글. 이선응 차장 / 김영준 과장 아이크래프트㈜ SNT본부 기술1팀

방송시스템의 보안강화 - 4

- Part 4. 디지털 방송시스템의 네트워크 보안 적용방안

연재 목차

최근의 방송시스템은 기존의 Tape 위주의 아날로그방식에서 영상음성신호를 디지털화하여 모든 자료를 파일로 처리하는 방식으로 변경되었다. 기존에 있는 사내 업무망의 경우 인터넷이 연결되어 있어 외부로부터의 공격에 많이 노출되어 있기 때문에, 보통은 업무 성격에 따라 방송제작, 송출, 저장시스템 등으로 구분하여 사내 업무망과 분리된 별도의 망으로 많이 구성하고 있다.

[그림 1]과 같이 인터넷과 사내 업무망 사이에 인터넷방화벽을 두어 외부로부터의 다양한 정찰행위 및 공격시도를 일차적으로 필터링하고, 사내업무와 방송제작망 사이에도 내부 방화벽을 두어 사내에 위치하기만 하면 접속이 가능하던 것을 차단하고, 허가된 사용자들만 제작망에 접속이 가능하도록 구성한다. 이런 구성은 인터넷을 통한 직접적인 공격시도를 차단하는 이점이 있으나, 사내 PC 특히, 전산관리자나 관리자급이 악성코드에 감염될 경우 치명적인 보안사고로 확산될 수 있는 문제가 있다.

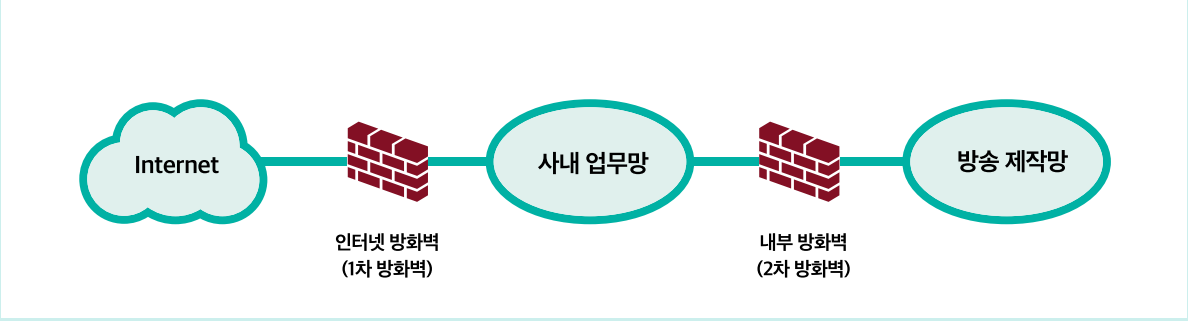

그림 1. 방송망의 구성 위치

[그림 2]와 같이 방송시스템 내에서도 각 시스템을 기능별로 분리하고, 분리된 그룹 간에 독립된 방화벽을 구축하여 사내망에서의 방송시스템 접근 시 그룹별로 분리된 접근정책을 구성할 수 있고, 시스템그룹 간에도 방화벽을 통해서 접근을 제한하기 때문에 한쪽 그룹이 침입을 당하더라도 다른 그룹까지 쉽게 영향을 미치지 못 하도록 구성이 가능하다. 방화벽의 원래 목적이 불이 번지는 것을 막는 기능이 있는 것처럼, 침입을 당하더라도 피해가 확산하는 것을 차단할 수 있는 구성이다.

