OVHcloud

Cómo proteger su empresa online

La guía completa para proteger su empresa de 3 riesgos principales

Contenido

Introducción

EL CRECIMIENTO DEL NEGOCIO CONLLEVA MÁS OPORTUNIDADES Y RIESGOS

A medida que el panorama digital se expande y evoluciona rápidamente, también lo hacen los riesgos a los que se enfrentan las pymes.

Sabe que debe mejorar su presencia online para tener éxito en el mercado actual competitivo. Si desea aprovechar totalmente los beneficios de la digitalización, como la escalabilidad, una mayor productividad, una mejor experiencia del cliente y la exposición a una audiencia global, es esencial que desarrolle un plan para construir una infraestructura digital sólida.

Existen tres tipos de riesgo principales (de reputación, financiero y de ciberseguridad) para los que debe prepararse si desea crecer online. Afortunadamente, en la actualidad esto resulta menos complejo. Las soluciones vitales para proteger su empresa (alojamiento web, protección de dominios, copias de seguridad de los datos, etc.) han avanzado hasta el punto de que ya no tendrá que contratar expertos técnicos a tiempo completo ni trabajar con varios proveedores costosos para alcanzar sus objetivos.

Así es como puede realizar acciones prácticas y adoptar tecnología fácil de usar con el objetivo de proteger su negocio y destacar sobre la competencia con una estrategia digital ganadora.

OVHcloud

01

Proteja su marca y su reputación a medida que crece su presencia digital

La reputación es un activo que no tiene precio

El 90 % de los compradores online han optado por no efectuar una compra de una determinada empresa por su mala reputación.[1]

La gestión de la marca y la reputación cobra cada vez más importancia a medida que su empresa escala su presencia digital. Expandirse a varias plataformas online, como su sitio web, redes sociales y marketing por correo electrónico, le permitirá interactuar con más clientes potenciales. Un mayor público, a su vez, crea oportunidades adicionales para las ventas y el crecimiento.

Una reputación de marca fiable no solo ayuda a atraer nuevos negocios, sino también a mantener la lealtad entre los clientes actuales. Las investigaciones de Trustpilot1 concluyeron que la «buena reputación online» es el factor principal que aumenta la confianza. Más del 95 % de los consumidores creen que la reputación supone una diferencia tangible a la hora de comprar de una marca determinada.

Sin embargo, esto puede ser un arma de doble filo: a medida que crece su presencia online, las ideas y opiniones de sus clientes también se amplifican a través de publicaciones en redes sociales, blogs, reseñas y más. Una sola mala experiencia puede ser transmitida a una gran audiencia, dañando su reputación y animando a los compradores a buscar en otra parte.

A continuación, tres pasos que debe tomar para ayudar a su marca a mantener una excelente reputación para inspirar confianza online.

---

[1] Rapport Trustpilot - La valeur d'une réputation de marque fiable

DISEÑE UNA ESTRATEGIA DE DOMINIO

Elegir y conservar el dominio del sitio web correcto es crucial para dar una buena primera impresión. Un dominio es una dirección única que se utiliza para acceder a su sitio web (por ejemplo, ovhcloud.com). Pero es mucho más que una simple dirección web: un dominio es parte de la identidad de su empresa.

Un dominio seguro debe ser corto, memorable y relevante para su marca.

Al adquirir un dominio, debe diseñar una estrategia a fin de proteger su empresa de riesgos para la reputación. La suplantación de dominio, por ejemplo, es una táctica común que usan los actores maliciosos para suplantar una marca y engañar a los usuarios para que divulguen información sensible. Por ejemplo, los ciberdelincuentes pueden intentar registrar nombres de dominio similares al suyo que contengan una extensión de dominio ligeramente diferente (por ejemplo, .co en lugar de .com) o una extensión engañosa relacionada con el objetivo de su sitio web (por ejemplo, ovh.cloud en lugar de ovhcloud.com).

