수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

평범한 회사와 직장인을 위한 정보 보안 기본서

1차시 - 정보 보호와 정보 보안의 개념

▶ 정보 보안의 특성

정보 보안은 현대 사회에서 매우 중요한 문제로 부상하고 있습니다. 하지만 정보 보안에 대한 대책을 설치할 때 그 효과를 완전히 확신하기는 어렵습니다. 왜냐하면 보안 대책이 모든 가능한 위협으로부터 시스템을 완전히 보호할 수 있는 것은 아니기 때문입니다. 100% 완벽한 정보 보안은 존재하지 않습니다. 공격자들은 시스템의 취약점을 이용하여 보안을 뚫을 수 있으며, 새로운 위협이나 기술적인 발전에 따라 보안 대책이 무력화될 수 있습니다.

따라서 정보 보안 대책의 효과성은 실패율에 의해 측정됩니다. 즉, 공격이나 침입 시도가 성공적으로 막히는 비율이 얼마나 높은지를 보고 대책의 효과를 평가합니다. 이러한 관점에서, 정보 보안은 지속적인 프로세스이며 완벽한 해결책은 없습니다.

여러 가지 정보 보안 대책을 동시에 사용하는 것이 바람직합니다. 하나의 대책만으로는 시스템을 완전히 보호할 수 없으며, 다양한 측면에서의 보안 대책들이 서로 보완하여 시스템의 안전성을 높일 수 있습니다. 예를 들어, 방화벽과 침입 탐지 시스템(IDS)을 함께 사용하면 외부 공격을 막는 데에 보다 효과적일 수 있습니다. 이러한 다층적인 보안 체계는 시스템의 취약점을 최소화하고 위험을 감소시키는 데에 도움이 됩니다.

▶ 암호화

암호화는 정보를 보호하기 위해 사용되는 중요한 보안 기술 중 하나입니다. 이러한 기술에는 다양한 방법과 수단이 있습니다.

첫째, 복잡한 비밀번호 설정은 일반적으로 사용자 인증을 위해 가장 널리 사용되는 방법 중 하나입니다. 강력한 암호는 길이가 길고 다양한 문자, 숫자, 특수 문자를 포함하는 것이 좋습니다. 이는 무차별 대입 공격 등의 공격으로부터 보호하기 위한 것입니다.

둘째, 생체 정보인 지문 및 홍채를 사용한 인증도 일반적으로 사용되고 있습니다. 이러한 생체 인식 기술은 개인의 고유한 생체적 특성을 활용하여 접근을 제어하고 보안을 강화하는 데 사용됩니다. 지문 및 홍채 인식은 비밀번호보다 보안성이 높고 편리하게 사용할 수 있습니다.

마지막, 암호화 기술은 데이터를 안전하게 전송하고 저장하기 위해 사용됩니다. 데이터를 변환하여 외부에서 볼 수 없는 형태로 만드는 것을 의미합니다. 암호화된 데이터는 해독 키가 없는 한 읽을 수 없으므로 정보 유출을 방지하고 데이터의 무결성을 보장하는 데 중요한 역할을 하고, 보안 카드는 물리적 보안 기술로, 카드에 내장된 칩과 PIN 번호를 사용하여 접근을 제어합니다. 이는 암호화 기술과는 다르며, 주로 물리적인 접근 통제를 위해 사용됩니다.

.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

2차시 - 공짜 와이파이를 믿지 마세요

▶ 공공 와이파의 대두되는 문제점

공공 와이파이는 편리성과 접근 용이성을 제공하여 많은 이용자들에게 인기가 있지만, 이러한 편의성은 보안적인 측면에서 다양한 문제점을 내포하고 있습니다.

첫째로, 보안 취약점은 공공 와이파이에서 가장 큰 문제 중 하나입니다. 보안 환경을 강화하더라도 여전히 해커나 악의적인 사용자들이 존재하며, 공공 와이파이는 이들에게 공격의 목표가 될 수 있습니다. 암호화되지 않은 공개 네트워크이기 때문에 개인 정보가 유출될 위험이 큽니다.

둘째로, 공공 와이파이는 편의와 공공성을 추구하는 대조적인 측면을 가지고 있습니다. 사용자들은 휴대폰이나 노트북 등을 이용하여 어디서든 인터넷에 접속할 수 있어 편리하지만, 이는 동시에 보안의 취약성을 증가시키는 요인이 될 수 있습니다. 개인 정보나 중요한 데이터를 이용하는 경우, 보안이 우선시되어야 하지만 공공 와이파이의 보안 수준은 그렇게 높지 않습니다.

셋째로, 공공 와이파이는 개방된 환경으로 인해 보안 위협에 노출될 여지가 매우 큽니다. 와이파이를 통해 네트워크에 접속하는 사용자들은 불특정 다수이며, 이는 해커들에게 쉬운 목표가 될 수 있습니다. 해커들은 중요한 정보를 탈취하거나 악의적인 코드를 주입하여 공격할 수 있습니다.

이러한 문제점들을 해결하기 위해서는 공공 와이파이를 사용할 때 추가적인 보안 조치를 취해야 합니다. 예를 들어, VPN(Virtual Private Network)을 사용하거나 암호화된 통신을 이용하여 개인 정보를 안전하게 보호할 수 있습니다. 또한, 공공 와이파이를 사용할 때에는 인터넷 뱅킹이나 개인 정보에 접근하는 행위를 피하는 것이 중요합니다. 이러한 조치들을 통해 공공 와이파이를 보다 안전하게 이용할 수 있습니다.

▶ 이블 트윈

이블 트윈은 악의적인 공격자들이 합법적인 네트워크로 위장하여 로그인한 사용자들을 속이고, 그들의 비밀번호나 개인정보를 훔치기 위해 설치하는 무선 네트워크입니다. 이러한 공격은 사용자들이 신뢰하는 네트워크에 연결될 때 발생할 수 있으며, 공격자는 이를 통해 사용자들의 민감한 정보를 탈취하거나 악용할 수 있습니다. 이러한 공격을 피하기 위해서는 안전한 네트워크에 연결하는 것이 중요하며, 공공 와이파이를 사용할 때에는 신뢰할 수 있는 네트워크인지를 확인하는 것이 필요합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

▶ 공공 와이파이 이용 시 주의사항

공공 와이파이를 이용할 때에는 몇 가지 주의사항을 염두에 두어야 합니다. 첫째로, 웹사이트에 접속할 때 해당 사이트가 암호화된 네트워크에서 데이터를 전송하고 있는지 확인해야 합니다. 암호화되지 않은 네트워크에서는 개인 정보가 탈취될 수 있으므로 주의가 필요합니다. 둘째로, 방화벽이 작동 중인지 확인해야 합니다. 방화벽이 활성화되어 있으면 악성 소프트웨어와 같은 위협으로부터 보호될 수 있습니다. 마지막으로, 보안 설정이 되어 있지 않은 무선 랜을 통해 민감한 서비스를 사용하는 것은 피해야 합니다. 보안 설정이 되어 있지 않은 네트워크는 해커에 의해 침입될 위험이 있으며, 개인 정보가 유출될 수 있습니다. 이러한 주의사항을 준수하여 안전한 공공 와이파이 이용이 가능합니다

▶ 제공자가 확인되지 않은 공중 무선 랜

제공자가 확인되지 않은 공중 무선 랜에서는 사진 촬영과 같이 비교적 민감하지 않은 서비스만을 이용해야 합니다. 왜냐하면 보안 설정이 없는 무선 랜에서는 이용자의 접속 행위나 개인정보 등이 유출될 수 있기 때문입니다. 금융거래, 기업 업무, 로그인이 필요한 서비스, 개인정보를 입력하는 서비스 등과 같이 민감한 정보를 다루는 서비스는 이러한 환경에서 사용하지 않는 것이 안전합니다. 따라서 공중 무선 랜을 이용할 때에는 보안에 신경을 쓰고, 가능한한 민감한 정보를 다루지 않는 것이 중요합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

3차시 - 비밀번호를 철저히 관리하는 방법

▶ 비밀번호

비밀번호는 사용자를 인증하고 시스템 또는 서비스에 접근할 수 있는 권한을 부여하기 위해 사용되는 보안 요소입니다. 일반적으로 "Password"라고 불리지만, 더 넓은 의미로는 "Passcode"나 "Personal Identification Number(PIN)" 등으로도 불릴 수 있습니다. 이러한 비밀번호는 사용자가 기억하기 쉽고 다른 사람에 의해 추측하기 어려운 형태로 설정되어야 합니다.

