Forensic
Service

FA Forensic Team
백철호 상무
02-6676-2250
cbaek@deloitte.com

정보유출보안 통제와 디지털 포렌직의 활용

정보유출보안에 대한 지속적 투자에도 불구하고 정보와 데이터 도난의 위험에서 벗어나지 못하고 있다.

1990년 중반만 해도 PC의 보급 및 활용이 그다지 많지 않았다. 그 시절 우리가 알고 있는 일반적인 PC는 데이터의 처리 속도가 상당히 느리고 데이터 보관을 위한 저장매체 또한 상당히 고가였다고 기억된다.

당시 1기가바이트(GB)라는 단위는 일반인들에겐 매우 생소할 뿐만 아니라 접하기도 어려운 단어였으나 요사이엔 PC 보급률의 급증 덕분인지 수백 기가바이트 또는 테라바이트(TB)란 단어는 주위에서 자주 듣는, 그다지 생소하지 않은 단어가 되었다.

이처럼 데이터의 처리 속도는 상당히 빨라졌고 데이터를 저장하는 저장매체 또한 대용량화되었다. 특히 정보·데이터에 대한 가치 부여 정도는 하루가 다르게 높아지고 있다. 그러나 안타깝게도 이들 가치의 정도에 상관없이 정보·데이터의 도난 사건 또한 급증하고 있는 것도 사실이다.

이러한 정보·데이터 도난을 방지하기 위해 많은 기업들이 정보유출 보안을 위한 통제 시스템 구축에 상당한 투자를 지속하고 있다. 하지만 그럼에도 불구하고 정보·데이터의 도난·유출 사건은 지속적으로 증가하는 추세다. 이는 제아무리 효과적인 통제 시스템이라고 해도 정보와 데이터에 대한 도난의 위험에서 완전히 안전할 수 없다는 방증이다.

이에 국내 정보유출보안 현황, 정보유출의 현주소, 그리고 정보유출에 따른 사후 조사 방안에 대해 짚어보고자 한다.

정보유출보안 현황

정보의 양이 기하급수적으로 증가함에 따라 기업들의 정보보안에 대한 관심과 투자 또한 증가하고 있다.

디지털 정보의 홍수

10년 전까지만 해도 이동식저장장치(USB)는 고작해야 몇백 메가바이트(MB) 정도였지만 이후 매년 저장 용량은 2배씩 성장해 이제는 몇십 기가바이트(GB)는 보통일 정도로 발전했다. 그뿐만 아니다. 몇 해 전 한 시장조사업체에 따르면 1인당 평균 데이터 보유량이 128기가바이트에 이르고 있다고 한다.

미국 대통령 과학기술자문위원회(President's Council of Advisors on Science and Technology·PCAST)에서는 최근 '디지털 미래 전략(Designing a Digital Future)'이라는 보고서를 통해 "모든 미 연방정부 기관들은 '빅데이터' 전략이 필요하다"라고 결론지었다. 시장조사 기관인 IDC의 '디지털 유니버스 보고서(Digital Universe Study)'에 따르면 올해 생산되는 디지털 정보량이 무려 1.8제타바이트(1ZB=1조 GB)에 달할 것으로 파악되었다. 이 보고서에서 따르면 2020년까지 관리해야 할 정보의 양은 현재보다 약 50배가 증가할 것으로 예측되고 있다.

보안 솔루션의 활용

한 기관에서 시행한 정보보호와 관련한 기업의 투자 현황 조사에 따르면 참여한 조사 대상 기업 6,529개 중 36.5%가 정보보호에 대한 투자를 실시하고 있으며, 이 중 19.9%가 전년 대비 투자 규모를 증가시킨 것으로 조사되었다.

또한 몇 해 전 한국인터넷진흥원의 조사에 따르면 정보보호 솔루션 제공업체들의 정보보안 제품 매출이 전년 대비 21.1% 성장했고, 정보보호 솔루션 서비스 부문 매출 역시 23.8% 증가했다고 알려졌다. 이는 기업들이 정보보안에 지속적인 관심을 기울이며 투자하고 있음을 알 수 있는 대목이다.

