망분리 환경에서 취약성 및 침해사고 분석

최예원 · 이동휘*

동신대학교

Analysis of vulnerabilities and Breaches in a network separation environment

Ye-won Choe · DongHwi Lee*

Dongshin University

E-mail : dpdnjs3328@naver.com / dhclub@dsu.ac.kr

요 약

인터넷의 발전과 이용자의 증가에 비례하여 이를 이용한 사이버 침해사고 발생 비율이 높아지고 있다. 이에 대한 대책으로 사용자들이 접근할 수 있는 시스템과 주요정보가 담긴 시스템을 분리하여 서로 접근하지 못하도록 하는 망분리 방식이 등장하고 있다. 그러나 인터넷망을 사용해야 하는 업무의 경우는 사이버 공격에 그대로 노출되며 망간 자료전송 방식/시스템과 관리·운영적인 부분에서 많은 허점이 발생하여 폐쇄망의 감염이 발생하고 있다. 본 연구에서는 이러한 망분리 환경에서 침해사고 발생 유형과 사례에 대한 조사를 통해, 망 연계시스템의 안전성을 높이고자 한다

ABSTRACT

In proportion to the development of the Internet and the increase in users, the rate of cyber-incident using it is increasing. As a countermeasure, there is a network separation method that separates the system accessible to users and the system containing key information from each other. However, in the case of tasks that require the use of the Internet network, it is exposed to cyber attacks, and there are many loopholes in the method of data transmission between networks and the management and operation of the system, resulting in infection of the closed network. In this paper, we aim to enhance the safety of the networking system by investigating the types and cases of infringement accidents in these network separation environments.

키워드

망분리, 망연계시스템, 침해사고. 사례분석

Ⅰ. 서 론

사이버 위협에 따른 피해가 발생함에 따라 `사이버 침해사고를 막기 위한 대책으로는 무엇이 있을까?`라는 연구 과제 중 하나로 `망분리`가 등장하였다. 정부에서는 2012년 8월 정보통신망법의 개정으로 100만 명 이상 이용자의 개인정보를 보유했거나 정보통신서비스 매출이 100억 원 이상인 정보통신서비스 사업자의 경우 `망분리`를 의무적으로 도입할 것을 법으로 의무 했다. 그러나 망분리를 적용했음에도 악성 코드 감염 피해가 발생한 사례가 있다. 2014년 한국수력원자력의 상업용 네트워크 침투를 통한 데이터 유출, 2016년 국방부의 내부망 망연계 솔루션의 취약점을 이용한 해킹 등이 있다. 이처럼 망분리 방식이라고 무조건 안전한 것은 아니다.

본 논문에서는 지난 5년 동안 발생한 대표적인 망연계 시스템의 침해사고 사례를 분석해보고 그에 대한 대응 방안을 제안한다. 이를 통해 망연계 시스템에 대한 관리체계를 분명히 하고, 사용자 주의 외에도 정기적인 모니터링 및 점검 등의 방법으로 보안을 강화한 망연계시스템이 등장할 것으

* corresponding author

로 기대한다.

II. 망분리

2.1. 물리적 망분리

망분리에는 크게 물리적 망분리와 논리적 망분리 2가지가 있다. 물리적 망분리는 인터넷망과 업무망을 물리적으로 분리하며, 업무망을 폐쇄망으로 운영하여 외부의 접속이 불가능하게 하는 방식이다[1].

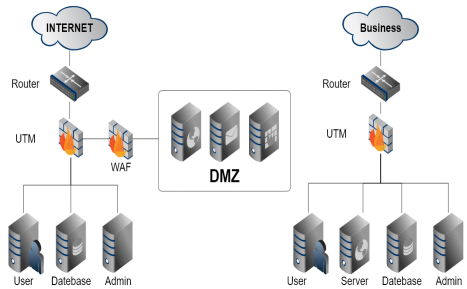

그림 1. 물리적 망분리

2.2. 논리적 망분리 (서버 기반 가상화)

논리적 망분리 중 서버 기반 가상화(SBC, Server Based Computing)는 사용자가 PC에서 수행했던 응용프로그램의 실행, 자료저장 등의 모든 작업을 터미널을 통해 서버에서 실행되는 방식으로, 업무망은 전용 통신 프로그램을 사용하여 업무 자료의 대외 유출을 차단한다[1].