▶ 키로깅

키로깅은 사용자의 키보드 입력을 기록하고 저장하는 악성 소프트웨어 또는 장치를 가리킵니다. 이를 통해 공격자는 사용자가 입력한 모든 정보를 수집하고 암호, 계정 정보, 개인 정보 등을 탈취할 수 있습니다.

하드웨어 키로깅은 키보드와 컴퓨터 사이에 물리적으로 연결된 장치를 사용하여 입력을 기록하는 방식입니다. 이러한 방식은 백신 프로그램이나 보안 솔루션으로 예방하기가 어렵습니다. 그러나 하드웨어 키로깅은 물리적 액세스가 필요하기 때문에 실제로는 잘 사용되지 않는 경향이 있습니다.

▶ 크리덴셜 스터핑

크리덴셜 스터핑은 해커가 훔친 개인정보를 사용하여 여러 웹사이트나 온라인 시스템에 자동으로 대입하여 로그인을 시도하는 공격 기법입니다. 이러한 공격은 사용자가 비밀번호를 정기적으로 변경하지 않는 경우에 특히 취약합니다. 해커들은 훔친 개인정보를 인터넷 상에서 공유하고 판매하기도 하며, 이를 이용하여 대량의 로그인 시도를 수행합니다. 이런 방식으로 해커는 다양한 온라인 계정에 접근하여 중요한 정보를 탈취하거나 불법적인 활동을 수행할 수 있습니다

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

4차시 - 사무실 내에서의 생활 보안 강화

▶ 사무실PC 악성코드 피해 예방 방법

사무실 PC의 악성코드 피해를 예방하기 위한 방법은 여러 가지가 있습니다. 첫째, 출처가 불분명한 메일에 첨부된 파일을 실행하는 것을 자제해야 합니다. 이는 스팸 메일이나 피싱 메일을 통해 전달된 악성 파일에 의한 감염을 방지하는 데 도움이 됩니다. 둘째, 컴퓨터의 운영체제, 오피스 소프트웨어, 그리고 인터넷 브라우저의 보안 패치를 항상 최신 상태로 유지해야 합니다. 이를 통해 알려진 보안 취약점에 대한 공격으로부터 시스템을 보호할 수 있습니다. 마지막으로, 백신 소프트웨어를 최신 버전으로 유지하고 정기적으로 업데이트해야 합니다. 이를 통해 악성코드와 같은 위협으로부터 컴퓨터를 보호할 수 있습니다. 이러한 조치들을 취함으로써 사무실 PC의 보안을 강화할 수 있습니다.

▶ 사무실 PC 보안

사무실 PC 보안을 강화하기 위해서는 여러 가지 조치를 취할 수 있습니다. 정기적인 윈도우 보안 패치 업데이트는 시스템의 취약점을 최신 보안 패치로 보완하여 해커의 공격으로부터 보호하는 데 중요합니다. 또한, 승인되지 않은 불법 소프트웨어를 사용하지 않도록 정책을 시행하여 시스템에 악성 소프트웨어가 설치되지 않도록 합니다. 또한, PC 암호의 복잡도를 설정하여 안전한 암호를 사용함으로써 비인가자의 접근을 방지합니다. 이러한 조치들을 통해 사무실 PC의 보안을 향상시킬 수 있습니다.

▶ 정보보호 수칙 10가지

정보보호를 위해 꼭 지켜야 할 실천 수칙은 여러 가지가 있습니다. 먼저, 의심스러운 메시지는 절대로 열지 말고 바로 삭제하는 것이 중요합니다. 이메일이나 문자 메시지 등에서 의심스러운 링크나 첨부 파일이 포함된 경우, 해당 메시지를 열지 않고 바로 삭제해야 합니다. 또한, 백신 프로그램을 설치하고 정기적으로 바이러스 검사를 수행하여 시스템을 보호해야 합니다. 백신 프로그램은 최신 바이러스 및 악성 소프트웨어로부터 시스템을 방어하는 데 중요한 역할을 합니다. 마지막으로, 비밀번호를 설정하고 주기적으로 변경하는 것도 중요합니다. 강력한 비밀번호를 사용하고 주기적으로 변경함으로써 계정을 보호하고 해킹 및 무단 접근으로부터 시스템을 안전하게 유지할 수 있습니다. 이러한 실천 수칙을 준수함으로써 개인 및 기업의 정보보안을 강화할 수 있습니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

5차시 - 기업의 영업비밀 유출, SNS를 조심하세요

▶SNS에서의 보안 위협

SNS에서의 보안 위협으로 인해 발생할 수 있는 문제점은 다양합니다. 그 중 일부는 산업 스파이, 사이버 스토킹, 사이버 괴롭힘 등과 같은 사회적 위협에 해당합니다. 이러한 위협은 개인이나 조직의 프라이버시를 침해하거나 개인을 괴롭히는 데 사용될 수 있습니다. 또한 계정 해킹은 개인의 프라이버시나 ID 관련 문제에 대한 위협으로 이어질 수 있습니다. 이러한 문제들은 SNS 사용자들에게 심각한 피해를 줄 수 있으며, 적절한 보안 조치가 필요합니다.

▶ SNS 보안 위협에 대한 기업 측의 대응 방안

기업은 SNS 보안 위협에 대응하기 위해 몇 가지 조치를 취할 수 있습니다. 먼저, SNS 사용에 대한 보안 정책을 수립하여 직원들에게 안전한 사용 방법을 제공하고 규제할 수 있습니다. 이 정책은 회사의 정보 보호를 강화하고 민감한 정보의 노출을 방지하기 위한 목적을 가지고 있습니다. 둘째, 사이버 윤리에 대한 교육을 강화하여 직원들에게 SNS를 안전하게 사용하는 방법과 사이버 위협에 대한 인식을 높일 수 있습니다. 마지막으로, 회사 자체의 SNS 가이드라인을 마련하여 직원들에게 어떤 종류의 콘텐츠를 공유할 수 있는지, 어떤 종류의 정보를 비공개해야 하는지 등을 안내할 수 있습니다. 이러한 대응 방안을 통해 기업은 SNS를 안전하게 활용하면서 보안 위협으로부터 자산을 보호할 수 있습니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

6차시 - 모르는 사람이 보내온 이메일의 정체

▶ 악성 메일 대처

악성 메일을 대처하기 위한 요령은 다음과 같습니다. 먼저, 받은 메일의 보낸 사람 이메일 주소를 면밀히 확인하여 의심스러운 경우에는 해당 이메일을 열지 않습니다. 둘째, 메일에 첨부된 파일을 함부로 열지 않고, 특히 알 수 없는 출처의 파일은 절대로 실행하지 않습니다. 마지막으로, 출처가 불분명한 메일은 읽지 않고 즉시 삭제합니다. 이러한 요령을 따르면 악성 메일로부터 개인 및 기업 정보를 안전하게 보호할 수 있습니다.

