OVHcloud

Come proteggere la tua attività online

Una guida completa per proteggere la tua azienda dai 3 principali fattori di rischio

Contenuto

Introduzione

LA CRESCITA DELL'ATTIVITÀ PORTA MAGGIORI OPPORTUNITÀ... E RISCHI

Man mano che il panorama digitale si espande ed evolve, aumentano anche i rischi per le piccole e medie imprese (PMI).

Per avere successo nel mercato competitivo di oggi, bisogna migliorare la propria presenza online. Per sfruttare al meglio i vantaggi della digitalizzazione, come scalabilità, maggiore produttività, migliore customer experience ed esposizione a un pubblico globale, è fondamentale sviluppare un piano per costruire un'infrastruttura digitale efficace.

Esistono tre fattori di rischio principali legati alla reputazione, ai costi e alla cybersicurezza, che bisogna essere in grado di gestire man mano che la propria attività online cresce. Per fortuna, affrontare questi rischi è più semplice che mai. Le soluzioni fondamentali per proteggere un'attività (ad esempio hosting Web, sicurezza dei domini, backup dei dati) sono talmente sviluppate da non rendere più necessario assumere tecnici full time o lavorare con fornitori costosi per raggiungere i propri obiettivi.

Ecco come realizzare azioni pratiche e adottare una tecnologia di semplice utilizzo per proteggere l'attività e distinguersi dalla concorrenza grazie a una strategia digitale vincente.

OVHcloud

01

Proteggi il marchio e la reputazione man mano che la tua presenza digitale cresce

La reputazione è un bene inestimabile

Il 90% degli acquirenti online dichiara di non aver acquistato da un'azienda a causa della sua cattiva reputazione.[1]

La gestione del marchio e della reputazione diventa sempre più importante man mano che l'azienda aumenta la propria presenza online. Espandersi tramite diverse piattaforme online, come siti Web, social media e e-mail marketing, significa interagire con un numero maggiore di potenziali clienti. Un pubblico più vasto apre nuove opportunità di vendita e crescita.

Una reputazione del marchio affidabile non solo aiuta il business, ma contribuisce a mantenere la fedeltà dei clienti attuali. Una ricerca condotta da Trustpilot[1] ha dimostrato che una "buona reputazione online" è il principale fattore che aumenta la fiducia dei consumatori. Oltre il 95% di loro afferma che la reputazione fa una notevole differenza quando si tratta di scegliere se acquistare o meno da un marchio.

Tuttavia, si tratta di un'arma a doppio taglio: man mano che la presenza online cresce, i pensieri e le opinioni dei clienti vengono amplificate tramite post, blog, recensioni e altro ancora. Una sola esperienza negativa può essere trasmessa a un pubblico ampio, danneggiando la tua reputazione e spingendo gli acquirenti a rivolgersi altrove.

Ecco tre step da seguire per aiutare il tuo marchio a mantenere una reputazione eccellente e ispirare fiducia.

---

[1] TrustPilot, The Value of a Trustworthy Brand Reputation Report

ELABORA UNA STRATEGIA PER I DOMINI

Scegliere e mantenere il dominio giusto è fondamentale per fare una buona impressione. Un dominio è un indirizzo unico utilizzato per accedere al sito Web (ad esempio, ovhcloud.com). Tuttavia, è molto di più di questo: un dominio è parte dell'identità dell'azienda.

Un dominio sicuro deve essere breve, facile da ricordare e legato al marchio.

Quando acquisisci un dominio, devi definire una strategia per proteggere l'azienda dai rischi legati alla reputazione. Il cybersquatting, ad esempio, è una tecnica utilizzata da malintenzionati che impersonano un marchio e ingannano gli utenti affinché condividano dati sensibili. Ad esempio, i cybercriminali potrebbero tentare di registrare un dominio simile al tuo e contenente un'estensione leggermente diversa (ad esempio .co invece di .com) o un'estensione ingannevole legata allo scopo del tuo sito Web (ad esempio, ovh.cloud invece di ovhcloud.com).

