YTN + 박형일 · YTN 디지털 기획팀 차장

디지털 뉴스룸 시스템(3)

– 방송 네트워크의 보호기술 –

개요

디지털 뉴스룸 시스템은 다양한 하드웨어와 소프트웨어를 네트워크를 통해 서로 조합되어 작동한다. 따라서, 하드웨어, 소프트웨어, 네트워크의 성능뿐만 아니라, 연계성, 호환성이 매우 중요하다.

특히, 네트워크를 보호함으로써 전체 시스템에서 필요로 하는 최상의 성능을 보장해주는 것이 필요하다. 방송 네트워크의 보호는 망 분리가 원칙이지만, 일반 네트워크와 연결돼야 정보의 사용이 원활하기 때문에 완전히 격리된 네트워크를 가질 수 없다. 따라서, 일반 사용자의 접근을 통제하고 사용을 제한하며, 정보의 누출과 시스템 침입을 막기 위해 많은 정책과 기술이 필요하다.

네트워크와 시스템의 보안에서 최우선돼야 할 것은 정책과 전사적인 지원과 협조이다. 하지만, 본고에서는 정책 부분은 가능한 배제했으며, Network의 기술적인 공격 형태와 일반적인 보호기술에 대해 나열한다. 이를 조합하고 적용하는 것은 각자의 몫이며, 여기에도 기술되지 않은 다양한 공격과 방어방법들이 있음을 미리 알려둔다.

네트워크 공격 형태

인터넷 웜

웜은 바이러스와 달리 자신을 스스로 복제하고, 감염시키는 악성코드이며, 이메일 웜, 윈도우 웜, 인터넷 웜으로 나눌 수 있다.

이메일 웜은 메일 서버에 등록된 사용자 또는 클라이언트에 등록된 주소로 웜이 내포된 메일을 파일 형태로 송신하여 감염시킨다. 이메일 웜은 이메일을 여는 순간, 감염되는 경우도 있고, 첨부파일을 열 때 감염되는 경우도 있다.

윈도우 웜은 운영체계가 윈도우 계열에서 파일공유 관련 네트워크를 실행시킬 때 감염되는 형태이다.

인터넷 웜은 바이러스와는 다른 형태의 성질을 가지며, 네트워크를 통해 전파되고, 블래스터 웜, 슬래머 웜, 코드레드 웜, 베이글 BC 웜 등은 아주 많이 알려진 웜의 형태이다.

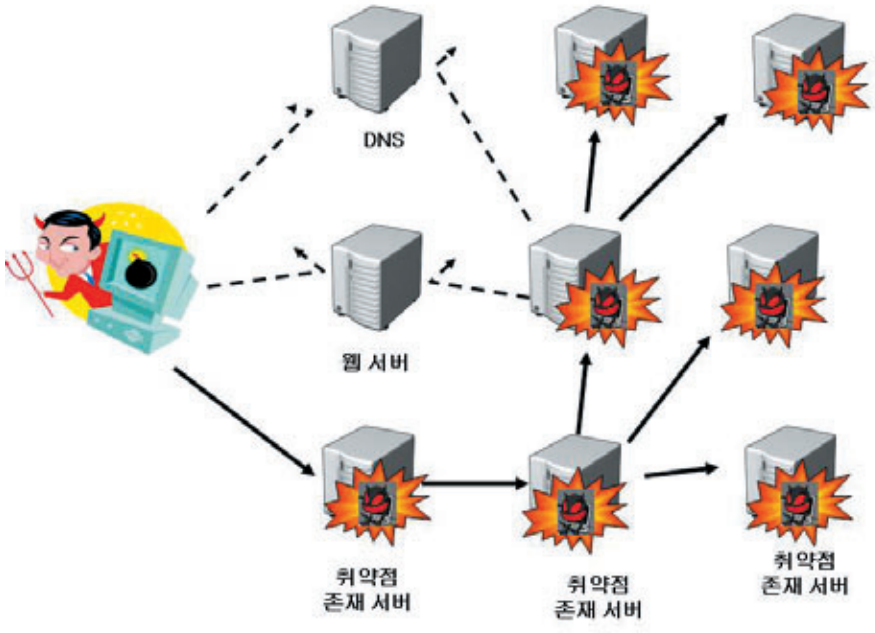
(1) 블래스터 웜은 전 세계적 대란을 야기했으며, 2003년 8월 처음 발견됐고, 윈도우 NT계열의 RPC DCOM 취약점을 이용하여 전파된다. 감염된 시스템은 트래픽이 증가하며, 재부팅되거나 에러 메시지가 뜨고, 포트를 통해 다른 컴퓨터로 웜을 전송한다.

