OVHcloud

Como proteger o seu negócio online

Um guia completo para proteger a sua empresa contra 3 riscos principais

Contente

Introdução

O CRESCIMENTO DE UM NEGÓCIO TRAZ MAIS OPORTUNIDADES... E RISCOS

À medida que a paisagem digital se expande e evolui rapidamente, também os riscos que as pequenas e médias empresas (PME) enfrentam aumentam.

Também sabe que precisa de reforçar a sua presença online para vencer o mercado competitivo atual. Para usufruir plenamente dos benefícios da digitalização — como a escalabilidade, uma maior produtividade, uma melhor experiência do cliente e uma exposição a um público mundial —, é essencial desenvolver um plano para construir uma infraestrutura digital robusta.

Existem três tipos de risco principais (reputação, financeiro e cibersegurança) para os quais deve estar preparado durante o seu crescimento online. Felizmente, precaver-se é menos complexo do que nunca. As soluções essenciais para a proteção da sua empresa (por exemplo, alojamento web, segurança de domínio, backups de dados) evoluíram de tal forma que já não é necessário contratar especialistas técnicos a tempo inteiro, nem trabalhar com vários fornecedores onerosos para atingir os seus objetivos.

Veja como realizar ações práticas e adotar tecnologias intuitivas para proteger o seu negócio e destacar-se da concorrência graças a uma estratégia digital vencedora.

OVHcloud

01

Proteja a sua marca e reputação à medida que a sua pegada digital cresce

A reputação é um bem inestimável

90% dos compradores online optaram por não comprar a uma empresa devido à sua má reputação.[1]

A gestão da marca e da reputação torna-se cada vez mais importante à medida que a pegada digital do seu negócio aumenta. A expansão para múltiplas plataformas online — como o seu site, as redes sociais e o e-mail marketing — permite interagir com um maior número de potenciais clientes. Um público maior, por sua vez, abre oportunidades adicionais para vendas e crescimento.

Uma reputação de marca fiável não só ajuda a atrair novos negócios, como também a manter a lealdade por parte dos clientes atuais. Uma pesquisa da Trustpilot[1] concluiu que « a boa reputação online » é o fator número um que aumenta a confiança. Mais de 95% dos consumidores acreditam que a reputação faz uma diferença tangível na sua vontade de comprar de uma marca.

No entanto, esta é uma faca de dois gumes — à medida que a sua presença online cresce, as ideias e opiniões dos seus clientes também são amplificadas através de publicações sociais, blogues, críticas, e muito mais. Uma única má experiência pode ser divulgada para um público maior, prejudicando a sua reputação e levando os compradores a procurar noutro lado.

Estes são três passos que deve seguir para ajudar a sua marca a manter uma excelente reputação, de modo a que seja considerada fidedigna online.

[1] Relatório « The Value of a Trustworthy Brand Reputation » da TrustPilot

DESENHE UMA ESTRATÉGIA DE NOMES DE DOMÍNIO

Escolher e preservar o nome de domínio correto de um site é crucial para causar uma boa primeira impressão. Um domínio é um endereço único utilizado para aceder ao seu site (por exemplo, ovhcloud.com). Mas é muito mais do que um simples endereço web: um nome de domínio faz parte da identidade da sua empresa.

Um nome de domínio forte deve ser curto, fácil de lembrar e relevante para a sua marca.

Aquando da aquisição de um domínio, deve conceber uma estratégia para proteger a sua atividade dos riscos reputacionais. Fraude em domínios, por exemplo, é uma tática comum usada por agentes maliciosos para se fazerem passar por uma marca e levar os utilizadores a divulgarem informações sensíveis. Por exemplo, os cibercriminosos podem tentar registar nomes de domínio semelhantes ao seu e que contenham uma extensão de domínio ligeiramente diferente (por exemplo, .co em vez de .com) ou uma extensão enganosa relacionada com o objetivo do seu site (por exemplo, ovh.cloud em vez de ovhcloud.com).