정보유출을 막으려는 다각적 노력에도 불구하고 그 피해액은 수조 원에 이르고 있다.

정보유출 현주소

국내 기업들의 정보유출 현황

법무부 통계 자료에 따르면 검찰이 처리한 기술 유출 범죄 사건은 1999년 총 39건(95명)에서 2009년 292건(807명)으로 꾸준히 증가하는 추세다. 또한 산업기술보호센터의 발표에 따르면 국내 기술을 해외로 불법 유출하려다가 적발된 사례가 2004년 26건에서 2010년 41건을 기록한 이후 2013년까지 급증하고 있다. 발표 기관에 따라 편차가 있긴 하나 지난해 산업기술 유출에 따른 피해액은 수조 원에 이르고 있다.

보안 노력에도 불구하고 유출되는 정보

문제는 정보유출을 막으려는 다각적인 노력에도 불구하고 정보유출이 매년 꾸준히 증가하고 있다는 사실이다. 결국 기업이 엄청난 투자를 통해 정보유출 방지를 위한 노력을 해도 의도적인 유출을 막기란 쉽지 않다는 것이다.

세계적인 보안업체가 몇 해 전 외부 설문조사업체와 공동으로 실시한 설문조사 결과를 보면 응답자의 59%가 전 직장에서 고객 리스트 등 기밀 정보를 유출한 적이 있는 것으로 나타났다. 기밀을 빼내는 데 이용된 수단으로는 CD나 DVD가 53%, USB와 개인 이메일 전송이 각각 42%와 38%로 나타났다. 특히 응답자의 82%는 퇴사 전 종이·전자문서에 대한 아무런 감사나 검토가 이뤄지지 않았으며, 응답자의 24%는 퇴사 후에도 기업 컴퓨터 시스템이나 네트워크에 자신의 아이디로 접속할 수 있었다고 답해 기업들의 정보보안에 커다란 문제점이 있음을 보여주고 있다.

디지털 포렌직을 활용한 정보유출 사고의 사후 조사

디지털 시대가 도래함에 따라 법정에서 디지털 증거를 다루기 위한 디지털 포렌직 분야에 대한 관심이 높아지고 있다.

디지털 포렌직이란?

'포렌직'이란 증거가 될 만한 대상을 법정에서 증거로 받아들여질 수 있도록 무결성보전절차(chain of custody)를 통해 식별(identify), 수집(collect), 분석(analyze) 및 제출·보고(submit·report)를 하는 전반적인 행위를 일컫는다.

보통은 국립과학수사연구소가 수행하는 업무처럼 물리적, 생물학적, 화학적 증거를 주로 다루었지만 디지털 시대가 도래함에 따라 디지털 증거를 다루기 위해 디지털 포렌직 분야가 생기게 되었다.

디지털 포렌직은 컴퓨터나 디지털 저장매체에서 발견되는 증거를 포렌직 기법을 사용해 식별하고 수집, 복구, 분석, 제출·보고하는 업무를 포함한다. 디지털 포렌직은 분석 대상에 따라 컴퓨터 포렌직, 네트워크 포렌직, 모바일 포렌직 등으로 나눌 수 있다.

매체를 따라 이동하는 디지털 정보 분석을 통해 정보 유출에 대한 증거분석을 하는 것이 디지털 포렌직의 한 부분이다.

정보유출 조사에 디지털 포렌직 활용

비즈니스 기록의 디지털화로 유출할 기술 정보의 대상이 디지털 정보로 옮겨감에 따라, 기술유출 사건의 대부분은 유출 발생 후 상당한 시간이 흐른 뒤 사실이 감지되어 조사를 시작하는 경우가 있다. 이 또한 초반에는 정보유출에 대한 심증만 있을 뿐 확실한 물증이 없어 조사에 어려움을 겪는 경우가 대부분이다. 하지만 디지털 정보는 매체를 따라 이동하기 때문에 증거가 존재하는 한 분석을 통해 대부분 발견된다. 바로 이렇듯 정보유출에 대한 증거를 분석하는 것이 디지털 포렌직의 한 부분이다.

