Tel. +39 02 365738
info@overneteducation.it
www.overneteducation.it

OEC111

Sicurezza e privacy nell'era del Cloud Computing

Durata: 3 gg

Descrizione

L’ente di certificazione internazionale ISO ha pubblicato uno standard specificamente elaborato per i fornitori di servizi di cloud computing. Si tratta dell’ISO 27018, il primo ed unico al mondo nel suo genere, un set di regole costruito sugli standards ISO 27001 e 27002 per garantire il rispetto dei principi e delle norme privacy dettate dalla Direttiva 95/46/CE, da parte dei providers di public cloud che se ne dotano.

L’ambizione dichiarata di questo standard è quella di rappresentare una risposta pratica – di privacy by design – alle principali questioni giuridiche, sia di natura legale che contrattuale, legate alla gestione dei dati personali in infrastrutture informatiche distribuite seguendo il modello del cloud pubblico.

Descrizione Corso

Il Cloud Computing consente alle aziende di esternalizzare le risorse IT e di trasferirle su data center distribuiti sulla rete. Questo consente di ottimizzare l’utilizzo delle risorse e di risparmiare sui costi dell’IT ma pone nuove problematiche relative alla sicurezza dei sistemi, dei dati, e sulla protezione di dati sensibili (privacy). Le normative vigenti, inoltre, non sono completamente pronte a supportare queste nuove tecnologie. Ma quali sono i rischi reali di sicurezza e privacy nell’adozione del paradigma Cloud? Quali sono gli strumenti di protezione?

Questo corso, di carattere introduttivo, descrive le principali problematiche di sicurezza e privacy dei servizi Cloud, alcune best practices e una panoramica sugli strumenti per la loro gestione.

A chi è rivolto?

Capi progetto, Analisti, Progettisti, Sviluppatori, Chiunque sia interessato ad approfondire i concetti relativi al Cloud Computing.

Prerequisiti

Non sono previsti pre-requisiti

Contenuti

Introduzione

- •Cos'è il Cloud Computing
- •I principali servizi del Cloud e la definizione del NIST (IaaS, PaaS, SaaS)
- •Architettura di riferimento del Cloud Computing
- •Virtualizzazione e multi-tenancy
- •Le normative europea e italiana sul Cloud Computing
- •Definizione di “rischio” e assement sulla sicurezza per la migrazione al Cloud
- •Requisiti di sicurezza del Cloud Computing

Infrastructure-as-a-Services (IaaS) Security

- •Architettura generica di un IaaS, i “rischi” di sicurezza di un IaaS
- •Protezione dell’infrastruttura fisica (reti, server…)
- •Protezione dell’infrastruttura virtuale

•Sicurezza delle virtual machine
•Tecnologie e strumenti per la sicurezza di un IaaS

Platform-as-a-Services (PaaS) Security
•Architettura generica di un PaaS
•I “rischi” di sicurezza di un PaaS
•Protezione della piattaforma
•Tecnologie e strumenti per la sicurezza di un Paas

Software-as-a-Services (SaaS) Security
•Architettura e tipologie di SaaS
•I principali rischi di sicurezza di SaaS: il modello OWASP
•Tecnologie e strumenti per la sicurezza di un SaaS

Strumenti per la verifica della sicurezza di un Cloud
•Security Assesment
•Strumenti per il testing della sicurezza di un Cloud

Governance della security
•Il processo di governance del Cloud
•Security as a Services
•Auditing degli accessi
•Policy
•Account management & provisioning, Disaster Recovery & Business Continuity Planning
•Intrusion detection & Incident Response

Concetti generali sulla norma ISO/IEC 27001 e 27002
•Analisi della norma ISO/IEC 27001 (Information Security Management System).
•Analisi della norma ISO/IEC 27002 (Code of practice for information security controls)
•Valutazione delle minacce e delle vulnerabilità più comuni dei sistemi informativi e del conseguente innalzamento dei livelli di rischio.

Problematiche di privacy del Cloud Computing
•Dove vengono memorizzati i dati delle aziende?
•Principali rischi relativi alla sicurezza dei dati, protezione dei dati sensibili, tecnologie e strumenti per la protezione dei dati nel Cloud (memorizzazione e trasferimento)
•Protezione dei dati sensibili.
•Analisi della norma ISO/IEC 27018:2014 (Code of practice for protection of personally identifiable information (PII) in public clouds).

Information Security Risk Management:
•Analisi della norma ISO/IEC 27005 (Information security risk management).
•Definizione di Rischio informatico.
•Relazione fra Rischio, Asset e Processi.
•Le metriche del Rischio.
•Valutazione dei rischi: approccio quantitativo, qualitativo ed ibrido.
•Fasi di gestione del Rischio.

Certificazioni