(2) 슬래머 웜은 1434UDP 포트를 이용한 SQL 서버가 설치된 서버를 대상으로 침입하여 감염시키는 웜으로 2002년 7월 24일 발견된 SQL 서버의 버퍼 오버프로우 취약점을 이용하여 확산됐다. 이는 메모리에 상주하는 악성코드이며, 작동하게 되면 랜덤 패킷을 보내 감염시키기 때문에 많은 보안장비를 무력화시킨다.

(3) 코드레드 웜은 마이크로소프트의 인덱스 서버 취약점을 이용하여 공격한 것으로 2001년 8월 1일부터 확산됐다. 감염된 컴퓨터는 다른 사이트에 대한 감염을 시도하기 때문에 네트워크의 과부하가 발생한다.

(4) 새로운 변종인 베이글 BC 웜은 2004년 10월 가짜 이메일을 통해 빠른 속도로 확산됐고, 전 세계의 게이트웨이에서 시스템 과부하를 일으킬 우려가 있는 인터넷 웜이다.

인터넷 웜은 시스템 및 응용 프로그램의 취약점을 이용하여 최초의 감염 PC가 발생되면, 해당 PC에서 네트워크 스캐닝 기법을 통해 다른 네트워크와 시스템으로 전파를 시도하게 되는데 제로데이 공격을 이용하는 경우에는 급속히 확산된다.



[인터넷 웜 공격]

봇넷(Botnet)

봇 마스터는 다른 사람의 시스템이나 PC에 원격제어가 가능한 악성코드를 유포한다. 이때 악성코드에 감염되어 원격으로 제어되는 시스템이나 PC를 봇(Bot) 또는 좀비 PC라고 한다. 봇 마스터는 봇넷 C&C(Command & Control) 서버를 사용하여 다수의 봇들을 효율적으로 관리한다.

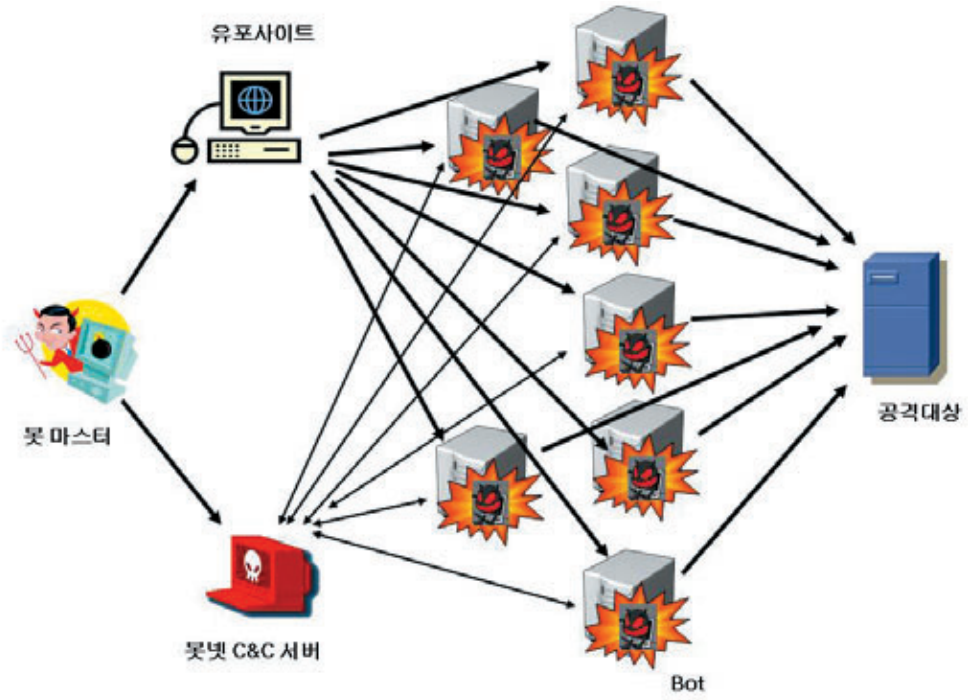
봇은 여러 가지 악성코드기술을 혼합한 것으로 다른 공격과 혼동하기가 쉽다. 웜/바이러스, 백도어, 스파이웨어, 루트킷 등 다양한 악성코드들의 특성을 복합적으로 지니고 있다.

