사이버 공격 패턴 탐지 등 기술적인 내용과 비밀번호 무단도용 차단 등 보안관련 팁에 대한 내용을 담고 있다. 새로운 사이버 공격 패턴을 탐지하고 독창적인 분석과 증명을 바탕으로 위협에 대응하며, 개인정보 열람시 네티즌의 사전 동의를 확보한다는 것이 주된 내용이다. 또한, 콜센터 등 업무처리담당자 단말기에 대한 철저한 보안과, 모든 정보이용 로그는 법적인 테두리 내에서 네티즌이 요구할 때 공개하도록 했다.

이와 함께 네티즌의 보안의식 강화를 위해 어린이 보안 · 프라이버시 프로그램을 만들어 안전하게 친구를 만나고 교류하도록 하고 있다.

■ 정보보호를 위해 구축한 시스템은 어떤 것이 있나?

침입탐지 모니터링을 위한 IDS, IPS 장비와, 유해 트래픽을 차단하기 위한 Firewall, 내부 네트워크 보호를 위한 VPN, 악성 코드 방역을 위한 안티바이러스 시스템, 패치관리 시스템, 넷 플로우 분석 시스템 등을 운영, 관리하고 있다.

■ 정보보호를 위한 예산은 어느 정도 책정하고 있나?

정보보호 관련 예산은 연중 30억원에서 50억원 정도이며 인건비를 제외하고, 각종 솔루션 유지관리, 아웃소싱, 기술개발, 교육훈련비 등에 사용된다.

■ 최근 기업에서 내부정보 유출현상이 급증하고 있는데 이에 대한 대비책은 어떻게 준비하고 있나?

주로 고객들의 개인정보유출 방지에 초점을 맞추어 고객정보 보호팀을 신설하고 직원들의 업무 프로세스 개선에 초점을 맞추고 있다. 최근 한게임이 개인정보보호 인증을 받았다. NHN은 우리나라를 대표하는 포털사이트인 만큼, 기업 내부의 정보유출 뿐 아니라 이용자들의 개인정보 보안도 중요하다. 포털사이트의 정보보안 체계는 사람들의 삶과 매우 밀접한 관계에 있기 때문이다. 네티즌의 정보보호를 위해 네이버 툴바의 무료 악성코드 치료 서비스와 패치 배포, 관리 서비스, 한게임 이용자들의 안전한 게임 문화 이용방안 제시 등을 통해 안전한 포털문화를 만들고 있다. 또한, 정보통신부, 산업자원부, 경찰청 등 정부기관과 한국정보보호진흥원, 한국침해사고대응팀협의회(CONCERT) 등 다양한 외부기관과 연계해 정보보안 서비스를 실시하고 있다.

■ 정보보호 관련 인력은 어느 정도인가?

최근 인력을 충원하고 있다. 현재는 20명이며, 올해 말 30명 정도 될 예정이다.

■ 2007년 정보보호를 위해 새롭게 소개할 만한 내용들이 있다면?

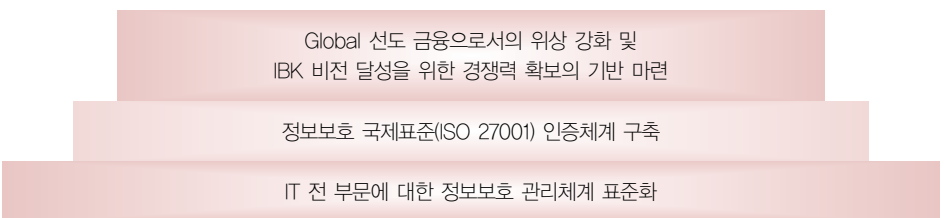
'정보보호 기본을 지키자'는 모토 아래 글로벌 보안체계의 완벽한 구축을 목표로 하고 있다.

02

IBK 기업은행 정보보호팀 최길남 차장
knchoi@ibk.co.kr

최고를 생각하고, 실천해 ISO/IEC 27001 인증 획득

기업은행 IT 본부는 '최고를 생각하고 가장 먼저 실천한다'는 슬로건을 앞세워 2006년 국내은행 최초로 IT 전 부문과 인터넷뱅킹 부문에서 ISO 27001 인증을 획득했다. 이를 위해 주요 정보시스템에 대한 위험과 취약성 분석 및 평가를 통해 정보보호 관리체계를 만들고, 정보보안 포털 시스템을 구축해 보안정보 통합 · 관리 및 임직원의 보안의식을 강화하였다.



[그림 1] IBK 정보보호 관리체계 추진 개요도

기업은행 IT 본부의 슬로건은 '최고를 생각하고, 가장 먼저 실천한다'이다. 그리고 이를 실천한 결과가 2006년 5월 국내은행 최초로 인터넷뱅킹 부문 정보보호 국제표준(ISO 27001) 인증 획득, 8월 IT 서비스 관리 국제표준(ISO 2000) 인증 획득, 11월 표준의 날 산업자원부장관상 수상, 인터넷뱅킹 서비스 평가 2회 연속 1위라는 영예로 돌아왔다. 또

단 계	산출물 제목	내 용
착수	프로젝트 수행 계획서	• 프로젝트 수행에 대한 계획 및 일반적인 내용
현황파악	현황분석 보고서	• 시스템 현황분석 내역 • 조직 및 관리체계 분석 내역 • 정보보호 관리체계 수준 평가 및 Gap 분석
분석	취약점 진단 보고서 (메인 프레임 등)	• IT 시스템 취약점 진단 및 모의해킹 결과와 조치방안
	위험분석 및 평가보고서	• 위험분석 및 평가결과 • 위험조치계획 및 대응방안
설계	보안정책 설계서 보안정책/지침/절차	• 전행적 보안정책 통합 방안 및 세부 실행지침/절차 수립
	보안 아키텍처 설계서	• 보안 아키텍처 개념설계 및 영역별 상세 설계
	보안 인프라 및 관리체계 설계서	• 보안 관리체계 아키텍처 개념설계 및 주요 과제별 상세 설계
구현	긴급조치 보고서	• 긴급조치 및 해결결과에 대한 보고서 • 전행 확산방안 수립
	정보보안 마스터플랜	• 단기 및 중장기 과제 및 일정 계획
	기반시설 보호대책	• 기반시설 보호대책 수립
이행	ISMS 표준화 방안 보고서	• ISO 27001 기준의 ISMS 표준화 방안 • 통합 보안정책 적용방안 수립 • 전행 확산방안 수립
	교육방안 보고서	• 교육과정 개발

[표 1] ISMS 단계별 수행내용

한, 12월에는 정보통신부의 '정보보호대상'을 수상하고, 국내은행 최초로 IT 전 부문에 대한 정보보호 국제표준(ISO 27001) 인증을 획득하였다.

기업은행이 추진하고 있는 정보보호 업무 중 가장 모범사례로 꼽는 것은 IT 전 부문 정보보호 국제표준(ISO 27001) 인증이다. 기업은행은 2006년 초 해킹 위협과 침해사고로부터 주요 핵심시설인 '수지 IT센터', '본부 무인원격 자동 백업센터'를 보호하기 위해 국제수준의 정보보호 관리체계 구축작업을 시작하였다. 주요 정보 시스템에 대한 위험과

취약성 분석, 평가를 통해 적정수준의 보호대책을 체계화하여 전행적인 정보보호 관리체계(ISMS)를 만든다는 계획이었다.

먼저, 인력과 예산, 정보보호업체를 선정하고, IT 전체 정보자산 분류, 취약점 및 위험평가를 실시했으며, 각종 지침에 산재되어있는 보안지침을 발췌해 변경 전 · 후 매핑과 상위 지침인 보안규정 개정작업을 시작했다. 2006년 5월부터 8월까지 약 4개월간 단계별로 ISMS 구축사업을 실시하여, IT 선진화를 위한 내부 보안관리 체계를 재정비하고, 관련법규와 고객요구 충족을 위해 제 · 규정 등을 개선해 국제표준 규격에 부합하는 정보보호 관리체계를 구축하였다.

이를 통해 잠재된 IT 위험통제와 정보보호를 체계적으로 관리할 수 있는 경영시스템을 구축할 수 있었으며, 직원들의 인식 및 능력을 향상시켜 고의적, 비고의적 실수에 따른 보안사고를 예방할 수 있었다. 체계적이고 정량적인 정보자산에 대한 위험평가 수행을 통해 당행이 안고 있는 위험파악을 위한 예방적 관리시스템을 구축 하였다. 종합적이고 체계적인 관리를 통해 국제적으로 검증된 정보보호 경영시스템을 구축해 기업은행의 정보보호 관리체계를 강화할 수 있는 계기가 되었다.

행내 정보보안 포털 시스템 구축해 보안의식 고취

기업은행의 정보보호 모범사례 중 또 다른 중요한 한 가지는 행내에 정보보안 포털 시스템을 만들었다는 것이다. 이는 정보보안과 관련한 다양한 정보를 온라인으로 제공하며 보안관련 업무를 해결할 수 있도록 구현된 보안전문포털로, 행내에 산재되어 있는 보안시스템에서 발생하는 각종 보안정보를 하나의 웹 서버로 통합하여 관리하는 시스템이다. 분산되어 있는 각종 보안관련 정보를 통합해 체계적으로 관리하는 이 시스템은 어려운 정보보호 업무를 쉽고 편하게 접근할 수 있도록 구성하여 정보보호 업무가 특정부서, 특정 담당자만의 것이 아니라 전 직원이 함께 하는 것이라는 인식을 심어 주었다.

기업은행은 정보보안 포털 시스템을 통해 정기적인 교육과 홍보로 임직원의 보안의식을 지속적으로 제고시켰으며, 새로 도입되는 시스템에 대한 보안성 심의업무를 표준화하고, 자동화하여 업무처리의 효율성과 생산성을 높일 수 있었다. 수시로 발생되는 각종 위

단 계	산출물 제목	내 용	비 고
보안 포털 시스템	웹 서버 시스템	• 행내 보안경보 수준 공지 • 바이러스 및 백신정보 게시 • 패치관련 정보 게시 • 각종 보안관련 정보 다운로드 • 기존 보안시스템과 연계(통합보안, 바이러스 백신, 패치관리, 정보유출 방지 등) • 전자결재 연동	H/W 포함
	보안성 심의 시스템	• 보안성 심의절차 준용 • 심의절차 자동화 • 전자결재 연동	
	IT 보안 국제표준 사후관리 시스템	• IT 보안 국제표준(ISO 27001) 사후관리 업무 시스템화 • 전자결재 연동	
	실시간 추적 시스템	• 인터넷 뱅킹 불법 침입자 실시간 추적 및 방어 • 통합보안 시스템과 연계	H/W 포함

[표 2] 정보보안 포털시스템 구축내용과 시스템 구성

험과 취약성에 대하여 국제표준에 맞게 체계적으로 관리, 대응 · 조치하여 보안위험을 최소화하였다. 정보보안 포털 시스템의 주요 기능은 다음과 같다.

- 보안정보 나눔터 : 정보보안 관련규정과 당 행 보안현황 정보를 공유해 직원들의 보안의식 향상, 정보보호 실천 도모
- 보안규정 및 업무 : 보안규정 및 세칙의 정보 열람, 보안관련 전자결재 리포트 시스템 운영, 외부인 방문 예약과 반 · 출입 규제
- 보안시스템 현황 : 사용자 보안, 네트워크 보안, 서버 보안의 이벤트 통합, 당 행 전체, 부서별/지점별/개인별 보안현황 진단
- 보안관제 센터 : 침해사고 대응현황과 보안사고 접수 · 보고, 침해사고 대응에 대한 체계적인 운영현황 제공
- 보안성 심의 : 보안성 심의업무 체계 정의, 심의 프로세스 시스템화
- 보안위험 관리 : 시스템 취약성 점검 및 사후 관리와 정보의 기밀성을 고려하여 효과적인 권한 통제, 국제표준(ISO 27001) 요구에 의거한 보안위험 관리

"정보보안 포털시스템 구축으로 보안의식 강화"

기업은행 정보시스템부 정보보호팀 최길남 차장(knchoi@ibk.co.kr)

■ 기업은행에서 실시하는 정보보호 관련 정책에는 어떤 것들이 있나?

2006년 추진한 정보보호컨설팅에서 수행한 현황 및 GAP 분석을 통하여 보안업무 규정 및 지침, 절차를 전면 제·개정했다. 내용으로는 보안업무의 최상위 규정인 '보안업무 규정', IT 보안업무에 대한 포괄적인 지침으로 'IT 보안업무 지침', 세부적인 절차를 정의한 '절차서 6종'으로 구성되어 있다.

■ 정보보호를 위해 구축한 시스템에는 어떤 것이 있나?

인터넷뱅킹 서비스 네트워크 구간에는 침입차단 시스템, 침입탐지시스템을 운영하고 있으며, 주요 업무 서버에 대해서는 서버 접근통제 시스템(SecureOS)과 호스트(Host) 기반 침입탐지 시스템 등을 구축, 운영하고 있다. 또한, 취약점 점검 시스템을 통해 주기적으로 진단·조치하여 침해사고를 사전에 대비하고 있다.

클라이언트 영역에는 일반적인 백신, 악성 프로그램 진단·삭제 시스템, 패치관리 시스템을 구축하였으며, 사용자의 인증을 위한 스마트카드와 사설 인증기반의 Single Sign-On 시스템을 운영중이다.

■ 최근 기업들의 내부정보 유출현상이 급증하고 있는데 이에 대한 대비책은?

행내에서 생산되는 중요정보의 대부분은 결국 사용자(직원)의 업무용 PC로 집적된다고 보고, 외주직원과 내부 사용자에 대하여 에이전트 방식의 '내부정보 유출방지 시스템'을 설치, 운영하고 있다.

주요 통제항목은 USB, 플로피디스켓 등 이동식 저장매체와 출력 차단, 워터마크 삽입 등 출력 시스템 통제, 웹을 통한 첨부, 폴더공유 통제, 프로젝트 PM, 부서책임자의 승인하에 정책변경을 통해 업무를 처리하고 있다. 운영하면서 발생하는 각종 이벤트는 주기적으로

모니터링 하고, 위험요소가 있는 경우 직접 확인하고 있다.

■ 직원 교육은 어떻게 실시하고 있나?

기본적으로는 정보보안 포털시스템과 행내 그룹웨어를 이용하여 직원들에게 각종 보안정보를 제공하고 있으며, 주기적으로 외부의 전문가를 초청하여 상황에 맞는 주요 이슈에 대한 교육을 통하여 보안의식을 제고하고 발생 가능한 보안사고를 미연에 방지하고 있다. 정보보호업무 담당직원의 경우, 보안 시스템 운영, 정보보호 국제표준 등의 교육을 수시로 실시하고 있으며, 보안분야의 전문가 자격취득 교육과정을 수시로 이수하도록 지원하고 있다.

■ 직원들이 사용하는 PC는 어떻게 관리가 되고 있나?

본부와 영업점의 업무용 PC에 대한 인터넷 사용 제한을 없애면서 각종 웜 · 바이러스 및 악성 프로그램으로 인한 피해가 지속적으로 발생하고 있다. 이에 대한 대비책으로 필수 보안 패치에 대한 중앙관리를 위하여 패치관리 시스템(PMS)을 운영하고 있다. 바이러스 백신과 악성 프로그램 진단 · 삭제 프로그램 또한 전체 PC를 통합관리할 수 있는 시스템을 이용하여 일괄적인 진단 · 치료 엔진 업데이트 및 주기적인 예약검사, 실시간 모니터링 등을 실시하고 있다.

PC 사용자 인증을 위하여 스마트카드 및 사설인증서 기반의 SSO 시스템을 구축해 불법 접근을 차단하고 있으며, IP 관리 시스템을 이용하여 비인가자나 일정기간 미사용 PC의 네트워크 사용을 제한하고 있다."

■ 2007년 정보보호 정책으로 새롭게 소개할 만한 내용들이 있다면?

기존의 보안 시스템의 확대 및 강화계획 외에 직원의 보안의식 고취를 위한 온 · 오프라인상의 다양한 프로모션을 계획하고 있다. 예를 들어, 정보보호에 대한 기본사항을 온라인 컨텐츠로 제작하여 행내 연수의 필수 이수과정으로 신설하고, 신입행원 연수교육과정에도 포함시키는 등 직원의 보안의식을 강화할 수 있는 다양한 이벤트를 계획하고 있다.

03

(주)한국무역정보통신 보안파트 권오준 과장
ojkwon@ktnet.com

정기적인 정보보호 컨설팅 통해 ISO 27001 인증 획득

전자무역전문 서비스 기업인 한국무역정보통신(KTNET)은 정기적인 정보보호 컨설팅을 통해 국제 정보보호 체계 인증 ISO 27001을 획득했다. 또한, 내부자 정보유출 차단을 위해 유해 사이트 접속차단, 이동식 저장매체 및 출력통제, 정기적인 보안교육 등을 실시했으며, 지속적인 정보보호 정책을 마련하기 위해 보안대책 실무협의회를 정기적으로 열고 있다.

(주)한국무역정보통신(KTNET)은 무역업체와 무역관련 기관 · 단체를 위한 전자무역 전문 서비스 기업으로 2006년 12월 전자무역촉진에 관한 법률에 의거한 전자무역 기반 사업자로 지정되었다. KTNET이 제조 · 서비스 부문 사업자 중에서 2006년 정보보호 대상을 수상할 수 있었던 것은 정보보호에 대한 인식이 사업 초기부터 자리잡았기 때문이다. KTNET은 2003년과 2006년 정보보호 컨설팅을 통해 국제적인 보안체계를 수립해 국제 정보보호 체계 인증인 ISO 27001을 획득하였으며, 사내에 정보보호 관련 정책과 지침을 제정해 임직원에게 배포, 교육해오고 있다.

KTNET이 보안사업에서 가장 중요하게 여기고 있는 것은 내부자 정보유출 차단이다. 또한, 성인사이트나 게임사이트 등의 접속을 차단하는 것이다. 이러한 사이트는 업무 효율을 떨어뜨릴 뿐 아니라 바이러스나 악성 코드에 감염되기 쉽기 때문이다. 관련기관

이나 업체와 자료를 공유하는 것을 자제하도록 하고, 웹하드와 메신저, P2P를 통한 문서 전송은 금지해야 한다. 그리고 온라인을 통해 정보가 빠져나가는 것을 막기 위해서는 전자문서 보안시스템(DRM)을 도입하는 것이 효과적이다. DRM은 자료를 암호화함으로써 설사 자료가 유출되었다 해도 해독을 불가능하게 하고, 비인가자가 접근했을 때 접근을 차단하고 보안담당자가 알 수 있도록 경고한다.

보안통제와 함께 임직원 교육 통해 전사적인 보안목표 설정

가장 흔히 일어나는 정보유출 사건은 직원들이 내부문서를 출력해 가방에 넣어 정문을 통과해 밖으로 나가는 것이다. 출입문에서 직원들의 가방을 일일이 검사할 수 없으므로 이같은 악의적인 정보유출을 막는다는 것은 현실적으로 어려운 일이다. 오프라인으로 문서가 외부로 유출되는 것을 막기 위해서는 회사 전 PC의 CD, DVD, USB 사용을 금지해야 한다. 프린트나 팩스 등으로 출력하는 모든 문서에 출력자와 출력일시, 출력 PC를 기록하여 출력물 사본을 서버에 별도 저장한다.

이러한 시스템은 회사 내부의 프로세스를 많이 변경해야 하며, 임직원의 이해와 적극적인 참여가 필요하다. 아무리 강력한 보안정책을 만든다 해도 실무자들이 불편하고 업무 효율성이 떨어진다고 느낀다면 효과적인 보안업무가 이뤄질 수 없다. 강력한 보안정책 보다 정기적으로 임직원을 교육시켜 보안의식을 강화하는 것이 훨씬 더 효과적이다. 특히, 임원을 포함한 경영자에게 보안의식을 심어주는 것이 중요하다. 정기적인 교육과 훈련으로 보안목표를 설정하고, 정기적인 보안대책회의를 열어 보안 취약성을 점검하고 대책을 마련해야 한다.

정기적으로 내 · 외부 기관을 통해 보안 컨설팅을 받는 것도 적극적으로 추천되는 일이다. 기업내 핵심 구성요소와 정보자산을 식별하고 평가해 위험도와 잔여위험을 측정하는 것은 매우 중요한 일이다.

또한, 컨설팅을 통해 도출되는 결과를 지속적으로 이어가는 것도 간과할 수 없는 것이다. 보안담당자의 많은 시간과 노력이 투입되어야 하고, 회사 내부의 반발도 상당하기 때문에 보안을 실행에 옮기는 데에는 많은 어려움이 따른다. 이를 해결하기 위해서는 위험관리체계 시스템을 도입하는 것이 좋은 방법이다. 정보보호 포털을 만들어 전 직원을 참

구 분	점검 항목
내부자 정보유출 방지	• 유해 사이트 차단 • 외부로 데이터 전송/모니터링 차단 • 사용자 계정 정리 • 이동식 저장매체 사용 금지, 출력물 사본 저장
공동의 보안목표 설정	• 임직원이 동참하는 정기적인 보안교육 • 보안 프로세스 수립/홍보 • 보안대책 실무협의 마련
위험관리 및 대응체계 구축	• 내 · 외부 기관의 보안 컨설팅 • 컨설팅 결과에 대한 지속적인 관리 • 정보보호 포털사이트를 구축해 임직원 참여 독려
정보보호 솔루션 투자, 활용	• 단순화/표준화/통일화 된 보안솔루션 도입 • 보안담당자에 대한 투자 • 보안업무 아웃소싱

[표 1] 성공적인 보안업무를 위한 핵심 요소

여시키면 모범적인 정보보호 활동 사례가 될 수 있으며, 성과지표를 만들어 제시함으로써 정보보호 관리활용을 높일 수 있다.

시스템 취약성을 해결하기 위해서는 다양한 정보보호 솔루션을 활용하는 것이 좋지만, 성능이 뛰어난 제품 구비만으로 보안을 장담할 수 있는 것은 아니다. 보안담당자가 각 제품을 다루고 관리할 수 있는 기술을 갖춰야 하지만, 제품을 많이 다룰 줄 안다고 해서 훌륭한 보안담당자가 되는 것도 아니기 때문이다. 보안솔루션을 도입할 때는 제품을 도입한 후 운영에 투입되는 시간과 유지보수 비용을 따져 가장 단순하고 통일된 정책을 기반으로 하는 것이 좋다. 단순한 업무는 아웃소싱을 적절히 병행하며 보안담당자의 업무를 줄이는 것이 좋다. 정보보호 관리의 목표는 위험관리의 효율적인 활용이다. 위험관리만 잘해도 기업 정보보호를 다했다고 해도 과언이 아니다. 그러나 대부분의 기업에서 보안에 대한 투자를 물리적 보안이나 기술적 보안에 집중해왔기 때문에 위험상황이 닥치면 대책을 마련해 근본적인 위험관리 대책이 될 수 없었다. 보안솔루션을 도입하는 것만큼 중요한 것이 보안 프로세스를 마련하는 것이며, 사람에 대한 적절한 투자가 함께 이루어져야 한다. 이를 위해서는 경영진의 협조가 반드시 있어야 하며, 전 직원을 상대로 한 교육과 홍보가 필수적이다.

