전사원이 알아야할 랜섬웨어와 악성코드 예방법

학습노트

한국교육개발진흥원(주)
Korea Education Development Center

[1차시]

1. 사이버 보안이란?

컴퓨터와 네트워크, 데이터를 악의적인 전자적 공격으로부터 보호하는 전반적인 활동을 말한다. 즉, 인터넷으로 연결된 컴퓨터, 서버, 모바일 디바이스, 네트워크를 사이버 공간에서 허가되지 않은 접근, 데이터 도난, 공격, 무단조작으로부터 보호하기 위한 것이라 할 수 있다.

2. 사이버 공격

(1) 사이버 공격이란? - 타인의 컴퓨터 네트워크에 대한 악의적인 공격을 말한다.
(2) 사이버 공격의 대상 - 개인, 기업, 공공 기관, 심지어 국가 전체의 인프라까지 거의 모든 대상이 사이버 범죄의 표적이 될 수 있다.
(3) 사이버 공격 동기 - 염탐, 방해 공작 등
(4) 공격 방법 - 스피어 피싱, SQL 삽입 공격, XSS(Cross-Site Scripting), 무차별 대입 공격, DDoS 등
(5) 공격으로 인한 결과 - 막대한 비용 발생, 생산성 저하, 평판의 훼손 등
(6) 사이버 공격의 변화 양상 - 사이버 공격의 양상은 빠르게 변화하고 있으며, 지금 이 순간에도 진행되고 있다. - 사이버 공격자들은 랜섬웨어를 사용하여 피해자의 컴퓨터 사용 불가하게 조작하며, 이를 복구하기 위해서는 돈을 지불해야 한다.

3. 사이버 보안 위협 TOP 5

(1) 타깃형 랜섬웨어 공격
(2) 클라우드 보안 위협
(3) 특수목적시스템 및 OT 보안 위협
(4) 정보 수집 및 탈취 공격 고도화
(5) 모바일 사이버 공격 방식의 다변화

4. 사이버 보안 강화

(1) 설계에 의한 보안 컨셉으로 어떤 제품이나 시스템을 개발할 때 보안을 내장해야 한다.
(2) IoT 디바이스들의 대한 보안 표준을 제정하고 채택해야 한다.
(3) 암호화와 인증을 통한 사이버 보완 시스템이 도입이 필요하다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[2차시]

1. 사이버 보안 종류의 개요

(1) 네트워크 보안
(2) 애플리케이션 보안
(3) 데이터 보안(정보 보안)
(4) 운영 보안
(5) 재해 복구

2. 네트워크 보안

(1) 네트워크 보안이란? - 허가되지 않은 액세스와 피해로부터 회사의 네트워크를 보호하기 위해 설계된 일련의 전략, 프로세스, 기술을 말한다.
(2) 네트워크 보안의 데이터 요소는? - 데이터 액세스, 데이터 가용성, 데이터 기밀성, 데이터 무결성
(3) 클라우드 - 클라우드 아키텍처 내에서 데이터와 정보를 보호하도록 설계된 기술 및 모범 사례를 포함하는 포괄적인 용어로 클라우드 보안은 클라우드에 저장된 데이터에 대한 데이터 개인정보 보호와 보안 및 규정 준수를 보장하는 것을 말한다.
(4) 네트워크 보안 모범 사례 9가지 - 소프트웨어를 유지 보수 - 가시성을 최우선 - 사용자의 권한 관리 - 신뢰할 수 있는 도구의 사용 - 규정 준수를 유지 - 보안 정책을 수립 - 데이터 백업 - 타사 사용자의 인지 - 사용자 교육

3. 애플리케이션 보안

(1) 애플리케이션 보안이란? - 무단 액세스 및 수정과 같은 보안 취약점에 대한 위협을 방지하기 위해 보안 기능을 개발하여 애플리케이션에 추가하고 테스트하는 과정
(2) 애플리케이션 보안 유형 - 인증, 권한 부여, 암호화, 로깅 및 애플리케이션 보안 테스트, 개발자의 애플리케이션을 코딩
(3) 애플리케이션 보안 제어 및 테스트 - 애플리케이션 보안 제어는 코딩 수준에서 애플리케이션 보안 수준을 향상하여 위협에 대한 취약점을 줄이는 기술 - 애플리케이션 보안 테스트 유형인 퍼징(fuzzing)은 일반적으로 비정상적인 데이터를 애플리케이션에 전달하여 에러를 유도하는 방법 - 애플리케이션 개발자는 소프트웨어 개발 프로세스의 일환으로 애플리케이션 보안 테스트를 수행하여 소프트웨어 애플리케이션의 새로운 버전 또는 업데이트된 버전에 보안 취약점이 없는지 확인
(4) 애플리케이션 보안 솔루션 - 시큐어 코딩 - 웹 스캐너 - 웹서버 악성코드 탐지 - 웹해킹차단시스템 – 데이터보안

copyright 2021. 한국교육개발진흥원 All rights reserved.

[3차시]

1. 정보 보안

(1) 정보 보안(Information security) 개요 - 컴퓨터 및 네트워크로 확대, 발전하는 정보환경에서 모든 정보자원 하드웨어, 소프트웨어, 데이터 등을 위/변조, 유출, 훼손 등과 같은 정보보안 사고로부터 보호함으로써 무결성, 기밀성, 가용성을 제공하는 것을 의미한다.
(2) 정보 보안 위협 - 해커, 감염된 컴퓨터 및 소프트웨어, 정보 손실 및 파괴, 정보의 조작, 서비스 거부 공격, 정보의 노출이 해당한다.
(3) 데이터 보안 강화 방법 - 데이터 보안 강화 방법으로는 중요한 데이터 파악, 크리덴셜 정리, 엄격한 내부 보안 경계선 규정, 데이터 암호화 상태 유지, 클라이언트 보호 등이 있다.
(4) 클라우드 사용에 따른 데이터 보안 위협 - 조직의 인프라가 디지털화 될 수록 데이터 유출 사고를 겪을 가능성이 높아지는데, 디지털 트랜스포메이션을 이행하는 조직들이 경쟁 우위를 선점하고 있어, 기업들은 빠르게 혁신 기술을 도입하고 있으며 이로 인해 전에는 발생하지 않았던 데이터 유출 사고 및 데이터 규제 위반 사례가 나타나고 있다. 민감 데이터를 보호하기 위한 첫 단계는 민감 데이터의 위치를 인지하는 것으로, 분류된 데이터는 강력한 멀티 클라우드 키 관리 전략으로 암호화 및 보호되어야 한다.을 남기는 것입니다.

2. 운영 보안

(1) 운영 보안의 개요 - 운영 보안이란 비즈니스 환경이 계획되고 검증된 일정 수준으로 보호되기 위한 일련의 조치와 통제가 수행되는 것을 의미한다. 운영 보안의 요소로는 위협, 취약성, 자산이 있다. 운영 보안의 상대는 내외부의 침입자와 부적절한 자원에 접근하는 사용자 및 운영자, 그리고 운영 환경에 대한 위협으로 볼 수 있다.
(2) 통제와 보호 - 통제란 위험을 감소시키기 위하여 만들어진 정책, 절차, 업무, 조직구조 등을 의미한다. 통제의 목적은 첫째, 조직의 경영 목적 달성 둘째, 위험이 적절히 예방되거나 적발 또는 수정될 것이라는 합리적인 확신을 제공 셋째, 경영진이 제기한 관심사를 기반으로 하는 것에 그 목적이 있다. - 통제의 종류에는 통제 적용 시점에 따라 예방 통제, 탐지 통제, 교정 통제가 있다. 이 외에 저지통제, 응용통제, 트랜잭션통제, 관리통제, 운영통제가 있다.
(3) 감사와 모니터링 - 감사는 IS 운영 전략이 조직의 운영 전략과 일치함을 보증하는 역할을 한다. IS 감사대상은 백업 통제, 프로세스 통제, 데이터센터 보안, 비상계획, 시스템 도입 및 개발 표준, 라이브러리 운영 절차가 있다. - 모니터링은 IS 설비에 영향을 미칠 수 있는 보안 사건을 식별하는 메커니즘과 도구, 기술을 포함한 개념으로, 문제 식별과 해결에 그 목적을 두고 있다. 모니터링을 위한 기술로는 침입 방지, 침투 테스트, 클리핑 레벨 설정을 통한 위반 분석이 있다.
(4) 위협과 취약성 - 위협은 자산의 손실을 발생시키는 원인이나 행위를 의미하며, 고의적이거나 우발적인 사건으로 발생시에 시스템의 손상을 일으켜 기밀성, 가용성, 무결성에 손상을 가져올 수 있다. 위협은 우발적 실수, 부적절한 행위, 의도적 공격이 포함된다. - 취약성은 위협이 이용 가능한 시스템상의 약점을 의미하며, 트래픽 분석을 통한 노출, 유지보수계정, 부팅이나 재부팅 등 IPL 취약성, Network address hijacking이 있다. - 위협과 취약성의 예를 들면 Oracle profile에서 사용하는 verify function은 사용자가 추론 가능한 암호 사용을 막아서 크랙할 가능성을 낮춰준다.
여기서 추론 가능한 암호를 사용하는 것은 취약성을 의미하며, 암호를 크랙하는 것은 위협이라고 볼 수 있다.

