

기업정보보안, 생존을 위한 필수 전략 _위협과 대응의 모든 것



학습자용 학습자료



종합평가

학습자용 학습자료

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

1차시

학습자료

증가하는 정보보안 위협 요인

정보보안 위협은 끊임없이 진화하고 있습니다. 디지털 전환으로 기업들이 온라인 환경에서 더 많은 정보를 다루게 되면서, 해커들의 공격 기회 또한 늘어났습니다. 특히, 인공지능(AI) 기반 해킹과 제로데이 공격은 기존 보안 시스템으로 탐지하기 어려운 새로운 위협으로 떠올랐습니다.

랜섬웨어 공격 역시 기업의 중요 데이터를 인질로 삼아 금전을 요구하는 악랄한 범죄로, 피해 규모가 급증하고 있습니다. 또한, 내부 직원의 실수나 악의적인 행동으로 인한 정보 유출 또한 심각한 문제입니다.

IoT 기기와 클라우드 서비스는 편리함을 제공하지만, 보안에 취약할 경우 해커들의 손쉬운 표적이 될 수 있습니다. 이처럼 날로 다양해지고 정교해지는 정보보안 위협에 대응하기 위해 기업들은 보안 시스템 강화와 직원들의 보안 의식 향상에 힘써야 합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

2차시

학습자료

해킹의 종류

1. 시스템 해킹

윈도우나 맥OS 같은 운영체제와 같이, 컴퓨터 시스템 자체의 약점을 이용해서 침입하는 방식입니다. 해커들은 이런 약점을 파고들어 시스템을 장악하거나 데이터를 빼돌립니다.

2. 네트워크 해킹

네트워크를 통해 시스템에 침입하는 방식입니다. 해커들은 네트워크를 돌아다니는 데이터를 엿보거나 조작해서 정보를 훔치거나 시스템을 마비시킵니다.

3. 웹 해킹

매일 사용하는 웹사이트에도 약점이 있을 수 있습니다. 해커들은 이런 약점을 이용해서 웹사이트를 변조하거나 개인정보를 빼돌립니다. 예를 들어, SQL Injection이나 Cross-Site Scripting(XSS) 같은 공격 기법을 사용해서 웹사이트를 공격합니다.

4. 애플리케이션 해킹

특정 프로그램의 약점을 이용해서 침입하는 방식입니다. 예를 들어, 은행 앱이나 게임 앱의 취약점을 이용해서 앱을 오작동시키거나 데이터를 훔쳐 갑니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

2차시

학습자료

해킹 및 랜섬웨어 대응 방안 _ 기술적 보안

기술적 보안은 기술을 활용해서 보안 수준을 높이는 것을 말합니다.

1. 윈도우나 오피스 프로그램 같은 소프트웨어는 항상 최신 보안 패치를 적용해야 합니다.
2. 방화벽, 침입 탐지 시스템(DS), 침입 방지 시스템(IPS) 같은 보안 솔루션을 도입하는 것도 중요합니다.
3. 안티바이러스, 안티랜섬웨어 소프트웨어도 꼭 설치하고 주기적으로 업데이트해야 합니다. 이런 소프트웨어는 악성코드 감염을 예방하고, 혹시라도 랜섬웨어에 감염되더라도 데이터를 복구할 수 있도록 도와줍니다.
4. 중요한 데이터는 정기적으로 백업해 두는 것이 좋습니다. 만약 랜섬웨어에 감염되어 데이터가 암호화되더라도 백업해 둔 데이터를 통해 복구할 수 있기 때문입니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

2차시

학습자료

랜섬웨어의 작동 방식

랜섬웨어는 주로 악성 이메일 첨부파일이나 웹사이트 링크를 클릭했을 때 몰래 숨어들어오거나, 소프트웨어의 취약점을 이용해서 침입하기도 합니다.

컴퓨터에 침투한 랜섬웨어는 중요한 파일들을 암호화해서 사용할 수 없게 만들며, 암호를 풀어주는 대가로 돈을 요구하는 메시지를 띄웁니다. 하지만 돈을 보낸다고 해서 꼭 파일을 돌려받을 수 있다는 보장은 없습니다. 오히려 추가 공격의 표적이 될 수도 있죠. 랜섬웨어는 한 번 감염되면 데이터 복구가 굉장히 어렵기 때문에 랜섬웨어 예방이 무엇보다 중요합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

3차시

학습자료

DDoS 공격 및 악성코드 대응 방안

1. 방화벽

네트워크 트래픽을 감시하고, 허가되지 않은 접근을 막아주는 역할을 합니다.

2. 침입 탐지 시스템(IDS)과 침입 방지 시스템(IPS)

실시간으로 트래픽을 분석해서 비정상적인 패턴이나 공격 시도를 탐지하고, 필요하면 차단까지 해줍니다.

3. DDoS 방어 솔루션

DDoS 공격은 엄청난 트래픽을 쏟아부어 시스템을 마비시키는 공격입니다. 이런 공격에는 'DDoS 방어 솔루션'이 필요합니다. 클라우드 기반 서비스를 이용하거나 자체적으로 시스템을 구축하여 DDoS 공격을 방어할 수 있습니다.