Para mitigar o risco reputacional resultante da fraude no domínio, deve registar nomes de domínio que irão minimizar essas ameaças. A OVHcloud facilita esta tarefa ao sugerir automaticamente opções do nosso catálogo de mais de 900 extensões amplamente utilizadas no mercado (por exemplo, .com, .net, .org), relevantes para a sua localização (por exemplo, .fr, .eu, .uk) e relacionadas com a sua indústria (por exemplo, .fashion, .health, .tech). Pode até utilizar a OVHcloud para registar erros ortográficos comuns do seu domínio ou nomes que pareçam visualmente semelhantes (por exemplo, um 0 no lugar de um o).

É igualmente essencial que mantenha a propriedade dos seus nomes de domínio o máximo de tempo possível. A perda de um nome de domínio pode levar a danos reputacionais (os clientes ficam confusos quando chegam a um site diferente) ou mesmo a custos exorbitantes para recuperar o nome de volta dos cybersquatters que aproveitam este erro para seu próprio benefício. Por esta razão, a OVHcloud renova automaticamente os nomes de domínio por predefinição, para reduzir o risco de alguém utilizar o seu nome.

Proteja a sua marca graças à segurança dos domínios

Além de uma estratégia sólida de nomes de domínio, existem outras medidas que deve adotar para proteger o seu domínio contra o risco cibernético. Agentes maliciosos podem tentar empregar técnicas como o domain slamming (por exemplo, pedidos de transferência ilegítimos) e o cache poisoning para redirecionar os utilizadores para outro site, que podem ser usados para ataques de phishing, distribuição de spam ou alojamento de conteúdo malicioso. Isto pode prejudicar gravemente a sua reputação e desgastar a confiança dos clientes.

Sugerimos que siga todos estes passos e adote uma abordagem em várias camadas para a segurança do domínio. Desta forma, se uma ciberameaça contornar um tipo de medida de segurança, haverá uma outra camada concebida para parar esse tipo de ataque.

Para se defender destes tipos de ataques de domínio sofisticados, a OVHcloud oferece uma abordagem simples, baseada num " botão " que lhe permite:

▶ 1

Ativar as Extensões De Segurança Do Sistema De Nome De Domínio (DNSSEC) para se proteger contra o cache poisoning, uma tática de cibercrime utilizada para desviar o tráfego para sites nocivos.

▶ 2

Desencadear um mecanismo para prevenir que o seu domínio seja alvo de notificações de renovação falsas e de outros pedidos de transferência fraudulentos.

▶ 3

Adotar mecanismos de segurança para sites e e-mails, como certificados SSL (Secure Sockets Layer) e TLS (Transport Layer Security).

Mantenha a confiança da marca com a continuidade do negócio

Claro que é impossível eliminar o risco digital com 100% de certeza. É por isso que deve ter um plano pronto para o caso de algo (por exemplo, um ataque informático ou um pico de tráfego) ameaçar deitar abaixo o seu site. O tempo de inatividade do site pode frustrar os clientes, prejudicar a receita e causar danos duradouros à reputação.