▶ EAC

이메일 계정을 탈취하여 접속하는 피싱 메일 기법을 EAC라고 합니다. EAC는 Email Account Compromise의 약어로, 실제로 이메일 계정을 침해하여 공격자가 해당 계정으로부터 메일을 발송하거나 다양한 사기 행위를 시도하는 공격 기법을 가리킵니다. 이러한 공격은 흔히 이메일을 통해 개인정보를 탈취하거나 금전을 요구하는 등의 피싱 공격에 이용될 수 있습니다. 따라서 이메일 보안을 강화하고, 사용자는 의심스러운 이메일에 대해 조심하는 것이 중요합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

7차시 - 저작권 및 GPL 라이선스 정리

▶ 저작권 침해의 원인

소프트웨어 분야에서 저작권 침해가 가장 흔하게 발생하는 이유는 낮은 저작권 의식 때문입니다. 소프트웨어에 대한 저작권 의식이 다른 창작물보다 낮기 때문에, 많은 사람들이 소프트웨어를 불법적으로 이용하거나 복제하여 사용하는 경향이 있습니다. 또한, 소프트웨어 저작권 침해에 대한 처벌이 다른 분야에 비해 미약한 경우가 많아서 법적인 위험을 감수하기보다는 불법적으로 이용하는 경우가 더 많습니다. 또한, 저작권 침해로 인한 피해액을 정확히 산정하기 어렵기 때문에 법적 대응이 어렵습니다. 이를 해결하기 위해서는 법과 제재의 강화뿐만 아니라 저작권 의식을 높이는 교육과 보호 조치를 강화하는 것이 필요합니다.

▶ CCL 보호 원칙

CCL(크리에이티브 커먼즈 라이선스)은 창작자의 의도를 보호하고자 하는 원칙을 중요시합니다. 이 라이선스는 창작자가 자신의 작품을 공유하고자 할 때 법적인 해석이 모호하거나 의도와 다르게 사용될 우려로 인해 공유하지 못하는 경우를 방지하기 위해 만들어졌습니다. 즉, CCL은 창작자가 자신의 작품이 의도한 대로 사용되도록 일정한 제한과 조건을 부여하여 창작물의 사용에 대한 규칙을 명확하게 정의합니다. 이를 통해 창작자는 자신의 작품을 공유함으로써 다른 이들이 자유롭게 활용할 수 있으면서도 자신의 의도와 목적을 존중받을 수 있게 됩니다.

▶LGPL 특징

LGPL(Lesser General Public License)은 자유 및 오픈 소스 소프트웨어 라이선스의 한 형태로, '작은 범용 공중 라이선스'라는 의미를 갖습니다. 이 라이선스는 GPL의 일종으로, GPL보다는 더 유연한 조건을 제공합니다. LGPL은 주로 라이브러리와 같은 소프트웨어 구성 요소에 사용되며, 사용자가 이 라이브러리를 수정하거나 배포할 때 GPL과 유사한 규정을 따라야 합니다. LGPL은 수정한 소스 코드의 공개를 요구하지 않으며, 주요 프로그램과 라이브러리 간의 결합을 허용하는 데 중점을 둡니다. LGPL을 사용하는 경우 출처를 표기하는 것은 필요하지 않습니다

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

8차시 - Zoom, WebEx 등 화상회의 도구의 안전한 사용

▶ Zoom의 보안 취약점을 개선하기 위한 권장 사항

- AES-256 사용: AES-256은 강력한 암호화 알고리즘 중 하나로, 높은 수준의 보안을 제공합니다. Zoom은 사용자들 간의 데이터 전송 및 저장에 AES-256를 사용하여 보안 수준을 향상시킬 수 있습니다.
- ECB(Electric Code Book) 모드 사용 지양: ECB 모드는 동일한 평문 블록이 동일한 암호문 블록으로 매핑되는 단순한 암호화 모드입니다. 이 모드는 패턴을 드러낼 수 있고 보안에 취약할 수 있으므로, 대신 보다 안전한 운영 모드를 사용하는 것이 좋습니다.
- AES in F8-mode 사용: F8 모드는 AES와 같은 블록 암호화 알고리즘을 사용하여 데이터를 암호화하는 스트림 암호화 모드 중 하나입니다. 이 모드는 패턴을 제공하지 않고, 높은 수준의 보안을 제공할 수 있습니다.

▶ WebEx의 보안 취약점

WebEx의 보안 취약점은 다음과 같습니다:

- 회의 리더에 의해 퇴장당한 후에도 오디오 피드를 유령으로 유지할 수 있다는 문제가 있습니다. 즉, 회의 리더가 참석자를 퇴장시키더라도 해당 참석자는 오디오 피드를 계속해서 전송할 수 있습니다.
- 회의실에 입장할 수 없는 경우에도 회의 참석자의 전체 이름, 이메일 주소 및 IP 주소에 액세스할 수 있다는 문제가 있습니다. 이는 회의실에 입장하지 않은 참석자도 다른 참석자들의 개인정보에 접근할 수 있다는 것을 의미합니다.
- 채팅 및 화면 공유 기능에 대한 전체 액세스 권한이 있는 유령으로 회의에 참여할 수 있다는 문제가 있습니다. 이는 악의적인 공격자가 회의에 참여하여 채팅을 남기거나 화면을 공유할 수 있다는 것을 의미합니다.

▶ Zoom 용어

Zoom 회의에 초대받지 않은 사람을 지칭하는 용어는 "Troll"입니다. 이는 회의에 참여하지 않은 사람이나 초대되지 않은 사람이 불쾌한 행동을 하거나 방해를 일으키는 경우 사용됩니다.
또한, Zoom 회의 도중 불쾌한 행동이나 방해가 발생하는 것을 "Zoom Bombing"이라고 합니다. 이는 회의에 참여하지 않은 사람이나 회의 초대가 아닌 사람이 회의를 침입하여 방해하는 행위를 의미합니다.
마찬가지로, WebEx에서 초대되지 않은 사람이나 회의에 참가하지 않은 사람을 지칭하는 용어는 "고스트(Ghost)"입니다. 이는 회의에 참여하지 않은 사람이나 초대되지 않은 사람이 회의에 침입하는 것을 의미합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

9차시 - 안전한 재택근무 환경 구축 방법

▶ 재택근무의 주요 보안 위협의 종류

재택근무의 주요 보안 위협은 물리적 위협, 인적 위협, 기술적 위협으로 구분할 수 있습니다.
물리적 위협은 주로 노트북이나 컴퓨터와 같은 장치가 유출되거나 도난당할 경우 발생합니다. 이는 재택근무 환경에서 사용되는 장치가 외부에 노출되어 있을 때 발생할 수 있습니다.
인적 위협은 주로 사용자의 부주의나 사소한 실수로 인해 발생합니다. 이는 암호나 개인정보를 부주의하게 다루거나 소셜 엔지니어링에 노출되어 정보가 유출될 때 발생할 수 있습니다.
기술적 위협은 주로 해커의 침입이나 악성 소프트웨어에 의한 공격으로 인해 발생합니다. 이는 해킹이나 악성 코드를 통해 재택근무 환경에 침입하여 정보를 탈취하거나 시스템을 손상시키는 경우에 발생할 수 있습니다.

