**전사원이 알아야할 랜섬웨어와 악성코드 예방법 \_ 요약집**

* **사이버 공격 방법으로는 스피어 피싱, SQL 삽입 공격, XSS(Cross-Site Scripting), 무차별 대입 공격, DDoS 등이 있다. 보이스피싱은 전화를 통하여 신용카드 번호 등의 개인정보를 알아낸 뒤 이를 범죄에 이용하는 전화금융사기 수법을 말한다.**
* **데이터 액세스는 사용자 인증(주로 PIN 또는 로그인 사용), 사용자 역할을 바탕으로 인증 및 권한 부여, 데이터 변경 사항 로깅 및 사용자 네트워크 활동 기록을 위해 사용자를 인증, 권한 부여 및 어카운팅(AAA)하는 시스템이 데이터 액세스를 제어하는 것을 말한다. 데이터 기밀성은 권한이 없는 사용자가 데이터에 액세스할 수 없으며, 사용할 수 있도록 유출되어서도 안된다. 데이터 암호화를 통해 데이터 전송을 보호하며 제3자의 불법 액세스를 방지한다.**
* **정보보안의 목표는 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 기밀성, 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없게 하는 무결성, 허락된 사용자 또는 객체가 접근 시 방해 받지 않도록 하는 가용성이라고 볼 수 있다.**
* **컴퓨터 기반의 사회공학 방법 공격**
  1. **피싱**
  2. **파밍**
  3. **스미싱**
* **PDCA 단계 업무 중 관리와 개선을 하는 단계로 ISMS가 제대로 운영되지 않는 경우, 원인을 분석하고 시정하는 단계 : 조치**
* **윈도우의 그룹 유형**
  1. **Guests**
  2. **Users**
  3. **power users**
* **"라우터"는 OSI 7계층 중 3계층에서 사용하는 장비**
* **멀웨어의 문제점은 공격자들의 진입 장벽이 매우 낮다는 것이다. 악의적 공격자들이 단지 39달러만 지불하면 멀웨어를 구축·배치하거나 경제적 수단으로 이용 할 수 있다.**
* **PC 부팅 시 메모리를 read 혹은 written 할 수 없다고 하는 Alert 창이 뜨거나, [확인] 버튼을 클릭해도 계속해서 뜨는 창이 뜬다면 악성파일이 응용프로그램 실행을 방해하고 있는 것이다.**
* **컴퓨터 바이러스 감염 예방법에 대한 설명**
  1. **데이터를 정기적으로 백업한다.**
  2. **출처가 불분명한 이메일은 열람하지 않는다.**
  3. **PC를 함께 사용하는 환경에서는 사이버 뱅킹이나 주식 거래, 온라인 쇼핑을 하지 않는다.**

**-------------------------------------------------------------------------------------------------------------**

* **보안을 위한 유의사항**
  1. **새로운 스마트홈 디바이스를 구매했을 때에는 즉시 기본 패스워드를 변경한다.**
  2. **소프트웨어를 항상 최신으로 유지한다.**
  3. **모든 중요 데이터를 주기적으로 다른 하드 드라이브나 클라우드에 저장한다.**
* **개인이 사이버 공격에 상대적으로 취약한 경우**
  1. **감염된 usb의 사용**
  2. **암호화 되지 않은 데이터**
  3. **바이러스 검사 프로그램의 사용**
* **네트워크 보안의 모범 사례**
  1. **개인이 소유 및 사용하는 스마트기기들과 IoT장치의 위험성을 파악한다.**
  2. **데이터를 항상 백업한다.**
  3. **네트워크 사용자를 교육한다.**
* **시큐어 코딩의 개발 단계는 취약성이 잔재할 수 있는 코드를 배제하고 안전한 소스와 프로그램을 사용하는 단계라 할 수 있다. 즉, 시큐어코딩이란 개발과정에서 개발자의 지식부족이나 실수 또는 각 프로그래밍 언어의 고유한 약점 등 다양한 원인으로 발생할 수 있는 취약점을 최소화하기 위하여 설계 단계부터 보안을 고려하여 코드를 작성하는 제작방식을 의미한다.**
* **퍼징(fuzzing)은 애플리케이션 보안테스트로써 비정상적인 데이터를 애플리케이션에 전달하여 에러를 유도하는 방법을 말한다.**