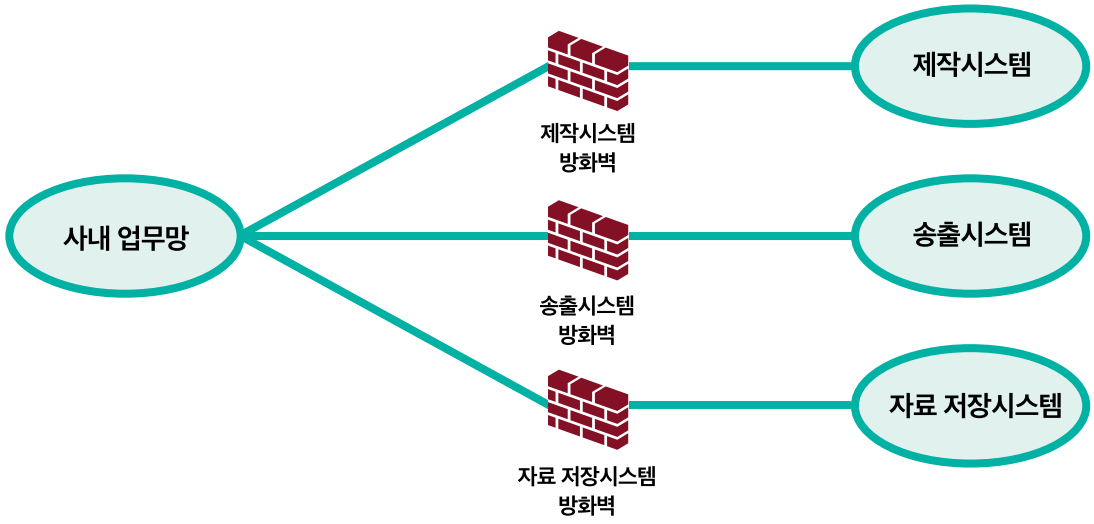

그림 2. 방송시스템 세부 구성도

최근에는 사내 PC가 악성코드로 너무나 쉽게 감염되어 공격의 출발점이 될 수 있기 때문에 조직 내부에 위치한다고 무조건 신뢰할 수가 없다. 소위 Zero-Trust라는 용어로 정의되듯이 내부에 있든 외부에 있든 위치에 관계없이 일단 의심을 하고 보안을 설계하라는 개념이 권장되고 있다. 이제는 내부 PC가 악성코드에 감염되었다는 전제하에 방화벽의 보안정책을 깐깐하게 설정하는 것을 권고하는 이유이다.

예를 들어 내부 PC가 인터넷으로 접속하는 경우에 기존에는 조건에 관계없이 모두 허용하는 정책을 설정하였는데, 이 경우 감염된 PC와 외부의 해커 사이에 자유로운 통신이 가능하고, 유출된 자료를 손쉽게 보낼 수 있는 문제가 발생하였다. 이를 방지하기 위해서는 외부로 나가는 통신을 필요한 서비스만 허용하고 나머지는 모두 차단하거나 URL 필터링 등으로 접속 가능한 홈페이지를 제한하는 방법 등을 사용할 수 있다.

[그림 3]과 같이 방송의 특성상 외부에서 취재하거나 제작한 기사나 영상정보를 신속한 방송을 위해 사내로 전송할 경우 방화벽을 통과하여 사내 영상저장서버까지 접근이 가능해야 한다. 이런 시스템이 외부를 통해 해킹되지 않기 위해서는 인터넷을 통해 아무나 접근하지 못하도록 방화벽 보안정책을 통해 접근을 차단하여야 하고, 자료전송과 열람을 위해 접근이 필요한 경우에는 VPN을 이용하여, 정보를 암호화하여 전송하는 것이 안전하다. 사전에 기자, PD에게 VPN 접속 주소와 접속정보(아이디/패스워드)를 발급하여, 인터넷이 가능한 어떤 장소에서도 자료를 안전하게 암호화하여 전송하도록 구성이 가능하다. 이때 자료 저장시스템 방화벽에는 VPN을 통해 접속하는 사용자가 접근이 가능하게 보안정책을 추가하면 된다.

다음으로 방송사 홈페이지의 경우 방영정보, 지난 방송보기, 시청자 게시판 등 다양한 서비스를 제공하고 있는데, 이 홈페이지에 대해 DDoS 공격이 들어오게 되면, 서비스가 불가능하게 된다. 이런 사고를 미연에 방지하기 위해서는 DDoS 방어시스템의 도입이 필요하나, 도입예산과 관리인력의 여건에 따라 전용방어장비를 도입하거나, 기능적으로는 부족한 점이 있어 인터넷방화벽의 DDoS 방어기능을 활용하는 것도 한 가지 방법이 되겠다.