▶ 재택근무 시 근무자 입장에서 지켜야 할 보안 수칙

재택근무 시 근무자는 다음과 같은 보안 수칙을 준수해야 합니다.

- 정기적인 보안 패치: 근무하는 장치 및 소프트웨어에 대해 제공되는 보안 패치를 정기적으로 설치하고 업데이트해야 합니다. 이는 시스템 및 소프트웨어의 취약점을 최소화하여 보안을 강화하는 데 도움이 됩니다.
- 업무 전용 공간 확보: 재택근무 시에는 업무 전용 공간을 마련하여 개인 및 가정용 환경과 분리해야 합니다. 이를 통해 개인 정보나 기밀 데이터가 외부로 유출되는 것을 방지할 수 있습니다.
- 공용 PC 사용 자제: 개인용 PC 또는 공용 PC에서는 업무 관련 작업을 피하고, 업무용 장비 또는 안전한 장소에서만 업무를 수행해야 합니다. 공용 PC에서의 작업은 보안 위험이 크기 때문에 최대한 자제해야 합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

10차시 - 내 스마트폰이 해킹 당하지 않으려면?

▶ 블루투스를 통한 침투

블루투스를 통한 침투는 다양한 형태의 공격이 가능합니다. 이를 통해 공격자는 사진, 영상, 개인 정보, 금융 정보 등을 탈취할 수 있습니다. 또한, 블루투스의 특성상 신호 도달 거리가 비교적 짧기 때문에 공격자는 물리적으로 피해자에게 가까워져야 합니다. 그러나 한 번에 많은 양의 정보에 접근이 가능하다는 특성을 갖고 있습니다. 이는 블루투스 기기 간의 동시 연결이 가능하기 때문에 대규모의 정보 침투가 가능하다는 의미입니다.

▶공동인증서 저장 권장 위치

공동인증서를 안전하게 저장하는 것은 중요합니다. 스마트폰이나 하드디스크에 저장하는 것보다는 USIM이나 USB와 같은 외부 저장 장치에 저장하는 것이 안전합니다. 외부 저장 장치는 물리적으로 분리되어 있어서 해킹이나 악성 소프트웨어에 의한 침입으로부터 보다 안전하게 보호될 수 있습니다. 따라서 공동인증서를 저장할 때에는 USIM이나 USB와 같은 외부 저장 장치를 사용하는 것이 권장됩니다.

▶스마트폰 보안 수칙

스마트폰 보안을 위한 중요한 수칙은 다음과 같습니다.

공식 앱 마켓 이외의 출처에서 앱을 다운로드하거나 설치하지 않습니다. 공식 앱 마켓에서 배포되는 앱은 일반적으로 보안 검사를 거치기 때문에 신뢰할 수 있습니다.

스마트폰에 보안 잠금을 설정합니다. 패턴, 비밀번호, 지문 인식 또는 얼굴 인식과 같은 잠금 방법을 사용하여 스마트폰에 대한 무단 접근을 방지합니다.

다양한 온라인 계정에 대해 강력한 비밀번호를 사용하고 주기적으로 변경합니다. 이는 스마트폰에 저장된 민감한 정보를 보호하는 데 도움이 됩니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

11차시 - 보안 침해 사고 대응 절차 정리

▶ 기업에서 경험한 가장 높은 침해사고 유형

기업에서 경험한 침해사고 유형에 대한 질문에서 가장 높은 응답을 받은 유형은 악성코드입니다. 악성코드는 기업 보안에 큰 위협을 가하며, 데이터 유출, 서비스 거부 공격 등과 함께 가장 흔히 보고된 침해 유형 중 하나입니다.

▶침해사고 대응 절차 중 초기 대응 단계

침해사고 대응 절차 중 초기 대응 단계에서는 침해사고 대응팀을 소집하고 네트워크와 시스템의 기본 정보를 수집합니다. 이는 사고를 신속하게 대응하기 위한 중요한 단계로, 침해의 규모와 영향을 파악하고 추가적인 조치를 취하기 위해 필요합니다.

12차시 - 보안솔루션이 있어도 해킹을 당한 이유

▶침입 탐지 시스템(IDS)의 기능

침입 탐지 시스템(IDS)은 네트워크나 시스템 상에서 발생하는 잠재적인 침입을 탐지하고 이에 대한 대응을 수행하는 보안 도구입니다. 주요 기능은 다음과 같습니다.

-**Signature 기반 탐지**: 사전에 정의된 패턴 또는 시그니처를 사용하여 알려진 침입 패턴을 식별합니다. 이를 통해 알려진 공격이나 악성 코드를 탐지할 수 있습니다.

-**비정상 행위 탐지**: 이전에 수집된 데이터와 비교하여 현재의 행위가 정상적인지 여부를 판단합니다. 기존 패턴과 다른 패턴이나 동작을 감지하여 침입을 식별합니다.

-**알림 및 경고**: 침입이 탐지되면 해당 이벤트를 실시간으로 감지하여 관리자에게 경고 및 알림을 전송합니다. 이를 통해 즉각적인 대응이 가능합니다.

▶네트워크 접근통제(NAC)의 기능

네트워크 접근통제(NAC)는 네트워크에 접근하는 사용자나 장치의 신원을 확인하고 인증하는 기능을 수행합니다. 이를 통해 인가되지 않은 사용자나 장치의 네트워크 접근을 방지하고, 권한을 설정하여 허용된 사용자나 장치에 대한 적절한 네트워크 자원 및 서비스 접근을 관리합니다. 또한 NAC는 사용자 및 장치의 계정을 관리하고 보안 정책을 준수하도록 강제할 수 있습니다.

▶올바른 보안 운영규칙

보안 솔루션의 최신 패치를 최대한 자주 수행하여 시스템을 최신 보안 취약점으로부터 보호합니다. 보안 솔루션, 서버 프로그램의 기본 계정(Default 계정)을 변경하여 사용하여 악의적인 공격으로부터 시스템을 보호합니다. 사용자의 편의성을 고려할 때보다는 보안 정책을 우선시하여 조직 전체의 보안을 유지하고 강화합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

13차시 - 식별, 인증, 권한부여의 핵심요약

▶ 인증의 의미

인증은 특정 주체가 자신이 주장하는 사람이나 시스템임을 증명하는 과정 또는 방법을 말합니다. 이는 주로 비밀번호, 생체 인식(지문, 홍채 등), 보안 토큰 등을 사용하여 이루어집니다. 인증은 정보 보안에서 중요한 요소 중 하나로, 무단 접근을 방지하고 정당한 사용자만이 시스템이나 서비스에 접근할 수 있도록 보장합니다

▶권한부여

권한 부여는 특정 사용자나 시스템에게 어떤 행위를 수행할 수 있는 권한을 부여하는 것을 의미합니다. IT 분야에서는 주로 시스템 리소스나 데이터에 접근하거나 조작할 수 있는 권한을 관리합니다. 이는 보안을 강화하고 데이터의 무단 액세스나 변조를 방지하기 위해 중요한 요소입니다. 권한을 부여할 때에는 최소한의 필요한 권한만을 부여하여 보안을 강화하는 최소 권한의 원칙을 준수합니다. 이를 통해 사용자나 시스템이 필요 이상의 권한을 가지지 않도록 하여 보안을 유지하고 관리합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

14차시 - 최소한의 권한을 부여해야 하는 이유

▶접근 통제 정책

접근 통제 정책은 시스템이나 네트워크에 접근하는 사용자 또는 프로세스가 어떤 자원에 접근할 수 있는지를 규정하는 정책입니다. 이러한 정책은 시스템의 보안을 강화하고 민감한 정보에 대한 접근을 통제하기 위해 사용됩니다.

