



보안 소개

© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

보안 소개를 시작하겠습니다.


교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- 기밀성, 무결성, 가용성(CIA)의 세 가지 측면에서 보안을 정의합니다.
- 여러 유형의 위협을 파악합니다.
- 보안 전략을 구성하는 요소를 파악합니다.
- 해킹, 크래킹, 침투 테스트의 차이점을 설명합니다.
- 보안 수명 주기 단계의 이름을 파악합니다.
- 사이버 법률과 규정이 조직의 보안 정책에 미치는 영향을 설명합니다.





보안이란?

토론: 보안 소개



4

며칠 동안 인터넷이 끊기면 여러분의 삶에 어떤 영향이 있습니까?

여러분의 개인 정보가 도난당하면 어떤 영향이 있습니까?

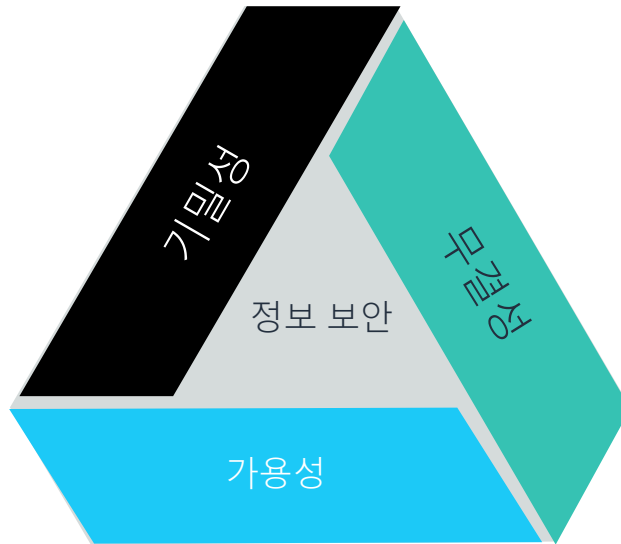
이런 일이 발생하지 않게 하기 위해 어떤 제어 조치를 마련해 두었습니까?



컴퓨터 및 관련 기술은 우리의 업무 환경과 개인 활동에 녹아 있으므로 보안은 누구에게나 중요해졌습니다.

IT 보안, 즉 사이버 보안은 컴퓨터와 네트워크, 프로그램, 데이터를 의도치 않거나 악의적인 액세스, 변경, 파괴로부터 보호하는 일입니다. 또한 합리적인 대응 또는 처리 속도로 방해를 최소화하며 비즈니스 기능과 개인 태스크를 계속해서 수행할 수 있도록 하는 일이기도 합니다.

보안이란?



5

aws re/start

이것이 바로 기밀성, 무결성, 가용성(CIA) 삼각형입니다. 정보 보안을 평가할 때는 여기에 있는 세 가지 중요한 관점을 고려해야 합니다.

- **기밀성** - 무단 액세스를 예방하기 위해 프라이빗 데이터가 보호되는가?
- **무결성** - 데이터가 조작되지 않고 정확하며 진본성을 유지하도록 조치가 구현되어 있는가?
- **가용성** - 권한이 있는 사용자가 필요할 때 데이터에 액세스할 수 있는가?

보안이 중요한 이유

보안이 열악하면 직원과 조직이 다음과 같은 보안 위험에 노출됩니다.



아이덴티티 도난



데이터 도난



네트워크 서비스
및 리소스 손실



비즈니스 평판
실추 또는 손상



기업 방해 공작
또는 간첩 행위

- **아이덴티티 도난** - 다음과 같은 개인 식별 번호(PII)를 목표로 하는 이벤트입니다.
 - 이름
 - 생일
 - 암호
 - 은행 계좌
 - 신용카드 번호
- **데이터 도난** - 절도범이 기업의 기밀 데이터 또는 지적 재산(IP)을 훔칠 수 있으며 데이터를 판매하려고 하거나 소유자에게 돌려주는 대신 배상금을 요구할 수 있습니다.
- **네트워크 서비스 또는 리소스 손실** - 네트워크 서비스를 목표로 하는 이벤트입니다. 이런 서비스가 중단되면 조직이 비즈니스를 수행할 수 없게 될 수 있습니다.
- **기업 방해 공작 또는 간첩 활동** - 경쟁 기업에서 경쟁 우위를 점하기 위해 간첩 활동을 수행할 수 있습니다. 불만을 품은 직원이 기업에 방해 공작을 하기 위해 기업 내부에서 이벤트를 시작할 수 있습니다.
- **비즈니스 평판 실추 또는 손상** - 이러한 이벤트는 잠재적으로 비즈니스 평판 실추로 이어질 수 있습니다. 기업이 서비스를 제공할 수 없게 되면 고객은 다

