# 우리 기업의 보안관리 취약점은 ?

지금까지 기업 정보보호를 위해 우수사례를 소개하는 기회는 많았던 반면 공통된 문제 즉, 기업 정보보호에 있어 각 기업이 공통적으로 안고 있는 문제점을 공유하는 기회는 상대적으로 적었다. 이런 상황에서 KISA가 기업 및 기관을 대상으로 실시해 왔던 정보보호관리체계 인증심사 및 사후관리 심사를 통해 기업들에게서 발견되는 문제점 발생빈도를 수치화해 '보안관리 취약점 Top 10'을 선정했다. 각 기업에게서 공통적으로 발견된 취약점에는 어떤 것들이 있었을까.

| 편집자 주 |

# 보안관리 취약점 Top 10

KISA는 지난 2007년 한 해 동안 총 40건의 정보보호관리체계 인증심사 및 사후관리 심사를 진행했고, 이를 통해 발견된 결함을 분석, 결함 발생순으로 '보안관리 취약점 Top 10'을 선정했다. 이중에는 '시스템 로그 백업 미흡 등 백업 절차 부재', '자산분류 기준 부재와 자산의 보안등급 미표기 및 취급절차 미흡', '관리자 계정 공동사용', '보안사고 예방 및 대응절차 미흡' 등이 공통적으로 안고 있는 취약점인 것으로 나타났다. 정보보호관리체계 인증은 개인정보 등 기업의 주요 정보자산 유출 및 피해를 사전 예방하고 대처하기 위한 종합적인 대책수립을 위해 도입된 제도로, 관리적, 기술적, 물리적 보호와 같은 종합적인 관리체계가 적절하게 운영되고 있는 지를 평가해 인증을 부여하는 제도다. 향후에도 매년 정보보호관리체계 인증심사를 통해 발견된 결함을 분석, 기업들이 특별히 관심을 갖고 대처해야 할 보안관리 취약점 Top 10을 선정해 발표할 예정이다.

고규만 IT기반보호단 기업정보보호팀 주임연구원(kmko@kisa.or.kr)

## 01 "장애발생 시 복구는? 침해사고 발생 시 추적은 어떻게?"

백업 및 복구는 예상치 못했던 재해 및 장애 등의 문제로 시스템이 손상됐을 경우, 업무 연속성을 보장하기 위해 가장 기본적으로 구현해야 하는 정보보호대책 중 하나다. 하지만 평균 인증심사 2회당 1번 꼴로 백업 및 복구에 대한 결함이 발견되고 있다. 이것은 대부분의 기업이 정보 시스템에 대한 백업을 수행하고는 있지만, 백업 범위(데이터, 시스템 로그, 환경설정 파일 등), 주기, 방법 등을 정의한 지침 및 절차가 마련돼 있지 않은 것을 의미하는 것으로, 기업이 시스템 장애 및 재해를 대비하는데 소홀히 하고 있다고 볼 수 있다. 다시 말해 백업이 명확한 절차에 의한 것이 아니라 담당자의 주관에 따라 임의적으로 이뤄지고 있다는 것을 의미한다. 시스템 접속 및 운영기록이 저장된 주요 로그 파일에 대한 백업이 이뤄지고 있지 않은 것은 침해사고 발생 시 사고조사 및 대응을 어렵게 만드는 원인이 될 수도 있다. 백업 및 복구관리와 관련해 주로 발견되는 결함을 살펴보면 다음과 같다.

