Ⅳ. 해킹의 확산과 기업의 대응 방안

EXECUTIVE SUMMARY

1. 논의 배경

- 최근 들어 야후와 아마존 등 인터넷 사이트에 대한 해킹 공격이 급증하고 있음
- 해커들의 수법은 시스템 파괴, 데이터 도용 등 더욱 고도화되고 위험한 수준으로 발전하고 있음

2. 국내의 해킹 발생 현황

- 국내 해킹 발생 건수는 1997년 64건에서 98년 158건, 99년 572건으로, 이는 미국이나 일본의 증가 속도보다 훨씬 빠른 것임
- 해킹의 가능성이 더욱 높아지고 있는 상황인데 반해, 대다수의 국내 인터넷 사이트들은 해커들의 공격에 무방비로 노출되어 있는 상황임

3. 기업 정보 보안을 위한 대응 방안

- 사전·사후 관리 차원의 대응 방안
  - 해킹이 의심되는 징후를 사전에 파악하는 관리 체제가 구축되어 있어야 함
  - 해킹 사고 발생시, 네트워크 중단, 대체 프로그램의 가동, 복구 작업이 체계적으로 이루어질 수 있도록 대응 방안이 마련되어야 함
  - 이외에도 해킹 피해에 대한 보상을 받을 수 있도록 미리 보험에 가입하는 것도 고려해야 함
- 정보 보안 장치의 활용
  - 침입차단시스템(방화벽) : 내부 자원에 대한 외부 접근을 통제하는 장치
  - 침입탐지시스템 : 내부 정보 흐름을 파악하여 방화벽을 통하지 않는 위협을 탐지
  - 가상사설망(VPN; Virtual Private Network) : 인터넷과 같은 공중망을 통해 사설망과 같은 안전한 정보 소통 채널을 구축하는 솔루션
  - 바이러스 백신 : 해킹 이외에 바이러스를 통한 시스템 파괴를 막는 소프트웨어

4. 시사점

- 해킹은 e-비즈니스를 수행하는 기업에 유·무형의 기업 가치 하락을 초래함
- 온라인 기업으로 변신을 도모하는 기업들은 e-비즈니스화가 기회와 위험을 동시에 가져올 수 있는 양날의 칼임을 명심하고 이에 대한 고려가 먼저 이루어져야 함

1. 논의 배경

- 최근 들어 인터넷 사이트에 대한 해킹 공격이 급증하고 있음
  - 지난 2월초 야후와 CNN, 아마존 등 세계적으로 유명한 인터넷 업체들이 해커들의 공격을 받아 서비스가 몇 시간 동안 중단되는 사건이 발생함
  - 이외에도 인터넷 주식 거래 중계 사이트인 이-트레이드와 정보통신 관련 뉴스 전문 제공업체인 ZD-net 등 다수의 전자 상거래 기업들도 비슷한 형태의 해킹을 당하는 등 인터넷 사이트에 대한 해킹이 빈발하고 있음
  - 국내에서도 비슷한 시기에 대검 중수부 컴퓨터 범죄 수사대에 해커가 침입하였으며, 점차 그 사례가 증가하고 있는 실정임

- 해커들의 수법은 더욱 고도화되고 위험한 수준으로 발전하고 있음
  - 단순히 시스템에 침범하여 자신의 실력을 과시하던 이전의 해커들과는 달리 최근에는 시스템 파괴, 데이터 도용, 정보 입수와 같은 나쁜 목적을 가진 해커들이 증가하고 있는 상황임
  - 해킹을 통해 경쟁사의 시스템을 파괴하거나 고객 정보를 훔쳐내고 범죄 행위를 위해 해킹을 활용하는 경우도 발생함
  - 해커들의 수법은 더욱 다양화되고 고도화되는데 반해, 인터넷 업체들이 해커들의 다양한 수법에 일일이 대응 조치를 마련하기에는 어려움이 너무 많은 상황임
  - 보안 관리에 만전을 기하고 있던 세계 최고의 인터넷 사이트인 야후나 아마존이 해커들에게 손쉽게 공격을 당했다는 것은 이를 말해 줌