Per limitare i danni alla reputazione causati dal cybersquatting, è bene registrare domini che riducano al minimo il rischio di queste minacce. OVHcloud semplifica questo processo suggerendo automaticamente delle opzioni dal nostro catalogo di oltre 900 estensioni come quelle più diffuse (ad esempio, .com, .net, .org), quelle legate alla localizzazione (.fr, .eu, .uk...) e quelle correlate al settore (ad esempio, .fashion, .health, .tech). OVHcloud offre inoltre la possibilità di registrare gli errori di ortografia più comuni del tuo dominio o nomi visivamente simili (ad esempio, uno 0 al posto di una o).

È inoltre fondamentale mantenere il possesso dei domini il più a lungo possibile. La perdita di un dominio può portare a danni alla reputazione (i clienti si confondono quando finiscono su un sito diverso) o anche a costi esorbitanti per recuperare il nome dai cybersquatters che sfruttano questo errore a proprio vantaggio. Per questo motivo, OVHcloud rinnova automaticamente i domini di default, in modo da ridurre il rischio che qualcun altro possa utilizzarli.

Proteggi il tuo marchio con un dominio sicuro

Oltre a queste strategie, esistono altre misure da adottare per proteggere il dominio dagli attacchi informatici. Gli attori malintenzionati possono ricorrere a tecniche come il domain slamming (ad esempio, richieste di trasferimento illegittime) e il cache poisoning per reindirizzare gli utenti verso un altro sito Web, che potrebbero utilizzare per attacchi di phishing, spam o hosting di contenuti dannosi. Questo può danneggiare gravemente la reputazione e minare la fiducia dei clienti.

Ti consigliamo di seguire tutti questi step e adottare un approccio multilivello per garantire la sicurezza del dominio. In questo modo, se una minaccia informatica riesce ad aggirare una misura di sicurezza, esiste un altro livello progettato per fermare quel tipo di attacco.

Per difendersi da questi sofisticati attacchi al dominio, OVHcloud offre un approccio semplice di tipo "push button" che consente di:

▶ 1

Attivare Domain Name System Security Extensions (DNSSEC) per proteggersi da cache poisoning, una tattica criminale usata per deviare il traffico verso siti Web malevoli.

▶ 2

Attivare un meccanismo per impedire al dominio di ricevere notifiche di rinnovo false e altre richieste di trasferimento fraudolente.

▶ 3

Adottare meccanismi di sicurezza per i siti Web e le email, come i certificati SSL (Secure Sockets Layer) e TLS (Transport Layer Security).

Mantenere la fiducia nel marchio con la continuità operativa

Ovviamente è impossibile eliminare al 100% i rischi del mondo digitale. Ecco perché è necessario disporre di un piano nel caso in cui si verifichi un evento (ad esempio un attacco informatico o un picco di traffico) in grado di mettere offline il sito. I tempi di arresto del sito Web sono frustranti per i clienti, possono incidere sui guadagni e causare danni alla reputazione duraturi.

Il downtime può costare alle piccole imprese fino a **427 dollari al minuto.**[2]

Un piano di continuità aiuta a mantenere il sito sempre operativo, con downtime minimi o nulli in caso di incidente. È parte integrante della strategia di protezione della reputazione che consente di mantenere stabile la propria presenza online. Per elaborare un piano di continuità, segui questi passaggi:

Identifica le applicazioni e i dati più importanti necessari per la business continuity;

