S-D CONSULTING
WEB SOLUTIONS

GDPR Compliance

La protezione dei dati con **S-D CONSULTING**

PREMESSA:
La nuova normativa UE che riguarda la protezione dei dati contiene parecchie novità per quanto riguarda sicurezza e responsabilità.

Con questo documento S-D Consulting vi dice cosa ha messo in atto per la GDPR compliance.
In alcuni casi il dato potrebbe essere utile al cliente che può integrarlo nella sua documentazione, dove avrà inserito i propri fornitori di servizi suddivisi per tassonomia, se soggetto interessato al nuovo Regolamento.

GDPR non è solo un impegno o un costo, ma vuole essere, come abbiamo già riportato sul nostro documento inerente l'informativa privacy, un nuovo modo di lavorare per portare trasparenza, integrità e garanzia di riservatezza dei dati personali.

Cosa è importante fare per le aziende:

- Check list: preparare una lista dove includere informazioni su come sono organizzati tutti i dati, come vengono censiti e i relativi processi di trattamento
- Rischi: spiegare come sono le infrastrutture, ad esempio gli storage, i backup scelti per l'archiviazione e la rindondanza e affidabilità degli apparati che contengono i dati

Il nuovo Regolamento europeo non si limità a richiedere quali siano le "misure minime" adottate per la conservazione dei dati, ma piuttosto le "**misure idonee**".

Vogliamo ovviamente ricordare che, ad eccezione dei dati dei nostri clienti diretti, trattati per mere questioni contabili o di inserimento del dato per le registrazioni dei servizi presso i partner - e di cui siamo titolari del trattamento dei dati - noi siamo la figura che nel nuovo Regolamento viene identificato come "**data processor**", mentre il cliente è definito "**data controller**".

Vogliamo anche informare i nostri clienti che S-D Consulting appoggia la propria infrastruttura "cloud server" a data center aderente al CISPE (Cloud Infrastructure Services Providers in Europe).

L'art. 24 del GDPR esprime un principio di "Accountability", ovvero chiede di dimostrare di aver adempiuto alle richieste normative, in quanto la forma non basta più: ogni operazione deve essere registrata e mantenuta per eventuali controlli, di qualunque natura essa sia e indicata nella informativa privacy adottata.

Quindi, per arrivare al punto cruciale:

- I servizi di S-D Consulting sono appoggiati su infrastruttura riconosciuta dal CISPE
- S-D Consulting si impegna a gestire i dati personali ai fini dell'esecuzione dei servizi e non per altri scopi
- I dati sono gestiti nel contesto del territorio italiano per quanto riguarda l'infrastruttura dei dati, e comunque all'interno del territorio europeo
- Vengono adottati i migliori standard di sicurezza
- I dati vengono protetti con sistemi di backup affidabili e ridondati (che saranno spiegati nelle pagine a seguire)

Per capire come S-D Consulting si pone rispetto ai dati secondo il Regolamento GDPR, deve essere fatto un ragionamento molto semplice:

- Se l'azienda è un provider di servizi e pone la sua infrastruttura su S-D Consulting
- Se l'azienda eroga servizi ad aziende terze e appoggia i suoi servizi su di noi

A questo punto noi siamo il "data processor".

Ma a sua volta, l'azienda che si identifica nei punti precedenti, è anch'essa "data processor" nei confronti dei propri clienti finali.

Se invece l'azienda è un cliente finale (quindi non una web agency o un rivenditore / integratore), S-D Consulting resta il "data processor", il cliente il "data controller".

Per riepilogare le righe e i concetti sopra esposti e quello che troverete in questo documento:

- La differenza tra "data controller" e "data processor" è sostanzialmente chi tratta i dati, e chi li processa: potenzialmente noi possiamo anche non sapere quale tipo di dato il cliente tratta nel contesto dei servizi che noi abbiamo fornito
- Risk analysis, che spiega la grande differenza tra quelle che prima erano identificate come "misure minime", mentre oggi sono le "misure idonee" adottate per la protezione dei dati
- Quali sono i miei fornitori, suddivisi per tassonomia e se operano nel contesto dell'Unione Europea oppure no
- Tra le novità, obbligo di disclosure e notifica dei data breaches (furto dei dati)
- Dimostrare quello che si dichiara, non basta più un documento statico come si faceva in passato
- Avviare l'"era dell'Accountability", ovvero dimostrare periodicamente quello che si dichiara
- Politiche di sicurezza fisica adottata (anche sulla infrastruttura tecnica interna agli uffici, uso di PC fissi e portatili, sistemi di allarme e di sicurezza, crittografia e molto altro)
- Redazione di informative chiare
- Predisposizione di procedure di data breach e disclosure
- Evidenziare sicurezza logica, infrastrutturale, dei servizi, organizzativa e risorse umane
- Far comprendere, attraverso la percezione e la consapevolezza, quale sia l'attenzione al problema, attraverso l'evidenziazione dei ruoli, procedure, audit, piani di workaround, way-out e recovery
- Adozioni anche di sistemi di difesa attraverso "patch"