최근의 기술유출은 출력된 문서를 통해서라기보다 디지털화된 상태로, 이를 테면 이메일, 전자파일, 디지털 사진 형태로 유출되는 경우가 많으며 이런 디지털 정보들은 보내는 컴퓨터로부터 받는 컴퓨터까지 이동 경로를 따라 흔적을 남기기 때문에 이런 흔적을 분석함으로써 유출 경로를 추적할 수 있다.

디지털 포렌직을 활용한 기술유출 조사는 유출, 취득, 사용이라는 세 가지 사실 파악을 목적으로 한다. 좀 더 이해를 돕기 위해 흔히 알고 있는 중요한 소스코드의 유출을 예로 들자면, 유출의 경우 비인가된 사용자 또는 접근이 제한된 사용자가 정보를 보호하는 시스템으로부터 기술 정보를 내려받는 행위 등을 파악하는 것이고, 취득은 유출된 정보와 무관한 사용자가 해당 자료를 보유하고 있는지를 파악하는 것이며, 사용은 유출된 정보가 개작된 결과물에 얼마나 사용됐는지를 파악하는 것이다.

이러한 디지털 포렌직에는 다양한 기술이 사용되며 이 다양한 기술에는

데이터 복구, 해쉬값 비교[1], 시그니처 분석[2], 암호 해독, 타임라인 분석, 레지스트리 분석[3] 등의 기술이 포함된다. 사안마다 다르지만 어떤 기술 정보가 어디에서 어떻게 유출되어, 현재 어떤 정보를 소유하고 있으며, 어디로 옮겼는지를 파악할 수 있다.

그러나 기술유출과 같은 화이트칼라 범죄는 그 방법이 해가 갈수록 지능화되어 가는 추세로, 디지털 포렌직도 정보 분석에 실제 어려움을 겪고 있는 것이 사실이나 어느 정도 의도적으로 삭제된 정보에서도 증거는 발견된 경우가 상당히 많다.

일례로 실제 복구된 사진 파일에서 기술 유출자들이 퇴사 후 차린 작업실 사진이 발견됐으며, 그 사진을 통해 압수되지 않은 과거 작업 시 사용했던 컴퓨터와 저장매체들이 포착되었다. 유출된 기술이 어느 정도로 사용됐는지에 대한 분석은 상당한 전문성을 요구하고 다양한 분야에서 다양한 기술을 활용해 분석해야 하므로 단순히 디지털 포렌직 전문가의 분석으로 완료되는 것이 아니다. 해당 분야의 전문가를 동원해 유출된 기술의 사용을 분석해야 하는 절차가 요구되는 것이 현실이다.

컴퓨터 포렌직이 기업의 기술 유출이나 횡령의 증거들을 포착해내는 유용한 방안으로 활용되고 있다.

컴퓨터 포렌직을 통한 디지털 증거 획득

기술유출이나 횡령 등의 부정이 발생했을 경우 가장 많은 디지털 증거가 발견되는 컴퓨터를 분석하는 것이 컴퓨터 포렌직이다. 컴퓨터 포렌직을 통해 인터넷 히스토리 분석, 파일 복구, 이메일 분석, 레지스트리 분석 등을 수행할 수 있다.