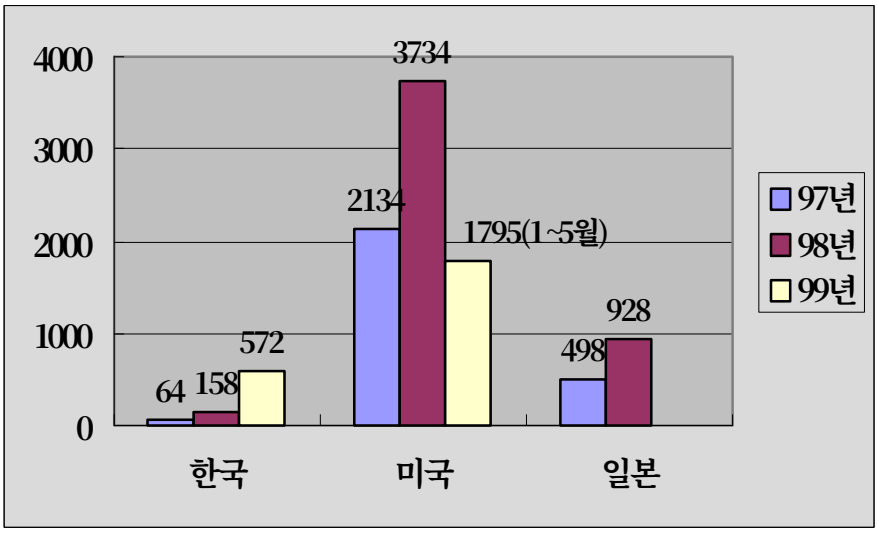
- 해킹은 인터넷 비즈니스에 심각한 악영향을 미침
  - 인터넷 사이트에 대한 해킹 공격이 증가함에 따라 인터넷 비즈니스의 활성화를 저해하는 커다란 요인으로 등장함
  - 인터넷 사이트가 해킹에 노출되면 해당 인터넷 사이트의 서비스 마비, 고객 정보의 유출, 기업 이미지 저하, 고객 이탈로 이어지는 최악의 사태가 발생할 수도 있음
  - 미국 2위의 온라인 증권업체인 이-트레이드의 경우 시스템의 다운으로 투자자들이 정상적인 주식 거래를 할 수 없게 되어 피해에 대한 소송 사태가 발생할 가능성이 높음

- 해킹에 대한 시급한 기술적 대책과 관리적 준비 노력이 필요한 시점임
  - 해킹에 대비한 철저한 보안 여부는 인터넷 비즈니스를 수행하는 기업의 생사를 가름하는 중요한 기준임
  - 해킹을 당한 사이트들은 고객들이 불신하여 거래를 중단하게 되어 비즈니스에 심각한 타격을 입게 됨
  - 예를 들어, 금융 거래가 잦은 전자상거래 업체나 사이버 증권회사, 인터넷 뱅킹 업체들의 경우 해킹을 당한다는 것은 곧 고객의 직접적인 피해로 이어짐
  - 따라서 해킹 공격을 당하지 않도록 시스템적으로 철저히 대비하고 해킹을 당했을 경우를 대비하여 관리적 대처 방안을 준비해야 할 것임

2. 국내의 해킹 발생 현황

- 국내에서도 인터넷의 확산과 더불어 해킹 사례가 매년 증가하고 있음
  - 지난해 국내에서 신고된 해킹 건수는 모두 572건으로 1998년의 158건에 비해 3배 이상 증가함
  - 그러나, 대부분의 해킹 사고가 공개되지 않은 것에 비추어 볼 때, 실제 발생 건수는 밝혀진 것보다 훨씬 많을 것으로 추정됨
  - 올해는 1천건 이상 발생할 것으로 예상되며, 이는 미국이나 일본의 증가 속도보다 훨씬 빠른 것임

