Seus dados estão realmente SEGUROS?

hostnet

Sumário

Introdução

O assunto Segurança de TI é muito falado e pouco executado. As pessoas sempre falam da relevância que a segurança tem e da preocupação que isto gera. Mas a maioria ignora quaisquer políticas de segurança, desde a troca periódica de senhas até a atualização de sistemas, passando por controles de acesso, filtragem e backup.

O objetivo deste ebook é esclarecer, alertar e ajudar.

Esclarecer questões relacionadas à segurança de TI;

Alertar sobre a necessidade de pensar em segurança de TI;

Ajudar a pensar e agir a respeito de segurança de TI.

Então, primeiro vamos falar um pouco sobre segurança, para que seja entendido porque ela é necessária e nunca suficiente.

Por que falar **em segurança?**

Por que falar em segurança?

Vivemos numa sociedade cada vez mais conectada e dependente de tecnologia. Um adolescente, por exemplo, não pode viver sem o seu celular conectado à Internet: escrevendo, lendo, consumindo conteúdo. E não são apenas os adolescentes; uma parte importante das mudanças que a sociedade mundial vem vivendo são devidos aos smartphones.

A Internet, transformou a sociedade mundial de uma forma impressionante em pouco tempo. Na verdade, muito do que já fazíamos antes da Internet, continua sendo feito agora. Mas aumentou e muito a agilidade, o alcance e a participação. Para tornar-se um produtor de conteúdo, é necessário muito menos do que antigamente. A neutralidade da rede (um dos pilares do Marco Civil da Internet) garante que um blog de uma senhora na terceira idade tenha tanta relevância para a rede quanto o portal de uma grande empresa de mídia. Todo mundo tem mais voz, e pode ter certeza: muitos deles querem falar o que acham.

E, por trás de tudo isso, existem programas, sistemas, redes, uma imensa infraestrutura que está longe de ser perfeita. Afinal, problemas acontecem.

O assunto "segurança" é algo muito falado e pouco exercido no dia-a-dia. Muitos deixam que outros se preocupem com o que eles deviam se preocupar, e com isso não sabem o que os contratos escondem ou as garantias que lhe são dadas. Diga, quem nunca ignorou uma licença de uso de um software ao instalar, e simplesmente clicou em Avançar sem realmente ter lido?

A Internet não é um parquinho infantil, mas também não é uma selva de pedra. Ela simplesmente reflete a sociedade onde vivemos, tanto positivamente quanto negativamente. Existem locais onde podemos ir, e locais onde ir torna-se perigoso; existem pessoas com as quais podemos conversar e outras que devemos ter pelo menos cautela na fala; e existem procedimentos que devemos tomar para nos proteger. Ninguém deixa a porta de casa destrancada e aberta, se não souber que realmente pode fazer isso.

Sendo assim, vamos falar sobre segurança.

Alguns números sobre segurança de dados

Existem várias fontes para obter dados a respeito de segurança de TI, e que traz à tona a questão de que não estamos tão protegidos como achávamos que estávamos. Segundo especialistas de segurança, as vulnerabilidades mais comuns são: software mal escrito, problemas com a criptografia, vazamentos de dados, acessos indevidos, validação de dados deficiente, entre outros.

Finalmente, vamos a alguns exemplos do que temos, em termos de segurança:

- **2016 foi o pior ano do phishing, segundo o Anti-Phishing Working Group**, num total de 1.220.523 incidentes, 65% a mais do que em 2015. Phishing é uma forma ilegal de obter informações pessoais a respeito de uma pessoa, como senhas ou cartão de crédito, CPF e número de contas bancárias. Isto é feito enviando e-mails falsos ou direcionando possíveis alvos a sites falsos.

- Apesar de alguns acharem que ligações telefônicas são seguras, **uma falha de segurança permite que sua privacidade seja invadida**, de forma que alguém possa ouvir suas ligações, copiar suas mensagens de texto, obter sua localização, entre outras possibilidades.

- Um banco de dados Oracle foi invadido e **informações (nomes, usuários e senhas) de centenas de funcionários da Petrobras e da empresa de consultoria Accenture foram colocados na Internet.** Por mais que a empresa diga que os dados são de um sistema interno de demandas administrativas em fase de desativação, com nível de proteção menor, ainda é assim uma invasão.

- Vazamentos de dados, causam prejuízos financeiros para empresas em geral, inclusive no Brasil. **Um estudo do Ponemon Institute** demonstra que as empresas perderam, em média, R$ 3,96 milhões com vazamentos de dados.

- Cerca de 38% dos vazamentos foram causados por ataques maliciosos. Aliás, vazamentos de dados são mais comuns do que parecem, visto que **uma falha humana fez com que dados do Cartão Nacional de Saúde fossem vazados na Internet.**

- Depois de roubar informações pessoais ou criar confusão nos computadores, agora temos os ransomwares. Estes são programas maliciosos que cifram (criptografam) toda a informação que há no seu computador e exigem uma quantia em dinheiro para divulgar a senha e permitir o processo inverso. Ou seja, esse software sequestra seus arquivos e exige um resgate. A própria Telefônica **de Espanha foi vítima de um ransomware**, e cerca de 85% dos seus computadores foram afetados.