봇넷을 통한 공격 형태는 스팸발송, 피싱사이트, DDoS 공격, 정보 불법 수집, 애드웨어, 스파이웨어 설치, 키로깅, 트래픽 스니핑 등 다양하다.

프로토콜에 의한 봇넷의 종류를 보면, IRC 봇넷, HTTP 봇넷, P2P 봇넷 등이 있으며, C&C 서버에 따라서는 집중형 봇넷, 분산형 봇넷, 하이브리드형 봇넷 등으로 분류할 수 있다.

[봇넷의 분류]

구분	IRC 봇넷	HTTP 봇넷	P2P 봇넷
특징	· IRC 채널로 통신 · 실시간 양방향성 · 탐지 가능성 높음	· 웹 서버는 항상 개방 · 탐지 가능성이 적음	· 어느 봇이든 C&C 서버가 될 수 있음 · 봇넷의 성능에 의존적이며 전송지연이 크다
종류	· 집중형 봇넷 · 하이브리드 봇넷	· 집중형 봇넷 · 하이브리드 봇넷	· 분산형 봇넷 · 하이브리드 봇넷
프로토콜	IRC	HTTP	P2P



[봇넷의 구성]

집중형 봇넷은 봇마스터가 봇넷을 구성할 때 하나의 C&C 서버를 두어 모든 봇을 제어 및 관리하는 봇넷이다. 봇넷의 C&C 서버는 IRC나 HTTP 같은 네트워크 서비스를 수행하고, 새로운 컴퓨터가 봇에 의해 감염되면, 봇넷 C&C 서버로 연결을 개시하여 봇넷에 가입하게 된다.

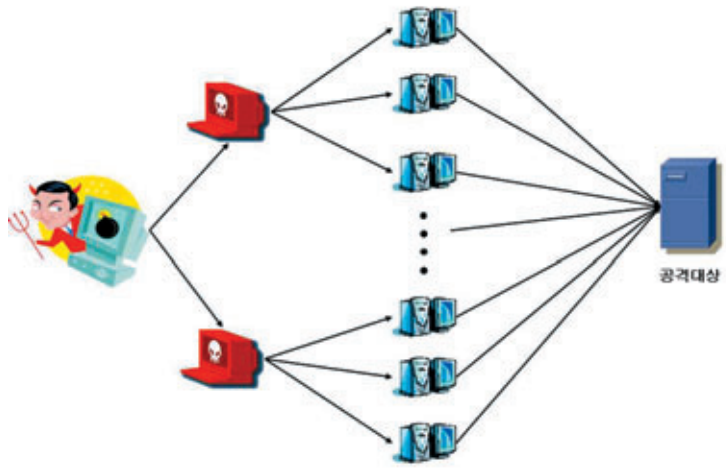
분산형 봇넷은 집중형 봇넷과는 달리, 봇넷을 구성하는 모든 봇이 봇넷 C&C 서버가 될 수 있는 형태의 봇넷이다. 최근에는 집중형 봇넷에서 P2P 방식의 봇넷으로 진화하고 있다. 분산형 봇넷은 P2P 기반 봇넷 C&C 서버를 모두 발견하고 없애야하므로 집중형 봇넷에 비해 제거가 훨씬 어렵다. 그러나, P2P 통신에 의존하기 때문에 비교적 소규모의 제어 · 관리만이 가능하다.