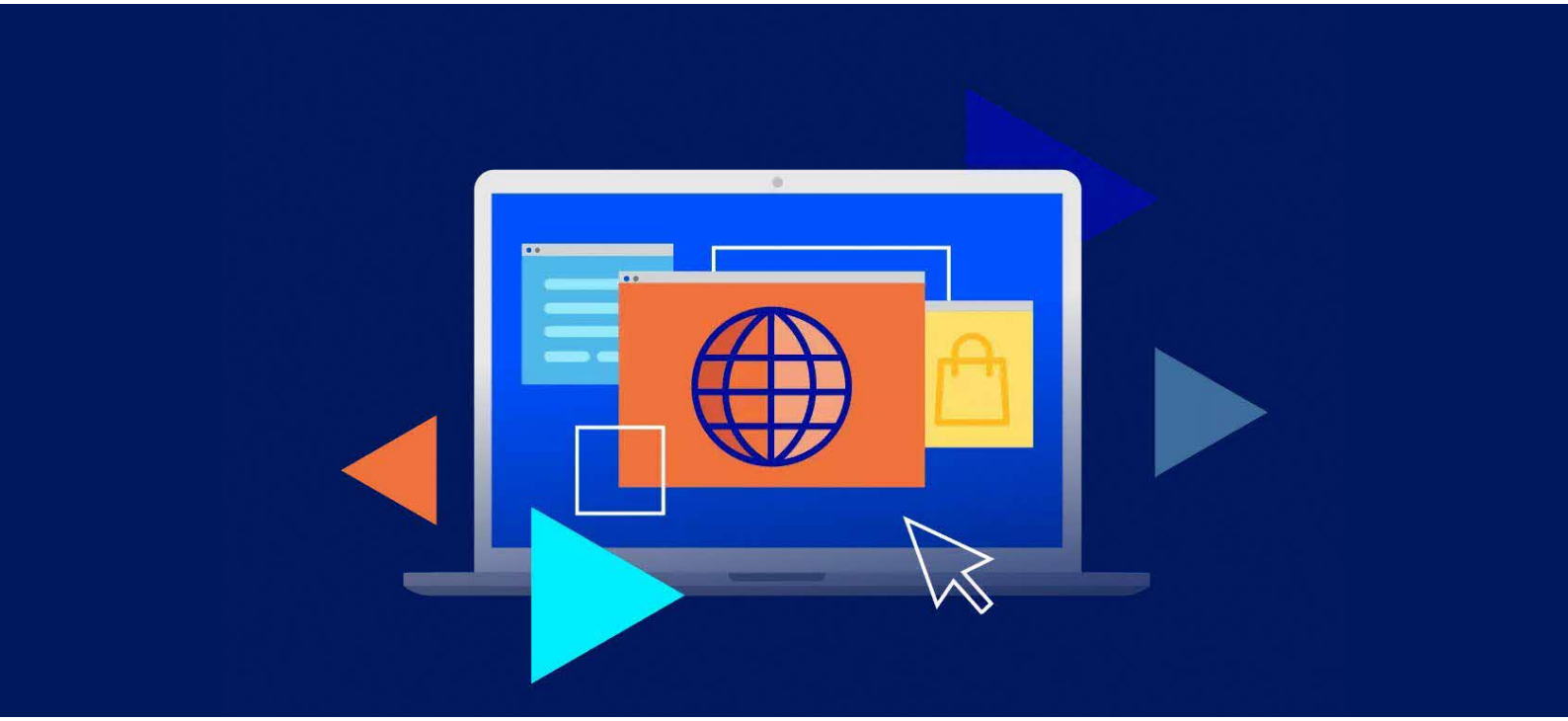
Para as pequenas empresas, o tempo de interrupção pode custar até **427 dólares por minuto**.[2]

Um plano de continuidade digital irá ajudá-lo a manter o seu site a funcionar sem grandes ou nenhumas interrupções em caso de incidente. É parte integrante da sua estratégia de proteção da reputação, que mantém a sua presença online estável. Um plano de continuidade deve incluir etapas tais como:

- Identificar as suas aplicações e dados mais valiosos necessários para a continuidade do negócio.
- Certificar-se de que apenas funcionários qualificados e com conhecimentos informáticos suficientes têm acesso à alteração de serviços críticos que possam pôr o sistema em baixo.
- Efetuar backups regulares de dados e sistemas críticos (como ficheiros, conteúdos, bases de dados, etc.) para permitir um restauro rápido do seu site, caso seja necessário.
- Escolher um fornecedor fiável que lhe permita otimizar o tempo de funcionamento das funções essenciais do seu site e, ao mesmo tempo, disponibilizar opções de recuperação de desastres, se necessário.

Para os clientes de alojamento web, a OVHcloud monitoriza a rede de modo a detetar tentativas de pirataria, como um número anormal de pedidos no servidor, e emite um alerta para que possa tomar medidas imediatas para resolver o problema.