1) 사람마다 유일한 지문이 있다면 파일도 '디지털 지문'인 고유의 해시 값을 가지고 있다. 이 해쉬 값을 통해 원본과 복사본이 동일하다는 무결성을 증명할 수 있다.
2) 어떤 직원들은 파일 유형을 의도적으로 숨기려고 파일 확장자를 변경한다. 예를 들어, 중요 문서 파일을 JPG 같은 잘못된 확장자로 변경하게 되면 프로그램에서 문서 파일로 인식하지 못한다. 따라서 파일 시그니처 분석을 수행함으로써 파일 확장자의 변경 여부를 확인할 수 있다.
3) 레지스트리는 윈도우 XP, 비스타 등의 운영체제에서 사용되는 데이터 베이스로, 응용 프로그램 운영에 필요한 사용자 로그인, 서비스 실행, 응용 프로그램 실행, 사용자 행위 등의 정보가 저장되어 있다. 레지스트리 분석을 수행함으로써 USB 연결 흔적, 응용 프로그램 사용 흔적 등 PC에서 발생한 전반적인 행위에 대한 정보를 파악할 수 있다.

모 자동차 관련 상품개발 연구실 개발자들이 중요 기술을 유출해 동일 제품이 경쟁사에서 생산된 사건이 발생했다. 디지털 증거 획득을 위해 컴퓨터 포렌직을 진행했고, 개발자들이 사용하던 컴퓨터와 서버 기록 등을 토대로 정보유출과 취득 여부를 확인할 수 있었다. 또한 인터넷 사용 기록을 토대로 유출된 정보를 저장하고 있는 위치를 식별해냈고 복구한 사진 파일에서 기술 유출을 모의한 공범의 참여 여부를 확인할 수 있었다.
에너지 사업 개발자가 생산공정 시설의 사진과 설계도를 유출한 사건에서도 컴퓨터 포렌직을 통해 개발자가 사용하던 컴퓨터를 복구 및 분석, 복구된 사진에서 휴대전화로 찍은 생산시설의 사진을 다량 발견할 수 있었고, 복구된 파일에서 실제 설계도를 발견하기도 했다.

개인정보보호에서 디지털 포렌직의 역할

최근 강화된 개인정보보호법이 기존의 신용정보법, 정통망법, 공공기관 개인정보보호법을 포괄, 강화됨에 따라 디지털 포렌직의 역할 또한 더욱 중요해지고 있다.

개인정보보호를 위한 디지털 포렌직 적용

최근 새로운 개인정보보호법이 제정, 공포되어 2011년 후반기부터 시행에 들어갔다. 개인정보보호법의 주요 골자는 개인을 식별할 수 있는 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등의 행위에 대해 개인정보 처리자의 의무를 규정하고 있다. 기존의 '신용정보법(신용정보의이용및보호에관한법률)', '정통망법(정보통신망이용촉진및정보보호등에관한법률)', '공공기관의 개인정보보호법에관한법률'을 포괄, 강화했다. 이는 최근 개인정보보호법에서조차 디지털 포렌직이 중요한 역할을 차지하고 있음을 의미한다고 할 수 있겠다.
새로운 개인정보보호법에서는 전자적 파일 형태의 개인정보는 복원이 불가능한 방법으로 영구 삭제하도록 규정해 놓았다. 따라서 서버, 컴퓨터 등에 있는 개인정보는 복원이 불가능한 형태로 파기해야 되나 파기하기 이전에 파기해야 할 정보를 찾는 일부터가 또 다른 큰 일이라 할 수 있다. 비즈니스 정보가 회사 파일서버에 들어 있기도 하지만, 영업 목적 또는 개발 목적으로 개인이 소지하고 있기도 하기 때문에 개인의 컴퓨터까지 관리해야 하는데 이는 쉬운 일이 아니다.
만약 IT아웃소싱업체와 같이 정보관리, 보관 및 처리자가 외부의 위탁사업자일 경우, 기업은 위탁처리업체가 개인정보를 잘 관리하는지를 정기적으로 점검할 필요가 있다. 따라서 제3의 검증기관이 전산 시스템상에 개인정보가 제대로 파기됐는지를 복원, 분석 방법을 통해 검증할 필요가 있을 것으로 본다. 이런 상황에 가장 도움이 되는 것이 디지털 포렌직이다. 디지털 포렌직을 이용해 기업 내 개인정보의 위치를 파악하고 삭제된 데이터가 복구되지 않는지를 식별하는 업무 지원도 할 수 있을 것이다.