3. 재해 복구

(1) 재해복구 개요 - 재해복구는 각종 재해 및 위험요소에 의해 정보시스템이 중단됐을 때 이를

copyright 2021. 한국교육개발진흥원 All rights reserved.

정상으로 회복시키는 것을 의미한다. IT에서의 재해는 사전적 의미를 벗어나 지진, 태풍 등의 자연 재해 및 전쟁, 해킹, 사용자 실수 같은 내외부적 요인에 의한 장애, 그리고 시스템 결함, 기계적 오류, 관리정책 오류 등 다양한 사례를 포함한다.

(2) 재해복구 핵심용어 - 백업은 데이터 복구의 핵심 구성요소로, 데이터의 특정 시점 복사본을 만드는 것을 의미한다. 백업 데이터는 구조적/비구조적 데이터 모두일 수 있다. - 비즈니스 연속성은 ' 비즈니스 회복성 ' 이라고도 하며 광범위한 형태의 데이터 보호를 지칭한다. 데이터와 IT 서비스의 복원뿐만 아니라 프로세스와 절차도 포함한다. - 지속적 데이터 보호는 ' 실시간 백업 ' 이라고도 하며 모든 변경의 복사본을 자동 저장하여 IT 관리자가 어느 시점으로든 데이터를 복원할 수 있도록 하는 데이터 백업을 의미한다. - 고가용성은 재해 중 비즈니스를 지속하는 데 도움이 될 수 있는 기술의 특성이다. 페일오버해서 원래 시스템을 대체하나, 손상에 대비한 보호 기능은 제공하지 않는다. - 복제는 재해 발생 시 IT 관리자가 최신 데이터를 복원할 수 있도록 한 위치에서 다른 위치로 데이터를 복사하는 프로세스이다.

(3) 재해복구 요소 및 절차 - 재해복구의 요소 및 절차에는 복구 제도 마련, 복구 조직 구성, 복구 시스템 구축, 복구 계획 및 절차 수립, 데이터 백업, 백업 관리, 복구 테스트, 사후 점검 및 확인이 있다.

(4) 재해 복구 계획 수립 - 재해 복구 계획 수립을 위해 필요한 사항은 총 9가지로 내부 시스템 감사, 외부 공급 업체 확인, 취약점 이해, 카탈로그 시스템 및 서비스, 위험 경감, 재해복구계획 문서화, 직원교육, 재해복구계획 테스트, 업데이트가 있다.

(5) 재해 복구 시스템 유형 및 구현기술 - 재해 복구 시스템 유형은 구축 형태별, 운영 주체별, 복구 수준별로 나눌 수 있다. 구축 형태별로 구분하면 독자 구축, 공동 구축, 상호 구축이 있고, 운영 주체별로는 자체 운영, 공동 운영, 위탁 운영이 해당된다. 또한 복구 수준별로 보면 미러 사이트, 핫 사이트, 웜 사이트, 콜드 사이트가 있다. - 재해 복구 시스템 구현기술로는 하드웨어적 복제 방식, 소프트웨어적 복제 방식, 데이터 전송 방식, 동기 복제, 비동기 복제가 있다.

(6) 재해 복구 시스템 구축 - 재해 복구 시스템을 올바르게 구축하기 위해서는 일정 및 방안을 수립하고 재해 복구 및 체계를 구현한 후 테스트를 진행해야 한다. 마지막으로 운영관리 및 완료 보고를 실시한다.

(7) 재해 복구 시스템 구축 시 고려 사항 - 재해복구 시스템 구축시 복구시간목표와 복구시점목표를 고려해야 한다. - 복구시간목표는 업무별로 서비스 중단을 감내할 수 있는 시간을 정의하는 것이다. - 복구시간목표에 대한 정의가 완료되면 복구할 데이터 중요도 및 비용을 고려하여 복구시점목표를 정의해야 한다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[4차시]

1. 사회공학적 사이버 범죄 이해

(1) 사회공학적 해킹 - 시스템이 아닌 사람의 취약점을 공략하여 원하는 정보를 얻는 공격기법
사회공학 해킹의 종류 - 전화사기, 이메일 피싱, 우편물 등을 통한 개인정보 도난 등 특별한 기술 없이도 손쉽게 기본 정보를 얻어내는 비기술적 침입과 같은 방법 등

2. 사회공학 사이버 범죄 기법

(1) 인간 기반 사회공학 기법 - 직접적인 접근 - 도청 - 어깨너머로 훔쳐보기 - 휴지통 뒤지기
(2) 컴퓨터 기반 사회공학 기법 - 포렌식을 이용한 시스템 분석 - 악성 소프트웨어 전송 – 인터넷 이용 - 피싱 - 파밍 – 스미싱

3. 사회공학 사이버 범죄 사례와 대응책

(1) 교육과 훈련(education and training)을 통해 사용자에게 올바른 행동지침 제시 및 인식제고
(2) 시스템 차원의 대비책을 적절히 병행하여 사용자의 실수를 최소화 하는 체계 구축 필요
(3) 새로운 유형의 사회공학적 해킹에 대해 연구하고 신속하게 대처할 수 있는 정부차원의 체계구축

copyright 2021. 한국교육개발진흥원 All rights reserved.

[5차시]

1. 사이버 보안 프레임 워크의 이해

(1) 5가지 사이버 보안 프레임 워크 프로세스 - 파악/ 보호/ 탐지/ 대응/ 복구
(2) SOC의 중요성 - IoT 기기들을 활용한 대규모 DDoS 공격 - 가상화폐 채굴을 위한 악성코드 - 지능형지속위협 공격
(3) SOC의 목적 - 조직의 정보자산을 보호하여 비즈니스를 활성화 (4) SOC의 운영관리 - 조직의 내부 직원 - 외부 보안관제전문기업(MSSP: Managed Security Service Provider)

2. 사회공학 사이버 범죄 기법

(1) 인간 기반 사회공학 기법 - 직접적인 접근 - 도청 - 어깨너머로 훔쳐보기 - 휴지통 뒤지기
(2) 컴퓨터 기반 사회공학 기법 - 포렌식을 이용한 시스템 분석 - 악성 소프트웨어 전송 – 인터넷 이용 - 피싱 - 파밍 – 스미싱

3. 사회공학 사이버 범죄 사례와 대응책

(1) 교육과 훈련(education and training)을 통해 사용자에게 올바른 행동지침 제시 및 인식제고
(2) 시스템 차원의 대비책을 적절히 병행하여 사용자의 실수를 최소화 하는 체계 구축 필요
(3) 새로운 유형의 사회공학적 해킹에 대해 연구하고 신속하게 대처할 수 있는 정부차원의 체계구축

copyright 2021. 한국교육개발진흥원 All rights reserved.