S-D CONSULTING
WEB SOLUTIONS

Sommario

La protezione dei dati con S-D CONSULTING *1*

Sicurezza dei dati: facciamo chiarezza *4*

Sicurezza logica e le indicazioni pratiche *4*

Cancellazione dei dati su un cloud server fornito da S-D Consulting 4

Sicurezza fisica *5*

Oltre ai datacenter, come si pone S-D Consulting sui locali operativi e commerciali 5

QSA Quick Security Assessment *6*

DOCUMENTO TECNICO *7*

Descrizione e caratteristiche dei datacenter 7

Caratteristiche dei Cloud Server adottati 7

Cloud server: i sistemi di sicurezza a più livelli adottati 9

SISTEMI ANTIMALWARE 9

SISTEMI DI MONITORAGGIO ADDIZIONALI E ANTIVIRUS 10

Ulteriori livelli di sicurezza lato software 11

Disaster Recovery e Business Continuity *11*

Il sistema di Cloud Backup 12

Cloud Backup: un test di dimostrazione e di procedura di recupero: 13

Modifiche al documento *13*

Revisione	Data	Descrizione
1	25/05/2018	Prima emissione condivisa

Sicurezza dei dati: facciamo chiarezza

La sicurezza dei dati è argomento di dibattito da sempre, in particolare da quando il Cloud Computing ha iniziato a diffondersi come tecnologia delle aziende.
Si parla di tecnologia cloud, sia private sia public, ma nell'immaginario collettivo si fa spazio il concetto di "perdita di controllo del dato".

La percezione è quella, in quanto il dato è nel cloud e non nel dispositivo fisico e visibile, ma l'attenzione all'infrastruttura cloud spesso è molto più ampia rispetto a quello che può essere la sicurezza locale, sia un device sia di un server magari posizionato in un sottoscala.

La sicurezza è un ambito molto delicato e che non riguarda un unico soggetto.
Nel contratto cloud, sono due le parti che si occupano di contribuire e tutelare i dati: il Provider e il Cliente:

- Provider: misure e strategie di sicurezza messe in atto con i servizi cloud offerti, le infrastrutture tecnologiche (data center utilizzati), programmi di monitoraggio e sorveglianza, sistemi di backup proposti
- Cliente: misure e strategie di sicurezza adottate nelle procedure quotidiane di gestione e diffusione dati all'interno della propria azienda e dal punto di vista applicativo (riguardo questo punto, rimandiamo al prossimo paragrafo per spiegare quanto la "sicurezza" diventi importante da parte del Cliente, indipendentemente da tutta la sicurezza che il Provider può offrire

Sicurezza logica e le indicazioni pratiche

S-D Consulting, in qualità di fornitore, non ha la possibilità di poter conoscere quale tipo di dato sta ospitando per conto del cliente e delle sue infrastrutture: infatti è il Cliente l'unico responsabile dei dati inseriti nel cloud offerto e ne determina la diffusione.

Da parte nostra quindi, nessun intervento avviene sui contenuti del cliente e non possiamo conoscere i dati che il cliente immette all'interno dei propri servizi acquistati.

Per questo il Cliente si deve preoccupare di comprendere quale sia la persona a cui affidare il controllo dei dati e quindi autorizzarlo all'interno della propria infrastruttura, al monitoraggio, l'uso e la distribuzione dei dati attraverso la piattaforma cloud.

Per quanto riguarda la possibile autorizzazione fornita a terzi per accedere ai dati del nostro cliente, può avvenire solo nel caso in cui ci sia una espressa e formale richiesta da parte di organi come la Polizia giudiziaria, con lo scopo di indagine informatica e accertamenti.
Per tale avvenimento è necessario un decreto firmato da un giudice, per quanto riguarda la normativa italiana.

Cancellazione dei dati su un cloud server fornito da S-D Consulting

La conservazione e la tutela dei dati conservati nei servizi cloud server forniti da S-D Consulting sulla propria infrastruttura sono strettamente legati alla scelta di una soluzione di backup.

Di default, tutti i servizi offerti su nostre VM (Virtual Machine) utilizzano un sistema di backup giornaliero incrementale, con una Policy di Retention di mantenimento dei file per 4 versioni.
Questo significa, per un cliente che mantiene i propri dati presso di noi, la possibilità di recuperare dati anche "lontani", tutto dipende da quante volte sono stati variati i file.

Per altre soluzioni, è il cliente che deve richiedere una infrastruttura di backup personalizzata.

Andando nello specifico, le nostre piattaforme cloud utilizzano un sistema TSM (Tivoli Storage Manager) basato su IBM.

La copia incrementale dei dati permette quindi più versioni dello stesso file.
Fin quando file/directory non verranno eliminati dal proprio disco, rimarrà una copia per sempre registrata sul sistema di backup.
Il dato viene definitivamente cancellato dopo 60 giorni, solo nel caso in cui l'origine viene cancellata.

Sicurezza fisica

Nonotante la diffusione di dubbi sulla sicurezza del cloud, un Cloud Provider che si dota di infrastrutture mirate a garantire la massima sicurezza fisica ed i migliori programmi di sorveglianza e monitoraggio potrà garantire al cliente una tranquillità ancora maggiore.