* **데이터 보안 강화 방법은 핵심데이터를 파악하는 것으로 핵심데이터를 가능한 작게 유지하고, 최소한의 필수 데이터만 저장하기 위해 비즈니스 가치와 민감도를 기준으로 데이터를 범주화해야 한다. 애초에 저장하지 않는 것이 가장 안전하기 때문에 데이터는 사용 기간이 끝나면 폐기 처분하는 것이 바람직하다.**
* **재해복구시스템 유형은 구축 형태별, 운영 주체별, 복구 수준별로 구분할 수 있다.**
* **재해복구시스템의 구현 기술**
  1. **하드웨어/소프트웨어 복제 방식**
  2. **데이터 전송 방식**
  3. **동기/비동기 복제 방식**
* **사회공학적 사이버 해킹 공격의 적용 통로**
  1. **이메일**
  2. **인터넷 메신저**
  3. **모바일**
* **인간 기반의 사회공학적 사이버 공격 중 직접적인 접근 방법**
  1. **권력을 이용한 접근**
  2. **동정심에 호소한 접근**
  3. **가장된 인간관계를 이용한 접근**
* **인터넷을 통한 개인정보의 수집이 용이해짐에 따라 유명인사나 기업 간부 등을 타겟으로 하는 해킹인 웨일링 증가하고 있다.**
* **SABSA의 계층구조**
  1. **Logical**
  2. **Physical**
  3. **Component**
* **ISMS의 목적**
  1. **국제적 신뢰도 향상**
  2. **정보자산의 안전, 신뢰성 향상**
  3. **정보보호서비스 산업 활성화**
* **ISO 27001의 보안 통제 분야**
  1. **보안 정책**
  2. **자산 관리**
  3. **공급자 관계**
* **가트너의 EISA 모델의 단계는 크게 개념, 논리, 구현 단계로 구성된다. 여기서 개념적 목표를 실현시키기 위한 이상, 방법론, 기술 적용 단계는 논리적 단계에 해당한다. 세부적으로 조직 아키텍처, 정보 보호 아키텍처, 정보 분류 레지스터, 기술 참조 모델, 정보 보호 기반 시설 아키텍처, 정보 보호 서비스 아키텍처 등 구체적 아키텍처 개발이 포함된다.**
* **부적절한 패스워드 유형**
  1. **단어로 입력된 패스워드**
  2. **키보드에 나열된 순서를 이용한 패스워드**
  3. **사용자 정보를 포함하는 패스워드**
* **취약점을 수정하기 위한 방법**
  1. **소프트웨어 재설정**
  2. **패치 설치**
  3. **네트워크 보안 정책 변경**
* **OSI 7계층 중 5계층 세션 계층에 대한 설명**
  1. **포트 연결이라고 할 수 있다.**
  2. **통신장치 간의 상호작용을 설정하고 유지하며 동기화 해준다.**
  3. **사용자간의 포트연결이 유효한지 확인하고 설정한다.**
* **네트워크 용어의 설명**
  1. **노드는 컴퓨터 네트워크상에 연결된 장치이다.**
  2. **호스트는 고유 IP 주소를 가진 노드이다.**
  3. **프로토콜은 데이터 통신을 원활하게 하기 위해 필요한 통신 규약이다.**
  4. **링크는 물리적으로 노드와 노드를 연결하는 통로이다.**
  5. **경로는 네트워크 상의 두 노드 간의 이동 경로이다.**
* **악성코드의 주요 감염경로**
  1. **보안 프로그램이 자동 업데이트 되는 과정에서 감염된다.**
  2. **P2P 서비스를 이용해 다운로드 받은 경우이다.**
  3. **내부자에 의하여 직접 악성코드가 설치되는 경우이다.**
* **악성코드의 역사에 대한 설명**
  1. **1990년대 안티바이러스 소프트웨어 시장 성장**
  2. **2000년대 중반기 컴퓨터 웜의 수는 수백개로 증가**
  3. **2013년 암호화폐 관련 랜섬웨어가 모습을 드러내기 시작**
  4. **1972년 컴퓨터 바이러스의 개념이 처음 등장한다.**
* **악성코드의 개요에 대한 설명**
  1. **멀웨어 공격은 대외비 데이터를 훔치는 방식으로 수행한다.**
  2. **개인과 기업에 추가적인 공격을 가하는 데 사용되거나 다른 악의적 공격자들에게 판매한다.**
  3. **멀웨어의 일종인 랜섬웨어는 금전적 이득을 취할 수단으로 점점 널리 악용되고 있다.**
* **지능화되는 악성코드의 유포 사례에서 볼 수 있는 방식**