[2] Pingdom, Average Cost of Downtime Per Industry



O alojamento web da OVHcloud também inclui backups automáticos para preservar a integridade dos dados e suportar uma recuperação rápida (por exemplo, se cometer um erro ao gerir o seu site), permitindo minimizar o tempo de interrupção do seu negócio e manter uma reputação positiva. Também sugerimos que os clientes executem uma estratégia de backup " 3, 2, 1 ":

3

Crie **três** cópias dos seus dados (isto é, a original e mais duas cópias de segurança).

2

Armazene-os em **dois** suportes diferentes (por exemplo, num disco num local distante, num armazenamento cloud, etc.).

1

Mantenha **uma** cópia offline numa solução de armazenamento desligada do resto da rede ou num suporte de armazenamento amovível.

Trabalhar com vários fornecedores para adquirir a tecnologia necessária para seguir estas melhores práticas pode ser dispendioso e difícil de gerir. A OVHcloud, por outro lado, é um parceiro web único e rentável que fornece ferramentas que contribuem para manter seguros o seu domínio e a sua reputação .

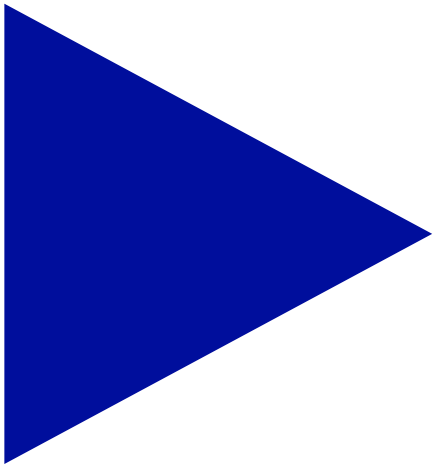
OVHcloud

02

Construir a estabilidade financeira para resistir a mercados imprevisíveis

O DINHEIRO É REI

O dinheiro tornou-se um ativo-chave para qualquer empresa, independentemente da sua dimensão. Mas as PME, em particular, ainda estão a recuperar dos efeitos financeiros devastadores da pandemia, o que significa que têm frequentemente um fluxo de caixa limitado e uma tolerância muito reduzida a custos inesperados.



“Nunca tirem os olhos do fluxo de caixa porque é a alma do negócio.” – Sir Richard Branson

É importante alcançar estabilidade e previsibilidade para a sua situação financeira. No entanto, poderá ficar desanimado quando souber que muitos dos produtos e serviços que está a considerar para aumentar a sua presença online vêm com custos adicionais, custos de renovação e outros custos ocultos. Podem também prender-vos a uma relação a longo prazo.

Por exemplo, algumas soluções de alojamento web parecem inicialmente atraentes porque são intuitivas (devido a uma personalização limitada). No entanto, a médio prazo, estas soluções aparentemente de baixo custo podem tornar-se extremamente dispendiosas, já que terá de começar tudo de novo se mudar para outro fornecedor.

Aqui estão três passos que deve seguir para evitar que o lançamento e manutenção do seu site representem um risco financeiro excessivo.

INCLUA A INFRAESTRUTURA DIGITAL NO SEU PLANEAMENTO FINANCEIRO

A expansão online deverá, em última análise, impulsionar e não prejudicar a rentabilidade da sua empresa. Se está a investir pela primeira vez numa ou várias destas capacidades digitais, é essencial planear com antecedência e colocar as questões certas para controlar os custos, evitar tensões financeiras e apoiar a escalabilidade a longo prazo.

As principais etapas a serem consideradas no planeamento financeiro da sua infraestrutura online incluem:

Avalie as despesas correntes:

Reveja os seus custos digitais (por exemplo, licenças de software, ferramentas de redes sociais, serviços de correio eletrónico, etc.) e confirme que todas as despesas estão a gerar valor em termos de receita, poupança de tempo, equidade de marca ou satisfação do cliente.

Defina um orçamento para serviços adicionais:

Sabendo que o seu site tem naturalmente que cumprir exigências em matéria de alojamento e de segurança, reserve uma parte do seu orçamento mensal/anual para alocar a esses serviços.