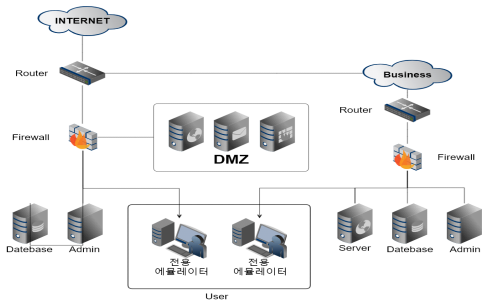

그림 2. 서버 기반 가상화(PC 기반, SBC)

2.3. 논리적 망분리 (PC 기반 가상화)

PC기반 가상화(CBC, Client Based Computing)는 업무용 PC에 가상화로 인터넷의 사용 가능 영역을 생성한 후, 가상화 영역에서만 인터넷 접속을 허용하여 네트워크를 논리적으로 분리하는 방식이다. 인터넷 접속은 가상사설망(VPN)을 통해 논리적이고 개별적인 통신 채널을 이용한다[1].

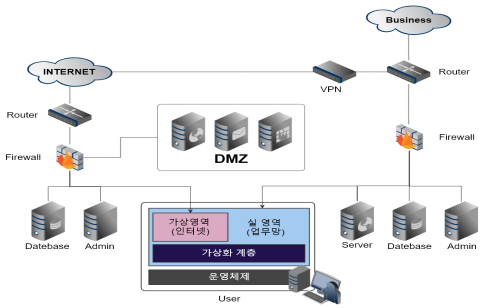

그림 3. PC 기반 가상화 (CBC)

III. 국내사고

3.1. 2016년 국방부 망연계 솔루션의 취약점 해킹

16.08.04~09.22 사이에 해커조직이 국방통합데이터센터(DIDC)가 관리하는 망분리 환경에서 망사이의 접점을 통해 국내부망에 침투하였다. 그 후, 파일 배포 기능이 있는 국방부의 백신 중계 서버에 악성코드를 유포하고, 이에 감염된 PC에서 약 170GB 이상에 달하는 군사자료가 탈취당하는 사고가 발생하였다.

기존의 통제대책으로는 NAC를 통한 사용자 인증절차를 구성하여 특정 사용자만 네트워크에 접속할 수 있게 하여, 보안위협을 탐지하는 것이 아닌 탐지된 보안위협을 신속히 조치하는 방안이었다. 그러나 추가로 내/외부의 트래픽 분석과 모니터링, 공격 발생 시에도 은밀하게 작동하는 활동 · 정보 유출 등을 자동으로 탐지, 지속적인 업데이트와 내부 네트워크 활동에 대해 학습능력을 갖춘 인공지능 장비 등을 사용하는 등의 정보보호체계를 도입하였다. [2]

3.2. 호스팅 업체 'A사' 랜섬웨어 감염사건

해커는 웹서버에 랜섬웨어 등의 악성코드를 업로드하고, 업체 관리자 계정 정보를 탈취하여 해당 업체 사무실의 관리용 PC에 백도어를 설치했다. 백도어를 이용해 IDC의 호스팅 웹서버 153대에 접속해 랜섬웨어를 감염시키고, IDC의 백업서버 데이터를 삭제하였다. 그리고 특정 시점에 웹서버 153대에 있던 랜섬웨어가 동작하도록 명령을 하여 153대 서버의 호스팅 고객 데이터를 잃고 복구할 수 없게 된 사고가 발생하였다.

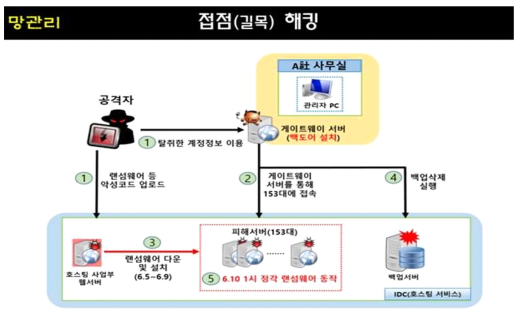

그림 4. 접점(길목) 해킹[3]

사고가 발생한 이유는 인터넷망과 DB 폐쇄망의 연결 접점이 해킹되어 폐쇄망에 접근할 수 있는 계정을 탈취해 가상사설망(VPN) 서버로 터미널에 접속하였고고 이후 내부 업무용 서버와 웹서버 같은 대외 서비스 인프라를 장악하였기 때문이다.

이에 대한 대응 방안으로 접점에 대한 취약점을 최소화 하고 게이트웨이 구간 무결성 확인, 접근할수 있는 관리네워크를 완전 분리하고, 주기적으로 망간 접점이 생기는 문제를 점검 하여야 한다.