하이브리드 봇넷은 집중형과 분산형 봇넷을 적절히 혼합한 형태로 두 개 이상의 프로토콜을 사용하거나, 다수의 봇넷 C&C 서버사에 존재하는 상태에서 봇넷 C&C 서버끼리 서로 P2P 방식으로 연결되어 좀비 PC를 제어 · 관리하는데 사용하는 봇넷이다.

하이브리드 봇넷의 대표적인 예는 2008년 Damballa에서 보고된 Mayday가 있다. Mayday는 HTTP 프로토콜뿐만 아니라 P2P 프로토콜을 사용하여 봇과 봇넷 C&C 서버와 통신할 수 있다. Mayday는 전략적인 봇넷 C&C 서버와 통신을 위해 타이머를 이용하여, 정해진 시간 내에 감염된 봇이 봇넷 C&C 서버로 연결하지 않을 경우 봇의 연결을 차단하는 능력도 갖추었다.

서비스 거부공격(Denial of Service)

서비스 거부공격은 공격 목표 시스템의 정상적인 서비스를 방해할 목적으로 대량의 트래픽을 발생시켜 목표 대상 네트워크의 대역폭이나 시스템의 자원을 급격히 소비시키는 공격 방법이다. 이러한 DoS는 보통 다수의 컴퓨터를 동원하여 효과를 극대화 시키는데 이러한 공격을 분산 서비스 거부공격(DDoS : Distributed Denial of Service)이라고 한다.



[DDoS의 형태]

서비스 거부공격은 악성코드에 감염된 PC들이 대량의 트래픽을 발생시켜, 공격 목표로 전송함으로써 서비스 마비를 유발한다. 하지만, 각 좀비 PC는 소량의 트래픽만 발생하기 때문에 사용자가 느끼기 힘든 경우도 많다. 공격 방법으로는 SYN 플러딩, UDP 플러딩, ICMP 플러딩 등과 같이 네트워크 프로토콜의 취약점을 이용한다. 그러나, 서비스 거부공격도 정상적인 트래픽과 공격 트래픽을 구분하는데 구별이 힘든 경우도 많다. 최근 출시되는 DDoS 관련 장비는 다양한 방법을 통해 트래픽을 구분하지만, 공격 트래픽을 구분하는데 부족한 점이 많다.

최근에는 백신의 업데이트를 방해하고, 공격이 끝난 후 하드디스크를 파괴하는 등 복합적인 공격을 하는 경우도 많다. 드리고, 분산 반사 서비스 거부공격(Distributed Reflect DoS, DRDoS)은 DDoS가 한 단계 더 진화한 형태의 공격 방식도 존재한다.

제로-데이(Zero-day) 공격

제로-데이 공격은 시스템 및 응용 소프트웨어의 보안에 대한 취약점이 노출됐을 때, 취약점의 존재가 널리 공표되어 보안패치가 발표되기 이전에 공격자가 해당 취약점을 대상으로 네트워크 공격을 한다. 이 공격은 알려지지 않았거나 숨겨져 있는 패치가 필요한 시스템이나 소프트웨어를 악용하는 위협이다. 제로-데이 공격은 자동화된 강력한 Tool의 무료배포, 불법 소프트웨어의 사용 등으로 소프트웨어의 취약성이 증가하면서 더욱 증가하고 있다.