  1. **고객 안내 페이지로 위장 악성코드 유포한다.**
  2. **보안 프로그램 설치 위장 피싱페이지 접속 유도 후 보안 프로그램을 다운로드 받으면 감염시킨다.**
  3. **입사지원서를 가장한 다운로드 한 파일은 아이콘은 PDF 문서이지만, 실제로는 악성코드가 포함된 실행파일(exe)이다.**
* **엔드포인트에서 발생하는 모든 행위를 파악하고 보안 위협이 발생할 경우 신속하게 대응하기 위한 솔루션 : EDR 솔루션**
* **바이러스 분석 방법**
  1. **간접호출**
  2. **심볼릭 실행**
  3. **코드만 분석**
* **컴퓨터 바이러스의 역사에 대한 설명**
  1. **1970년대 인터넷 선구자인 아파넷에서 최초의 바이러스가 발견되었다.**
  2. **매크로 바이러스가 일상화된 것은 1990년대이다.**
  3. **크로스 사이트 스크립팅을 사용하여 확산된 바이러스가 학술적으로는 2005년에 증명됐다.**
* **스스로 복제하여 다른 프로그램을 감염시키고 컴퓨터의 파일이나 데이터를 파괴하거나 속도 저하, 정보유출, 오작동 등을 일으키는 악성 프로그램 : 컴퓨터 바이러스**
* **트로이목마의 설치된 후 하는 행동에 대한 설명 : 메일파인더(Mailfinders)는 사용자의 주소록을 훑어 스팸에 이용할 이메일 주소를 확보한다.**
* **트로이 목마의 역사에 대한 설명 : 최초의 트로이목마는 1951년 UNIVAC이라는 영업용으로 출시된 최초의 컴퓨터에서 실행되는 ANIMAL이라는 게임이다. 1974년 최초로 구현된 것은 프로그래머 존 워커에 의해서이다. 1980년대부터 현대적 모습의 트로이목마가 등장한다.**
* **현재 백도어를 열고, 영향을 받는 장치를 제어, 사용자 데이터를 유출, 공격자에게 전송, 영향을 받는 시스템에서 다른 악성 소프트웨어를 다운로드하여 실행하는데 사용되는 가장 일반적인 악성코드 : 트로이 목마**
* **웜에 대한 설명**
  1. **컴퓨터 시스템을 파괴하거나 작업을 지연 또는 방해하는 악성 프로그램**
  2. **통신망 등을 통해서 널리 확산한다.**
  3. **웜과 바이러스의 큰 차이점은 감염 대상을 가지고 있는가에 따라 구분한다.**
* **웜의 한 종류로 인터넷을 통해 전파된 최초의 웜 : 모리스 웜**
* **웜의 역사에 대한 설명**
  1. **제록스 파크(Xerox PARC)의 두 명의 연구자에 의해 최초로 구현**
  2. **1978년 제록스 파크(Xerox PARC)의 두 명의 연구자에 의해 최초로 구현됐다.**
  3. **2003년 슬래머 웜(SQL Slammer)이 발견되었다.**
* **해킹 피해 유형**
  1. **컴퓨터 시스템 이상 동작 유발**
  2. **해킹 경유지 이용 피해**
  3. **디스크 자료 불법 열람, 삭제 및 변조**
* **해킹의 새로운 공격기법**
  1. **에이전트화**
  2. **분산화**
  3. **은닉성**
* **유닉스 기반의 해킹 시나리오 단계 : 정보수집 → 불법적인 컴퓨터 접근 → root 권한 획득 → 스니퍼 설치 → 뒷문프로그램 설치 → 구체적 피해 행위**
* **해킹 기법**
  1. **버퍼오버플로우**
  2. **서비스 거부 공격**
  3. **뒷문 프로그램**
* **방화벽의 주요 기능**
  1. **접근 통제**
  2. **로깅**
  3. **사용자 인증**
  4. **암호화**
* **방화벽의 보안기능 중 중요한 데이터나 침입차단시스템을 통하여 전송되는 데이터에 변경이 발생하는 경우 이를 확인하는 기능 : 무결성**
* **방화벽의 운영방식 중 모든 입출력 트래픽에 대한 로그 정보 기록 및 통제 기능을 가지며, 높은 수준의 보안 기능을 제공하는 방식 : 응용 게이트웨이 방식**
* **Kumar의 침입탐지시스템 분류 중 비정상침입 탐지방법**
  1. **통계적 방법**
  2. **신경망**
  3. **특징 추출**
* **Kumar의 침입탐지시스템 분류 중 오용 침입 탐지방법**
  1. **전문가 시스템**
  2. **상태 전이 분석**
  3. **모델에 근거한 침입 탐지**