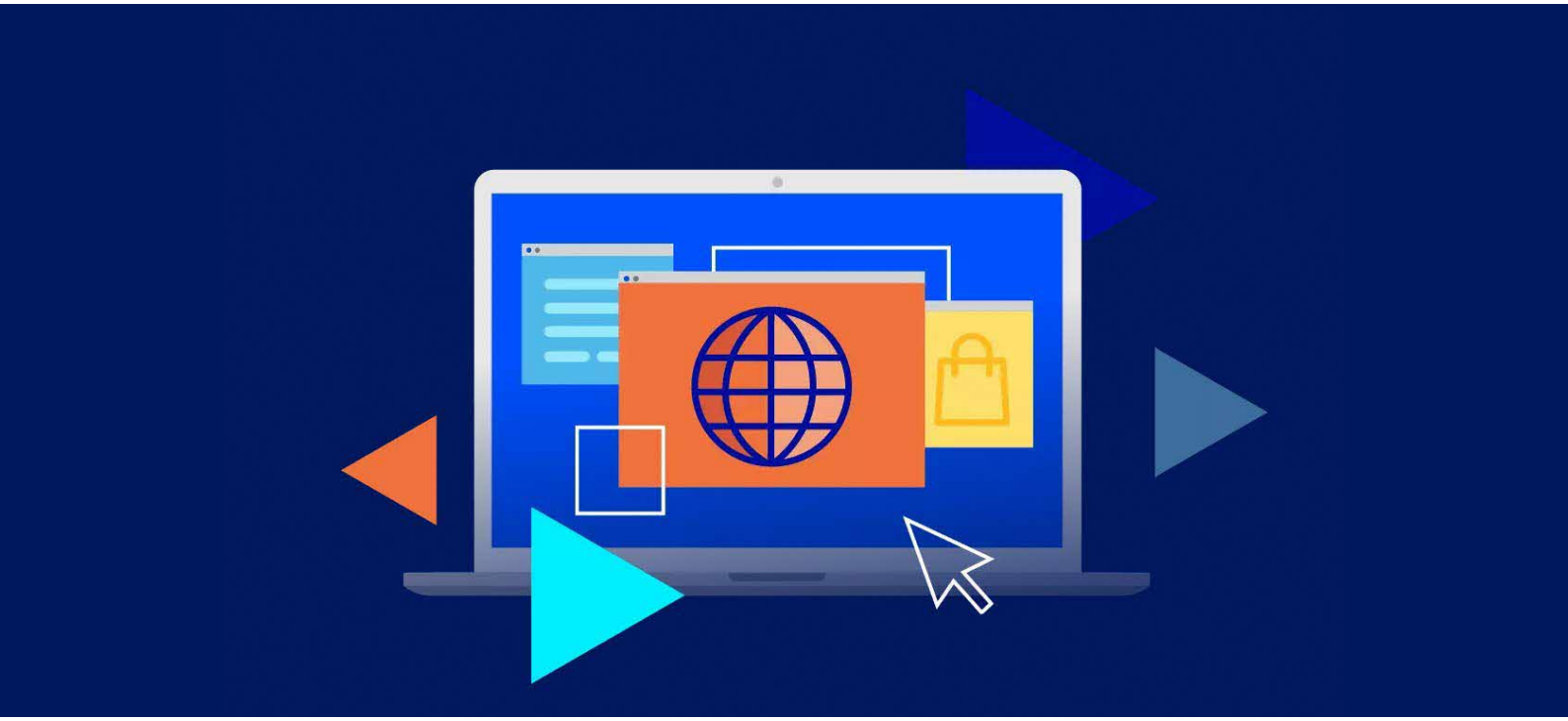
Assicurati che solo i dipendenti qualificati e con competenze IT adeguate possano accedere e modificare i servizi critici che potrebbero mettere il sistema fuori servizio;

Effettua regolarmente il backup di dati e sistemi critici (ad esempio, file, contenuti, database, ecc...) in modo che il sito Web possa essere ripristinato rapidamente, se necessario;

Scegli un provider affidabile in grado di fornire un uptime ottimale per le funzioni essenziali del tuo sito Web e opzioni di disaster recovery.

Per i clienti che utilizzano un hosting Web, OVHcloud monitora la rete per rilevare tentativi di hacking, ad esempio un numero anomalo di richieste sul server, e invia un alert per consentire agli utenti di intervenire immediatamente per risolvere il problema.