른 곳과 거래하게 될 수 있습니다. IP 도난은 기업이 시장 점유율을 획득하는
능력을 약화시킬 수 있습니다. 기업에서 고객 데이터를 도난당해서 고객이 아
이덴티티 도난의 위험에 처하게 할 수도 있습니다.

위협 유형

- 적절한 보안 조치로 다음과 같은 위협을 완화할 수 있습니다.
 - 맬웨어
 - 암호 이벤트(사전, 무차별 대입)
 - 분산 서비스 거부(DDoS)
 - 중간자 공격(MITM)
 - 피싱
 - 소셜 엔지니어링
 - 드라이브 바이

- **맬웨어** - 컴퓨터 시스템을 방해하거나 손상을 입히거나 무단 액세스를 획득하기 위해 설계된 소프트웨어. (Oxford 사전)
- **암호 이벤트** - 컴퓨터 시스템에 저장되거나 컴퓨터 시스템에서 전송된 데이터에서 암호를 복구하는 프로세스
- **분산 서비스 거부(DDoS)** - 하나의 시스템에 침입하기 위해 침입을 받은 여러 개의 시스템이 사용됨
- **중간자** - 서로 직접 통신하고 있다고 믿는 두 주체 사이의 통신을 외부 주체가 비밀스럽게 중계함
- **피싱** - 외부 주체가 암호 또는 신용카드 번호와 같은 개인 정보를 얻기 위해 합법적인 기업 행세를 하는 이메일 메시지를 전송함
- **소셜 엔지니어링** - 보안 세부 정보에 대한 액세스를 얻어 시스템에 침입하기 위해 사람과의 교류를 이용하여 사람을 조종하는 이벤트
- **드라이브 바이** - 사이버 범죄자가 보안되지 않은 웹 사이트를 사용하여 악성 코드를 심고 사용자의 컴퓨터에 자동으로 다운로드되도록 함



보안 전략

보안의 유형

시스템 보안

인프라 보안

액세스 관리

아이덴티티 관리

데이터 보안

소프트웨어 보안

물리적 보안

전략



물리적 보안



액세스 관리



알려진 보안 위험 및
일반적인 부정 이용 행위



정책 및 절차

적절히 예방 조치를 취하면 보안 문제가 발생할 확률이 줄어들고, 문제가 발견 되었을 때 미치는 영향 또한 줄어듭니다. 사용할 수 있는 도구는 다음과 같습니다.

- **물리적 보안** - 물리적 액세스는 더 광범위하고 의도하지 않은 액세스로 이어 집니다. 먼저 리소스에 대한 물리적 액세스를 제어하십시오. (이 내용은 이 과정에서 다루는 범위를 벗어납니다.)
- **액세스 관리** - 리소스에 대한 액세스를 제어하십시오. 액세스를 더 많이 제어 할수록 환경이 더 안전해집니다. 액세스할 수 있는 사람을 제어하고 사용자가 본인이 맞는지 신원을 확인하는 등의 제어 조치를 고려해 보십시오.
- **알려진 보안 위험 및 일반적인 부정 이용 행위** - 패치가 출시되고 난 후 가능한 한 빨리 취약성을 패치함으로써 영향의 범위를 줄이십시오. 패치가 가능하지 않다면 다른 보안 조치를 구현합니다.
- **정책 및 절차** - 모든 보안 전략을 설정하고 관리하는 방법, 보안 이벤트가 발생했을 때 처리하는 방법 등을 설명하십시오.

토론



기업에서는 다양한 수준과 유형의 보안 제어 조치를 구현할 수 있습니다.

현대적인 네트워크와 조직에 구현된 보안 제어 조치의 동인은 무엇입니까?