- 백업대상, 백업방법, 백업주기 등을 명시한 백업 관련 지침 및 구체적인 백업 계획 부재
- 백업 관련 지침 및 계획 미준수, 백업 관리대장 관리 미흡
- 백업매체의 소산 미흡 및 소산장소 미지정

## 02 "도대체 무엇을 보호해야 하는 거야?"

나폴레옹 보나파르트는 "모든 것을 보호하려는 것은 보안을 하지 않는 것과 같다" 라고 했다. 다시 말해, 정보보호관리체계 범위 내의 주요 자산을 파악하고 효율적이고 안전하게 관리하기 위해서는 기업이 가진 모든 자산을 완벽하게 보호하는 것이 아니라, 자산을 적절한 기준에 따라 분류하고, 그 가치를 중요도에 따라 구분해 관리해야 한다. 하지만 많은 기업들은 정보자산의 분류기준이 정책, 지침에 구체적으로 명시가 되어 있지 않거나, 분류기준에 따라 정보자산을 분류하고 있지 않은 경우가 많았다. 분류기준을 명확히 정의하고 이에 따라 정보자산을 식별하고 관리한다면 이 통제항목에 대한 결함은 크게 줄일 수 있을 것으로 예상된다. 예를 들어, 정보자산은 데이터, 문서, 하드웨어, 소프트웨어, 설비, 인적자산으로 분류할 수 있다. 정보자산의 분류와 관련해 주로 발견되는 결함을 살펴보면 다음과 같다.

- 정보자산의 분류 기준 부재
- 정보자산의 분류 기준에 부합하지 않는 정보자산 관리
- 전자정보(고객정보 DB 등)와 문서(기밀문서, 보고서 등)자산의 정보자산 분류 누락

한편, 분류된 정보자산은 중요도에 따라 분류해야 하며, 추가적으로 그 중요도에 따라 보안등급을 표시하고 취급절차를 마련하여야 한다. 기업들 중에는 자산의 중요도를 산정하고 있기는 하지만, 실제로 그 중요도에 따라 명확한 처리절차를

갖고 있지 못하거나, 있다 해도 절차를 준수하지 않는 경우가 많았다. 정보자산의 보안등급 및 취급과 관련해 주로 발견되는 취약점은 다음과 같았다.

- 정보자산에 해당 보안등급의 물리적, 전자적 표시 미흡
- 문서자산의 경우 자산의 중요도 산정(1/2/3등급 등)과 문서자산 보안등급(기밀, 대외비, 사외비 등) 간의 일관성 결여
- 정보자산 보안등급에 따른 취급절차 미흡

## 03 "금고 열쇠를 아무나 복사해서 갖고 있다니!"

주요 시스템의 가용성을 보장하거나 시스템에 저장된 고객정보 등 기업이 보유한 민감한 정보의 유출을 방지하기 위해서는 사용자 계정의 접근 권한관리를 통한 통제가 필수적이다. 특히, 최근에는 내부자에 의한 정보의 유출 사고 사례가 증가하고 있어, 자칫 소홀해지기 쉬운 내부자 접근 관리에도 특별히 주의를 기울여야 한다. 특히, 주요 시스템의 관리자 계정을 내부 직원들이 공동으로 사용하고 있는 것은 접근통제의 중요성을 인식하지 못한 잘못된 사례라고 할 수 있다.

- 주요 시스템의 공동계정 사용
- 사용자 계정 등록 및 해지절차 미흡
- 신규 사용자 계정 발급에 대한 책임자의 승인 누락
- 사용자 권한 변경내역에 대한 주기적인 점검 미흡

## 04 "정보자산 변경 시 철저한 관리 필요"

'정보자산 식별'에 관한 요구사항에 따라 정보보호관리체계를 수립한 기업들은 보호받을 가치가 있는 정보자산을 식별해 자산목록으로 관리하고 있다. 하지만, 새로운 소프트웨어, 하드웨어 설치 등으로 인한 정보자산의 변경 시 준수해야 하는 변경 관리절차가 부재하거나, 있다 해도 따르지 않는 경우가 종종 발견되고 있다. 초기 정보자산의 식별뿐만 아니라, 정보보호관리체계의 운영과정에서 발생하는 자산의 변경에 대해서 그 내역을 철저히 관리하고 점검할 필요가 있다. 정보자산의 변경관리와 관련해 자주 발견되는 결함을 살펴보면 다음과 같다.