Con el fin de reducir el riesgo reputacional de la suplantación de dominio, debe registrar dominios que reduzcan al mínimo estas amenazas. OVHcloud facilita esta tarea proponiéndole automáticamente opciones de nuestro catálogo de más de 900 extensiones ampliamente utilizadas en el mercado (por ejemplo, .com, .net, .org), que se ajusten a su localización (por ejemplo, .fr, .eu, .uk) y que estén relacionadas con su actividad (por ejemplo, .fashion, .health, .tech). Incluso puede utilizar OVHcloud para registrar errores ortográficos comunes de su dominio o nombres visualmente similares (por ejemplo, el número 0 en lugar de la letra o).

También es fundamental que mantenga la titularidad de sus dominios durante el mayor tiempo posible. La pérdida de un dominio puede perjudicar a su reputación (los clientes se confunden cuando acceden a otro sitio web) o incluso conllevar costes exorbitantes al recuperar el nombre de los cibersquatters (ciberokupas) que explotan este error en beneficio propio. Por eso, OVHcloud renueva automáticamente los dominios por defecto con el fin de reducir el riesgo de que otra persona se haga con su nombre de dominio.

Proteja su marca protegiendo su dominio

Además de una estrategia de dominios sólida, existen otras medidas que debe tomar para proteger su dominio de riesgos de ciberseguridad. Los actores maliciosos pueden intentar utilizar técnicas como el slamming de dominios (es decir, solicitudes de transferencia ilegítimas) y el envenenamiento de cache para redirigir a los usuarios a otro sitio web, que podrían utilizar para ataques de phishing, distribución de spam o alojamiento de contenido malicioso. Esto puede dañar seriamente su reputación y erosionar la confianza de los clientes.

Le aconsejamos que siga todos estos pasos y que adopte un enfoque multinivel con respecto a la protección de los dominios. De esta manera, si una ciberamenaza elude un tipo de medida de seguridad, existe otra capa en su lugar diseñada para detener ese tipo de ataque.

Para defenderse de estos ataques de dominio, OVHcloud le ofrece una solución sencilla y potente que le permite:

▶ 1

Activar las DNSSEC (extensiones de seguridad del sistema de dominio) para protegerse contra el envenenamiento de la caché, una táctica que utilizan los ciberdelincuentes para desviar el tráfico a sitios web maliciosos.

▶ 2

Activar un mecanismo para evitar que su dominio reciba notificaciones de renovación falsas y otras solicitudes de transferencia fraudulentas.

▶ 3

Adoptar mecanismos de seguridad de sitios web y correo electrónico, como los certificados SSL (secure sockets layer) y TLS (transport layer security).

Mantenga la confianza de su marca con la continuidad del negocio

Obviamente, es imposible eliminar el riesgo digital con una certeza del 100 %. Por eso necesita tener un plan listo en caso de que algo (por ejemplo, un ciberataque o un pico de tráfico) amenace con dejar su sitio web sin conexión. La interrupción del sitio web puede frustrar a los clientes, perjudicar los ingresos y causar un daño duradero a la reputación.