1. MAC(Mandatory Access Control): MAC는 강제 접근 통제로, 시스템 관리자가 정의한 보안 정책에 따라 사용자나 프로세스의 접근을 통제하는 방식입니다. 이는 사용자의 권한 수준에 관계없이 시스템이 자동으로 접근 권한을 부여하거나 거부합니다.
2. DAC(Discretionary Access Control): DAC는 재량적 접근 통제로, 자원의 소유자가 해당 자원에 대한 접근을 허용하거나 거부하는 방식입니다. 즉, 사용자가 자신이 소유한 자원에 대한 접근 권한을 설정하고 관리할 수 있습니다.
3. RBAC(Role Based Access Control): RBAC는 역할 기반 접근 통제로, 사용자의 역할에 따라 접근 권한을 부여하는 방식입니다. 각 사용자는 특정 역할에 할당되며, 해당 역할에 대한 권한을 부여받게 됩니다. 이를 통해 권한을 관리하고 역할에 따라 접근을 제어할 수 있습니다.

▶ 최소권한의 원칙

최소권한의 원칙은 사용자나 프로세스에게 권한을 부여할 때, 해당 업무나 작업을 수행하는 데 필요한 최소한의 권한만을 부여하는 원칙입니다. 이는 사용자나 프로세스가 필요 이상의 권한을 가지지 않도록 하여 보안을 강화하고, 불필요한 권한으로 인한 잠재적인 위협을 최소화하는 데 도움이 됩니다. 따라서 각 사용자나 프로세스는 자신이 수행하는 업무에 필요한 권한만을 부여받게 되어, 보안을 유지하면서도 업무 효율성을 유지할 수 있습니다.

▶최소 권한의 원칙

내부자에 의한 기밀 정보 및 기술 유출을 예방할 수 있다. 내부자가 접근할 수 있는 정보의 범위를 최소화함으로써 의도적이든 실수든 정보 유출의 위험을 크게 줄일 수 있다.

보안성을 강화하고 해킹 피해 시 피해 범주를 줄이기 위해 최소 권한의 원칙이 필요하다. 시스템에 접근할 수 있는 권한을 최소한으로 제한하면, 만약 외부 해커가 침입하더라도 피해를 입힐 수 있는 범위가 제한되어 피해를 최소화할 수 있다.

권력 및 권한의 오남용을 방지하기 위해 시스템적인 대비가 필요하다. 최소 권한의 원칙을 적용하면, 특정 사용자가 지나치게 많은 권한을 가져서 이를 오남용하는 상황을 방지할 수 있다. 이는 조직 내에서 권한 남용으로 인한 부정행위나 비리 발생을 예방하는 데 도움을 준다.

인재를 예방하기 위해 최소 권한의 원칙을 지켜야 한다. 직원들이 본인의 역할과 업무에 꼭 필요한 권한만을 가지게 하여 실수로 인한 데이터 손실이나 시스템 오류 등의 사고를 예방할 수 있다. 이로 인해 업무 효율성도 높아지고, 안전한 시스템 운영이 가능해진다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

15차시 - 보안 담당자의 역할과 보안 팀워크

▶ 기업의 보안 담당자 자격 요건

기업의 보안 담당자로서 요구되는 자격 요건은 여러 가지가 있습니다. 먼저, 윤리 의식이 중요합니다. 보안 담당자는 사용자의 개인 정보나 기업의 기밀 정보를 다루기 때문에 높은 윤리적 표준을 준수해야 합니다. 또한, 관련 법규에 대한 이해와 전문성이 필요합니다. 보안 담당자는 개인 정보 보호법, 정보 보안에 관련된 규정 등에 대해 잘 알아야 하며, 이에 따라 기업의 정보 보호 정책을 수립하고 시행할 수 있어야 합니다. 마지막으로, 시스템에 대한 전문 지식이 필요합니다. 보안 담당자는 네트워크 및 시스템 구성, 보안 기술 및 도구에 대한 지식을 보유하고 있어야 하며, 보안 위협에 대응할 수 있는 기술적 능력을 갖추고 있어야 합니다. 이러한 요건을 충족하는 보안 담당자는 기업의 정보 자산을 보호하고 보안 위협으로부터 회사를 안전하게 지킬 수 있습니다.

▶보안에 대한 기업의 정보 공유의 이점

기업 간 정보 공유는 여러 가지 이점을 가지고 있습니다. 먼저, 정보 공유를 통해 기업의 보안을 강화할 수 있습니다. 다른 기업이나 보안 전문가들과의 정보 교환을 통해 새로운 보안 위협에 대한 인식을 높일 수 있고, 효과적인 대응 전략을 마련할 수 있습니다. 또한, 신종 악성 코드에 대한 대응 방법과 예방 방법을 연구하고 개발하는 데 도움이 됩니다. 다양한 기업이나 보안 전문가들의 경험과 지식을 공유함으로써 보다 효과적인 보안 솔루션을 개발할 수 있습니다. 마지막으로, 정보 공유를 통해 잠재적인 보안 위험을 미리 감지하고 예방할 수 있습니다. 기업 간의 협력을 통해 보안 사고를 사전에 예측하고 대비할 수 있으며, 보다 안전한 영업 환경을 조성할 수 있습니다. 이러한 이점들은 기업이 보다 강력한 보안 전략을 수립하고 사이버 위협으로부터 더욱 효과적으로 자산을 보호할 수 있도록 도와줍니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

16차시 - 안전한 웹서버 운영 노하우

▶ 유닉스 서버 운영체제

유닉스(Unix) 서버 운영체제는 다음과 같은 종류가 있습니다

Unix: 초기에 개발된 유닉스 운영체제로, 다양한 변형이 존재

Linux: 오픈 소스 운영체제인 리눅스는 유닉스와 호환되는 기능을 제공하며, 많은 서버 및 컴퓨팅 시스템에서 사용

AIX: IBM이 개발한 유닉스 기반의 운영체제로, 주로 IBM의 서버 및 워크스테이션에서 사용

▶ 서버 아키텍처 구성

웹 서버: 클라이언트의 요청을 받아들이고, 정적인 콘텐츠(HTML 파일, 이미지 등)를 제공하는 서버입니다.

웹 클라이언트: 사용자가 웹 서버에 요청을 보내고 응답을 받는 소프트웨어 또는 브라우저입니다.

WAS(Web Application Server): 동적인 콘텐츠(웹 애플리케이션, 서버 사이드 스크립트 등)를 실행하고, 데이터베이스와의 상호 작용을 처리하는 서버입니다.

