기업문서 유출 방어대책 시급하다.

조 성 호
가드쉘 대표이사

국가정보원은 흥미로운 자료를 발표 했다.

500개 기업을 대상으로 조사한 자료에 따르면 조사업체 대부분이 내부문서를 허술하게 관리해 산업경쟁력의 저해요소가 되고 있다는 내용 이었다.

보고서에 따르면 500개 기업중 기밀자료 유출로 피해를 입은 기업이 27%였고 보안관리를 위한 규정이나 지침 조차 없는 기업이 절반이 넘는 50.6% (253개)에 달했다.

또 보안교육을 한번도 받아보지 못한 직원도 64.5%에 달해 회사를 그만 둘때 자기가 개발한 자료를 갖고 퇴사 하는 것이 비일비재하며 그만큼 회사기밀 유출이 심각한 상황이라고 지적했다.

기업의 핵심기술 유출문제가 산업계의 '핫이슈'로 떠올랐다. 이는 정보화가 진전될 수록 기술유출 방법이 가속화, 다양화되기 때문이다. 1, 2명이 근무하는 작은 회사라도 PC는 반드시 쓰게 마련이고 임직원은 중앙컴퓨터와 통신망으로 연결된 PC를 기본으로 모든 업무를 처리한다.

PC를 이용해 자료를 무단유출하는 행위는 크게 복제(copy)·전송(transfer)·프린트 등 몇가지로 나눌수 있으나 암·복호화 무력화 방법이나 고도의 PC기술을 가진 사용자가 시도하는 메모리 해킹방법 등 세부적으로 나누면 50개 가까운 방법이 있다.

과거에 가장 많이 이용된 전자문서의 무단유출 방법은 회사의 자료를 디스켓이나 CD에 무단복제해 사외로 갖고 나가는 것이 었다. 그러나 회사의 출입통제가 강화되고 e메일이 보편화 된후에는 이를 통한 자료유출이 매우성행하고 있다. 회사에 앉아 업무를 보는 척하며 회사자료를 검색한 후 해당자료를 자기개인의 포털 메일박스에 전송해 버리는 것이다.

그후 집으로 돌아와 전송된 회사자료를 잘 정리해 요약한 후 다른회사로 전직하는데 이용하거나 경쟁사에 돈을 받고 팔아버린다. 특히 요즘에는 새끼 손가락 한개 크기의 휴대가 매우 간편한 장치인 USB 저장장치가 나와 자료의 무단 유출이 더욱 손 쉬워졌다. USB 저장장치는 고밀도· 고집적이 급속히 진행돼 1기가 바이트급 USB도 시장에 나와 있는 상황이다. 이를 방지할 수 있는 가장 효과적인 방법이 바로 전자문서 보안기술의 도입이다.

전자문서 보안은 전자문서 유출을 사전에 방지하고 조직원에 의한 불법 사용내역을 자동리포트 해주는 제반컴퓨터 시스템을 말한다. 전자문서보안시스템은 암호화를 기본으로 해킹을 불가능 하게하고 사용자 또는 문서의 중요도에 따라 이용할 수 있도록 전산환경을 사전에 조절해 준다. 즉 조직원끼리 노하우 공유를 위해 지금처럼 검색과 열람은 자유롭게 허용해 주면서도 허가 없는 자료의 무단복제, 전송, 프린트나 스크린 캡처 등 자료의 무단 유출이 일어날 수 있는 모든 방법을 차단해 준다.

만약 허락이 안된 사람이 중요 자료의 복제나 전송· 프린트 등을 시도하면 그 행위는 자동차단돼 무단유출이 안될 뿐아니라 이행위가 중앙컴퓨터에 자동으로 보고돼 관리자나 보안담당자가 그내용을 알수 있도록 만들어져 있다. 전자문서 보안시스템은 6가지의 주요기술과 기능을 결합해 구성해야 한다.

첫째가 인증처리시스템이다. 인증기술은 조직내 사용자의 적법성 여부를 확인하기 위한 과정으로 다양한 기술을 활용할 수 있다. 가장 쉽게 접근 할수 있는 방법은 기존 ID와 패스워드에 PC 각각이 갖고 있는 유일한 하드웨어 식별자(Mac 어드레스)를 결합해 사용하는 것이다. 또 기업에서 스마트카드 시스템이나 PKI 인증센터를 사용해 이들 시스템과 연동하는 방식으로 보안의 효율성을 높일수 있다.