[6차시]

1. 계정 관리의 이해

(1) 계정 - 시스템에 접근하는 가장 기본적인 방법으로 기본 구성 요소는 아이디와 패스워드
(2) 보안 인증방법 - 알고 있는 것, 가지고 있는 것, 자신의 모습, 위치하는 곳
(3) 운영체제 계정 관리 - 윈도우 : administrator/ 그 외 사용자 계정 - 유닉스 : root/ 그 외 사용자 계정
(4) 데이터베이스 계정 관리 - 관리자 계정(MS-SQL의 관리자 계정은 sa이고, 오라클의 관리자 계정은 sy와 system) / 일반 사용자 계정
(5) 응용 프로그램의 계정 관리 - FTP나 웹 서비스 같은 응용 프로그램은 고유의 계정을 가지거나 운영체제와 계정을 공유
(6) 네트워크 장비의 계정 관리 - 패스워드로 접근 가능
(7) 패스워드 - 부적절한 패스워드와 적절한 패스워드를 구분하여 안전한 패스워드 사용을 지향

2. 접근 제어의 이해

(1) 접근 제어 정책-임의 접근 제어 -강제 접근 제어 - 역할 기반 접근 제어 - 속성 기반 접근 제어
(2) 운영체제의 접근 제어 - 운영체제에 대한 접근 목적의 인터페이스를 결정한 다음 접근 제어 정책을 적용 - 접근 제어 정책은 기본적으로 IP를 통해 수행됨
(3) 데이터베이스의 접근 제어 - 접근 제어는 필수지만 모든 데이터베이스가 제공하는 것은 아님 - 설치된 방화벽을 통한 IP 접근 제어를 수행하는 MS-SQL의 윈도우 인증 모드 / 혼합 인증 모드(윈도우 인증+SQL 인증)
(4) 응용 프로그램의 접근 제어 - IIS(Internet Information Service)와 아파치는 IP에 대한 접근 제어를 제공 - SSL(Secure Socket Layer)은 클라이언트와 서버 인증서를 이용한 접근 제어
(5) 네트워크 장비 접근 제어 - IP에 대한 접근 제어 가능

3. 취약점 관리의 이해

(1) 취약점 관리(Vulnerability management) - 소프트웨어와 펌웨어에서 취약점을 인식, 분류, 개선 그리고 완화시키는 것의 주기적인 업무이며, 특히 컴퓨터 보안과 네트워크 보안에서 필수적인 부분 - Vulnerability scanner, 퍼즈 테스팅 등을 사용하여 취약점 발견 - 수정 : 패치 설치, 네트워크 보안 정책 변경, 소프트웨어 재설정, 사용자 교육 등 - 조직은 상시 취약점 관리 수행
(2) 패치 관리, 응용 프로그램의 고유 위험파악, 응용프로그램의 정보 수집 제한이 적절하게 이루어져야 함

copyright 2021. 한국교육개발진흥원 All rights reserved.

[7차시]

1. 연결 지향 프로토콜과 비연결 프로토콜

(1) 연결지향 프로토콜 - 통신 연결이 유지되는 것을 지향하는 프로토콜 - 비용이 비쌈 - TCP 프로토콜 - 이미 연결되어 있어 어떤 사람이 질의를 보냈는지 연결을 이용해 알 수 있음

(2) 비연결 프로토콜 - 연결을 유지하지 않는 프로토콜 - 비용이 저렴 - IP 프로토콜, HTTP 프로토콜 - 매번 새롭게 연결이 성립되기 때문에 필요한 경우 매 연결 시 자신이 누군지 알려줘야 함

2. OSI 7계층의 목적

OSI 7계층의 가장 중요한 목적은 2가지이다. 표준과 학습도구이다.

(1) 표준(호환성)을 통해 여러 장비 간의 호환성으로 비용 절감을 하고

(2) 학습도구는 정보통신기술 학습에 좋은 도구로 쓰이고 있다.

3. TCP/IP 4계층에 대해한 이해

(1) 4계층 응용 계층 -TCP/IP 기반의 응용 프로그램을 구분할 때 사용-프로토콜 : FTP, HTTP, Telnet, DNS, SMTP

(2) 3계층 전송 계층 -통신 노드 간의 연결을 제어하고, 자료의 송수신을 담당
–프로토콜 : TCP, UDP

(3) 2계층 인터넷 계층 -통신 노드 간의 IP패킷을 전송하는 기능 및 라우팅 기능 담당
-프로토콜 : IP, ARP, RARP, ICMP, OSPF

(4) 1계층 네트워크 액세스 계층 -CSMA/CD, MAC, LAN, X25, 패킷망, 위성 통신, 다이얼 모뎀 등 전송에 사용 -프로토콜 : Ehternet(이더넷), Token Ring, PPP

copyright 2021. 한국교육개발진흥원 All rights reserved.

[8차시]

1. 악성코드란

악성 소프트웨어, 유해한 소프트웨어(惡性-) 또는 맬웨어(영어: malicious software 또는 malware)는 컴퓨터, 서버, 클라이언트, 컴퓨터 네트워크에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭이다. 악의적인 목적을 위해 작성된 실행 가능한 코드의 통칭으로 자기 복제능력과 감염 대상 유무에 따라 바이러스, 웜, 트로이목마 등으로 분류된다.

2. 악성코드의 주요 감염경로

(1) 웹페이지를 검색할 때 홈페이지를 방문하거나 링크를 클릭하는 것만으로도 스파이웨어 쿠키와 같은 웹서핑 트레킹 도구가 사용자의 컴퓨터에 만들어질 수 있다.
(2) P2P 서비스를 이용할 때 카자, 당나귀와 같은 P2P 프로그램은 애드웨어를 내장하고 있어서 타켓 광고를 일방적으로 내보낼 수 있다.
(3) 어웨어를 사용할 때 플리쉬겟, 리얼미디어 등의 많은 쉐어웨어 프로그램은 그 자체에 애드웨어를 포함한다.
(4) 불법복제 프로그램을 사용할 때 불법복제 프로그램은 바이러스는 물론 각종 해킹 프로그램을 유포시키는 중요한 경로이다. 정상적인 프로그램에 악성코드를 은닉시키는 기법을 주로 이용한다.
(5) 해커가 직접 설치할 때 내부자에 의하여 직접 악성코드가 설치되는 경우이다. 불만을 가진 내부인이 회사의 기밀 사항을 빼내거나 퇴직 후 계속 시스템에 침입하기 위하여 사용된다.
자동 업데이트되는 과정에서 해당 기관들의 컴퓨터가 대량으로 악성코드에 감염되는 경우이다.
(6) 전자우편의 파일 또는 메신저 파일을 열 때 전자우편의 첨부 파일 또는 메신저로 전송한 파일을 열다가 감염된다.

3. 악성코드의 분류

악성코드는 악의적인 목적을 위해 작성된 실행 가능한 코드의 통칭으로 자기 복제능력과 감염 대상 유무에 따라 바이러스, 웜, 트로이목마 등으로 분류할 수 있다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[9차시]

1. 악성코드의 징후

(1) 속도 저하: 한 번에 많은 프로그램을 돌리거나 하드 드라이브에 공간이 부족할 경우, 윈도우 최신 업데이트가 설치되지 않은 경우이다.
(2) 브라우저 리디렉션(하이재킹) :특정 페이지를 열기 위해 링크를 클릭했을 때 해당 페이지가 아닌 다른 사이트로 리디렉션 한다.
(3) 팝업 : 브라우저를 실행한 것도 아닌데 팝업이 지속적으로 뜨거나, 브라우저 광고 차단을 사용 중임에도 팝업이 뜬다면 애드웨어 또는 스파이웨어에 감염된 것이다.
(4) 기본 홈페이지 변경 : 기본 홈페이지 설정을 아무리 바꿔도 다시 원래대로 돌아가고, 도구 모음 바가 삭제되지도 않는 경우이다.
(5) 자동 실행 파일 : PC 부팅 직후 브라우저나 파일을 열기까지 대기 시간이 길다면 자동 실행 파일을 점검한다.
(6) 응용프로그램 오류 Alert 메시지 : PC 부팅 시 메모리를 read 혹은 written 할 수 없다고 하는 Alert 창이 뜨거나, [확인] 버튼을 클릭해도 계속해서 뜨는 창이 뜬다면 악성파일이 응용프로그램 실행을 방해한다.