웹 서버 아키텍처에서는 웹 서버와 웹 클라이언트가 주요 구성 요소이며, WAS는 웹 서버와 함께 동적인 웹 애플리케이션을 실행하기 위해 사용됩니다. 데이터베이스(DB) 역시 중요한 구성 요소 중 하나이지만, 직접적으로 웹 서버 아키텍처에 포함되는 것은 아닙니다

▶ Apache 데몬

Apache 데몬을 root가 아닌 별도 계정으로 구동하는 이유는 해킹 시 root 권한이 노출되는 것을 막기 위해서입니다. 웹 서비스 데몬을 root 권한으로 실행하면 파일을 수정하거나 생성하는 과정에서 모든 파일에 대해 root 권한이 부여되어 보안에 취약해집니다. 이는 해커가 서버에 침입하여 root 권한을 획득할 경우 시스템에 막대한 피해를 줄 수 있습니다. 따라서 웹 서버를 실행하는 데몬은 최소 권한으로만 동작하도록 설정하여 보안을 강화하는 것이 중요합니다

▶윈도우 서버에서 Everyone 그룹으로 공유를 금지하는 이유

윈도우 서버에서 Everyone 그룹으로 공유를 금지하는 이유는 익명 사용자의 접근을 차단하기 위함입니다. Everyone 그룹에 속한 모든 사용자가 공유 폴더에 접근할 수 있기 때문에 보안상의 위험이 증가합니다. 이로 인해 내부 정보의 유출이나 악성 코드의 감염 가능성이 높아지게 됩니다. 따라서 공유 폴더에 Everyone 그룹으로의 공유를 금지함으로써 익명 사용자의 접근을 차단하여 시스템 보안을 강화합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

▶ 웹 클라이언트, 웹 서버, WAS의 정의

웹 클라이언트(Web Client)는 네트워크를 통해 서버로부터 콘텐츠, 정보, 서비스를 제공받는 사용자의 웹 브라우저를 의미한다. 웹 브라우저를 통해 사용자는 인터넷에 접속하여 다양한 웹 사이트를 탐색하고 필요한 정보를 얻을 수 있다.

웹 서버(Web Server)는 웹 클라이언트의 요청을 받아 정적인 콘텐츠를 제공하는 프로그램이 설치된 장치를 말한다. 웹 서버는 HTML, CSS, 이미지 파일 등과 같은 정적 자원을 클라이언트에게 전달하며, 주로 정적인 웹 페이지를 처리하는 역할을 한다.

WAS(Web Application Server)는 웹 클라이언트의 요청 중 데이터베이스 조회나 비즈니스 로직 처리와 같은 동적인 처리를 담당하는 프로그램이 설치된 장치를 의미한다. WAS는 동적인 웹 애플리케이션을 실행하여 사용자 요청에 맞는 맞춤형 데이터를 생성하고, 이를 웹 서버를 통해 클라이언트에게 전달한다. 이를 통해 사용자에게 동적인 콘텐츠와 서비스를 제공할 수 있게 한다.

▶ '계정 관리 분야'의 세부 점검 항목

유닉스 서버의 운영 체크리스트 중 '계정 관리 분야'의 세부 점검 항목은 다음과 같다.

먼저, 루트 계정의 원격 접속을 제한하는 설정을 수행한다. 이는 보안상의 이유로 루트 계정이 원격으로 접근할 수 없도록 하여 불필요한 위험을 줄이기 위함이다.

다음으로, 루트 계정 이외의 계정의 UID를 0으로 설정하지 않으며, 모든 계정의 UID를 고유하게 설정해야 한다. 이는 각 사용자가 개별적인 권한을 갖도록 하여 보안 사고를 예방하기 위함이다.

패스워드 복잡성 설정도 중요한 항목이다. 이는 사용자가 강력한 패스워드를 사용하도록 규칙을 설정하여 비밀번호 추측 공격이나 사전 공격으로부터 시스템을 보호하기 위한 조치이다.

패스워드 파일 보호 역시 중요한 점검 항목이다. 시스템 내에 저장된 패스워드 파일이 적절하게 보호되도록 권한을 설정하고, 암호화된 형태로 저장하여 비인가자가 접근하지 못하도록 한다.

마지막으로, 세션 타임아웃 설정을 통해 일정 시간 동안 활동이 없는 세션을 자동으로 종료시키는 정책을 적용한다. 이는 장시간 사용되지 않는 세션이 남아있을 경우 발생할 수 있는 보안 위험을 줄이기 위한 것이다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

17차시 - 최신 웹 취약점 알아보기(OWASP top10)

▶OWASP top 10

OWASP Top 10 중 'A10:2021-Server-Side Request Forgery (서버 측 요청 위조)'는 2021년 버전에서 새롭게 등장한 취약점으로, 일반적으로 'SSRF'로 알려져 있습니다. 이 취약점은 웹 애플리케이션에서 사용자가 제공한 URL의 유효성을 검사하지 않고 원격 리소스를 가져올 때 발생합니다. 공격자는 변조된 요청을 생성하여 웹 애플리케이션을 통해 사용자에게 전송하는 공격 방법을 사용할 수 있습니다. 이를 통해 공격자는 악의적인 목적으로 내부 시스템에 대한 정보를 노출하거나 공격할 수 있습니다.

18차시 - 정보보호 분야 컴플라이언스 총정리

▶ 국방수권법

국방수권법은 미국의 국방정책과 예산에 관한 법률입니다. 이 법은 미국 국방부의 지침과 재원을 결정하며, 미국 군대의 활동 및 군사작전에 대한 규정도 포함됩니다. 특히 주한미군과 관련하여 군대의 배치, 장비, 군사적 역할 등을 규제하고 지원하는데 사용됩니다

19차시 - 업무에서 암호화의 중요성

▶대칭키

대칭키는 데이터를 암호화하거나 복호화하는 데에 동일한 키를 사용하는 암호화 방식을 가리킵니다. 이러한 암호화 방식에는 IBM의 루시퍼 시스템, DES (Data Encryption Standard), AES (Advanced Encryption Standard) 등이 있습니다. 이들은 모두 대칭키를 사용하여 데이터를 안전하게 보호하고 전송하는 데에 널리 사용됩니다.

▶Diffie-Hellman 공개키

Diffie-Hellman은 공개키 암호화 방법 중 하나로, 최초의 공개키 알고리즘 중 하나입니다. 이 방법은 대칭키의 키 전달 문제를 해결하기 위해 개발되었습니다. Diffie-Hellman 알고리즘은 두 개의 통신 당사자가 서로의 공개키를 교환하고 이를 사용하여 안전한 대칭키를 생성하는 데 사용됩니다. 이 과정을 통해 데이터의 안전한 전송이 가능해집니다.

▶취약한 암호화 방식

취약한 암호화 방식으로는 RC4, MD5, 3DES 등이 있습니다. 또한, RSA의 경우 1024비트 이하의 키 길이를 사용할 경우 안전하지 않습니다. 이러한 암호화 방식들은 현재의 보안 요구 사항을 충족시키지 못하고 있으며, 해독이 상대적으로 쉽게 이루어질 수 있습니다. 따라서 이러한 암호화 방식을 사용하는 것은 권장되지 않습니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

20차시 - 효과적인 보안 교육 훈련 방안

▶일반 사무직 직원을 위한 보안 교육 훈련

일반 사무직 직원을 대상으로 하는 보안 교육 훈련은 다양한 주제를 다룰 수 있습니다.

1. **신뢰할 수 없는 출처의 콘텐츠를 주의한다:** 이 부분에서는 이메일의 첨부 파일이나 링크를 클릭하기 전에 출처를 확인하고, 의심스러운 콘텐츠를 열지 않도록 경고하는 내용을 교육할 수 있습니다.
2. **종합적인 안전 교육 및 인식 교육 프로그램을 이수한다:** 보안 교육 프로그램을 통해 사이버 위협에 대한 인식을 높이고, 올바른 보안 관행을 습득하도록 돕는 것이 중요합니다. 이를 통해 직원들은 사이버 위협에 대응할 수 있는 능력을 키우고, 보안 정책 및 절차를 준수할 수 있습니다.
3. **생활 보안을 강화하기 위한 방법을 교육한다:** 개인적인 기기 및 계정 보안에 대한 중요성을 강조하고, 간단한 생활 보안 관행을 실천하도록 교육할 수 있습니다. 이를 통해 직원들은 개인 정보 유출과 관련된 위험을 최소화하는 데 도움을 받을 수 있습니다.