둘째는 암호화처리 기술이다. 암호화 기술은 전자문서를 보호하는 가장 기본이다. 전자문서를 암호화해 보호하고 특정키를 보유한 사람만이 이를 사용할수 있도록 해주는 기술로 공개키 암호기반(PKI)으로 대표되는 비대칭키 방식과 대칭키 방식이 있다.

셋째는 다양한 사용권한관리 기술을 꼽을 수 있다. 조직내의 전자문서는 모든 사원이 모두 볼 수 있는 수평구조와 특수한 일부 사람만이 보게 되는 수직 구조 문서로 나눌 수 있다. 매트릭스 구조의 전자문서의 사용권한을 관리할 수 있는 기술이 필수적인 것이다. 매트릭스 구조란 수직적으로는 한 부서 또는 특수한 몇 명만이 공유하는 권한과 수평적으로는 직급에 따라서 공유하고 관리하는 권한이 있음을 의미한다. 이 기술은 열람권리, 배포권리, 문서를 수정할 수

있는 편집과 복사, 다운로드, 출력, 사용기간, 양도권한 등을 관리하는기술이다.

넷째 템퍼 프루핑(temper proofing) 혹은 크래킹 방지기술이다.

전자문서보안시스템에서 자료유출 방법중 소프트웨어 구성의 허점을 찾아 내거나 모듈간 통신프로토콜의 약점과 암·복호키의 분배, 보관과 같은 관리상의 허점을 찾아낸후 크래킹을 시도하는 방법도 있다. 따라서 알고리듬의 구현이나 설계시에 불법사용자에 의한 프로토콜 공격에 대비할 수 있는 기술을 적용하는 것이 필수적이다.

다섯째는 사용자의 다양한 환경이나 응용소프트웨어를 지원할 수 있는 커널 수준의 전자문서 보안시스템 모듈 기술이다. 현재 조직내 대부분의 사용자는 윈도환경을 사용중이다.

그러나 이용자마다 윈도 버전은 매우 다양하다. 기업에 따라서는 윈도95에서 윈도XP까지 다양한 환경을 사용해 하나의 운용체계로 통일 할 수 없는 상황에서는 운용체계 버전으로 인한 오류가 발생하지 않도록 세심한 모듈 개발이 필요하다. 또 조직마다 활용하는 PC 응용소프트웨어가 달라 이들을 통합해 지원 할 수 있는 모듈기술이 필수적이다.

마지막으로 출력자나 유출자 추적기술이다. 권한이 없는 사용자는 읽기기능 이외의 모든 문서 유출행위를 막아야한다. 그러나 권한이 있으면 출력이나 복제 또는 e메일 전송 등으로 유출 시켰을때, 출력자나 유출자를 추적할수 있어야 한다. 이런 추적기술로는 핑거프린팅(혹은워터마킹) 기술을 활용한다. 워터마킹기술은 디지털문서에 사용자 정보를 은닉해 출력물이나 디지털문서에서 유출자 정보를 추출해 불법행위를 추적하는 기술이다.

이 6가지 기능을 통해 구현된 문서보안시스템은 구현기술에 따라 장단점을 가지고 있다. 주요기능을 모두 포함하더라도 시스템 구축시 프로그래밍 과정에서 어떤 기술을 실제로 적용 하는가에 따라 문서보안시스템의 품질은 크게 차이가 난다. 문서보안시스템을 만드는 핵심기술의 종류와 기술에 따른 장단점은 이렇다.

첫째 많이 사용된 구현기술은 데이터를 불러오는 애플리케이션 메뉴를 제어한다.