Defina as necessidades de alojamento:

Compare os fornecedores de alojamento com base em fatores como preços, funcionalidades, apoio ao cliente e tempo de disponibilidade ideal, dando prioridade àqueles que dispõem de preços transparentes e sem custos surpresa .

Tenha cuidado com o aprisionamento tecnológico:

Algumas empresas tornam muito difícil mudar de fornecedor e de infraestrutura pois exigem o pagamento de valores extremamente elevados. Para evitar isso, faça perguntas como " Oferece reversibilidade total? " e " Como fazem para evitar o aprisionamento tecnológico? "

Tenha em conta a escalabilidade:

Escolha um fornecedor que permita uma escalabilidade vertical (por exemplo, atualizações de alojamento) e horizontal (por exemplo, serviços adicionais) para que o seu alojamento possa evoluir em função das necessidades da sua empresa

A OVHcloud tem como objetivo tornar o seu planeamento financeiro o mais fácil possível, graças à transparência dos preços. Além disso, também oferecemos servidores privados virtuais (VPS) e servidores dedicados, caso precise de ter maior controlo sobre os servidores para criar aplicações web, sites mais complexos e infraestruturas digitais.

ESCOLHA UM FORNECEDOR DE ALOJAMENTO COM TIPOS DE SUBSCRIÇÃO GRANULARES

É importante associar-se a um fornecedor de alojamento web que lhe permita ajustar uma subscrição que inclua apenas as funcionalidades e os benefícios que lhe serão valiosos. Pretende pagar apenas pelos serviços e funcionalidades que irá utilizar, podendo modificar a sua subscrição à medida que as suas necessidades evoluem.

Prefere escolher entre uma pequena e rígida seleção de planos ou uma gama completa de opções de subscrição flexíveis, que possam ser adaptadas às suas necessidades?

A OVHcloud oferece opções de subscrição, o que significa que está a obter o preço ideal para as funcionalidades necessárias ao seu site. O nosso objetivo é proporcionar a relação preço/desempenho ideal para todos os nossos serviços.

Com a OVHcloud, sabe exatamente quais serão os custos todos os meses, o que torna a previsibilidade e previsão financeiras menos stressantes. Sabemos que a política de « o mesmo para todos » não é aquela que procura. É por isso que desenvolvemos planos de preços granulares, para propor o que realmente precisa em cada etapa do seu projeto.

Adquira ferramentas de segurança fáceis de utilizar

A segurança das PME é um aspeto frequentemente negligenciado da estabilidade financeira. Um site sólido tem como objetivo proteger dados sensíveis, manter a confiança dos clientes e mitigar as perdas financeiras que possam resultar de uma fuga ou atividade fraudulenta. Esta é uma ameaça crescente na paisagem digital atual — uma investigação mundial da Mastercard[3] indica que as empresas europeias enfrentam um elevado risco de fraude.

Dois em cada três revendedores online na Alemanha notaram um aumento de fraudes online.[3]

Se gere ou processa informações financeiras, sugerimos o uso de ferramentas e plugins (Ex: PayPal, Stripe, etc.) de confiança e atualizados, que se podem integrar facilmente ao seu sistema de gestão de conteúdos (CMS). Tanto os CMS como as empresas de processamento de pagamentos atualizam frequentemente os seus softwares em função da evolução das ameaças, pelo que é importante atualizar regularmente as suas ferramentas e plugins.

Com a OVHcloud, pode ter a certeza de que protegeremos a sua infraestrutura de alojamento do site para que se possa concentrar na identificação de dados sensíveis ou críticos e no desenvolvimento de um plano para proteger esta informação.