보안 제어



12

aws re/start

보안 제어는 예방, 탐지, 교정의 세 가지 유형으로 정의됩니다. 각각 보안 수명 주기의 세 단계와 연결됩니다. 제어 유형마다 물리적, 기술적, 관리적 보안 조치를 구현함으로써 정보의 기밀성, 무결성, 가용성(CIA)을 보장할 수 있습니다.

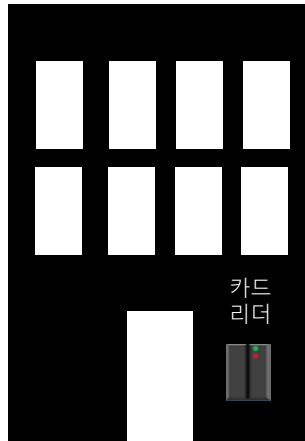
이어지는 강의에서 보안 수명 주기의 각 단계에서 구현할 수 있는 구체적인 보안 제어 조치에 관해 배울 것입니다.

보안 제어 조정

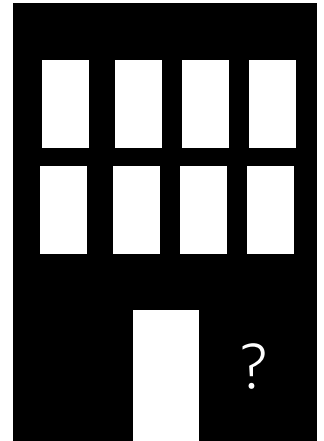
기본 데이터 센터에는 카드 리더 시스템이 있습니다. 대체 사이트에 방문하니 그 데이터 센터에는 같은 시스템이 없습니다.

대체 데이터 센터에 입장할 수 있는 사람을 제어하기 위해 어떻게 해야 합니까?

기본 데이터 센터



대체 데이터 센터



여러 자산을 보호해야 하는 경우 같은 유형의 보안 제어를 사용하지 않을 수 있지만 여전히 같은 보안 수준을 구현해야 합니다.

해킹이란?

위험 요인 및 대상:

- 물리적
- 기술적
- 소셜

해킹 및 크래킹



무단 액세스

침투 테스트

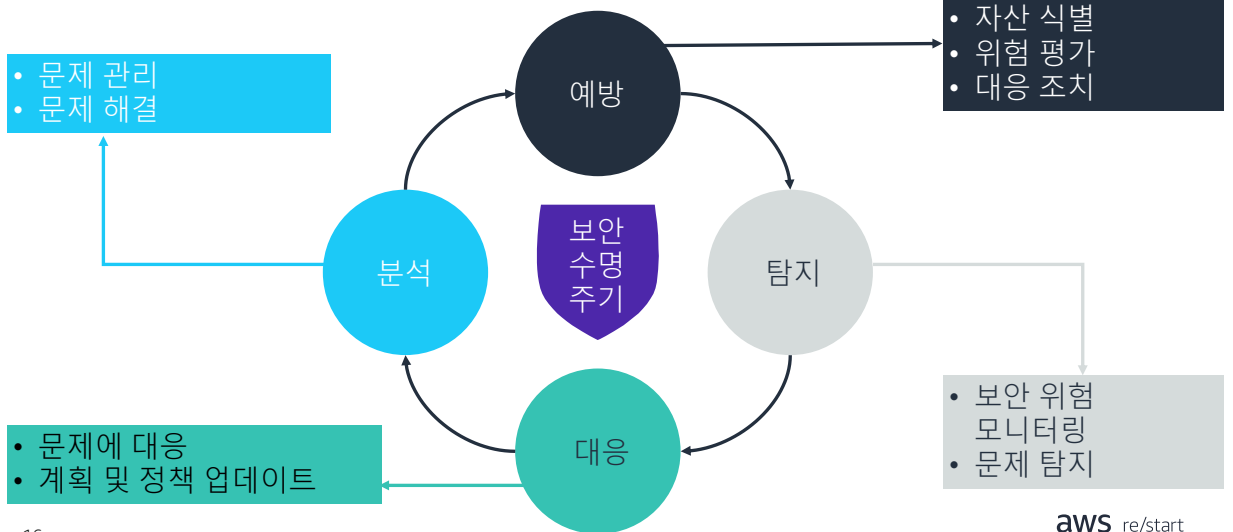


잠재적 침해 테스트



보안 수명 주기

보안 수명 주기



토론



17


실제 상황에서 보안 수명 주기는 어떤 모습입니까?