2. 악성코드 감염 위험 요소

(1) 보안 버그: 운영 체제, 웹 브라우저 및 브라우저 플러그인과 같은 소프트웨어에는 공격자가 악용할 수 있는 약점이 있다.
(2) 사용자 오류: 알 수 없는 소프트웨어에서 소프트웨어를 열거나 신뢰할 수 없는 하드웨어에서 컴퓨터를 부팅하면 심각한 위험을 초래한다.
(3) OS 공유: 네트워크상의 모든 컴퓨터에서 단일 운영 체제를 사용하면 Malware (맬웨어) 감염 위험이 증가 모든 컴퓨터가 동일한 OS에 있으면 하나의 웜이 모두 감염될 수 있다.

3. 악성코드 감염 예방

(1) 이메일에 첨부된 파일이나 링크는 함부로 열지 않는다. 모르는 주소로 수신된 메일 삭제하고, 첨부파일은 가급적 실행하지 말아야 한다. 특히 .exe 파일로 된 첨부파일은 경계하여야 한다.
(2) 기업/공공기관에 효과적인 보안 솔루션을 운용한다. 악성코드를 효과적으로 차단할 수 있는 보안 솔루션을 설치, 운용한다.
(3) 사이냅 문서뷰어로 미리보기 사이냅 문서뷰어는 악성코드 감염 예방뿐 아니라 변환 결과 암호화, 워터마크, URL 접근제한 등 다양한 보안 기능을 제공하여 기업의 문서보안 환경 구축에 효과적으로 적용될 수 있다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[10차시]

1. 바이러스의 감염경로

(1) 일반적인 경로는 불법복사, 컴퓨터 통신, 컴퓨터 공동 사용, LAN, 인터넷 등이 있다.
(2) 불법 복제한 소프트웨어 디스켓을 사용하거나, 여러 사람이 공동으로 사용하는 컴퓨터에서 작업하면 바이러스 감염의 가능성이 높아 디스켓 또는 프로그램에 감염된다.
(3) 감염된 디스켓이나 프로그램을 자신의 컴퓨터에서 사용하면 자신의 컴퓨터도 감염된다.
(4) 자료를 주고 받을 때 급속도로 바이러스가 확산되기도 한다.

2. 감염 부위에 따른 분류

(1) 부트 바이러스 : 컴퓨터가 처음 가동되면 하드디스크의 가장 처음 부분인 부트 섹터에 위치하는 프로그램이 가장 먼저 실행되는데, 이곳에 자리잡는 컴퓨터 바이러스를 부트 바이러스라고 한다. 대표적으로 브레인 바이러스와 지금까지도 많은 피해를 주고 있는 멍키 바이러스 및 감염 빈도가 높은 Anti-CMOS 등이 있다.
(2) 파일 바이러스로 실행 가능한 프로그램에 감염되는 바이러스를 말한다. 감염되는 대상은 확장자가 COM, EXE인 실행파일이 대부분이다. 국내에서 발견된 바이러스의 80% 정도가 파일 바이러스에 속할 정도로 가장 일반적인 바이러스 유형이다.
(3) 부트/파일 바이러스 부트 섹터와 파일에 모두 감염되는 바이러스로 대부분 크기가 크고 피해 정도가 크다.
(4) 매크로 바이러스: 새로운 파일 바이러스의 일종으로, 감염 대상이 실행 파일이 아니라 마이크로소프트사의 엑셀과 워드 프로그램에서 사용하는 문서 파일이다.

3. 컴퓨터 바이러스 감염 증상

(1) 빠른 전파력을 지닌 이메일 바이러스의 스팸메일화 : 초기의 이메일 바이러스는 비교적 간단한 형태의 제목, 본문, 첨부파일을 지닌 형태였으나, 클레즈 웜 변종의 경우, 매우 다양한 제목과 본문, 첨부파일명을 지니고 전파되어 일반 사용자들이 실제 메일과 구별하기가 어려웠고 메일 필터링 기능을 통한 예방에 한계가 있다.
(2) 백신 공격형 웜 증가 : 백신 관련 프로그램을 삭제 또는 그 기능을 중지하여 백신으로부터 자기 자신을 탐지 못하도록 하는 백신공격형 웜이 증가한다.
(3) 빠른 전파력과 무서운 파괴력을 지닌 웜 바이러스 출현 : 하나의 파일 안에 트로이목마나 웜 등이 포함된 복합형 웜 바이러스들이 생겨나고, 웜의 전파기능과 바이러스의 파괴력을 지니고 있다.
(4) 윈도우 취약점 공격형 웜 증가 : 바이러스 제작자들의 공격기법이 날로 지능화되고 제작기술이 고도화되면서, 애플리케이션 프로그램에 존재하는 취약점을 공격대상으로 하는 해킹기법의 공격형 웜들이 많이 나타나고 있으며, 특히 취약점을 많이 지니고 있는 윈도우시스템을 공격대상으로 하는 웜들이 많이 늘어나고 있다.
(5) 정보유출형 인터넷 웜의 지속화 : 시스템정보 혹은 엑셀이나 워드문서와 같은 것을 선택 후 자체 메일을 통하여 정보 유출하도록 하는 형태의 웜이 사라지지 않고 있다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[11차시]

1. 트로이 목마의 특징

(1) 트로이목마는 자료삭제·정보 탈취 등을 목적으로 사용되는 악성 프로그램으로, 해킹 기능을 가지고 있어 인터넷을 통해 감염된 컴퓨터의 정보를 외부로 유출하는 것이 특징이다.
(2) 트로이목마도 일종의 프로그램이므로 컴퓨터 바이러스와 마찬가지로 일반적인 프로그램이 수행하는 모든 일을 할 수 있다.
(3) 트로이목마 프로그램은 특정 파일을 지울 수 있으며, 최악의 경우 하드디스크를 포맷해버리는 것도 얼마든지 가능하다.
(4) 트로이목마는 자체적인 전파 기능을 가지고 있지 않지만, 현재 다수의 웹 해킹을 통해 악의적인 스크립트가 삽입된 웹페이지에 의해 전파한다.
(5) 트로이목마가 설치되면, 공격자는 시스템의 모든 제어권을 가진다.

2. 트로이 목마의 유형

(1) 침입 방법에 따른 분류로는 컴퓨터를 공격하는 방식이 있다. 백도어 트로이목마는 컴퓨터의 방어망에 해커가 침투할 수 있는 구멍을 뚫는다. 다운로더 트로이목마는 해커 사이트에서 더 악의적인 코드를 다운로드해 컴퓨터에 대한 장악력을 더 확대한다. 루트킷 트로이목마는 다른 공격자가 이용할 수 있는 숨겨진 해킹 툴킷을 설치한다.
(2) 침입 목적에 따른 분류로 설치된 후 하는 행동이다. 메일파인더는 사용자의 주소록을 훑어 스팸에 이용할 이메일 주소를 확보한다. DDoS 트로이목마는 컴퓨터를 탈취해 좀비화해서 다른 공격 목표에 대한 DDoS 공격에 이용한다. 일단 첫 침해가 이뤄지면 다양한 범주의 많은 악성코드 프로그램이 서로 비슷한 방식으로 실행된다.