4. 백신 프로그램과 안티 멀웨어 솔루션

악성코드는 컴퓨터 바이러스와 같이 시스템에 침투하여 데이터를 훼손하는 악성 소프트웨어입니다. 이런 악성코드를 막기 위해서는 '백신 프로그램'과 '안티 멀웨어 솔루션'이 필요합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

4차시

학습자료

내부 위협 대응 방안

1. 정보 접근 통제

허가받지 않은 사람이 함부로 정보에 접근하지 못하게 막는 시스템입니다. 내부 직원들은 기업 정보에 대한 접근 권한이 높아서, 악의적인 의도가 없더라도 실수만으로도 회사에 막대한 피해를 줄 수 있기 때문입니다.

정보 접근 통제 방법은 여러 가지가 있는데, 가장 대표적인 것이 '역할 기반 접근 통제(RBAC)'입니다. 직원의 역할에 따라 정보 접근 권한을 다르게 주는 방식입니다.

2. 보안 교육

정보보안의 중요성을 강조하고, 최신 해킹 수법이나 보안 위협 정보를 공유하고, 안전한 행동 수칙을 숙지시켜야 합니다. 단순히 지식만 전달하는 것이 아니라, 실제 상황에서 발생할 수 있는 보안 위협에 대한 대응 능력을 키워주는 것이 중요합니다. 피싱 이메일을 구별하는 방법, 안전한 비밀번호 설정 방법, 개인정보보호법 준수 방법 등 실질적인 내용을 교육해야 직원들의 보안 의식을 높이고 정보 유출 사고를 예방할 수 있습니다.

3. 모니터링 시스템

내부 위협은 외부 해킹보다 탐지하기 어렵기 때문에 모니터링 시스템은 필수적입니다. 네트워크 트래픽, 시스템 로그, 사용자 행위 등을 실시간 감시하고 분석하여 정보 유출 시도를 조기에 탐지하고 차단할 수 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

4차시

학습자료

정보 유출 경로 및 유형

1. 스마트폰

스마트폰 안에는 개인정보, 금융 정보는 기본이고, 회사 관련 중요 자료까지 모든 정보가 담겨 있습니다. 스마트폰 하나를 잃어버리는 순간, 모든 정보가 위협에 노출되는 겁니다. 모바일 기기는 해킹에도 취약합니다. 출처 불분명한 악성 앱을 설치하거나, 보안 설정을 제대로 하지 않거나, 공공장소에서 안전하지 않은 와이파이를 사용하는 순간, 해커들이 우리 스마트폰에 몰래 침투할 수 있습니다. 이렇게 되면 저장된 정보가 고스란히 해커의 손에 넘어가게 됩니다.

2. 이메일

매일 수십 통씩 주고받는 이메일은 편리한 만큼 위험하기도 합니다. 악성 첨부파일이나 피싱 링크를 클릭하는 순간, 악성코드에 감염되거나 개인정보가 술술 새어나갈 수 있습니다. 특히 특정 개인이나 조직을 노리는 '스피어 피싱' 공격은 마치 낚시꾼이 특정 물고기를 잡기 위해 맞춤형 미끼를 쓰는 것처럼, 해커들도 우리 정보를 이용해 그럴듯한 이메일을 만들어 보내 돈을 뜯습니다.

3. USB, 외장하드

'USB'나 '외장하드' 같은 휴대용 저장 장치는 작고 가볍다는 장점 때문에 중요한 자료를 담아 외부로 가지고 나가서 잃어버리거나, 악성코드에 감염된 USB를 회사 컴퓨터에 꽂는 순간, 정보 유출 사고가 발생할 수 있습니다.

4. 클라우드 서비스

최근에는 '클라우드 서비스'도 정보 유출의 핵심 경로로 떠오르고 있습니다. 언제 어디서든 데이터에 접근하고 공유할 수 있다는 편리함 뒤에는 보안의 위험이 숨어있습니다. 계정 관리를 조금만 소홀히 하거나, 데이터 접근 권한 설정을 잘못하면 정보가 유출될 위험이 있습니다.

5. 출력물

아날로그 방식이지만 여전히 위험한 '출력물'도 잊어서는 안 됩니다. 중요 정보가 담긴 문서를 제대로 폐기하지 않으면, 누군가 악의를 가지고 정보를 빼낼 수 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

5차시

학습자료

시스템 오류 및 관리 부실 대응 방안 _ 정보 관리 체계 구축

1. 정보 자산 분류 및 목록화

기업이 보유한 정보 자산을 중요도, 기밀성, 가용성 등의 기준에 따라 분류하고 목록화해야 합니다. 예를 들어, 고객의 개인정보는 기밀성이 높은 정보 자산으로 분류되어 엄격하게 처리됩니다. 이렇게 정보 자산을 분류하고 목록화하면 각 자산의 가치를 평가하고, 그에 맞는 보안 수준을 설정할 수 있습니다.

2. 접근 통제 정책 수립 및 이행

직원의 직급이나 업무 내용에 따라 정보 접근 권한을 다르게 부여하고, 불필요한 정보 접근을 제한해야 합니다. 예를 들어, 임원에게는 모든 정보에 대한 접근 권한을 부여하고, 일반 직원에게는 업무에 필요한 정보에 대한 접근 권한만 부여하는 것이죠. 또한, 누가 언제 어떤 정보에 접근했는지 기록을 남겨서 문제가 생겼을 때 추적하고 책임 소재를 명확히 할 수 있어야 합니다.