I data center su cui S-D Consulting si appoggia si trovano in Italia, sui due nodi principali italiani di Milano e Frosinone.
E' discrezione di S-D Consulting il posizionamento del cliente su l'uno o l'altro data center, salvo richiesta specifica durante l'ordine.

E' chiaro che i sistemi di backup saranno, per effetto della ridondanza del dato, sempre sul data center opposto, quindi se un cloud server che ospita il dato si trova a Frosinone, il sistema TSM di Backup si troverà a Milano.

L'accesso ai data center sono ovviamente protetti anche dal punto di vista fisico, quindi con accesso riservato esclusivamente al personale del datacenter, con un sistema di riconoscimento a doppio fattore (badge e impronta digitale).

L'accesso al data center è ulteriormente subordinato a autorizzazione a mezzo SmartCard e Impronta Digitale in possesso solo di personale autorizzato alle attività di data center.

Tutti gli accessi sono sottoposti a logging su sistema informatico, eventuali terzi accedono unicamente accompagnati da personale interno e vengono registrati previo accertamento dell'identità e verifica della motivazione/autorizzazione all'accesso.

I locali vengono sorvegliati 365/7/24 da personale interno o esterno autorizzato con sistemi di monitoraggio remoto.
Viene anche utilizzato un sistema di videosorveglianza perimetrale esterno e interno con telecamere che utilizzano registrazioni e ritenzione a norma di legge che permette anche il rilevamento di movimenti in aree critiche con conseguente attivazione di un circuito di allarme.

Durante le ore di minore frequentazione, la sicurezza è garantita da sorveglianza armata.
Esiste anche un sistema di rilevamento intrusioni per tutti i locali con segnalazione di tipo ottico/acustico locale e remoto a mezzo radio allarme verso l'istituto di vigilanza preposto.

Le certificazioni adottate quindi dal data center su cui si appoggia S-D Consulting sono quindi le ISO/IEC 27001.
Le norme inerenti quest'ultima hanno l'obiettivo di proteggere le risorse informative da eventuali minacce e assicurare una corretta gestioen dei dati sensibili.

Oltre ai datacenter, come si pone S-D Consulting sui locali operativi e commerciali

S-D Consulting presenta due sedi:

- La sede legale di Via Cefalonia 55 a Brescia, che è la sede dove viene gestita tutta la contabilità dei servizi offerti ai clienti;
  in questa sede è quindi presente la sola contabilità aziendale e nessun altro dato operativo che riguardi i dati espressamente gestiti e processati sulle nostre infrastrutture informatiche
- La sede operativa di Via Cipro 136 a Brescia, dove viene svolta tutta l'attività commerciale e tecnica, dove vengono svolti i processi informatici, custoditi gli accessi e quindi tutti i collegamenti remoti ai due data center di Milano e Frosinone

I locali indicati presso la sede operativa sono protetti con un sistema di monitoraggio indicato in:

- Sistema perimetrale
- Sistema di movimento interno
- Sistema di avviso tramite chiamata a combinatore telefonico

Tutti i dati informatici sono custoditi all'interno di apparecchiature dotate di sistema di login con accesso e su dischi soggetti a crittografia, siano essi gestiti su sistemi Apple Mac o Windows, di ultima generazione.

Anche i supporti informatici portatili sono comunque garantiti da sistemi di login e crittografia del disco, quindi con un alto livello di protezione dei dati in essi contenuti.

I locali sono anche protetti da intrusione fisica con finestre con sistemi di chiusura antisfondamento e saracinesca automatica, sempre collegati, in caso di movimento, ad un sistema di allarme centralizzato che si occupa della chiusura istantanea di tutti i locali da un unico punto di accesso.

Nessun documento informativo contenente dati personali cartaceo viene custodito all'interno dei locali, il cui accesso è consentito al personale dipendente e a clienti ma previo registrazione e accompagnamento da parte del personale autorizzato.

QSA Quick Security Assessment

S-D Consulting, anche grazie all'esperienza acquisita nel corso dei tanti anni di operatività, ha dato particolare importanza alle procedure (seguire il capitolo specifico).

Per questo ha eseguito dei test rapidi ed efficaci sulla propria infrastruttura, su più livelli, per comprendere eventuali punti di debolezza e soprattutto per suggerire soluzioni anche a quei clienti che non hanno ben compreso quale sia l'importanza e la protezione dei propri dati, anche attraverso aggiornamenti e applicazione di patch di sicurezza ai propri software.

I nostri sistemi proseguono costantemente nell'analisi dell'infrastruttura, tenendo monitorati i siti web, le applicazioni degli utenti, anche per individuare i rischi e eventuali aspetti da perfezionare.

Vengono quindi stabilite priorità alle attività per mitigare i rischi identificati.
Gli attacchi informatici alle piattaforme web e agli applicativi possono essere identificati, e permettono di comprendere eventuali vulnerabilità del sistema IT del cliente.

Il concetto di sicurezza deve essere compreso dai Clienti, soprattutto quando utilizzano piattaforme web che richiedono costanti aggiornamenti proprio per evitare quelle vulnerabilità note a tutto il mondo del web, siano esse piattaforme open source o altro.

Le nostre attività di monitoraggio ci fanno comprendere quando il cliente presta attenzione all'aspetto relativo alla sicurezza, e laddove apprendiamo bassi livelli di attenzione, è nostra cura segnalarlo al Cliente invitandolo a intervenire, con o senza il nostro aiuto.