- 정보자산 변경절차의 부재 및 절차준수 미흡
- 변경에 대한 공식적인 승인절차 미준수
- 신규 네트워크 장비 설치, 소프트웨어 설치 등 변경에 대한 사전 영향분석 미흡
- 정보자산 변경내용, 변경이유, 변경날짜 등 변경기록 미흡

## 05 "긴급상황, 하지만 대응팀은 허둥지둥, 갈팡질팡"

보안사고는 해킹, 바이러스, 웜, 사람 등의 다양한 위협요소로 인해 언제든지 발생할 수 있다. 2003년 1·25 인터넷 침해사고 발생 당시, 많은 기업들은 보안사고에 대한 체계적인 대응절차를 수립하지 못해 그 피해가 컸던 것이 사실이다. 만약 각 기업이 1·25 인터넷 침해사고의 징후를 인지한 후 사전에 마련된 보안사고 대응절차에 따라 신속하게 대응했다면 피해를 상당히 줄일 수 있었을 것이다. 최근에는 국가 전체에 영향을 미치는 대규모 보안사고 뿐만 아니라, 단순 바이러스 감염 등에도 기업의 업무가 마비될 수 있기 때문에, 기업별로 업무특성에 적합한 보안사고 대응절차를 마련할 필요가 있다. 결국, 주기적인 보안점검을 통해 보안사고를 미연에 방지하는 것이 중요하지만, 보안사고 발생한 후 그 피해를 최소화하는 것도 그에 못지않게 중요한 일이다. 보안사고 대응계획 수립과 관련해 주로 발견되는 취약점은 다음과 같다.

- 보안사고 발생 시 긴급연락체계 작성 미흡
- 보안사고의 범위 및 정의 미흡
- 보안사고의 중요도에 따른 보고라인 및 처리방법 부재

## 06 "아하, 정보보호는 이래서 필요하구나!"

직원들에게 신규 취약점, 위협 등 정보보호 관련 이슈를 공유하고 기업의 정보보호 정책, 지침, 절차를 숙지시키기 위해 기업들이 선택하는 방법이 바로 정보보호 교육 및 훈련의 시행이다. 이를 통해 기업은 직원의 정보보호 인식수준을 기업이 원하는 적정수준 만큼 높일 수 있다. 정보보호관리체계 인증 획득 기업 중 전반적으로는 연간 정보보호교육 계획을 수립해 체계적으로 정보보호교육을 실시하고 있으나, 교육 실시 후 교육 내용에 대한 평가 및 분석을 하고 차기 계획에 결과를 반영하는 경우는 드물다. 정보보호 교육 시행 및 평가와 관련해 발견되는 결함을 살펴보면 다음과 같다.

- 연간 정보보호교육 계획서 미작성
- 교육 후 참석자 서명, 강사 평가 등 기록관리 미흡
- 교육 및 훈련 내용에 대한 효과 측정 및 분석 절차 누락

## 07 "아무나 출입할 수 없습니다!"

특별한 보호가 필요한 시설 및 장비를 비인가자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 보호하기 위해 제한구역, 통제구역, 사무실 구역 등 보호구역을 정의하고, 이에 따른 보안대책을 수립해야 한다. 하지만, 물리적 보호구역에 대한 정의가 명확하게 되어 있지 않거나 보호구역에 따른 정보보호대책이 수립되어 있지 않은 사례가 적지 않게 발견되고 있다. 물리적 보호구역과 관련해 주로 발견되는 결함은 다음과 같다.

