망분리

I. 최근 보안위협의 통향 및 망분리 유형별 개념 ...._ 보안을 위한 망분리의 개요_

가. 최근 보안위협의 동향 (망분리의 필요성)

- 최근 인터넷을 통해 발생하는 다양한 보안 위협들은 이제 그 범위를 서서히 확장하여 지능형 타깃 지속 공격(APT: Advanced Persistent Threat) 으로 발전하고 있음
- APT 공격에 의해 발생하는 트래픽은 이미 장악된 내부망을 통해 들어오기 때문에 정상 트래픽으로 인지되어 이를 방어하기는 기존 보안솔루션만으로는 역부족임
- 따라서, 업무를 수행하는 업무망과 인터넷을 하는 인터넷망(비업무망)을 완전히 분리하여 인터넷을 통해 악성코드가 사내에 침투하더라도 업무 인프라에는 영향을 미치지 않도록 하기 위한 방법이 필요함

나. 논리적 망분리와 물리적 망분리의 개념

논리적 망분리	물리적 망분리
- 한 대의 PC에서 가상화 기술을 이용하여 내부망과 외부망을 분리하는 방식 - 사용자가 인터넷 사용시 가상화 기술을 이용하여 외부 인터넷 접근함 -가상화 기술을 사용하는 VDI 방식, PC 운영체제를 분리하는 OS 커널 분리 방식	**- 물리적은 2대 이상의 PC 또는 네트워크 회선을 달리하여 내부망과 외부망을 분리하는 방식** - 내부망 PC와 인터넷 망 PC가 존재하거나 별도의 망 전환 스위치를 통한 접속

II. 물리적 망 분리의 개요

가. 물리적 망 분리이 개념

그림 삽입

인터넷용과 업무용으로 분리된 네트워크에 인터넷 PC와 업무용 PC를 이용하여 사용하는 방식

III. 물리적 망 분리의 침입 블랙홀 취약점

가. 악성코드에 감염된 USB 메모리를 이용한 자료 교환의 취약점

그림 삽입

- 업무용 PC와 인터넷 연결 PC의 자료 교화에 일반적으로 보안 USB가 많이 사용됨
- 외부망을 통해 유입된 악성코드들이 USB 메모리를 통해 내부로 확산됨

나. 악성코드에 감염된 내부망 PC의 공유 폴더 취약점

그림 삽입

- 내부 특정 PC 한대가 감염이 된 상황에서 공유 폴더를 통한 파일교환으로 악성코드 확산

다. 내부 직원에 의한 취약점

구분	상세 설명
고의적인 정보 유출	- 내부 직원에 의해 고의적으로 내부 정보유출이 발생 가능함
정보보호 의식 저하	- 물리적 망분리에 따른 업무 효율성 저하에 따라 내부 직원의 불법 적 외부망 이용에 따른 취약점 - 사례: 외부망과 차단된 업무용 PC에 별도의 랜카드를 장착하여 외부망 접근

관련 문서

Plugin Backlinks: 아무 것도 없습니다.