<그림> 주요국의 해킹 사고 발생 현황



자료 : 한국정보보호센터

- 현재 약 300~400명의 전문 해커가 국내에서 활동 중인 것으로 조사됨
  · 이외에도 약 3,000명의 아마추어 해커가 활동하고 있는 것으로 추정되고 있으며, 그 숫자는 더욱 증가하고 있는 추세임
  · 해커들이 주로 공격 대상으로 삼는 사이트는 기업의 홈페이지나 대학교의 전산 시스템이며, 연구소나 정부 기관의 홈페이지도 침범함

- 국내 기업들의 인터넷 사이트들은 해킹에 거의 무방비로 노출되어 있음
  · 해킹의 가능성이 더욱 높아지고 있는 상황인데 반해, 대다수의 국내 기업의 홈페이지나 정부 기관 또는 전자상거래 사이트들은 해커들의 공격에 무방비 상태인 것으로 나타남
  · 더욱 심각한 문제는 국내 인터넷 사이트들의 허술한 보안 관리 시스템을 악용하여 외국의 전문 해커들이 한국을 해킹을 위한 경유지로 삼고 있는 상황임

3. 기업 정보 보안을 위한 대응 방안

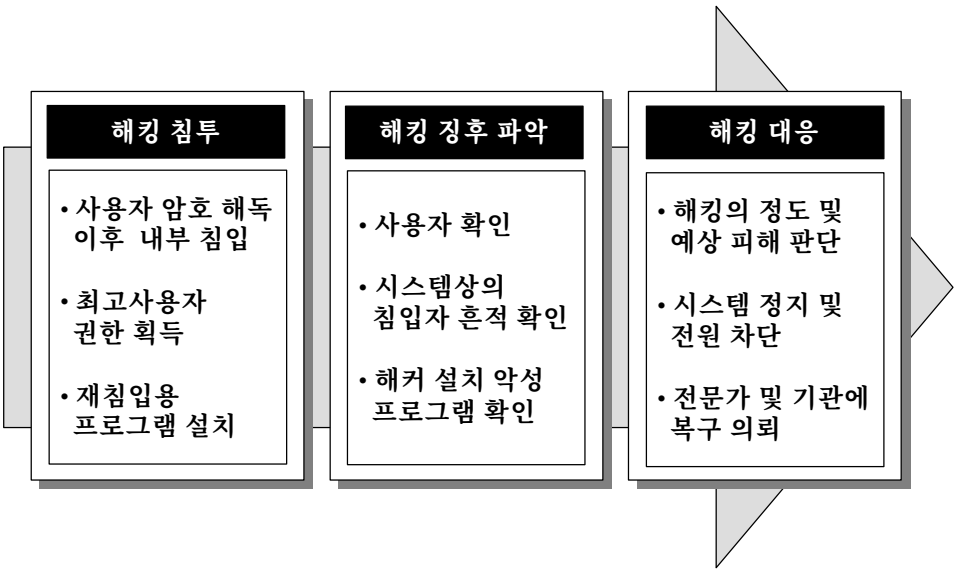
○ 사전 · 사후 관리 차원의 대응 방안

- 해킹이 의심되는 징후를 사전에 파악하는 관리 체제가 이루어져야 함
  · 기업의 전산 담당자 및 관련자는 평소 발생 가능한 해킹의 위험 및 보안 문제에 대한 체계적인 관리 체제를 구축하고 있어야 함
  · 사이트 이용자 중 평소에 접속하지 않던 이용자의 움직임이 활발하거나, 접속 실패 기록이 많은 이용자가 있을 경우 해킹을 의심해야 함
  · 또한 사이트가 비정상적으로 오랜 시간 가동되지 않거나 중앙처리장치가 특정인에게 과도하게 점유되고 있는 경우도 의심해야 함

- 해킹 사고시 신속한 대응 훈련이 체계화되어 있어야 함
  · 해킹 상황 발생시 전문가가 있다면 인터넷 시스템 상에서 해커가 활동하지 못하도록 차단하거나 네트워크를 중단해야 하며, 전문가가 없는 경우에는 시스템이 네트워크상에서 분리될 수 있도록 네트워크 케이블을 뽑아야 함
  · 시스템에 치명적 손상을 입힐 수 있는 상황이라고 판단될 경우 해당 프로그램을 중단해야 하며, 최악의 경우 전원을 차단하는 방안도 있음