Per noi comunque la sicurezza si estende anche a mantenere tutte le performance delle nostre attrezzature, per questo motivo il monitoraggio dei nostri sistemi cloud ci permette di comprendere il livello di rischio e dove intervenire in forma preventiva, anche per evitare danni peggiori.

Prevediamo anche contratti a monteore dove la sicurezza la curiamo noi, sempre con il benestare del Cliente che deve essere conscio che sta proteggendo un investimento e anche la propria immagine sul web.

DOCUMENTO TECNICO

Descrizione e caratteristiche dei datacenter

Le caratteristiche dei due data center su cui ci appoggiamo:

Sede	Caratteristiche
Milano	• Tecnologia convenzionale (raffredamento perimetrale) • Classificazione TIER II • Sistema di rilevazione dei fumi e del fuoco • Estinzione incendi e saturazione argon • Gruppi elettrogeni di emergenza N+1
Frosinone	• Tecnologia convenzionale (raffredamento perimetrale) • Classificazione TIER II+ • Sistema di rilevazione dei fumi e del fuoco • Estinzione incendi a CO2 e polvere • Gruppi elettrogeni di emergenza e N1 (dipende dai locali)
Tutti i datacenter sono attrezzati di controlli di accesso, rilevamento intrusioni, videosorveglianza, conformi alle certificazioni CEI (per i dettagli potete scrivere via mail per le caratteristiche precise di ogni certificazione che potremo richiedere direttamente al data center).	

Caratteristiche dei Cloud Server adottati

I cloud server adottati da S-D Consulting, per quanto concerne la fornitura diretta dei servizi, sono dei server virtuali con ottime prestazioni e scalabili, con parametri garantiti che riguardano:

•Memoria RAM

•CPU servita

•Rete

Sono creati all'interno di macchine multiprocessore multicore ridondate N+1 e co storage SAN ad alta disponibilità.

Le caratteristiche minime adottate:

•Memorie da 4 a 12 Gigabyte RAM assegnato

•CPU da 2 a 8 unità

- Banda garantita da 1 Gbps
- Sistema Cloud Backup basato su TSM (Tivoli Storage Manager) IBM

Sono tutti sistemi Linux e dotati di:

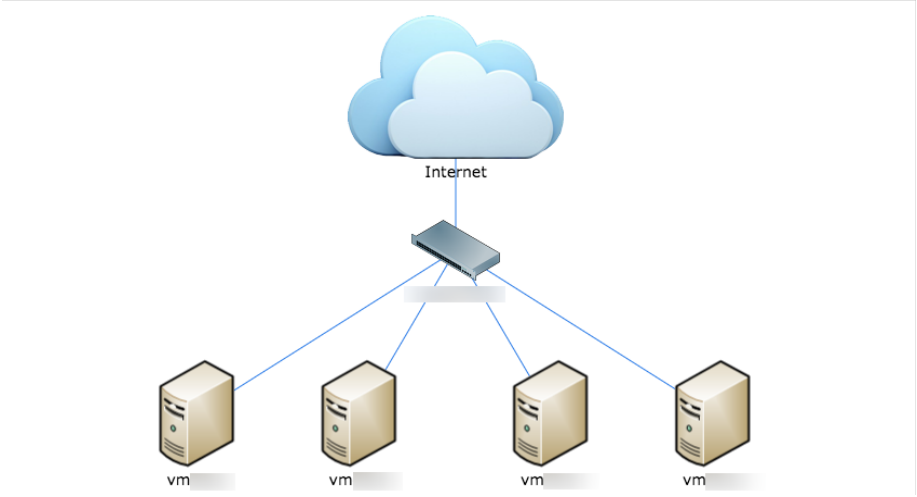
- Controllo completo via web (accensione, spegnimento, monitoraggio)
- Rete dedicata

- Ambiente virtualizzato dedicato senza overbooking
- Storage ad alte prestazioni
- Uptime garantito al 99,90% con penale, pari al 100% dei costi sostenuti
  (rapporto contrattualizzato tra S-D Consulting e data center, non tra S-D Consulting e Cliente finale, eventualmente da perfezionare a parte)