- Uma triste estatística para o nosso país é saber que empresas brasileiras, como bancos, são **o quarto maior alvo de ataques hackers**, conforme visto numa pesquisa que listou ataques semelhantes em 31 países.

- Até mesmo o WhatsApp, conhecido programa de mensagens instantâneas, foi vítima de golpes. Apesar de implementar criptografia na comunicação entre usuários (o que aumenta em muito a segurança), golpes são infelizmente comuns. Podemos listar **o golpe baseado em futebol que fez mais de 2 milhões de vítimas**. E não foi o primeiro golpe e nem será o último. Antes desse golpe, vários outros foram aplicados, inclusive um, **por ocasião da Páscoa, que fez pouco mais de 300 mil vítimas.**

- Hoje em dia, falamos muito da Internet das Coisas (IoT), onde dispositivos eletrônicos usados no dia-a-dia (como aparelhos eletrodomésticos, eletroportáteis, máquinas industriais, meios de transporte etc.) estão sendo interligados à Internet. E eles já são vítimas de ataques cibernéticos. **Um software malicioso recentemente descoberto é capaz de atacar mais de 1000 diferentes modelos de câmeras IP, e é certo que contaminou mais de 100 mil câmeras ao redor do mundo.**

- Em servidores Web, o problema não é diferente. **Recentemente, uma falha de segurança foi encontrada no servidor Web IIS 6.0, da Microsoft**, e a empresa não deve liberar uma correção para esse software, visto que esse software foi descontinuado. Mas isto não quer dizer que falhas não ocorram em outros servidores Web, linguagens e sistemas. Elas ocorrem, e são listadas em sites como o SecurityFocus.

- Na Internet brasileira, é célebre a história do site encurtador de URLs **migre.me**. O serviço estava hospedado em um provedor brasileiro, que perdeu todos os dados do serviço em seu storage, durante uma migração. O serviço teve um backup antigo restaurado e foi migrado para outro provedor.

Ninguém está livre **de problemas**

Ninguém está livre de problemas

Não se engane: já se foi o romantismo dos primeiros hackers, que entravam em sistemas pelo simples prazer da descoberta. Hoje em dia, ataques contra infraestruturas são desferidos por quadrilhas internacionais, especializadas em roubo de informações e dados; iscas são plantadas por e-mail para pegar os usuários mais incautos e roubar dados sigilosos, e a falta de cautela é amiga do golpe.

É muito comum o sentimento de que isso não acontecerá comigo. Muitas pessoas acham que problemas só acontecerão com os outros, mas nem todos estão imunes. Nada mais longe da verdade. Vários serviços, por mais que tenham equipes de resposta a incidentes e diversas políticas de segurança, ainda assim sofrem indisponibilidades.
Alguns dos sites que sofreram falhas são:

- WhatsApp;
- Skype;
- Facebook;
- Amazon;
- Twitter, Spotify e Reddit.

Um tipo de ataque comum nos dias atuais é o **Ataque Distribuído de Negação de Serviço**, ou **DDoS**. O objetivo é causar lentidão ou indisponibilidade de um serviço na Internet, fazendo uso de dispositivos que estão conectados à rede e que podem ser controlados à distância, a partir da exploração de uma falha de segurança. Este é o que chamamos de um equipamento zumbi, ou bot. Logo, um servidor que foi dimensionado para receber um certo número de requisições por segundo, recebe uma quantidade muito maior e não tem como lidar com isso.

Uma botnet é uma rede de bots, equipamentos como computadores ou dispositivos conectados à Internet (a Internet das Coisas, ou IoT) que são infectados e controlados à distância para cometer atos ilícitos. Um uso comum para uma botnet é gerar um alto número de acessos simultâneos a uma rede ou serviço. Dessa forma, temos uma sobrecarga ao consumir todos os recursos disponíveis no servidor. Note que esta não é uma invasão, mas sim a invalidação de um serviço por sobrecarga. As empresas citadas acima sofreram ataques desse tipo, e tem aumentado muito nos últimos anos.

É comum os provedores de hospedagem sofrerem ataques. Um atacante pode realizar o ataque motivado em retirar determinado conteúdo do ar, ou interessado em prejudicar empresas e usuários. Ele realiza uma investida contra o servidor onde esse conteúdo é disponibilizado, na forma de um site, e pode tornar o serviço indisponível.