21차시 - 4차 산업혁명 시대의 보안 이슈 – 1

▶ICBM 보안 이슈 대처법

CBM 시스템의 보안 이슈를 대처하기 위한 방법은 다양합니다.

- **모바일 인증 보호기능 강화:** 모바일 기기를 통해 시스템에 접근하는 경우, 강력한 인증 및 보호 기능을 갖춘 모바일 인증 시스템을 도입하여 접근을 제한하고 보호합니다. 이는 인증 과정에서의 보안 강화를 통해 민감한 정보에 접근하는 것을 방지하고, 불법적인 접근을 차단합니다.
- **물리적 공격 대응:** ICBM 시스템은 극도로 중요하고 민감한 시설이므로, 물리적인 보안도 중요합니다. 이를 위해 시설 주변에 경계를 설정하고, 침입 감지 및 감시 시스템을 구축하여 물리적인 침입을 탐지하고 대응할 수 있도록 합니다. 또한, 접근이 제한된 지역에는 출입 통제 시스템을 설치하여 불법적인 접근을 방지합니다.
- **보안 게이트웨이:** 시스템에 대한 외부 접근을 관리하기 위해 보안 게이트웨이를 도입하여 외부로부터의 공격을 차단하고 허용된 트래픽만을 허용합니다. 이를 통해 시스템에 대한 보호를 강화하고, 외부에서의 침입을 방지합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

22차시 - 4차 산업혁명 시대의 보안 이슈 – 2

▶Stuxnet

2010년에 발견된 스턱스넷은 이란의 우라늄 농축 시설에 침투하여 오작동을 유발하는 악성코드입니다. 이 악성코드는 지멘스사의 산업용 소프트웨어를 이용하여 이란의 핵 개발 시설에 침투했으며, 이로 인해 이란의 핵 개발 시설에 큰 피해를 입혔습니다. 또한, 스턱스넷은 이란뿐만 아니라 중국을 비롯한 여러 국가에도 빠르게 확산되어 다양한 산업 시설들을 감염시켰습니다.

▶ Level 3.5 : Industrial DMZ

산업운영관리시스템의 완충지대는 Level 3.5인 Industrial DMZ입니다. 이 계층은 OT(Operational Technology) 환경과 외부 IT(Information Technology) 환경을 연결하는 중요한 지점으로, 주로 센서 데이터를 저장하는 알티디비와 히스토리안, 애플리케이션 서버, 그리고 패치 서버 등이 속합니다. 최근에는 OT 보안 침해 사고의 증가와 IT-OT 융합보안의 중요성이 부각되면서 이러한 완충지대의 역할이 주목받고 있습니다.

24차시 - 랜섬웨어의 원리와 예방

▶웜 바이러스

웜 바이러스는 컴퓨터 시스템에 영구적인 손상을 입힐 수 있는 특징을 가지고 있습니다. 이는 파일을 삭제하거나 수정함으로써 시스템의 기능을 파괴할 수 있습니다. 또한, 웜 바이러스 감염으로 인해 블루스크린이 뜨거나 컴퓨터가 켜지지 않는 등의 문제가 발생할 수 있습니다. 이러한 특징들은 웜 바이러스가 컴퓨터 시스템에 심각한 피해를 줄 수 있음을 보여줍니다.

▶네스티 스터프

네스티 스터프는 파일을 직접적으로 암호화하여 사용자가 파일을 알아볼 수 없게 만들고, 해당 파일을 복원하려면 금전을 요구하는 랜섬웨어의 한 종류입니다. 이러한 악성코드는 파일을 암호화할 때 강력한 암호화 알고리즘을 사용하며, 해독하는 데 필요한 키는 공격자만이 가지고 있기 때문에 사용자가 직접 파일을 복원하는 것이 거의 불가능합니다. 따라서 사용자가 원하는 파일이나 데이터를 되찾기 위해서는 공격자에게 요구된 금액을 지불해야 할 수 있습니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

25차시 - 위험한 보안 취약점, 대응 방법 요약

▶ One-day

취약점이 발견되었으나 해당 취약점에 대한 패치가 이미 개발되어 공개되었지만, 아직 해당 패치가 시스템에 적용되지 않은 상태를 우리는 "One-day(원데이)"라고 합니다. 이 용어는 보안 커뮤니티에서 널리 사용되며, 이러한 취약한 상태는 시스템이 잠재적으로 공격에 노출될 수 있는 위험한 상태를 의미합니다. 따라서 취약점이 발견되고 패치가 나왔지만 아직 적용되지 않은 상태는 보안적인 측면에서 주의가 필요한 상황입니다.

▶ 취약점

취약점에 해당하는 HeartBleed, FREAK, SMB는 각각 다음과 같은 특징을 가지고 있습니다.

1. HeartBleed: OpenSSL 라이브러리의 버전 1.0.1에서 1.0.1f까지의 버전에 존재하는 취약점으로, TLS(Transport Layer Security)에서 사용되는 Heartbeat 확장 기능에 대한 구현 오류로 인해 발생합니다. 이 취약점을 이용하면 서버 및 클라이언트 간에 주고받는 정보가 노출될 수 있으며, 악의적인 공격자가 개인 정보를 탈취할 수 있습니다.
2. FREAK: FREAK 취약점은 SSL 및 TLS 프로토콜에서 발견된 보안 결함으로, 클라이언트 및 서버가 DHE(Diffie-Hellman Ephemeral) 및 RSA 보안 키 교환 방법을 지원하지 않을 때 발생합니다. 이 취약점을 악용하면 중간자 공격이 가능해져 클라이언트와 서버 간 통신이 암호화되지 않을 수 있습니다.
3. SMB: Server Message Block(SMB)은 파일 및 프린터 공유, 시스템 통신 등을 위한 네트워크 프로토콜로, 이 프로토콜을 이용한 공격이나 취약점은 주로 원격 코드 실행, 인증 바이패스 등의 공격 형태로 나타납니다. 이 취약점을 악용하면 공격자가 원격 시스템에 액세스하거나 시스템을 조작할 수 있습니다.

▶ CVE

CVE는 Common Vulnerabilites and Exposure의 약어로, 컴퓨터 시스템 및 소프트웨어에서 발견된 보안 취약점을 식별하고 추적하기 위한 공개적인 목록입니다. 이 목록은 각각의 취약점에 고유한 식별자(CVE ID)를 부여하여 관련 정보를 쉽게 공유하고, 보안 업계 및 사용자들이 보다 빠르고 효과적으로 대응할 수 있도록 지원합니다. CVE 목록은 공식적으로는 MITRE Corporation이 관리하고 있으며, 보안 업계의 다양한 조직과 개인들이 CVE에 기여하고 업데이트를 제공하여 보다 포괄적인 보안 정보를 유지하고 있습니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

▶ Bash shell의 취약점

Shellshock는 GNU Bash 셸에서 발견된 취약점으로, 공격자가 환경 변수를 통해 악의적인 코드를 주입하여 원격에서 시스템 명령을 실행할 수 있는 보안 취약점입니다. 이 취약점은 2014년에 발견되었으며, 많은 리눅스 및 유닉스 시스템에서 사용되는 Bash 버전에서 발생합니다. Shellshock 취약점을 악용하면 웹 서버, 메일 서버 등과 같은 여러 서비스를 운영하는 서버에 치명적인 영향을 줄 수 있습니다. 이러한 취약점으로 인해 공격자는 시스템 명령을 실행하거나 시스템에 대한 완전한 제어를 얻을 수 있어 보안 전문가들의 주요 관심사 중 하나가 되었습니다.