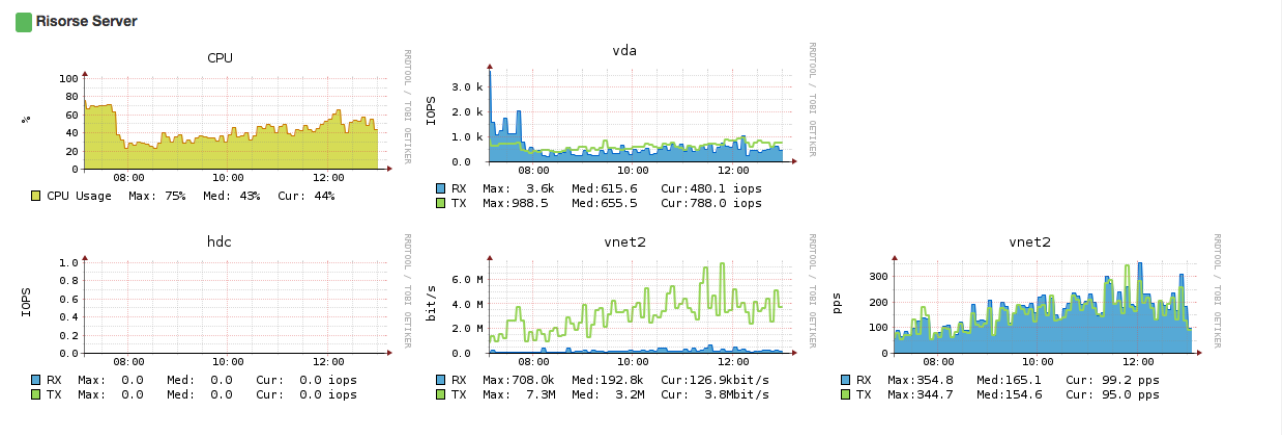
Al fine di garantire un alto livello di affidabilità, un sistema di Help Desk tra S-D Consulting e il data center è stato adottato per interventi rapidi 365/7/24.

Tutti i sistemi sono protetti con appositi sistemi Firewall (Advanced Adaptive Firewall) e sistemi di backup.

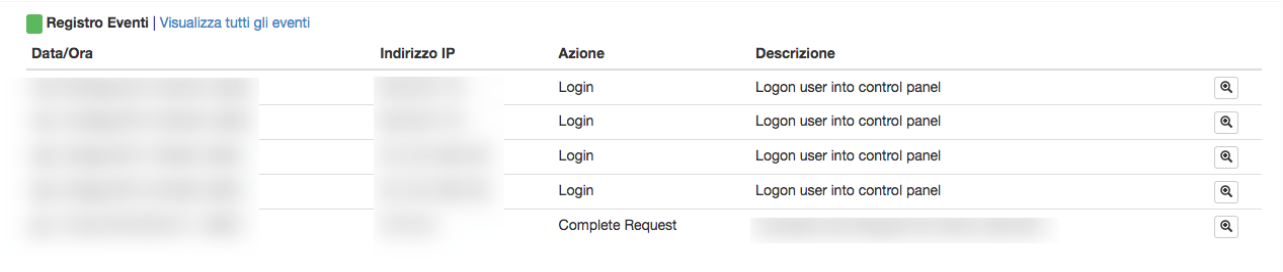
Qui di seguito un esempio delle infrastrutture gestite:



Un esempio di gestione statistico/grafica del monitoraggio delle risorse di ogni server:



Un esempio di gestione di registro degli eventi a disposizione in caso di verifiche:



Cloud server: i sistemi di sicurezza a più livelli adottati

Quanto evidenziato sopra mostra già i diversi livelli di sicurezza adottati che partono da:

- L'adozione di un firewall che garantisce già un ampio livello di filtraggio degli attacchi provenienti dalla rete
- L'adozione di un sistema di monitoraggio delle risorse
- L'adozione di un registro eventi che ci consente di comprendere molte delle informazioni che riguardano ogni cloud server gestito direttamente da noi

Ma la sicurezza non si ferma qui.

Abbiamo più volte sottolineato l'importanza della sicurezza a livello infrastrutturale, ampiamente documentato sopra, ma quella a livello di utilizzo di piattaforme web note non è da meno, anzi.

L'adozione di C.M.S. (Content Management System) da parte di web agency e di clienti finali ormai negli ultimi anni ha preso il sopravvento.
I C.M.S. sono prodotti sicuri, ma per mantenersi tali hanno bisogno di costanti aggiornamenti in quanto spesso soggetti ad attacchi informatici.

Chi commette attività illecite in questo senso, sfrutta le vulnerabilità di queste piattaforme, spesso per fare attacchi verso terzi e per grossi volumi di spam.

Per fare questo, vengono effettuati attacchi informatici verso piattaforma non efficienti e aggiornate e che non adottano livelli di sicurezza adeguati per proteggere i dati.

Molti clienti sottovalutano il concetto di sicurezza fin qui esposto, fin quando non si trovano poi ad essere sottoposti a verifiche che vadano a comprovare che la sicurezza sulla base del dato trattato è venuta meno.
Per fare un esempio, se la mia azienda tratta la vendita di prodotti on line tramite un sistema e-commerce, io devo proteggere i dati degli acquirenti.
Se tramite una vulnerabilità un hacker riesce ad acquisire i dati degli acquirenti, questo va a rientrare in quello che viene definito data breach, ovvero furto di dati.