최근에 가장 이슈가 되고 있는 APT 공격에 대해서는 공격 초기 단계인 사내 PC의 악성코드 감염을 차단하는 것이 효과적인데, 이를 위해서는 메일에 첨부된 파일을 열어보거나, 본문 내용의 URL 링크를 클릭하는 것을 방지하는 것이 중요하다. 악성코드에 감염된

이선응 차장/김영준 과장
아이크래프트㈜
SNT본부 기술1팀

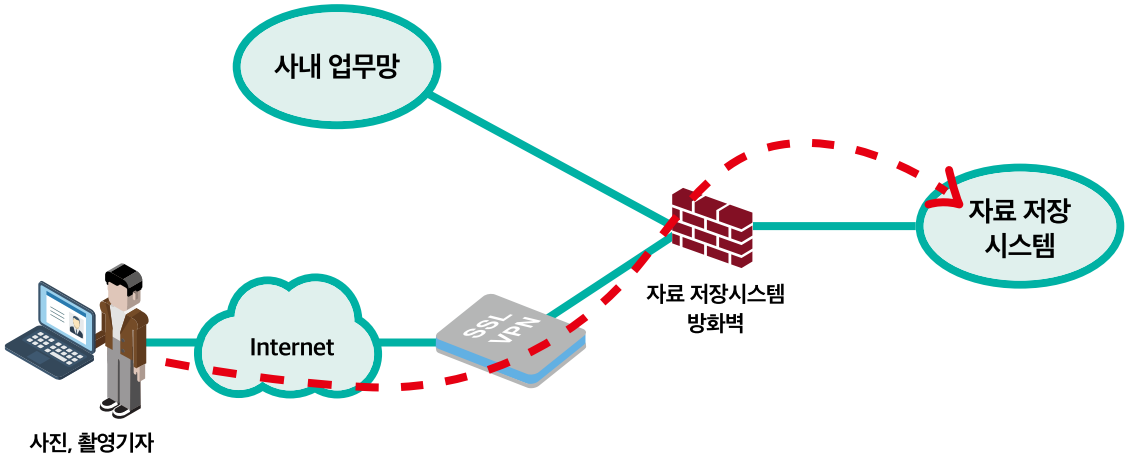

그림 3. VPN을 이용한 기사, 영상 송고

파일을 확인하여 사용자가 해당 파일을 열어보지 못하도록 이메일 보안시스템을 도입하고, 방화벽에 URL 필터링 기능을 추가하는 방법이 있으나, 이런 장비의 도입 이전에 먼저 갖추어 져야 할 사항이 있다.

바로 임직원 대상의 정보보안교육이다. 아무리 좋은 장비를 도입하더라도, 100% 공격을 차단하는 것은 불가능하기 때문에 사용자의 올바른 사용습관으로 장비의 부족한 면을 보완하여야 한다. 특히 정보시스템에 접근할 수 있는 권한이 높거나, 중요한 정보를 많이 취급하는 사용자인 CEO, CFO 등의 간부급 직원, 재무부서, 기획부서, 전산부서 등의 인력들에 대한 집중적인 교육이 필요하다. 최근에는 이런 보안인식이 많이 확산되어서, 전 직원 대상의 분기/반기별 정보보안교육이나, 중요 정보취급자 대상의 심화 보안교육 등이 이루어지고 있다. 교육 이수 후 교육의 내용이 임직원에게 얼마나 잘 전달되었는지 확인할 방법이 있는데, 일반적으로 모의해킹이라는 서비스를 제공해주는 업체에 의뢰하여, 조직의 전산시스템에 대한 전반적인 보안진단을 수행할 수 있다.

모의해킹은 의뢰자와 사전 동의 후에 실제 해커의 관점에서 수행하는 진단으로 홈페이지, 메일서버 등 대외 공개서버에 대한 보안진단과 사내 보안 상태 등을 점검한다. 조직의 정보시스템에 대한 취약점을 검사하여 보완 방안을 리포트 하거나, 임직원 대상으로 테스트용 코드가 포함된 파일을 첨부한 메일을 보내 얼마나 많은 사람들이 해당 파일을 열어보는지 확인하여 보안교육의 효과나 필요성을 고객에게 알려주는 서비스를 제공하고 있다.