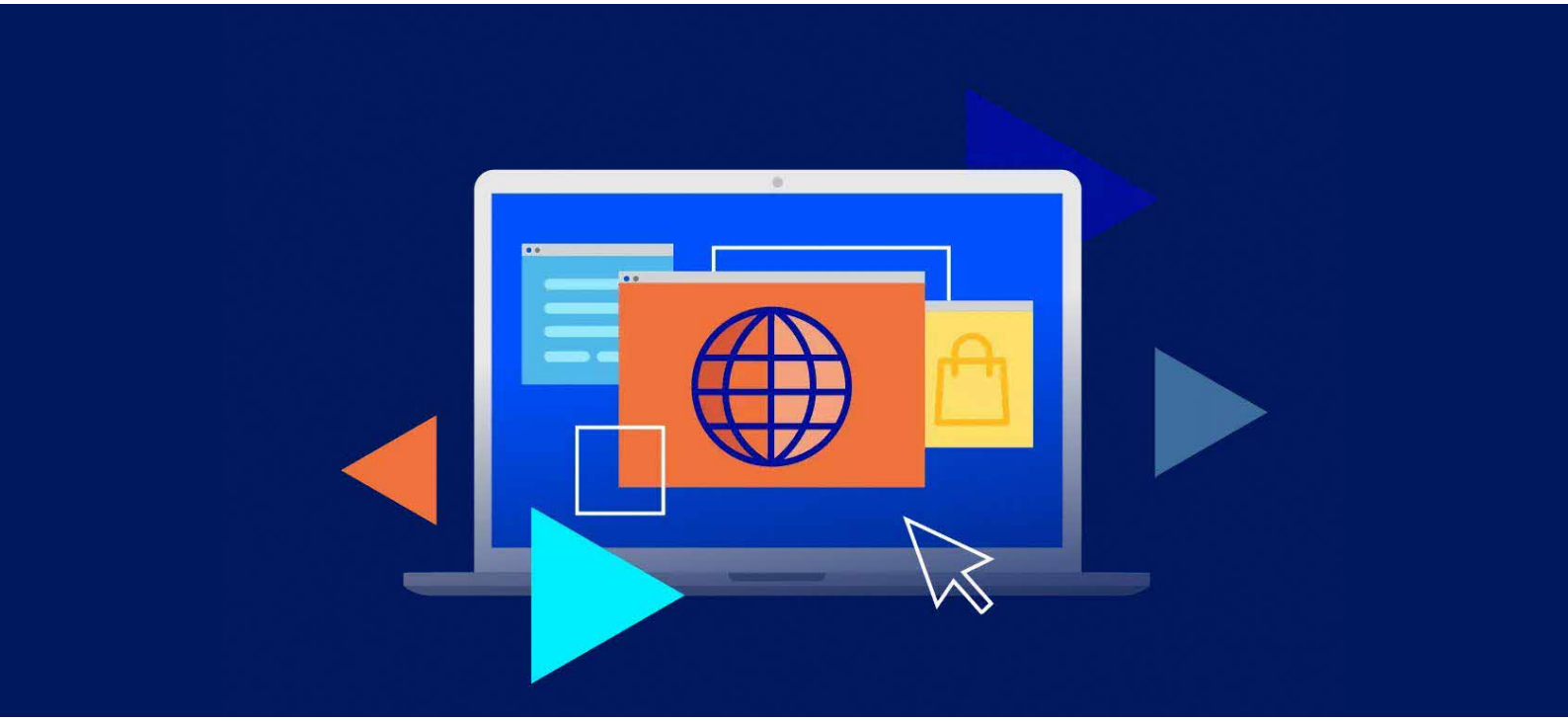
La interrupción del servicio puede costar a las pequeñas empresas hasta **427 dólares por minuto.**[2]

Un plan de continuidad digital le permite estar preparado para mantener su sitio web en funcionamiento con un tiempo de inactividad mínimo o nulo en caso de incidente. Es una parte integral de su estrategia de protección de la reputación que mantiene su presencia online estable. Un plan de continuidad debe incluir pasos como:

- Identificar sus aplicaciones y datos más valiosos que son necesarios para la continuidad del negocio.
- Asegurarse de que sólo los trabajadores capacitados con suficiente experiencia en TI tengan acceso para modificar los servicios críticos que podrían hacer caer el sistema.
- Realizar copias de seguridad periódicas de los datos y sistemas críticos (por ejemplo, archivos, contenido, bases de datos, etc.) para poder restaurar rápidamente su sitio web por si hiciera falta.
- Elegir un proveedor acreditado que pueda proporcionar una disponibilidad óptima para las funciones esenciales de su sitio web, mientras proporciona opciones para la recuperación ante desastres por si fuera necesario.

Para los clientes de un alojamiento web, OVHcloud supervisa la red con el fin de detectar posibles intentos de hackeo, como una cantidad anormal de consultas en el servidor, y emite una alerta con el objetivo de que usted pueda tomar medidas inmediatas para resolver el problema.