Content Distribution Network, ou CDN

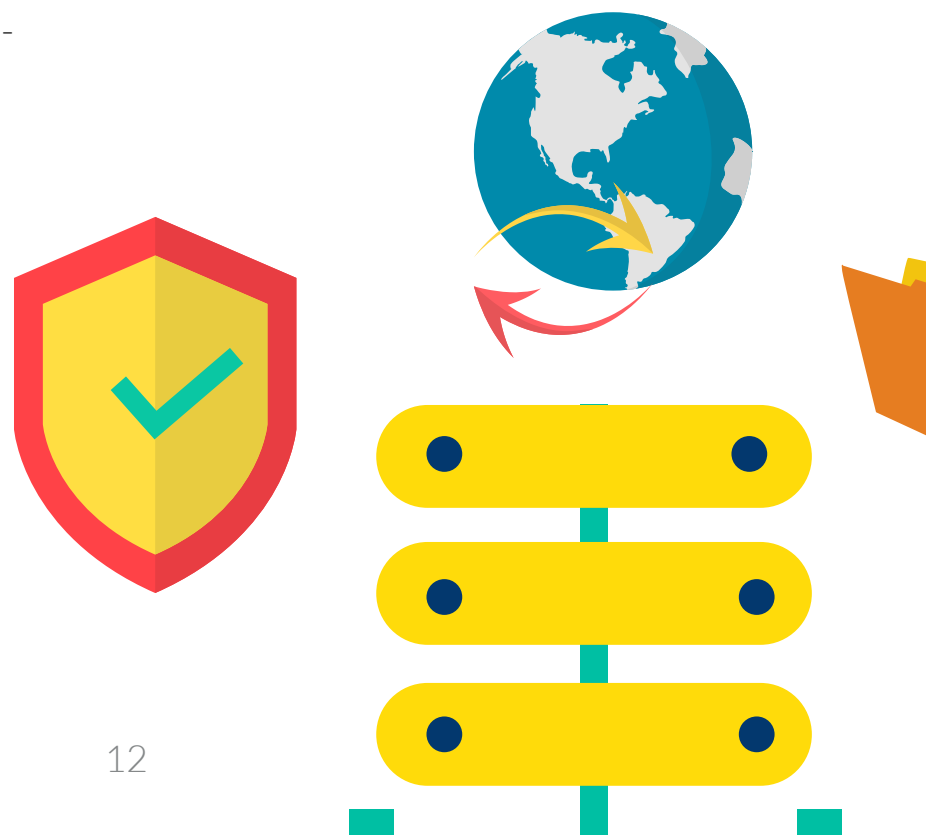
Uma CDN (Content Delivery Network, ou Rede de Entrega de Conteúdo) é uma rede de distribuição de informação, cujo objetivo é entregar conteúdo Web de forma mais rápida a usuários geograficamente dispersos.

Ela é composta por servidores espalhados geograficamente pelo globo terrestre, com o conteúdo a ser acessado sendo replicado e distribuído por todas essas máquinas. O usuário é então conduzido ao servidor que contém aquele conteúdo e tem condições de respondê-lo rapidamente. Ou seja, o servidor mais próximo, com menos nós intermediários (hops).

Dessa forma, é possível diminuir o gasto com largura de banda e otimizar o acesso aos conteúdos. Afinal, o servidor que responderá, será aquele que tiver condições de responder mais rapidamente.

As CDNs trazem mais segurança, pois permitem mitigar ataques do tipo DDoS (Ataque Distribuído de Negação de Serviço). Logo, todos esses acessos são distribuídos pelos servidores aos quais compõem a CDN e contêm cópias do site que está sofrendo ataque.

Em resumo, o ataque é diluído por vários servidores, o que minimiza os efeitos desse tipo de ameaça.



Falhas acontecem, e não só as humanas...

Vale lembrar que **nenhum software é 100% seguro**. Falhas de segurança são fatos consumados e elas podem ser exploradas por criminosos digitais para todo o tipo de ação maliciosa. E todos os softwares podem conter falhas, sejam em grande ou menor quantidade.

Por isso, os responsáveis por trás desses softwares têm sido muito mais cautelosos com falhas de segurança, seguindo listas de vulnerabilidades e mantendo equipes de resposta a incidentes que corrigem e disponibilizam rapidamente correções para esses softwares. A Microsoft, por exemplo, após negligenciar a segurança dos seus softwares por muito tempo, voltou atrás e hoje em dia tem várias iniciativas, como: divulgação de boletins de segurança; liberação de correções para os seus softwares de forma semanal; patrocínio de um *bounty program*, entregando prêmios em dinheiro para quem encontrar falhas de segurança nos seus softwares. Essas são algumas das iniciativas que ela e várias outras empresas promovem.

Por que a atualização é fundamental?

A atualização é fundamental, e iremos explicar o motivo trazendo um exemplo. No mês de maio de 2017 houve um grande ataque hacker, promovido pelo malware[1] WanaCrypt0r 2.0. Este é um ransomware[2] que contém um algoritmo de espalhamento muito agressivo, e que infectou centenas de milhares de máquinas pelo mundo todo, em pouco tempo.

A falha de segurança que esse malware faz uso foi identificada pelo Equation Group, um grupo de hackers que é tido como vinculado à Agência Nacional de Segurança (NSA), dos Estados Unidos. A Microsoft divulgou uma correção para essa falha de segurança no mês de março de 2017, ou seja, dois meses antes do ataque. Todos os usuários que atualizaram o seu sistema operacional (como o Windows 7, 8 ou 10) não estavam vulneráveis a esse ransomware.