최근 관심이 집중되고 있는 인공지능(AI) 분야를 정보보안에 활용하려는 움직임도 보인다. 해커는 자신이 개발한 악성코드가 보안장비에 탐지되지 않고 무사히 업무 PC에 설치되게 하기 위해 다양한 방법으로 공격탐지장비의 허점을 이용하여 자신을 은폐한 후 침투한다. 방어자의 입장에서는 이런 악성코드를 좀 더 정확히 탐지하기 위해 지금까지 수집된 다양한 악성코드 패턴을 학습시켜, 정확도가 높은 인공지능 탐지엔진을 개발하기 위해 노력하고 있으며, 일부 제품이 시장에 출시되고 있다.

다음으로 인공지능이 적용되는 분야는 공격로그를 분석하는 용도이다. 방화벽 등의 보안장비는 동작 중 다양한 경고 메시지(alarm log)를 엄청나게 많이 생성시킨다. 다양한 업무를 해야 하는 관리자의 입장에서는 발생된 경고 메시지를 일일이 확인하는 것이 거의 불가능한 상황이 되면, 외부에서의 공격시도를 정확히 확인하기 힘들어지며 내부에 이미 해커가 침투하여 중요자료가 외부로 유출되었더라도 이 사실을 인지하지 못할 확률이 높다. 이를 방지하기 위해 대량의 경고 메시지를 인공지능을 통해 신속하고 정확하게 인식하여 관리자에게 알려주는 시스템이 개발되고 있다.

최근의 뉴스나 신문에 나오는 다양한 개인정보 유출사고는 최소한 관리자가 개인정보유출여부를 보안시스템의 경고 메시지를 통해 인지한 경우이기 때문에 확인이 가능하였던 것이다. 안타깝게도 국내의 많은 기업들은 보안시스템이 부족할 뿐만 아니라 이를 관리하는 조직이나 인력이 미비한 관계로 자신들의 기업정보가 외부에 유출되었더라도 인지조차 못 하는 경우가 비일비재하다.

그래서, 이러한 사고를 근본적으로 방지하기 위한 보안강화 방안으로 인터넷망과 사내망을 완전히 물리적으로 분리하는 "망 분리" 사업이 많이 진행되고 있다. 보안이 우선순위에 있는 조직의 경우 예를 들면 국방 안보 관련, 연구개발, 사회 인프라(전기, 수도, 가스, 교통)등의 경우 외부로부터의 침입으로 인한 피해가 치명적이고 광범위하기 때문에 원천적으로 공격을 차단하기 위해 망 분리 구성을 권장하고 있다. [표 1]과 같이 사회인프라시스템의 많은 부분이 점점 더 자동화, 지능화되기 위해 네트워크에 연결되면서 공격을 당할 수 있는 빈틈이 증가하게 되었다. 2010년 USB를 통해 이란 원자력발전소의 내부시스템을 침투하여 내부설비를 파괴한 경우도 있으며, 2014년 독일 철강회사의 용광로 제어시스템에 침투하여 제조시설에 큰 피해를 발생시키는 등 사이버공간에 국한되었던 공격들이 이제 물리적 공간으로 확장되고 있는 추세이다.

연도	사고 명	주요 내용
2010년	스턱스넷 완전해킹	이란 발전소 원전 제어시스템 스턱스넷 감염, 원심분리기 1000여 대 고장
2014년	일본 핵발전소 악성코드	일본 모 핵발전소 내부 컴퓨터 악성코드 감염 개인정보 등 4만 2000건 문서 유출
2014년	독일 철강회사 해킹	독일 철강회사를 해커들이 제어시스템 기능 차단, 용광로가 제대로 멈추지 못해 엄청난 피해 발생
2017년	인프라시스템 랜섬웨어 감염	석유, 철강, 선반, 자동차 회사 공장 등 산업 관련 기업 위너크라이, 페트야 랜섬웨어 감염, 업무시스템 마비 발생

표 1. 주요 산업제어시스템 사이버보안 사고사례 / 출처 : 전자신문

현재 기준으로 대부분의 정부기관은 망 분리 구성이 대부분 완료되었고, 정부 산하기관에서도 구축사업을 활발히 진행 중이다. 망 분리는 인터넷을 통한 침입을 원천적으로 차단하기 위해 새로운 네트워크망을 추가로 구축해야 하기 때문에 시간과 예산이 많이 투입되는 사업이므로, 현재 사내 망 구성을 자세히 분석하여, 체계적으로 진행하여야 한다.