04

CJ시스템즈(주) 정보보호센터 정보보호파트 한재순 과장
yapy@cjsystems.net

기준에 맞는 프로세스 구축으로 보안성 강화

글로벌 기업으로 도약하기 위해 CJ시스템즈는 보안을 기초로 한 기본 인프라 구축을 강화하고 있다. 이를 위해 관리적 측면에서 체계적인 프로세스를 구축하고, 이를 수행하는 것에 초점을 맞추면서 일정한 지침을 정하고, 교육을 통하여 직원들의 정보의식을 높이고 있다.

[그림 1] CJ Systems의 보안관리 정책 목표

CJ 그룹은 글로벌 기업으로 도약하기 위하여 각 사업분야의 핵심 역량을 강화하고 있다. 이를 위한 기본 인프라 구축에 보안을 기초로 한 기업자산 보호, 경쟁력 강화를 모색하고 있다. 보안관리의 토대가 되는 위험관리의 체계적인 사전관리를 통해 웜, 바이러스, 해킹, 전자문서 위 · 변조, 개인정보 등의 보안사고의 위협을 최소화하고 있다.

이같은 배경에서 CJ Systems가 실시하고 있는 정보보호 활동을 살펴보면 우선, 관리적 측면에서 체계적인 프로세스를 구축하고 정해진 프로세스대로 수행하는 것에 초점을 맞추고 있다. CJ Systems는 업무 프로세스에서의 보안적인 요소를 찾아 정형화하여, 이를 지침으로 정하고 지속적인 교육을 통하여 사용자를 제도권 안으로 유도한다.

물리적 보안으로는 출입통제 관련 부분에 있어 카드인식 통제, CCTV 저장제어 등을 실시하며, 문서저장에 있어서는 보안 등급별로 구분된 자료를 구분된 관리자에 의해 관리하게 하는 등의 접근제어 방법을 사용한다.

기술적인 면에서의 보안정책은 개인정보 시스템과 서비스용 시스템을 구분하고, 논리적으로 구분된 권역에 따라 신뢰구역, 비 신뢰구역, 공통구역, 강화구역 등으로 나누었다. 각각의 환경에 따라 방화벽, IPS, 웹 방화벽 등으로 접근제어 및 유해차단을 적용했다. 개인 PC 보호를 위해서는 백신, 패치관리, 매체제어 관리 등을 운용하며 운용요청 부서와 운용실무 부서, 감사부서로 구분해 기술적 보안관리에서 발생할 수 있는 오류를 제어한다.

[그림 2] 보안방법에 따른 정보보호 활동

보안관리의 핵심은 기준에 맞는 프로세스 구축과 실천

보안관리에 있어서 가장 중요한 것은 기준에 맞는 보안관리 프로세스를 마련하고 이를 실천하는 것이다. 만들어진 프로세스를 실천하는 것도 어려운 일이지만, 제대로 된 프로세스를 만드는 것 역시 어려운 일이다. 잘못된 프로세스는 수많은 시행착오를 낳기 때문이다. CJ Systems는 보안관리의 가장 근본인 프로세스를 개별 영역의 특성에 맞게 글로벌 표준에 맞추어 정형화하고 있으며, 이들의 변화관리를 병행하여 시행착오를 최소화하고 있다.

이를 위해 중 · 장기적인 마스터플랜을 세워 장기적인 방안으로 그룹 목표에 준하는 보안 수준을 목표로 분야별 계획을 수립하고 있다. 한편, 중 · 단기적인 방안으로 현재 이슈가 되는 중요사항에 대한 우선순위를 높여 세부 실행계획을 통하여 수행한다. 또한, 각 단계별 계획 내에 포함되지 않은 이슈 사항에 대하여 중요도에 따라 별도의 위험관리를 통하여 관리하고 있다.

05

(주)DHC코리아 전산팀 김기현
khkim@dhckorea.com

보안의 시작은 합리적인 정책 실천

DHC코리아는 2006년을 '보안의 해' 로 정하고, 정보보호 안전진단 필증, 인터넷 사이트 안전마크 인증, 개인정보보호 우수 사이트 인증, eTrust 인증, 보안 서버 인증 등 외부 공인기관의 인증을 획득했다. 정기적인 모의해킹과 웹 애플리케이션 취약성 점검, 홈페이지 위 · 변조 모니터링을 실시해 보안 취약성을 점검했으며, 전문 보안 아웃소싱 업체와 협의하며 안정적인 네트워크 보안에 힘썼다.

정보통신부의 2006 제5회 정보보호 대상 우수상을 수상한 (주)DHC코리아는 애초에 2006년을 '보안의 해' 로 정하고 보안강화를 위한 많은 노력을 했다. 외부의 공인기관으로부터 객관적인 평가를 받기 위해 2006년 한 해 동안 정보보호 안전진단 필증, 인터넷 사이트 안전마크 인증, 개인정보보호 우수 사이트 인증, eTrust 인증, 보안 서버 인증 등 거의 모든 기관의 인증마크를 획득하였다.

DHC코리아가 보안 강화에 많은 노력을 기울인 것은 많은 기업들이 개인정보를 수집하면서도 개인정보의 기술적 관리보호 기준 고시를 준수하지 않고 있는 현실에 비추어보면 상당히 우수한 사례라고 할 수 있다.

한국정보보호진흥원(KISA)이 2006년 종업원 5인 이상 사업자 사이트 2만8000여 개를 대상으로 실시한 사업자 개인정보보호 실태조사에 따르면, 기업의 정보보호 관리자들

이 개인정보를 수집할 때 정보통신망법에 의해 고지해야 할 사항은 잘 지키지만, 기술적인 관리보호 기준 고시는 준수하지 않는 곳이 많은 것으로 드러났다. 중소기업에서의 보안은 보안부서와 보안담당자의 노력과 함께 최고경영자의 의지가 필수적이다. 회사의 비즈니스에 보안관리가 미치는 영향을 파악하고, 체계적으로 구현할 수 있는 회사의 보안정책 수립이 필요하다.

기업 보안정책은 보호해야 할 자산이 무엇이고 효율적이고 안전하게 사용하는 방법을 찾는 것에서부터 시작한다. DHC코리아의 입장에서 본다면 지켜야 할 가치가 있는 자산은 고객정보와 기업 내부의 정보라고 할 수 있다. 기업 내부의 기밀사항은 기업이 갖고 있는 매우 중요한 자산임에 틀림없지만, 고객정보는 그렇지 않다. 고객정보는 본인인증을 위해 사용된 도구일 뿐이며, 개인정보의 주인은 고객 자신이다. 이 때문에 기업이 고객의 정보가 유출되지 않도록 노력해야 하며, 개인정보의 가치를 이해하고 보호하는데 앞장서야 한다.

고객정보 보호위해 보안 강화

기업이 갖고 있는 고객정보는 이름과 휴대폰 번호, 이메일 주소, 집 · 사무실 주소 등 기본적인 사항과 사회경력, 경제관계, 건강, 종교, 위치정보 등 개인정보 전반에 이른다. 고객들이 무심코 참여하는 기업의 각종 이벤트 등을 통해 수집되는 정보들이 어딘가에서 새어나가 개인들에게 피해를 입히는 경우가 종종 있다. 이미 고객들은 개인정보 유출에 무방비 상태로 노출되어 있는 것이다.

그러나 개인정보는 사적인 가치 외에도 공적인 가치와 상업적인 가치를 갖고 있으며, 반드시 보호되어야 한다. 국가적인 측면에서 개인정보를 보면 공공질서 유지와 치안, 국가 방위 등을 위해 개인정보가 높은 가치를 갖는다. 주민등록표 등을 작성해 국가에 주민으로 등록하는 것처럼 개인은 전체 사회의 안정을 위하여 개인정보를 등록하여야 한다.

공적 가치는 상업적인 가치로 전환되지 않도록 통제되지만, 때로 상업적인 가치로 활용될 수 있도록 육성시키기도 한다. 개인정보에 소비유형이나 소득수준, 라이프스타일 등의 정보는 고객관리와 사업확장 등을 위한 전략에 중요하게 쓰일 수 있기 때문이다. 단, 개인정보를 상업적으로 이용할 때 기업은 본인에게 반드시 통보하고 승낙을 얻어야

하며 대가를 지불해야 한다.

이처럼 중요한 개인정보가 보안정책에 정의되어 있지 않은 다른 이들에게 노출되는 것을 데이터의 손실이라고 한다. 데이터 손실이 발생하는 이유는 물리적인 분실부터 시작해 해킹, 악의를 가진 내부인의 소행, 네트워크 보안상의 문제, 담당자의 관리소홀이나 실수 등 다양한 유형으로 나타난다.

DHC코리아는 점차 사회 전 분야로 확대되는 데이터 손실을 방지하기 위해 정보보호 조직과 개인정보보호 조직을 구성하고, 웹 해킹에 대비한 정기적인 모의 해킹과 웹 애플리케이션 취약성 점검을 하며, 홈페이지에 대한 상시 위 · 변조 모니터링 체계를 가동하고 있다. 각 시스템과 애플리케이션에 대한 취약성 점검을 통해 혹시 모를 침해사고를 예방하고, 전문적인 보안 아웃소싱 업체와 업무 협의를 통해 안정적인 네트워크 보안 및 시스템 장애에 대비해 고객정보 유출방지와 안정적인 온라인 쇼핑 인프라를 제공하기 위해 노력하고 있다.

하드웨어적인 노력으로만 보안정책을 유지하는 것은 '사상누각' 이나 다를 바 없다. 정보유출에 있어 가장 취약한 부분은 내부 사용자에 대한 것이기 때문이다. DHC코리아는 내부 사용자 교육과 통제, 시스템 구축을 위해 지속적으로 노력하고 있으며, 그 결과로 많은 인증을 획득하고 여러가지 상을 수상할 수 있었다.

기업보안은 비즈니스가 보안정책 안에서 원활히 이루어지는 것

기업운영에 있어 필요한 정보를 제때 제공하는 것은 기업 경쟁력 확보에 필수적인 요소이다. 요즘과 같이 인터넷 비즈니스의 중요성이 커가는 시점에서는 더욱 그렇다. 보안의 가용성과 보안성의 균형이 중요하듯, 회사입장에선 비즈니스가 보안정책 체계 안에서 원활히 이루어지는 것이 궁극적인 목표가 된다. 이러한 보안목표를 달성하기 위해 선택 가능한 대안에 대해 적절한 검토가 이루어져야 하고 회사 외부와 내부의 보안환경 변화에도 민감하게 대처해야 한다.

이런 경제성의 논리를 달성하기 위해 보안정책의 수립, 실행, 평가의 과정이 비용 효율적으로 실행되어야 하고 이를 위해 내부, 외부의 네트워크가 필수적이다. 특히, 최고경영자의 인식과 의지, 내부 구성원의 인식이 없는 보안정책은 공허하다. 그리고 정부의 합

리적인 정책, 외부 전문가들과의 효율적인 네트워크 구축 및 대안선택 과정에서의 협의도 회사 전체의 보안성을 높이는데 필수적이다.

이와 함께 요구되는 또 다른 사항은 기업보안에 대한 적절한 정보제공과 체계적인 지원이다. 아직 우리 정부는 인터넷 사업자들이 개인정보 보호를 효율적으로 할 수 있도록 하는 구체적인 지원책을 마련하지 못하고 업체들에게 개인정보보호 의무만을 강조하고 있어 중소기업들이 많은 어려움을 겪고 있다. 앞으로 정보보호 정책이나 법률안을 제정할 때 현실적인 문제들을 반영하여 중소기업의 개인정보보호 정책이 실효를 거둘 수 있게 해야 한다.

06

㈜씨앤에스테크놀로지 보안관리 진나니 주임
nani@cnstec.com

보안의 시작은 보안 프로세스 도입

㈜씨앤에스테크놀로지는 설계도면과 소스, 인력을 주요자산으로 파악하고 유출경로를 추정, 루트 봉쇄로 기업 정보유출을 막는 정책을 마련했다. 네트워크 상의 기업정보 유출을 막기 위해 위험구간별 IPS를 설치하였다. 내부자에 의한 정보유출을 막기 위해 회사 내에서 무선 랜을 금지하고 허가된 사이트에만 쓰기 기능을 부여하는 등 종합적인 보안정책을 펼쳤다.

대부분 중소기업의 보안관리는 전산담당자가 전담하고 있어, 전산장비와 함께 여러 종류의 보안관련 장비를 관리해야 한다. 아무리 좋은 보안솔루션을 도입한다 해도 소수의 전산담당자가 여러 분야의 장비를 다루다 보니 장비가 제 기능을 수행하지 못하는 경우가 많다. 이를 해결하기 위해서는 보안 프로세스를 갖추는게 가장 좋다. 보안담당자라 해도 모든 종류의 보안장비를 100% 완벽하게 다룰 수는 없기 때문이다.

㈜씨앤에스테크놀로지에서 시행하고 있는 보안정책은 우선 자산을 파악한 후 이를 지키는 방법을 연구하는 것이다. 씨앤에스는 칩 설계도면과 소스, 인력, 기획 · 영업 문서, 현금이 주요자산으로 파악되었으며, 이러한 자산이 유출될 수 있는 경로를 추정하여 루트를 봉쇄하는 노력을 하고 있다.

가장 많은 유출사례는 외부 저장장치를 통해 밖으로 빠져나가는 것이다. 현재 이를 제

어하는 보안제품이 출시되어 있으며, 기업에서 도입하려 할 때에는 우선 도입목적과 적용범위를 정확히 파악해야 한다. 매체제어 프로그램은 운영체제의 드라이버 단을 제어하는 것이기 때문에 매우 어렵고 까다롭다. 실무 현장에 확대 설치할 때 블루스크린이 뜨거나 하드디스크가 통째로 망가지는 경우도 발생하므로 직원들의 PC 환경과 사용패턴, 직원 컴퓨터와 네트워크 수준을 충실히 이해하고 있어야 한다. 또한, 이메일을 통한 유출을 차단하기 위해 '메일 책임제'를 실시, 메일을 발송한 사람의 직속상관에게 복사본을 전달하고, 보안솔루션에 저장해 1년간 보관한다.

웹 메일이나 P2P, 개인블로그, 비밀게시판을 통한 정보유출을 막기 위해서는 읽기 기능은 열어두고 '쓰기 기능'은 허가된 사이트에만 허락하는 보안정책을 세웠다. 이와 관련한 보안솔루션을 도입하기로 하고, 사용자의 인터넷 이용을 모니터링 하여 패턴을 분석한 다음 DB를 만들었다. '찾기', '로그인', '결제', '은행', '예약', '쇼핑'이 포함된 곳

구 분	내 용
자산 파악	• 지켜야 할 자산 파악, 자산유출 경로 추적, 루트 봉쇄
외부 저장장치 이용한 정보유출 차단	• 직원 PC 사용환경 및 패턴 파악해 보안수준과 장비 선택
이메일 통한 정보유출 차단	• 메일 책임제 • 메일 사본, 보안제품에 저장
웹 통한 정보유출 차단	• 허가된 사이트에만 쓰기 허용 • 웹 메일, 블로그, 카페, 비밀게시판 쓰기 금지
위험구간별 IPS 설치	• 네트워크 망 중 보안이 취약한 곳에 IPS 설치 • 관리 포인트가 지나치게 많아지면 취약점 될 수 있음
허가받지 않은 컴퓨터의 네트워크 접근 금지	• IP Scanner 도입으로 허가받지 않은 컴퓨터 차단, IP 관리
무선 인터넷 차단	• 무선 보안제품 도입, AP 수거, 노트북 확인 • 모바일 무선 인터넷 차단은 불가능하다는 한계 있음
인재유출 차단	• 회사 내 구직활동 금지 • 외부 헤드헌터 접근 통제
물리적 보안 강화	• CCTV 설치, 출입문 경비업체 로그 확인 • PC 하드 도난방지 위해 하드에 센서 부착
인식의 변화	• 정기적인 보안교육 실시

에는 읽기와 쓰기를 허용하고, '웹 메일', '블로그', '까페', '동호회', '비밀 기능이 있는 게시판' 에는 읽기만 허용하고 쓰기는 금지시킨 후 허용 사이트 DB를 구축했다.

인력도 주요 자산, 유출방지 위한 정책 마련

네트워크 보안을 위해서는 보안성이 취약한 곳과 보안등급이 높은 곳을 찾아 위험구간별로 IPS를 설치했다. 특히, 연구소 등의 PC에는 철저한 보안상태가 유지되어야 하므로, 보안성을 강화해야 한다. 방화벽을 통제하고, 바이러스 월을 활용했지만, 회사 특성상 연구 개발망은 많은 포트를 열어두어야 하는 경우가 발생할 수도 있다. 이런 경우에 관련 세그먼트 앞뒤로 IPS를 설치했다. 그러나 너무 많은 IPS를 두면 관리 포인트가 증가해 바람직하지 않으므로 보안등급과 관리인력을 감안해 적당한 선에서 조절하는 것이 필요하다.

보안의 가장 기본은 허가받지 않은 컴퓨터가 네트워크에 접근하는 것을 막는 것이다. 특히, 직원들이 집에서 작업을 하기 위해 개인의 노트북을 사용한다고 할 때 보안담당자들이 이를 무조건 막아야 하는지, 일정부분 허용해야 하는지 난감한 상황이 벌어질 수 있다. 이에 대한 대응책으로는 IP Scanner가 유용하다. 허가받지 않은 컴퓨터를 차단하고, IP 관리에도 유용하게 이용할 수 있다.

무선 인터넷의 경우, 기업 내에서 무선 인터넷을 사용하지 못하게 정책적으로 금지시키고, 사내의 AP를 수거하고, 노트북에 대해서는 로그를 확인하고 주의를 주었다. 그러나 회사 주위의 건물에서 무선 인터넷 사용이 가능하므로 노트북 통제에 한계가 있어 무선 보안제품을 도입해 허가된 노트북만 AP를 사용할 수 있게 하였다. 무선 인터넷을 이겼다고 생각하는 순간, TV 광고에서는 유명 탤런트가 자동차를 타면서 핸드폰 통신을 통해 인터넷을 하고 있었다. 이처럼 보안은 현대기술과의 끝없는 전쟁이다.

또한, 회사에서 가장 중요한 자산을 꼽으라고 하면 인력이 1순위에 오를 것이다. 문서나 정보가 유출되는 것 보다 주요 인력이 경쟁사로 빠져나가는 것이 회사에는 더 치명적인 영향을 미칠 수 있다. 인력유출을 방지하기 위해 회사 메일로 들어오는 스카우트 제의와 회사 내 구직활동을 일부 제한하는 방법을 사용하였으나 인력유출은 물리적으로 완전히 막을 수 없으므로 경영자가 인력관리 전략을 잘 세우는 것이 무엇보다 중요하다.

회사에 외주업체와 고객의 출입이 잦아지면 출입통제도 매우 중요하다. 실제로 경비

업체의 로그를 확인하면 누락되는 정보가 있으며, 이에 대해 지속적으로 시정조치를 요구해야 한다. CCTV를 설치하고 경비원 교육을 강화하는 방법으로 물리적인 보안조치를 취했다. PC의 하드 드라이버 도난을 방지하기 위해서는 하드 드라이버 위치가 바뀌거나 누군가가 빼내서 가져갈 경우를 대비해 하드 자체에 센서를 부착해 경보음이 울리도록 하였다. 또한, 사내 모든 장비에 RFID 태그와 AM 태그를 부착해 불법장비 반출을 차단하고 있다.

아무리 기술적인 보안이나 물리적인 보안을 완벽하게 갖추고 있다 해도 누구라도 마음만 먹으면 얼마든지 정보를 빼낼 수 있다. 이 때문에 직원을 대상으로 한 보안교육이 무엇보다 중요하다. 씨엔에스테크놀로지는 신입사원을 대상으로 월 1회 정기적인 보안교육을 실시하고 있으며, 전 직원을 대상으로 분기별로 외부 전문가 초청 교육을 실시하고 있다.

“기술유출 방지위해 직원 보안교육 강화”

㈜씨앤에스테크놀로지 서승모 대표(smseo@cnstec.com)

■ 기술유출을 예방을 위한 정책은 어떤 것이 있나?

기술유출 방지를 위해 가장 중요하게 생각하는 것이 직원들의 보안교육이다. 기술정보가 흘러나가는 것은 내부 직원의 실수나 악의를 가진 행동때문인 경우가 많기 때문이다.

보안의식 정립을 위해 신입사원의 경우, 1달에 1번씩 주기적으로 보안교육을 실시한다. 회사 보안정책과 보안수위에 대해 지속적으로 인지시키고, 메일사용 기준부터 시작해서 출입통제까지 출근해서 퇴근시까지 지켜야할 모든 보안사항에 대해 교육을 하고 있다. 또, 새로운 보안정책이 나오면 각 부서 신입사원들에게 가장 먼저 교육하고 이들이 각 부서로 가서 자세하게 전달하는 식으로 보안인식 확산을 꾀하고 있다. 전 직원 대상의 보안교육은 1년에 4회 이상 실시하며, 분기별로 교육원에서 실시하는 정기교육 프로그램 참여도 실시하고 있다.

■ IT 기술을 가진 기업의 경우, 이메일과 웹을 통한 정보유출이 많이 발생한다. 이를 막기 위한 대책은 무엇이 있나?

직원 한 사람이 보낼 수 있는 이메일의 총용량이 정해져 있다. 일정한 회수와 용량이 초과되면 그 때마다 부서 팀장과 부서장, 대표이사에게 자신이 보낸 메일이 똑같이 전달된다. 이렇게 이메일 관리가 이루어지면, 직원들이 발송한 메일 복사본이 팀장에게 전송되어 부재시 업무에 대해서도 파악할 수 있어 보안과 업무 효율적인 측면에서 효과가 크다.

웹을 통한 정보유출 차단을 위해 허가된 사이트 외에는 글쓰기를 할 수 없게 했다. 2006년 5월 중순부터 7월 초까지 전 직원의 인터넷 생활을 분석하고 이를 토대로 DB를 구축한 후, 사이트 접속은 가능하지만, 게시판 댓글이나 비밀글을 남기는 것은 전면 차단하고 있다. 이 정책은 시행 초기에 많은 반발을 낳았으며, 특히 쇼핑몰을 선별하는 일이 가장 힘들었다. 글쓰기 차단 솔루션을 처음 도입하면서, 기존의 시스템에서 안정화 되지 못했

던 점도 어려운 점이었다. 업체와의 지속적인 커뮤니케이션과 직원들의 설득으로 현재는 안전하게 운영되고 있다.

■ PC 보안은 어떻게 이루어지고 있나?

2006년 1월부터 사내 PC 표준화 작업을 통해 모든 OS를 통일하고 인가된 S/W만 사용하도록 기준을 정하였다. PC가 표준화 되어있지 않아 어떤 장애가 발생했을 때, 원인을 파악하고 문제를 해결하는데 어려움이 있었기 때문이다. 지금은 모든 PC에 백신이 설치되어 있고, PC의 IP마다 방화벽에 등록해 회사에서 필요한 부분까지만 열 수 있도록 통제하고 있다. 업무 특성마다 자신이 접근할 수 있는 사내 망이 구분돼 있고, 자신의 업무와 상관없는 DB에는 접근할 수 없다.

