방송사 보안, 필수적이고 전략적인 관리

글. 김지혜 SBS 미디어IT팀 차장대우

디지털 미디어 환경의 급격한 변화 속에 있는 방송사는 전통적인 콘텐츠 송출 방식을 넘어 디지털 전환(DX, Digital Transformation)에 직면하고 있습니다. 이러한 기술 발전과 변화는 방송사에 더 많은 기회를 제공하는 반면, 다양한 종류의 사이버 보안 위협을 동반하고 있어 정보보안 기술의 역할과 중요성이 커지고 있는 추세입니다. 방송 보안은 이제 단순한 '정보 보호'를 넘어서 지속적인 신뢰성 확보, 법적 규제 준수, 비즈니스 연속성 보장, 콘텐츠 자산 및 개인정보보호를 위한 전략적 차원의 문제로 접근하고 있습니다.

방송사의 보안 목표

정보보안의 3대 요소는 ① 기밀성(Confidentiality), ② 무결성(Integrity), ③ 가용성(Availability)입니다. 일반적인 기업과 마찬가지로 이 세 가지 필수 보안 요소를 기준으로 하여 정보보안 계획을 수립하고 있으며, 방송사에서도 업무 특성을 고려하여 우선순위를 설정하고, 세 가지 요소가 균형을 이루도록 보안을 설정하고 있습니다.

기밀성 비인가자로부터 민감한 정보를 보호하고 비정상적 시스템 접근을 차단

방송사는 아직 방송되지 않은 뉴스 콘텐츠, 방송 프로그램의 제작 정보, 사업 계약 내용 등 다양한 종류의 정보 자산을 가지고 있습니다. 권한이 없는 사용자가 이러한 중요 정보에 무단 접근하거나, 권한 있는 사용자 계정을 악용하여 정보를 탈취한 후 외부로 유출하지 못하도록 철저히 보호하고 있습니다. 내부 데이터가 외부의 공격자나 무단 접근자에 의해 유출되면 방송사의 신뢰성에 심각한 영향을 미치게 됩니다. 이에 방송시스템 접근제어, 침입 차단, 데이터/네트워크 트래픽 암호화, 정기적인 보안 점검 등을 통해 기밀성을 유지하고 있습니다.

무결성 콘텐츠나 데이터가 제3자에 의해 변조되거나 조작되지 않도록 보안

방송사는 콘텐츠의 무결성을 보장하기 위해 데이터 변조 방지 기술을 활용하고, 변조되거나 조작된 콘텐츠가 악의적으로 유통되는 일이 없도록 모니터링 시스템을 강화하고 있습니다. 방송 콘텐츠의 정확성과 신뢰성을 유지하는 역할을 합니다.

가용성 방송사에서 최우선으로 고려하고 있는 중요 요소 '무중단'