[그림 4]와 같이 완전히 분리된 두 대의 PC로 사내망과 인터넷망에 각각 연결하게 되면 아무리 인터넷 연결 PC가 악성코드에 감염되었더라도 사내 업무망에 접속할 수 있는 통로가 물리적으로 완전히 차단되기 때문에 보안을 강화할 수 있다. 기존 업무망과 완전히 분리된 인터넷망을 추가로 구축할 경우 구축비용이 과다하게 소요되는 문제가 있어 최근에는 인터넷 연결을 가상 PC로 구성하고, 기존 사내망 PC 한 대로 가상 PC까지 연결하여 사용하는 방식 등으로 많이 구축되고 있다.

이렇게 망 분리를 하게 되면 이론적으로는 완벽한 보안이 가능하다. 그런데, 이런 시스템을 사용하는 것이 사람이고, 사람들은 언제나 편리함을 추구하기 때문에 보안취약점이 생기기 마련이다. 인터넷에서 내려받은 자료를 업무에 활용하거나 업무에서 생성한 자료를 인터넷으로 전송해야 하는 경우, 인터넷 PC와 업무 PC 간 자료를 서로 교환해야 할 필요가 생기고, 자료 이전을 위해 USB를 이용하는 방법이 사용되고 있다. 해커는 이런 빈틈을 이용하여, USB에 악성코드를 심어 업무망으로 전파시켜, 업무망에서 자료를 수집해 두었다가 외부망에 연결되는 순간을 기다렸다가 자료를 외부로 유출시키는 방법을 고안하였다.

이선응 차장/김영준 과장
아이크래프트㈜
SNT본부 기술1팀

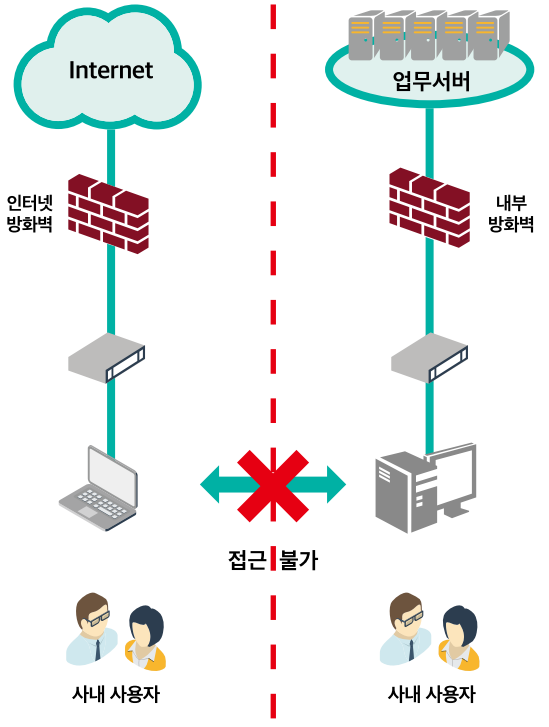

그림 4. 망 분리 개념도

그 이외에도 업무 PC에 설치된 바이러스 백신의 업데이트를 위해, 인터넷 연결이 필요하나 업무PC의 인터넷 연결이 불가능하기 때문에 업데이트를 중계해주는 서버를 이용하게 되는데, 해커는 이런 인터넷망과 사내망을 중계 해주는 서버에 침투하여 이를 통해 내부 업무망에 침입하는 사례도 발생하고 있다. 이렇듯이 아무리 완벽한 구성을 하더라도, 빈틈은 생기기 마련이고 적절한 관리를 통해 이런 취약점을 찾아 없애는 일을 주기적으로 해 주지 않으면, 해커의 침투는 단지 시간문제일 뿐이다.

