# 중앙 집중식 관리 통한 사내보안 인식 급증

## 내부 보안 강화는 곧 외부 보안 강화로 이어져…

보안의 강화는 개인 정보가 좀더 안전하게 보호될 수 있다는 긍정적인 측면이 있는 반면, 패스워드 입력 횟수가 늘고 승인 절차가 복잡해져 결과적으로 IT 기업의 업무를 가중시키는 부정적인 측면도 있다.

이론적으로 볼 때 신원 관리 시스템을 이용하면 패스워드 입력, 승인 과정을 단순화시켜 네트워크 보안 서비스 담당자의 업무를 덜어 줄 수 있다. 신원 관리 시스템은 사용자들의 다양한 계정, 접속 코드, 패스워드 등을 중앙에서 통제함으로써 개인 정보를 관리하는 것을 말한다.

흔히 사용되는 은행 계좌를 생각해보자. 당좌 예금, 저축 예금, 금융 시장 계좌 등을 비롯한 온라인 증권 계좌에 이르는 다양한 계좌가 있으며, 배우자 명의로 개설된 부부 공동 계좌도 있다.

### 전체 피해의 70%는 내부 공격

사무실의 경우를 한 번 보자. 컴퓨터 한 대에 프린터와 내부 서버 등이 2-3대씩 연결돼 있으며, VPN과 연결된 컴퓨터도 있다. 시스템과의 접속은 사용자들이 개설한 계정을 통해 이뤄진다. 중앙 집중식 신원 관리 시스템은 데이터를 한 곳에 모아 관리를 손쉽게 한다.

다음으로 분산 시스템을 유지, 관리하는 데 있어서의 위험성에 대해 알아보자. 소규모 기업의 IT 인력이 쇄도하는 승인 요청을 모두 처리하려면 매일 야근해야 할 지도 모른다. 지나치게 많은 계정을 사용자들에게 부여했다는 것과 과도한 업무로 인한 IT 담당자들의 실수로 밤새 계정이 갑자기 사라지는 경우가 있다는 것이다.

이같은 실수는 급성장기나 사업 착수기에 있는 업체에서 특히 잘 나타난다. 이같은 시기에 있는 업체들이 엄청난 양의 업무를 맡고 있는 직원을 지원하기 위해 추가 IT 관리자를 고용하는 것에 난색을 표하는 데는 그럴만한 이유가 있다.

요즘처럼 해고당하는 근로자들이 많은 경기 침체기에는 보안 관리가 특히 어렵다. 해고 근로자들이 사용했던 계정에 대한 기록은 남아있지 않은 경우가 많다. IT 부서는 전직 근로자들의 주요 네트워크 로그인 자료를 삭제하지만, 근로자가 회사를 그만 둔지 한참이 지난 후에도 회사쪽에서는 전직 근로자의 e-메일 계정을 제거하지 못할 수도 있다.

예를 들어, 4층에 있는 원격 파일 서버에 접속해 업무봤던 해고 근로자의 특수 계정이나 VPN 사용권은 어떻게 처리할 것인가? 오늘날 대부분의 대기업의 시스템에는 전직 근로자의 잔해가 남아 있는 셈이다. 다행스럽게도 전직 직원들이 회사에 유해한 영향을 미치는 경우는 거의 없다. 하지만 해고 사실을 미리 알게 된 직원이 가계정을 설정한 다음 계정 탐색을 통해 회사 시스템에 접속해 손해를 입힐 수도 있다.

회사에 반감이 있는 직원들이 저지르는 내부 공격으로 인한 피해가 전체 피해의 70%를 차지한다. 이러한 내부 공격으로 인해 회사는 시간과 돈의 손실은 물론 사내 정보 유실 등의 피해를 입을 수 있다. 뿐만 아니라 전직 근로자들이 스팸이나 바이러스를 이용해 e-메일 서버를 마비시킬 수 있으며, 동료 직원들의 계정과 특권을 무력화시킬 수도 있다. 또한 사내 정보를 외부에 팔아 넘길 수도 있다. 내부 공격은 주로 전직 근로자들에 의해 이뤄지며, 회사 측에서는 회사 이미지가 손상되는 것을 우려해 이같은 사실을 외부에 알리지 않는 것이 보통이다.

### 신원 관리 시스템 통한 사전 관리 중요

근로자들의 보안 정보를 중앙 집중식으로 관리하면 IT 부서는 해고 근로자 정보는 확실하게 제거하고 신규 사원들의 계정은 효율적으로 관리할 수 있다. 이론적으로 볼 때, IT 부서에서 좀더 폭 넓은 자유 감사 권한을 행사하고, 기존 계정을 좀더 철저히 관리함으로써 핵심 시스템의 출입 지점의 보안을 확실히 하는 것이 필요하다고 한다.

중앙 집중식 관리는 근로자들에게 자신들의 행동이 모니터링되고 있다는 사실을 알림으로써, 이들이 회사 보안에 피해를 주는 행위를 저지를 가능성을 줄일 수 있다. 또한 내부 보안이 강화되면 외부인에 의한 공격도 줄어드는 것이 일반적이다. 이같은 점을 놓고 볼 때, 가까운 미래에 신원 관리 시스템 이용이 한층 늘어날 것으로 생각된다.