[2] Pingdom, Average Cost of Downtime Per Industry



El alojamiento web de OVHcloud también incluye copias de seguridad automáticas para preservar la integridad de los datos y facilitar una rápida recuperación (por ejemplo, si se equivoca al administrar su sitio web), lo que permite a su empresa reducir el tiempo de inactividad y mantener una reputación positiva. También sugerimos que los clientes realicen una estrategia de backup « 3, 2, 1 »:

▶ 3

Crear **tres** copias de sus datos (el original y dos copias de seguridad).

▶ 2

Almacenarlas en **dos** medios diferentes (por ejemplo, un disco en un sitio remoto, almacenamiento en el cloud, etc.).

▶ 1

Mantener **una** copia sin conexión en una solución de almacenamiento desconectada del resto de la red o en un medio de almacenamiento extraíble.

Trabajar con varios proveedores para adquirir la tecnología necesaria con el fin de seguir estas prácticas recomendadas puede resultar costoso y difícil de gestionar. Por otro lado, OVHcloud es un partner único y rentable que ofrece herramientas que contribuyen a proteger su dominio y su reputación.

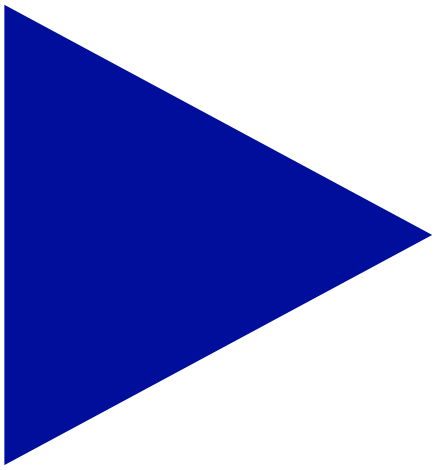
OVHcloud

02

Desarrolle estabilidad financiera para hacer frente a mercados impredecibles

EL EFECTIVO ES ESENCIAL

El efectivo se ha convertido en un activo clave para todas las empresas, sin importar su tamaño. Pero las pymes, en particular, aún se están recuperando de los efectos financieros devastadores de la pandemia, lo que significa que a menudo tienen un flujo de caja limitado y muy poca tolerancia a los costes inesperados.



«Nunca aparte la vista del cashflow, es un elemento vital de cualquier negocio». – Sir Richard Branson

Es importante lograr estabilidad y previsibilidad con su situación de caja. Sin embargo, es posible que se sienta desalentado al saber que muchos de los productos y servicios que está pensando usar para aumentar su presencia online incluyen cargos por uso adicional, tarifas de renovación y otros costes ocultos. También podrían encerrarle en una relación de dependencia a largo plazo.

Por ejemplo, algunas soluciones de alojamiento web parecen en un principio atractivas porque son fáciles de usar (debido a la personalización limitada). Sin embargo, con el paso del tiempo, estas soluciones de aparente bajo coste pueden resultarle caras, ya que tendría que empezar desde cero si cambia a otro proveedor.

A continuación, los tres pasos que debe seguir para evitar que su empresa asuma demasiados riesgos financieros al iniciar y mantener su sitio web.

TENGA EN CUENTA LA INFRAESTRUCTURA DIGITAL EN SU PLANIFICACIÓN FINANCIERA

La expansión online debería impulsar, no obstaculizar, la rentabilidad de su empresa. Si es la primera vez que invierte en una o más de estas capacidades digitales, es crucial que planifique con anticipación y haga las preguntas correctas para controlar los costes, evitar la presión financiera y mantener la escalabilidad a largo plazo.

Entre los pasos clave que debe contemplar en la planificación financiera de su infraestructura online se incluyen:

Evaluar los gastos actuales: Revise sus gastos digitales (por ejemplo, licencias de software, herramientas de redes sociales, servicios de correo electrónico, etc.) y confirme que cada gasto genera valor en cuanto a ingresos, ahorro de tiempo, valor de la marca o satisfacción del cliente.