보안 수명 주기는 업계마다 어떻게 다른니까?

개별 보안 요구 사항에 대한 규칙은 누가 정합니까?

aws re/start

규정 준수 프레임워크는 여러분의 구체적인 보안 요구 사항과 관련한 수명 주기에 대한 구조를 제공합니다. 규정 준수 프레임워크는 다음 주제에서 다룹니다.



■ 규정 준수

규정 준수

- 보안 제어 조치는 규정으로 요구되는 경우가 많습니다.

규정

- 국가
- 업계

계약

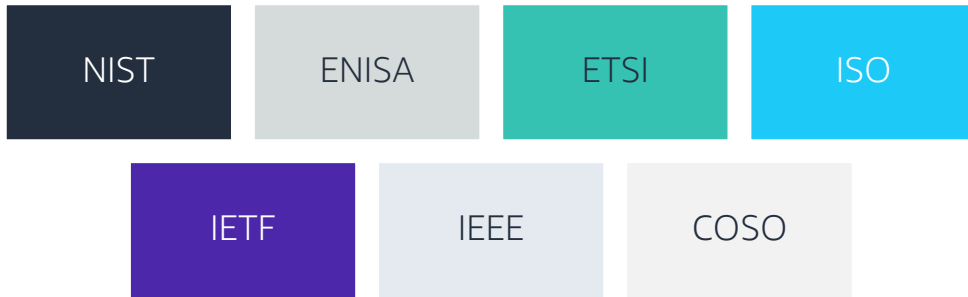
- SLA
- PLA

- 지역, 관할 구역, 문화 사이에서 갈등을 피해야 합니다.

- 서비스 수준에 관한 계약(SLA)
- 프로젝트 노동 계약(PLA)

사이버 보안 표준

- IT의 표준은 계속해서 변화합니다. 하나의 표준만을 모든 환경에 적용하거나 미래에 대비하는 데 활용할 수 없습니다.
- 표준 개발에 중점을 두는 조직:



- National Institute of Standards and Technology(NIST)
- European Union Agency for Cybersecurity(ENISA)
- European Telecommunications Standards Institute(ETSI)
- International Organization for Standardization(ISO)
- Internet Engineering Task Force(IETF)
- Institute of Electrical and Electronics Engineers(IEEE)
- Committee of Sponsoring Organizations(COSO)

규정 준수

- 외부 당국:
 - 정부 또는 법률. 규정 준수 필수
 - 공개 표준. 규정 준수 참여가 요구됨
 - 모범 실무. 선택적 규정 준수
- 규정 미준수 시 결과가 따름:
 - 정부 또는 법률. 민사, 형사상 또는 재정적 처벌
 - 공개 표준. 재정적 처벌 또는 참여가 거부됨
 - 모범 실무. 고객, 파트너 또는 수익 손실
- 규정 준수를 입증하기 위해 적절히 보고해야 합니다.

결제 카드 산업(PCI) 보안 표준

- PCI는 보안 환경을 유지 관리하기 위해 규제되는 요구 사항의 집합입니다.
 - 요구 사항은 데이터 보안의 다양한 측면에 초점을 둡니다.
- 결제 카드 데이터 처리에 관여하는 모든 엔터티가 PCI 보안 표준을 준수해야 합니다.
- PCI 보안 표준 위원회에서 보안 평가 절차도 제공합니다.

PCI에 관한 자세한 정보는 <https://www.pcisecuritystandards.org/>를 참조하십시오.

규정 준수 표준: 유럽 연합

가장 중심이 되는 **General Data Protection Regulation(GDPR)**은 **유럽 연합(EU)** 시민에게 데이터에 대한 더 향상된 통제권을 부여하기 위한 규정의 집합입니다.



General Data Protection Regulation(GDPR)은 **유럽 연합(EU)** 시민에게 데이터 개인 정보 보호와 보안에 대한 더 향상된 통제권을 부여하기 위한 규정의 집합입니다. GDPR은 EU 시민 보호와 규정 준수를 위한 책임 원칙에 관해 포괄적인 접근 방법을 제공합니다.