일반적으로 정보유출사고를 차단하기 위해 다양한 보안장비를 도입하면 문제가 해결될 것으로 생각하지만, 보안 분야에서는 장비 도입 이외에도, 도입 후 사후관리가 되지 않으면 장비를 구축한 효과가 낮아지게 된다. 장비 도입 시에는 없던 사업 분야가 신설되면 새로운 전산설비가 확장 또는 신규로 구축되고, 회사 조직개편이 되는 등 다양한 업무환경 변화에 맞추어 보안시스템 구성을 수정, 보완 해 주어야 하는데, 이런 관리가 부족하면 장비도입의 효과가 떨어지게 된다. 대기업과 금융회사를 제외한 대부분의 회사의 경우 전산관리인력 중 보안을 전담하는 인력이 부족한 실정이다. 통상 전산부서에 소프트웨어(개발) 조직과 하드웨어(전산기기) 조직으로 분리되어 있고, 하드웨어 조직은 여러 가지 하드웨어 시스템을 관리하는 업무를 담당하고 있는데, 통상 서버&스토리지와 네트워크&보안, PC 등 세 부분으로 구분하여 업무분장을 많이 하고 있다.

문제는 네트워크를 담당하는 인력이 보안까지 겸직하는 경우가 많기 때문에, 보안 부분은 우선순위에서 밀리는 경우가 많다. 인터넷 접속속도가 떨어지거나, 사내 서버에 접속이 되지 않는 등 서비스에 직접적인 영향을 미치는 장애는 대부분 네트워크 부분에서 발생하는 문제이기 때문에 여기에 업무 순위가 우선될 수밖에 없다. 네트워크 기능이 부족하거나 통신 속도가 느려질 경우, 인터넷 회선속도를 증속하거나 높은 성능의 네트워크 장비로 교체하면, 네트워크 속도가 2배 이상도 빨라질 수 있어서 사용자 입장에서 바로 투자의 효과를 체감할 수 있다. 그러나 보안장비의 경우는 네트워크 장비와 반대의 경우가 많다. 아무리 기능이 많고, 성능이 좋은 장비를 도입하더라도, 도입 후에 속도가 빨라지는 현상을 체감할 수도 없을뿐더러, 오히려 기존에 자료 접근 시 필요 없었던 다양한 절차(아이디/패스워드 입력 등)만 추가되어 오히려 사용자 관점에서는 절차만 복잡해져서 사용이 불편해지는 경우가 허다하다.

또한 예산을 결정하는 CEO의 입장에서도 투자 대비 효과가 얼마나 있는지 예상을 하고 예산배정을 하게 되는데, 보안장비에 많은 예산을 투입하더라도 투자 대비 효과를 정확히 측정할 수 없기 때문에 예산 배정순위에서 밀려 나는 경우가 많이 있다. 그러나 [표 2]와 같이 최근 5년 사이에 국내의 대형금융기관을 중심으로, 정보 유출사고 뿐만 아니라 해외의 경우 무단으로 현금이 인출되는 사고까지 발생되면서 정보보안에 대한 투자가 대폭 확대되고 있다. 국내의 경우도 대부분의 은행업무를 영업점에 방문하지 않고, PC나 스마트폰을 통해 이루어 지면서, 보안사고의 위험성이 커짐에 따라 보안관련 투자를 대폭 늘려가는 추세이다.

금융권 이외의 분야에도 점차 보안관련투자가 늘어나고 있는 추세다. 이제 보안투자를 비용의 관점에서만 바라보지 않고, 투자의 관점에서 바라보는 시각의 변화가 이루어지기 시작했다. "우리 회사만 아니면 돼"라는 생각으로 운이나 요행에 기대어 정보유출이 일어나지 않기 만을 기대하고 있었다면, 이제는 이런 사고방식을 바꿔야 하는 시기가 온 것이다.