Portanto, todas as vítimas desse maciço ataque hacker sofreram por não terem atualizado seus softwares, sejam eles ferramentas de combate a malwares (como antivírus e firewalls) sejam eles sistemas operacionais. Várias das vítimas estavam usando ainda Windows XP nos seus computadores, um sistema operacional que a Microsoft lançou em 2001 e encerrou o suporte em abril de 2014. A Microsoft já aconselhou a todos atualizarem para versões mais novas dos seus sistemas operacionais, mas ainda há muitos usuários que não o fizeram.

Logo, vemos a necessidade de manter os softwares atualizados. Entenda que quando falamos atualizados, não é necessariamente a última versão. Algumas falhas de segurança que ocorrem, são independentes da versão do Windows adotado, por exemplo. Migrar de um Windows 7 para o 10, por exemplo, não quer dizer que você estará livre de falhas.Nota-se que **é fundamental manter seu sistema atualizado**. Falhas de segurança são descobertas o tempo todo, e correções são disponibilizadas pelos produtores do software com razoável periodicidade. Por mais que para o usuário essa rotina seja penosa e repetitiva, este é um hábito que deve ser adquirido, como um meio de prevenção.

1. Malware é a designação padrão para programa malicioso, ou seja, é um software destinado a infiltrar-se em um computador de forma ilícita, com o intuito de causar danos ou roubar informações.

2. O ransomware é um tipo de malware que limita o acesso ao sistema contaminado e cobra um resgate para que o acesso possa ser restabelecido.

O que é criptografia?

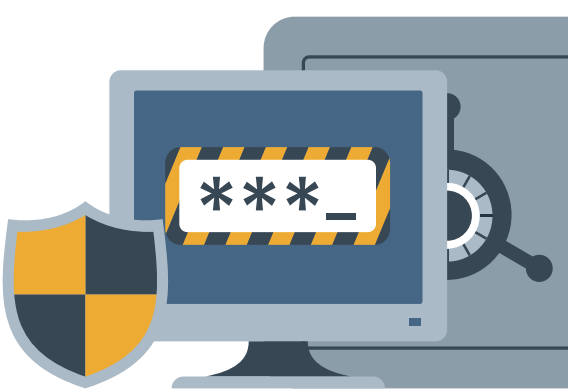
Criptografia é uma área de estudo da Matemática que aborda princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra, que seja ilegível. Logo, o conteúdo original só pode ser lido por quem possuir a "chave secreta", o que a torna difícil de ser lida por alguém não autorizado.

O uso de criptografia não é algo novo, pelo contrário: os primeiros usos conhecidos foram identificados em hieróglifos irregulares encontrados em monumentos do Antigo Império do Egito, ou seja, cerca de 4500 anos atrás. Mas ela tornou-se popular recentemente, saindo dos círculos acadêmicos e diplomáticos (como os códigos diplomáticos de diversos países), e sendo amplamente empregada com o aumento do uso da Internet.

Criptografia é algo tão sério que vários países ainda têm restrições quanto ao uso de algoritmos de cifragem. Até 1996, a exportação de algoritmos de criptografia, a partir dos EUA, usando chaves maiores do que 40 bits (que é uma chave muito insegura) era severamente limitada.

Hoje em dia, vários serviços usam criptografia. Em particular, a criptografia de chave pública (ou assimétrica) é amplamente usada para transações seguras via Internet. Esse tipo de criptografia requer duas chaves:

- A **chave pública** é usada para encriptar a informação ou para verificar uma assinatura digital. Essa chave é pública pois ela pode ser amplamente divulgada, já que ela só “fecha” a informação.
- A **chave privada** é usada para decifrar a informação. Essa chave é usada para “abrir” a informação ou para criar uma assinatura digital, e é privada pois seu uso deve ser restrito apenas a quem interessa acessar os conteúdos cifrados.



Todo o diálogo estabelecido entre cliente e servidor pode ser protegido pelo protocolo SSL (Secure Socket Layer). A informação que sai do cliente é cifrada pela chave pública e decifrada pela chave privada, no servidor. Se observarmos o navegador, em alguns sites veremos um ícone de um cadeado, na barra de endereços. Isto significa que o diálogo é cifrado, entre cliente e servidor. Nada impede que alguém que esteja entre os extremos dessa conexão copie os pacotes de dados. Este é o tipo de ataque que chamamos de ataque do homem no meio. Mas como os pacotes estão cifrados, o atacante terá que "quebrar" a chave para ler o conteúdo. E quanto maior for a chave, muito maior será o tempo necessário para descobrir o seu conteúdo.

Exemplificando: se tivermos uma chave de 128 bits, e um computador hipotético que avalia 1 trilhão de possíveis combinações de chaves por segundo, esta mesma máquina levaria 10.790.283.070.806.014.188,97 anos para investigar todas as possíveis chaves. E hoje em dia usam-se chaves muito maiores, com 256, 512 ou 1024 bits. Ou seja, virtualmente inquebráveis.

E os backups?

O backup é o que conhecemos como cópia de segurança. Consiste basicamente em fazer uma ou mais cópias de dados, de um dispositivo de armazenamento para outro. Dessa forma, caso ocorra perda dos dados originais, seja por apagamentos acidentais ou corrupção de dados, é possível restaurá-los a partir dessa cópia.