Planificar un presupuesto para servicios adicionales: Puesto que sabe que su sitio web conlleva naturalmente ciertos requisitos de alojamiento y seguridad, asigne una parte de su presupuesto mensual/anual a estos servicios.

Definir las necesidades en materia de alojamiento: Compare proveedores de alojamiento en función de factores como el precio, las características, el soporte al cliente y el tiempo de disponibilidad óptimo, dando prioridad a aquellos que tienen precios transparentes y sin costes inesperados.

Evitar la dependencia del proveedor: Algunas empresas dificultan enormemente el cambio de proveedores e infraestructuras sin unos costes extraordinariamente elevados. Con el fin de evitar este problema, debe preguntar: «¿Ofrecen reversibilidad total?» y «¿Cómo evitan la dependencia del proveedor?».

Considerar la escalabilidad: Elija un proveedor que permita la escalabilidad, tanto vertical (por ejemplo, las mejoras de hosting) como horizontal (por ejemplo, los servicios adicionales), para que su plan de hosting crezca en función de las necesidades de su empresa.

El objetivo de OVHcloud es simplificar al máximo la planificación financiera mediante la transparencia de los precios. También ofrecemos servidores virtuales (VPS) y servidores dedicados si decide que necesita un mayor control sobre sus servidores a fin de crear aplicaciones web, sitios web más complejos e infraestructuras digitales.

ELIJA UN PROVEEDOR DE HOSTING CON TIPOS DE SUSCRIPCIÓN GRANULARES

Es importante optar por un proveedor de alojamiento web que le permita elegir una suscripción que incluya solo las características y ventajas que le resultarán útiles. Lo ideal es pagar únicamente por las funciones y servicios que usted vaya a utilizar, con la posibilidad de modificar su suscripción a medida que cambien las necesidades de su empresa.

¿Preferiría elegir entre una selección pequeña y rígida de planes o una gama completa de opciones de suscripción flexibles que se pueden adaptar a sus necesidades?

OVHcloud le ofrece distintas opciones de suscripción, permitiéndole pagar el precio ideal por las funcionalidades necesarias para su sitio web. Nuestro objetivo es ofrecer siempre la relación rendimiento-precio ideal para todos nuestros servicios.

Con OVHcloud, sabrá exactamente cuáles serán los costes mensuales, ayudándole a que la previsibilidad financiera y la previsión de costes sean menos estresantes. Sabemos que usted no busca un modelo genérico con soluciones únicas. Por eso ofrecemos planes de precios granulares para proponer lo que realmente necesita en cada etapa de su proyecto.

Adquiera herramientas de seguridad fáciles de usar

La seguridad de las pymes es un aspecto de la estabilidad financiera que suele pasarse por alto. Un sitio web sólido tiene como objetivo proteger los datos confidenciales, mantener la confianza del cliente y mitigar las pérdidas financieras que pueden resultar de un fallo de seguridad o una actividad fraudulenta. Esta es una amenaza que está aumentando en el panorama digital actual: un estudio global de Mastercard[3] indica que las empresas europeas se enfrentan a un alto riesgo de fraude.

Dos de cada tres minoristas online en Alemania han notado un aumento en el fraude online.[3]

Si maneja o procesa información financiera, le sugerimos que utilice herramientas y plugins de confianza y actualizados (por ejemplo, PayPal, Stripe, etc.) que se puedan integrar fácilmente con su sistema de gestión de contenidos (CMS). Tanto los CMS como las empresas de procesamiento de pagos actualizan con frecuencia su software en función de la evolución de las amenazas, por lo que es importante actualizar sus herramientas y plugins con regularidad.

Con OVHcloud, tiene la garantía de que protegeremos su infraestructura de web hosting para que usted pueda centrarse en la identificación de datos críticos o sensibles y en el desarrollo de un plan para proteger esta información.