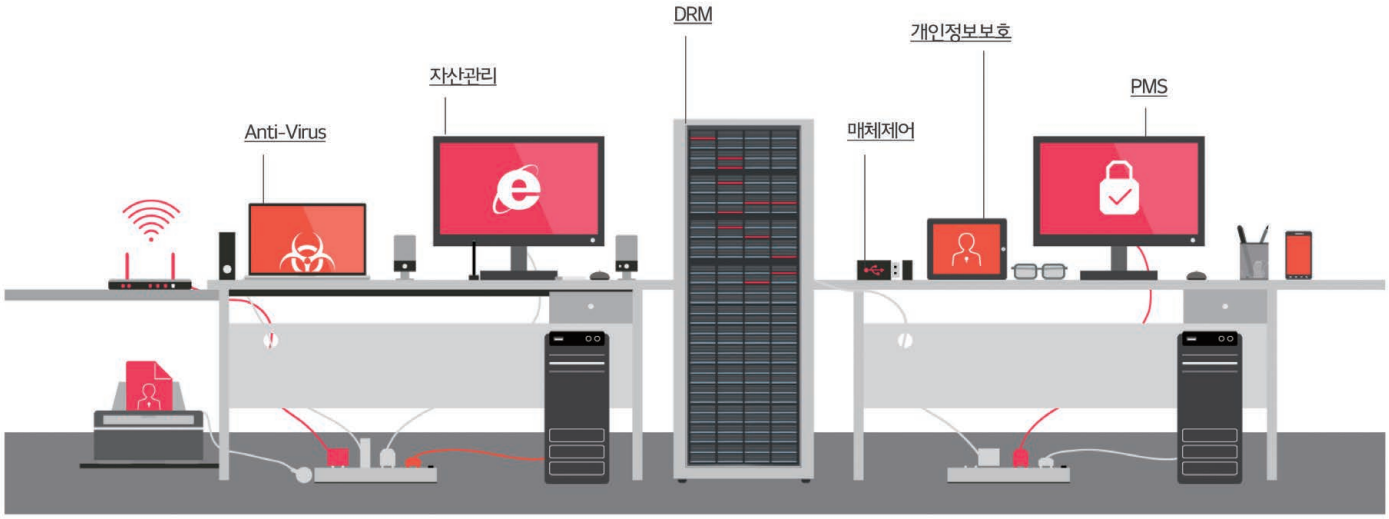
방송사 보안의 가장 중요한 목표는 '무중단 방송송출'을 보장하는 것입니다. 실시간으로 방송 송출과 콘텐츠 배포를 진행하는 특수성을 갖고 있기 때문에, 시스템 오류, 시스템 다운타임, 보안침해사고가 발생할 경우 즉각적으로 방송 서비스에 영향을 주게 되어 단기적으로는 재정적 손실을 줄 뿐 아니라 신뢰도와 기업 이미지, 브랜드 가치에도 중대한 영향을 미치게 됩니다. 따라서 시스템 다운타임을 최소화해야 하며, 장애가 발생했을 때 빠르게 복구할 수 있는 체계를 마련해야 합니다. 방송사는 가용성을 보장하기 위해 시스템을 이중화 구성하고, 재해 복구(Disaster Recovery, DR) 계획을 수립하여 예상치 못한 사고 발생 시 빠르게 복구할 수 있도록 준비합니다. 또한, 실시간 모니터링 시스템을 통해 잠재적인 장애를 사전 감지하고 대응할 수 있는 체계를 갖추고 있습니다.

다중 계층 방어 전략

외부 공격을 100% 막을 수 있는 보안 장비는 없습니다. 하나의 작은 보안 Hole만으로도 보안이 무너질 수도 있으므로 다중 계층 방어 전략을 채택하여 보안을 강화하고 있습니다.

방송사의 네트워크는 **방화벽**(Firewall), **침입차단시스템**(IPS) 등을 통해 외부 위협을 실시간으로 차단하고, 네트워크 트래픽을 세밀하게 모니터링합니다. 강력한 사용자 인증 방식을 도입하여 임의 접근 시도를 무력화하고, 승인되지 않은 접근을 사전에 차단하는 **최소 권한 원칙**(Least Privilege)을 적용하여 사용자 및 시스템 권한을 최대한 제한함으로써 불필요한 위험을 최소화하고 있습니다.
또한 네트워크를 용도에 따라 세분화하여 분리하고 **독립된 네트워크 구성**을 통해 핵심 시스템을 보호하고 있습니다. 송출 시스템, 제작 시스템, 뉴스 시스템 등은 별도의 네트워크로 분리하여, 하나의 시스템에서 침해가 발생하더라도 다른 시스템으로의 확산을 차단합니다. 각 시스템에 대해 세밀한 접근 제어를 통해 중요 데이터와 시스템을 보호할 수 있습니다.