3. 정보 생명 주기 관리

정보는 생성부터 폐기까지 전 단계에 걸쳐 체계적으로 관리되어야 합니다. 정보가 생성될 때 보안 등급을 부여하고, 사용 목적에 따라 접근 권한을 관리하며, 불필요한 정보는 안전하게 폐기해야 합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

5차시

학습자료

시스템 오류 및 관리 부실 대응 방안 _ 정기적인 점검 및 감사

1. 취약점 점검

취약점 점검 도구를 사용하여 시스템의 약한 부분을 찾아내는 과정입니다. 예를 들어, 웹 애플리케이션 취약점 점검 도구를 사용하면 SQL Injection, XSS 등 해커들이 악용할 수 있는 취약점을 찾아내고, 보안 패치를 적용하여 이를 해결할 수 있습니다.

2. 보안 감사

정보보안 정책, 절차, 시스템 등이 제대로 작동하고 있는지 확인하는 과정입니다. 외부 전문 기관의 시각으로 꼼꼼하고, 객관적인 평가를 받는 것이 좋습니다. 예를 들어, 개인정보보호법 준수 여부, 정보보안 정책 이행 현황, 보안 시스템 운영 상태 등을 감사하여 미비점을 보완할 수 있습니다.

3. 로그 분석

시스템의 활동 기록을 꼼꼼히 살펴보는 과정입니다. 시스템 로그를 분석하면 비정상적인 활동이나 시스템 오류를 탐지할 수 있습니다. 예를 들어, 특정 사용자가 비인가 된 정보에 접근했는지, 악성코드 감염 시점은 언제인지 등을 파악하여 정보 유출 사고의 원인을 분석하고 재발을 방지할 수 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

6차시

학습자료

IoT 기기 보안 취약점

1. 사용자들의 보안 인식 부족

IoT 기기를 처음 설정할 때 기본 비밀번호를 그대로 사용하는 경우 개인정보가 유출 될 위험이 커집니다. 또한 귀찮다는 이유로 보안 패치 업데이트를 미루는 경우가 있는데, 소프트웨어 업데이트에는 보안 취약점을 보완하는 중요한 패치가 포함되어 있기 때문에 반드시 즉시 업데이트해야 합니다.

2. 제조사 측면 문제

IoT 기기는 저렴한 가격으로 경쟁해야 하다 보니, 보안 기능 강화에 필요한 비용을 투자하기가 쉽지 않습니다. 따라서 보안에 취약한 저가 부품을 사용하거나 보안 전문 인력을 충분히 확보하지 못하는 경우가 많습니다.

3. IoT 기기 자체의 기술적 한계

IoT 기기는 작고 저렴하게 만들어야 하기 때문에, 고성능 보안 기능을 탑재하기 어려울 수 있습니다. 예를 들어, 스마트 전구나 스마트 플러그 같은 소형 IoT 기기는 저장 공간이나 처리 능력이 제한적이기 때문에 강력한 암호화 기술을 적용하기 어려울 수 있습니다. 게다가 수많은 종류의 IoT 기기가 존재하기 때문에 모든 기기에 적용할 수 있는 표준화된 보안 기술을 개발하는 것도 쉽지 않습니다. 이러한 기술적 한계는 IoT 기기 보안 강화를 위한 노력을 더욱 어렵게 만듭니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

6차시

학습자료

기업의 IoT 기기 보안 강화 방안

1. 기업은 IoT 기기를 만들 때부터 보안을 염두에 두어야 합니다. 안전한 하드웨어와 소프트웨어를 사용하고, 강력한 암호화 기술을 적용하며, 혹시 모를 취약점을 찾아내기 위한 점검도 철저히 해야 합니다.
2. 보안 취약점이 발견되면 신속하게 패치를 제공하고, 사용자들이 쉽게 업데이트할 수 있도록 지원해야 합니다. 자동 업데이트 기능을 제공하거나, 업데이트 알림을 통해 사용자에게 업데이트 필요성을 알리는 것도 좋은 방법입니다.
3. 사용자 인증 강화도 중요합니다. 비밀번호 외에도 지문, 홍채 인식, 일회용 비밀번호(OTP) 등 다양한 인증 방식을 적용하여 보안 수준을 높여야 합니다. 이렇게 하면 비밀번호가 유출되더라도 추가적인 인증 절차를 거쳐야 하기 때문에 해킹 위험을 줄일 수 있습니다.
4. 사용자들이 IoT 기기를 안전하게 사용할 수 있도록 상세한 보안 가이드라인을 제공해야 합니다. 복잡한 기술 용어는 쉬운 용어로 바꾸고, 그림이나 동영상 등 시각 자료를 활용하여 누구나 쉽게 이해할 수 있도록 해야 합니다.
5. IoT 기기 보안의 중요성을 알리고 사용자들이 보안 수칙을 잘 지키도록 교육하고 홍보하는 것도 기업의 중요한 역할입니다. 온라인 교육, 오프라인 세미나, 홍보 자료 배포 등 다양한 방법을 활용하여 사용자들의 보안 의식을 높여야 합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

6차시

학습자료

개인의 IoT 기기 보안 강화 방안

1. 안전한 비밀번호 설정

가장 기본적인지만 중요한 것은 '안전한 비밀번호 설정'입니다. 반드시 기본 비밀번호를 변경하고, 추측하기 어려운 복잡한 비밀번호를 설정해야 합니다. 여러 기기에 동일한 비밀번호를 사용하는 것도 피해야 합니다. 주기적으로 비밀번호를 변경하고, 2단계 인증을 활용하는 것도 좋은 방법입니다.