Hoje em dia, além dos meios de armazenamento de dados tradicionais (como CD-ROMs, DVDs, discos rígidos internos e externos, fitas magnéticas e outros), é possível também realizar cópias de segurança externamente, fazendo uso de redes ou algum serviço online. Dessa forma, seus dados estão em outro computador, seja em uma rede local, seja externo à sua rede (na "nuvem", como se convencionou falar).

O backup é uma parte fundamental de qualquer política de segurança, e deve ser levada a sério, por mais que seja um

processo penoso e demorado, e que os usuários não têm o menor apreço em realizar. É comum não encontrar backups dos arquivos, ou se existir, serão backups desatualizados.

Infelizmente, existe o pensamento de que problemas sempre acontecerão com os computadores dos outros, não com os seus próprios. Mas discos rígidos podem apresentar defeito, CDs e DVDs podem ter problemas para leitura, e por aí vai. Como diz o ditado, é melhor prevenir do que remediar. É bom enfatizar a necessidade de manter pelo menos uma cópia atualizada dos seus arquivos mais importantes em outra mídia, preferencialmente de forma remota, em outro computador, acessível via Internet.

Tipos de ataque

Além dos ataques distribuídos de negação de serviço (DDoS), que atingem um ou vários servidores, existem ataques que podem contaminar um conjunto de domínios ou apenas um. Vamos ver quais são:

SQL Injection - este é um ataque que consiste na inserção (conhecido como injeção) de uma query para o banco de dados, via aplicação web. Aqui, o invasor consegue através de brechas no site executar queries ou statements arbitrários numa base de dados via "injeção" de comandos em campos de formulários. Para se proteger de ocorrências de SQL Injection, verifique se todo parâmetro passado para o seu site é tratado antes que seja concatenado na query.

Script Injection - é possível explorar scripts que permitem a inserção de parâmetros na URL. Dessa forma, o invasor pode executar um script externo para envio de spam usando seu website, por exemplo. Sugerimos que os scripts afetados filtrem a ocorrência de padrões como: "http://" nos parâmetros da URL, impedindo a chamada de scripts externos.

Mail Form Injection - o invasor insere comandos SMTP nos campos (ou variáveis) que permitem enviar mensagens de spam, a partir de formulários para envio de e-mails. Sugerimos que os scripts filtrem a ocorrência de padrões como "CC:", "Cc:", "cc:", "BCC:", "Bcc:" e "bcc:", impedindo seu uso para envio de spams.

Upload de códigos maliciosos - este é o tipo mais comum de invasão hoje em dia.
O código malicioso na forma de scripts é colocado em formulários de upload sem autenticação de acesso, ou a partir de uma invasão de áreas vulneráveis do site. O recomendável é que o acesso à área de uploads de arquivos seja protegido por senha. Além disso, mantenha os softwares de terceiros (como lojas on-line e CMS) sempre atualizados e com vulnerabilidades corrigidas.

Invasão via FTP - aqui, a senha de acesso é obtida usando programas que estão no computador do cliente, que capturam essa informação, e a enviam-na para terceiros que posteriormente, os usam para publicação de scripts para envio de spam, propagação de vírus ou hospedagem de sites falsos. O recomendável é manter uma solução de segurança atualizada na sua máquina, trocar a senha periodicamente e também evitar acessar o site via FTP em computadores de uso comum, como os disponíveis em lanhouses e
cibercafés.

Como eu posso **me prevenir?**

Como eu posso me prevenir?

Até aqui, tivemos uma visão nada romântica e bem mais realista dos problemas computacionais atuais, e das necessidades que temos em termos de segurança.

Hoje em dia, ataques contra infraestruturas são desferidos por quadrilhas internacionais, especializadas em roubo de informações e dados; iscas são plantadas por e-mail para pegar os usuários mais incautos e roubar dados sigilosos, e a falta de cautela é amiga do golpe. Como se prevenir disso tudo? Como minimizar o risco de que incidentes como esses venham a lhe afetar diretamente? Veremos então algumas práticas que podemos fazer como prevenção. Vale lembrar que:

- Não existe sistema 100% a prova de falhas;
- Toda corrente é tão forte quanto o seu elo mais fraco;
- O fator humano pode comprometer toda a infraestrutura;

Vamos às considerações.

Quanto aos softwares

Evite usar softwares piratas. Prefira usar software original, vindo de fontes confiáveis. Jogos, aplicativos de escritório, sistemas operacionais e editores de imagens estão entre os softwares mais pirateados. Além de ser ilegal e criminoso, programas nessa condição podem ser distribuídos com malwares e não podem realizar atualizações de segurança que são distribuídas para as cópias originais.

