사이버보안 의미

사이버 보안은 악의적인 의도를 가지고 시스템, 네트워크 등에 접근하는 시도를 사전에 차단하는 다양한 활동을 의미합니다. 우리가 일상적으로 하는 SNS 로그인 암호부터 금융기관 인증서, 개인 통신메시지 부터 국가 전력망 까지 다양한 분야에 해당합니다.

사이버보안 5가지 유형

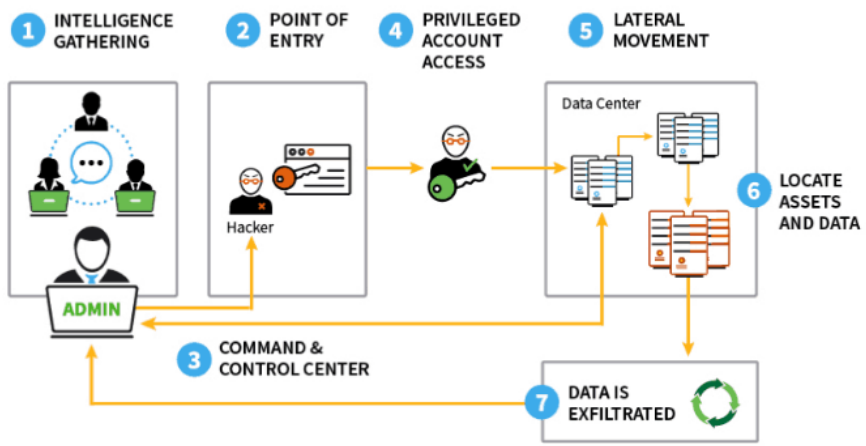
사이버 보안조치는 크게 5개의 유형으로 분류할 수 있습니다.

1. 사회기반시설 보안

예를들어 원자력발전소와 같은 전력시설이 뚫려서 제어권이 공격자에게 넘어갔다면 그 피해의 범위는 상상하기도 어렵습니다. 이처럼 사회기반시설은 공격을 당할경우 피해의 범위가 국가적이라는 특징이 있습니다.

사회기반시설 공격의 대표적인 유형은 APT (Advanced Persistent Threat) 공격으로 다양하고 지속적으로 타깃을 위협합니다.

APT 공격



APT공격절차

절차

(1) 공격을 위해 정보를 수집하는 단계 (스피어피싱, 사회공학적 공격기법 사용)

(2) 취약점 파악

(3)-(4) 관리자 권한 취득

(5)-(7) 데이터 탈취

공격특징

우선 공격타겟이 명확합니다. 앞서 설명 드린 원전과 같이 특정 대상을 노리고 지속적으로 정보를 수집합니다. 또한 직접 공격하는 것은 다양한 루트로 보안으로 어렵기에, 내부 직원을 이용하는 등 우회전략을 쓰기도 합니다. 그리고 이 전략은 성공시까지 지속적(Persistent)이고 지능적인 특징이 있습니다.
APT 보안공격의 대표적 유형으로는 다음과 같은 기법이 사용됩니다.

공격유형	설 명
스피어피싱	특정인, 유명인사, 사이트 운영자 등을 대상으로한 피싱공격
PLC 공격	스턱스넷 이란 핵시설 프로그램 방해공격이 대표적으로 의도한 결과를 얻기까지 지속적으로 정보를 수집하는 침투공격.망분리 까지 무력화하는 도구로 활용될 수 있습니다.
익스플로잇	각종 전자제품이나 SW의 취약점, 버그 등을 이용한 공격으로 컴퓨터의 제어권 획득이나 DoS를 목적으로 합니다.
사회공학적 기법	개인적으로 접근하여 신뢰도를 높이거나 다른 공신력있는 기관을 가장하여 악성코드 전송등을 통해 공격하는 방법

2. 네트워크 보안

스마트 디바이스, IoT 장치의 증가와 함께 모든 장치들이 네트워크에 연결되어가면서 세이프네트워크의 필요성은 점차 높아지고 있습니다. 안전한 네트워크 보안기술은 여러가지가 있지만 우선 크게 3가지 측면에서 강화되어야 합니다.

1) 무선 WIFI 보안

요즘엔 집에서 쓰는 공유기도 암호를 걸어놓지 않는 경우는 없지요. 무선랜 보안기술도 WEP, WPA, WPA2 등 다양하며 이 중에서도 AES 기반의 WPA2 방식이 비교적 강력한 보안기능을 제공합니다.

> 무선침입방지 시스템 WIPS 개념 및 구성요소

2) 망분리/망은닉 기술

사회기반시설의 경우 네트워크 보안을 위해 망 자체를 외부와 분리하거나 망을 보이지 않도록 은닉하는 기술을 사용합니다.

망분리에는 물리적으로 분리하는 방식이 가장 보안성은 높지만 별도 망구축으로 비용이 높아지는 단점이 있습니다. 그래서 보통 기업에서는 논리적 망분리 기술인 SBC, CBC 를 도입하는 것도 비용측면에서 효과적입니다.

3) 고신뢰 VPN 기술

터널링기법을 통한 공중망 사이의 두 네트워크를 마치 전용선을 통해 연결하는 효과를 주는 기술입니다. 구현기술에 따라 IPSec VPN, SSL VPN, L2F, L2TP, PPTP, MPLS VPN 등의 다양한 유형이 있습니다.

3. 각종 IT Device 보호

이제는 TV, 냉장고와 같은 일반 가전제품들도 모두 무선접속을 통해 스마트폰에서 편리하게 제어하고 모니터링이 가능한 세상이 되었습니다. 가량 차량이 해킹되어 무선주행기능이 오작동한다면 생명의 위협에 노출될 수 도 있습니다.

관리 및 이용측면에서 이런 Device 장치의 보안을 높이는 방법은 다음이 있습니다.

- 방화벽 및 보안장비 활용
- 기기의 암호설정 (어려운 암호 및 패턴)
- 주기적으로 최신 보안업데이트 적용
- 카메라와 같은 장치 미사용시 물리적으로 렌즈 가리기

4. 클라우드 보안

요즘 구글 드라이브, 원드라이브 같은 클라우드 서비스를 하나정도는 사용하는 것 같습니다. 물론 개인사용자라면 암호관리 등은 기본적이지만 이를 서비스하는 기업에서도 개인정보유출, 서비스 중단과 같은 여러 클라우드 위협에 대한 보안이 필요합니다.

클라우드는 다양한 기술이 결합한 서비스로 각 구간별로 보안기술이 적용되고 있습니다. 가령 구간별로 다음과 같은 기술적용을 들 수 있겠습니다.

클라우드 구간	보안기술
플랫폼	접근제어, 사용자 인증
스토리지	검색가능 암호시스템 적용, PPDM(프라이버시 보존형 데이터 마이닝)
네트워크	SSL, IPSec 인증방식 제공방화벽, DDoS 방어기술 제공
단말기	TPM, CryptoCel 등을 통한 암호화 기술

5. 어플리케이션 보안

스마트폰에서 사용하는 앱보다 더 큰 개념으로 다양한 SW 응용프로그램을 포함하여 각종 시스템 개발에서 발생할 수 있는 취약점에 대한 보안을 의미합니다. 가령 이제는 누구나 사용하는 스마트폰의 경우 다음과 같은 보안을 강화하기위한 전략들이 사용됩니다.

- 애플리케이션 화이트리스팅
- 생체인증 기술
- 데이터 암호화 (메모리 내)
- Application 마다 접근권한 부여
- 샌드박스를 통한 분리