■ IT 기술을 보유한 업체이기 때문에 물리적 보안체계도 중요할 것으로 보이는데.

출입통제를 하는 사설경비업체의 서비스를 받고 있는데, 일부 누락되는 정보가 발생했다. 경비업체에 지속적으로 시정조치를 통보해 업체가 많은 비용을 부담하며 사내 장비를 최신형으로 교체해주었다. 몇 번씩 밤을 새면서 무인경비시스템을 점검해 문제점을 발견하고 이를 수정해 나갔다.

사내에는 64대의 CCTV를 설치했으며, 개인 프라이버시를 침해할 소지가 있는 장소의 카메라는 위치를 조정하고 하나하나의 동작을 체크하였다. 입구 경비원 교육을 강화해 경비원에게도 사내 보안교육을 실시하였다.

또한, PC내 하드 보안을 위해 하드에 센서를 부착해 하드가 움직일 때 경보음이 울리도록 하였다. 사내 모든 장비에 RFID 태그를 부착해 불법장비 반출을 차단하고 있다.

■ 보안정책을 수립하려는 중소기업에게 조언을 해준다면?

회사에서 도입하는 모든 장비와 보안 소프트웨어는 사내 시스템에 맞추는 것이 중요하다. 특히, 연구 · 개발에 주력하는 기업은 연구활동에 방해가 되지 않도록 보안업무를 실행해야 한다.

07

교보증권(주) IT센터 김원걸 센터장
wgkim@kyobotrade.co.kr

새로운 위협에 대처하며 안전한 시스템 운영위해 노력

증권사의 정보보안은 고객의 자산과 밀접한 관계에 있기 때문에 그 어느 기업보다 보안이 중요하다. 교보증권은 매년 외부기관의 취약성 분석평가 컨설팅을 받고, 일상생활 공간에 보안의식을 고취하는 스티커를 부착해 보안의식을 생활화하고 있다. 또한, 보안정책으로 인한 효과를 정량화된 데이터로 수치화해 경영진의 보안에 대한 이해를 높이고 있다.

보안위협의 증가와 함께 엄청나게 다양한 보안기술이 쏟아져 나오고 있다. 보안담당자가 해야 할 일이 그만큼 늘어나고 있다는 것이다. 보안담당자에게 맡겨지는 기본 업무는 조직의 보안정책 수립, 네트워크에 들어오고 나가는 각종 패킷에 대한 모니터링, 네트워크와 시스템 OS 취약점 점검, 보안시스템의 이상 유무 검사, 직원들의 보안인식 교육 등이다. 보안사고가 발생했을 때 원인 파악과 해결을 해야 하며, 만약의 사태에 대비하여 BCP(Business Continuity Planning)/DRS(Disaster Recovery System) 계획을 세우고 테스트하며 백업센터 운영도 곁들어야 한다. 이 모든 것이 조직이 감당해야 할 위협에 대한 대비와 대응책이며, 조직의 생존과 직결되는 것이다. 이 업무를 보안담당자 혼자 감당한다면, 담당자의 역량에 따라 회사의 보안수준이 결정되어 회사는 위험한 상황에 처할 수 있다.

보안은 조직 구성원이 함께 지고 가야 할 몫이라는 것은 아무리 강조해도 지나치지 않다. 특히, 고객 자산에 대한 책임을 지고 있는 증권회사에서 보안은 더 특별한 의미를 갖는다. 실시간으로 움직이는 데이터는 고객 수익과 직결되어 고객의 주문이 조금이라도 늦어지면 손해를 볼 수 있다. 그렇다고 해서 보안을 소홀히 했다가는 고객 개인정보가 유출되는 등의 피해를 입게 된다. 보안을 강화하면 성능이 떨어지고, 성능을 중시하면 보안성이 떨어진다. 이는 보안담당자가 언제나 안고 있는 딜레마이며, 보안과 성능을 모두 만족시킬 수 있는 방법을 찾는 것은 보안담당자와 조직 전체가 해결해야 할 숙제이다.

'주요 정보통신 기반시설'로 지정되어 있는 교보증권(주)는 매년 외부기관으로부터 취약성 분석평가를 위한 컨설팅을 받고 있으며, 정보보호 관련 전산시스템을 주기적으로 점검하고 있다. 또한, 직원에 대한 업무별 권한관리를 통해 정보보호를 생활화하고 있다. 2007년에는 ISO 27001 인증을 준비하고 있으며, 위험과 자산에 대한 분석, 보안정책을 기반으로 한 대책을 마련하고 있다. 이로써 보안을 더욱 강화하고, 그 결과를 공식적으로 인증받아 교보증권 시스템의 안정성과 신뢰성을 높이고자 한다.

보안성과 홍보해야 보안위협 줄어든다

보안성 강화를 위한 일련의 일들 중에서 보안담당자들이 가장 많이 털어놓는 고민은 위협이 증가하고 있다거나 일이 많다는 게 아니라 눈에 보이는 성과가 없다는 것이다. 가장 훌륭한 보안은 아무 문제없이 시스템이 잘 돌아가는 것이기 때문에 위험에 처하지 않으면 보안을 의식하고 있기 힘들다. 따라서 보안담당자는 누구보다 눈에 많이 띄어야 한다. 보안에 위배되는 행위를 하는 사람이 있으면 반드시 그 행위에 대해 어떤 위험이 뒤따르는지 설명하고, 눈에 보이는 성과가 있으면 적절한 수단을 통해 홍보해야 한다. 그리하여 보안이 생활의 일부분이 되어야만 보안위협은 줄어들게 마련이다.

수많은 보안솔루션 중 어떤 제품을 선택하는 것이 좋은지 결정하는 것도 보안담당자들이 머리 아프게 생각하는 것 중 하나이다. 방화벽, IPS/IDS와 같은 기본적인 보안에 P2P와 부적절한 사이트의 접근을 차단하는 L7 스위치(QoS 기능 제공), 비인가 단말기의 접근을 차단하는 IP 관리툴, 스팸 · 바이러스 메일 및 피싱 공격으로부터 사용자를 보호하기 위해 메일 필터링 시스템 구축, 유해 트래픽 차단과 웜의 확산을 방지하기 위한 백

신 프로그램을 설치한다. 직원 컴퓨터에 불법 S/W 사용을 금지하고, 윈도우 OS 자동패치 관리 시스템을 도입한다.

교보증권은 각 보안제품을 검토하고 성능을 시험하며 제품 도입의 적당한 시기와 성능을 제품 선택의 기준으로 삼았다. 초기 방화벽 제품에는 패킷 필터링 방식(Packet Filtering)이 많았지만, 성능이 떨어져 최근에는 딥 패킷 인스펙션 방식(Deep Packet Inspection)이 많이 도입된다. 그러나 딥 패킷 인스펙션은 속도가 떨어지기 때문에 이 두 방식의 중간단계인 애플리케이션 게이트웨이(Application Gateway) 방식이나 스테이트풀 인스펙션(Stateful Inspection) 방식을 많이 도입한다. 교보증권은 패킷 전송 속도에 민감하기 때문에 일반 OS보다 가벼운 제품을 선택하였다. 제품을 설치한 후에는 제품이 시스템 내에서 안정화 될 때 까지 기존 제품과 병행 사용하면서 데이터를 이관하여 교체를 완료하였다.

스팸메일은 단순한 해커 · 크래커들의 장난 이상을 넘어선지 오래 되었다. 최근에는 스팸메일을 이용해 은행을 이용하는 고객들의 정보가 유출되고 있으며, 넘쳐나는 스팸메일 때문에 정상적인 메일을 받지 못하는 경우도 생겨 업무에 지장이 많다. 이제 메일 보안은 선택이 아니라 필수가 되어 많은 조직이 메일 필터링 시스템을 구축하여 사용하고 있다. 다른 보안 시스템은 사고가 나야 투자에 대한 효과를 볼 수 있지만, 메일 필터링은 눈에 보이는 효과를 가져오므로 보안담당자들이 '생색' 낼 수 있는 좋은 기회가 되기도 한다. 시중에 판매되고 있는 메일 필터링 시스템은 스팸 차단률 90% 정도에 이르고 있어 바이러스나 피싱의 공포에서도 해방될 수 있다.

보안 효과를 수치화해 경영진 설득

보안의 효과를 눈으로 보여주는 것은 결코 쉽지 않은 일이다. 대부분의 경영진은 아직도 보안에 대한 투자를 사치로 생각하고 있어 수치로 계산된 자료로 경영진을 설득하여 투자를 이끌어내는 것은 매우 어려운 일이다. 가장 좋은 방법은 과거의 사례를 통해 ALE(연간 추정손실액)를 정량적으로 측정해 제시하거나, 최근 발생한 사고의 사례의 피해액을 산술적으로 추출하여 제시하는 방법이다. 보안의 성과가 현금화 되는 것이 아니라 해도 적절한 데이터를 통해 경영진을 설득하여 투자를 유도하는 것은 위험을 낮출 수

있는 지름길이다.

경영진을 설득하기 전에 보안담당자가 먼저 해야 할 일은 회사에서 보안이 가장 취약한 부분을 찾는 것이다. 아마도 대부분의 보안담당자들은 보안 취약성으로 '사람'을 꼽을 것이다. 보안사고의 70%는 내부 직원의 실수나 부정으로 인해 일어나기 때문이다. 보안의식 교육은 아무리 강조해도 지나치지 않는다. 직무분리는 권한을 분산하여 부정을 효과적으로 예방할 수 있으며, 직무순환은 부정을 적발하는데 효과적이다. 또한, 보안사고 예방을 위해 보안인식 교육은 필수적이다.

예를 들어 회사 엘리베이터 버튼에 '매주 목요일은 윈도우즈 업데이트의 날', 거울에는 '전화를 통한 패스워드 전송은 범법 행위입니다'라는 메시지가 붙어 있거나, PC를 부팅할 때 '불법 소프트웨어 사용에 대한 책임은 전적으로 본인에게 있습니다'라는 메시지를 클릭해야 윈도우 화면을 볼 수 있고, 스크린 세이버가 작동하고 있을 때 보안관련 퀴즈를 맞춰야 원래 화면으로 돌아올 수 있다면 보안의 생활화를 위한 직원 의식교육이 될 수 있다.

보안에는 마침표가 없다. 무엇을 한다고 해도 새로운 위협은 항상 존재할 것이며 영원히 안전한 시스템이란 존재하지 않는다. 끊임없이 새로운 위협에 대처하며 더욱 안전한 시스템의 구축과 운영을 위해 노력하는 것만이 보안담당자의 올바른 자세이다.

"교보증권, 단 1초의 장애도 용납 못해"

교보증권(주) IT센터 김원걸 센터장(wgkim@iprovest.com)

■ 교보증권에서는 어떤 정보보호 관련 정책들을 실행하고 있나?

정보보호 관련 IT 관리지침(정보보안 관리지침, 변경 관리지침 등)을 제정·운영하고 있다. 또, 당사가 '주요 정보통신 기반시설'로 지정되어 있는 것과 관련해 매년 제3의 기관으로부터 취약점 분석평가를 위한 컨설팅을 받고 있다. 정보보호 관련 전산시스템을 주기적으로 점검해 사용자계정 재확인, 웹 서버 최신 패치확인, 침입차단 시스템 관리자 비밀번호 변경 로그 백업 등을 실시한다. 직원에 대한 업무별 권한관리 부여를 통해 고객계좌정보 조회 및 유출을 통제하고, 고객정보가 담긴 오프라인 문서 유출금지, 외주직원에 대해 보안서약서를 받고, 계약서 작성시 정보유출 등 보안관련 책임조항을 포함해 정보보호를 생활화하고 있다.

■ 정보보호를 위해 구축한 시스템은 어떤 것들이 있나?

외부로부터 비정상적인 접근을 차단하기 위한 방화벽과 IPS, IDS, P2P 및 부적절한 사이트의 접근을 차단하는 L7 스위치(QoS 기능 제공), 비인가 단말기의 접근을 차단하는 IP 관리툴을 구축해 사용하고 있다. 또, 스팸·바이러스 메일 및 피싱 공격으로부터 사용자를 보호하기 위해 메일 필터링 시스템을 구축했으며, 유해 트래픽 차단과 웜 확산을 방지하기 위해 사내 모든 PC에 백신을 설치했다. 한편, 불법 S/W 사용을 금지하고 윈도우 OS 자동 패치 관리 시스템도 도입해 사용하고 있다.

■ 최근 기업에서 내부정보 유출현상이 급증하고 있는데, 이에 대한 대비책은 무엇인가?

중요정보의 보호를 위해 입사시 경영진이 보증하는 비밀유지 동의서와 AUP(Acceptable Use Policy)를 작성 확인하며 보관하고 있다. 물리적, 논리적, 관리적 보안을 통해 정보유출 가능성을 낮추고 있으며, 정기적인 보안인식 교육을 통해 직원들의 보안의식을 향상시

키고 있다. 퇴사시에는 계정처리 정책에 따라 ID를 삭제하고 개인 전산장비를 회수하고 있다. 이메일을 통한 유출에 대비하여 이메일 송수신 내역도 기록 · 관리되고 있다.

■ 사내 직원들에게 정보보호 관련 교육은 어떤 방법으로 실시하고 있나?

정보보호 전담인력의 경우, 사외 교육기관을 통해 관련 교육을 수강하도록 하며, 관련 자격증 취득에 대한 권유를 통해 관련 지식을 습득하도록 하는 등 교육기회를 제공하고 있다. 신규 직원 입사시에도 '신입직원 교육 프로그램'에 보안인식 교육을 포함하여 오프라인 교육도 실시하고 있고, 보안의 중요성에 대해 인지시키고 있다. 입사 후에는 정기적으로 사이버 강의를 통해 보안인식 교육을 실시하고 그 성과를 측정하고 있다.

■ 사내 직원들이 사용하는 PC는 어떻게 관리되고 있나?

모든 사내 PC에 대해 사용자의 이력을 관리하고 있으며, 불법 트래픽을 차단하기 위한 개인 방화벽과 웜 · 바이러스를 예방 및 치료하는 상용 백신이 깔려있다. 또, PMS를 사용해 자동으로 윈도우 패치관리가 이루어지고 있고, 불법 사용자를 차단하는 IP 관리 툴과 불법 사이트 접근을 차단하는 L7 스위치가 사용자 PC 보안을 지켜주고 있다. 장비 회수에는 7회 정도의 포맷으로 하드디스크 초기화 작업을 거치고 폐기시에도 정보 유출을 차단하기 위해 철저한 PC 폐기관리를 하고 있다."

■ 사내에 정보보호 관련 인력은 몇 명인가?

침해사고대응팀(CERT)은 4명으로 구성돼 있지만 직원들의 적극적인 동참이 없으면, 완벽한 정보보호는 불가능하다. 그래서 모든 직원이 정보보호 인력이라고 생각한다.

■ 올해 IT센터 내에서 계획이 있다면?

전자금융거래법이 시행되면서 금융사가 부담해야 하는 부분이 강화됐다. 문제가 발생하면 금융사에서 책임을 져야 하기 때문에 IT센터의 역할이 예전보다 더욱 중요해졌다. 따라서 고객 정보보호와 각종 불법침해사고가 발생하지 못하도록 보안에 더욱 신경을 쓸 계획이다.

08

㈜이글루시큐리티 보안관제센터 선임컨설턴트 안선옥
soahn@igloosec.com

보안은 기술이 아니라 관리

통합보안관리 솔루션과 서비스를 제공하고 있는 ㈜이글루시큐리티는 고객의 정보자산을 안전하게 관리하기 위한 보안정책을 마련하였다. 통합보안관제 시스템과 중앙집중관리로 보안담당자 업무의 70%를 줄였으며, 전 임직원에게 '개인정보 유출예방 10계명'을 교육하고 있다. 보안을 위해 보안솔루션 도입도 중요하지만 관리와 효과적인 운영이 더욱 중요하기 때문이다.

우리나라는 IT 강국으로 급부상하면서 정보보호에 주력하지 않아 사이버 침해라는 대가를 톡톡히 치르고 있다. 사이버 테러는 사회 전반으로 빠르게 확장되고 있으며 급속도로 지능화 되고 있지만, 이를 저지하려는 노력과 인식은 절대적으로 부족하다. 진정한 IT 강국이 되기 위해서는 정보보호에 대한 인식 제고가 시급하지만, 아직도 IT 시스템을 구축할 때 정보보호는 가장 마지막에 고려되고 있다.

정보보호 관련 2006년의 가장 큰 사고는 엔씨소프트가 리니지 명의도용 사건으로 8500여명의 이용자에게 집단 소송을 당한 것이다.

또한, 전자정부 사이트에서 주민등록 등본 10만 건이 무단 발급되는 사건도 발생해 우리사회의 개인정보 보호가 매우 취약한 현실임을 여실히 드러냈다. 통계에 의하면 기업의 정보량은 매년 70% 이상 성장하고 있지만, 증가하는 비정형 정보의 90%가 관리되

지 않고 있다고 한다. 네트워크 시스템 중심의 보안이 점차 정보 유출로 초점을 옮겨가고 있는 것은 이 때문이다.

(주)이글루시큐리티에서 서비스하고 있는 사업은 고객사의 보안관제, 통합보안관제 시스템 구축 등으로 고객의 보안관련 자료와 상당히 민감한 자료를 관리하고 있어 고객정보를 보호해야 한다는 요구가 매우 높았다. 고객사에 대해 정확하게 알아야 하는 동시에, 이를 보호해야 하는 의무가 주어졌기 때문에 '개인정보 유출 예방 10계명'을 작성해 임직원에게 체계적으로 교육하고 있다.

개인정보 유출 예방 10계명

1. 인터넷에서 자료나 프로그램을 함부로 다운로드하지 않는다.
2. 개인정보, 계좌정보 등을 요구하는 수상한 이메일의 경우, 피싱이 아닌지 의심해보고 각별히 주의한다.
3. 필요없는 웹사이트는 회원가입을 하지 않는다.
4. 웹사이트 방문시 '보안경고' 창이 뜰 때는 신뢰할 수 있는 기관의 서명이 있는 경우에만 프로그램 설치에 동의한다.
5. 바이러스 백신을 설치하고 실시간 감지기능을 설정하며, 항상 최신 버전으로 업데이트 한다.
6. 최소 한 달에 한 번 이상 최신 윈도우 보안 패치를 모두 설치한다.
7. 로그인 계정의 비밀번호는 영문이나 숫자, 특수문자를 조합해 8자리 이상으로 설정하고 반드시 한 달에 한 번 이상 변경한다. 생년월일, 전화번호 등의 유추 가능한 비밀번호는 사용하지 않도록 한다.
8. 메신저로 전달되는 파일이나 이메일에 첨부된 파일, P2P 프로그램을 통한 자료 다운로드는 피하며, 꼭 필요한 경우에는 보낸 이가 직접 보낸 것이 맞는지 확인하고, 파일이 악성코드에 감염된 것이 아닌지 감염여부를 검사한 후 실행한다.
9. 외부에서 회사 내부에 접속할 때, SSL VPN을 사용하여 보안인증을 거치도록 한다.
10. 컴퓨터를 폐기할 경우에는 하드를 포맷하거나 파기하도록 한다.

직원의 보안의식 강화는 임원의 보안 마인드 수립에서부터 시작한다. 아무리 훌륭한 보안책임자가 있다 해도 경영진의 마인드가 없다면 보안강화 정책이 효과를 발휘할 수 없다. 경영진에게 '보안은 선택사항이 아닌 우리 모두의 생존전략' 이라는 생각이 없으면 보안성 강화는 요원한 일이 될 수 밖에 없다. 기업 내부보안의 중요성에 대해 다른 기업보다 빨리 인지하고 실천하는 것이 무엇보다 우선시 되어야 한다.

보안 강화 위해 보안관리자 업무 감량

보안 강화를 위해 이글루시큐리티는 보안관리자의 업무를 줄이는 작업을 시작했다. 모니터링/로그 분석, 보고서 산출 등 단순 · 반복 업무를 자사의 통합보안관리 시스템(ESM)과 중앙집중관리 및 통합보안관제 서비스 'Husky Service' 를 도입해 70% 이상의 시간과 비용절감 효과를 얻었다.

이렇게 절감된 비용과 시간으로 보호되어야 할 자산을 파악하고, 보안 프로세스를 수립하며, 취약점 분석을 시작하였다. 또한, 위험의 심각성에 따라 지표화하고, 부문별 · 자산별로 위험도를 산출하며 단계별 대응체계 구축과 효율적인 보안관리 방안을 수립하고 있다. 내부의 위험을 파악하여 침해사고 발생시 신속하게 대처하는 방안도 마련하고 있다. 보호대책은 시간이 지나면서 그 효과가 감소하게 되므로, 위험수준을 지속적으로 유지하기 위해서는 위험분석에 대한 지표측정과 위험관리가 지속적이고 반복적으로 추진되어야 한다는 점을 인지하여, 위험관리를 핵심 활동과제로 삼고 지속적인 위험관리를 위한 프로세스 마련에 힘쓰고 있다. 뿐만 아니라, 지속적이고 순환적인 형태로 위험을 관리할 수 있도록 위험관리 과정을 조직관리 과정의 일부로 포함하고 있다.

최근 보안 이슈는 '엔드유저' 이다. 보안솔루션과 보안기법의 발달로 시스템이나 서버에 대한 공격이 어려워지자 상대적으로 보안이 취약한 엔드유저를 상대로 한 공격이 발달하고 있는 것이다. 특히, 메신저나 메일을 통한 웜, 개인정보 유출은 매번 반복되는 문제이지만 그 피해는 날이 갈수록 증가하고 있다. 엔드유저 공격을 막기 위해 기업에서는 내부인의 실수를 통해 정보가 새어나가지 않도록 엔드유저의 행동 패턴을 목록으로 만들고 문제요인을 나열하여 합당한 대응방안을 정하고 철저한 교육을 실시하여야 한다. 특히, 제로데이 공격에는 엔드유저의 피해가 가장 심각하므로, 신속히 보안정보를 입수하

고, 공유하여 피해 확산을 막는 프로세스가 필요하다. 이글루시큐리티는 사내에 정보보호 공유서버를 이용해 그동안 발생했던 문제에 대한 이력관리를 시행하고, 각 사이트에서 발생하는 공격에 이용될 수 있는 문제점과 공격기법, 해결 노하우를 실시간 공유하였다. 또한, 내 · 외부의 침해사고대응팀을 이용하여 주기적으로 취약성을 점검하고, 현 보안상태 점검 수행 및 현재 설정된 보안정책의 수준을 평가하여 보안정책의 위반 여부를 파악하였다.

더욱 복잡하고 빨라진 다양한 위협요소들로부터 시스템을 보호하는데 있어 IT 시스템의 최대 복구 허용시간이 갈수록 줄어들고 있어 보안 라이프 사이클을 고려한 보안 프로세스의 체계적인 관리 필요성이 대두되고 있다.

