침해사고의 대응과 복구

긴급! 침해사고가 발생했어요

밤 11시. 오랜만에 일찍 사무실을 빠져나와 달콤한 휴식을 취하던 김 대리는 '환상기업'의 시스템과 네트워크를 관리하는 '◎◎' IDC 관계자로부터 침해사고 징후가 발견됐다는 연락을 받았다. 얼마나 큰 사고가 발생했는지, 그 원인은 무엇인지, 피해 규모는 어느 수준인지, 사고현장에서는 무엇을 해야 할 지 등 순식간에 김 대리의 머릿속은 복잡해져 갔다. 침해사고를 직접 경험하게 될 줄은 생각도 못했던 김 대리. 늦은 밤 사고현장으로 급하게 이동했다.

정보보호뉴스 취재팀

침해사고가 발생하기 이전에 예방하는 것이 가장 중요하겠지만, 일단 침해사고가 발생했다면 사고를 수습하고, 그 원인을 찾아 그에 상응하는 조치를 취해야 하는 것이 바람직하다. 사고현장에 도착한 김 대리 역시 사고수습을 위해 그동안 준비해 왔던 단계별 침해사고 대응 전략을 하나씩 수행하기 시작했다.

초기 대응, 신속·정확하게

침해사고 분석과 수습을 위해 김 대리는 먼저 '환상기업'의 시스템을 관리하는 IDC 시스템 관리자와의 면담을 시작으로 침해사고 초기대응을 시작했다. 담당자 면담, 침입탐지 시스템의 로그 분석 등을 통해 현재의 정황을 파악하게 된 김 대리는 침해사고 발생에 대비해 마련해 뒀던 환상기업의 '침해사고 대응전략 매뉴얼'을 꺼내 들었다.

침해사고 대응전략 매뉴얼

침해사고 대응전략 매뉴얼은 침해사고 발생 시 사고분석 및 수습을 신속하고 정확하게 수행하기 위한 문서로, 문서 제작 시에는 각 기업의 보안 정책, 기술, 법, 업무현황, 인원 등 IT 자산과 관련된 요인들을 전체적으로 고려해야 한다. 특히, 대응전략은 수립 자체로 의미를 갖기보다 사내 구성원 및 관련 외부 인력과의 정기적인 훈련에 중점을 둬 사고 발생 시 신속한 대처가 가능하도록 해야 한다. 아래 내용은 대응전략 매뉴얼에 포함되는 초기 대응 시 점검사항이다.

- 피해 PC 혹은 서버가 얼마나 중요하고 위험한 것인가.
- 피해를 당하거나 도난당한 정보가 얼마나 민감한 것인가.
- 사건이 외부에 알려졌는가.
- 직/간접적인 공격자는 누구인가.
- 공격자에 의해 침해된 비안가 접근의 수준은 어느 정도인가.
- 공격자의 수준은 어느 정도인가.
- 시스템과 사용자의 업무중단 시간은 어느 정도인가.
- 경제적 피해는 어느 정도 발생했는가.

대응전략 매뉴얼에는 공격환경과 대응능력을 고려해 다양한 방안이 마련되어야 하며 특히, 아래 표에서 볼 수 있는 것처럼 공격유형 변화에 따라 사고유형을 다양하게 변경시킬 수 있도록 해야 한다.

사고유형	피해 예시	대응 전략	예상 결과
DoS공격	TFN DDoS 공격	Flooding의 효과를 최소화 하기 위해 라우터 재설정	라우터 재설정으로 공격의 효과를 완화
비인가 사용	업무용 컴퓨터 오용	증거물의 포렌식 이미지 확보와 조사 용의자와 면담	범인 식별, 징계를 위한 증거 확보. 해당 직원의 직위나 과거 조직 정책의 위반 등을 고려하여 징계
파괴 행위	웹 사이트 손상	웹 사이트 모니터 온라인 상태로 조사 웹 사이트 복구	웹사이트의 복구 범인 식별을 위해 수사기관이 참여할 수 있음
정보의 도난	신용카드 도난 및 고객 정보 유출	관련된 시스템의 이미지 확보, 도난 신고 법적 대응 준비	상세한 조사 시작, 수사 기관 참여 예상된 피해복구를 위한 민사 소송 얼마간 시스템의 오프라인 유지
컴퓨터 침입	Buffer Overflow 또는 IIS 공격을 통한 원격 접속	공격자의 활동 감시 비인가 접속 봉쇄 시스템의 보안 재설정 및 복구	침입에 사용된 취약점을 식별하고 수정 및 패치 시행 범인의 식별 유무를 결정