[2] Pingdom, Average Cost of Downtime Per Industry



L'hosting Web OVHcloud include anche backup automatici per garantire l'integrità dei dati e un rapido ripristino (ad esempio in caso di errore nella gestione del sito Web), consentendoti di ridurre al minimo i tempi di inattività e mantenere una buona reputazione. Ti suggeriamo inoltre di adottare una strategia di backup "3, 2, 1":

3

Crea **tre** copie dei dati (l'originale più due copie di backup).

2

Salvali su **due** supporti diversi (ad esempio, un disco in un sito remoto, uno storage Cloud, ecc.).

1

Mantieni **una** copia offline su una soluzione di storage disconnessa dal resto della rete o su un supporto di storage rimovibile.

Lavorare con più fornitori per acquisire la tecnologia necessaria a seguire queste best practice può essere costoso e complesso da gestire. OVHcloud, invece, è un partner unico e conveniente che offre strumenti in grado di proteggere il tuo dominio e la tua reputazione.

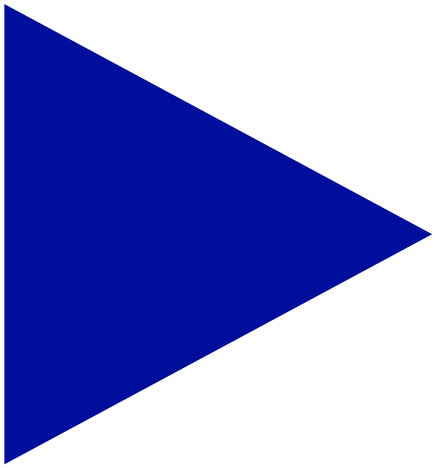
OVHcloud

02

Costruisci una stabilità finanziaria per affrontare mercati imprevedibili

CASH IS KING

Il denaro è diventato una risorsa preziosa per le aziende di tutte le dimensioni. Le PMI, in particolare, si stanno ancora riprendendo dalle conseguenze economiche devastanti della pandemia, il che significa che hanno spesso un flusso di cassa limitato e una tolleranza molto bassa per le spese impreviste.



“Non distogliere mai lo sguardo dal flusso di cassa, perché è la linfa vitale del business.” – Sir Richard Branson

È importante che il flusso di cassa sia stabile e prevedibile. Tuttavia, potresti essere scoraggiato dal sapere che molti dei prodotti e servizi che stai considerando per costruire la tua presenza online includono costi aggiuntivi, spese di rinnovo e altri costi nascosti. La conseguenza potrebbe essere quella di rimanere bloccati in un rapporto a lungo termine.

Ad esempio, alcune soluzioni di hosting Web possono apparire interessanti perché sono di semplice utilizzo (a causa di una personalizzazione limitata). Tuttavia, queste offerte apparentemente a basso costo possono diventare eccessivamente costose, dato che è necessario ricominciare da capo se si passa a un altro provider.

Ecco tre step da seguire per evitare di assumersi rischi finanziari eccessivi legati al lancio e alla manutenzione del sito Web.

TIENI CONTO DELL'INFRASTRUTTURA DIGITALE NELLA PIANIFICAZIONE FINANZIARIA

L'espansione online dovrebbe stimolare, e non ostacolare, la redditività. Se stai investendo per la prima volta in una o più di queste capacità digitali, devi pianificare con anticipo e porti le domande giuste per controllare i costi, evitare le difficoltà finanziarie e supportare la scalabilità a lungo termine.

Ecco alcuni step da considerare nella pianificazione finanziaria della tua infrastruttura online:

Valutazione delle spese correnti:

controlla le tue spese digitali (ad esempio, licenze software, social media, servizi di posta elettronica, ecc.) e verifica che ogni spesa stia portando risultati in termini di fatturato, risparmio di tempo, valore del marchio e soddisfazione del cliente.