Muitas vezes a desculpa usada para a pirataria é o alto custo das licenças de software. Bem, as empresas estão no seu direito de cobrar o valor que bem entendem para a sua propriedade intelectual. Se o valor é alto demais, prefira o software livre - muitas vezes são soluções tão boas quanto os softwares proprietários - ou procure por promoções nas licenças de uso, para minimizar o gasto.
Se você usa programas de compartilhamento (como o Bit Torrent) ou faz download de arquivos de sites especializados, fique atento ao que baixar. Verifique se o arquivo tem alguma característica estranha, como:

- Mais de uma extensão (como fulano.mp3.exe);
- Tamanho muito pequeno para o tipo do arquivo;
- Descrição suspeita.

Muitos malwares se passam por arquivos de vídeo, som, aplicativos ou outros para enganar. Não se esqueça de examinar o arquivo baixado com um antivírus.
Desconfie de ofertas de softwares que oferecem algo impossível, como aumentar drasticamente o desempenho da rede ou melhorar drasticamente a performance, por exemplo.
Esteja atento à instalação dos softwares: durante esse processo, é comum a ferramenta de instalação deixar de maneira já marcada, a ativação conjunta de outros programas, como barras para navegadores ou supostos aplicativos de segurança. Acompanhe as etapas de instalação e rejeite qualquer oferta do tipo.
Hoje em dia é comum encontrar soluções integradas de segurança, que incorporam antivírus, anti-spyware, firewall e outras ferramentas para tornar a sua navegação mais segura. Recomenda-se fortemente que seja empregada uma solução como esta.

Quanto ao uso da Internet

O primeiro e mais importante conselho é lembrar que no momento em que usamos a Internet, estamos trazendo o mundo todo para próximo de nós. Temos acessos a conteúdos de procedência confiável, mas também muito lixo, conteúdo impróprio e riscos diversos, entre os quais já mencionamos aqui. Deve-se ter plena consciência disso.

Ao acessar qualquer serviço online (redes sociais, Internet Banking, comércio eletrônico, etc) que exija um login e senha, ao finalizar o seu uso, clique no botão (ou link) intitulado Logout, Logoff, Sair, Desconectar ou algo do tipo. Fechar a janela ou a aba do navegador não resolve, deve-se finalizar o acesso. Alguém que acesse esse computador depois, pode abrir esse mesmo endereço e ter acesso às suas informações.

Esteja atento a essa situação principalmente em computadores públicos.
Dê preferência a acessar sites via conexão segura, ou seja, sites com HTTPS (o cadeado fechado na barra de endereços aponta isso). Assim é certo de que toda informação que será trocada entre seu navegador e o servidor, será cifrada.

E-mails

O phishing é uma prática muito comum, e apesar da diminuição do uso de e-mails, continua em alta: Se você recebeu um e-mail declarando, por exemplo, que você tem dívidas; que um documento seu está ilegal; que você ganhou um prêmio; que há provas de que você foi traído; que você precisa atualizar seus dados bancários; que você está sendo intimado judicialmente a comparecer perante um juiz, ou outros. Atenção, tudo isso tem uma grande chance de ser golpe, com o objetivo de obter informações sigilosas a seu respeito, como números de documentos, senhas, logins e números de cartões de crédito. Ignore esses e-mails, e cadastre-os no serviço anti-spam do seu provedor de e-mail. Assim, estes e-mails não chegarão à sua caixa postal novamente.

Comércio eletrônico e Internet Banking

Comércio eletrônico e Internet Banking lidam diretamente com dinheiro. Logo, devemos ser cautelosos. Vamos a algumas lembranças:

- Se for usar o comércio eletrônico, faça-o em sites com boa reputação. Caso haja interesse em algum produto vendido em um site desconhecido, pesquise o site para saber se há reclamações a respeito dele. A reputação dos sites pode ser averiguada a partir de pesquisa em sites ligados ao direito do consumidor (como Reclame Aqui e outros).

- Ao acessar algum seviço privado pela Internet, tenha cuidado. Evite fazê-lo em computadores públicos ou redes Wi-Fi públicas. Verifique sempre se o endereço do site pertence mesmo ao serviço e siga todas as normas de segurança recomendadas. Existem programas que capturam os toques digitados no teclado ou fazem cópia das imagens que estão na tela. Depois, eles remetem essa informação para outras pessoas, que tirarão proveito disso. Muito cuidado!

Redes sociais

O ponto mais importante nas redes sociais é basicamente: seja desconfiado. Existem muitos golpes que tiram proveito da ingenuidade do usuário, e da sua falta de prudência. Cautela é algo que não podemos abrir mão. Vamos então a alguns conselhos:

- Em redes sociais ou em qualquer serviço onde informações pessoais estão expostas, evite dar detalhes, como onde é a sua residência, seu local de trabalho ou de estudo.
- Evite também disponibilizar informações que tragam detalhes relevantes, como a placa do seu carro ou a fachada da sua casa, principalmente via fotos.
- Se você receber ameaças, provocações, intimidações ou qualquer coisa via Internet, evite o confronto. Além de evitar aborrecimentos, isto impede também que o autor da afronta obtenha informações importantes a seu respeito que são reveladas no calor do momento. Podemos falar demais quando estamos irritados.
- Se você perceber que a ameaça é séria ou se você se sentir ofendido, mantenha uma cópia de tudo e procure orientação das autoridades legais.
- Em redes sociais, é possível que um contato te recomende um link sem saber que o conteúdo é malicioso ou um aplicativo duvidoso pode fazer uma postagem sem que a pessoa tenha percebido.