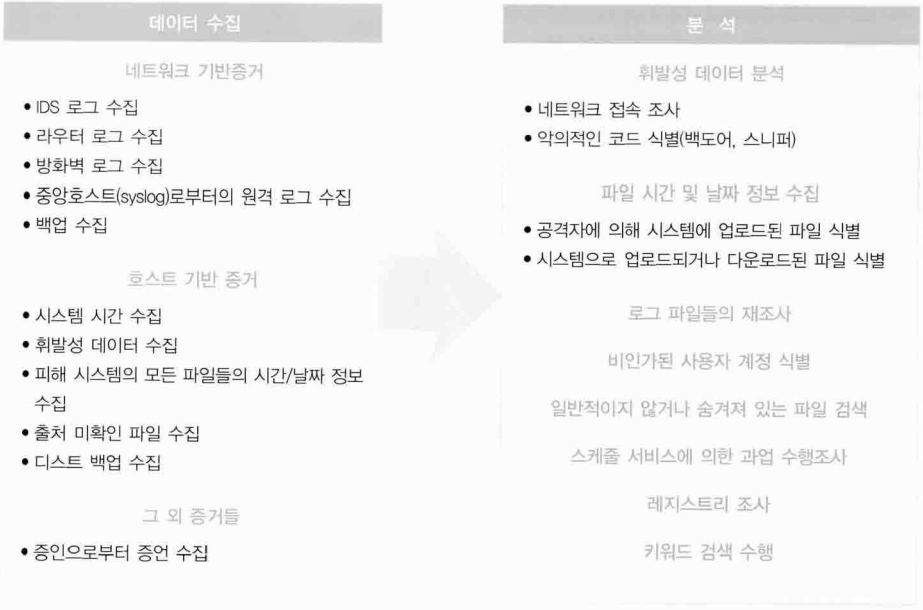
▲ 사고유형에 따른 전략수립의 한 예(출처 : 2007 CERT 구축 및 운영 가이드(CONCERT, KISA 공동발행))

민간기업 침해사고는 국번없이 118

사고분석을 시도한 김 대리는 취약점 패치가 적용되지 않은 서버가 악성코드에 감염돼 침해사고가 발생했다는 결론을 얻게 됐다. 무엇보다 사전에 마련해 둔 대응전략 매뉴얼 덕분에 공격유형과 피해규모 등에 대한 분석을 신속하게 마칠 수 있었다. 다만, 이번 사고를 KISA 인터넷침해사고대응지원센터나 경찰청 사이버테러대응센터와 같은 외부기관에 신고해 도움을 받을 것인지 여부에 대해서는 경영진의 판단에 맡기기로 한 김 대리. 그렇지만 혹시 있을지 모를 외부기관과의 협력을 위해 침해사고에 대한 자료를 수집해 놓기로 결정했다. 경찰이 사건 현장을 철저히 보존해 놓듯 말이다.

사고 조사와 데이터 수집 및 분석

일반적으로 KISA 인터넷침해사고대응지원센터나 경찰청 사이버테러대응센터와 같은 외부기관이 기업의 사고현장을 찾아 사고내용을 분석하기 위해서는 사고 당시의 데이터들이 적절하게 보존돼 있어야 한다. 특히, 공격자에 대한 법적 소송을 고려하게 된다면 증거로 채택될 수 있는 데이터들이 무결성과 적법성을 유지해야 한다는 점을 기억해야 한다. 또 사고조사에 필요한 데이터를 수집할 경우에는 호스트 기반과 네트워크 기반 증거를 구분해 놓아야 한다. 아래 그림은 데이터 수집과 분석 과정의 한 예다.



▲수집된 데이터 분석의 예(출처: 2007 CERT 구축 및 운영 가이드(CONCERT, KISA 공동발행))

데이터 분석에는 로그 파일을 비롯해 시스템 설정 파일, 웹 브라우저 히스토리 파일, 이메일 메시지와 첨부파일, 설치된 애플리케이션 그리고 그림 파일을 포함하게 되며, 소프트웨어 분석, 시간/날짜 스탬프 분석, 키워드 검색 등의 과정을 수행하게 된다.

다음날, 경영진 보고 후 사고재발 방지와 피해예방을 위해 전문가에게 사고조사를 맡기기로 한 '환상기업'은 결국 국내 민간분야의 침해사고 발생 시 전문적으로 도움을 제공하는 KISA 인터넷침해사고대응지원센터로부터 도움을 받기로 했다. 지체없이 118(국번없이)로 전화한 김 대리는 환상기업이 처한 상황을 간단하게 설명한 후 파견된 전문가와 함께 향후 대책과 재발방지를 위한 방안을 수립하기 시작했다.

비록 대규모의 침해사고가 아닌 일부 시스템에 국한된 사고라는 점에서 안도의 한숨을 김 대리. 그러나 이번 사고를 계기로 향후에는 보다 철저한 예방활동이 필요하다는 사실을 다시 한번 깨달았다. **S**