논리폭탄

논리폭탄은 날짜, 시간, 명령 등의 특정한 이벤트에 의해 공격 대상 시스템이나 파티션 정보를 삭제하여 시스템을 파괴하는 악성코드이다. 즉, 공격 대상 컴퓨터 파일을 교란시키도록 프로그램된 일종의 시한폭탄 같은 컴퓨터 바이러스이다. 정해진 날짜와 시간에 정보를 빼낼 수도 있으며, 다양한 명령으로 직접 제어할 수 있거나 기존의 정보를 변경할 수도 있다.

피싱(Phishing)

피싱은 Private와 Fishing의 합성어로 인터넷을 통해 사용자를 현혹시키고, 인지적인 차원에서 사용자의 접근을 자연스럽게 유도하여 개인 정보나 중요한 정보를 불법적으로 수집하는 행위이다. 유명기관의 홈페이지를 가장하여 중요 정보를 입력하도록 유도하기도 한다.

백도어 공격

백도어는 한 번 해킹한 시스템을 다시 해킹하지 않고 손쉽게 루트권한을 얻기 위해 시스템에 심어 놓은 프로그램이다. 본래 백도어는 시스템의 보안이 제거된 비밀통로로써 서비스 기술자나 유지보수 프로그래머들의 재접근 편의를 위해 시스템 설계자가 고의적으로 만들어 놓은 통로이다.
그러나, 공격자들은 비정상적인 방법으로 시스템에 접근하기 위해 백도어 기술들을 개발했고, 악의적인 기능으로 사용한다. 트로이 목마가 대표적인 백도어 프로그램이다.
백도어 프로그램은 자기복제 기능이 없는 독립적인 프로그램이며, 원격으로 컴퓨터의 모든 작동의 제어가 가능하다. 초기의 유닉스 버전에서는 특정 패스워드로 접근하고, 재컴파일 된 암호코드를 삽입하여 컴퓨터 계정으로 접근이 가능하도록 하는 치명적인 보안결함도 있었다.

네트워크 보호기술

네트워크 보호기술은 다양한 정책과 방법들이 있으나, 대표적인 기술적 방법(방화벽, 침입 탐지 시스템, 침입 방지 시스템, VPN, UTM)을 소개하고자 한다.

방화벽(Firewall)

방화벽은 인터넷과 같은 외부 네트워크와 그와 연결된 내부 네트워크 사이에 위치하여 외부네트워크의 불법적 침입으로부터 내부 네트워크를 안전하게 보호하는 정책 및 이를 지원하는 하드웨어나 소프트웨어이다. 외부 공격자로부터 내부 네트워크를 방어하며, 두 네트워크 간의 트래픽을 제어한다.
방화벽은 내부 네트워크와 외부 인터넷 사이에서 불법적인 접근을 방지하고, 내부 네트워크의 정보를 보호하려는 목적을 가지고 있다. 또한, 접근제어, 사용자 인증, 로깅, 암호화 등의 기능을 제공하여 외부로부터의 공격을 차단한다.