2. 소프트웨어 업데이트

최신 소프트웨어 업데이트는 필수입니다. 보안 패치는 IoT 기기의 취약점을 보완해 주는 역할을 하기 때문에, 제조사에서 제공하는 보안 패치는 꼭 즉시 적용해야 합니다.

3. 안전한 네트워크 사용

공공 와이파이 등 안전하지 않은 네트워크에 IoT 기기를 연결하면 해커들이 데이터를 가로챌 수 있습니다.

4. 의심스러운 링크 클릭 금지

의심스러운 링크 클릭 금지는 너무나 당연한 이야기지만, 여전히 많은 사람들이 이를 간과하고 있습니다. 출처가 불분명한 이메일이나 문자 메시지의 링크는 절대 클릭하지 말아야 합니다.

5. 보안 설정 확인

IoT 기기를 구매하거나 사용하기 전에 '보안 설정'을 꼼꼼하게 확인해야 합니다. 방화벽 설정, 원격 접속 제한, 로그 기록 설정 등을 통해 보안 수준을 높일 수 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

7차시

학습자료

클라우드 보안 취약점

1. 클라우드 서비스는 기본적으로 온라인 접근성이 뛰어납니다. 인터넷만 연결되어 있다면 언제 어디서든 접근할 수 있다는 점은 엄청난 편리함을 제공하지만, 동시에 해커들에게도 손쉬운 접근 기회를 제공합니다.
2. 클라우드는 여러 사용자가 자원을 공유하는 다중 사용자 환경입니다. 클라우드 환경에서도 한 사용자의 실수나 부주의, 또는 악의적인 행동이 다른 사용자에게까지 영향을 미칠 수 있습니다.
3. 클라우드 서비스는 가상화 기술을 기반으로 운영됩니다. 가상화는 하나의 물리적인 서버를 여러 개의 가상 서버로 나누어 사용하는 기술인데, 이는 마치 하나의 컴퓨터를 여러 사람이 동시에 사용하는 것과 같습니다. 이렇게 되면 각각의 가상 서버는 물리적인 서버보다 보안에 취약해질 수밖에 없습니다.
4. 클라우드 환경에서는 여러 사용자가 자원을 공유하기 때문에, 한 사용자의 시스템이 악성코드에 감염되면 다른 사용자의 시스템에도 영향을 미칠 수 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

7차시

학습자료

클라우드 안전하게 이용하기

1. 클라우드 워크로드 보호 플랫폼(CWPP)
클라우드 서버를 지켜주며, 침입 탐지 및 방지, 웹 애플리케이션 방화벽, 파일 무결성 감시 등 다양한 기능으로 서버를 24시간 지켜줍니다.
2. 클라우드 접근 보안 중개(CASB)
클라우드 서비스 사용자의 접근을 제어하고 데이터 유출을 방지합니다. 사용자 인증, 권한 관리, 데이터 암호화 등 다양한 기능으로 클라우드 서비스에 대한 접근을 철저하게 통제합니다.
3. 클라우드 보안 형상 관리(CSPM)
클라우드 환경의 보안 설정을 끊임없이 감시하고, 규정 준수 여부를 확인합니다. 잘못된 설정이나 취약점을 자동으로 찾아내고 수정하여 보안 사고를 예방합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

8차시

학습자료

기업의 정보보안 거버넌스

정보보안 거버넌스

정보보안 거버넌스는 기업의 정보보안 관리 체계를 의미하며, 기업의 정보 자산을 지키고, 정보보안 위협을 관리하기 위한 모든 활동을 포괄한다고 할 수 있습니다. 기술적인 보안 시스템 구축은 물론이고, 정보보안 정책 수립, 직원 교육, 사고 대응, 감사 및 평가 등 정보보안과 관련된 모든 활동이 포함됩니다.

기업의 정보보안 거버넌스 필요성

1. 기업의 정보 자산 보호

고객 정보, 영업 비밀, 기술 정보 등은 기업의 가치를 창출하고 유지하는 데 중요한 역할을 합니다. 정보보안 거버넌스는 이러한 정보 자산을 안전하게 지키는 역할을 합니다.

2. 위험 관리

정보보안 거버넌스는 지속적으로 발전하고 있는 해킹 기술과 위협을 미리 파악하고 평가하여, 적절한 대응 방안을 마련하고 실행하는 체계적인 시스템입니다.

3. 법규 준수

개인정보보호법, 정보통신망법 등 정보보안 관련 법규는 점점 강화되고 있습니다. 법규를 위반하면 막대한 벌금이나 영업 정지 등의 제재를 받을 수 있고, 기업 이미지에도 큰 타격을 입을 수 있습니다. 정보보안 거버넌스는 기업이 관련 법규를 준수하고 법적 책임을 다할 수 있도록 지원합니다.

4. 기업 경영 효율성 증대

정보보안 거버넌스는 정보보안 관련 의사결정 체계를 명확히 하고, 효율적인 정보보안 관리 시스템을 구축하여 기업 경영의 효율성을 높이는 데 기여합니다. 예를 들어, 중복 투자를 방지하고, 보안 예산을 효율적으로 배분하며, 정보보안 사고 발생 시 신속하고 효과적인 대응을 가능하게 합니다.