26차시 - 해커들이 해킹을 하는 이유와 그들이 노리는 것

▶전문 해커집단

전문 해커 집단은 다양한 목적을 가지고 활동하는 해커 그룹으로, 주로 상업적이거나 정치적인 이유로 활동합니다. 이들은 경쟁사를 사보타주기도 하며, 산업 스파이나 경쟁자의 기밀 정보를 탈취하여 경쟁 우위를 확보하기 위해 공격을 실행할 수 있습니다. 또한, 의뢰인을 위해 정보 수집을 수행하여 기업이나 개인의 개인 정보를 유출하거나 기밀 정보를 탈취할 수도 있습니다. 그들은 회사들의 버그 바운티 프로그램에 참여하여 보안 취약점을 발견하고 이를 보고하여 보상을 받는 경우도 있습니다. 이러한 전문 해커 집단은 보통 높은 기술력을 가지고 있으며, 이를 이용하여 다양한 공격을 수행하는 경우가 많습니다. 그들의 활동은 사회적, 경제적인 영향을 미치며, 이에 대한 대응 및 방어가 중요한 보안 문제로 인식되고 있습니다.

▶ APT 그룹 털라(Turla)

APT 그룹 털라(Turla)는 백도어인 코피루왁을 사용하여 시스템에 접근하고, 키로깅 등의 스파잉 행위를 통해 사용자의 활동을 감시합니다. 또한, 브라우저에 확장 프로그램을 설치하여 사용자의 비밀번호를 탈취하는 등의 공격을 수행합니다. 이 그룹은 고도로 정교한 기술과 전략을 활용하여 타깃을 공격하며, 장기간에 걸쳐 지속적으로 공격을 진행하는 특징을 가지고 있습니다. 그들의 활동은 국가적인 정보 수집 및 사이버 스파이 활동으로 알려져 있으며, 다양한 산업 분야와 정부 기관에 대한 공격을 수행합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

29차시 - 비즈니스 스캠(업무사기)에 효과적 대응

▶비즈니스 스캠을 예방하기 위한 실천 자세

비즈니스 스캠을 예방하기 위해서는 다음과 같은 자세를 실천해야 합니다.

보낸 사람의 이메일 주소를 면밀히 확인한다: 이메일의 발신자가 신뢰할 만한 출처인지 확인하기 위해 이메일 주소를 주의 깊게 살펴보고, 의심스러운 주소에 대해서는 조심스럽게 대응합니다.

첨부파일을 함부로 열지 않는다: 이메일의 첨부 파일이나 링크를 열기 전에 반드시 그 출처와 내용을 신중하게 확인하고, 의심스러운 파일은 열지 않거나 다운로드하지 않습니다.

출처가 불분명한 메일은 읽지 않는다: 의심스러운 이메일의 출처가 명확하지 않은 경우 해당 이메일을 읽지 않고 바로 삭제하거나, 보안 담당자에게 신고합니다. 외부에서 온 이메일에 대해서는 특히 주의를 기울여야 합니다.

위의 자세를 실천하여 비즈니스 스캠으로부터 안전을 유지하고, 회사의 정보 및 자산을 보호할 수 있습니다

▶Online shopping, classfield and auction scams (온라인 쇼핑, 경매 관련 스캠)

classfield and auction scams (온라인 쇼핑, 경매 관련 스캠)은 온라인 쇼핑, 분류, 및 경매 관련하여 사용자들에게 발생할 수 있는 위험을 나타냅니다. 사용자들은 이러한 사기에 주의하고, 거래 전에는 신뢰할 수 있는 판매자와의 거래를 선호해야 합니다. 또한 공동 구매나 경매에 참여하기 전에는 사기의 가능성을 고려하여 신중한 판단이 필요합니다.

수업 중 궁금증이 생기면 교안 내 검색(ctrl+f) 기능을 활용하여 완벽한 학습을 진행할 수 있습니다.

30차시 - 트로이목마 해킹 공격을 막아보자

▶ 트로이목마 의심 증상

트로이목마에 감염되었을 때 나타나는 몇 가지 의심 증상 중 하나는 컴퓨터의 속도가 느려지거나 빠른 속도로 변하는 것입니다. 이는 감염된 프로세스가 시스템 리소스를 많이 사용하기 때문에 발생할 수 있습니다. 또한, 감염된 시스템에서는 디스크 공간이 부족하다는 경고 메시지가 표시될 수 있습니다. 이는 트로이목마가 시스템의 파일을 복사하거나 생성하여 공간을 차지하기 때문에 발생할 수 있습니다. 따라서 컴퓨터의 속도 변화나 디스크 공간 부족과 같은 이상 증상이 나타날 경우, 트로이목마에 감염되었는지 확인하는 것이 중요합니다.

▶트로이목마 감염 예방 방법

트로이목마와 같은 악성 소프트웨어에 감염되지 않도록 예방하는 방법은 다음과 같습니다.

1. 소프트웨어를 주기적으로 업데이트하여 최신 보안 패치를 적용합니다.
2. 신뢰할 수 없는 소스로부터 오는 링크나 첨부 파일을 클릭하거나 열지 않습니다.
3. 계정 보안을 강화하기 위해 강력한 암호를 사용하고, 가능한 경우 다단계 인증을 활성화합니다.
4. 트로이목마 및 다른 악성 소프트웨어의 위험을 피하기 위해 토렌트 사이트보다는 공식 앱스토어나 웹사이트에서 소프트웨어를 다운로드합니다.

▶트로이목마의 종류

트로이목마(Trojan horse)는 여러 가지 유형으로 나타날 수 있으며, 그 중 일부는 다음과 같습니다:

-백도어 트로이목마(Backdoor Trojan): 백도어 트로이목마는 해커가 시스템에 히든 백도어(backdoor)를 설치하여 원격으로 시스템에 액세스할 수 있게 합니다. 이것은 해커가 시스템에 대한 완전한 제어권을 얻을 수 있도록 해주는 위험한 종류의 트로이목마입니다.

-다운로더 트로이목마(Downloader Trojan): 다운로더 트로이목마는 주로 다른 악성 소프트웨어를 다운로드하고 설치하는 기능을 수행합니다. 주로 다른 악성 코드를 시스템에 소프트웨어적으로 배포하고 설치하는 데 사용됩니다.

-게임시프 트로이목마(GameThief Trojan): 게임시프 트로이목마는 주로 게임 계정 정보를 탈취하고 이를 악용하여 게임 내 가상 자산을 훔치는 데 사용됩니다. 이는 온라인 게임 플레이어 및 게임 기업에게 매우 위험한 유형의 트로이목마입니다.

이 외에도 다양한 트로이목마 유형이 존재하며, 이들은 시스템에 다양한 방식으로 침투하고 피해를 입히기 위해 다양한 기술을 사용합니다. 사용자들은 이러한 트로이목마에 대해 주의를 기울여야 하며, 최신의 보안 소프트웨어와 보안 조치를 취하여 시스템을 보호해야 합니다.