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

OVHcloud

03

Defiéndase contra las ciberamenazas

Tome las riendas de su seguridad

Los ciberdelincuentes no siempre eligen objetivos en función del tamaño o el tipo de negocio, a menudo buscan oportunidades fáciles de aprovechar, como un CMS obsoleto o una política de seguridad débil. Además del robo de datos, los actores maliciosos pueden infiltrarse para manipular sus servicios y su marca o suplantar su negocio para ayudarles a llevar a cabo futuros ataques.

Tomar medidas que mitiguen el riesgo para la seguridad es ahora un requisito del negocio. Sin embargo, muchas organizaciones no se sienten preparadas para hacer frente a las ciberamenazas actuales. En una encuesta realizada a pymes de toda la UE[4], el 90 % dijo que los problemas de ciberseguridad tendrían un impacto negativo grave una semana después de producirse un incidente.

Más de la mitad (57 %) de las pymes creen que muy probablemente tendrían que declararse en quiebra o dejarían de operar después de un incidente de ciberseguridad.[3]

Si bien la ciberseguridad puede resultar abrumadora, existen muchas medidas simples pero eficaces que puede implementar para reducir significativamente los riesgos. A continuación, tres pasos que debe seguir para mejorar la postura en materia de seguridad y la resiliencia de su negocio.

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

SIGA LAS MEJORES PRÁCTICAS EN MATERIA DE CIBERSEGURIDAD

Los ciberdelincuentes suelen utilizar herramientas automatizadas para escanear miles o incluso millones de entidades empresariales a fin de identificar los vectores de ataque que deben explotar. Les interesa encontrar algo que puedan aprovechar rápidamente con un mínimo esfuerzo. De hecho, existen investigaciones[5] que muestran que los vectores más comunes incluyen credenciales robadas (nombre de usuario y contraseñas), phishing (el envío de correos electrónicos fraudulentos suplantando su identidad) y explotación de vulnerabilidades (un error o fallo en un sistema).

Es esencial que usted y sus trabajadores tomen las precauciones adecuadas para mitigar el riesgo de que estos ataques dañen su negocio. Según un informe del Foro Económico Mundial[6], el 95 % de todos los problemas de ciberseguridad pueden atribuirse a errores humanos. Afortunadamente, no tiene que empezar de cero para reducir sus riesgos de ciberseguridad, ya que existen mejores prácticas establecidas y comprobadas que puede utilizar para proteger su negocio. Incluimos a continuación algunas de estas medidas.

Implementar políticas de contraseñas seguras: Imponga el uso de contraseñas complejas y autenticación multifactor para bloquear los intentos de bajo nivel de evitar la seguridad.

Realizar actualizaciones y aplicar parches de forma regular: Mantenga actualizado todo el software, incluidos los sistemas operativos, las aplicaciones y los plugins, y corrija las vulnerabilidades conocidas.

Cifrar los datos: Utilice protocolos de cifrado para proteger los datos en tránsito y cifrar información confidencial almacenada en servidores y bases de datos.

Instalar firewalls: Implemente firewalls para monitorear y filtrar el tráfico de la red, lo que ayuda a evitar el acceso no autorizado y a detectar actividades sospechosas.

Realizar copias de seguridad de los datos regularmente: Realice copias de seguridad de los datos críticos y confirme que la información se almacena de forma segura y que se puede restaurar en caso de incidente cibernético.

Comprender sus obligaciones: Reconozca la importancia de la responsabilidad compartida y lo que se espera que haga (por ejemplo, realizar actualizaciones de software regularmente) con las herramientas que se le proporcionan.

[5] Verizon, 2023 Data Breach Investigations Report

[6] World Economic Forum, Global Risks Report 2022

No existe una solución perfecta y genérica para conseguir una seguridad completa: una protección por capas es la única defensa viable.

En OVHcloud, ofrecemos soluciones de seguridad en paquetes para su aventura digital. Por ejemplo, todos nuestros servicios de dominio incluyen DNSSEC para la seguridad administrada de su dominio, y nuestros servicios de alojamiento web incluyen certificados SSL para el cifrado de datos.