보안은 관리로 완성된다. 효과적인 보안정책, 비용적인 측면, 결과물(Output)을 만들어 나갈 수 있도록 관리자, 실무자들도 전문적인 교육을 계속 받고 '정책-담당자-보안솔루션' 이라는 카테고리가 유기적으로 연관되어 돌아갈 수 있도록 해야 한다. 즉, 보안을 위해 보안솔루션 도입도 중요하지만 관리와 효과적인 운영이 더욱 중요하다.

09

뉴텔정보통신㈜ 대표이사 추명조
newtel@lycos.co.kr

보안솔루션 도입보다 회사 보안정책 결정이 먼저

중소기업 정보통신 시스템은 해킹의 주요 타깃이 되거나 해킹 경유지로 악용되고 있지만, 많은 중소기업이 정보보호에 힘쓰지 못하고 있다. 중소기업의 정보보호 강화를 위해서는 기업의 보안정책이 가장 먼저 결정되어야 한다. 또한, 보안정책을 관리하고 운용할 수 있는 인력과 예산을 책정한 후 기준에 따라 단계적으로 보안정책을 시행해야 한다.

정보보호는 더 이상 간과해서는 안될 문제로 떠오르고 있지만, 많은 자금력과 인력을 보유한 대기업과 달리 대다수의 중소기업에서는 정보보호에 힘쓰지 못하고 있다. 국내 기업의 대부분을 차지하는 중소기업의 정보통신 시스템이 각종 해킹 피해 및 해킹의 경유지로 악용되고 있다. 웜바이러스에 감염시 중소기업의 피해로 끝나지 않고 인터넷 망으로 연결된 사회전체로 확산될 수 있다. 그러나 중소기업 내에는 정보보호를 전담하는 조직과 전문인력이 매우 부족하다. 예산부족으로 정보보호에 대한 투자가 거의 이루어지지 않고 있으며, 체계적인 시스템을 구축하기도 어려운 상황이다. 70% 이상의 중소기업이 예산상의 이유로 방화벽이나 침입탐지 시스템(IDS)과 같은 기본적인 정보보호시스템도 갖추지 못하고 있다. 게다가 대부분의 중소기업은 정보보호에 대한 인식이 낮아 피해를 막지 못하고 있다. 실제로 보안의 기본 장비인 방화벽이 설치된 중소기업은 30%에 불

과하고, 보안정책이라곤 바이러스 백신을 설치한 것이 고작인 곳이 대부분이다. 이마저 갖추지 않은 곳도 허다해 중소기업의 정보보호 정책은 사실상 '없다' 고 봐도 지나치지 않다.

방화벽은 외부로부터 내부망의 침입을 감지하여 정보 및 자원을 보호하는 시스템으로 FTP, TELNET, WEB 등 각 서비스 별로 시스템의 IP 주소와 포트 번호를 이용하여 외부의 접속을 차단한다. 또는 사용자 인증에 기반을 두고 외부 접속을 허용하거나 차단하고, 상호 접속된 내 · 외부 네트워크에 대한 트래픽을 감시하고 기록한다. 네트워크의 출입로를 단일화해 보안관리 범위를 좁히고 접근제어를 효율적으로 할 수 있어, 외부에서 불법으로 네트워크에 침입하는 것을 방지하면서 내부의 사용자가 네트워크를 자유롭게 사용할 수 있다. 또한, 기록된 정보를 통해 어떠한 네트워크 접근이라도 그 흔적을 찾아 역추적이 가능하다.

최근에는 방화벽의 기본적인 기능 외에 웹사이트 필터링이나 컨텐츠 필터링 기능이 추가되어 액세스 차단기능을 확장하고 있다. 이러한 추가기능을 사용해 직원들이 음란 사이트와 같은 특정 컨텐츠에 액세스하지 못하도록 제어할 수 있다. 이러한 기능을 통해 음란물 뿐만 아니라 업무상 불필요한 많은 웹사이트에 대한 서비스 및 컨텐츠의 범주를 규정할 수 있다.

방화벽 구축시 장점	취약한 서비스로부터 보호	• 네트워크 보안 증가, 내부 시스템 위험 감소
	외부 시스템의 접근제어	• 허용된 접근 외의 외부 시스템 접근 차단
	네트워크 환경관련 정보 차단	• IP/DNS 통한 내부 시스템 정보유출 차단
	보안정책 마련	• WEB/E-MAIL/FTP/TELNET 접근제어. 기업 네트워크 정책 관리/적용

조직의 시스템 운영정책에 따라 방화벽 구축

방화벽을 구축할 때 주의할 점은 조직이 어떻게 시스템을 운영할 것인 지에 대한 정책을 반영해야 한다는 것이다. 대부분 중소기업은 네트워크 구조가 단순하기 때문에 방화벽 설치에 큰 어려움은 없다. 복잡한 시스템이라 해도 기업 홈페이지 운영을 위한 웹 서

버, 사내 직원을 위한 이메일 서버, 사내 정보전달을 위한 그룹웨어 정도가 도입되어 있다. 중요한 네트워크에서의 작업을 제외하고는 모든 접속을 거부하는 방식으로 시스템을 운영할 것인지, 아니면 덜 위협적인 방법으로 접속해 오는 모든 트래픽에 대해 조사하고 점검하는 방식으로 시스템을 운영할 것인지 선택해야 한다. 그 후 어느 정도 수준의 모니터링과 백업, 제어가 필요한지에 대한 기준이 세워져야 한다. 무엇을 모니터링하고, 허용하며, 거부할지 체크리스트를 작성하고 기업 전체적인 목적을 결정한다.

외부에 접근을 허용해야 하는 부분과 접근이 통제되어야 하는 부분에 대한 영역을 나누고, 네트워크의 속도와 트래픽 규모에 따라 적절한 방화벽을 선택한다. 이때, 향후 기업의 인원 증가 등의 요인으로 증가될 트래픽을 미리 고려해야 한다. 방화벽 구입과 관리, 이를 운영할 때 필요한 인력 등을 고려해 기업이 감당할 수 있는 예산범위 내에서 적절한 제품을 선택해 최소의 비용으로 최대의 효과가 이루어질 수 있도록 해야 한다.

방화벽은 가장 효과적인 정보보호 제품임에는 틀림없지만, 접근을 허용한 포트나 패킷에 대한 보안이 어렵다는 한계를 갖고 있기도 하다. 최근 가장 문제가 되고 있는 이메일을 통한 웜 바이러스는 방화벽 자체에서 메일 서비스를 차단하지 않는 이상 필터링이나 차단을 하기 어렵다. 악의적인 해커에 의한 서비스 거부공격(DOS)은 적절한 방어책이 나오지 않았으며, 시스템의 OS나 애플리케이션의 버그 문제에 대한 대응도 어렵다. 따라서 정보보호에 대한 관심으로 방화벽 도입을 고려하고 있다면 방화벽에서 제공하지 못하는 부분을 보완할 수 있는 바이러스 백신, IDS 등 다른 보안솔루션도 검토해 보는 것이 좋다.

방화벽 구축시 고려사항	기업의 시스템 운영정책	• 허용된 사이트의 접근만 허락할 것인가, 차단할 사이트를 지정할 것인가
	모니터링, 백업, 제어 수준	• 위험평가에 근거한 모니터링/백업/제어수준 결정
	경제성	• 도입비용, 운영 및 관리 비용, 인건비 등 감안

무엇보다 중요한 것은 시스템에 대한 점검 및 보안관리 규정의 수립 등 기업 내부적으로 정보보호를 위한 관리적인 부분에 대한 고려이다. 우리의 네트워크 환경은 하루가 다르게 새로운 위험 요소들이 등장하고 있으며, 지난 인터넷 대란과 같은 사태는 기업의 네

트워크를 한 순간에 무력화시킬 수 있다. 방화벽만 도입한다고 해서 보안문제에서 해방되는 것은 아니다. 방화벽은 단지 네트워크 상에서 정보보호를 위한 격리 · 차단만을 제공할 뿐이며, 방화벽을 도입한다 하더라도 어설픈 운용과 느슨한 정책을 채택하면 더 심각한 문제를 일으킬 수 있다. 이와 함께 기업 내부적으로도 정보보호의 중요성과 윤리의식의 뒷받침도 빼놓을 수 없는 중요한 점이 된다.

정보보호에 대한 사회적인 인식이 높아지면서
기업들이 앞 다투어 정보보호 정책을 만들고
정책수립으로 보안이 완성되었다고 여긴다.
그 결과 보안예산은 꾸준히 증가하지만,
보안수준은 제자리에 머무르게 된다.
정보보호 전문업체들이 추천하는
보안 성공사례를 통해 보면 정보보호에
성공한 기업들은 '보안의 생활화' 라 해도
과언이 아닐 만큼 일상생활에서의
보안 실천을 중시하고 있음을 알 수 있다.

정보보호
이론이 아닌
실천이 중요하다

01

㈜시큐브 정보보호SI팀 이규호 팀장
perry@secuve.com

대외적으로 노출되는 웹 서비스 서버의 보안체계 구축

이동통신 사업자 OO텔레콤에 서버보안 시큐어 OS인 Secuve TOS®를 도입한 서버보안 사업은 대외적으로 노출될 수밖에 없는 웹 서비스 서버에 대한 해킹과 정보유출 등 보안사고 발생 가능성을 제거하기 위해 OS 커널(Kernel) 레벨에서 파일시스템과 주요 서비스 보호체계를 구축해 웹 서비스 시스템에 대한 보안체계를 강화했다.

2006년에 진행된 OO텔레콤 서버보안(시큐어OS) 도입사업은 직접적인 고객서비스 업무를 수행하고 있는 웹 서비스 서버를 대상으로 수행되었다.

OO텔레콤은 최접점에서 고객을 맞고 있는 서버를 서버보안 사업의 1차 도입대상으로 선정하였다. 이 시스템은 방화벽 등 네트워크 단위에서의 보호장치가 있지만 외부에 공개되어 있으며, 외부로 열린 서비스 포트가 있어 외부의 악의적인 공격시도가 발생한다면, 제 1차 목표가 이 시스템이 될 수 있었다. 또 다른 이유는 Secuve TOS® 시스템이 시스템 커널(Kernel)에 보안 커널(Security Kernel)을 삽입하는 방식이므로, 시스템에 영향을 줄 수 있어, L4 장비에 의해 로드 밸런싱(Load Balancing)이 이루어지고 있는 시스템에 설치해 안정성을 검증한 후 확대 적용하기로 한 것이다. Secuve OS의 안정성은 널리 인정받은 것이지만, 고객이 서버보안 솔루션을 처음 접하고 있으며, Secuve TOS®

역시 처음 접하는 만큼, 고객의 이같은 요구를 수용해야 했다.

웹 서비스 가용성 확보, 정보유출 방지에 초점

웹 서버 시스템에 서버보안(시큐어OS)을 구축하면서 가장 우선시 한 것은 웹 서비스의 가용성(Availability) 확보와 고객정보와 같은 중요한 정보의 유출방지였다. 대부분의 다른 기업도 마찬가지이지만, OO텔레콤에서 웹 서버는 기업홍보와 고객지원 서비스를 24시간, 365일 지원하고 있다. 또한, 고객지원 서비스를 위해 고객인증이 필요하고, 이를 위해서는 고객정보가 필요하게 되는데, 이러한 정보가 유출되면 금전적으로 환산하기 어려울 만큼 기업 이미지에 대단한 손상을 입게 된다. 따라서 고객정보의 유출, 웹페이지 위 · 변조, 불법 시스템 다운, 불법 웹 서버 프로세스 종료 등 서비스 가용성을 해치는 위협요소를 제거하는 것이 가장 중요한 업무가 됐다. Secuve TOS® 구축과 관련한 보안정책은 이러한 위협요소로부터 보호대상 시스템을 안전하게 지켜내는 것에 초점을 맞춰 수립되었다. 이 때문에 고객 웹 서버 시스템에 대해 〈표 1〉과 같은 사항에 대한 환경조사를 실시하게 되었다.

구 분	내 용
시스템 구성	• 웹 서버 시스템의 물리적 구성도 및 네트워크 구성 조사
웹 서비스 구성	• 웹 서버 시스템 내의 디렉토리 및 프로세스 구성 조사 • 웹 서비스 포트 조사
웹 서비스 관리자/개발자 계정	• 웹 서비스 관리/개발 영역 사용자 파악 및 사용실태 조사 사용계정/접근 IP/접근방식(Telnet, SSH, dtlogin, FTP 등)

[표 1] 환경조사내역 요약

조사내역을 바탕으로 보안정책을 수립하기 시작하기 전에 웹 서버의 가용성을 위한 시스템 자체의 가용성을 확보하는 일에 착수했다. 웹 서버 프로세스도 시스템 입장에서 보면 하나의 애플리케이션이므로, 시스템의 가용성이 확보되지 않은 상태에서 웹 서버의 가용성을 확보하는 것은 불가능하다. Secuve는 시스템의 OS별로 제공하는 OS 기본 보안정책을 고객에게 제공하였으며, 주된 내용은 각종 시스템의 주요설정 파일의 위 · 변조 방

지, 시스템 로그 데몬의 불법적인 Kill 방지, 시스템 로그 파일의 위 · 변조 방지 등이다.

1	시스템 주요 설정 파일	필수
2	부팅관련 스크립트 보호	필수
3	시스템 로그 파일 보호	필수
4	시스템 로그 데몬 보호	필수
5	시스템 시간변경 방지	권장
6	시스템 명령어 변조방지	필수
7	시스템 종료/재부팅 방지	필수
8	시스템 Module 사용 감사	권장
9	시스템 Mount 사용 감사	권장

[표 2] 시스템 기본 보안정책 요약

이것으로 기본적인 시스템 보안정책은 수립되었으므로 앞서 조사한 환경조사내역을 가지고 웹 서비스 자체의 가용성 보장을 위한 Secuve TOS® 보안정책을 수립하기 시작하였다.

먼저, 웹 서버 자체에 대한 보안설정을 위해 웹 서버에 대한 Kill/Terminate 권한은 특정 시스템 관리자와 보안관리자만이 가능하도록 하고, 일반적인 Root 권한이나 일반 계정 권한으로는 웹 서버 Kill 자체가 불가능하도록 설정하였다. 웹 문서 디렉토리의 경우, 모든 사용자는 읽기만 가능하도록 하고, 개발자만 특정 기간 동안 쓰기 권한을 갖도록 하였다. 웹 페이지 위 · 변조를 방지하고, 웹 페이지 업데이트는 내부적인 업무 절차에 따라 정해진 기간동안 개발자가 업데이트 하도록 설정하였다. 웹 서버에 대한 네트워크 접근은 환경조사에 의해 파악된 결과에 따라 등록된 Source IP에서만, 등록된 계정으로 로그인하도록 설정하여, 시스템관리자와 보안관리자, 개발자만이 시스템에 로그인할 수 있도록 설정하였다.

보안은 최악의 경우를 대비하는 자세가 중요

고객정보 유출 관련된 Secuve TOS® 보안정책은 일반적으로 많이 사용되는 공격기법들을 방어하기 위하여 /tmp나 운영중인 게시판의 upload 디렉토리에서의 모든 파일들에 대한 실행권한을 제거해 웹 서버 자체 취약성 및 게시판 upload 취약성에 의한 실행파일 실행, DB Query 실행 등을 제한하도록 설정하였다. 이와 더불어, 운영중인 사이트가 XSS, SQL Injection 등에 취약한 페이지로 제작되었는지 점검하고, 점검결과와 권고사항을 전달하여, 웹 페이지 자체의 취약성으로 인해 고객정보가 유출될 수 있는 상황을 방지할 수 있도록 하였다.

고객정보 유출방지는 이 사업의 시스템 현황파악에서 가장 큰 문제로 지적된 것이다. 시스템 접근에 대한 내부통제가 방화벽과 ID/PW에만 의존하고 있으며, ID와 패스워드의 관리가 전혀 이뤄지고 있지 않았던 것이다. OO텔레콤의 웹 서비스 서버는 대외 고객서비스를 하고 있으며, DMZ에 있는 서버인 만큼 외부에서 들어오는 트래픽에 대해 방화벽과 네트워크 기반 침입탐지 시스템을 운영하고 있었다. 그러나 시스템에 더 큰 피해를 입힐 수 있는 공격자는 내부 공격자라는 인식이 부족한 상태였다. 같은 임직원끼리 서로를 잠재적인 범죄자로 간주하고 바라보아야 한다는 의미는 아니지만, 보안은 최악의 경우를 대비하는 자세가 중요하다.

내부 임직원 뿐 아니라 단기간 출입하는 외주직원이 많아 ID와 패스워드뿐만 아니라 접근 가능 IP 등 여러 가지 측면에서 철저한 통제가 시급히 필요했다. OO텔레콤의 서버는 내부 네트워크에서는 ID/PW만 알아도 어떤 행위도 시도할 수 있었으며, ID/PW에 대한 정확한 파악 및 관리조차 이루어지지 않고 있었다. 이번 서버보안 도입 사업을 계기로 이에 대한 철저한 현황조사와 Secuve TOS®에서 생성된 로그 분석을 통해서 현실을 정확히 파악하고, 내부적인 관리정책을 수립할 수 있는 계기가 마련된 것만으로도 고객은 큰 수확을 얻었다고 볼 수 있다.

보안솔루션, 시스템 성능저하 막는 것이 관건

이번 사업을 성공적으로 완수할 수 있었던 핵심 포인트는 시스템 성능저하를 막는 것

이었다. 서버 보안을 도입할 경우, 일반 사용자가 느낄 수 있을 만큼 심각한 수준은 아니지만, 일반적으로 3~5% 이내의 성능저하가 일어나게 된다. 게다가 OO텔레콤의 웹 서비스는 한 서버에서 3개의 사이트를 운영하는 등 시스템 자체만으로도 CPU 부하율이 98%까지 올라가는 시스템이 있다. 자칫하면 서비스 응답시간이 매우 늦어질 수 있어 이에 대한 해결책이 필요했다. 각 시스템에 대한 부하율을 분석하고, Secuve TOS®의 튜닝 기능을 통해 반드시 통제해야만 하는 기능만 활성화하는 작업을 진행하였다. 이로써 주간 업무시간대의 시스템 성능에는 큰 문제가 일어나지 않았다.

가장 난제는 매일 0시에 각 웹 서버에서 데몬을 재시작하는 과정이었다. 이 서버들은 서버의 Rebooting 하는 것이 아니라 웹 서버 데몬을 멈추었다가 다시 시작하게 되어있었다. 각 서비스 별로 L4에서 로드 밸런싱(Load Balancing)을 수행하고 있었으나, 순차적으로 1분 간격으로 웹 서비스를 재시작할 경우, 한쪽으로 서비스가 몰리게 된다. 새벽 0시는 사용자가 적지 않아 한 시스템이 고객의 요구를 담당하기에는 역부족인 상황이 발생하게 되었다. L4 장비가 웹 서버 데몬이 재시작된 것을 빨리 감지하지 못해 응답시간이 현저히 늦어지거나 웹 서버 데몬이 비정상적인 동작을 수행하는 경우가 있었다. 게다가 L4 장비는 OO텔레콤과 유지보수 계약이 체결되지 않아 제조사나 공급사를 통한 지원도 받기 어려웠다.

Secuve는 OO텔레콤과 함께 각 시스템과 사이트 별로 Secuve TOS®의 튜닝과 웹 서버 데몬의 재시작 스크립트를 편집하여 재시작 간격을 조절하는 등 2주간에 걸친 야간 테스트 작업을 통해 서비스가 정상적으로 구동되도록 하였다.

Secuve TOS® 구축사업에서 문제가 됐던 또 다른 한 가지는 통합보안관리 시스템(ESM : Enterprise Security Management)과의 연동이었다. Secuve TOS®는 고객이 사용중인 ESM과 이미 연동이 되는 제품이었지만, Secuve TOS®가 설치되는 시스템에 ESM 에이전트가 모두 설치되어 있지는 않았다. 여분의 ESM 에이전트 라이센스는 1 Copy 밖에 보유하고 있지 않았으며, 추가 예산도 확보할 수 없어 자체적으로 ESM 연동을 실현해야 했다.

초기에는 Secuve TOS®의 에이전트에 해당 기능을 추가해, ESM에 직접 로그를 전송하도록 하려고 하였다. 그러나 ESM 에이전트의 라이센스는 에이전트 설치시 필요한 것이 아니라, ESM 매니저가 로그 수집 노드(Node)를 얼마나 연결할 수 있는가를 라이센스

로 산정하는 것이었다. 따라서 Secuve TOS® 에이전트에서 ESM으로 직접 로그를 전송한다면, ESM 에이전트가 설치되지는 않았지만, ESM 에이전트를 설치한 것과 동일한 라이센스 카운트를 하게 되어 1개 에이전트의 로그밖에 연동할 수 없는 상황이었다.

이를 대신해 ESM 에이전트를 Secuve TOS®의 Manager에만 설치하고, Secuve TOS®의 AlertPoint 기능을 통해서 ESM 에이전트에 Secuve TOS®의 로그를 전송하는 방식을 선택하였다. 이를 위해서는 Secuve TOS®의 AlertPoint 기능과 ESM 에이전트를 약간 수정하였다. Secuve는 고객과 ESM 업체와 회의를 통해 전체 구성설계와 통신 프로토콜을 정의하여, 하나의 ESM 에이전트를 통해 13개의 Secuve TOS® 에이전트가 전송하는 로그를 ESM과 연동할 수 있도록 구축하였다.

기업 내부 현황파악, 관리정책 수립이 가장 큰 수확

OO텔레콤의 대외적인 홍보 및 고객 서비스를 제공하고 있는 웹 서버에 서버보안 시큐어 OS인 Secuve TOS® 도입 사업을 통해 OO텔레콤은 내 · 외부 사용자의 불법적인

[그림 1] Secuve TOS 운영방안 중 조직별 역할(조직 R&R 정리)

시스템 접근차단과 웹 서비스 · 웹 서버 시스템의 가용성 확보, 고객 정보보호라는 보안성 향상이라는 목적을 달성했다.

이보다 더 큰 수확이라면 이 사업을 통해 OO텔레콤의 내부 현황을 파악하고, 이를 관리할 수 있는 정책을 수립했다는 점이다. OO텔레콤이 운영하던 계정관리 시스템은 일반 계정과 관리자 계정으로 나뉘기는 했으나, 접근권한에 대한 현황파악조차 어려운 상황이었다. 이번 서버보안 사업을 통해 이러한 것들을 정보보안팀에서 모두 통합 관리할 수 있게 되어 언제라도 발생할 수 있는 잠재적인 위협을 확실히 제거할 수 있는 기회가 되었다.

그 예로, Secuve는 내부조직간의 R&R(Role & Responsibility)을 제시하여, 각 조직간의 업무분담을 명확히 하도록 하였다. 이와 더불어 Secuve TOS® 운영상 발생할 수 있는 각 상황에 대해, 업무의 워크플로우(Workflow)와 해당 플로우(Flow) 상에서의 각 조직의 수행역할을 제시했다. 이러한 산출물을 통해 고객은 단순히 하나의 솔루션을 도입하고 설치한 것이 아니라, 작은 규모의 보안컨설팅을 받은 것과 같은 효과를 얻을 수 있었다. 또한, OO텔레콤이 운영 중인 시스템과 정보보안을 담당하고 있는 조직에 대한 이해를 높일 수 있었던 것으로 보인다.