3. 트로이 목마의 예방 및 대응

(1) 주로 사용하는 이메일에는 스팸 차단 기능을 설정하고, 신원이 불분명한 사람의 이메일은 아예 열지 않는 것이 좋으며 의심이 되면 해당인에게 연락을 해보거나 백신 프로그램으로 검사한 후 열어보는 것이 좋다.
(2) 불법 소프트웨어에는 트로이목마가 숨어 있을 수 있으니 정품 소프트웨어를 사용한다. 셰어웨어가 필요할 때는 믿을 만한 곳에서 다운로드하고, 불가피하게 P2P를 이용할 때는 반드시 백신 프로그램 등의 보안 제품으로 검사해야 한다.
(3) 백신 프로그램과 윈도는 항상 최신 버전을 유지할 수 있도록 업데이트에 신경 쓴다.
(4) MS 윈도 업데이트는 의심스러운 실행파일을 차단하거나 보안상의 취약점을 보완할 수 있으니, 자동으로 업데이트되도록 설정해 둔다.
(5) 인터넷 익스플로러도 최신 버전을 사용하되, 가능하면 보안 설정을 높게 유지한다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[12차시]

1. 웜의 정의 및 개념

웜은 1988년 유명 해커 모리스 웜에 의해 최초로 개발된 악성코드로, 인터넷 또는 네트워크를 통해서 전파되는 악성 프로그램이다. 윈도우 또는 응용 프로그램의 취약점을 이용하거나 이메일, 공유 폴더를 통해 전파되며, 공유 프로그램(P2P)를 이용하여 전파되기도 한다. 웜은 스스로 복제된다는 점에서는 바이러스와 비슷하지만, 숙주 프로그램이 필요하지 않고 스스로 전파되며 독립적을 실행된다는 점에서 차이가 있다.

2. 웜의 특성

(1) 복제능력이 매우 뛰어나 사용자의 이메일, 인스턴트 메신저 등의 주소록을 뒤지고 스스로를 첨부해 네트워크를 통해 퍼진다.
(2) 외국에서 발견된 지 몇 시간 만에 한국에서도 발견될 정도로 전염성이 강하다.
(3) 최근 등장한 웜들은 강력한 전염성을 무기로 네트워크 전반에 치명적인 타격을 입히기도 한다.

3. 웜의 유형

(1) MASS Mailer형 웜 자기 자신을 포함하는 대량 메일 발송을 통해 확산되는 웜이다. 제목이 없거나 특정 제목으로 전송되는 메일을 읽었을 때 감염되며, 시스템 내부에서 메일 주소를 수집하여 끊임없이 메일을 발송하는 형태이다. 대표적으로 베이글(Bagle), 넷스카이(Netsky), 두마루(Dumaru), 소빅(Sobig) 등이 있다.
(2) 시스템 공격형 웜 운영체제 고유의 취약점을 이용해 내부 정보를 파괴하거나 컴퓨터를 사용할 수 없는 상태로 만들거나, 혹은 외부의 공격자가 시스템 내부에 접속할 수 있도록 백도어를 설치하는 웜이다. 간단한 패스워드 크래킹 알고리즘을 포함하고 있어 패스워드가 취약한 시스템을 공격하는 웜도 있다. 대표적으로 아고봇(Agobot), 블래스터(Blaster.worm), 웰치아(Welchia) 등이 있다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[13차시]

1. 해킹의 개요

(1) 해커 - 과거: 정보는 자유롭게 공개되어야 한다는 이념을 추구 - 현재: 범죄자로서의 해커

(2) 해킹의 의미 - 넓은 의미: 해커들이 저지르는 모든 불법적인 행위들 - 좁은 의미: 정보시스템 전산망에서의 보안 침해사고를 발생시키는 행위들

(3) 해킹 피해 유형 - 비인가자의 컴퓨터 이용 - 디스크 자료 불법 열람, 삭제 및 변조 - 컴퓨터시스템 이상동작 유발 - 해킹경유지 이용 피해

(4) 해킹기법 - 사용자 도용, 버퍼오버플로우, 구성설정오류, 악성프로그램, 서비스거부공격, 이메일관련공격, 취약점정보수집, 사회공학기법

(5) 해킹 시나리오 - 정보수집→불법적인 컴퓨터 접근→root권한 획득→스니퍼 설치→뒷문프로그램 설치→구체적 피해 행위

(6) 해킹의 동향 - 전통적: 스캔공격, 서버 중심 공격 - 현재: 에이전트화, 분산화, 자동화, 은닉성

2. 국내 해킹 피해 현황

(1) Ramen Worm

(2) 1i0n Worm

(3) Adore Worm

(4) sadmind/IIS Worm

(5) Cheese Worm

(6) Code Red Worm

3. 해킹 예방 및 대응

(1) 해킹 예방법 - 안전한 컴퓨터 구성 및 운영 - 네트워크에서의 불법접근 방지 조치 – 사용자계정 및 패스워드의 안전 관리 - 파일시스템 안전관리 - 기록 점검 및 관리 - 올바른 네트워크 구성과 보안 관리

(2) 해킹 대응 방법 - 공격사이트 연락처 찾기 - 공격사이트와의 연락

(3) 해킹 시스템 복구 절차 - 침입으로부터의 복구 시스템 제어 회복 침입자가 변조한 파일을 복구하고 시스템 다시 설치 로그시 분석된 다른 기관이나 시스템 관리자에게 연락・체크 - 시스템 보안 작업 패치 설치 CERT 기술권고문 등 관련 자료 참고 해킹방지 보안 도구들을 설치 로그시스템을 다시 운영 시작 네트워크 방화벽 시스템 설치 및 운영 유닉스 보안 구성지침에 따라 보안상태 검토 사용자 패스워드 교체 네트워크 재접속 및 운영 시작

copyright 2021. 한국교육개발진흥원 All rights reserved.

[14차시]

1. 들어가기

(1) 방화벽 시스템 - 내부망과 외부망 사이에서 망간 정보의 흐름을 안전하게 통제하는 시스템으로써 비인가자가 내부 정보통신망에 연결되어 있는 정보자원에 불법적으로 접근하지 못하도록 신분확인, 접근통제 등 보안관리기능을 지원하는 소프트웨어나 하드웨어를 말한다.

(2) 방화벽의 주요기능 - 접근통제, 사용자 인증, 로깅, 암호화

2. 기술적 구성체계

(1) 신분확인 - 침입차단시스템에 접근하는 관리자 및 사용자의 신분을 증명하는 기능

(2) 접근통제 - 주체가 침입차단시스템을 통하여 객체에 접근을 시도하는 경우 미리 정해진 접근통제규칙을 적용하여 접근을 통제하는 기능

(3) 무결성 - 침입차단시스템의 중요한 데이터나 침입차단시스템을 통하여 전송되는 데이터에 변경이 발생하는 경우 이를 확인하는 기능

(4) 비밀성 - 침입차단시스템을 통하여 전송되는 데이터가 인가되지 않은 사용자에게 노출되는 경우 그 내용이 알려지는 것을 방지하는 기능

(5) 감사기록 및 추적 - 침입차단시스템을 통하여 이루어지는 보안관련 활동 및 사건을 기록 조사하고 침입사건의 발생을 탐지하는 기능

(6) 보안관리 - 관리자가 침입차단시스템의 보안관련 데이터와 보안기능을 안전하게 유지하기 위하여 수행하는 기능

3. 운영방법

(1) 패킷 필터링 방식

(2) 서킷 게이트웨이 방식

(3) 응용(어플리케이션) 게이트웨이 방식

(4) 하이브리드 방식

4. 문제점

(1) 제한된 서비스

(2) 백도어 위협

(3) 내부 사용자에 의한 보안 침해

(4) 기타 문제점 - WWW(World Wide Web), gopher, WAIS(Wide Area Information Servers) - MBONE(Multicase Backbone) - 바이러스 - 데이터 처리 - 보안 기능의 집중화

5. 보안대책 수립

(1) 네트워크 접근 정책 - 성공적인 구현을 위해서는 실질적이고 완벽해야 함

- 방화벽 설치 전 배포되어야 함

(2) 방화벽 시스템 설계 정책 - 거부되지 않은 모든 서비스는 허가함

- 허가되지 않은 모든 서비스는 거부함

(3) 방화벽 서비스 정책의 고려사항 - 조직에서 사용하고자 하는 인터넷 서비스

- 서비스를 사용하고자 하는 장소, 가정에서의 다이얼 인 접속, 또는 원격지에서 인터넷 접속 – 암 호 화 나 다이얼 인의 지원 등 추가적인 요구 - 이러한 서비스나 접속과 관련된 위험 - 보안에 소요 되는 경비와 네트워크 가용성에 미치는 영향 - 보안과 가용성에 대한 고려 : 위험부담과 보안 비용 이 큰 서비스의 보안

copyright 2021. 한국교육개발진흥원 All rights reserved.