GDPR은 개인 정보 보호 및 보안 표준을 위반하는 주체에게 강력한 처벌을 가합니다. 일부 처벌은 수천만 유로에 달하는 벌금이 될 수도 있습니다.

GDPR 규정 준수를 더 정확히 이해하려면 아래에서 EU 시민의 데이터를 처리하기 위한 법적 근거 목록을 검토하시기 바랍니다.

- (a) 데이터 주체가 자신의 개인 데이터 처리에 동의를 제공한 경우
- (b) 데이터 주체와의 계약 의무를 이행하려는 경우 또는 계약을 체결하는 과정에 있는 데이터 주체의 요청에 따라 작업을 수행하려는 경우
- (c) 데이터 컨트롤러의 법적 의무를 준수하려는 경우
- (d) 데이터 주체 또는 다른 개인의 사활적 이익을 보호하려는 경우
- (e) 공익 또는 직무 권한으로 작업을 수행하려는 경우
- (f) 데이터 컨트롤러 또는 제3자의 법적 이익을 위한 경우. 단, 이 이익보다 데이터 주체의 이익 또는 데이터 주체의 Charter of Fundamental Rights에 따른 권리가 더 큰 경우는 제외(특히 데이터 주체가 아동인 경우)

미국: HIPAA

- 1996년 발효된 미국 Health Insurance Portability and Accountability Act(HIPAA)
 - 의료 정보 처리 방법을 현대화함
 - 개인 식별 정보를 보호하는 방법을 규정함
 - 의료 보험 적용 범위의 한계를 다룸
 - 법률을 명시하는 다섯 개의 표제로 구성됨
- 예: 의료 종사자는 환자의 가족에게 유선상으로 환자의 신원을 공개하지 않음

Health Insurance Portability and Accountability(HIPAA)는 환자의 허락 없이 환자의 의료 정보가 공개되지 않도록 보호하기 위한 미국 연방법입니다.

규정 준수 표준: 유럽 연합

가장 중심이 되는 **General Data Protection Regulation(GDPR)**은 **유럽 연합(EU)** 시민에게 데이터에 대한 더 향상된 통제권을 부여하기 위한 규정의 집합입니다.



General Data Protection Regulation(GDPR)은 **유럽 연합(EU)** 시민에게 데이터 개인 정보 보호와 보안에 대한 더 향상된 통제권을 부여하기 위한 규정의 집합입니다. GDPR은 EU 시민 보호와 규정 준수를 위한 책임 원칙에 관해 포괄적인 접근 방법을 제공합니다.

GDPR은 개인 정보 보호 및 보안 표준을 위반하는 주체에게 강력한 처벌을 가합니다. 일부 처벌은 수천만 유로에 달하는 벌금이 될 수도 있습니다.

GDPR 규정 준수를 더 정확히 이해하려면 아래에서 EU 시민의 데이터를 처리하기 위한 법적 근거 목록을 검토하시기 바랍니다.

- (a) 데이터 주체가 자신의 개인 데이터 처리에 동의를 제공한 경우
- (b) 데이터 주체와의 계약 의무를 이행하려는 경우 또는 계약을 체결하는 과정에 있는 데이터 주체의 요청에 따라 작업을 수행하려는 경우
- (c) 데이터 컨트롤러의 법적 의무를 준수하려는 경우
- (d) 데이터 주체 또는 다른 개인의 사활적 이익을 보호하려는 경우
- (e) 공익 또는 직무 권한으로 작업을 수행하려는 경우
- (f) 데이터 컨트롤러 또는 제3자의 법적 이익을 위한 경우. 단, 이 이익보다 데이터 주체의 이익 또는 데이터 주체의 Charter of Fundamental Rights에 따른 권리가 더 큰 경우는 제외(특히 데이터 주체가 아동인 경우)

규정 준수 표준: 러시아

개인 데이터에 관한 **러시아** 연방법:

- 개인의 동의가 필요함
- 개인 데이터 주체는 이전에 동의한 사항을 철회할 수 있음
- 개인 데이터를 러시아 연방 외부로 전송하려면 대상 국가의 적절한 보호 조치가 필요함

- 2006년 7월 27일 도입됨
- 개인의 데이터를 처리하려면 개인의 동의가 필요함
- 개인 데이터 주체는 언제든지 이전에 동의한 사항을 철회할 권한이 있음

일반적으로 개인 데이터를 러시아 연방 외부로 전송하려면 운영자는 개인 데이터 주체의 권리가 대상 국가에서 적절히 보호되도록 해야 합니다.