5. 고객 신뢰 확보

정보보안 거버넌스를 통해 고객 정보를 안전하게 보호하고, 정보보안 사고 발생 시 투명하게 대응함으로써 고객 신뢰를 얻고 유지할 수 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

8차시

학습자료

정보보안 위협 관리의 단계

1. 위협 식별 단계

회사 정보 자산에 어떤 위협이 있는지 파악합니다. 예를 들어, 고객 개인정보를 다루는 회사라면 해킹, 랜섬웨어, 내부 직원의 정보 유출 등이 위협 요인이 될 수 있습니다.

2. 위협 분석 및 평가 단계

각 위협 요인이 얼마나 위험한지 점수를 매깁니다. 숫자로 계산하는 방식도 있고, 전문가의 판단에 따라 평가하는 방식도 있습니다.

3. 위협 대응

위험 평가 결과를 바탕으로 어떻게 대응할지 결정합니다. 위험을 피하거나, 줄이거나, 다른 곳으로 넘기거나, 감수하는 등 다양한 방법이 있습니다. 예를 들어, 랜섬웨어 감염 위험이 높다면, 랜섬웨어 대응 솔루션을 도입하고, 데이터 백업을 강화하고, 직원 교육을 실시하는 등의 대응 방안을 실행할 수 있습니다.

4. 위협 모니터링 및 검토

위험 관리 활동이 잘 되고 있는지 지속적으로 확인하고, 필요하면 계획을 수정해야 합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

9차시

학습자료

방화벽의 종류

1. 패킷 필터링 방화벽

가장 기본적인 패킷 필터링 방화벽은 네트워크 계층에서 패킷의 출발지 IP 주소, 목적지 IP 주소, 포트 번호 등을 기반으로 패킷을 허용하거나 차단합니다. 간단하고 빠르지만, 애플리케이션 계층의 공격에는 취약하다는 단점이 있습니다.

2. 상태 저장 방화벽

네트워크 계층과 전송 계층에서 패킷의 상태 정보를 기반으로 패킷을 허용하거나 차단합니다. 패킷 필터링 방화벽보다 보안성이 높지만, 애플리케이션 계층의 공격에는 여전히 취약합니다.

3. 애플리케이션 레벨 게이트웨이(ALG)'는 애플리케이션 계층에서 패킷의 내용을 검사하여 특정 애플리케이션의 트래픽을 허용하거나 차단합니다. 애플리케이션 계층의 공격을 방어할 수 있지만, 성능이 저하될 수 있다는 단점이 있습니다.

4. 차세대 방화벽(NGFW)

패킷 필터링, 상태 저장, ALG 기능을 모두 제공하며, 침입 방지 시스템(IPS), 웹 필터링, 애플리케이션 제어 등 다양한 보안 기능을 통합적으로 제공합니다. 보안성도 높고 다양한 기능을 제공하지만, 비용이 비싸다는 단점이 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

10차시

학습자료

정보 접근 통제 모델

1. 임의 접근 통제(DAC)

정보 자산 소유자가 접근 권한을 부여하는 방식입니다. 예를 들어, 여러분이 작성한 보고서에 대해 누가 접근할 수 있는지 여러분 스스로 결정하는 것입니다.

2. 강제 접근 통제(MAC)

보안 등급에 따라 정보 접근 권한을 부여하는 방식입니다. 정보 자산과 사용자에게 각각 보안 등급을 부여하고, 높은 등급의 사용자만 낮은 등급의 정보에 접근할 수 있도록 제한합니다.

3. 역할 기반 접근 통제

직원의 역할에 따라 정보 접근 권한을 부여하는 방식입니다. 예를 들어, 영업팀 직원은 고객 정보에 접근할 수 있지만, 회계 정보에는 접근할 수 없도록 하는 것입니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

11차시

학습자료

데이터 백업

1. 전체 백업

전체 백업은 모든 데이터를 백업하는 가장 안전한 방법이지만, 시간이 오래 걸리고 저장 공간을 많이 차지한다는 단점이 있습니다.

2. 증분 백업

증분 백업은 마지막 전체 백업 이후 변경된 데이터만 백업하는 방식으로, 백업 시간은 짧지만, 복구 시 시간이 오래 걸릴 수 있습니다.

3. 차등 백업은 마지막 전체 백업 이후 변경된 데이터만 백업하지만, 증분 백업과 달리 매번 전체 백업과 비교하여 변경된 데이터를 백업합니다. 복구 시간이 짧다는 장점이 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

12차시

학습자료

정보보안 전문가

정보보안 전문가는 보안 시스템 구축부터 운영, 취약점 분석 및 대응, 보안 사고 발생 시 신속한 대처, 직원 보안 교육 등과 같은 역할을 합니다.

하지만 안타깝게도 정보보안 전문 인력은 턱없이 부족한 상황입니다. 이는 전 세계적인 문제인데요, 기업들은 보안 전문가를 구하기 위해 치열한 경쟁을 벌이고 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

12차시

학습자료

정보보안 문화의 정착

1. 경영진의 강력한 의지와 지원

정보보안 문화를 정착시키기 위해서는 경영진의 지속적인 관심과 지원이 필수적입니다.

2. 직원들에게 정기적인 정보보안 교육 실시

정보보안에 대한 이해도를 높이고 보안 의식을 강화해야 하며, 정보보안 교육을 통해 직원들의 보안 역량을 강화해야 합니다.