[3] Artigo " Ecommerce Fraud Trends and Statistics Merchants Need To Know in 2023 " da Mastercard

OVHcloud

03

Defenda-se das ciberameaças

Assuma o controlo da segurança

Os cibercriminosos nem sempre escolhem alvos em função do tamanho ou do tipo das empresas. Em vez disso, procuram formas de explorar fáceis, como um CMS obsoleto ou uma política de segurança fraca. Além do roubo de dados, os agentes maliciosos podem aproveitar uma fuga para manipular os seus serviços e marca ou para fazerem-se passar pela sua empresa, de modo a ajudá-los a realizar ataques futuros.

Tomar medidas para atenuar os riscos de segurança é agora um requisito empresarial. Mas muitas organizações não se sentem preparadas para lidar com as ciberameaças atuais. Num inquérito realizado junto das pequenas e médias empresas (PME) de toda a UE[4], 90% afirmou que as questões de cibersegurança teriam um impacto negativo grave no espaço de uma semana após a ocorrência de um incidente.

Mais de metade (57%) das PME acreditam que, muito provavelmente, iriam entrar em falência ou fechar portas após um incidente de cibersegurança[4]

Embora a cibersegurança possa parecer intimidante, existem muitas medidas simples mas impactantes que pode implementar para reduzir significativamente os riscos. Aqui estão três passos que deve seguir para melhorar a postura de segurança e a resiliência da sua empresa.

[4] Relatório sobre a Cibersegurança das PME, da Agência da União Europeia para a Cibersegurança

SIGA AS BOAS PRÁTICAS DE CIBERSEGURANÇA

Os cibercriminosos costumam usar ferramentas automatizadas para analisar milhares ou mesmo milhões de entidades de negócio, de modo a identificar vetores de ataque a explorar. É do interesse deles encontrar algo de que possam tirar rapidamente partido com o mínimo de esforço. De facto, as pesquisas[5] mostram que os vetores mais comuns incluem credenciais roubadas (por exemplo, nome de utilizador e palavras-passe), phishing (por exemplo, o envio de e-mails fraudulentos em seu nome), e exploração de vulnerabilidade (por exemplo, um bug ou falha num sistema).

É essencial que todos, incluindo os seus colaboradores, tomem as precauções adequadas para prevenir o risco de estes ataques prejudicarem a sua empresa. De acordo com um relatório do Fórum Económico Mundial[6,] 95% de todos os problemas de cibersegurança podem ser atribuídos a erros humanos. Felizmente, não é necessário começar do zero para reduzir o risco informático, uma vez que existem boas práticas testadas e comprovadas que podem ser utilizadas para proteger o seu negócio. Por exemplo:

Implementar políticas de palavras-passe seguras: Garanta a utilização de palavras-passe complexas e da autenticação multifatorpara bloquear tentativas de baixo nível de contornar a segurança.

Realizar atualizações regulares e correções: Mantenha atualizados todos os softwares, incluindo sistemas operativos, aplicações e plugins, e corrija vulnerabilidades conhecidas.

Encriptar os seus dados: Utilize protocolos de encriptação para tornar os dados em trânsito seguros e encriptar informações sensíveis armazenadas em servidores e bases de dados.

Instalar firewalls: Implementar firewalls para monitorizar e filtrar o tráfego na rede, ajudando a evitar o acesso não autorizado e a detetar atividades suspeitas.

Efetuar cópias de segurança regulares dos dados: Faça o backup dos dados críticos, confirmando que a informação é armazenada com segurança e pode ser restaurada em caso de ciberincidente.

Compreender as suas obrigações: Reconheça a importância da responsabilidade partilhada e daquilo que se espera que faça (por exemplo, realizar atualizações regulares de software) com as ferramentas que lhe são fornecidas.

[5] Relatório " 2023 Data Breach Investigations " da Verizon

[6] Relatório "Global Risks" de 2022 do Fórum Económico Mundial

Não existe uma solução perfeita e universal para uma segurança total — a única defesa viável é através de camadas.

Na OVHcloud, oferecemos pacotes de soluções de segurança para a sua jornada digital. Por exemplo, todos os nossos serviços de domínio incluem DNSSEC para a segurança gerida do seu nome de domínio e os nossos serviços de alojamento web incluem certificados certificados SSL para a encriptação de dados.