02

㈜에이쓰리시큐리티컨설팅 보안전략팀 임창욱 과장
ihmcw@a3sc.co.kr

엔드 포인트 보안강화로 주요 정보와 애플리케이션 보호

서버기반 컴퓨팅을 통한 엔드 포인트 보안강화로 중요한 정보와 애플리케이션을 보호하고, 장비나 연결방식에 관계없이 필수적인 업무 자원에 안전하게 접근할 수 있도록 한다. 또한, 클라이언트 애플리케이션의 빠른 설치와 간편한 버전 관리, 애플리케이션 버전 및 보안 패치 등의 표준화를 이룰 수 있다.

서버기반컴퓨팅(SBC : Server Based Computing)이란, 데이터와 애플리케이션을 서버로 집중시키고 클라이언트를 단순한 입출력 단말기로만 사용하는 기술을 말한다. 시스템 자체만을 놓고 봤을 때 정보보호 시스템이라 할 수 없지만, 효과적이며 효율적인 엔드 포인트 보안강화로 보안목표와 IT 인프라스트럭처의 목표도 달성할 수 있다.

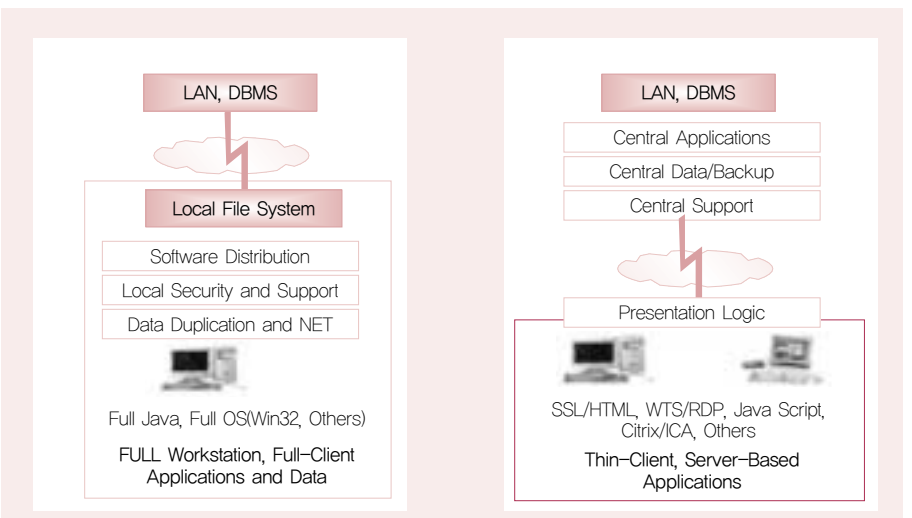
SBC라는 개념이 처음 등장한 것은 지난 1997년 오라클이 네트워크 컴퓨터를 소개할 때였다. 당시에는 네트워크 인프라가 미흡하였고 저가형 PC가 출현하면서 네트워크 컴퓨터에 대한 필요성이 낮았으며, 무엇보다 네트워크 컴퓨터 시장이 성숙하지 못했기 때문에 별다른 호응을 받지 못했다. 그러나 2000년을 전후해 다양한 바이러스에 의한 피해와 정보유출 사고가 등장하면서 정보보호 관점에서 서버기반 컴퓨팅이 재조명되었다. 최근에는 기가비트 이더넷과 초고속 인터넷 인프라가 구축되고 네트워크 컴퓨터 자체의 성

능도 개선돼 SBC 도입이 지속적으로 증가되고 있다.

일반적으로 기업이나 각 조직이 SBC를 도입하는 이유는 조직에서 요구하는 관리적인 측면과 보안측면에 가장 잘 부합되기 때문이다. SBC를 활용할 때 애플리케이션의 관리와 배포를 서버에만 적용하면 자동적으로 모든 클라이언트에 일괄 적용할 수 있어서 일관된 애플리케이션 버전 관리가 가능하다. 또한, 중요한 애플리케이션과 데이터가 서버 단위에 저장되기 때문에 불법 정보유출을 예방할 수 있고 일관된 보안 패치 관리를 통해 웜 바이러스 등의 보안위협에도 효과적으로 대응할 수 있다. 더불어 자체 보안프로토콜을 사용하여 클라이언트에서 애플리케이션 실행시 서버에서 동작하는 스크린 업데이트, 파일, 오디오, 클립보드 등의 서버에서 해석된 정보만을 받기 때문에 클라이언트에는 실제로 저장할 수 없다.

SBC, 정보유출 방지 업무연속성 확보

SBC가 갖고 있는 엔드 포인트 보안기능은 크게 다섯 가지 측면에서 볼 수 있다. 첫째는 정보유출 방지와 업무 연속성을 확보한다는 것이다. SBC는 각 조직의 데이터 저장 정



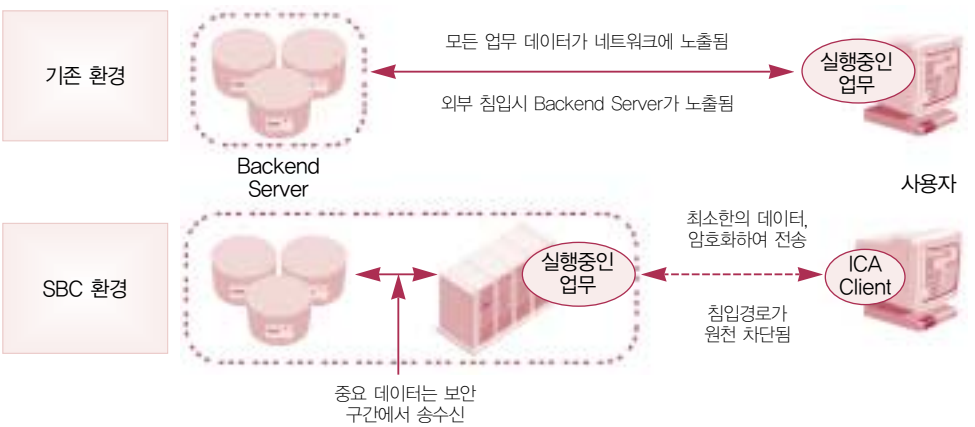
[그림 1] 기존 아키텍처와 SBC 아키텍처 비교

책에 따라 달라질 수 있으나, 기본적으로 데이터를 사용자 PC에 저장하지 않고 서버 단에 저장하도록 강제하고, 서버 단의 보안을 강화한다.

USB나 CD 등의 저장매체에 대한 통제도 서버 단에서 일괄적으로 이뤄지며, 일반 컴퓨팅 환경보다 강력한 저장매체 통제가 가능하다. 이동형 저장매체를 이용한 정보유출 가능성을 최소화할 수 있어 악의적인 내 · 외부자의 정보유출이 어렵고, 노트북 등 이동형 장비를 분실했을 때도 이동형 장비에 중요 정보가 저장되어 있지 않기 때문에 정보유출 사고를 예방할 수 있다. 중요한 정보를 서버에 저장하기 때문에 사용자의 관리 소홀로 인한 정보유실도 예방할 수 있으며, 정보유실로 인한 업무중단을 방지할 수 있다. 사용자가 어떤 위치와 환경에 있다 해도 일괄적으로 업무를 처리할 수 있도록 지원하여 업무의 연속성을 확보한다.

이처럼 SBC 환경에서는 조직 내부의 중요정보에 대한 외부유출을 원천적으로 차단할 수 있으며, 필요에 따라서는 DRM(Digital Lights Management)을 연계시켜 주요 정보자산에 대한 보안을 강화할 수 있다.

두 번째는 접근통제의 측면에서 보안기능 강화이다. SBC는 언제, 어디서나 모든 사용자가, 모든 네트워크에서, 모든 전달경로를 통해 애플리케이션과 정보에 안전하고 쉽게 접근할 수 있도록 한다. 이를 위해서 'Access Scenario'에 따라 중앙 서버가 사용자

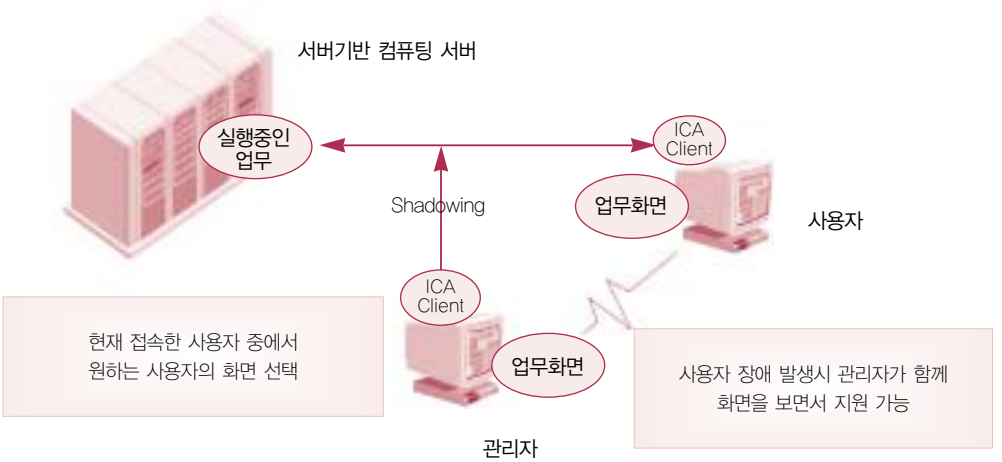


[그림 2] SBC를 통한 네트워크 보안

의 접근권한을 설정해, End-to-End 암호화 연결로 OTP(One-Time Password)나 스마트카드, 생체인식 기술 등 강력한 인증기능을 통해 사용자 접근을 통제할 수 있다.

기존 환경에서는 사용자 PC와 서버간 업무 데이터를 전송할 때 네트워크에 정보가 노출되지만, SBC에서는 100% 서버 리소스를 사용하여 애플리케이션을 실행한 후 결과값만 사용자에게 암호화해 전송한다. 가상화된 애플리케이션 환경을 제공하여 Interface와 Execution을 분리하기 때문에 효과적인 네트워크 보안도 가능하다. Keystroke이나 마우스 클릭, 스크린 업데이트 정보만 전송하기 때문에 허가받지 않은 사람이 데이터를 얻게 된다 해도 안심할 수 있다.

SBC에서는 중앙 집중화된 시스템을 구성해 빠른 애플리케이션 배포가 가능하므로 바이러스가 발생했을 때 이와 관련된 보안 패치를 빠르고 효과적으로 모든 사용자 PC에 적용할 수 있다. 모든 소프트웨어 설치를 중앙에서 통제하기 때문에 사용자의 불법 소프트웨어 설치를 사전에 차단하기도 한다. 또한, 현재 접속한 사용자가 실행중인 업무의 화면을 관리자가 동시에 볼 수 있는 기능을 지원하는 솔루션이 있다. 이를 이용하면 원격지의 사용자가 업무중 발생하는 문제에 대해 관리자가 화면을 보면서 지원할 수 있어 빠른 대처와 복구가 가능하다. 의심스러운 사용자의 업무수행 내용을 관리자가 모니터링할 수 있어, 악의적 사고를 미연에 방지할 수 있다.



[그림 3] 서버 기반 컴퓨팅에서 제공하는 사용자 지원 및 감시기능

해외 사용자와 설계도면 공유하면서 보안 유지

SBC를 도입해 보안을 강화한 실제 사례를 통해 살펴보면, 국내 대표적인 반도체 기업인 A사는 해외 등에서도 사내와 동일한 애플리케이션을 사용하고, 다수의 PC에 애플리케이션을 자주 설치하거나 제거하는 교육장에서 효율적인 관리환경을 요구했다. SBC 도입으로 인해 A사는 해외 사용자와 설계도면을 효율적으로 공유하면서 설계도면 보안을 유지할 수 있었으며, 해외에 출장간 직원이나 해외 법인 사용자에게도 국내와 같은 애플리케이션을 사용할 수 있게 할 수 있었다. 교육장의 애플리케이션 관리도 물론 가능했다.

국내의 대표적인 제2 금융권 기업인 B사는 M&A 이후 시스템 통합문제를 효과적으로 해결하는 것이 관건이었다. SBC 도입 후 B사는 애플리케이션과 데이터를 모두 중앙에서 관리해 사용자에게 애플리케이션을 따로 배포할 필요가 없게 돼 최단시간에 최소의 비용으로 관리를 단순화 할 수 있었다.

SSL과 VPN을 통해 언제 어디서든 안전하게 인증받은 사용자가 정보에 액세스하여 업무를 수행하고, 어떤 단말기를 사용하든지 관계없이 안전하고 쉽게 업무를 지속해 안전성과 유성을 갖추었다. 애플리케이션을 모두 중앙 서버에 집중시켜 M&A 이후, 서로 다른 시스템을 쉽게 관리할 수 있었다.

보안이 최대 이슈가 된 국가기관인 C사의 경우, 터미널 서버 방식으로 인터넷 망과 내부 망을 분리해 외부로부터의 해킹 및 바이러스에 대한 위험을 원천적으로 방지할 것을 요구했다. SBC는 인터넷 사용의 중앙집중화와 관리를 통한 보안성을 확보했으며, 네트워크 분리에 따른 비용을 대폭 절감하고 망 분리시 발생할 수 있는 사용자의 불편함을 해소해 생산성을 높여 비용을 절감할 수 있었다.

이같은 사례를 두고 봤을 때 SBC는 기업환경에서 중요 정보와 애플리케이션을 보호하고, 장비와 연결방식에 관계없이 필수적인 업무자원에 안전하게 접근할 수 있는 기능을 제공한다고 할 수 있다. 애플리케이션 개발단계에서는 클라이언트 애플리케이션의 빠른 설치와 버전관리를 간편하게 할 수 있으며, 보안 패치를 표준화할 수 있다. 멀리 떨어진 지점과 지사 사무실, 혹은 해외나 지방 출장, 재택근무자들도 회사의 중요한 애플리케이션을 활용해 업무를 수행할 수 있으며, 저속의 네트워크에서도 본사의 LAN과 같은 성능을 보장받을 수 있다.

03

㈜제이컴정보 보안기술연구소 문제헌 팀장
suroot@jcsi.co.kr

통합 보안관리로 보안관리 포인트 일원화

지방자치단체나 정부조직에 설치된 네트워크 망의 보안시스템은 내부에서 개별적이고 단편적으로 흩어져 있어 실시간 위협에 적극적으로 대처하지 못해 통합 관리할 수 있는 보안시스템이 요구되었다. 시스템의 보안 취약성을 분석하고, 보안의 관리 포인트를 일원화하며, 통합관제 시스템과 관제센터를 구축해 보안관리의 효율성을 향상시켰다.

기업도 마찬가지이지만 특히 정부조직은 다양한 대국민 서비스를 실시하기 위해 여러 가지 시스템을 연차적으로 도입하면서 각 시스템 내부에 보안관리 체계를 구축하고 있다. 그러나 조직 전체의 시스템에서 보았을 때 보안관리 체계가 시스템 내부에서 개별적으로 흩어져 있어 보안관리에 인력과 비용이 많이 소요되며, 교묘하고 정교한 위협에 대응하지 못하는 상황에 처하는 경우가 많다. 통합 보안관리 시스템은 보안관리 체계를 중앙에 집중시켜 일관성 있는 보안관리를 통해 보안업무에 과도한 재원이 투입되는 것을 막고, 관리자를 일원화 해 긴급상황이 발생했을 때 신속하게 대응할 수 있도록 한다.

정보보안 시스템을 통합, 제어함에 따라 방화벽과 IDS 보안정책 변경, 사용자 ID와 비밀번호, 주요파일 무결성 관리 등을 효율적으로 추진할 수 있어 사이버 침해사고에 빠른 대응이 가능하다. 또한, 보안관련 작업 이력에 대한 데이터베이스를 구축하고, 사이버

포렌식 자료관리를 통해 보안 · 침해사고에 대한 히스토리 관리기능을 강화할 수 있다.

제이컴정보가 지방자치단체인 ○○구청과 정부조직인 ○○원에 통합 보안관리 시스템인 'e-Pentagon ESM'을 구축한 사례를 통해 살펴보면 통합 보안관리 시스템은 안정성과 신뢰성을 높여 대국민 서비스의 질을 향상시키며, 국가기관의 표준을 선도해 경쟁력을 높일 수 있다는 장점을 갖고 있다.

통합 보안관리로 구민 서비스 향상

문화행정, 고객행정, 가치행정, 창조행정, 효율행정, 열린 행정을 주요 전략 목표로 하고 있는 ○○구청은 구민들에게 각종 서비스를 제공하기 위해 여러 전산시스템을 도입하고 있다. 그러나 각 시스템의 관리방법이 달라서 NMS(Network Management System) 기능이나 보안관리, 운영업무, 관리인력 전문성 확보가 어렵고, 보안시스템 활용도도 낮았다. ○○구청 시스템은 내 · 외부망에 구축된 방화벽, IDS, VPN 등 보안장비와 스위치, 라우터 등 네트워크 장비 등이 구성되어 있지만, 지능화되고 자동화된 해킹과 바이러스의 위협에 대응하지 못하고 있는 실정이었다.

○○구청 시스템에는 각 동사무소 간의 네트워크 관리기능과 상급기관과 자동화된 업무수행 체계를 구축하기 위해 기존에 구축된 네트워크, 광통신망(SDH), Metro Ethernet, Service Server Farm, VoIP와 각종 보안장비에 대한 통합 보안관리(ESM), 네트워크 관리(NMS), 시스템 관리(SMS)가 필요했다.

또한, ○○구청은 구민들에게 보다 품격 높은 서비스를 제공하기 위해 시스템 확장을 계획하고 있어 인적 · 물리적 소요를 최소화할 수 있는 방안이 요구됐다.

이를 위해서는 시스템의 안정성과 신뢰성을 높이고, 시스템 간 연계성이나 유연한 확장성을 높여, 안정적이고 능동적으로 운영될 수 있는 온라인 전산업무 체계와 전사적인 통합 보안관리 · 관제 시스템이 필요했다.

'○○구청 통합 보안관리 시스템 구축' 사업의 핵심은 단편적이고 개별적으로 흩어져 있는 보안체제를 통합시켜 일상적인 위험에 실시간으로 대응할 수 있도록 하는 것이었다. 단일화된 통합 관제 시스템을 제공하고, 웜과 바이러스의 위험으로부터 정보자산을 보호하며 모든 시스템을 한 눈에 볼 수 있는 관제센터를 구축해 상부기관의 감사와 지침

에 능동적으로 대처할 수 있도록 하는 것이 필요했다. 이는 ○○구청을 다른 구청보다 앞선 보안관리 전문성 확보로 대외 경쟁력 향상을 기대할 수 있는 사업이었다.

사업을 시작하면서 가장 우선순위를 둔 것은 보안관리 전문성 향상을 위한 통합 보안관리 시스템(ESM)과 침입차단 시스템(IPS)의 도입이었다. 시스템 내 · 외부망에 별도로 ESM과 IPS를 도입하고, 정보화 사회에 맞는 신속하고 안전하며 쾌적한 전산실을 만들어 각종 장비의 상황을 실시간으로 분석하고, 이를 토대로 전사적인 관리와 운영의 효율성을 향상시키기 위해 통합 보안상황(관제)센터를 구축하였다.

㈜제이컴정보는 4주간 ○○구청의 요구사항을 수렴하고, 시스템, 네트워크, 보안시스템을 분석한 후 통합 보안관제 시스템을 구축하였다. 관리자 교육과 기술이전을 완료해 통합 보안관제 시스템이 원활하게 운영되게 하고 있으며, 시스템이 완벽하게 안정될 수 있도록 지속적으로 기술지원을 하고 있다.

보안관리 기능 강화는 물론이고, 각 동사무소간 네트워크 관리는 e-Pentagon ESM의 전용 통신계층을 통해 기존 NMS의 대량 이벤트와 보안시스템의 이벤트를 한꺼번에 처리할 수 있게 되었다.

'○○구청 통합 보안관리 시스템 구축' 사업을 통해 ○○구청은 내부에 산재되어 있던 단위보안 시스템을 체계적이고 효율적으로 관리, 운영해 보안을 집중하고, 중앙에서 통제할 수 있게 되었다. 이벤트의 감사와 관리수행에 있어서 전문성이 확보돼 업무 효율성 또한 증대되었다. 기술적 측면에서 확장성이 보장되었고, 새로운 보안시스템을 추가할 때 연동과 통합관리가 용이하게 되었으며, 중단없는 서비스가 가능한 시스템이 준비되었다.

상부기관 감사와 지침에 대한 능동적인 대처방안이 마련되었으며, 관공서의 표준화를 선도해 대외 이미지도 높아졌다. 안정적인 운영기반 지원을 통해 외부 서비스에 대한 신뢰도를 높이고, 선진 관공서 시스템의 일환으로 타 관공서 보다 앞선 보안관리 전문성을 확보하게 되어 대외 경쟁력을 갖추게 되었다.

통합 보안관리로 보안 취약성 최소화, 보안비용 절감

○○원은 2001년 주요 정보통신 기반시설로 지정되었으며, 보안조직의 유기적인 대응

프로세스로 위기관리와 대응능력 향상이 요구되었다. 개별로 적용되던 보안정책을 통합 관리하여 보안업무의 효율성을 높이고, 중앙집중적인 실시간 보안관리 체계가 필요했다.

○○원의 네트워크 망은 백본 라우터와 백본 스위치로 구성되어 있었다. 지능화되고 자동화된 해킹과 바이러스의 위협에 대응하기 위해 국가망 인터넷 서버팜 보안장비로 방화벽 7대와 침입탐지 시스템 3대 등의 포인트 보안솔루션을 도입, 운영하였다. 그러나 ○○구청과 마찬가지로 보안장비의 관리 포인트가 단편적이고 개별적으로 흩어져 있어 상

[그림 1] ○○원 네트워크 구성도

존하는 위험에 실시간 대응할 수 있는 관리체제는 미흡한 편이었다. 이를 해결하기 위해 운영지원 시스템과 통합 보안관리 시스템을 상호 연동해 ○○원 망의 통합 관제 시스템으로 발전시켜야 했다.

○○원의 통합 보안관리 시스템 구축사업을 위해 우선 기존에 구축된 방화벽과 IDS 등의 보안장비에 ○○원 통합 보안관리 시스템 에이전트를 설치하였다. 이를 통해 보안 로그를 수집하고 수집된 보안 로그는 통합 보안관리 서버에서 분석하도록 시스템을 구성하였다. 신속한 보안관련 보고 및 대응체계 확립을 위하여 모니터링 체계를 단일화하고, 자동화 보고서, 긴급 상황에 대처할 수 있는 기능개발을 추진했으며, 보안정책 수립을 위한 취약점 분석, 보안 로그 분석을 실시하였다. 운영의 효율성을 위하여 ○○원 운영지원 시스템인 망 관리 시스템, 트래픽 분석 시스템, 유해 트래픽 탐지시스템, 유해 트래픽 차단 시스템의 관리화면 통합을 추진하였다. 마지막으로 운영지원 시스템 관리화면을 통합해 초기 관리화면을 개발하였다.