- 물리적 보호구역의 구분 및 정의 누락
- 물리적 보호구역 경고 표시 미부착
- 물리적 보호구역 내 장비, 문서, 매체 반출입 절차 부재

## 08 "우리 정보자산에는 어떤 위험이 있지?"

앞서 기업 정보자산 분류에 이어 기업은 식별된 정보자산에 영향을 줄 수 있는 모든 위협, 취약성, 위험을 식별하고 분류해야 하며, 이 정보자산의 가치와 위험을 고려해, 잠재적 손실에 대한 영향을 식별·분석해야 한다. 하지만, 위험분석 범위에 고객정보 등 중요자산이 누락되어 있거나 식별된 자산의 모든 위협요인은 고려하지 않고, 취약성 정도만을 분석하는 등 평가 방법에 문제가 있는 경우가 많았다.

- 위험분석 범위 내에 고객정보 등 중요자산 누락
- 위험분석 및 평가 방법론이 정의되지 않음
- 지침에 명시되어 있는 자산가치 산정기준, 취약성 및 위협 평가기준을 따르지 않음
- 목표위험수준(DoA)의 최고책임자 승인 누락

## 09 "나는 볼 수 없으나, 제3자는 볼 수 있다"

기업은 수립된 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되고 관리되고 있는 지를 점검하기 위해 감사의 기준, 범위, 주기 및 방법을 규정하고, 규정에 따라 별도의 감사조직을 통해 내부감사를 수행하여야 한다. 하지만 조직에서 규정하고 있는 내부 감사기준이 정보보호관리체계의 관리실태를 파악하기에 미흡한 사례가 많았으며, 또한 규정된 기준에 의거 내부감사를 진행하고 있지 않은 경우가 많았다.

- 구체적인 내부감사 규정을 마련하고 있지 않음
- 조직에서 규정하고 있는 감사기준에 따른 주기적 감사 미흡
- 독립된 감사조직에 의한 감사가 이뤄지지 않음

## 10 "이것만은 꼭 준수하겠습니다."

마지막으로 각 기업은 영업비밀에 해당하는 주요 정보를 이용하고 있는 직원이나 임시직원 등 정보에 대한 접근권한이 있는 자에 대해 정보 유출방지를 위한 비밀유지 서약서를 요구해야 함에도 불구하고, 정직원이 아닌 임시직 또는 제3자에 대한 비밀유지서약서의 요구 및 관리가 이뤄지지 않은 조직이 많이 있다. 최근 핵심 기술정보 유출 등으로 피해가 늘어나고 있는 실정이므로 가치가 높은 주요 정보를 법적으로 보호받기 위해서는 비밀유지서약서 요구 등 기업 스스로의 보안관리 노력이 필요하다.

- 정규직원 이외에 조직의 정보 접근권한을 갖고 있는 비정규직원, 제3자에게 비밀유지서약서 미 요구
- 신입직원에 대한 비밀유지서약서 미 요구
- 비밀유지서약서 관리 미흡