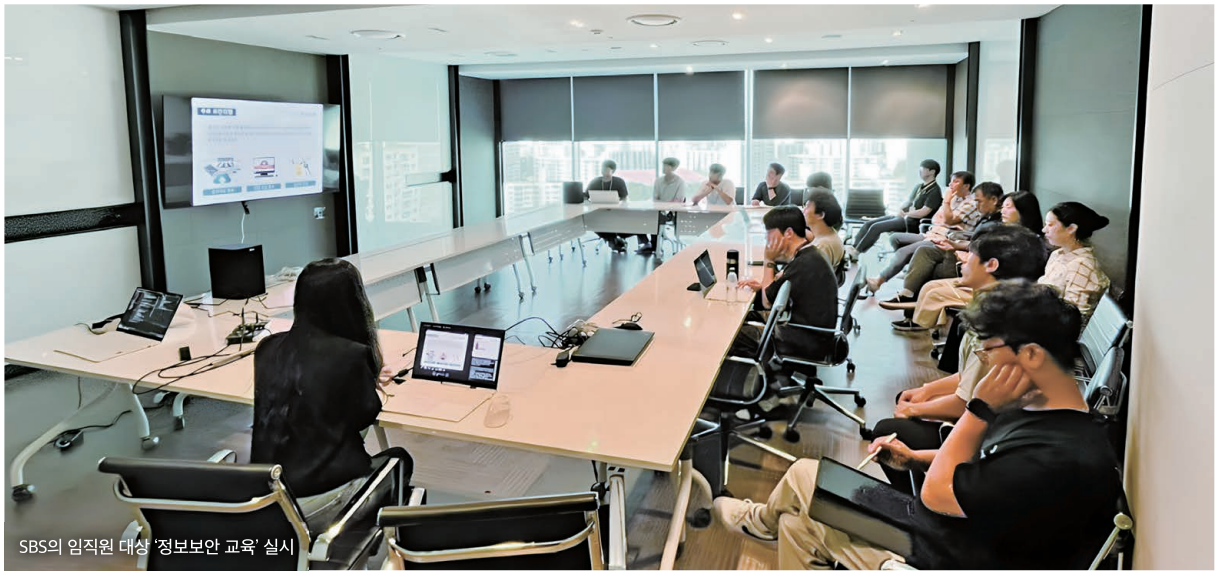
마지막으로 **지속적인 모니터링과 실시간 대응 체계**가 필수적입니다. 방송사는 다양한 위협 시나리오를 기반으로 한 실시간 모니터링 시스템을 통해 공격 이상 징후를 빠르게 탐지하고, 사고 대응 프로세스를 통해 침해 발생 시 신속하게 대응할 수 있도록 합니다. 그리고 모의해킹, 취약점 관리와 정기적인 보안 점검을 통해 기존의 보안 체계를 지속해서 강화하며, 새로운 보안 위협에 대비합니다.



보안 인식 교육 및 직원 훈련

보안전문가들은 정보보안의 가장 약한 연결고리(Weakest Link)를 '사람'으로 보고 있습니다. 악의적이든 그렇지 않든 실제 보안 사고의 상당 부분은 내부 직원의 실수나 부주의에서 발생합니다. 이에 따라 정기적인 임직원 대상 **보안 인식 교육**(Security Awareness Training)은 중요한 정보보안활동 중 하나입니다. 보안 교육은 직원들이 사회공학적 공격(Phishing, Spear Phishing 등)에 대비하고, 악성 코드 및 랜섬웨어 공격에 대비하는 데 도움이 됩니다.

정기적인 보안 훈련(Security Drills) **및 비상대응훈련**을 통해 실제 네트워크나 시스템이 중단된 상황을 시뮬레이션하고, 직원들이 긴급 상황에서 신속하게 대응할 수 있도록 훈련하는 것이 중요합니다. 이 과정에서 직원들은 보안 위협을 실시간으로 인지하고, 사고 발생 시 적절한 대응 방법을 빠르게 선택하여 조치할 수 있도록 훈련하게 됩니다.