통합 보안관리 시스템인 e-Pentagon ESM은 ○○원 내에 위치한 보안장비에서 발생되는 대량의 이벤트에 대해 집중화된 통합관리를 수행하면서 신속한 대처와 보안정책 수립을 통해 중요한 시스템과 자산을 보호하는데 능동적으로 대처할 수 있는 방안을 제공하였다. 시스템, 보안장비 외에 네트워크 장비들에 대해서도 통합 보안관리를 제공하며, 향후 타 망과의 연계를 통해 완벽한 통합 보안관제 서비스를 제공하게 되었다.

이 사업을 통해 ○○원은 전사적 통합 보안관리 · 관제 시스템을 통한 보안 취약성을 최소화할 수 있었으며, 관리자 기능을 일원화해 긴급상황이 발생했을 때 신속하게 대응할 수 있는 능력이 강화되었다. 또한, 일관성 있는 보안관리를 통해 보안업무에 투입되는 비용을 줄였으며, 이기종 시스템 운영에 따른 지적 업무 부담과 관리비용이 감소되었다. ○○원 운영지원 시스템의 관리화면을 통합해 운영의 효율성을 증대하고, 취약점 분석, 보안 로그 분석을 통해 ○○원 특성에 맞는 보안정책을 수립해 사이버 침해사고에 대한 신속한 대응능력을 강화하였다.

국가기관, 통합 보안관리로 장애 · 중단없는 서비스 제공

국가기관이나 지방자치 단체 등 보안이 특히 강화되어야 하는 조직에 통합 보안관리

시스템을 도입해 국민들에게 장애와 중단없는 서비스를 제공할 수 있다. 그러나 새롭게 구축한 시스템을 안정화하고, 구성된 각종 자원을 효율적으로 유지 · 관리할 수 있도록 지속적인 유지 · 보수가 필요하다. 또한, 도입된 신규 시스템을 독자적으로 운영하기 위해 전문적인 기술인력과 다양한 기술경험이 필수적이므로, 운영담당자에 대한 정기적인 교육과 기술지원이 있어야 한다. 중단없는 서비스를 위해서는 운영전문가 양성을 할 수 있는 최적화된 교육 훈련체제를 정립하고 운영자에 대한 기술이전 교육도 이루어져야 한다. 이로써 운영상 발생할 수 있는 문제를 최소화하고, 자체적인 서비스 개선과 기술능력 배양도 이루어질 수 있다.

04

㈜잉카인터넷 솔루션사업부 기술지원 1팀 장민석 팀장
msjang@inca.co.kr

중앙에서 개별 PC 관리해 보안 취약성 해결

전국적인 지사 및 영업망을 가진 조직의 경우, 각 지사와 영업망의 개별 PC 보안이 취약하여 이를 통한 정보유출이나 보안사고가 일어나게 된다. PC 보안체계를 잘 갖춘다 해도 개별 PC의 보안 패치 업데이트만으로는 신종 공격에 빠르게 대처하지 못한다는 한계도 갖는다. 중앙집중적인 통합 PC 보안으로 전산업무에 익숙하지 못한 일반 직원 PC 보안도 강화할 수 있다.

서버와 네트워크의 보안 시스템을 완벽하게 갖추고 중앙집중적인 통합보안 시스템을 구축한다고 해서 보안작업이 완성되었다고 할 수 없다. 대부분의 침해사고는 예상하지 못한 시스템의 보안 취약성이나 사용자 부주의에 의해 발생하기 때문이다. 보안정책의 가장 하위부분에 속하는 사용자 개별 PC는 보안의 가장 큰 취약점이라 할 수 있다.

전국적인 지사나 영업망을 갖춘 조직이나 해외에 본사나 지사를 두고 있는 글로벌 기업의 경우가 개별 PC의 보안사고에 대한 좋은 예가 된다. 작은 영업소나 지점에는 전산관리자가 따로 파견되지 않아 PC 관리를 잘 하지 못하는 일반 직원들이 PC 보안 패치를 적용하지 않거나 바이러스 백신을 정기적으로 업데이트 하지 않아 각종 공격에 무방비로 노출되는 예가 많다. 게다가 백신 프로그램은 알려진 악성 코드만 퇴치할 뿐이어서 신종 바이러스 등의 공격에 대한 근본적인 해결이 불가능하다는 한계를 갖고 있다.

고객 최접점의 PC 보안 강화로 서비스 업그레이드

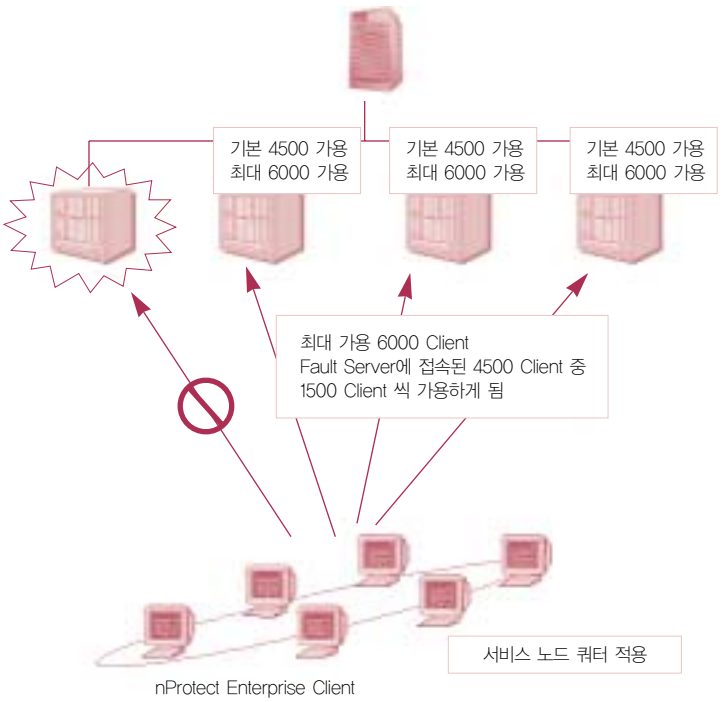
통합 PC 보안 시스템 구축에 성공한 K공사는 전국의 행정구역 단위에 190여개에 이르는 지사와 지점을 운영하고 있는 가장 대표적인 사례이다. K공사는 고객을 직접 만나는 지역에서의 현장 서비스 수준을 높이기 위해 일선에 이동 서비스 망을 구축했다. 특히, 농어촌 인구 밀집지역에 60여개의 서비스센터를 설치하는 등 전국망을 체계화했다. 이로써 K공사는 2만1000 클라이언트로 구성된 중대형 규모의 네트워크 망을 갖게 되었다.

K공사는 관리 노드 단위가 전국적인 규모로 분산됨에 따라 보안 이슈에 대한 효율적인 대응방안이 시급히 필요한 상황이었다. 잉카인터넷은 K공사의 서버를 지역별로 분산해 지역 중심적인 클라이언트 운영기반을 유지하면서 중앙에 통합관리 데이터베이스 시스템을 구축해 통합 PC 보안을 중앙에 집중시켰다. 그리고 사무실 PC에서 윈도우 기반 제어용 시스템에 이르기까지 전사적인 시스템의 보안 취약점 패치를 실시했다. 악성 코드의 공격에 대비해 윈도우 기반 시스템의 보안 패치를 전사적으로 적용했다. PC 방화벽 시스템을 구성해 내부 악성 코드 침입을 차단하고 확산을 방지시켰으며, 유입경로를 파악할 수 있도록 하였다. 더불어 윈도우 기반 시스템의 보안취약 사항에 대한 보안 패치 적용을 중앙에서 집중 관리하여 정보시스템 보안을 강화했다.

K공사와 마찬가지로 전국의 네트워크 망을 갖고 있는 D화재보험은 본사와 전국 영업점 뿐만 아니라 설계사의 노트북에 까지 전사적인 통합 PC 보안 시스템이 요구되었다. 자동차 보험을 비롯한 장기 손해보험, 화재보험, 해상보험, 개인연금 등 손해보험의 전 종목을 취급하는 D화재보험은 고객의 작은 불편이라도 1시간 이내에 해결할 수 있는 첨단의 정보 서비스 체계를 갖추고 있어 개별 PC에 대한 보안이 절실한 상황이었다.

D화재보험의 관리 서버 안전성을 확보하기 위하여 자체 서비스 노드 쿼터를 부여해 최적의 상태로 서비스가 이뤄지도록 하였다. 여러 유형의 관리 서버 장애가 동시에 발생할 경우를 대비해 클라이언트에서의 페일 오버 기능을 구성하였다. 이를 통해 관리 서버 서비스 장애가 발생해도 클라이언트 서비스에 문제가 발생되지 않도록 하였다. 사용자 환경은 도메인 계정을 사용하여 로그인 할 수 있도록 했으며, 본사의 보안솔루션을 탑재해 승인된 사용자가 아니면 사용할 수 없도록 보안설정을 구성했다. 내부 인트라넷에서의 웜이나 악성 코드의 불법 접근을 방지하기 위해 PC 방화벽 기능을 구성하였으며, 업

무에 사용되는 소프트웨어 외의 프로그램에 대한 불법 접근이나 이상 트래픽을 완전히 차단했다.



[그림 1] D화재보험 구축 현황도

이 프로젝트는 블레이드 서버를 도입해 확장성을 확보하였으며, 노드 쿼터를 적용해 확장성과 안전성을 갖추었다. 또한, 모든 관리요소를 통합한 보안관리 콘솔을 구성해 중앙집중식으로 관리하도록 해 전사적인 통합 보안솔루션을 만들었다.

05

㈜잉카인터넷 솔루션사업부 기술지원 1팀 장민석 팀장
msjang@inca.co.kr

USB 중앙통제로 직원 보안의식 고취

USB는 배터리가 필요없고, 크기도 작으며, 여러 기능과 대용량 저장공간을 갖추고 있어 기업의 보안 관리자에게 눈엣가시가 되어오고 있다. 그러나 개인적인 용도로도 많이 쓰이고, 편리한 기능을 가진 USB 사용을 무조건 금지할 수는 없다. 전사적인 통합 PC 보안으로 USB 사용도 안심할 수 있다.

보안정책이 아무리 완벽하게 갖춰져 있다고 해도 보안의 허점은 어디에나 존재한다. 아무리 잘된 보안정책이라 해도 직원들이 정상적인 방법으로 정보를 외부로 가져갈 수 있다면 막대한 예산을 투입한 보안정책은 모두 헛수고가 되어버린다. 악의를 가진 직원들에 의한 유출이 아니라 중요한 정보를 USB나 노트북 등에 저장해가지고 다니다가 잃어버리게 될 수도 있다.

2006년 8월 영국에서 발생한 테러 위험사고로 전 세계에 항공보안 강화 바람이 불었을 때, 갓난아기의 우유병을 제외하고 어떤 액체물건도 비행기 반입이 금지되었으며, 배터리가 포함된 MP3 플레이어에서부터 핸드폰, 디지털 카메라 등 디지털 기기도 거부당했다. 이런 와중에서 틈새를 찾은 제품이 USB(Universal Serial Bus)이다.

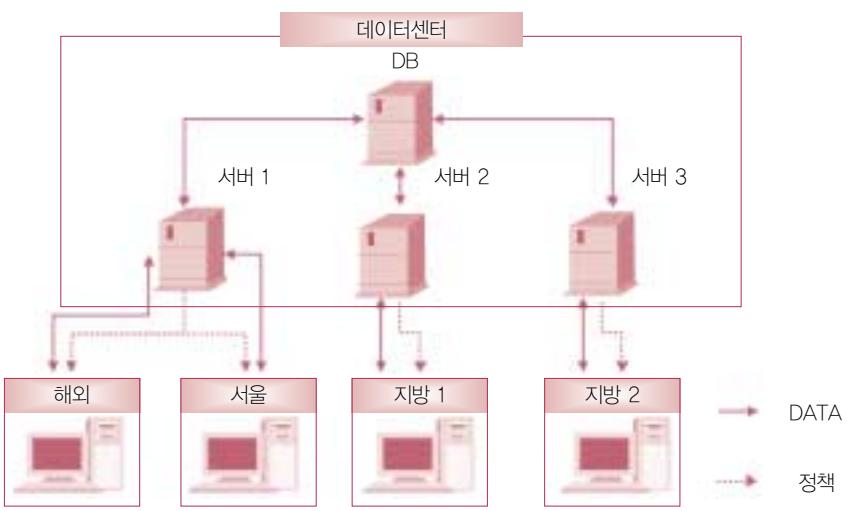
USB는 배터리가 필요없고, 크기도 작으며, 여러 가지 기능과 대용량 저장공간을 갖

추고 있어 기업의 보안관리자에게 눈엣가시가 되어오고 있다. PC에서 정보자산 유출경로를 차단한다 해도 중앙에서 관리가 이뤄지지 않으면 비정상적인 방법을 통해 정보가 유출 될 수 있으며, 추적조차 불가능한 상황도 일어난다. 사무실 PC에서 공장의 무인 제어 시스템에 이르기까지 모든 IT 인프라가 연결되어 있는 네트워크 환경에서 내 · 외부 사용자에 의한 정보자산 유출경로는 점차 복잡하고 다양해지고 있는 상황이다. 이 때문에 많은 기업에서 USB 등 외부 저장매체를 사용하지 못하도록 하는 정책을 도입하고 있지만, 개인적인 용도 외에도 여러 기능을 가진 USB 도입을 무조건 막는다는 것도 한계가 있다. 이럴 때 중앙에서 모든 정보를 관리하는 통합 PC 보안체계가 답이 될 수 있다.

이동형 저장매체 제어장치로 정보유출 방지

글로벌 기업인 P사는 해외 시스템과 국내 사무실의 업무용 PC, 공장의 자동화 기기 시스템에 이르기까지 이동형 저장매체 보호 시스템을 도입했다. 윈도우 기반 업무 시스템에 대한 회사의 정보자산 보호를 위한 대비책이었다.

P사는 이동형 저장매체를 제어할 수 있는 정보유출 방지 시스템을 구축해 집중 관리



[그림 1] P사 통합 PC 보안 시스템 구축 현황도

하였다. 개별 PC에 정보유출 방지 솔루션을 적용하고, 중앙 모니터링 시스템을 도입해 정보이동을 중앙에서 직접 통제할 수 있게 되어 직원들의 보안의식을 고취하는 성과도 거두고 있다.

통합 PC 보안 시스템을 통해 중앙에서 정보를 관리하게 되었다면, 직원들에게는 보안 USB를 사용할 것을 권고하는 것도 좋은 방법이다. 보안 USB는 기존의 USB 기능에 비밀번호를 설정해 데이터 위 · 변조를 막는 기능을 더한 것이다. 스마트카드처럼 암호화된 칩이 있어 인증을 받아야 사용할 수 있다. 인터넷이나 네트워크 통신상 필요한 인증을 받는다. PC 내에 중요한 정보가 들어있을 경우, 일정한 권한을 가진 사용자만 접근할 수 있도록 USB를 활용할 수 있다. 비밀번호를 잊어버렸을 경우, 자료를 볼 수 없으며, 제품을 사용하기 원한다면 USB 자체를 포맷해야 할 정도로 보안기능이 강력하다.

최근에는 바이러스 백신 솔루션이 탑재되어 있는 제품도 나오고 있다. USB 자체에 안티바이러스 솔루션이 있어 바이러스와 스파이웨어를 효과적으로 탐지하기도 한다. 또한, 특정 PC에서만 연동되는 USB도 출시되고 있다.

06

㈜잉카인터넷 게임보안센터 국내서비스팀 김기환
khkim@inca.co.kr

게임전문 보안시스템으로 고객 신뢰도 향상

온라인 게임을 제작할 때 매우 민감한 문제 중 하나가 인터넷에서 쉽게 해킹 툴을 구할 수 있다는 것이다. 이 해킹 툴은 여러 가지로 변종이 가능하며 실시간 업데이트 되고 있어서 유저들에게 피해를 확산시킨다. 온라인 게임에 전문보안 시스템을 구축해 각종 핵 공격으로부터 유저를 보호하고 고객 신뢰도를 향상시킬 수 있다.

게임 제작자들이 매우 민감하게 여기는 문제 중 하나는 특정 유저들이 인터넷에서 쉽게 구할 수 있는 해킹 툴로 게임상에서 레벨과 고급 아이템을 얻는 것이다. 이 과정에서 일부 유저의 게임계정이 유출되기도 해 게임에서의 보안이 매우 중요한 요소가 되고 있다.

게임 해킹의 대표적인 유형은 메모리와 파일 변조이다. 메모리 변조는 메모리 에디트 프로그램을 이용해 메모리 내에서 특정값을 변조하는 것이다. 이 과정에서 데이터 분석을 이용하면 게임전용 핵을 제작할 수 있다. 파일 변조는 게임 클라이언트와 맵, 스크립트 등 데이터 파일을 분석하거나 조작하는 것이다. 역공학을 이용해 클라이언트의 보안 코드를 건너뛰는 방법도 사용된다.

스피드 핵은 게임 내에서 자신의 이동속도나 공격강도를 조절하는 것이다. 클라이언

트 PC 속도를 임의로 조정해 게임 속도를 조절하기도 한다. 매크로와 오토마우스는 게임의 편의상 제공되는 매크로를 프로그램화 해 자동으로 사냥하거나 물약을 복용하고, 스킬을 사용하는 것을 말한다. 몬스터 사냥을 계속 해 다른 사용자의 불만을 살 수 있고 서버 부하를 가중시킬 수도 있다.

패킷 핵 혹은 BOT라 불리는 공격기법은 서버로 전송되는 게임 패킷을 임의로 치환해 다양한 조작을 통해 공격 패킷을 여러 번 전송하는 것이다. 혹은 게임 패킷을 완전히 분석하여 몬스터의 위치를 파악해 자동 사냥을 한다. 이중 Non-Client BOT는 매우 심각한 유형으로, 게임 클라이언트를 디버깅하고 패킷 구조를 완벽히 분석하여 로그인부터 게임 진행, 종료까지 실제 게임 클라이언트와 동일한 메시지를 생성시켜준다. 단순한 다이얼로그 박스로 이루어져있고 수십 개의 프로그램을 동시에 실행할 수 있어 해킹 툴 중 가장 악성적이고 대응이 어렵다. 중국과 대만의 조직적인 해킹그룹이 이를 만들고 있다.

전용 핵은 특정 게임을 겨냥해 만든 툴로 기존의 해킹 툴을 사용할 때 알아야 할 별도의 지식이 없어도 쉽게 사용할 수 있다. 전용 핵은 최근에 많이 발생하고 있으며, 유료로 판매되고, 배포 규모가 확산되고 있다. 계정 해킹은 인터넷 상에서 구할 수 있는 백도어나 키로거 프로그램으로 다른 사람의 계정정보를 훔치는 것을 말한다. 게임 해킹의 가장 대표적인 행위로, 중국의 해커그룹에서 조직적으로 이뤄지고 있으며, 그 피해가 아주 심각한 상태이다.

게임 보안전문 솔루션 도입으로 게임 해킹에 대응

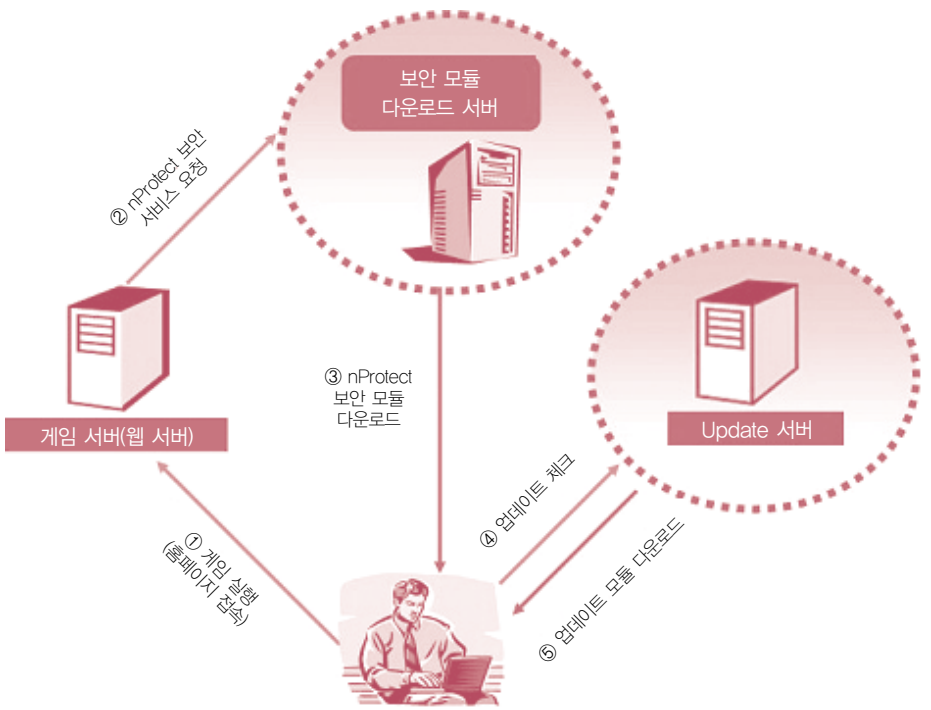
해킹 사고는 날이 갈수록 지능적이고 고도화 되고 있으며, 피해 확산속도가 걷잡을 수 없이 빠르게 진행되고 있다. 이 때문에 일부 게임업체들은 자체적인 보안시스템을 구축하기 위해 인력 충원을 계획하기도 하지만, 게임보안 전문인력을 채용하기가 힘들고, 비용이 많이 들며, 개발과정에 투입될 때까지 시간이 소요된다는 문제점이 있다. 보안전문업체에서 하는 것 만큼 대응이 빠르지 않다는 한계도 지적되고 있다. 이 때문에 게임업체들이 전문 게임 보안솔루션을 도입하는 경우가 늘고 있다.

ㅇㅇ게임사에서 '도약(가칭)' 이라는 게임을 만들어 클로즈베타와 오픈베타를 진행하는 과정에서도 동일한 문제점이 발생해 잉카인터넷의 'nProtect GameGuard'를 도입

하기로 했다. 이에 따라 잉카인터넷은 본격적인 사업 착수에 앞서 게임 클라이언트와 게임 서버 취약점을 분석했다. 그 결과 메모리 변조를 할 수 있는 UCE 방식으로 제작된 치트 엔진으로 능력치를 높이거나 아이템을 습득할 수 있는 취약점이 발견되었다. 자체 게임 클라이언트의 보안 코드를 뛰어넘는 역 어셈블리를 이용해 해킹할 수 있다는 문제점도 드러났다. 사용자들에게 매우 큰 피해를 끼칠 수 있는 키로거 프로그램을 이용한 게임 계정 유출도 가능했으며, 전용 Non-Client Bot가 시중에 유통되고 있기도 했다.

분석결과를 바탕으로 nProtect GameGuard 설치를 시작했다. 설치과정은 우선 서버를 구성하고 게임 제작사에 모듈을 제공하면 게임 제작사가 클라이언트에 장착해 클라이언트 업데이트 패치에 GameGuard를 추가하고 테스트를 거치면 완료된다. 소요기간은 서버 구성을 제외하고 일주일에서 열흘 정도 걸린다.