즉 메뉴바에서 카피나 프린트 또는 전송 등의 메뉴를 사용하지 못해 무단 유출을 막게 되는데 이기술을 사용해 만든 문서보안시스템은 방어에 효과적이지 못하다. 메뉴를 제어하거나 사용하지 못하게 하는 기술로 만든 시스템은 해커가 방어시스템을 쉽게 분해하고 메뉴를 다시 사용하게 만들어 중요 문서를 유출시킬수 있기 때문이다. 이기술의 80~90% 정도는 인터넷에서 쉽게 구할 수 있으며 문서보안시스템 중 3등급 기술로 구현된 시스템이다.

둘째 구현된 기술은 가상 드라이버시 스템과 메시지 후킹기술을 원천기술로 사용하는 경우다. 메뉴 제어기술 보다는 진보된 기술이기는 하지만 이역시 문제가 생길 수 있다. 왜냐하면 윈도시스템이 제공하는 메시지큐(queue)가 작아 메시지가 오버플로우(over flow) 되면 시스템에 치명적인 오류가 생긴다. 또 레지스트리(registry)를 방어하지 못해 해커가 침투할 수 있으며 문서보안 시스템이 방어하기 전에 고도의 기술을 가진 해커가 먼저 메시지를 후킹하면 무단유출 시스템 자체가 무력화 될 수 있기 때문이다. 이 기술로 만든 시스템은 2등급 기술을 사용했다고 보면 된다.

이 문제를 해결하면서 방어에 보다 완벽한 문서 보안을 만들려면 셋째 기술을 원천기술로 사용해 만들어야 한다. 그것은 '디바이스 드라이버(device driver)' 제어기술과 하드웨어 API 후킹기술 및 RAM을 디스크화해서 사용하는 기술 등을 기반으로 문서보안시스템을 만드는 것이다. 디바이스 드라이버시스템이란 프린터·마우스·네트워크장치 또는 하드디스크 등이 작동되는 기반 프로그램을 말하는데, 문서유출은 이들기기를 반드시 이용 할 수 밖에 없어 이들장치를 사전에 제어하는 보안시스템을 만들면 보다 완벽한 문서보안시스템을 구축할수 있다. 또 RAM 디스크기술을 사용하면 고의로 전기공급을 차단·에러를 일으킨채 PC를 다운시킨 다음 재부팅때 나타나는 선행 에러메시지를 분석해서 문서보안시스템을 무력화시키는 해킹기술을 차단할수있다. 이런기술로 만들어진 문서보안시스템을 기술수준 1등급 수준으로 만들어졌다고 평가하는데, 윈도OS 레이어(layer) 기반의 커널 Ring 제로(0) 수준의 최고기술이다.

'경제전쟁'이라는 말까지 사용되는 지금의 기업환경에서 어느기업도 산업스파이로부터 자유롭지 못하다. 외부에서 회사전산망으로 들어오는 해커를 막는 것도 중요하지만 내부직원 또한 언제 우리 회사의 기업비밀을 빼갈지 모른다. 믿고 살아가야 하는 동료 직원을 믿지 못하는 현실이 아쉽기는 하지만 직원에 의해 중요 전자문서가 빠져 나가는 것이 현실이니 만큼 이제는 방어 대책을 수립하고 시행해야만 할 때다. 특히 IMF 외환관리 이후 평생기업이라는 개념이 사라진 현재 여건에서 언제, 누가 회사의 기밀 자료를 유출 할지는 아무도 모른다.

국가정보원은 지난 6년간 해외로 빠져나가는 국내기술을 38건이나 막았다. 유출방지 금액을 돈으로 환산해보니 무려 22조원이나 되는 천문학적인 금액에 이른다. 이를 국가별로 보면 예상대로 중국이 가장많아 36.8%인 14건에 이르고 2위는 세계 초강대국인 미국으로서 23.6%인 9건에 달했다. 세계최강인 미국기업도 이제는 우리나라가 개발하는 신제품 개발기술을 노리고 있는 것이다.

현재처럼 전산망이 무차별적으로 개방되어 있으면 아무리 좋고 우수한제품 개발력을 갖고있더라도 핵심기술이 무단 유출되어 엉뚱한 시기에 엉뚱한 나라에서, 예상치 못한 강력한 경쟁회사가 나타나 자기회사의 시장을 빼앗어 갈지 모르는 것이다. 전자문서 보안문제는 이제 산업계의 당장 시급한 이슈가 되었다.