**(물음 1) 스피어피싱 공격을 막기 위한 방법을 개인과 기업으로 구분하여 서술하시오.(기업은 중소기업과 일반기업으로 구분하여 서술할 것)**

1. 스피어싱 공격 : 이메일을 통한 공격

1. 유형 : 첨부파일을 이용하는 형태, 본문 링크클릭을 유도하는 형태
2. 정교화 경향 : 사회공학적 기법과 연계되어서 동장, 공격의 목표가 되는 사용자의 이메일 주소를 인터넷이나 SNS를 통해 획득 후에 공격 시도

2. 스피어싱 공격에 대한 기본적인 주의사항

1. 의심되는 이메일의 첨부파일은 절대 열어보지 말 것
2. 이메일에 포함되어 있는 URL을 클릭할 때 주의할 것
3. 사용하는 PC의 소프트웨어와 운영체제는 항상 최신버전으로 유지할 것
4. 백신소프트웨어의 자동검사 기능을 항상 사용할 것

3. 스피어싱 공격을 막기 위한 방법

1. 개인

- 바이러스토탈을 통한 확인

 바이러스토탈은 구글이 운영하는 전세계 최대의 무료 보안검사

및 공유사이트로, 의심스러운 웹사이트에는 접속하기 이전에 바이러스토탈

등에서 검사하여 안전성 여부를 확인한 후에 접속하는 것이 좋음

- 웹메일의 중복사용을 통한 방법

 네이버, 구글 지메일, 마이크로소프트 아웃룩 웹 등 웹메일 솔루션은

기본적으로 악성코드 탐지기능을 제공함

각기 다른 악성코드 탐지엔진을 사용하기 때문에 이를 조합하여 사용하면

매우 유용함

1. 중소기업 : 클라우드 기반의 이메일 보안솔루션 도입

스팸필터링과 이메일 악성코드 탐지/차단 서비스를 함께 제공

클라우드 기반이므로 큰 비용부담 없이 사용 가능한 것이 장점

1. 일반기업 : 스피어피싱 방어가 가능한 최신의 보안솔루션 검토 및 적용

대기업은 복잡하고 비용이 고가일 수도 있으나 스피어피싱 방어가 가능한 고급/최신 보안솔루션을 적극적으로 도입하는 정책을 펼칠 필요가 있음

**(물음 2) DDOS 공격과 악성코드의 연관성에 대해 서술하시오**.

1. 악성코드

1. 정의 : 악의적인(Malicious) 소프트웨어(Software)
2. 기능 : 컴퓨터시스템 파괴, 정보유출, 허가 없이 시스템 접속
3. 종류 : 바이러스, 웜, 트로이목마, 백도어, 에드웨어, 랜섬웨어
4. 감염경로 : 이동식디스크, 이메일, 내부네트워크, 웹사이트

2. DDOS (Distributed Denial of Service, 분산 서비스 거부 공격)

1. 특정 서버를 대상으로 정상적인 서비스가 불가능하게 하려는 목적으로 시도하는 악의적인 공격 기법으로, 공격자는 특정 서버를 대상으로 지속적인 트래픽을 유발함으로써 서버가 감당할 수 없을 만큼의 리소스를 발생시켜 서버를 마비시킴
2. 가정이나 회사에서 PC를 사용하다 보면 갑자기 PC가 느려지거나 멈추는 경우가 있는데, 이는 PC가 처리할 수 있는 양보다 훨씬 많은 작업(Task) 요청이 들어와 이를 PC가 감당하지 못하게 되는 것임
3. 즉, PC에 내장된 중앙처리장치(CPU)나 주기억장치(Main Memory)가 처리할 수 있는 능력 이상의 요청이 발생할 때 PC는 과부하(過負荷)로 이를 감당하지 못해 느려지거나 멈추는 현상이 발생함

3. DDOS 공격과 악성코드의 연관성

1. 해커는 악성코드를 유포시켜 다수 사용자의 PC를 감염
2. 감염된 PC들은 좀비PC가 됨
3. 해커는 가능한 많은 좀비PC 확보 후 명령제어서버(C&C)를 통해 원하는 목표로 공격명령을 내림
4. 수많은 좀비PC들이 한번에 표적으로 공격을 수행함
5. 결국 악성코드에 의한 좀비PC 감염 그리고 봇넷의 구성이 시작점이 됨

**(물음 3) 랜섬웨어의 주요 감염경로에 대해 서술하시오**.

1. 랜섬웨어어란 : Ransom(몸값)과 Software의 합성어로 시스템 혹은 소프트웨어의 데이터를 암호화하여 사용불능상태로 만들어 이를 인질로 잡고 돈을 요구하는 악설프로그램을 말함

2. 랜섬웨어의 감염경로

1. 신뢰할 수 없는 사이트 : 단순접속만으로도 감염 가능
2. 스펨메일 및 스피어피싱 : 첨부파일 또는 첨부URL을 통해 악성코드 유포
3. 파일공유 사이트 : Torrent, Webhard 등 P2P사이트를 통해 감염
4. 사회관계망서비스(SNS) : SNS에 올라온 단축URL 및 사진을 통해 유포
5. 네트워크망 : 최신 보안패치가 적용되지 않은 PC를 스캔하여 악성코드를

감염, 확산

3. 대처법

1. 출처가 불분명한 파일의 경우 열기 전 반드시 백신검사를 실시
2. 사용하는 운영체제와 프로그램들을 항상 최신 버전으로 유지