GameGuard는 실시간 게임 핵을 차단해 윈도우 패킷 에디터, 각종 매크로 조작을 원



[그림 1] GameGuard 적용 구성도

천적으로 막으며, 스피드 핵을 진단할 수 있는 드라이버를 제공하고, 클라이언트 PC의 속도변조를 체크해 변종 스피드 핵을 차단할 수 있다. 스피드 핵의 여러 가지 우회사용 차단과 원격제어와 오토 마우스 구동을 차단하는 DLL 모듈을 제공하고, 윈도우 커널 디버거를 진단해 규정된 게임 정책에 따라 게임 진행 여부를 정한다.

게임 클라이언트 암호화를 통해 기본 방어선을 구축하고, 게임 서버와 GameGuard 간의 인증기능을 강화해 GameGuard를 무력화하려는 시도를 원천적으로 차단하며, 입력된 키보드 값을 암 · 복호화해 키로거 프로그램을 무력화시킨다. 새로운 방식의 키로거 프로그램이 출현해도 모듈 업데이트가 가능해 현재 웹페이지와 게임 클라이언트에 쉽게 적용할 수 있다.

온라인 게임에 GameGuard를 도입함으로써 게임 프로그램에 개인보호 정책수립이 가능해졌으며, 인터넷 서비스 보안 취약점을 해결하고, 고객보호차원의 마케팅 효과를 높여 신뢰도가 향상되었다. 자동 업데이트로 신종 해킹 툴과 바이러스에 대한 신속한 대처가 가능하며 각종 핵에 대한 서비스를 전문으로 하는 업체에 맡겨 인건비 절감과 지속적인 서비스 관리를 받을 수 있게 되었다.

■보안솔루션 가이드

㈜시큐브 Secuve TOS®_ 서버보안

㈜시큐브 eTOS 서비스_ 중소기업 온라인 토탈 보안 서비스

㈜안철수연구소 V3 IS 7.0 플래티넘 엔터프라이즈_ PC 보안

㈜안철수연구소 AhnLab TrusGuard_ 네트워크 보안

어울림정보기술㈜ SEPION 4000_ 통합보안

인포섹(주) WEBFRONT_ 웹 방화벽

㈜에이쓰리시큐리티컨설팅 TASCoM_ 정보보호 컨설팅

㈜제이컴정보 e-Pentagon ESM_ 통합보안

㈜잉카인터넷 nProtect Enterprise 2.5_ 엔드포인트 보안

㈜정보보호기술 TESS TMS_ 위협관리 시스템

※침해사고 경보단계 및 대응기관 연락처

보안솔루션 가이드 & 침해사고 대응기관

서버보안 : Secuve TOS®

세계 최초 보안서버 PKI 인증 적용 특허

㈜시큐브 | T. 02-3470-8500 | www.secuve.com

방화벽이나 침입탐지 시스템 등 네트워크를 기반으로 한 보안솔루션은 우회적인 해킹 등 보안 취약성을 가지고 있으며, OS의 결함으로 발생하는 해킹과 정보유출에 대응할 수 없다는 한계를 갖고 있다. 이에 대한 보완책으로 제시되고 있는 것이 서버보안이다. 미국은 이미 1990년대부터 서버보안을 중요한 보안 인프라로 인식하여 연구 개발을 장려하고 있다. 우리나라에는 2000년에 ㈜시큐브가 처음으로 제품을 출시해 기존의 네트워크 기반 보안솔루션의 한계를 극복했다. 또한, Linux, Unix, Window 운영체제 보안(시큐어OS)에 대한 연구개발을 지속적으로 추진하고 이다.

㈜시큐브의 대표적인 서버보안 솔루션은 Secuve TOS®이다. Secuve TOS®는 세계 최초로 전자서명(PKI) 사용자 인증방식을 적용해 보안성을 강화했다. 이로써 공공기관이나 금융기관, 민간기업체의 모든 최고 경영자와 보안관리자가 안고 있는 최대 고민인 핵심 기술과 정보자산의 유출을 막아준다. Secuve TOS®의 사용자 인증방식은 국내는 물론, 미국, 일본, 중국, 호주 등 해외에 특허출원해 기술등록이 되어있으며, 이 외에도 MAC/MLS/RBAC 등 다양한 접근통제 정책을 갖고 있다.

- 세계 최초 보안서버 전자서명 사용자 인증 적용
- 미국 국방성 TCSEC B1급 보안기능 · 보증 요구사항 제공
- 관리자 권한이 있어도 인증절차 없으면 접근 통제
- 전자서명 인증기반 파일 시스템 해킹 방지기술

다른 솔루션과 가장 크게 차별화 되는 점은 시스템 관리자 권한을 부여받았다 해도 적법한 인증절차를 거치지 않으면 시스템 접근이 불가능하다는 것이다. 기존의 서버보안 방식이 ID와 패스워드를 이용한 사용자 인증방식에 머물러 있어 인터넷에서 구할 수 있는 해킹 툴로도 간단하게 무너질 수 있다는 취약성을 해결한 것이다. 이를 통해 해커나 크래커 또는 비인가된 내부사용자 등 불법침입자의 시스템 접근권한을 통제하고, 홈페이지와 파일에 대한 위 · 변조를 방지하며, 불법 정보유출을 차단하고, 컴퓨터 운영체제 상에 내재된 보안상 결함으로 인하여 발생할 수 있는 각종 해킹으로부터 컴퓨터 시스템을 보호한다. 또한, 시스템과 네트워크 공격을 실시간 탐지하고 즉각 차단할 수 있는 지능형 침입탐지 및 방지장치를 통해 웜, 바이러스, 해킹을 원천적으로 막을 수 있는 견고한 방어체계를 구축한다.

Secuve TOS®의 보안성은 미국 국방성의 안전한 컴퓨터 시스템 평가기준인 TCSEC(Trusted Computer System Evaluation Criteria)의 B1급에 해당하는 기능과 보증 요구사항을 제공할 만큼 안전하고 강력하다. 로그 관리와 분석보고서를 제공하며, 보안정책 사전 시뮬레이션과 접근권한 목록 편집기능이 있어 관리자가 쉽게 사용할 수도 있다.

현재 판매되고 있는 Secuve TOS® V2.0은 국가정보원의 CC 인증을 받고, 행정 정보보호 시스템으로 선정되었으며, 조달단가를 등록했다. GS 인증과 VeriTest 인증을 받았고, IR52 장영실상, 세계 일류상품에 선정되기도 했다. 또한, 중앙정부 기관과 지방자치단체의 행정정보화 시스템, 금융권, 전국 초 · 중 · 고교와 대학교, 일반 기업, 육 · 해 · 공군 상위부대 전자결재 시스템, 의료기관 등 2000여 고객사를 보유하고 있다.

온라인 토탈 보안서비스 : eTOS서비스

중소기업 맞춤형 온라인 토탈 보안 서비스

㈜시큐브 | T. 02-3470-8500 | www.secuve.com

정보유출이나 해킹 등의 사고는 보안이 취약한 중소기업에서 발생하는 경우가 많다. 보안솔루션이 제대로 갖춰져 있지 않은데다가 직원들의 보안의식도 약해서 사소한 실수로 정보가 유출되기 때문이다. 악의를 가진 직원들이 외부에서 정보를 몰래 빼가도 알아차리지 못하는 경우도 있다. 보안에 대한 인식수준이 높아지면서 대기업과 공공기관의 보안시스템은 어느 정도 갖추어진 편이지만 중소기업의 보안은 매우 열악한 수준이다. 이 때문에 중앙정부가 먼저 나서서 중소기업의 보안성 강화를 위한 대책을 마련하고 있지만, 중소기업의 입장에서 보안은 아직도 '지나친 사치'로 인식되고 있다.

㈜시큐브의 'eTOS서비스'는 보안의 사각지대에 있는 중소기업을 위한 맞춤형 토탈 보안 서비스이다. 온라인 다운로드를 통해 서버보안 솔루션인 Secuve TOS®를 자유롭게 사용할 수 있으며, 보안 취약성 점검과 컨설팅도 받을 수 있다.

Secuve TOS®는 세계 최초로 특허기술을 받은 전자서명 사용자 인증과 다양한 접근통제 정책을 결합시켜 악의를 가진 공격자에 대한 접근을 막을 수 있다. Secuve TOS®는 국내업계 최초로 CC 인증계약을 체결하고, Windows, Linux, Unix(Solaris, HP-UX,

- 정보보호 사각지대인 중소기업의 정보보호 수준 제고
- 서버보안, 중소기업 보안취약성 진단, 컨설팅 제공
- 월 10만원 수준의 저렴한 비용
- 중소기업 보안 · 전산관리자 교육으로 운영상 문제점 해결

IBM AIX, HP Tru64, Unixware) 등 모든 OS 플랫폼에 대해 국가정보원의 보안성 검토를 승인받아 행정정보 보호용 시스템으로 선정되었다. 강력한 해킹 탐지와 차단, 침입방지 체계로 견고한 방어체계를 구축하며, 웜, BOF를 원천적으로 차단하고, 시스템과 네트워크 공격을 실시간으로 차단한다. 미국 국방성의 안전한 컴퓨터시스템 평가기준인 TCSEC B1 등급 수준의 보안성을 제공하며, 친숙한 GUI 구성과 편리한 관리자 기능, 통합 로그 관리 툴을 통해 관리를 보다 편리하게 할 수 있다.

이 모든 과정은 온라인으로 이루어져 있으며 판매 원가가 크게 낮아져, 이 모든 서비스를 이용하는데 드는 비용은 월 10만원 수준으로 중소기업의 부담을 덜어준다. 또한, 전산 · 보안관리자를 대상으로 관리자 운영교육을 정기적으로 실시해 전산관리자의 부담을 낮추고, 중소기업의 인력 충원에 대한 부담도 경감시켜준다. eTOS서비스의 이같은 장점 때문에 예산과 관리문제로 서버보안 도입을 망설였던 중소기업 CEO와 전산 · 보안관리자로부터 좋은 반응을 얻고 있다.

제품의 구성도를 간략하게 설명하면, 사업자가 인터넷을 통해 서비스를 다운로드 받으면, eTOS의 통합관리 서버에서 보안기능 제어, 로그 관리 등의 서비스를 실시한다. 이를 다시 사용자의 서버에 알리면서 보안관리와 모니터링을 해준다.

㈜시큐브는 중소기업의 경제적 · 관리적인 부담을 경감시키면서 정보보호 수준을 강화할 수 있도록 'eTOS서비스' 수준을 더욱 높여갈 계획이다. 또한, 현재 개발계획을 가지고 있는 서버보안 시큐어eTOS와 웹 방화벽, 보안취약성 분석 툴을 통합한 TOS UTM 버전(패키지S/W)을 eTOS서비스에 맞게 확대, 적용해나갈 예정이다.

PC 통합보안 솔루션 : V3 IS 7.0 플래티넘 엔터프라이즈

사전 · 사후방역에 최적화까지, PC 보안의 모든 것

㈜안철수연구소 | T. 02-2186-3000 | www.ahnlab.com

최근 보안사고는 취약성을 이용한 침투나 메신저, 유해 사이트 접속을 통한 악성 코드 등으로 다양해지고 있으며, 취약점이 발견된 후 24시간 안에 공격 툴이 만들어지는 '제로데이 공격' 이 증가하고 있다. 공격유형은 인터넷 뱅킹이나 온라인 게임 등 금전적 손실을 유발하는 것이 대세를 이루고 있다. 이러한 시대적인 흐름을 반영하듯, 최근 PC 보안 솔루션은 사후 대응보다 사전 대응, 개별 시스템 대응에서 공동 대응으로, 제품단위에서 시스템 단위 서비스로 변화하고 있다.

우리나라의 대표적인 안티 바이러스 소프트웨어 업체인 안철수연구소가 기업 PC용 통합 보안제품으로 내놓은 것이 'V3 인터넷 시큐리티 7.0 플래티넘 엔터프라이즈' 이다. 이 제품은 안티 바이러스, 안티 스파이웨어, PC 방화벽 기능이 탑재되어 있으며, 국제인증 획득으로 성능을 검증받은 '스파이 제로' 를 통합해 강력한 전문 안티 스파이웨어 기능을 제공한다. 또한, 스팸이나 피싱으로 인한 피해를 막기 위해 바이러스, 웜, 트로이목마 등 악성 코드와 스파이웨어, 해킹을 지능적으로 진단하고, 치료하며 차단해준다.

더욱 지능화 되고 있는 개인정보 유출 범죄를 효과적으로 막을 수 있도록 URL 필터

- 안티 바이러스, 안티 스파이웨어, PC 방화벽 기능 제공
- 사전 · 사후 방역 제공으로 최신 엔진 업데이트 안해도 위협 차단
- 초보자도 쉽게 쓸 수 있는 GUI
- 개인정보 유출 차단, URL 필터링, 시스템 최적화 제공

링 기능을 제공하며, 시스템 최적화, 보안 취약점 리포트와 해결방법을 제시한다. 이외에도 자원관리, 시스템 클린업 등의 기능으로 보안위협 요소가 침입하기 어려운 환경을 구축해준다. 보안상태, 보안기능 설정을 한눈에 볼 수 있고, 수동검사, 빠른 검사, 사용자 정의 등 다양한 검사방법을 선택할 수 있으며, 원하는 시간에 자동으로 검사할 수 있는 예약검사 기능을 제공한다.

기존의 백신 제품은 사용자가 수동으로 엔진을 업데이트하기 때문에 백신 프로세스를 정지시키는 악성 코드가 침투하면 속수무책이 되곤 했다. V3 플래티넘은 엔진 업데이트를 하지 않아도 신종 공격의 피해를 막을 수 있으며, 감염된 후에도 시스템 최적화를 지원한다. 시스템의 취약점 관리에서 출발하여 비정상적인 트래픽 관리, 긴급상황 대응, 엔진 업데이트를 통한 치료, 실시간 방역을 제공하며, 보안제품을 처음 사용하는 초보 사용자부터 고급 사용자까지 편리하게 제품을 사용할 수 있도록 구성되어 있다. 통합 로그 및 이력관리, 다양한 예약기능, 사용자 정의 기능, 손쉬운 보안설정 변경 등 메뉴별로 사용자 입맛에 맞는 세심한 기능을 제공하고 있다.

V3 플래티넘의 또 다른 장점은 중앙관리 솔루션인 '폴리시 센터(AhnLab Policy Center 3.0)' 와 연동되어 전사적 관리가 가능하며, 안철수연구소의 긴급 대응조직인 시큐리티 대응센터가 24시간 365일 지원해 악성 코드와 보안 이슈가 발생했을 때 신속하게 대응할 수 있다는 것이다. 이에 따라 V3 플래티넘을 사용하는 기업은 보안환경 구축으로 업무 생산성을 높이고, 정보자산을 안전하게 보호할 수 있다. 그러므로 하나의 솔루션으로 다양한 보안위협에 대응할 수 있어 보안 소프트웨어 도입비용을 절감하고 관리부담을 줄일 수 있다.

네트워크 보안 : AhnLab TrusGuard

웜 발생 · 소멸 패턴 예측 차단해 네트워크 보안

㈜안철수연구소 | T. 02-2186-3000 | www.ahnlab.com

기업의 보안담당자들이 가장 골치아프게 생각하는 것은 웜과 스파이웨어다. 웜 · 스파이웨어는 매우 간단한 툴로 대량의 PC를 감염시킬 수 있기 때문이다. 웜은 직원 한 사람의 사소한 실수로 PC 한 대가 감염되면, 기업 전체 PC를 감염시킬 수 있을 만큼 무서운 번식력을 갖고 있다. 웜은 이메일이나 특정 사이트, 메신저 뿐 아니라 PC 보안 취약성을 이용한 네트워크 공격도 서슴지 않는다. 스파이웨어는 주로 개인 사용자를 상대로 공격하고 있지만, 이것이 기업 전체 생산성을 저하시키는 주된 요인으로 꼽히고 있다. 최근 스파이웨어는 바이러스나 웜과 결합되거나 트로이목마와 결합돼 정보유출 기능까지 갖춘 형태로 제작되고 있다.

보안위협은 시시각각 변하고 있지만, 기존의 네트워크 보안제품은 이러한 변화에 발을 맞추지 못하고 있다. 방화벽은 인터넷 마비의 주범인 슬래머(Slammer) 웜으로 유발되는 패킷이 정상 포트로 들어올 때 모두 통과시키는 등 오탐률이 매우 높다. IDS와 취약점 점검 솔루션은 관리자가 이상 징후를 파악하는데 도움을 주지만, 실제로 침입 사실을 알았을 때는 이미 전 네트워크에 웜이 퍼져, 시스템이 위험에 처하는 경우가 많다. IPS도

- 웜/스파이웨어/DoS/네트워크 스캐닝 차단
- 웜 발생 패턴 예측, 3단계 자동 방역
- AST 서비스로 제로데이 공격 실시간 차단
- 보안제품 없는 PC를 네트워크에서 격리

신종 웜을 효과적으로 방어하지 못하며, 일부 정상적인 패킷을 공격 패킷으로 오인하는 문제를 갖고 있다.

안철수연구소의 AhnLab TrusGuard 1100/3100/4100 시리즈는 SCM(Secure Contens Management) 어플라이언스 제품으로 웜, 스파이웨어를 차단하고, DoS (Denial of Service) 공격, 네트워크 스캐닝 등 빈번한 네트워크 공격을 효과적으로 탐지하고 차단하며, 치료한다. TrusGuard는 웜이 발생하는 시점부터 소멸할 때까지 패턴을 예측하고 차단한 후 아웃브레이크 조기 차단, 네트워크 웜 차단 등 3단계에 걸친 자동 방역기능을 수행한다.

1단계에서는 새로운 취약점과 패치가 발표되면 웜의 공격 패턴을 예측해 차단정책을 만들어내며, 2단계에서는 이메일을 통해 확산되는 웜을 차단하고, 3단계에서는 웜의 수집과 분석이 끝난 후 시그니처(Signature : 웜 · 바이러스 정의 파일) 기반의 차단정책을 자동으로 배포한다. 또한, 클라이언트 보안제품이 설치되어 있지 않거나 취약한 공유 폴더를 사용하는 PC를 네트워크에서 격리해 감염이 의심되는 PC의 모든 트래픽을 차단하여 시스템 전체에 웜이 확산되는 것을 방지해준다.

안철수연구소는 각 네트워크에 설치된 TrusGuard에 신종 웜 · 스파이웨어 차단정책을 24시간, 365일 실시간 자동으로 배포해주는 서비스 시스템인 AST(AhnLab Security Tower)를 자체 개발해 운영하고 있다. 이에 따라 최근 문제가 되고 있는 제로데이 공격을 실시간으로 차단하고, 이메일이나 네트워크 취약점 등 악성 코드가 침투할 수 있는 다양한 경로에서 실시간으로 작동하므로 빈틈없이 방어할 수 있다.

통합 보안관리(UTM) : SEPION 4000

시나리오 기반의 정밀 분석 지원

어울림정보기술㈜ | T. 02-2142-0500~6 | www.oullim.co.kr

네트워크가 발달하면서 방화벽, VPN, IDS, 안티 바이러스, 안티 스팸, 메일 보안 등 다양한 보안솔루션이 출시되어 각종 공격으로부터 정보시스템을 보호해주었다. 그러나 보안솔루션이 증가하면서 이를 운용하고 관리하는 업무의 과부하를 일으켜, 인력과 비용을 증가시켰다. 이 때문에 대다수의 기업과 기관은 모든 보안솔루션을 하나로 합쳐 통합 관리할 수 있기를 바라기 시작했고, 이 때문에 통합 보안관리 시스템(UTM)의 개념이 나오게 되었다.

초기 UTM 제품은 상용 CPU를 사용하여 개발되었으나, 다양한 기능을 동시에 처리하면서 성능이 저하된다는 문제점이 나타났다. 이 때문에 UTM은 SOHO용으로나 가능하다는 부정적인 평가가 나오게 되었다. 그러나 네트워크 장비와 보안장비의 상호 보완적인 관점에서 제품개발이 이루어지고, 네트워크 상에서 보안기능 처리에 적합한 NPU(Network Process Unit)가 개발되면서 대형 네트워크까지 적용할 수 있는 제품이 출시되고 있다.

어울림정보기술㈜의 UTM 제품은 방화벽, IPSec 또는 SSL 가상사설망(VPN), 침입

- 방화벽, IPSec/SSL/VPN/IPS/컨텐츠 보안
- 웹 방화벽/NAC
- 고객사 환경에 따라 컨텐츠 필터링 옵션 선택
- 전문 업체들과 협력으로 최신의 정책 유지

방지 시스템(IPS), 컨텐츠 보안(Contents Filtering) 기능에 해당되는 안티 바이러스, 안티 스팸, 실시간 메신저 보안, P2P 보안기능을 포함하고 있다. 웹 방화벽과 NAC (Network Access Control) 기능이 추가된 제품도 나오고 있어 안전한 정보시스템 보호의 범위를 지속적으로 확대하고 있다.

일반적으로 SOHO용 UTM 제품은 성능보다 기능을 중시하는 반면, 고성능 UTM 제품은 강화된 기능에 성능이 뒷받침 되어야 한다. 제품이 기능에 치중될 경우, 성능상의 문제점이 발생하며, 성능을 우선시하면 기능상 미비점이 발생하여 보안장비로서의 의미가 퇴색되기 때문이다. 어울림의 고성능 UTM 장비는 기능을 우선 구현하고, 구현된 기능이 성능의 저하없이 정상적으로 동작되기 위한 하드웨어 아키텍처를 설계해 이같은 문제를 해결하고 있다. (주)어울림정보기술의 고성능 UTM 제품은 NPU를 기본적으로 탑재해 다수의 CPU를 병렬처리 하며, 최신의 멀티코어 CPU를 적용하고, 전용 ASIC을 통해 CPU에 비해 상대적으로 빠르게 처리하도록 하였다. 또한, NPU를 적용해 CPU에 비해 처리가 빠른 네트워크 프로세스를 지원한다.

다른 UTM 제품은 패킷을 기반으로 하기 때문에 정상적인 통신을 공격으로 오인하거나, 조작된 공격을 탐지하지 못하는 경우가 종종 발생한다. 어울림정보기술㈜의 제품은 방화벽으로부터 시작해 세션을 기반으로 하는 시나리오 기반의 DI 엔진을 탑재해 정밀한 분석을 지원해 이러한 문제를 해결한다.

UTM 제품에 탑재되는 각 기능들은 상호 보완적인 측면으로 동작이 되고 있으며, 각각의 기능이 최적의 상태를 유지하도록 하기 위해 해당 솔루션의 전문 업체들과 협력해 가장 최신의 정책을 유지할 수 있도록 한다.

웹 방화벽 : WEBFRONT

전원 이상에도 서비스 이상 무

인포섹㈜ | T. 02-2104-5114 | www.skinfosec.co.kr

해킹 기법이 발달하면서 보안인식이 강화된 덕분에 국내 주요 시스템의 네트워크 보안은 어느 정도 갖추어져 있다고 볼 수 있다. 그러나 웹에서는 사정이 다르다. 웹의 취약점을 이용한 공격은 초보 해커들도 자주 사용하고 있으며, 시스템 설계상 오류로 인해 시스템 DB를 침입당하는 일도 발생한다. 이 때문에 웹 보안을 할 수 있는 웹 방화벽에 관심을 갖는 기업들이 늘어나고 있다.