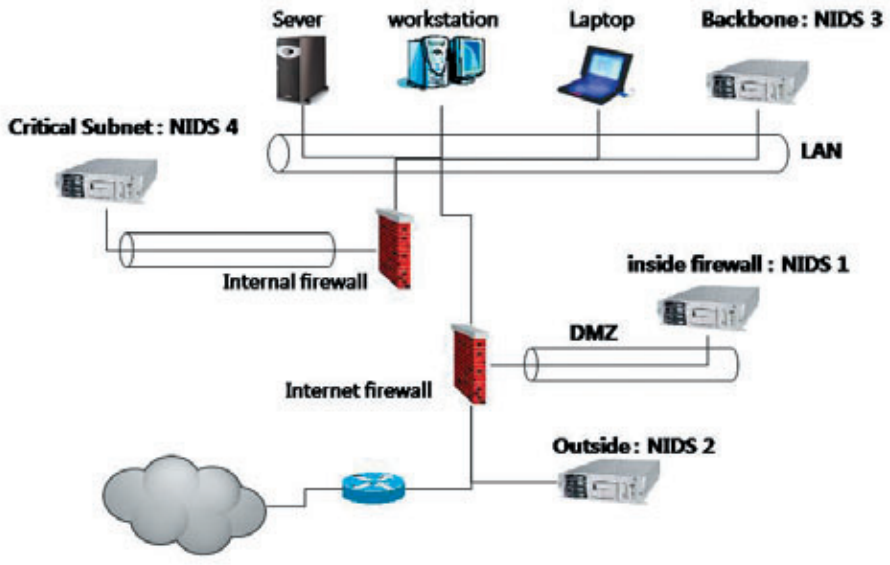
(1) 접근제어는 허용된 자원이나 서비스만을 내부 네트워크로 접근이 가능하게 하는 기능이다.
(2) 사용자 인증은 정당한 사용자만이 내부 네트워크의 자원을 사용할 수 있도록 사용자를 확인하는 기능이다.
(3) 로깅은 시간적 추이에 따른 접근상태를 기록하는 기능이다.
(4) 암호화는 전송되어 지는 중요한 트래픽을 보호하는 기능이다.

방화벽은 방화벽을 경유하지 않는 공격에 대해서는 방어하지 못하며, 내부 사용자에 의한 침입위협은 방어하지 못한다. 적절한 보안정책에 의해 주로 Layer 3, 4 레벨 수준에서 트래픽을 제어한다. 최근에는 Application 레벨(L7)의 취약한 보안을 위한 Web 방화벽, VoIP 방화벽이 출시되기도 했다.

침입 탐지 시스템(IDS : Intrusion Detection System)

침입 탐지 시스템은 실시간으로 네트워크의 탐지 영역에서 인가되지 않은 행위와 비정상적인 행동을 탐지하고, 탐지된 불법행위를 경보하는 보안기술이다. 컴퓨터 시스템 자원의 비밀성, 무결성, 가용성을 저해하는 비정상적인 사용과 오남용 등을 탐지하여 자동으로 대응하거나 관리자에게 경고 메시지를 보내주는 역할을 한다. 침입의 패턴 데이터베이스와 전문가 시스템을 사용하여 네트워크나 시스템의 사용을 실시간으로 모니터링 한다.

내외부 네트워크의 구분과 Firewall 및 IDS의 배치



[네트워크에 위치하는 Firewall 및 IDS의 배치형태]

[IDS의 위치에 따른 특징]

구분	장점	단점
Internet Firewall 내부에 위치한 NIDS	· 외부 Network에서 들어온 공격을 확인 · F/W 구성정책에서 생긴 에러 감지를 피할 수 있음 · DMZ 시스템을 모니터하는 것이 목적 · 기관 내부에서 외부로의 공격을 감지 가능	· F/W에서 filtering되어 공격을 모니터링 못함 · 외부 network과 근접하여 강력하게 보호되지 못함
Internet Firewall 외부에 위치한 NIDS	· F/W에서 가려지는 모든 공격을 감지 가능 · 이 구성은 F/W의 효과적인 방안을 분석 가능	· 수집되는 data가 극도로 복잡하고 양이 많음
major Backbone에 위치한 NIDS	· 많은 양의 트래픽을 모니터하고 Spotting Attack의 가능성 탐지 · critical Subnet에 영향을 줄 수 있는 DOS의 차단 가능성을 높임	· 수집 data의 양이 많고, 정당하고 합법적인 data를 캡처하는 Risk
critical Subnet에 위치한 NIDS	· Network asset의 제한 된 자원만을 감시	· IDS와 관련 data가 network 부하를 증가시킬 수 있음

침입 방지 시스템(IPS : Intrusion Prevention System)

침입 방지 시스템은 공격을 탐지만 하는 침입 탐지 시스템의 한계점을 보완하는 보안기술로써, 네트워크의 트래픽을 분석하여 공격 시그니처를 찾아내고, 정의한 정책에 따라 실시간으로 자동 대처한다.