Se ciò avviene, il nuovo Regolamento europeo, pena sanzioni, obbliga chi ha subito questo furto a esporlo in pubblico, attraverso una pagina web riconoscibile e anche attraverso comunicazioni dirette ai propri clienti, ammettendo il danno e spiegando i fatti:

- Come, quando e perché è avvenuto
- Quando si è intervenuti e in che modo
- Cosa è stato fatto per il futuro

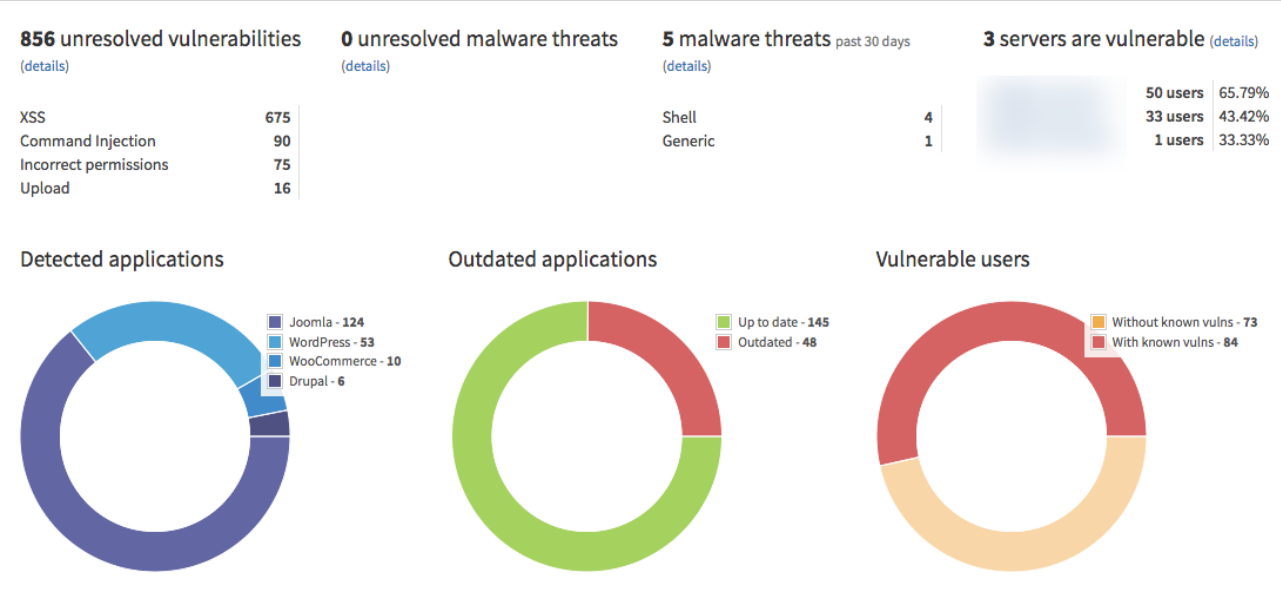
Partendo quindi da un concetto fondamentale, che nessun sistema è invulnerabile al 100%, bisogna entrare nel concetto esposto nella premessa, ovvero l'adozione di "**misure idonee**" per la protezione dei dati.

Per questo motivo, sia per proteggere i nostri dati sia quelli dei nostri clienti, S-D Consulting ha introdotto negli anni ulteriori livelli di sicurezza che, però, non possono comunque sostituirsi al comportamento dei clienti che, di base, non comprendono che sono loro i primi a dover proteggere adeguatamente le proprie piattaforme con tutti gli strumenti possibili.

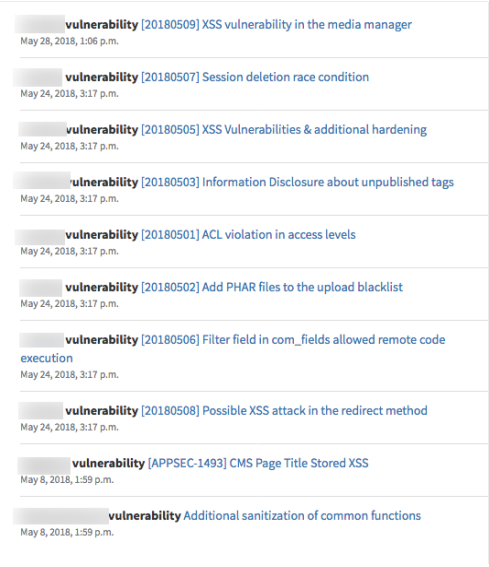
Quali sono quindi i sistemi che utilizziamo oltre alle protezioni lato hardware?

SISTEMI ANTIMALWARE

Tramite degli agent tutti i nostri server sono dotati di un sistema di monitoraggio in tempo reale che mantiene scansionate tutte le piattaforme web presenti sui nostri cloud server:



Come si evince dalla immagine in esempio, questo sistema monitora, verifica e segnala tutte le vulnerabilità di ogni piattaforma, mostrandone anche il livello di criticità.



Non si limita solo alla segnalazione; attraverso delle policy di sicurezza, laddove il cliente non interviene (ad esempio delle outdated applications), applica delle patch di sicurezza che possono impedire l'utilizzo di vulnerabilità note per effettuare attacchi.
Questo fa si che l'applicativo venga mantenuto il più possibile integro e che si evitino danni ulteriori.

E' poi cura nostra segnalare al cliente di intervenire, e nei casi più rari, oscurare il sito web in attesa di un intervento laddove il cliente non dia riscontro alle nostre segnalazioni.

Questo viene fatto per proteggere i dati di tutti i nostri clienti.

Il sistema segnala peraltro anche ulteriori informazioni che riguardano le vulnerabilità note, con suggerimenti per gli utenti sull'adozione di modalità di intervento.