| 순위 | 발견된 취약점(결함사항) | 통제 내용 | 결함건수 |
|---|---|---|---|
| 1 | 백업대상, 주기, 방법 등이 명확하게 정의되어 있지 않고 특히 시스템 로그백업이 미흡함 | – 데이터 및 장비의 무결성과 가용성을 유지하기 위해 백업 계획을 수립하여 이행하고 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다. | 16 |
| 2 | 백업대상, 주기, 방법 등이 명확하게 정의되어 있지 않고 특히 시스템 로그백업이 미흡함 | – 정보자산이 신청기관에서 차지하는 가치와 신청기관에 미치는 영향을 고려하여 분류방식을 선택하고 분류하여야 한다.<br>– 중요도에 따라 분류된 정보자산에 보안등급을 부여하고, 물리적, 전자적 보안등급 표시를 부착, 관리하여야 한다. 또한 보안등급의 부여에 따른 취급절차도 정의하여 이행하여야 한다. | 15 |
| 3 | 관리자 계정 공동사용, 계정등록 해지절차 미흡 | – 정보시스템 및 서비스에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하여야 한다. | 12 |
| 4 | 정보자산의 변경절차 부재 및 절차준수 미흡 | – 정보시스템 관련 자산들을 조사하고, 모든 변경사항들을 반영할 수 있는 공식적인 관리책임 및 절차를 수립하여야 한다. | 10 |
| 5 | 보안사고 예방 및 대응절차 미흡 | – 보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생 시 보고 및 대응 절차, 사고 복구조직의 구성, 교육계획 등을 포함한 보안사고 대응 계획을 수립, 이행하여야 한다. | 9 |
| 6 | 정보보호교육 계획 부재 및 교육 미실시 | – 교육 및 훈련은 정기적으로 실시하여야 하며, 정보보호정책이나 절차 및 역할의 변경이 있는 경우에는 수시로 실시하고 이에 대한 기록을 남겨야 한다. 또한 교육훈련 종료 후 검토를 통하여 차기 교육에 반영하여야 한다. | 9 |
| 7 | 물리적 보호구역 미정의, 반출입 절차 부재 | – 물리적 보호구역에 대한 출입은 적절한 출입통제절차에 의하여 통제되어야, 출입자를 식별하고 기록·관리하여야 한다. | 8 |
| 8 | 고객정보 등에 대한 위험분석 누락 및 위험분석 및 평가방법론 부재 | – 식별된 정보자산에 영향을 줄 수 있는 모든 위협, 취약성, 위험을 식별하여 분류하여야 하며, 이 정보자산의 가치와 위험을 고려하여, 잠재적 손실에 대한 영향을 식별·분석하여야 한다. | 7 |
| 9 | 기업 내 보안활동에 대한 내부감사 규정 부재 및 주기적 감사 미흡 | – 기업은 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는 지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다. | 7 |
| 10 | 기업의 주요정보 유출방지를 위한 비밀유지서약서 미요구(정규, 비정규직원, 제3자 등) | – 직원으로부터 비밀유지 서약서에 서명을 받아야 하며, 임시직원이나 제3자에게 정보에 대한 접근 권한을 부여할 경우에도 그들로부터 비밀유지 서약서에 서명을 받아야 한다. | 7 |

▲ 2007 기업 정보보호 관리 취약점 Top 10

### ISMS 인증을 받게 되면

정보보호관리체계인증(ISMS : Information Security Management System)은 개인정보 등 기업의 주요 정보자산 유출 및 피해를 사전 예방하고 대처하기 위한 종합적인 대책 수립을 위해 도입된 제도로, 관리적, 기술적, 물리적 보호와 같은 종합적인 관리체계가 적절하게 운영되고 있는 지를 평가해 인증을 부여하는 제도다. 특히 각 기업 및 기관이 인증 획득 준비과정을 통해 '직원의 정보보호인식 제고', '대외 이미지 제고' 등 효과를 거둘 수 있을 뿐만 아니라, 다음과 같은 실질적인 혜택을 얻을 수 있다.

| 구분 | 시행기관 | 혜택 내용 |
|---|---|---|
| 요금할인 | 보험사 | 정보보호관련 보험(배상책임보험 등) 가입 시 할인율 적용 |
| 가산점 부여 | KISA | 정보보호대상, 입찰, 과제선정 평가 시 ISMS 인증 취득 기업에 가점 부여 |
| | 교육부 | 원격대학 평가 시 가점부여 |
| | 신용평가 기관 | 한국신용평가정보 등의 경우 기업신용평가 시 가산점 부여 |
| | 기술보증기금 | 중소기업이 기술평가 보증을 받고자 할 때 가산점 부여 |
| | 국가·공공기관 | 국가·공공기관 용역사업 선정 평가 시 가점 부여(기관별 자체 시행)<br>예) 정통부 중소기업 지원사업 가점 부여 – 우수기술지원사업(2점), 산업경쟁력 강화지원 사업(2점), 협업기술 개발사업(2점) |
| 면제 | 정통부 | 인증을 받은 해당 연도 안전진단 면제 |

▲ KISA ISMS 추가 혜택 항목