Budget per servizi aggiuntivi:

dato che il sito comporta dei requisiti di hosting e sicurezza, dedica una sezione del budget mensile/annuale da destinare a questi servizi.

Esigenze di hosting:

confronta i provider di hosting in base a fattori come prezzi, funzionalità, supporto clienti e uptime, dando la priorità a quelli che offrono tariffe trasparenti e senza costi nascosti.

Attenzione al lock-in:

alcune aziende rendono molto difficile cambiare provider e infrastrutture senza costi estremamente elevati. Per evitare di trovarti in questo tipo di situazioni, chiedi al provider se viene offerta la piena reversibilità e come evitare il vendor lock-in.

Scalabilità:

scegli un provider che offra scalabilità, sia verticale (ad esempio, aggiornamenti dell'hosting) che orizzontale (ad esempio, servizi aggiuntivi), in modo che il piano di hosting possa adattarsi alla crescita dell'attività.

OVHcloud punta a rendere la pianificazione finanziaria il più semplice possibile grazie a tariffe trasparenti. Inoltre, proponiamo server privati virtuali (VPS) e server dedicati se volessi avere maggiore controllo sui server per creare applicazioni Web, siti Web più complessi e infrastrutture digitali.

SCEGLI UN HOSTING PROVIDER CON TIPOLOGIE DI ABBONAMENTO GRANULARI

È importante scegliere un hosting provider che ti permetta di includere nell'abbonamento solo le caratteristiche e i vantaggi che ti interessano. Devi poter pagare solo le funzionalità e i servizi che utilizzerai effettivamente, con la possibilità di modificare l'abbonamento man mano che le esigenze cambiano.

Preferisci avere a disposizione una selezione ridotta e rigida di piani o una gamma completa di abbonamenti flessibili che possono essere personalizzati in base alle esigenze?

OVHcloud offre diverse opzioni di abbonamento, permettendoti di ottenere il prezzo ideale per le funzionalità e caratteristiche del tuo sito Web. Il nostro obiettivo è offrire il rapporto prezzo/performance ideale per tutti i nostri servizi.

Con OVHcloud, sai esattamente quali saranno i costi mensili, rendendo meno stressante la pianificazione finanziaria. Sappiamo che non esiste una soluzione adatta a tutti. Per questo motivo creiamo piani tariffari granulari per proporti ciò di cui hai bisogno in ogni fase del progetto.

Scegli strumenti di sicurezza di semplice utilizzo

La sicurezza delle PMI è un aspetto spesso trascurato della stabilità finanziaria. Un sito Web ben costruito deve proteggere i dati sensibili, mantenere la fiducia dei clienti e mitigare le perdite finanziarie che possono derivare da una violazione o da un'attività fraudolenta. Si tratta di una minaccia crescente nell'attuale panorama digitale: una ricerca globale di Mastercard[3] indica che le imprese europee sono esposte a un elevato rischio di frode.

Due venditori su tre in Germania hanno notato un aumento delle frodi online.[3]

Se gestisci o elabori informazioni finanziarie, ti consigliamo di utilizzare strumenti e plugin affidabili e aggiornati (come PayPal, Stripe, ecc.) che possono essere facilmente integrati nel tuo sistema di gestione dei contenuti (CMS). Sia i CMS che le aziende di elaborazione dei pagamenti aggiornano frequentemente il software in base all'evoluzione delle minacce, pertanto è importante aggiornare regolarmente i propri strumenti e plugin.

OVHcloud garantisce la protezione dell'infrastruttura di hosting dei siti Web, in modo da permetterti di concentrarti sull'individuazione dei dati critici o sensibili e sullo sviluppo di un piano per proteggerli.