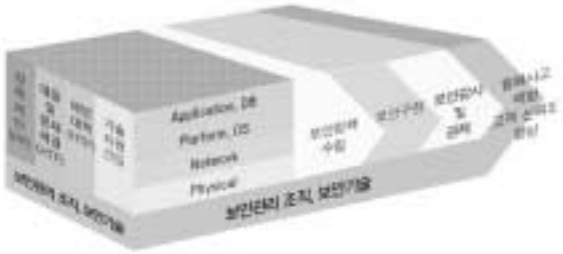
'WEBFRONT'는 종합 정보보호 회사인 인포섹㈜와 애플리케이션 스위치 전문업체 파이오링크가 함께 개발한 웹 방화벽이다. 기존의 웹 방화벽은 단순히 소프트웨어를 하드웨어에 장착하는 방식으로 구성되어 있지만, WEBFRONT는 전용 네트워크 보안 플랫폼을 기반으로 자체 설계, 개발하였다. 이로써 대용량 트래픽을 처리해야 하는 고객에게도 응답 지연시간을 최소화하고, 패킷의 손실을 최소화해줄 수 있다. 전원에 이상이 생겼거나 서버가 오동작 하는 등 비상상황에도 웹 서비스에 차질이 없도록 하기 위해 하드웨어 바이패스(Hardware Bypass)를 제공하며, 세션을 이중화하는 Stateful Failover를 구성했다.

- 전용 네트워크 보안 플랫폼 기반 설계
- 초당 4Gbps 이상 웹 트래픽 처리, 200만개 이상 동시 세션 지원
- 하드웨어 바이패스로 전원 이상 · 오동작 대비
- Stateful Failover, 이중화 구성

애플리케이션 트래픽 관리기술과 컨텐츠 관리기술을 핵심으로 안전한 웹 비즈니스 환경을 구축하고, 운영할 수 있도록 웹 서버팜의 앞단에 위치하여 불법적인 사용자의 웹 서비스 공격시도와 침입을 막는다. 모든 애플리케이션 단위에서 불법공격을 차단하는 웹 애플리케이션 방화벽 기능에 네트워크 인프라에 대한 보안기능을 제공한다. SSL, L7 컨텐츠 필터링, DoS/DDoS, 웜, 바이러스 등의 네트워크 인프라에 대한 공격위협에 대응하기 위해 네트워크 인프라에 대한 보안기능과 모든 애플리케이션 단위에서 불법 공격을 차단하는 웹 애플리케이션 방화벽 기능을 제공한다. 이 모든 기능이 단일 장비에서 수행될 수 있도록 개발되었기 때문에 투자비용이 적고, 관리 포인트가 단일화되어 안정적인 웹 서비스를 제공할 수 있다.

국내 인터넷 트래픽의 80% 이상이 웹을 통해 발생하며, 대형 포털과 금융기관, 대기업 등에서는 수십기가에 이르는 트래픽이 흐르고 있다. 이 때문에 최근 출시되는 웹 방화벽은 대용량 트래픽을 감당할 수 있는 기능을 가져야 한다. WEBFRONT는 대용량 트래픽 환경에서도 정확한 탐지와 차단을 수행할 수 있는 구도로 설계되어 4기가 이상의 웹 트래픽을 단일장비로 처리하며, 200만개 이상의 동시 세션을 지원할 수 있다.

기업의 보안관리자들이 솔루션을 도입할 때 매우 중요하게 여기는 것 중 하나가 관리하기가 얼마나 편하고 쉬운가 하는 점이다. 웹의 속성상 페이지의 변화가 심하고, 또 외부의 지속적인 위협요소가 존재하기 때문에 관리자의 부담은 더욱 늘어난다. WEBFRONT는 초기 보안설정시 고객의 환경에 적합하고 손쉽게 설정될 수 있도록 자동화된 설정과 자동학습을 통한 보안설정 기능을 제공한다. 또한, 다양한 보고서와 보안분석을 지원하는 웹프론트 애널라이저와 정책설정 마법사를 함께 제공해 사용이 편리하다.



정보보호 컨설팅 : TASCoM

물리적 보안에서 시스템 보안까지 정보보호 컨설팅

㈜에이쓰리시큐리티컨설팅 | T. 02-6292-3001 | www.a3sc.co.kr

해킹 등 악성 공격이 지능화 되면서 점차 사회는 보안에 대한 관심이 높아지고, 보안 의식이 성숙되기 시작하였다. 많은 기업들이 보안 컨설팅과 보안에 대한 국제표준 인증에 주목하기 시작하였으며, 이에 대한 관점도 상당히 다양화 되어 애플리케이션 보안, 소스코드 진단, 시스템 개발단계의 보안성 검토 등 광범위하면서도 세부적인 사항을 요구하고 있다. 자연스럽게 컨설팅 전문업체의 서비스도 다양하고 광범위하게 실시되고 있으며, 이를 위한 표준 모델이 나오고 있다. ㈜에이쓰리시큐리티컨설팅에서 제공하는 컨설팅도 이러한 추세에 맞춰 고객의 요구를 충족시키는 맞춤형 서비스로 다양화, 특화되고 있다.

(주)에이쓰리시큐리티의 컨설팅 서비스는 조직의 목적을 달성하는데 있어 전산 시스템과 네트워크, PC 등 모든 IT 자산과 정보자산을 운영하거나 관리하면서 발생할 수 있는 위험을 분석하고 대책을 수립하며, 관리자와 조직이 실현할 수 있도록 지원한다. 이를 위해 관리적인 관점과 물리적인 관점, 기술적인 관점에서 취약점을 파악하고, 위험을 분석하며 보다 실질적이고 구체적인 보안대책을 수립할 수 있도록 하고 있다. 정보통신 기

- 우리나라 환경에 맞는 보안 컨설팅 모델 제시
- 물리/네트워크/OS/응용 프로그램 보안 구축
- 소스코드 진단으로 취약점 해결
- 시스템 개발단계에서의 보안성 검토 강화

반보호법에 따른 주요 정보통신 기반시설 취약점 진단과 모의해킹, 종합 보안 컨설팅, 인증지원 컨설팅, 정보보호 안전진단 등 각종 산업분야에 대한 다양한 정보보호 컨설팅 서비스를 제공하고 있다.

㈜에이쓰리시큐리티컨설팅이 제공하는 시큐리티 모델은 BSI의 BS 7799, ISACA의 COBIT, FFIEC 등 보안 모델을 참조하여 국내 전산 통제환경에 맞도록 개선한 것이다. 기업과 기관의 물리적 보안, 네트워크 보안, 로컬 시스템의 OS 보안, 응용 프로그램 보안의 4가지 계층을 포함하며, 각 계층에 대해 보안정책과 절차, 보안구현, 보안감사와 관제를 실시한다.

이 모델을 구현하기 위해 ㈜에이쓰리시큐리티컨설팅은 TASCoM(The A3 Security Consulting Methodology)이라는 방법론을 제안하고 있다. TASCoM은 물리적 보안과 네트워크 보안, 로컬 시스템의 OS 보안, 응용 프로그램 보안의 4가지 계층을 포함하며, 각 계층에 대한 보안정책과 절차를 구현하고, 보안감사와 관제를 통해 침해사고를 예방하고 신뢰도를 향상시킨다. TASCoM은 총 6개의 단계와 15개의 모듈, 32개의 페이스, 102개의 태스크와 102개의 산출물로 이루어진 아키텍처로 구성돼 있다.

웹을 통한 취약점을 노리는 공격이 다수 발생하면서 웹 애플리케이션 취약점 진단 수요가 급증하고 있으며, 정보보호 컨설팅 업체들은 모의해킹 기법을 사용해 요구를 수용하고 있다. 그러나 대부분의 모의 해킹이 침투와 패치를 사용하는 것에 그치고 있다는 한계를 안고 있다. 이를 해결하기 위해 TASCoM은 소스코드 진단방법을 함께 사용해 취약점을 파악한다. 시스템 개발단계에서의 보안성 검토 및 수요도 늘어나고 있어 지속적인 교육과 시스템 개발 라이프 사이클 전반에 걸친 보안성 검토를 실시하고 있다.

통합보안 관리시스템 : e-Pentagon ESM

시스템 통합관리로 일원화된 대응체계 마련

㈜제이컴정보 | T. 02-6675-7770 | www.jcsi.co.kr

우리나라는 네트워크의 발전과 더불어 인터넷 강국으로 부상했지만, 인터넷 침해사고와 해킹 등 사이버 공격이 매년 증가하고 있다. 이에 따라 기업들은 정보보호에 큰 관심을 갖게 되었고, 방화벽과 IDS, IPS, 바이러스 패치 등을 도입하였다. 그러나 공격 패턴이 다양하고 과감해지면서 단위 보안장비만으로는 일관된 보안정책을 수립하고 적용하기 어렵다는 한계에 부딪히게 되었다. 보안관리자들이 전문화된 보안제품에 대한 전문지식을 습득해야 하고, 이기종 장비간의 효과적인 연동대책이 마련되어 있지 않기 때문이다. 게다가 실제로 위험한 공격이나 이상 징후보다 이벤트 모니터링과 분석업무에 더 많은 노력이 필요하게 되어 침해사고가 발생했을 때 실시간 대응하지 못하는 경우가 발생하고 있다. 기업은 이제 다양한 보안제품을 한 곳에서 모니터링하고, 관리할 수 있도록 관리 포인트를 단일화하고, 중요한 이벤트만 추출해 상관분석에 기반한 정교한 보안업무를 수행할 수 있어야 한다고 요구하고 있다.

㈜제이컴정보의 'e-Pentagon ESM'은 이러한 문제를 해결할 수 있는 효과적인 통합보안솔루션이다. 개별적으로 구축된 기존 보안장비의 상호 운용성을 향상시키고, 시스템

- 다양한 장비에서 발생하는 로그 · 이벤트 처리
- 주요 보안제품과의 뛰어난 연동성
- ISO 27001 기반의 자산 위험도 9단계 구분
- 불안정한 네트워크에서도 대용량 이벤트 전송 가능

을 통합 관리하여 보안 및 관리업무의 효율성을 높인다. 중앙에 집중된 실시간 보안 관리 체계를 마련해 위기관리능력을 배양하고 사후 보안정책을 수립하며, 사이버 포렌식 자료 관리 등 일원화된 대응체계를 마련해준다.

e-Pentagon ESM은 OPSEC, Syslog, File I/O, ASEN, SNMP Trap 등 표준 프로토콜을 통해 로그를 수집하므로 주요 보안제품과 연동성이 뛰어나다. 이벤트 처리를 통신계층에서 구현해 불안정한 네트워크 상황에서도 대용량 이벤트 전송이 가능하며, 부하분산을 위한 Load Balancing이나 Fault Tolerance 기능을 내장하고 있어 에이전트를 늘리거나 매니저 서버를 추가하는데 장애가 없다. ISO 27001 기반으로 자산 위험도를 9단계로 구분하며 자산 평가를 통해 대상 자산의 위험관리 기능을 제공하며, 긴급한 위험상황에 닥쳤을 경우 시나리오화된 자동실행 명령을 통해 침입을 막거나 고립시킬 수 있다.

또한, 가공되지 않은 데이터를 그대로 수집하거나 보안규칙 설정에 따라 규정된 이벤트만 수집할 수 있어 불필요한 트래픽 발생을 최대한 줄일 수 있으며, 지원되는 모든 기능과 생성되는 그룹에 대해 권한을 부여할 수 있다. 시스템 자체에서 무결성 검사를 실시해 파일이 변경되었다는 사실을 발견하면 사용자에게 알리고 이벤트 로그를 데이터베이스에 저장한다.

특허 출원된 매니저 구조는 Oracle 상용 DBMS를 지원해 다양한 장비에서 발생하는 로그 및 이벤트의 처리능력을 보장하고, 각종 이벤트 로그에 대해 필터링 등을 통한 효율적 관리를 제공한다. 지원되는 ESM의 모든 기능과 생성되는 그룹에 대해 권한부여가 가능해 이의 조합을 통한 새로운 관리자 등급을 생성시켜 고객의 다양한 직무체계에도 적합한 권한관리 시나리오 작성이 가능하다.

엔드 포인트 보안 : nProtect Enterprise 2.5

PC 보안 강화는 네트워크 보안 강화

㈜잉카인터넷 | 1566-0808 | www.inca.co.kr

보안의 중요성이 강조되면서 새로운 패러다임의 발전과 기술이 개발되고 있지만, 네트워크의 엔드 포인트인 개인 PC에 대한 취약점과 위험요소 대응은 상대적으로 소극적인 편이다.

바이러스와 해킹 툴은 점점 더 지능화, 네트워크화 되고 있어 적극적이고 강력한 보안 시스템을 구축해도 취약점을 파고들어 치명적인 위협을 가하게 된다. 특히, 최근의 공격 툴은 SQL 슬래머 웜, 블래스터 웜에 의한 네트워크 공격, Pop Spam으로 인한 업무 장애 등에서 볼 수 있듯이, 개인 PC 시스템의 취약점을 통해 전체 네트워크와 시스템에 문제를 야기하는 형태로 발전하고 있다. 아무리 강력한 보안시스템을 구축했다 해도 사용자 PC의 보안 수준이 엉망이라면 많은 비용과 시간을 들인 보안시스템은 무용지물이 될 수 있다. 그러나 대다수 기업의 PC는 보안 패치와 백신 업데이트 등 공격을 받은 후 처리하는 수준에 머물러 있어, 전체 시스템을 위협하는 요인이 되고 있다.

정보유출의 80% 이상이 기업 내 구성원을 통해 이루어지고 있다는 각종 통계자료에서 볼 수 있듯이, 신뢰구간 내의 PC에 의한 보안사고와 보안 취약성으로 인한 문제는 점

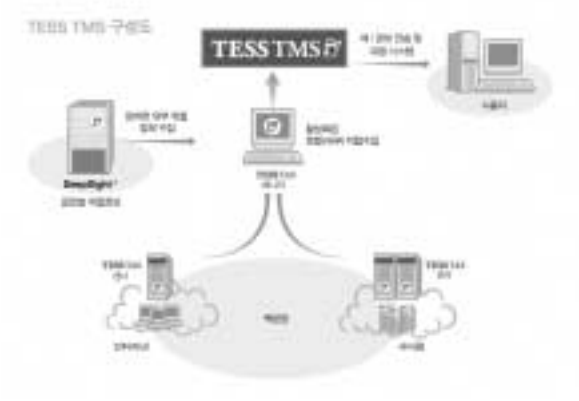
- 애플리케이션 패치 자동화, 패치 미설치 PC 인터넷 차단
- 이동식 저장매체 제어, 데이터 암 · 복호화
- 알려지지 않은 프로그램 제어
- 중앙시스템에서 외부 노출된 웜 차단

점 더 심각하게 나타나고 있다.

㈜잉카인터넷의 'nProtect Enterprise 2.5'는 다양한 보안 요소에 대한 중앙 보안 정책 수립과 배포를 통해 개인 PC 시스템에서 정보유출에 대한 불법침입을 사전에 차단하고 모니터링해 보다 안전하고 체계적인 통합 보안시스템을 구축한다. 윈도우 계열의 OS와 애플리케이션 패치를 자동으로 설치하도록 하며, 주요 패치가 설치되지 않은 PC의 인터넷을 차단한다. 웜 패턴을 파악해 자동으로 차단하며, 알려지지 않은 웜에 대해서는 임계값을 설정해 차단한다. 개인 PC 방화벽을 통한 접근제어와 사이트 차단, 해킹 툴 탐지와 삭제, 알려지지 않은 프로그램 제어기능도 제공한다.

사용자 PC의 외부 저장매체를 제어하며, 실시간 암 · 복호화를 통한 무단 유출을 막는다. OS의 로그온, 암호, 화면보호기, 공유 폴더 등의 취약성을 관리하고, 관리 콘솔을 통한 사용자 실시간 관리기능과 사용자의 웜 차단, 접근제어, 매체 기록정보에 대한 실시간 로그 모니터링을 한다. 전사적인 보안관리에 필요한 보안정책을 만들고 관리하는데 소요되는 비용과 솔루션을 운영, 관리하는 보안관리자의 시간을 최소화시키며, 인사이동으로 사용자와 그룹이 이동할 때에도 보안정책을 유지할 수 있도록 한다.

실제, 이를 구축한 기업의 사례를 통해 보면, 네트워크 부하의 80% 이상이 웜으로 인한 피해이며, nProtect Enterprise 구축 후 웜 발생이 10% 미만으로 저하되었다. 유해 사이트 차단으로 업무시간에 불필요한 사이트에 접근하는 것이 줄어들고, 매체제어 접근제어를 통한 내부 문서 유출을 줄이고, 보안의식을 강화시켰다. 또한, 소프트웨어와 하드웨어에 대한 효율적인 관리효과도 동시에 얻은 것으로 나타났다.



위협관리 시스템 : TESS TMS

제로데이 공격, 위협관리 시스템으로 해결

(주)정보보호기술 | T.02-2142-0999 | www.infosec.co.kr

보안위협이 심각해지면서 기업의 공통적인 요구사항은 알려지지 않은 공격에 대해서도 미리 예방할 수 있어야 한다는 것이다. 보안관리자가 시스템에 대한 공격을 인지한 후 대책을 마련하기 까지 걸리는 시간 동안 기업은 엄청난 손해를 입기 때문이다. 또한, 시스템 취약성이 알려진 후 대책이 마련되기 전 공격기법이 나오는 제로데이 공격에 대해서도 기업은 보다 근본적인 대안을 바라고 있다.

국가의 중요한 시설을 관리하는 국가기관의 경우는 예측할 수 없는 공격에 대해 더욱 완벽한 보안을 원하고 있다. 특히, 유비쿼터스 환경에서의 공격 · 침해 대상은 개인 PC를 넘어 보안침해 역작용이 큰 홈 네트워크, 교통, 병원, 전자지불, 재난관리 시스템 등을 위협한다. 이로 인해 국민들은 매우 큰 피해를 입게 될 뿐만 아니라, IT 강국으로서 우리나라의 이미지와 신뢰도에도 치명적인 영향을 미치게 된다.

이러한 배경에서 위협관리 시스템(TMS : Thread Management System)이 등장하게 되었다. TMS는 다가오는 위협을 조기에 감지하고 발생한 위협을 완화하거나 확산을 막으며, 피해를 최소화할 수 있도록 해준다. TMS는 지난 2003년 1 · 25 인터넷 대란직

• 국내 최초,유일의 CC 인증 위협관리 시스템
• 센서/네트워크 가상화로 조직관리 기능 제공
• 통계/DB의 최적화 등 사용자 편의 기능 제공
• 시만텍과 협력해 해외 보안정보 습득

후 대두되었으며, 현재 주요 정부 중앙부처와 공공 및 민간의 침해사고 대응기관과 대형 인터넷 서비스 제공업체가 위협관리 시스템이나 조기 예 · 경보 시스템을 구축하고 있다.

(주)정보보호기술의 'TESS TMS'는 우리나라에서 유일하게 CC 인증을 가진 위협관리 시스템이다. 기존의 보안솔루션은 이미 알려진 사이버 공격을 위주로 탐지하는 반면, TESS TMS는 트래픽의 세부 구성요소에 대해 각각의 프로파일을 생성한 후 이를 기반으로 비정상 탐지기능을 제공해 제로데이 공격 등 알려지지 않은 공격에 대처할 수 있다.

기존의 IDS는 사이버 공격의 근원지에 대해 조직의 내 · 외부 분류만 제공하지만, TESS TMS는 사이버 공격 모니터링 체계를 조직내부의 관리체계와 동일하게 설정할 수 있도록 네트워크 분류별로 위협수준 측정을 할 수 있다. 이를 통해 공격발생 초기에 공격 근원지와 피해지를 파악하고, 문제 네트워크를 격리해 피해가 확산되는 것을 막아준다.

정보시스템 보안관련 업무에서 방화벽, IDS 등 보안솔루션과 별도의 네트워크 모니터링 시스템을 사용하던 고객이 TESS TMS를 도입하면, 정보보안 사고에 대한 인지 · 분석 · 조치 · 보고 등 업무단계가 TESS TMS를 통해 단일화되어 원인분석과 심화분석이 가능해져 사이버위협 대응절차 전반에 걸친 서비스를 제공받을 수 있다.

글로벌 기업인 시만텍과 협력을 통해 해외의 정보를 습득할 수 있고, 다른 보안솔루션이 탐지할 수 없던 변종공격과 최신 사이버위협에 대해 예 · 경보 및 이상징후 탐지를 할 수 있어 관리자는 쉽게 네트워크 위협에 대처할 수 있으며, 현재의 상황을 직관적으로 파악할 수 있어 전사적 위협관리체계 환경을 구축할 수 있다.

TESS TMS는 국가 주요 기간망을 대상으로 하는 통합 보안관제 센터에서 통합 보안관제 도구로 활용되고 있다.

※ 침해사고 경보단계 및 대응기관 연락처

■ 침해사고 지원기관

기 관	홈페이지	전화번호	이메일	비 고
한국정보보호진흥원 인터넷침해사고대응지원센터	www.krcert.or.kr	118	cert@certcc.or.kr/ cert@krcert.or.kr	민간보안사고
국가사이버안전센터	www.ncsc.go.kr	111/3432-0462	info@ncsc.go.kr	정부기관, 공공기관 보안사고
대검찰청 인터넷 범죄수사센터	icic.sppo.go.kr	1301	icic@icic.sppo.go.kr	컴퓨터 보안사고 수사
경찰청 사이버테러 대응센터	www.ctrc.go.kr	02-393-9112	-	컴퓨터 보안사고 수사

■ 경보단계와 발령기관

구 분	설 명	발령기관
관 심	• 위험도 높은 웜/바이러스 취약점, 해킹 기법 및 공격 코드 출현으로 인해 피해 가능성 증대 • 해외에서 침해사고 확산 또는 일부 국내 유입 및 확산 가능성 증대 • 국내 인터넷 이상 트래픽 발생 가능성 증대	한국정보보호진흥원
주 의	• 웜/바이러스, 해킹 등으로 국지적 피해 발생 • 국지적인 인터넷 소통장애, 인터넷 관련 서비스에 장애가 발생되거나 매우 우려되는 경우 • ISP/IDC, 일반 사용자, 기업 등의 긴급대응 및 보안태세 강화 필요	한국정보보호진흥원
경 계	• 복수 ISP 망 또는 주요 정보통신 기반시설의 피해 발생 • 해킹 및 신종위협으로 주요기업 및 포털, 연구소 등 민간부문에 중대한 피해 발생 • 웜 · 바이러스, 해킹 등 침해사고로 민간부문에 대규모 피해 발생 • 상황 해결을 위해 민 · 관 각 분야의 협조 및 공동 대응이 필요한 상황	정보통신부
심 각	• 국내 인터넷 전 분야에 소통장애 발생 • 주요 정보통신 기반시설의 피해로 인하여 대국민 서비스 지장 발생 • 민간부분 전반에 인터넷 사용 불가능 • 국가적 차원에서 공동 대처해야 할 필요성이 있는 상황	정보통신부