- 인터넷상의 피해로 인한 보상을 받을 수 있는 보험에 가입하는 것도 만약의 사태에 대한 준비 방안 중 하나임
  - · 기존 인터넷 기업이 가입하고 있는 보험은 주로 고객 신상 정보의 유출에 따른 피해 보상을 대비한 제3자 배상 책임형 상품이 대부분임
  - · 이와 함께 해킹이나 시스템 다운 등으로 인한 정보 유출 및 피해를 보장할 수 있는 보험 가입을 통해 손실을 줄이도록 해야 함

<그림> 해킹 및 대응 절차의 주요 흐름



○ 정보 보안 장치의 활용

- 침입차단시스템(방화벽)
  - · 방화벽은 가장 기본적인 보안 장치로 내부 자원에 대한 외부 접근을 통제하는 장치로 내부 인트라넷과 인터넷망을 분리하는 지점에 설치됨
  - · 방화벽은 내부 정보 유출 방지 및 컨텐츠 보호, 다이얼인 모뎀 제어,[1] 부서간 정보 접근 제어 등의 역할을 담당함

- 침입탐지시스템
  - · 방화벽은 외부 침입에 대해서는 방어 효과가 크지만, 내부인에 의한 위협이

1) 내부 직원이 외부에서 전자우편 확인 등의 필요에 의해 내부 시스템에 접근하는 경우 모뎀에 의한 다이얼인을 시도하게 됨. 이 경우 방화벽은 특정 서비스만을 개방할 뿐 기타 내부 자원에 대한 접근을 막는 역할을 함

나 방화벽을 통하지 않는 인터넷 접속 방식에 대해서는 방어가 어려움
· 침입탐지시스템은 이러한 방화벽의 단점을 보완하는 것으로 내부 정보 흐름을 파악하여 위협의 형태를 감지해 내는 역할을 수행함

- 가상사설망(VPN : Virtual Private Network)
· VPN은 인터넷과 같은 공중망을 통해 사설망과 같은 안전한 정보 소통 채널을 구축하는 솔루션을 의미함
· VPN은 인터넷이라는 공중망을 통해 이루어지므로 저렴한 비용, 관리의 편리성, 용이한 확장성 등의 장점을 지니고 있음

- 바이러스 백신
· 외부 해커의 침입이나 내부인의 정보 유출 이외에도 바이러스에 의한 시스템 파괴는 정보 보안에 커다란 영향을 미치는 사건임
· 일반적으로 전체 파일 시스템에 대한 정기 스캐닝을 통해 점검하는 방식의 바이러스 백신이 많이 활용됨

4. 시사점

- 해킹은 e-비즈니스를 수행하는 기업에 유·무형의 기업 가치 하락을 초래함
· 단기적으로는 아마존, 타임워너, e-베이 등의 사례에서 보듯이 해킹 당한 기업의 주가가 하락함
· 보다 중요한 것은 오랜 시간 구축한 기업 신뢰와 이미지가 저하되어 고객의 외면을 당하게 됨

- e-비즈니스의 긍정적 측면과 더불어 기업에 미치는 부정적 측면의 위험에 대한 고려가 동시에 이루어져야 함
· 정보화 사회의 진전은 새로운 시장에 대한 무한한 가능성을 제공함
· 반면, 해킹으로 인하여 수십년간 쌓아온 신뢰가 한순간에 무너질 수도 있다는 측면이 있음
· 온라인 기업으로 변신을 도모하는 기업들은 e-비즈니스화가 기회와 위협을 동시에 가진 양날의 칼임을 명심해야 함

(윤성한 : ysh@hri.co.kr ☎ 3669-4058)
(김태홍 : thkim@hri.co.kr ☎ 3669-4057)