규정 준수 표준: 중국

중화인민공화국의 사이버 보안법:

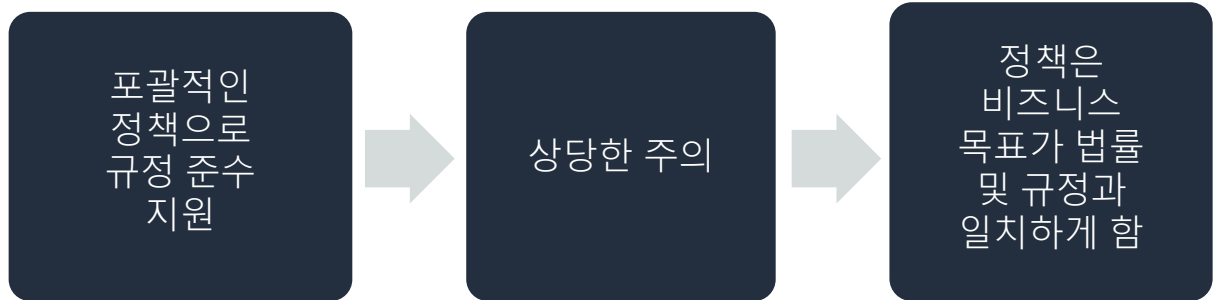
- 특정 데이터를 중국에 저장하도록 요구함
- 중국 당국이 기업의 네트워크 운영에 무작위 검사를 수행하도록 허용함

- 2017년 6월 1일 도입됨
- 네트워크 운영자가 중국 내에 특정 데이터를 저장하도록 요구하며 중국 당국이 기업의 네트워크 운영에 무작위 검사를 수행하도록 허용함
- 이 법의 특징:
 - 사이버 공간 주권의 원칙을 규정함
 - 인터넷 제품 및 서비스 공급자의 보안 의무를 정의함
 - 개인 정보 보호 규정을 더 완전하게 정의함
 - 주요 정보 인프라에 대한 보안 시스템을 확립함
 - 핵심 정보 인프라에서 데이터의 트랜잭션 전송에 대한 규칙을 도입함

기타 표준

법률 및 규정	미국	캐나다	유럽 연합
Sarbanes-Oxley Act(SOX)	X		
Gramm-Leach-Bliley Act(GLBA)	X		
Federal Information Security Management Act(FISMA)	X		
General Data Protection Regulation(GDPR)			X
Personal Information Protection and Electronic Documents Act(PIPEDA)		X	
Financial Industry Regulatory Authority(FINRA)	X		
Family Educational Rights and Privacy Act(FERPA)	X		
Dodd-Frank Wall Street Reform and Consumer Protection Act - 미국	X		

규정 준수 및 기업 정책



핵심 사항



© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

30

- 정보 보안을 다룰 때는 기밀성, 무결성, 가용성의 관점에서 생각합니다.
- 보안 문제의 일반적인 유형에는 맬웨어, 피싱, 소셜 엔지니어링 등이 있습니다.
- 훌륭한 보안 전략은 예방, 탐지, 대응, 분석이라는 보안 수명 주기의 단계를 구현하는 전략입니다.
- 훌륭한 보안 관행을 시행하기 위한 프레임워크를 제공하기 위해 다양한 업계 보안 규정 준수 표준이 존재합니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- 정보 보안을 다룰 때 고려해야 할 관점은 기밀성, 무결성, 가용성입니다.
- 보안 문제의 일반적인 유형에는 맬웨어, 피싱, 소셜 엔지니어링 등이 있습니다.
- 훌륭한 보안 전략은 예방, 탐지, 대응, 분석이라는 보안 수명 주기의 단계를 구현하는 전략입니다.
- 훌륭한 보안 관행을 시행하기 위한 프레임워크를 제공하기 위해 다양한 업계 보안 규정 준수 표준이 존재합니다.