자료 : 정보통신산업진흥원(NIPA), 금융보안연구원(FSA), 언론 보도자료 등

금융회사		발생시기	주요 내용	특징	유출건수 또는 피해금액
국내	현대 캐피탈	2011.4	악성 공격(해킹)	정보 유출	1,750,000건
	한화 손해보험	2011.5	악성 공격(해킹)		160,000건
	삼성카드	2011.8	내부직원 정보 복제		800,000건
	IBK 캐피탈	2011.12	내부직원 정보 복제		5,800건
	한국SC은행	2012.2	외주업체직원 정보 복제		104,000건
	한국씨티은행	2013.4	내부직원 정보 복제		34,000건
	메리츠화재	2013.5	내부직원 정보 복제		164,000건
	국민·농협·롯데카드	2014.1	외주업체 정보 복제		1억4,000,000건
해외	JP Morgan 등 투자은행(미국)	2010.7	악성 공격(해킹)	현금 인출	1,250만 달러
	Barclays 은행 (영국)	2013.1	악성 공격(해킹)		130만 파운드
	30개국 은행 (러시아·미국 등)	2013-2014	악성 공격(해킹)		10억 달러
	HSBC 터키	2014.11	악성 공격(해킹)	정보 유출	270,000건
	스위스 BCGE은행(스위스)	2015.1	악성 공격(해킹)		30,000건

표 2. 국내외 금융회사의 주요 정보보안사고 유형 및 특징

모든 공격을 방어할 수 있는 완벽한 보안체계는 존재할 수 없다. 다시 말하면 위험 수준을 Zero로 만드는 것은 불가능하다. 정보보안의 목적은 해당 조직이 잔여 위험을 수용 가능한 위험 수준으로 낮추는 것이다. 풀어서 설명하자면, 조직에서 취급하는 중요자산을 파악하여, 자산별 등급을 매겨서, 중요도가 높은 순위부터 위험에 대한 대응책을 우선 순서로 준비하되 너무 한곳에 집중하지 말고, 다른 자산의 보안수준도 적정한 수준에 맞추는 것이다.

모든 조직의 예산은 한정적이기 때문에 모든 자산의 보안수준을 최상위로 유지할 수 없다. 중요도를 산정하여, 우선순위가 높은 부분에 우선 투자하되, 무한정 한곳에 투자를 집중하는 것보다는 일정 수준에 도달하여, 혹여 보안사고가 발생하더라도 조직이 감당할 수 있는 범위 내가 되면, 다른 분야의 수준도 적정한 수준에 맞추는 방식을 권장한다.

예로 들면, 어떤 회사는 홈페이지를 통해 매출이 일어나지 않고 중요한 정보도 없으며, 잠시 접속이 되지 않아도 관계없으면 웹방화벽이나 DDoS 방어장비를 구축하는 것보다는, 사내 PC가 좀비 PC가 되는 것을 예방하기 위해 기존에 설치된 바이러스 백신을 통합으로 관리할 수 있는 시스템을 구축하거나, 사내 중요 서버의 보안강화를 위해 내부 방화벽을 추가하는 것을 우선 고려해 볼 수 있다. 이후 다음 순서로 사내 이메일 보안을 좀 더 강화할 수 있는 시스템 도입을 고려하는 식으로 정보의 중요도에 따라 투자순서로 정하되 너무 한쪽에 집중되지 않게 적절히 안배하는 것이다.

다른 예로 기업과의 거래보다 고객과의 거래에서 대부분의 매출이 일어나는 조직의 경우는 고객정보를 1순위 자산으로 구분하여, 고객정보유출을 최우선순위로 방어해야 한다. 이를 위해 고객정보를 취급하는 인원에 대한 보안교육은 물론이고, 고객정보가 포함된 자료의 생성, 수정, 출력에 대한 문서보안 및 고객정보가 저장된 저장소를 위한 DB 방화벽도입, 고객정보의 무분별한 열람으로 인한 유출위험을 줄이기 위한 내부열람규정 적용 등에 우선순위를 두고 대응책을 강구하는 것이 필요하다.

지금까지 총 4회에 걸쳐서 방송시스템의 보안강화란 주제로 설명해 드렸다. 글을 쓰고 나니 짧은 지면에 너무 많은 내용을 전달하려고 욕심을 부리지 않았나 걱정이다. 정보보안이란 분야를 이해하는데 조금이라도 도움이 되었으면 하는 바람이다. 지금까지 긴 글 읽어 주셔서 고맙습니다.