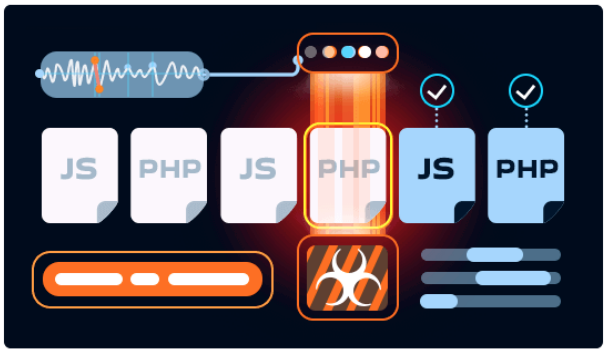
Attraverso degli appositi cruscotti, ma anche attraverso segnalazioni mediante posta elettronica immediata, è attivo un monitoraggio in tempo sostanzialmente reale di quanto sta avvenendo su tutti i nostri cloud server.

SISTEMI DI MONITORAGGIO ADDIZIONALI E ANTIVIRUS

Attraverso uno strumento di rilevamento di malware e virus, abbiamo installato un sistema di controllo automatico che verifica, due volte al giorno:

- La presenza dei nomi a dominio assegnati ai clienti all'interno di blacklist
- Qualsiasi tipo di file dannoso tra cui backdoor, web-shell, virus, strumenti di hacker, script "blackhat SEO", pagine di phishing e molto altro

Si tratta di un sistema che supporta tutti i C.M.S. basati su piattaforma PHP come Wordpress, Joomla, Drupal, Magento, Bitrix e siti web html statici.
Il sistema, previo un potente sistema di filtraggio, prevede la scansione e la pulizia automatica di tutto ciò che viene rilevato.
Al fine di proteggere la piattaforma del cliente, invece di procedere a una rimozione definitiva, pone in quarantena per 7 giorni i file, per poi cancellarli definitivamente.



Quando vengono rilevate situazioni come quelle sopra descritte, il nostro help desk si mette in contatto con il Cliente per segnalare il problema e per suggerire gli interventi da svolgere nell'immediato.

Il sistema si preoccupa anche di aggiornare costantemente il proprio database per riconoscere con sempre più precisione vulnerabilità note, malware e altri elementi che possono causare danni.

Ulteriori livelli di sicurezza lato software

Adottiamo altri sistemi di monitoraggio addizionale basati su piattaforme esterne che si preoccupano di monitorare i file e blacklist, sempre con l'intento di definire il livello di intervento da svolgere nel caso di una segnalazione.

Sono tutti sistemi di cui il cliente può apprendere il funzionamento mettendosi in contatto con il nostro DOP.

Disaster Recovery e Business Continuity

Una premessa è doverosa al fine di spiegare ai clienti la differenza tra Disaster Recovery e Business Continuity in quanto ancora oggi c'è ancora molta confusione.

La preoccupazione di subire un guasto tecnico o una perdita di dati al momento di progettare la propria infrastruttura Cloud è importante.

Per questo motivo – e lo spiegheremo nel paragrafo successivo su come S-D Consulting si è mossa – è importante innanzitutto un sistema di backup che permetta, in tempi rapidi, il recupero di una piattaforma web relativo al sito di un cliente o comunque di un suo applicativo.

Ma quale è la differenza tra Disaster Recovery (in seguito "DR") e Business Continuity (in seguito "BC")?

Il DR non è altro che un sistema di backup che permette il recupero dei dati in caso di disastro.
Per mettere in pratica un sistema del genere, significa salvare i dati su un sito secondario.

Ovviamente per "disastro" si intende un evento di qualsiasi natura, da quello più grave derivante da una catastrofe naturale, fino ad arrivare al banale errore - che potrebbe essere accidentale - derivante dall'operatività sulla propria piattaforma.

Il DR non riguarda solo i dati, ma anche il resto dei sistemi, quindi deve includere non solo i dati salvati ma anche tutto quello che serve per ripristinare il servizio in caso di disastro.

La principale preoccupazione di un cliente che implementa un piano di Disaster Recovery riguarda due aspetti:

- RTO (Recovery Time Objective), ovvero la durata massima del fermo, che va stabilita nella pianificazione del lavoro
- RPO (Recovery Point Objective), ovvero la quantità massima di dati a cui un'azienda è disposta a rinunciare a seguito di un problema

Il DR, cosi come concettualmente esplicato sopra, non evita un fermo lavoro, in quanto il tempo fisico di recupero dei dati non permette comunque l'uso del proprio applicativo fin quando non si è completato il ripristino.

La BC invece si riferisce al tempo in cui un Cliente è disposto ad attendere per il ripristino dei propri dati. Se il Cliente vuole mantenere una continuità operativa in caso di disastro o danno ai sistemi, deve comunicarlo in quanto va strutturata una infrastruttura che preveda anche un sistema di IP failover che

consenta di effettuare uno switch del DNS associato al cloud server da una server farm a un'altra, riducendo al minimo il blackout che potrebbe derivare.

Il sistema di Cloud Backup

S-D Consulting adotta per tutti i cloud server anche un sistema di Cloud Backup che si occupa di effettuare un backup giornaliero di tutti i dati, con una policy di retention a 4 versioni.