Dê prioridade à segurança em caso de ataque DDoS, uma ciberameaça crescente

Os ataques distribuídos por negação de serviço (DDoS), uma tática maliciosa para obstruir o acesso a um site, estão a tornar-se cada vez mais frequentes. A barreira de entrada aqui é muito baixa — quase todos podem realizar um ataque DDoS com um conjunto barato de ferramentas automatizadas.

Estes ataques são únicos, na medida em que não envolvem normalmente uma violação de segurança ou roubo de dados. O objetivo é simplesmente eliminar o seu site. Os autores podem ser criminosos que tentam pedir um resgate para restaurar os serviços, concorrentes maliciosos que querem manchar a sua reputação, ou simplesmente vândalos digitais que procuram causar problemas.

Os ataques DDoS aumentam 200% ano após ano.[7]

É por isso que deve confirmar que a prevenção DDoS está incluída no seu site, de forma a estar protegido contra esta ameaça comum. Embora isto possa ser difícil de implementar sozinho, a boa notícia é que os serviços de alojamento da OVHcloud incluem mecanismos de segurança, incluindo o anti-DDoS. Por exemplo:

- Deteção contínua de ataques e mitigação rápida de tráfego malicioso.
- Utilização ilimitada, o que significa nenhum custo adicional, independentemente do volume de ataque.
- Sem limite de tempo, com uma proteção que se mantem durante todo o ataque DDoS.

A nossa tecnologia anti-DDoS funciona perfeitamente em segundo plano no seu site. Independentemente do número de vezes que os hackers tentam dominar os seus servidores, a OVHcloud esforçar-se-á por desviar as tentativas para que a sua perceção de qualquer tipo de interrupção seja minimizada.

[7] eBook " The Truth and Trends of DDoS Attacks " do Zayo Group

Melhore a segurança do e-mail

O comprometimento de e-mail empresarial (BEC, siga em inglês) é um tipo de ataque muito comum no qual os criminosos enviam e-mails fraudulentos, muitas vezes imitando os de uma empresa, para roubar informações confidenciais. Se forem bem-sucedidos, estes ataques podem ser difíceis de detetar, uma vez que não são frequentemente assinalados por alertas de segurança. O autor da fraude pode ter acesso a informações e/ou sistemas críticos durante vários meses.

A identificação e contenção de uma fuga de dados resultante de um comprometimento de e-mail profissional demora, em média, **266 dias**.[8]

A OVHcloud oferece uma autenticação robusta, mecanismos antispam, protocolos SPF, DKIM e DMARC automaticamente instalados, que reduzem significativamente o risco de incidentes relacionados com o correio eletrónico. Estes métodos de autenticação protegem a sua empresa contra e-mails indesejados e spam, impedindo a alteração de dados como spoofing de e-mails (ou seja, falsificar um endereço do remetente). Embora muitos fornecedores deixem que os clientes configurem estas funcionalidades sozinhos, nós configuramos estas medidas de segurança para uma eficácia máxima.

Ao escolher a OVHcloud para os seus serviços de e-mail, também pode ficar descansado ao saber que as nossas soluções funcionam em três datacenters diferentes. Isto significa que as suas comunicações continuarão a funcionar sem problemas, mesmo na eventualidade de uma falha ou interrupção do serviço numa localização.

[8] IBM Cost of a Data Breach Report

A sua marca e reputação, a sua posição financeira e a sua postura de segurança estão todas profundamente interligadas, o que significa que não deve ignorar nenhum dos passos acima para não colocar a integridade de todo o negócio em causa.

Felizmente, tomar as medidas necessárias para proteger a sua empresa é menos stressante e mais fácil de gerir do que nunca. Em vez de avaliar e investir em várias soluções pontuais diferentes e dispendiosas, pode optar por estabelecer uma parceria com a OVHcloud, uma solução única e acessível para as suas necessidades digitais.

Saiba mais sobre as nossas soluções de nome de domínio e de alojamento web para descobrir como podemos apoiar o sucesso da sua estratégia digital.