3.2. 원격 SW 회사 '공급망' 인프라 위협

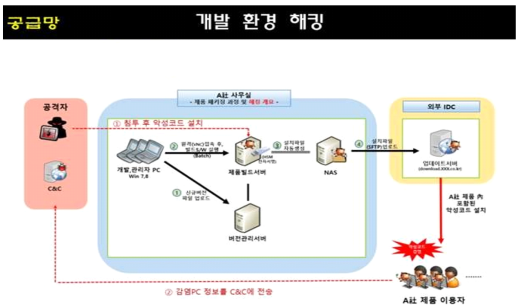

그림 5. 개발 환경 해킹[3]

해커는 B사 사무실의 제품 빌드 서버에 침투하여 악성코드를 설치하였다. B사는 이를 모른 채 SW 제품 신규 버전 파일을 버전 관리 서버에 업로드 후, 제품 빌드 서버에 원격 접속하여 빌드 작업을 실행했다. 감염된 서버는 악성코드가 포함된 설치파일을 자동 생성했고 이 파일은 외부 IDC 업데이트 서버로 업로드되었다. 이후 악성코드는 이를 설치한 B사 제품 이용자 PC를 감염시키고 정보를 탈취해 해커의 서버로 전송했다.

사고 발생 이유는 해커가 직접 해킹이 어려워지자 우회경로를 찾으면서 개발망과 인터넷망에 모두 접속 가능한 개발자 PC를 장악하였기 때문이다. 또 기업 고객 지원망에 접근할 수 있는 고객지원 PC를 해킹해 데이터 백업 서버를 거쳐 IDC의 고객사 서버에 악성 코드를 유포할 수 있었다.

이에 대한 대응 방안으로 보안아키텍처 구축을 통한 환경 개선, 해당 기관에 적용 될수 있는 유지보수 및 개발 보안 매뉴얼을 구성하여, 이를 통한 수시 관리 및 점검, 관리 인력에 대한 보안 교육과 유사한 사례를 수집하여 분석하고 그에 대한 취약점을 제거하는 것이다.

Ⅳ. 결 론

망분리 네트워크에서 발생하는 침해사고들의 원인은 크게 4가지로 분류할 수 있다. 첫째, 업무망과 인터넷망 간의 데이터 이동을 위해 불가피하게 발생하는 접점이 공격의 경로로 악용되는 형태이다. 둘째, 망간 자료전송에 대한 예외 처리에서 발생하는 취약점이다. 셋째, 호스트 컴퓨터에서 다수의 OS를 동시에 실행 및 관리하는 하이퍼바이저에 대한 취약점도 존재한다. 마지막으로, 망분리 환경을 무력화시키는 예측 불가능한 보안위협에도 주의를 기울여야 한다.

즉, 망분리 기술의 문제가 아닌 관리의 문제이다. 가상화 소프트웨어의 호환성 문제나 망연계 구간에 대한 문제는 존재 할 수 밖에 없고, 보안 허점이 발생하고 관리도 어렵다. 대응방안으로는 망분리 접점을 수시로 점검하고, 트래픽을 분석하고 실시간으로 망간 취약점을 스캔 할수 있는 기술이 필요하고, 망연계 상황에서 관리자 구역을 별도로 지정하고 접근 권한에 관한 정책과 계정관리에 대한 정책을 수립하며, 해당 기관에 적용된는 점검 매뉴얼을 구축해서, 지속적인 체크리스트 점검만이 안전을 담보 할 수 있다

References

[1] S. R. Lee, H. Berry, O. Temam, and M. Lipasti, "A Study on the Improvement of Security Monitoring in the Separate Network Environment" *Korea Knowledge Information Technology Society*, Vol. 9, No. 6, pp. 805-819, Dec. 2012.

[2] Shim Bo-hoon, Kang Hye-kyung, Lee Yong-sung, Lee Joon-hyung, "A Study on the Countermeasures for the Elimination of Cyber Vulnerability in Korea", Defense and Technology, No. 462, p. 122-129, August. 2017.

[3] ZDNet Korea. Top 3 Hacking Points analyzed as Real Cases [Internet]. Available : https://zdnet.co.kr/view/?no=20180528103548

[4] IGLOOSECURITY. The Importance of Network Separation Management in the Interpark Personal Information Leakage [Internet]. Available : http://www.igloosec.co.kr/BLOG?searchItem=&searchWord=&bbsCateId=17&gotoPage=1