In caso quindi di disastro, tutti i sistemi sono ridondati sulla sede del data center opposto affinchè siano protetti e quindi rientrino nell'ottica di una protezione da danno che non sia solamente incidentale, ma proprio infrastrutturale dell'edificio.

La BC quindi è adottata solamente per i clienti che ne hanno fatto espressa richiesta, ma invitiamo alla attenta lettura delle informazioni a seguire per quanto riguarda la nostra policy legata alla protezione dei dati.

Il nostro Cloud Backup opera sui concetti di RTO e RPO sopra esposti.

Per questo infatti abbiamo adottato un sistema che:

- Mette al sicuro il dato
- Utilizza un sistema di livello Enterprise basato su IBM Spectrum Protect
- Consenta un utilizzo rapido tramite amministrazione e controllo completo via web
- Ci permetta di gestire una assistenza tecnica in loco 365/7/24

Le caratteristiche principali del sistema:

- Spazio dati che consenta di gestire una grossa mole di dati e che si autoadatti a livello di storage per quello che è necessario in quel momento, senza rischi di perdita di dati
- Nodi di backup aggiuntivi
- Scelta personalizzata di policy di retention
- Traffico compreso con un sistema di verifica dei file trasmessi al fine di ridurre al minimo l'utilizzo della connessione e quindi spreco di risorse inutili

Il tutto tramite installazione di un client appositamente studiato per i cloud server oggetto di backup.

Come sopra esposto, il servizio erogato su hosting tradizionali non comprende alcun servizio specifico di BC o DS, ma grazie al nostro Cloud Backup viene eseguito un Disaster Recovery (target di memorizzazione in un diverso data center) che poi forniamo gratuitamente al cliente.
I clienti che pretendono una BC devono richiedere appositamente il servizio.

Avendo a disposizione più data center, esiste un distinguo di tempi di ripristino, in caso di disastro, diviso in tre time:

1. Estrazione dei dati dal backup
2. Riprisitno della infrastruttura in un diverso data center
3. Ripristino funzionale dell'infrastruttura con i dati di backup

Il tempo complessivo dei tre time è dato quindi da una latenza iniziale organizzativa e da un tempo operativo necessario per il ripristino della infrastruttura tecnologica e dei dati.

Per fornire quindi il tutto in una tabella, qui di seguito i tempi sopra descritti:

Cluster di criticità	**Tempo di latenza**	**Tempo operativo**
Estrazione dei dati dal Cloud Backup	6h	30min per TB (tempo minimo)
Ripristino rete	1h	8h
Ripristino infrastruttura in diverso data center *	1 – 30gg	1 – 30gg

* In assenza di una previsione di servizio di DR i tempi includono il provisioning di apparecchiature non presenti al momento del disastro.

Cloud Backup: un test di dimostrazione e di procedura di recupero:

Riprendendo quindi quanto affermato nel paragrafo QSA, svolgiamo periodicamente analisi infrastrutturali per apprendere se l'efficienza dei nostri sistemi si mantiene sempre costante nel tempo.

Qui di seguito un esempio di recupero di backup che va a dimostrare quale sia il tempo di recupero di una grossa mole di dati per un sito web che ha subito un eventuale attacco o non raggiungibile per motivi imputabili a molteplici fattori:

Estrazione dei dati dal Cloud Backup e loro posizionamento in diversa directory:

```
Total number of objects restored:       125,891
Total number of objects failed:               0
Total number of bytes transferred:         8.35 GB
Data transfer time:                      333.63 sec
Network data transfer rate:           26,244.30 KB/sec
Aggregate data transfer rate:         14,363.36 KB/sec
Elapsed processing time:               00:10:09
```

Al fine di mantenere tempi rapidi, il recupero dei dati nell'esempio riportato richiede anche il recupero delle tabelle del database.
I nostri processi, come ulteriore sistema di backup, utilizzano anche uno script giornaliero che si preoccupa di creare un archivio SQL di tutti i database presenti sul Cloud Server, e di creare una copia statica degli ultimi 30 giorni.

L'esempio sopra è quindi di un sito web con le seguenti caratteristiche:

Tipologia del dato recuperato	**Mole dati**	**Tempo di ripristino**
Recupero dei file dal cloud backup	8,35 Gigabyte 125.891 file	Circa 10 minuti
Database SQL	4 Gigabyte	2 minuti
UP del sito web		20 / 30 minuti

I tempi qui sopra esposti nella procedura ipotizzano il recupero del backup ma non sostituiscono i tempi di recupero della rete e della tempistica di realizzazione in una diversa infrastruttura (si parla chiaramente di disastri dove un intero data center risulta impraticabile).

Modifiche al documento

La stesura del presente documento (GDPR Compliance) è disponibile dal **25 maggio 2018**, come indicato nella tabella delle revisioni alla seconda pagina del presente documento dopo il sommario.

S-D Consulting si riserva di modificare o semplicemente aggiornare il contenuto, in parte o completamente, anche a causa di variazioni della normativa applicabile o semplicemente per dei cambi infrastrutturali.

Se le modifiche riguardano cambiamenti sostanziali, o possono avere comunque un impatto rilevante sugli interessati, S-D Consulting avrà cura di notificarlo opportunamente agli interessati.