3. 보안 캠페인 및 홍보 활동

보안 캠페인이나 홍보 활동을 통해 정보보안에 대한 관심을 유도하고, 보안 수칙 준수를 독려해야 합니다.

4. 보안 인센티브 제도

보안 인센티브 제도를 도입하는 것도 좋은 방법입니다. 정보보안 활동에 적극적으로 참여하는 직원에게 인센티브를 제공하여 보안 의식을 고취하고, 정보보안 문화 정착을 유도할 수 있습니다.

5. 사고 발생 시 원인 규명 및 대책 마련

정보보안 사고가 발생했을 때, 사고 내용과 원인을 분석하고 재발 방지 대책을 마련하여 전 직원과 공유해야 합니다. 이를 통해 직원들은 정보보안 위협에 대한 경각심을 갖고, 보안 수칙 준수의 중요성을 깨닫게 됩니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

13차시

학습자료

개인정보보호법

1. 개인정보를 수집할 때는 수집 목적과 항목, 보유 기간 등을 명확하게 알리고, 정보 주체의 동의를 얻어야 합니다. 예를 들어, 온라인 쇼핑몰에서 회원 가입을 할 때, 쇼핑몰은 회원 가입 약관에 개인정보 수집 및 이용 목적, 수집 항목, 보유 기간 등을 명시하고, 이용자의 동의를 받아야 합니다.
2. 수집된 개인정보는 명시된 목적 범위 안에서만 이용해야 합니다. 예를 들어, 마케팅 목적으로 수집한 개인정보를 고객 상담이나 민원 처리에 사용하면 안 되는 것이죠. 또한, 정보 주체의 권리를 보장해야 합니다. 정보 주체는 자신의 개인정보를 열람하고, 정정하고, 삭제할 권리가 있습니다. 만약 쇼핑몰에서 회원 탈퇴를 원할 경우, 쇼핑몰은 해당 회원의 개인정보를 삭제해야 할 의무가 있습니다.
3. 개인정보를 제3자에게 제공할 때도 정보 주체에게 제공 사실을 알리고 동의를 얻어야 합니다. 예를 들어, 보험회사가 고객의 개인정보를 제휴 병원에 제공하려면, 고객에게 어떤 정보를 어떤 목적으로 제공하는지 알리고 동의를 받아야 합니다.
4. 개인정보는 안전하게 관리해야 합니다. 기술적인 보호 조치는 물론이고, 직원 교육, 출입 통제 등 관리적인 보호 조치, 그리고 안전한 시설 및 장비 구축 등 물리적인 보호 조치까지 총체적으로 이루어져야 합니다. 예를 들어, 기업은 개인정보 데이터베이스에 암호화 기술을 적용하고, 접근 권한을 제한하며, 데이터센터에 CCTV를 설치하는 등 다양한 보안 조치를 해야 합니다.
5. 보유 기간이 지났거나 처리 목적이 달성된 개인정보는 지체 없이 파기해야 합니다. 예를 들어, 쇼핑몰에서 회원 탈퇴를 한 경우, 쇼핑몰은 해당 회원의 개인정보를 파기해야 할 의무가 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

13차시

학습자료

정보통신망법에 따른 정보통신 서비스 제공자의 의무

1. 접근 통제를 통해 허가받지 않은 사람이 정보통신망에 함부로 접근하지 못하도록 막아야 합니다.
2. 침입 차단 시스템을 구축하여 해킹 등 침입 시도를 조기에 탐지하고 차단해야 합니다.
3. 개인 정보는 암호화하여 저장하고 전송해야 합니다.
4. 보안 취약점을 정기적으로 점검하고 발견된 취약점은 신속하게 조치해야 합니다.
5. 정보보호 관리 체계(ISMS) 인증을 획득하여 정보보안 수준을 향상시켜야 합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

14차시

학습자료

금융보안원

1. 금융보안원은 금융 정보보호 관련 정책을 수립하고 시행하며, 금융회사의 정보보호 수준을 평가하고 감독합니다. 또한, 금융 정보보호 표준 개발, 금융 정보보호 기술 연구개발, 금융 정보보호 인력 양성 등을 통해 금융권 정보보호 수준을 향상시키는 데 기여하고 있습니다.
2. 금융보안원은 금융회사 간 사이버 위협 정보를 공유하고 분석하여 금융권 전체의 정보보호 수준을 높이는 데 기여하고 있습니다.
3. 금융권 침해사고 대응 훈련을 실시하여 금융회사의 침해사고 대응 능력을 강화하고 있습니다. 2023년에는 금융권 사이버 위협 정보 공유 시스템을 고도화하여 실시간 정보 공유 및 분석 체계를 구축했습니다.
4. 금융보안원은 금융회사를 대상으로 금융 IT 보안 컨설팅 및 기술 지원 서비스도 제공합니다. 보안 취약점 점검, 보안 시스템 구축, 보안 교육 등 다양한 지원을 통해 금융회사의 정보보안 수준을 향상시키는 데 도움을 주고 있습니다.
5. 금융보안원은 금융 정보보호 인력 양성을 위한 교육 프로그램도 운영하고, 금융 정보보호 관련 자격증 시험도 주관합니다. 또한, 금융 정보보호 포털, 홍보 자료 등을 통해 금융 소비자의 정보보호 인식을 높이는 데 노력하고 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

14차시

학습자료

우리나라의 정보보안 관련 기관 및 단체

1. 과학기술정보통신부

과학기술정보통신부는 정보보호 정책의 총사령관이라고 할 수 있습니다. 정보보호 관련 법률을 만들고 개정하고, 정보보호 산업을 육성하고, 정보보호 인력을 양성하는 등 정보보호 정책 전반을 총괄하는 부처입니다.