* **COAST의 침입탐지시스템의 분류 중 데이터 소스를 기반으로 하는 분류 방법**
  1. **단일 호스트 기반**
  2. **네트워크 기반**
  3. **다중 호스트 기반**
* **ISO/IEC에서는 침입탐지시스템의 모듈 중 수집된 데이터와 보안 관련 정보를 비교하여 침입을 판단하며, 이전 분석의 결과에 반영, 이후 분석을 위해 필요한 데이터로 사용, 그리고 정상행위 학습 정보 등으로 이용되는 단계 : analyzer**
* **침입탐지방법론 중 오용탐지 방식에서 타당한 방법으로 새로운 입력 출력쌍을 얻기 위해 두 집합의 정보간 관련성을 학습하고 일반화하는데 사용되는 알고리즘 기법 : 신경망**
* **비정상행위를 탐지하는 방법론으로 finite state transition의 한 방법으로 음성인식분야나 DNA 시퀀스 모델링 분야에서 광범위하게 사용되는 확률적인 모델기법으로써 생성메커니즘을 알 수 없는 이벤트들을 모델링하고 평가하는 강력한 도구 : HMM**
* **비정상행위를 탐지하는 방법론에서 가장 널리 사용되는 방법으로 자료를 충실히 표현하기에는 너무 단순한 문제가 존재하여 보다 발전된 형태로 장기 및 단기간 사용자 활동 프로파일을 비교하는 방식에 해당하는 것 : 통계적 방법**
* **ICSA IDSC의 침입탐지시스템의 분류 중 모니터링 접근방식에 따른 분류**
  1. **응용 기반**
  2. **호스트 기반**
  3. **대상 기반**
* **정보보호 대책을 위한 구성요소로 정보시스템의 안전, 신뢰성을 확보하기 위해 기본사항에 대한 보호대책을 법제정 또는 사규, 규정 등의 차원에서 대응하는 것 : 관리적 보안대책**
* **인터넷과 같은 공중망을 통해 통신하는 경우, 통신 채널을 암호화하여 전송되는 데이터의 기밀성을 보장, 사설망과 같은 효과를 주는 네트워크 암호화 시스템 : VPN**
* **PCAP 라이브러리 함수 중 네트워크 장치로부터 반복하여 패킷을 읽는 함수의 형태 : pcap\_loop()**
* **TCP packets 중 비정상 패킷에 해당**
  1. **SYN FIN**
  2. **SYN FIN RST**
  3. **SYN FIN PSH**
* **Dos의 공격 종류 중 Land attack에 대한 설명 : 출발지 IP/Port를 타겟 IP/Port로 설정하여 시스템의 부하를 발생시키는 공격**
* **컴퓨터가 봇넷에 등록되어 있는지 확인할 수 있는 징후**
  1. **잦은 충돌**
  2. **긴 로드 시간**
  3. **이상한 오류 메시지**
* **DoS의 종류**
  1. **Ping of death**
  2. **Smurf**
  3. **Teardrop**
* **APT의 공격과 기존 악성코드의 차이점 중 APT공격에 대하여 맞게 기술한 것 : APT는 지속성있는 공격을 한다.**
* **APT 대응방안**
  1. **앤드포인트 보안**
  2. **서버 보안**
  3. **네트워크 보안**
* **APT 사례 중 스턱스넷에 대한 설명 : 사이버 공격으로도 사회기반 시설이 파괴될 수 있다는 가능성을 보였다.**
* **지능형 지속 공격의 개요**
  1. **과거의 불특정 다수를 노렸던 공격과는 달리 하나의 대상을 목표로 한다.**
  2. **내부로 침입을 성공할 때까지 다양한 IT 기술과 공격방식을 기반으로 여러 보안 위협을 생산하여 공격을 멈추지 않는 특징이 있다.**
  3. **최근 지능형 지속 공격의 방법이 지능적으로 이메일을 이용해 악성코드 등을 심거나 강제로 암호화 한다.**
* **공유폴더 접속으로 감염되며, 특정 도메인에 접속 성공하면 동작하지 않는 킬스위치 기능을 가진 랜섬웨어 : 워너크라이**
* **컴퓨터 부팅시 자동으로 랜섬웨어에 감염시키는 방법 : 웜**
* **랜섬웨어 진화 순서 : 차단형 → 비밀형 → 타깃형**
* **주로 이메일을 통해 감염되며, 브라우저, 메일, 쿠키, ftp 계정 등의 사용자 정보를 탈취하는 랜섬웨어의 형태 : 크립트XXX**
* **랜섬노트에 week4004라는 메일 정보를 포함하고 있고 기존의 랜섬웨어와 다르게 파일 확장자 변경이 없는 랜섬웨어 : DMA Locker**