SBS의 임직원 대상 '정보보안 교육' 실시

사이버 공격 및 최신 보안 위협

사이버 공격의 배후에는 특정 국가 또는 조직적인 사회적 집단이 존재할 수 있으며, 이들은 정치적 목적, 경제적 이익, 또는 사회적 혼란을 야기시키려는 의도를 가지고 공격을 감행하는 경우가 많습니다. 또한 해킹 기술력을 과시하기 위해 고의로 영향력 있는 주요 인프라나 기관을 목표로 삼으면서 공격으로 인한 피해가 광범위한 영향을 미칠 수 있는 곳으로 설정됩니다. 방송사가 그 대표적인 예가 될 수 있습니다. 따라서 방송사는 최신 사이버 공격 트렌드에 항상 주의를 기울여야 합니다.

랜섬웨어, 서비스 거부 공격(DDoS), 사회공학적 공격(Phishing, Spear Phishing) 등은 방송사의 시스템을 위협하는 주요 공격 방식입니다. 이러한 공격들은 방송송출의 중단, 데이터 유출, 콘텐츠의 변조 등을 초래할 수 있기 때문에, 방송사는 이에 대비한 침해 탐지 및 대응 체계를 강화해야 합니다. 최신의 보안 인텔리전스를 통해 실시간 보안 위협을 파악하고, 악성 코드 및 비정상적인 네트워크 활동을 탐지할 수 있는 보안 시나리오를 이용하여 보안 로그를 모니터링해야 합니다.