Priorice la protección contra los ataques DDoS, una ciberamenaza creciente

Los ataques de denegación de servicio distribuidos (DDoS) —la táctica maliciosa para obstruir el servicio de un sitio web— son cada vez más frecuentes. La barrera de acceso es muy baja: casi cualquiera puede llevar a cabo un ataque DDoS con un conjunto barato de herramientas automatizadas.

Estos ataques son únicos en el sentido de que, por lo general, no implican una violación de la seguridad o un robo de datos. El objetivo es simplemente interrumpir el servicio de su sitio web. Los hackers pueden ser criminales que intentan solicitar un rescate a cambio de restaurar servicios; son pues competidores maliciosos que quieren manchar su reputación, o simplemente vándalos digitales que buscan causar problemas.

Los ataques DDoS aumentan un **200 %** año tras año.[7]

Por eso debe confirmar que la prevención DDoS está incluida en su sitio web para protegerse de esta amenaza común. Aunque esto puede ser difícil de realizar por su cuenta, la buena noticia es que los servicios de alojamiento de OVHcloud incluyen mecanismos de seguridad, como el anti-DDoS. Descubra las soluciones cloud de OVHcloud:

- Detección de ataques constante y rápida mitigación del tráfico malicioso.
- Uso ilimitado, lo que significa que no hay coste adicional independientemente del volumen del ataque.
- Sin límite de tiempo, con una protección que actúa durante todo el trascurso de un ataque DDoS.

Nuestra tecnología anti-DDoS funciona sin problemas en el contexto de su sitio web. No importa cuántas veces intenten los hackers sobrecargar sus servidores, OVHcloud intentará desviar los intentos a fin de minimizar su percepción de todo tipo de interrupción.

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

Mejore la seguridad de su correo electrónico

La infiltración del correo electrónico empresarial (BEC por las siglas inglesas) es un tipo de ataque muy común en el que los delincuentes envían correos electrónicos fraudulentos, a menudo imitando a los de una empresa, con el fin de robar información confidencial. Cuando tienen éxito, estos ataques pueden ser difíciles de detectar porque a menudo no activan alertas de seguridad. El actor malicioso puede tener acceso a información y/o sistemas críticos durante meses.

Se tarda un promedio de **266 días** en identificar y contener una violación de datos resultante de una infiltración en el correo electrónico empresarial.[8]

OVHcloud ofrece una autenticación sólida, mecanismos antispam, SPF, DKIM y protocolos DMARC instalados automáticamente, que reducen considerablemente el riesgo de incidencia relacionada con el correo electrónico. Estos métodos de autenticación de correo electrónico protegen su empresa contra el correo electrónico no deseado y el spam, evitando la alteración de datos como la suplantación de identidad (es decir, la falsificación de una dirección de remitente). Aunque muchos proveedores hacen que los clientes configuren estas funciones por su cuenta, nosotros configuramos estas medidas de seguridad con el fin de obtener la máxima eficacia.

Al elegir OVHcloud para sus servicios de correo electrónico, también puede estar tranquilo de que nuestras soluciones funcionan en tres datacenters diferentes. Esto significa que sus comunicaciones continuarán funcionando sin problemas incluso en caso de una caída del servicio o interrupción del servicio en una ubicación.

[8] IBM Cost of a Data Breach Report

CONSTRUYA UN FUTURO SEGURO PARA SU EMPRESA

Su marca, reputación, posición financiera y postura de seguridad están profundamente entrelazadas, lo que significa que no debe saltarse ni omitir ninguno de los pasos anteriores sin arriesgar la integridad de todo el negocio.

Afortunadamente, tomar las medidas necesarias para proteger su negocio es menos estresante y más sencillo que nunca. En lugar de buscar e invertir en muchas soluciones individuales costosas y diferentes, puede asociarse con OVHcloud, una solución asequible e integral para sus necesidades digitales.

Más información sobre nuestras soluciones de alojamiento web y dominios para descubrir cómo podemos ayudarle a desarrollar su estrategia digital.