2. 개인정보보호위원회

개인정보보호위원회는 개인정보보호법의 독립적인 집행 기관입니다. 개인정보 침해 신고를 접수하고 조사하며, 시정 조치나 과징금 부과 등 필요한 조치를 취합니다.

3. 경찰청 사이버안전국

경찰청 사이버안전국은 사이버 범죄 수사 및 예방을 담당하는 경찰 조직입니다. 해킹, 랜섬웨어, 개인정보 유출 등 사이버 범죄에 대한 수사를 진행하고, 사이버 범죄 예방 교육 및 홍보 활동을 수행합니다.

4. 한국정보보호산업협회(KISIA)

한국정보보호산업협회는 정보보호 산업 발전을 위한 기업들의 협의체입니다. 정보보호 기술 개발, 정보보호 산업 육성, 정보보호 인력 양성 등 다양한 사업을 추진하고 있습니다. 매년 '정보보호의 날' 행사를 개최하여 정보보호 산업 발전에 기여하고 있으며, 정보보호 관련 기업들의 목소리를 대변하고 정부와 협력하여 정보보호 산업 발전을 위한 정책을 제안하는 역할도 수행합니다.

5. 한국침해사고대응팀협의회(CONCERT)

한국침해사고대응팀협의회는 국내 주요 기업 및 기관의 정보보호 담당자들이 참여하는 협의체입니다. 사이버 위협 정보를 공유하고, 침해사고 발생 시 공동 대응하며, 정보보호 기술 연구 등을 통해 국내 정보보호 수준을 향상시키는 데 기여하고 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

15차시

학습자료

정보보안 자격증 취득이 기업에게 주는 혜택

1. 정보보안 수준 한 단계 상승

전문가가 직접 보안 시스템을 구축하고 운영하기 때문에, 보안 사고 발생 가능성을 낮출 수 있습니다.

2. 고객에게 안전한 서비스 제공

고객에게 안전한 서비스를 제공하여 기업 이미지를 높이는 데도 기여합니다. 정보보안 전문가가 있다는 사실만으로도 고객들에게 신뢰감을 줄 수 있습니다.

3. 정보보안 관련 법규 및 규제 준수에도 도움을 받을 수 있습니다. 정보보안 전문가는 관련 법규에 대한 전문 지식을 갖추고 있기 때문에, 기업이 법적 책임을 다하는 데 큰 도움이 됩니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

16차시

학습자료

인공지능(AI) 기반 범죄

1. 딥페이크(Deepfake) 기술은 인공지능을 이용하여 사람의 얼굴이나 목소리를 합성하는 기술입니다. 해커들은 딥페이크 기술을 이용하여 실제 인물처럼 위장하고, 피해자를 속여 금융 정보를 탈취하거나 불법적인 거래를 유도합니다.

2. AI는 취약점 분석, 악성코드 제작, 공격 실행 등 해킹 과정을 자동화하여 공격 효율성을 높이고 방어를 어렵게 만듭니다. 2022년에는 한 해커 그룹이 AI 기반 자동화 도구를 이용하여 수백 개의 웹사이트를 동시에 공격하여 마비시킨 사건이 발생하기도 했습니다.

3. AI는 개인정보 수집 및 분석을 통해 맞춤형 피싱 이메일이나 메시지를 작성하여 공격 성공률을 높입니다. 마치 타겟 광고처럼, 개인의 관심사나 약점을 정확히 파악하여 유혹적인 미끼를 던집니다.

4. AI는 사람의 심리를 분석하고, 이를 이용하여 사회 공학적 공격을 자동화합니다. 예를 들어, AI는 가짜 뉴스를 생성하고 유포하여 여론을 조작하거나, 특정 개인을 표적으로 삼아 악성 루머를 퍼뜨릴 수 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

16차시

학습자료

인공지능 기술 발전에 따른 윤리적 문제 _ 편향된 데이터 학습

1. 학습 데이터의 다양성

AI 학습 데이터의 다양성을 확보해야 합니다. 다양한 인종, 성별, 연령, 문화적 배경을 가진 사람들의 데이터를 포함하여 AI가 공정하고 객관적인 판단을 내릴 수 있도록 해야 합니다.

2. 알고리즘 작동 방식 공개 및 검증

AI 알고리즘의 작동 방식을 투명하게 공개하고, 외부 전문가의 검증을 받아야 합니다. 이를 통해 AI 시스템의 편향성을 확인하고 개선할 수 있습니다.

3. 결과에 대한 책임

AI 시스템이 차별적인 결과를 도출할 경우, AI 개발자와 운영자는 AI 시스템의 결과에 대한 책임을 져야 합니다.

4. 모니터링 및 개선

AI 시스템은 지속적으로 모니터링하고, 편향성이 발견될 경우 즉시 개선해야 합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

17차시

학습자료

블록체인의 특징

1. 중앙 서버 없이 여러 참여자들이 분산된 네트워크를 통해 데이터를 관리하기 때문에 데이터의 위변조 및 해킹 위험을 줄이고, 시스템의 투명성과 신뢰성을 높입니다.