[3] Mastercard, Ecommerce Fraud Trends and Statistics Merchants Need To Know in 2023

OVHcloud

03

Difenditi dalle minacce informatiche

Preoccupati della sicurezza

I cybercriminali non sempre scelgono i bersagli in base alla dimensione o al tipo di attività. Cercano invece delle opportunità da sfruttare, come un CMS obsoleto o una politica di sicurezza debole. Oltre al furto di dati, i malintenzionati possono sfruttare una falla del sistema per manipolare i servizi e il marchio dell'utente o per rappresentare l'azienda ed effettuare attacchi in futuro.

Adottare misure per ridurre i rischi per la sicurezza è ormai un requisito per tutte le aziende. Tuttavia, molte di loro non si sentono preparate ad affrontare le minacce informatiche attuali. In un sondaggio condotto su piccole e medie imprese (PMI) nell'UE[4], il 90% ha dichiarato che i problemi di sicurezza informatica avrebbero gravi conseguenze entro una settimana dall'incidente.

Oltre la metà (57%) delle PMI ritiene che molto probabilmente fallirebbero o cesserebbero l'attività dopo un incidente di sicurezza informatica.[3]

Anche se la sicurezza informatica può sembrare di difficile gestione, esistono diverse misure semplici ma efficaci da adottare per ridurre in modo significativo i rischi. Ecco tre step da seguire per migliorare la sicurezza e la resilienza della propria attività.

[4] European Union Agency for Cybersecurity, SME Cybersecurity Report

SEGUI LE BEST PRACTICE PER LA SICUREZZA INFORMATICA

I criminali informatici spesso utilizzano strumenti automatizzati per analizzare migliaia o addirittura milioni di realtà aziendali e identificare i vettori di attacco. È nel loro interesse trovare qualcosa di cui possano rapidamente approfittare con il minimo sforzo. Le ricerche[5] mostrano che i vettori più comuni includono le credenziali rubate (ad esempio, nome utente e password), il phishing (ad esempio, l'invio di email fraudolente per conto dell'utente) e lo sfruttamento delle vulnerabilità (ad esempio, un bug o una falla nel sistema).

È fondamentale che tu e i tuoi dipendenti prendiate le giuste precauzioni per diminuire il rischio di questi attacchi dannosi. Secondo un report del World Economic Forum[6], il 95% di tutti i problemi di sicurezza informatica è riconducibile a un errore umano. Fortunatamente, non è necessario partire da zero per ridurre i rischi informatici, poiché esistono best practice consolidate e testate nel tempo da utilizzare per proteggere l'azienda. Ad esempio:

Politiche di password sicure: imponi l'utilizzo di password omplesse e l'autenticazione a più fattori per bloccare i tentativi di attacco di basso livello.

Aggiornamenti regolari e patch: mantieni aggiornati tutti i software, inclusi i sistemi operativi, le applicazioni e i plugin, e correggi le vulnerabilità note.

Crittografia dei dati: utilizza protocolli di crittografia per garantire la sicurezza dei dati in transito e per crittografare le informazioni riservate salvate nei server e nei database.

Installazione di firewall: implementa firewall per monitorare e filtrare il traffico di rete, in modo da impedire accessi non autorizzati e rilevare attività sospette.

Backup regolari dei dati: esegui il backup dei dati critici, per verificare che le informazioni siano archiviate in modo sicuro e possano essere ripristinate in caso di incidente informatico.

Comprensione dei propri obblighi: riconosci l'importanza della condivisione delle responsabilità e di ciò che ci si aspetta da te (ad esempio, aggiornamenti software regolari) con gli strumenti che ti vengono forniti.

[5] Verizon, 2023 Data Breach Investigations Report

[6] World Economic Forum, Global Risks Report 2022

Non esiste una soluzione unica e perfetta per garantire la sicurezza: l'unica via percorribile è dotarsi di strumenti di difesa a più livelli.

In OVHcloud offriamo pacchetti di soluzioni di sicurezza per il tuo percorso digitale. Ad esempio, tutti i domini includono DNSSEC per la sicurezza gestita del dominio e i nostri servizi di hosting Web includono certificati SSL per la crittografia dei dati.