[15차시]

1. 들어가기

(1) 침입 - 침입을 정보 접근, 정보 조작, 시스템 무기력화 등에 대한 고의적이면서도 불법적인 시도의 잠재 가능성 - 보편적으로 정의하면 컴퓨터 자원의 무결성, 비밀성, 가용성을 저해하는 일련의 행위들의 집합을 의미하며, 컴퓨터 시스템의 보안정책을 파괴하는 행위

(2) 침입탐지 시스템의 목적 - 외부침입자뿐만 아니라 내부 사용자의 불법적인 사용, 남용, 오용행위를 탐지

(3) 침입탐지 시스템의 분류 - Kumar 분류 - COAST 분류 - ICSA IDSC((Intrusion Detection Systems Consortium) 분류 - IBM Zurich Research Lab. 분류 - ISO/IEC JTC1/SC27/WG1 분류

2. 기술적 구성체계

(1) 침입탐지 시스템의 일반모델의 모듈 - evenct generator, activity porfile, rule set

(2) ISO/IEC 침입탐지시스템 모델의 모듈 - Event Detection, Analyzer, Response, Data Storage

(3) IETF 침입탐지시스템 모델의 모듈 - Sensor, Analyzer, Manager

3. 운영방법

(1) 침입탐지 방법론 - 오용탐지 - 비정상행위 탐지

(2) 침입탐지 대응 - 수동적 대응과 능동적 대응

(3) 침입탐지 시스템의 보안기능 - 축약감사데이터 생성 - 보안위반 분석 - 보안감사 대응 - 신분확인 - 데이터 보호 - 보안감사 - 보안관리 - 보안기능의 보호

copyright 2021. 한국교육개발진흥원 All rights reserved.

[16차시]

1. 정보보호기술의 개념

(1) 정보 보안 위협 요소 - 도청, 신분위장, 전송메세지 내용, 부당목적s/w은닉

(2) 정보보호 - 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 강구하는 것 - 일반적으로 정보보호는 정보시스템 내에 보관되거나 통신망을 통하여 전송되는 정보를 내외부의 각종 위협으로부터 안전하게 보호하여 정보시스템의 가용성을 보장하는 것

(3) 정보보호 대책을 위한 구성요소 - 관리적 보안대책/ 물리적 보안대책/ 기술적 보안대책

(4) 기술적 정보보호 대책 - 침입차단시스템, 침입탐지시스템 - 인증시스템 - 공개 키 기반구조와 인증기관 - 바이러스 백신 - VPN - 서버 접근통제 시스템 - 취약성 및 위험분석 도구 – 웹사이트 보안 및 메일 보안 제품 - 통합 보안관리 시스템

2. 네트워크 모니터링 기술

(1) 네트워크 모니터링 원리 - BSD Pakcet Filter(BPF)

(2) 패킷 수집 라이브러리 – libcap

(3) PCAP 주요 함수 - pcap_lookupdev() / pcap_open_live() / pcap_snapshot() / pcap_lookupnet() / pcap_datalink() / pcap_compile() / pcap_setfilter() / pcap_loop() / Pcap_dispatch() / bpf_filter()

(4) 네트워크 모니터링 도구 - Netlog. TCPDUMP

(5) TCP packets의 비정상 플래그의 조합 - SYN FIN - SYN FIN PSH, SYN FIN RST, SYN FIN RST PSH와 같은 SYN FIN들의 다양한 변형들이 존재 - Nul l패킷

(6) 비정상 패킷 분석 - UDP Packets - ICMP Packets - IP 분할

copyright 2021. 한국교육개발진흥원 All rights reserved.

[17차시]

1. DoS의 정의

DOS란 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다. 특정 서버에게 수 많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함된다.

2. DDoS[Distributed Denial of Service]란

DDoS[Distributed Denial of Service]란 해킹 방식의 하나로서 여러 대의 공격자를 분산 배치하여 동시에 ' 서비스 거부 공격(Denial of Service attack ; DoS) ' 을 함으로써 시스템이 더 이상 정상적 서비스를 제공할 수 없도록 만드는 것이다.

3. DDoS공격을 방지하는 방법

(1) 잦은 충돌, 긴 로드 시간, 이상한 오류 메시지등 컴퓨터가 이상하게 작동한다고 생각되면 조치를 취하는 것이 가장 좋다.

(2) Windows, Mac, 및 Linux 용으로 권장되는 신뢰할 수 있는 바이러스 백신 소프트웨어를 설치하고 정기적인 바이러스 검색을 실행해야 한다.

(3) 풀 스캔에서 컴퓨터에 멀웨어가 있는지 알려줄 수 있어야 한다. 대부분의 경우 바이러스 백신은 바이러스를 제거할 수 있다. 빠른 온라인 바이러스 스캔도 역시 해롭지 않다.

(4) 이메일 첨부 파일이나 웹 파일에 대하여 그것이 무엇이고 누가 보냈는지 모르면 다운로드하지 않는다.

(5) 이러한 피싱 시도는 사용자가 모르게 장치에 멀웨어를 설치할 수 있다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[18차시]

1. 지능형 지속공격이란

(1) 지능형 지속 공격(advanced persistent threat)은 잠행적이고 지속적인 컴퓨터 해킹 프로세스들의 집합공격자가 악성코드를 심은 이메일을 보내 사용자가 열도록 하는 방식으로 PC를 감염시킨다.
(2) 감염된 좀비 PC가 증가하면서 서버가 파괴되도록 만들고, 내부 시스템에 잠복한 악성코드들이 데이터베이스 정보를 빼낸다.
(3) 지능형 지속공격(APT)은 조직이나 기업을 표적으로 정한 뒤 장기간에 걸쳐 다양한 수단을 총동원하는 지능적 해킹 방식이다.
(4) APT는 일반적으로 해킹 표적의 관심을 끌만한 내용의 이메일과 첨부파일을 끊임없이 보내, 사용자가 호기심에 이를 열어보거나 내려받는 순간 PC에 악성코드를 감염시킨다.
(5) 해커는 감염된 PC와 연결된 다른 PC를 차례로 감염시켜 전체 컴퓨터망을 해킹한다.

2. APT 공격 현황

(1) APT 공격의 주요 목표가 되는 대상은 아래 그림과 같이 정부기관, 사회 기간산업시설, 금융기업, 정보통신기업, 제조 기업 등으로 볼 수 있다. 이런 대상들이 공격을 받아 중요 데이터가 탈취 된다면 해당 기관이나 기업은 물론이고 사회적으로도 큰 문제가 발생 될 수 있을 것이다.
(2) 산업별 공격 노출률 및 유입 경로 산업별 APT 공격의 노출률을 살펴보면, 통신 산업과 정부기관이 상위 1,2위로 가장 많이 노출된 산업으로 나오고 있고 그 뒤를 이어 교육 산업, 첨단기술 사업, 금융 서비스업 등이 따라오고 있다. 이를 통해 통신, 첨단기술 산업, 정부기관 그리고 금융 서비스업이 공격의 주요 목표가 되는 것을 알 수 있다. 그리고 이런 목표들을 공격하기 위해 공격 파일을 유입시키는 경로는 압도적으로 이메일을 통한 공격이 많은 것을 볼 수 있다.