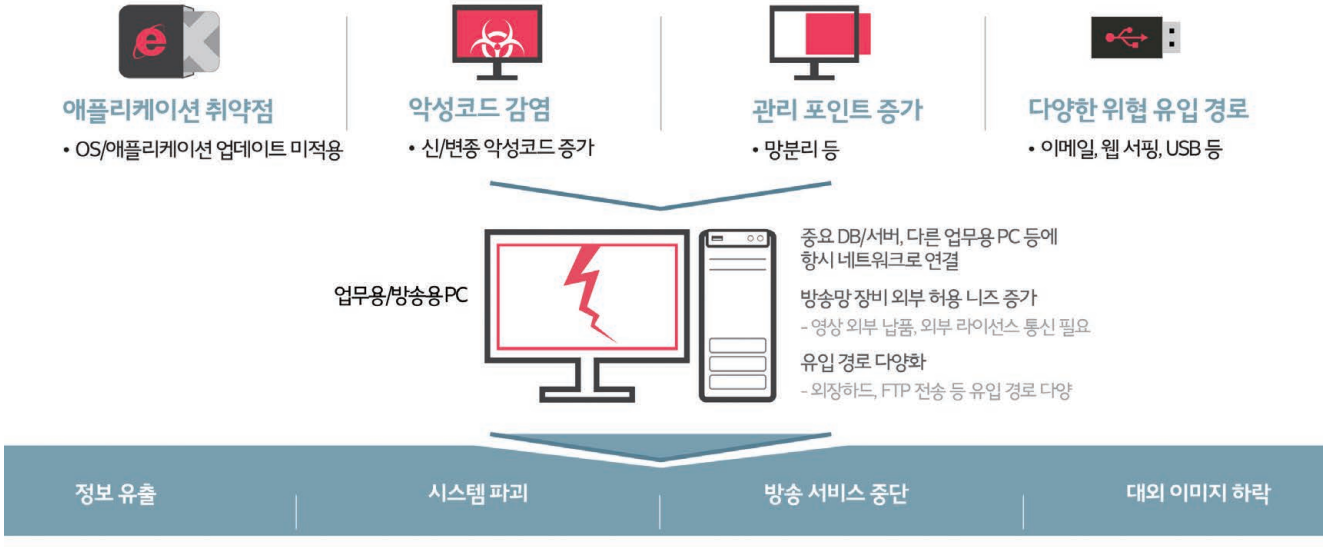
악성코드의 진화

악성코드의 진화는 사이버 보안의 가장 큰 도전 과제 중 하나로, 과거의 단순한 바이러스나 웜에서부터 점차 고도화된 형태로 발전하고 있습니다. 초기의 악성코드는 감염된 파일을 통해 확산하였으며 비교적 쉽게 감지되고 처리될 수 있는 방식으로 활동하여 백신 소프트웨어를 통한 대응이 가능했으나, 최근에는 훨씬 더 복잡하고 은밀한 방식으로 진화하고 있습니다.

특히 **지능형 지속 위협(APT, Advanced Persistent Threat) 공격**은 고도화된 악성코드의 대표적인 사례로 꼽힙니다. 2013년 3월 20일, 대한민국의 주요 방송사들과 금융기관들이 동시에 대규모 사이버 공격을 받은 사건은 단순히 내부 정보 탈취에 그친 것이 아니라, 시스템을 마비시켜 사회적 혼란을 초래하며, 국가 차원에서의 사이버 보안 강화 필요성을 촉구하는 중요한 계기가 되었습니다.
기존의 패턴 기반 탐지 방식으로는 APT 공격을 효과적으로 방어하기 어려운 상황이 되자, 보안 시장에서는 이를 보완하기 위해 APT 대응 솔루션을 내놓았습니다. 이 솔루션은 Sandbox 형태의 가상 환경에서 의심 파일을 실행하고, 악성코드의 주요 활동(예: 레지스트리 변경, 스케줄 등록 등)을 모니터링하여 탐지하는 방식입니다. 그러나 최근 들어 이러한 솔루션을 우회하는 악성코드들이 급증하고 있으며, 이들은 일정 기간 잠잠하게 숨어 있다가 특정 조건이 충족되었을 때만 활동을 시작하는 방식으로 APT 대응 솔루션의 탐지를 피하고 있습니다.

또한, 최근 악성코드는 **파일리스(fileless) 형태로 변형**되어 나타나는 경우가 많습니다. 이러한 악성코드는 파일로 존재하지 않고, 시스템 메모리 내에서 직접 실행되거나 합법적인 소프트웨어 및 프로세스를 악용하여 실행됩니다. 이로 인해 기존의 파일 기반 보안 솔루션으로는 탐지가 더욱 어려워졌습니다.
랜섬웨어는 단순히 사용자 PC의 파일을 암호화하는 것을 뛰어넘어, **시스템을 장악하여 타깃을 시스템으로 정해 범위를 넓히고 피해를 극대화하는 방식**으로 전략을 바꾸고 있습니다. 이런 랜섬웨어 역시 기업의 방어 시스템을 우회하고 공격을 은밀하게 진행하여 공격 대상이 알아채지 못하도록 활동합니다.

최근에는 **악성코드를 제작하여 배포까지 해주는 서비스가 등장**하면서, 악의적인 공격 시도가 더욱 확산하고 있습니다. 이는 공격자들이 전문 지식이 부족한 상태에서도 고도화된 악성코드를 쉽게 배포할 수 있게 만들어, 전반적인 사이버 공격의 수준을 높이고 있습니다.
악성코드의 이러한 진화는 보안 솔루션의 한계를 시험하고 있으며, 기업과 개인이 사이버 공격에 효과적으로 대응하기 위해서는 최신 보안 기술을 지속적으로 검토하고 도입하여 새로운 형태의 악성코드에 대한 대응 능력을 강화하고 있습니다. 고도화된 보안 기술과 체계적인 관리 시스템을 통해 방송사의 단말들을 보호할 수 있습니다.