Dai priorità alla difesa dagli attacchi DDoS, una minaccia informatica in aumento

Gli attacchi Distributed Denial of Service (DDoS), una tattica malevola per bloccare un servizio su un sito, stanno diventando sempre più frequenti. Le barriere all'ingresso sono scarse: praticamente chiunque può sferrare un attacco DDoS con un set di strumenti automatizzati ed economici.

La peculiarità di questi attacchi è che solitamente non comportano una violazione della sicurezza o il furto di dati, ma hanno semplicemente l'obiettivo di distruggere il sito. Gli autori potrebbero essere criminali che chiedono un riscatto per ripristinare i servizi, competitor malintenzionati che vogliono danneggiare la tua reputazione o semplicemente vandali in vena di creare problemi.

Gli attacchi DDoS aumentano del **200% ogni anno.**[7]

Per questo motivo devi assicurarti che una soluzione anti-DDoS sia inclusa nel sito Web per proteggerti da questa minaccia diffusa. Questo aspetto non è semplice da gestire in autonomia, ma non temere: i servizi di hosting OVHcloud sono dotati di meccanismi di sicurezza, incluso l'anti-DDoS. Questa soluzione include:

- Rilevazione permanente degli attacchi e mitigazione rapida del traffico malevolo
- Utilizzo illimitato, senza costi aggiuntivi indipendentemente dal volume dell'attacco
- Nessun limite di tempo, con protezione per l'intera durata di un attacco DDoS

La nostra tecnologia anti-DDoS funziona perfettamente in background. Indipendentemente dal numero di tentativi degli hacker di sovraccaricare i server, OVHcloud devierà gli attacchi, in modo da ridurre al minimo la percezione di qualsiasi tipo di interruzione.

[7] Zayo Group, The Truth and Trends of DDoS Attacks

Aumenta la sicurezza delle email

Gli attacchi BEC (Business Email Compromise) sono attacchi in cui i criminali inviano email fraudolente, spesso imitando quelle di un'azienda, per rubare informazioni sensibili. In caso di esito positivo, questi attacchi possono essere difficili da rilevare perché spesso non attivano gli allarmi di sicurezza. Il truffatore può avere accesso a informazioni e/o sistemi critici per diversi mesi.

Sono necessari in media **266 giorni** per individuare e contenere una violazione dei dati derivante da un attacco BEC.[8]

OVHcloud offre un'autenticazione sicura, meccanismi anti-spam e protocolli SPF, DKIM e DMARC installati automaticamente che riducono notevolmente il rischio di incidenti. Questi metodi di autenticazione proteggono la tua azienda da email e spam indesiderati, impedendo l'alterazione dei dati come nel caso dello spoofing delle email (indirizzo del mittente contraffatto). Sebbene molti provider facciano installare ai clienti queste funzionalità in autonomia, OVHcloud configura le misure di sicurezza per garantire la massima efficacia.

Scegliendo OVHcloud per i servizi di email, hai la garanzia che le nostre soluzioni funzionino in tre datacenter. Ciò significa che le comunicazioni continueranno a funzionare senza problemi anche in caso di malfunzionamenti o interruzioni del servizio in un sito.

[8] IBM Cost of a Data Breach Report

COSTRUISCI UN FUTURO SICURO PER LA TUA AZIENDA

Il marchio, la reputazione, la situazione finanziaria e la sicurezza sono aspetti strettamente correlati. Per questo motivo non bisogna dimenticare nessuno dei passaggi precedenti per non compromettere l'integrità dell'intera azienda.

Fortunatamente, adottare le misure di sicurezza è più semplice (e meno stressante) che mai. Anziché provare e investire in soluzioni diverse e costose, scegli OVHcloud: un unico provider economico per le tue esigenze digitali.

Scopri di più sulle nostre soluzioni di hosting Web e domini e su come possiamo accompagnarti in una strategia digitale di successo.