3. APT 대응방안

(1) 엔드포인트(End-Point): 보안 해커 입장에서 보면 엔드포인트는 내부망 침투를 위한 교두보를 만들어야 할 필수요소라고 할 수 있다. 엔드포인트에서 악성코드를 감염시키는 작업으로부터 공격이 시작되므로 외부 인터페이스 통제부터 백신, 방화벽, 악성코드 방어 솔루션 등을 사용하여 발생 가능성을 최소화하여야 한다.
(2) 네트워크 보안: 네트워크 단에서 악성코드를 분석하는 것이다. 내부로 유입되는 파일들을 가상환경에서 실행 시켜 실제 행위를 분석한 뒤 이상 유무를 점검하여 피해를 최소화하는 방법이다. 물리적인 장치를 통해 유입되는 악성코드가 아니라면 네트워크망을 타고 내부로 유입되는 악성코드를 탐지하고 차단하는데 효과적이다.
(3) 서버보안: 보다 강력한 접근 통제를 위해 2-Factor & 2-Channel 등의 인증을 통해 권한이 있다 해도 또 한 번의 인증을 거쳐야만 접근 및 명령을 할 수 있도록 통제한다. 또 SIEM같은 시스템을 이용하여 정보시스템들의 이벤트, 로그, 감사 정보 등을 모아 장시간 심층 분석을 통해 빠른 탐지 및 대응을 한다.
(4) 엔드포인트, 네트워크 보안, 서버 보안과 같이 종합적인 보안 인프라를 구축하여 공격에 대응하는 것도 굉장히 중요하다. 하지만 더 중요한 건 사용자의 보안인식 강화이다. 모든 공격의 시작은 사용자의 부주의한 활동에서부터 시작되는 만큼 주기적인 보안교육 및 공격자가 사용하는 방법을 실제로 이용한 모의 훈련까지 한다면 굉장히 좋은 효과가 있다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[19차시]

1. 랜섬웨어의 개요

(1) 랜섬웨어(Ransomware)란? -Ransom(몸값) + Software(소프트웨어)의 합성어로, 시스템을 잠그거나 이용자의 데이터를 암호화한 뒤, 복구를 위한 금전을 요구하는 악성코드 프로그램이다. -기간 내 요구사항을 처리하지 않으면 금액이 증가하고, 암호화된 데이터가 사용 불가 또는 삭제된다. -감염 후, 공유 폴더 및 기타 접근 가능한 시스템으로 확산 시도한다.

(2) 랜섬웨어 공격 절차 -감염 경로에 접속-PC로 랜섬웨어 다운로드 및 실행-암호화 대상 검색 및 암호화-복호화 대가 요구

(3) 랜섬웨어의 감염 경로 - 랜섬웨어가 유포 중인 홈페이지 방문하여 감염된다. - 이메일 및 SNS 첨부 파일 다운로드 및 링크 실행 시 감염된다. - 웜(자가전파)형태로 컴퓨터 부팅 시 자동 감염된다. - 타깃형(APT) 공격으로 서버 침투 및 악성코드를 설치해 감염시킨다.

(4) 랜섬웨어의 진화

① 컴퓨터 화면을 잠그거나, 인터넷 검색을 제한하는 등 데이터에 대한 접근 차단 방식의 차단형 랜섬웨어

② 데이터 암호화 후 몸값 입금 정보 제공, 복구하기 위한 도구와 복호키 제공하는 비밀형(암호화) 랜섬웨어

③ 높은 수익률을 위해 회사나 병원 등이 가지고 있는 주요 정보를 암호화하는 맞춤형 랜섬웨어

2. 랜섬웨어의 유형

주요 랜섬웨어의 유형 -로키(Locky) : 사용자가 인지하지 못하는 네트워크 경로를 찾아 데이터를 암호화한다. -테슬라크립트(TeslaCrypt) : 200MB이상의 파일은 손상시키지 않고 키를 공개하여 복호화 가능하다. -케르베르(Cerber) : 음성을 통해 암호화 사실을 전달한다. -비너스락커(Venus Locker) : 감염사실을 알리기 위해 바탕화면 변경하고 모든 폴더에 랜섬노트 생성한다. -워너크라이(WannaCry) : 특정 도메인 접속 성공 시 미동작하는 킬스위치 기능을 보유하고 있다. -에레버스(Erebus) : 감염사실을 알리기 위해 모든 폴더에 랜섬노트를 생성한다. -크립토락커(CryptoLocker) : 시스템 자체 백업본 삭제 후 동작한다. -크립토월(Cryptowall) : 감염 확장자 변조 없고 파일의 고유 서명 값을 위변조한다. -올크라이(AllCry) : 네트워크 연결 시 악성행위 동작하며, 감염 정보를 알리기 위해 다국어를 지원한다. -크립트XXX(CryptXXX) : 브라우저, 메일, 쿠키, ftp 계정 등 사용자 정보를 탈취한다. -배드래빗(Bad Rabbit) : Windows SMB 취약점에 의해 네트워크를 통해 전파하며 MBR 변조를 통해 운영체제 부팅이 불가하다. -매그니버(Magniber) : 모든 폴더에 한국어로 작성된 랜섬노트를 생성한다. -페트야(Petya) : MBR 변조로 인한 운영체제 부팅이 불가하다.

3. 랜섬웨어 피해 사례

랜섬웨어 피해 사례 - 전세계를 강타한 워너크라이(WannaCry) 랜섬웨어 ('17.5) - 국내 호스팅 사를 타겟으로 한 에레버스(Erebus) 랜섬웨어 ('17.6) - 우크라이나 정부를 타겟으로 한 페트야(Petya) 랜섬웨어 ('17.6) - 한국을 타겟으로 한 올크라이(AllCry), 마이랜섬 랜섬웨어 ('17.10)

4. 랜섬웨어 사전 예방

랜섬웨어 피해 예방 수칙 -모든 소프트웨어는 최신 버전으로 업데이트하여 사용한다. -백신 소프트웨어를 설치하고, 최신 버전으로 업데이트한다. -출처가 불명확한 이메일과 웹사이트 주소 URL은 실행하지 않는다. -파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의해야 한다. -PC내 중요 자료

copyright 2021. 한국교육개발진흥원 All rights reserved.

는 정기적으로 백업한다. 2.기업환경을 고려한 예방수칙

(1) 랜섬웨어 감염을 최소화하는 예방법 안내 -시스템 보호환경을 구축한다. / 취약점 관리 및 패치한다. / 실행코드를 제어한다. / 웹 브라우저 트래픽을 필터링한다, / 이동식 매체 접근을 통제한다. / 스팸메일을 차단한다.

(2) 랜섬웨어 공격 제한 방법 -이메일 및 웹 브라우저 사용을 주의하고 공유 네트워크 드라이브에 대한 사용권한 접근을 통제한다. -정기적인 데이터 백업에 대한 지침을 제공하고 백업 자료에 대해 실전 복구 테스트를 실시한다.

(3) 중요한 데이터 백업하기 -백업에 사용하는 장비는 매체 백업 시에만 연결한다. -필요 시에는 한 번만 저장 가능한 DVD 등의 매체를 이용한다, -백업에 대한 정확성은 정기적으로 확인한다. -운영체제에서 제공하는 백업 기능 등을 사용한다.

(4) 사이버 위생 수칙 -운영체제, 브라우저, 백신 등 주요 프로그램의 패치를 지속적이고 신속하게 한다. -정상 유통 채널이 아닌 파일 공유사이트 등을 사용하지 않는다. -SNS, 이메일로 송부된 링크는 다른 채널로 확인하기 전에 열람하지 않는다. -첨부파일은 반드시 백신으로 검사한 후 열람한다. -사용자의 비밀번호는 복잡하게 설정하고, 잘 관리해야 한다. -중요 자료는 정기적으로 분리된 저장매체에 백업한다.

copyright 2021. 한국교육개발진흥원 All rights reserved.

[20차시]

1. 랜섬웨어 감염 시 대응절차

(1) 랜섬웨어에 감염되었다면? - 백업장치, 동기화된 다른 기기, 이메일, 제3자 등에서 대체할 수 있는 파일이 있는지 확인한다. - 공개된 랜섬웨어 복구 정보를 이용한다. - 몸값을 지불할지 선택한다. - 대행업체의 도움을 받을 것인지 선택한다.