그러나, 실시간으로 네트워크의 데이터를 감시하고 공격을 탐지 및 방어해야하는 영역이 너무 넓기에 패킷필터링에 한계가 있고, 오탐지 가능성이 존재한다. 특히, SSL 통신에 취약하고, 시그니처 방식을 취함으로써 지속적인 업데이트가 필요하다.

가상 사설 망(VPN : Virtual Private Network)

가상 사설 망은 인터넷이나 네트워크 서비스 사업자가 제공하는 공중망을 자사의 전용 네트워크처럼 사용할 수 있는 네트워크를 말한다.

가상 사설 망은 저렴한 비용으로 안전한 네트워크를 구현하는 것이 목적이기 때문에 사용자 및 데이터 인증기술, 암호화기술, 데이터 무결성 및 신뢰성 보장기술들을 지원하며, 키 관리기술, 터널링기술, 가상 사설 망 관리기술 등을 제공한다. 구현방식에 따라 2계층의 PPTP, L2F, L2TP, 3계층의 IPSec, 4/5계층의 SSL VPN으로 나눌 수 있다.

통합 위협 관리(UTM : Unified Threat Management)

UTM은 방화벽, 침입 탐지 시스템, 침입 방어 시스템, 가상 사설 망, 안티 바이러스, 안티 스팸 등의 각종 보안 솔루션을 하나로 모으고, 각종 보안 시스템 및 주요 시스템 장비를 연동하여, 효율적으로 운용하는 중앙집중식 관리 체계이다.

그러나, 모든 네트워크 보호기술을 통합한다고 해도 취약점은 존재하며, UTM은 통합 보안 기능을 모두 적용했을 경우, 네트워크의 대량 트래픽을 감당하지 못하고 성능저하를 일으키는 경우가 있고, 장애가 발생할 경우 전체적으로 연계된다.

결론

NPS 등 네트워크 방송 제작 시스템에 관련된 보안의 위협요소와 보안 시스템을 알아보았다.

가장 안전한 방송을 위해서는 네트워크를 사용하지 않고, 단독으로 장비를 운용하는 것이다. 하지만, 방송과 통신, 컴퓨터의 융합이 이루어지면서 이러한 단독방식의 장비나 제작시스템은 줄어들고 있고, 시스템 내부구조는 점점 복잡해지고 있고, 눈에 보이지 않는 소프트웨어에 의해 운행이 되며, 네트워크로 장비 간 통신을 한다.

디지털 뉴스룸 시스템은 약 100여대 이상의 서버, 워크스테이션, PC가 Network로 통신하며, 수백 또는 그 이상의 사용자에게 서비스를 한다. 디지털 영상파일의 합법적 사용을 보호하고, 불법적인 사용을 막기 위해서는 보안 시스템과 감시 시스템이 뒷받침돼야 한다. 하지만, 보안 시스템은 많은 비용을 들여도 침입당하지 않을 수 있으며, 철옹성을 쌓는다 해도 잘못된 관리에 의해 허물어질 수 있다.

방화벽의 보안장비와 그를 지원하는 다양한 기술들은 절대 만능이 아니며, 보안을 위협하는 요소도 수백 수천가지에 달하고, 그것을 관리하는 장비와 사람은 기업별로 소수이다. 운용 방법과 정책에 따라 네트워크가 완전히 노출되기도 하고, 적절한 방어가 가능하기도하다.

방송 네트워크의 보안 시스템은 관련된 기술을 이해하고, 적절한 조합을 회사에 맞게 사용하는 것이다.