SocialCities s.r.l.
Via Selice 191/B - 40026 - Imola (BO)
P.iva 03368221200 - C.F. 03368221200
www.socialcities.it - info@socialcities.it

INFORMATIVA SUGLI STANDARD DI SICUREZZA INFORMATICA

SocialCities, nelle sue attività di fornitura servizi hosting e server managed/unmanaged, rispetta e segue le seguenti policy di sicurezza generale.

VIRTUAL SERVER SECURITY & EMPLOYEE ACCESS

La sicurezza dei virtual server e la data integrity sono fra le priorità di SocialCities. Per garantire la massima sicurezza, nessuna persona all'interno della nostra organizzazione ha accesso in alcun modo al sistema di hypervisor dei virtual server ed ai sistemi NAS/SAN dedicati allo storage dei dati dove risiedono gli snapshot ed i backup.

Tali sistemi garantiscono il funzionamento della infrastruttura informatica e solamente personale tecnico altamente specializzato ha accesso a tale infrastruttura.

PHYSICAL SECURITY

Tutta l'infrastruttura SocialCities risiede in co-locazione presso datacenter enterprise-grade / premiere-infrastructure. Le facilities di nostro utilizzo includono:

- Equinix / Telecity (http://www.equinix.com/services/data-centers-colocation/)
- Telx / DigitalReality (https://www.digitalrealty.com/data-center-solutions/colocation/)
- OVH Montreal / Paris / Strasbourg / Roubaix / Gravelines
- Executive Services / 00 Gate
- 18 regioni afferenti a Google Cloud Platform (https://cloud.google.com/about/locations/)

In ognuna di queste strutture è attivo uno staff 24/7/365 con sistemi di sicurezza onsite per la protezione di accessi non autorizzati nei locali server. I sistemi di sicurezza onsite includono camere di monitoraggio delle facilities premises e di tutte le aree interne del datacenter. Gli accessi avvengono tramite autorizzazione biometrica e autenticazione a due fattori.

I server sono unmarked e la loro posizione specifica è riservata.

CREDIT CARD SECURITY

Tutti i processi che coinvolgono transazioni finanziarie avvengono attraverso l'utilizzo del gateway Stripe. Il gateway garantisce transazioni online per migliaia di attività aziendali e piattaforme SaaS. Viene garantita piena aderenza agli standard PCI per lo storage e l'handling delle informazioni di transazione.

COMMUNICATIONS

Tutte le comunicazioni interne ed esterne ai datacenter da noi in utilizzo avvengono attraverso SSL (HTTPS) sia per i servizi pubblici web che per le interfacce API. L'accesso ai server avviene attraverso tecnologia SSH con chiavi a crittografia asimmetrica.

SocialCities s.r.l.
Via Selice 191/B - 40026 - Imola (BO)
P.iva 03368221200 - C.F. 03368221200
www.socialcities.it - info@socialcities.it

SNAPSHOT AND BACKUP SECURITY

Gli snapshot ed i backup (images) sono salvati in uno spazio interno non pubblicamente accessibile. I server NAS/SAN devono sottostare a specifiche policy di accesso e sono isolati dalla rete Internet. Gli snapshot sono inoltre inviati a più regioni geografiche in modo da aumentare la ridondanza geografica dei file.

SOFTWARE SECURITY

Tutti i nostri software godono di vari sistemi di sicurezza, quali:

- esclusione virus e malware tramite certificazione a chiave asimmetrica del software
- sistemi anti brute-force
- filtraggio degli IP e banning istantaneo
- crittografia dei dati sensibili attraverso algoritmi avanzati di hashing
- Cross site request forgery (CSRF) protection
- SQL injection protection
- Clickjacking protection
- Host header validation
- Session security

VARIE

I datacenter sono inoltre dotati delle seguenti tecnologie di sicurezza:

- sorveglianza video ed umana 24/7/365
- sistema rilevamento particelle di fumo
- ridondanza nei sistemi elettrici
- alternatori da 250 KVA
- gruppi elettrogeni con autonomia 48h
- collegamento di rete ridondato
- sale rete gemelle
- certificazione ISO 27001:2005, certificazione ISO 27002, certificazione ISO 27005
- certificazione SOC 1 - SOC 2 tipo II
- sale server a bassa climatizzazione con watercooling e aircooling
- PUE compreso fra 1 e 1.2
- rilevatori di movimento perimetrali ed indoor
- porte blindate
- sistema antincendio e porte antifuoco APSAD R4 conformità N4
- banda passante di 3Tbps in Europa, 8000 Gpbs in America del nord con connessione a 33 punti di peering in 3 continenti
- server con doppia alimentazione e doppia scheda di rete
- datacenter disgiunti geograficamente
- protezione anti-DDoS da 160Gbps con filtraggio fino a 480Gpbs
- nel più piccolo dei datacenter in utilizzo N° 73 controlli anti-intrusione, n° 19 sensori volumetrici, n° 24 telecamere di cui 16 a 24h, n° 29 rilevatori di presenza, n° 31 rilevatori di temperatura, n° 8 barriere infrarossi; Centralina esterna meteo in domotica, vari sensore antifumo – Impianto antincendio – 2 sensori anti allagamento interni, 2 allarmi con sirena per superamento livello di sicurezza (- 7 mt dal suolo del DataCenter) acque piovane; 4 sensori controllo umidità e CO2 interna

SocialCities s.r.l.
Via Selice 191/B - 40026 - Imola (BO)
P.iva 03368221200 - C.F. 03368221200
www.socialcities.it - info@socialcities.it

CASI CONCRETI

- gestione server AWS con tecnologia anti intrusione, anti manomissione, data retention a 2 anni, modalità dinamica di isolamento in caso di attacco in corso
- per infrastruttura server enterprise class, superato il penetration test X-Force Red di IBM
- memorizzazione big data ed analisi in tempo reale di informazioni riservate di consumo
- HORECA: gestione di VPS per un totale di +500 alberghi
- LocalJob: 0.000% di downtime dal 2013 ad oggi, ad esclusione degli interventi di manutenzione programmata
- 20+ server attualmente up and running con downtime dello 0,0000% negli ultimi 365 giorni, ad esclusione degli interventi di manutenzione programmata
- reazione immediata ad un attacco informatico subito nel 2016 ai danni di LocalJob; l'infrastruttura attaccante fu bannata automaticamente in <0,5 secondi dall'inizio dell'attacco
- SocialCities si affida inoltre, in casi di emergenza, ad un professionista della sicurezza informatica disponibile 7/24/365

PRIVACY DEL DATO

Allo scopo di preservare e difendere la segretezza delle informazioni contenute nei nostri server, tutte le comunicazioni avvengono all'interno di un ambiente protetto e crittografato SSL.

Le password vengono trattate esclusivamente tramite una criptazione one-way che ne impedisce il furto e i dati di pagamento vengono memorizzati in strutture apposite garantite PCI.

I backup vengono criptati prima di essere trasferiti all'ambiente di destinazione e vengono eseguiti esclusivamente nelle ore notturne e nei weekend. All'interno degli orari lavorativi lun-ven, 9-18 è quindi possibile depositare e rimuovere un dato senza che questo venga processato nei backup.

Ogni notte viene eseguito uno snapshot completo di tutto il datacenter che viene mantenuto per i successivi 7 giorni. All'ottavo giorno l'informazione viene distrutta e perduta.

Ogni weekend viene eseguito un backup incrementale che verrà memorizzato fino ai successivi 6 mesi. Al settimo mese l'informazione viene distrutta e perduta.

In nessun caso viene fornito accesso ai dati del server o dei backup ad aziende esterne. Tutti i dati sono depositati normalmente in territorio extra italiano e non sono pertanto soggetti a sequestro.

Su richiesta il dato può essere isolato in territorio extra europeo. Analogamente e sempre su richiesta, il dato può esser riservato su un particolare territorio europeo o anche esser mantenuto unicamente sul suolo italiano.