(2) 감영경로별 대응 방안 - 지속적이고 신속한 패치 및 위험해 보이는 웹사이트 방문을 자제한다. - 파일 공유사이트 등을 아예 이용하지 않는다. - 지인으로 위장해 링크를 보내올 경우 다른 채널을 통해 확인 후 열람한다. - 메일 첨부 파일은 독립된 환경에서만 열람 또는 백신소프트웨어로 사전검사를 한 후 열람한다. - 신뢰된 기기를 이용할 때도 사용자의 접속 계정, 비밀번호를 위임하지 말고 관리한다.

(3) 증상 확인하기 - 파일의 사용이 불가능하다. - 파일 확장자가 변경된다. - 부팅이 불가능하다. - 바탕화면이 변경 되고 감염 알림 창이 열린다. **피해 최소화를 위한 긴급 조치 - 외부 저장장치 및 네트워크 연결을 해제한다. - PC 전원을 유지한다. - 네트워크를 차단한다. - 복구 방법을 확인한다.

(4) 증거 남기고 신고하기 - 감염창과 암호화 된 파일 화면 캡쳐 및 저장, 신고기관에 제출한다.

(5) 데이터 복구하기 - 암호화되지 않은 PC 또는 이동식 저장장치(USB)에 데이터를 백업한다. - PC 포맷 및 운영체제 재설치, SW 최신 보안 업데이트한다. - 기존 백업매체 연결 및 데이터를 복구한다. - 랜섬웨어 복구도구 활용한다.

2. 업종별 랜섬웨어 감염 가능 시나리오

(1) 중소기업, 무역업체 - 인사담당자에게 채용 문의 피싱 메일을 송부하여 감염시킨다. - 이메일 무역사기와 랜섬웨어가 결합하여 송장이나 계좌번호 변경 안내 메일을 송부하여 감염시킨다. - 취약한 회사 홈페이지를 대상으로 관리자 권한 탈취 및 중요 자료에 접근하여 서버에서 직접 랜섬웨어를 실행한다.

(2) 저작권업체, 병원 - 해커의 맞춤형 공격으로 민감정보를 암호화한다. - 내부 직원의 인터넷 서핑 중 감염이 된다.

(3) 금융기관 - 단말 PC의 랜섬웨어 감염이 되는 경우이다. - 홈페이지가 악성코드 유포지로 이용되는 경우이다.

(4) 온라인업체 - 온라인 배너 광고를 통해 랜섬웨어를 유포한다. - 온라인 게시판을 통해 랜섬웨어를 유포한다.

3. 랜섬웨어 유포 경로 별 주요 사례

(1) 첨부파일에 문서, 이미지 등으로 위장한 악성코드를 첨부한 피싱 이메일로 랜섬웨어 실행을 유도한다.

(2) 악성코드에 감염된 페이지에 접속만으로 랜섬웨어에 자동으로 감염된다.

(3) 토렌드, 파일공유 사이트 등을 이용한 파일 다운로드를 통해 감염된다.

(4) 운영체제의 취약점을 이용해서 인터넷 연결만으로도 랜섬웨어에 감염되는 워너크라이가 발생했다.

(5) SNS의 단축 URL을 통해 유포된 사례가 있다.

4. 랜섬웨어 주요 피해 사례

(1) 2015년 - 4월 21일 새벽, '클리앙'의 광고 서버가 해킹되어 랜섬웨어가 배포됐다. - 4월 22일에는 'seeko', '디시인사이드'의 광고 서버가 해킹되어 랜섬웨어의 배포지가 됐다. - 10월 중순부터 모

copyright 2021. 한국교육개발진흥원 All rights reserved.

든 파일의 확장자 명을 cc나 ccc로 바꾸는 'ccc바이러스' 랜섬웨어가 유행했다. - 12월 5일에는 일본에서 시작된 걸로 보이는 통칭 ' VVV ' 랜섬웨어가 기승했다.
(2) 2016년 - 3월 ~ 4월 천리안 메일 계정으로 랜섬웨어가 심어진 스팸 메일이 무차별적으로 살포됐다. → Invoice(송장), payment, flight plan 등으로 시작하는 제목의 나에게 보낸 메일로 위장했다. - 3월, 맥에서 처음 구동되는 랜섬웨어 발견됐다. - 6월 5일 오전 중에 확장자명 .crypz 형식의 랜섬웨어가 발견됐다. - 7월 20일 윈도우 바로 가기 파일(.lnk) 형태의 랜섬웨어가 발견됐다. → 암호화된 파일 확장자 뒤에 '.vault' 추가된다.
(3) 2017년 - 5월 12일에 전세계를 강타한 워너크라이(WannaCry) 랜섬웨어가 발생했다. - 6월 8일경 중국에서 Lycorisradiata라는 신종 모바일 랜섬웨어가 발견됐다. - 6월 10일경 국내 유명 호스팅 업체 ' 인터넷나야나 ' 에 랜섬웨어의 공격을 당했다. - 6월 27일에 우크라이나를 공격한 ' 낫페트야 ' 가 전 세계로 확산됐다. - 8월 10일에는 ' 역사상 최악의 랜섬웨어 ' 라고 하는 '스캐럽'이 국내에서 발견됐다. - 11월 4일에 확장자를 .yjnowl로 바꾸는 랜섬웨어가 등장했다.
(4) 2018년 - 유튜브의 동영상을 내려받거나 MP3로 추출하는 웹사이트 'Convert2mp3'가 CrySis 랜섬웨어에 감염됐다. - 2월부터 기업 내 인트라넷을 타깃으로 Java 설치 파일로 위장한 랜섬웨어가 기승했다.
(5) 랜섬웨어 피해 한국 1위 - 대기업과 공공기관들도 주요 공격 대상으로 중요한 시스템과 데이터, 브랜드 네임때문에 돈을 뜯어내기가 용이하다.

5. 랜섬웨어 종류 및 특징

(1) AllCry 랜섬웨어 - 감염 파일 확장자를 '.allcry'로 변경하고 랜섬노트 파일 생성한다.
(2) CERBER 랜섬웨어 - 4자리의 '임의의 숫자 또는 영문자'로 파일 확장자를 변경한다.
(PC마다 확장자가 다름)
(3) DMA Locker 랜섬웨어 - 시간(96h)이 지나면 복호화 비용 증가하고, 파일 확장자 변경은 없다.
(4) Erebus 랜섬웨어 - '.ecrypt'로 파일 확장자를 변경한다.
(5) GlobeImposter 랜섬웨어 - '[i-absolutus@bigmir.net].rose'로 파일 확장자를 변경한다.
(6) Jigsaw 랜섬웨어 - '.lost, .fun, .kkk, .btc, .gws'로 파일 확장자를 변경한다.
(7) Kamil 랜섬웨어 - 일부 파일은 '.lock'로 파일 확장자를 변경하고, - 대부분 확장자 변경이 없다.
(8) Locky(diablo6) 랜섬웨어 - 'diablo6'로 파일 확장자를 변경한다.
(9) Locky(asasin) 랜섬웨어 - 'asasin'로 파일 확장자를 변경한다.
(10) Matrix 랜섬웨어 - '.matrix, .b10ckedl'으로 파일 확장자를 변경하고, 최근에는 파일확장자를 변경하지 않고 암호화를 진행한다.
(11) Magniber(MyRansom) 랜섬웨어 - - '.kgpvwnr, .ihsdj'로 파일 확장자를 변경한다.
(12) Spora 랜섬웨어 - 파일명, 파일 확장자 변조가 없다.
(13) SyncCrypt 랜섬웨어 - '.kk'로 파일 확장자를 변경한다.
(14) TechSupportScam 랜섬웨어 - 심각한 윈도우즈 오류가 나타난 것처럼 위장하며, 재부팅 후 PC 정상적으로 사용 가능하다.
(15) VenusLocker 랜섬웨어 - '.venus, .venusLfS, .venusLf' 등 "venus" 문자열이 포함된 파일 확장자로 변경한다.
(16) WannaCry 랜섬웨어 - 일정 시간이 지나면 가상통화 비용이 증가하며, 추가 시간 이후에는 복구 불가능하다, '.WNCRYT, .WNCRY'로 파일 확장자를 변경한다.

copyright 2021. 한국교육개발진흥원 All rights reserved.