이메일 보안

이메일을 통한 공격은 오래된 방식이지만 여전히 가장 널리 사용되는 사이버 공격 수단입니다. 해커는 상대적으로 적은 노력으로 많은 사용자에게 직접적인 공격을 시도할 수 있기 때문에 이메일은 매우 효과적인 공격 방법으로 여겨집니다. 공격자는 종종 수신자의 관심을 끌 수 있는 제목을 사용하여 이메일을 열게 유도하고, 본문에 악성 링크를 삽입하거나 악성코드가 포함된 첨부 파일을 통해 시스템을 감염시킵니다.

이메일 공격은 단순한 스팸메일을 넘어 악성코드 감염, 시스템 장악, 정보 탈취 등으로 확장될 수 있습니다. 특히 방송사와 같은 주요 기관을 대상으로 한 공격이 증가하고 있으며, 임직원들은 경각심을 가지고 이메일 열람에 주의를 기울여야 합니다.

최근 많은 조직들이 **이메일 모의훈련**을 적극적으로 시행하고 있습니다. 이메일 모의훈련은 임직원들에게 실제 피싱 이메일에서 사용하는 형태의 이메일을 의도적으로 발송하여, 수신자가 해당 이메일을 열람했는지, 이메일 본문 내 링크를 클릭했거나 첨부파일을 다운로드하여 열었는지, 또한 링크를 통해 연결된 페이지에서 개인정보나 계정 정보를 의심 없이 입력했는지를 점검합니다. 훈련에서 취약한 모습을 보인 임직원들에 대해서는 악성코드 감염 또는 정보 유출 위험을 최소화하기 위한 맞춤형 교육 자료를 제공하여 추가적인 보안 교육을 실시합니다.

이메일 모의훈련의 가장 중요한 효과는 **조직 내 보안 문화의 개선**입니다. 훈련을 통해 정보 보안에 대한 임직원들의 인식이 크게 향상되었으며, 의심스러운 이메일을 즉시 열지 않고 정보보안 담당자에게 신고하는 비율이 증가하였습니다. 그 결과, 피싱 이메일로 인한 피해가 현저히 감소하고, 전반적인 보안 대응 능력이 강화되었습니다.

마치며

보안 위험도는 다음과 같은 공식으로 정의할 수 있습니다:

$$* \text{ Risk} = \text{Asset} \times \text{Vulnerability} \times \text{Threat}$$

이 공식에 따르면, **보안 위험도는 자산의 가치, 시스템 내 취약점의 존재, 그리고 외부 위협의 수준에 의해 결정**됩니다. 자산의 가치가 클수록, 시스템이나 데이터에 대한 위협이 커질수록, 또한 취약점이 많을수록 보안 위험도는 비례하여 증가하게 됩니다.

특히 방송사와 같은 특수한 환경에서는 높은 자산 가치를 지닌 시스템과 빈번한 외부 공격 시도가 동시에 존재하는 상황이기 때문에, 이러한 위협 요소들을 직접적으로 통제하기 어려운 경우가 많습니다. 이에 따라 방송사는 취약점 관리와 보안 강화를 통해 위협을 최소화하고, 시스템의 안정성을 확보하는 데 주력해야 합니다.
방송사의 보안은 브랜드 신뢰성을 유지하고, 시청자/청취자 및 광고주와의 신뢰 관계를 지속해서 강화하기 위한 전략적 필수 요소입니다. 방송사는 최신 보안 기술과 규제 요건을 적극적으로 반영하며, 무중단 방송송출을 보장하기 위해 전방위적인 보안 관리 체계를 구축해야 합니다. 높은 보안 수준을 적용할 경우 사용자 편의성이 저하될 수 있으므로, 보안 정책의 실행에는 임직원들의 충분한 이해와 협조가 필수적입니다. 또한 정보보안에 대한 기업문화의 형성도 중요한 요소로 작용합니다.

방송사 보안의 성공적인 구현은 실시간 콘텐츠 송출의 안정성을 보장하고, 궁극적으로 방송사의 지속 가능한 성장을 촉진하는 중요한 역할을 하게 될 것입니다.

Broadcast Security