2. 블록체인에 기록된 데이터는 변경하거나 삭제할 수 없기 때문에 데이터의 무결성을 보장합니다. 이는 데이터의 신뢰성을 높이고, 정보 유출 및 훼손 위험을 줄이는 데 기여합니다.

3. 블록체인은 모든 거래 내역이 블록체인에 기록되고 공개되기 때문에 데이터의 투명성을 보장합니다. 누구든지 블록체인에 기록된 정보를 확인할 수 있으며, 이는 데이터의 신뢰성을 높이는 데 기여합니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

17차시

학습자료

블록체인의 데이터 무결성과 보안 강화

1. 블록체인에 저장되는 데이터를 암호화하여 데이터 유출 시에도 정보를 보호합니다.
2. 블록체인 네트워크 참여자의 접근 권한을 관리하여 허가받지 않은 사용자의 접근을 차단합니다.
3. 스마트 계약은 블록체인 상에서 자동으로 실행되는 계약으로, 데이터 처리 과정을 투명하게 관리하고, 위변조를 방지합니다.
4. 데이터를 여러 노드에 분산 저장하여 데이터 손실 위험을 줄이고, 시스템 안정성을 높입니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

18차시

학습자료

양자 컴퓨팅

양자 컴퓨팅은 양자 역학의 원리를 이용하여 정보를 처리하는 기술로, 기존 컴퓨터와는 완전히 다른 방식으로 작동합니다. 기존 컴퓨터는 0과 1, 즉 비트(bit) 단위로 정보를 처리하는 반면, 양자 컴퓨터는 큐비트(qubit)라는 양자 정보 단위를 사용합니다. 이 큐비트는 0과 1의 상태를 동시에 가질 수 있는 신기한 특징을 가지고 있으며, 이러한 큐비트의 특성 덕분에 양자 컴퓨터는 기존 컴퓨터보다 훨씬 빠르고 효율적인 연산을 수행할 수 있습니다.

양자 컴퓨터의 성능은 큐비트 수와 게이트 연산 정확도에 따라 결정됩니다. 현재는 큐비트 수가 제한적이고 게이트 연산 오류율이 높지만, 기술 발전에 따라 큐비트 수가 증가하고 오류율이 감소하면 양자 컴퓨터의 성능은 기하급수적으로 향상될 것입니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

18차시

학습자료

양자 컴퓨터의 기존 암호화 기술 무력화 문제

1. 개인정보 유출

인터넷 뱅킹, 전자상거래 등에서 사용되는 개인정보가 유출될 수 있습니다. 암호화 기술이 무력화되면 개인정보는 해커들의 손쉬운 먹잇감이 될 수 있습니다.

2. 금융 시스템 마비

금융 거래 정보가 유출되거나 변조되어 금융 시스템이 마비될 수 있습니다. 금융 시스템 마비는 경제 전체를 마비시킬 수 있는 심각한 문제입니다.

3. 국가 안보 위협

국가 기밀 통신이 해독되어 국가 안보가 위협받을 수 있습니다. 마치 적군에게 군사 기밀이 유출되는 것처럼, 양자 컴퓨터는 국가 안보에 치명적인 위협이 될 수 있습니다.

4. 사회 혼란

암호화 기술에 의존하는 다양한 시스템이 무력화되어 사회 혼란이 발생할 수 있습니다. 마치 전력 시스템이 마비되어 도시 전체가 암흑에 빠지는 것처럼, 암호화 기술 무력화는 사회 시스템 붕괴로 이어질 수 있습니다.

기업 정보보안, 생존을 위한 필수 전략 - 위협과 대응의 모든 것

19차시

학습자료

인공지능(AI)을 활용한 정보보안 강화

1. 인공지능(AI)은 방대한 데이터를 빠르게 분석하고 패턴을 학습하여 새로운 위협을 예측하고 대응하는데 탁월한 능력을 발휘합니다.
2. 이상 탐지 시스템은 AI의 대표적인 활용 사례입니다. 이 시스템은 정상적인 시스템 또는 네트워크 활동과 다른 이상 행위를 탐지하여 보안 위협을 예방합니다. 예를 들어, AI는 네트워크 트래픽, 시스템 로그, 사용자 행위 등을 분석하여 비정상적인 패턴을 감지하고, 해킹 시도나 악성코드 감염을 조기에 탐지할 수 있습니다.
3. 자동화된 보안 분석도 AI의 중요한 역할입니다. AI는 방대한 보안 로그, 이벤트 데이터 등을 분석하여 보안 위협을 탐지하고 신속하게 대응할 수 있도록 지원합니다. 예를 들어, 보안 로그를 분석하여 악성코드 감염 여부를 판단하고, 침입 경로를 추적하여 추가 피해를 예방할 수 있습니다.
4. AI는 또한 위협 인텔리전스 분야에서도 활약합니다. 다양한 소스에서 수집된 위협 정보를 분석하여 새로운 위협을 예측하고, 선제적으로 대응할 수 있도록 지원합니다. AI는 최신 해킹 기법, 악성코드 유형, 공격 패턴 등을 분석하여 기업의 보안 시스템을 강화하고, 잠재적인 위협에 대비할 수 있도록 돕습니다.