Mensageiros instantâneos

Alguns malwares podem, mesmo que por algum tempo, se aproveitarem do acesso do usuário a um serviço de mensagens instantâneas para enviar mensagens automáticas com links para vírus ou sites maliciosos. Logo, quem recebe, pensa que o emissor realmente enviou aquela mensagem e acaba clicando no link enviado. Se receber um link inesperado, peça confirmação ao emissor do porquê daquele link. Se ele negar, não clique no link e avise-o da possível contaminação do seu equipamento.

Sites

A métrica da desconfiança vale aqui também. Se o site:

- Tem uma temática muito apelativa, explorando conteúdo erótico, hacker ou de jogos de aposta (entre outros);
- Abre automaticamente várias páginas ou janelas com banners;
- O endereço (que também chamamos por URL), é complexo ou o nome do site é diferente da mesma;
- Exibe anúncios com oferta de prêmios, vantagens ou produtos gratuitos;
- Exige download de um programa para continuar o uso;
- Exige cadastro (inclusive pedindo número de celular ou de cartão de crédito) para continuar com determinada ação.

Ao se deparar com sites com essas ou outras características suspeitas, não continue a navegação.

Cadastros on-line

Existem sites que exigem que seja feito um cadastro para poder ter acesso aos seus serviços, e nesse cadastro, ele pede o número do seu celular, ou o número do seu cartão de crédito. É certo que há algo muito estranho aí. Afinal, para que ele quer saber do número do seu cartão de crédito ou do seu telefone, se você não irá adquirir nada?

Além disso, seus dados que foram inseridos neste site podem ser revendidos a empresas que enviam propaganda não autorizada, como por correspondência (mala direta), telefone (telemarketing) e e-mail (spam).

Por isso, se há desconfiança da lisura das pessoas por trás daquele site, pesquise antes, para verificar se há registro de alguma atividade ilegal. Avalie também se há necessidade de usar os serviços oferecidos ali.

Quanto às falhas, sejam humanas e/ou dos sistemas.

O ser humano comete falhas, isto é um fato. Um espaço em branco mal colocado em um comando a ser executado pode gerar um grande estrago, se esse comando for executado por um usuário com privilégios administrativos.

Senhas

- Evite usar senhas óbvias. Por mais que seja tentador usar senhas como nome de parentes, data de aniversário ou placa do carro, pela facilidade de decorar, evite. Prefira sequências que misturam letras, números e caracteres especiais;
- Use senhas com mais de seis caracteres. Quanto maior a senha, mais difícil dela ser quebrada;
- Não anote as senhas em documentos no computador ou em outro aplicativo que não tenha uma senha mestra para bloquear o acesso. Existem serviços, como o LastPass, que salvam todos os seus logins e senhas em um servidor central, e impedem o seu acesso, a não ser que você use uma senha mestra. Existem também aplicativos (tanto para desktops quanto para smartphones) que permitem guardar informações pessoais, que são acessíveis apenas com o uso de uma senha mestra. Agora, se for necessário anotar uma senha em papel (em casos extremos), destrua-o assim que decorá-la;
- Evite usar a mesma senha em vários serviços. Isso aumenta a vulnerabilidade da mesma;
- Uma boa dica é acrescentar um ponto (.) no final da senha. Isso aumenta a complexidade e a dificuldade da senha ser quebrada;
- Mude a senha de tempos em tempos. Um intervalo de três meses é razoável: Se alguém conseguir descobrir a senha do seu e-mail, por exemplo, poderá acessar as suas mensagens sem que você saiba, apenas para espioná-lo. Ao alterar sua senha, não será possível acessar as suas informações novamente;

Quanto às atualizações do sistema.

O sistema operacional mais seguro do mundo, na atualidade, é o OpenBSD. O projeto existe desde 1995, e até maio de 2017 foram encontradas apenas duas falhas de segurança (em 2002 e 2007) que permitiam um eventual invasor obter privilégios de administrador.
Outros sistemas que não são tão seguros (e também não tão complexos) podem ser usados, mas para isso, é preciso saber usar. Vejamos então alguns passos para lidar com essa situação:

- Mantenha seu sistema atualizado. As comunidades de software livre (como o Linux, e o próprio OpenBSD) divulgam correções para falhas de segurança rapidamente. Como o código é aberto, qualquer pessoa pode encontrar a falha e corrigi-la, submetendo a correção a quem é de direito. A Microsoft, com seu sistema operacional Windows, libera correções periodicamente. Logo, acostume-se a atualizar o seu sistema. A preocupação deve estender-se aos seus dispositivos móveis também, como tablets e smartphones. Falhas de segurança podem ser exploradas nos celulares, e dados pessoais podem ser roubados.
- Mesmo assim, há vezes em que o software chega ao fim da sua vida útil. A Microsoft, por exemplo, encerrou o suporte ao Windows XP depois de 13 longos anos. Algumas distribuições Linux tem suporte por 18 meses, a princípio. Mas existem versões, como a Ubuntu LTS, cujo suporte é por até cinco anos, podendo se estender por sete anos para as versões do sistema para servidores. No caso do CentOS, esse suporte pode chegar a uma década. Mas todo suporte acaba um dia. Logo, é necessário verificar se a versão do software que você está usando ainda é suportada, e isto não é só para o sistema operacional, mas vale também para todos os softwares que você usa. Migre sempre para uma versão mais nova, por questões de segurança.
- Muitos sites contêm scripts capazes de explorar falhas do navegador que o cliente está usando. Por isso é importante manter também o seu navegador atualizado. Existem outros sites que não possuem scripts, mas tentam convencer quem o acessa a clicar em um

link perigoso, fazer cadastro em um serviço suspeito e assim por diante. É relativamente fácil identificar esses sites.

- Mantenha seus softwares de proteção, como antivírus, firewall, anti-spyware, etc, atualizados. Não adianta nada combater uma infecção por vírus se o seu antivirus não tem as informações a respeito dos últimos vírus e malwares que tem atacado os sistemas.

Quanto ao uso de criptografia.

Use criptografia sempre que, ao enviar um e-mail, você quiser assegurar que somente o destinatário possa lê-lo.
Existem serviços como o DMARC (Domain-based Message Authentication, Reporting & Conformance), que servem para validar e-mails e também detectar e prevenir contra e-mails falsos. O DMARC reside sobre três mecanismos: o DNSSEC (Domain Name System Security Extensions), o SPF (Sender Policy Framework) e o DKIM (DomainKeys Identified Mail). Verifique se o seu provedor de e-mail faz uso de serviços como esses.
Use assinaturas digitais sempre que, ao enviar uma mensagem, você quiser garantir ao destinatário que foi você quem a enviou e que o conteúdo não foi alterado.

Quanto aos backups

Em termos de backups, é tudo uma questão de paranoia: Cabe a você definir o quão importantes os dados são, para estabelecer uma política de backups. E a importância é fundamental, só quem já perdeu arquivos por não ter uma cópia atualizada sabe como ele é importante. Então, vamos a alguns conselhos sobre backup.

Antes de tudo, é bom lembrar que o processo de realização de backups é lento e chato. Logo, é comum as pessoas não realizarem backups, e alegarem esses argumentos. Deve-se criar o hábito de realizar backups de tempos em tempos, por mais que a vontade seja não fazer. Faça backup periodicamente. A periodicidade adotada varia de acordo com a sua necessidade: há pessoas que fazem backup diário. Outras, semanalmente, outras mensalmente e ainda há quem faça semestralmente ou

anualmente. Depende do seu ritmo de trabalho.

O backup deve ser feito para um meio de armazenamento externo ao seu computador. Não adianta realizar o backup para o mesmo disco rígido onde seus dados estão, se esse HD der defeito, tanto o backup quanto os arquivos serão perdidos. Faça o backup para outro computador, para um HD externo, para um pendrive ou em mídia ótica (CD-ROM, DVD ou Blu-Ray).

Hoje em dia, existem serviços de hospedagem de arquivos no que convencionou chamar de "nuvem". Eles são uma boa opção para armazenamento de documentos, visto que estão acessíveis a partir de um link de Internet e são externos ao seu computador. Caso aconteça o pior e tanto o conteúdo do seu computador quanto do meio de armazenamento externo ao seu computador seja perdido, os dados armazenados na "nuvem" podem ser acessados, a fim de restaurar o que foi perdido.

Caso os dados sejam realmente importantes, cogite fazer mais de um backup, em mais de um meio de armazenamento de massa. Como dizem os antigos, seguro morreu de velho e o desconfiado ainda está vivo. Mas cuidado com a inconsistência das cópias: sempre que atualizar um backup, atualize todas as suas cópias.

Exemplificando: Suponha que você faça backup para dois meios, um pendrive e na "nuvem". E você tem o arquivo A. Feito o primeiro backup, os três meios (o HD do seu computador, o pendrive e a "nuvem") contém o arquivo A. Você continuou a trabalhar, e o arquivo A tornou-se o B. Você atualizou o backup, mas por esquecimento, só o fez no pendrive. Logo, você terá o arquivo B no HD do seu computador e no pendrive, e o arquivo A (a versão antiga de B) na "nuvem". Caso você perca o conteúdo do HD e do pendrive (uma possibilidade remota, mas existe), você terá uma versão antiga do arquivo, apenas.

Enfim, manter uma política de backup, mesmo que apenas do seu computador local, requer algo fundamental: disciplina. E como sempre dizem, prevenir é melhor do que remediar. Que assim seja.

Banco de dados

Os bancos de dados também podem sofrer com falhas de segurança e ataques do tipo SQL Injection[3]. Mas muitos dos problemas são causados pela má administração da base de dados, e veremos então alguns modos de minimizar problemas.
Vale lembrar que informações úteis podem ser usadas a favor e contra você ou sua empresa, o que pode acarretar prejuízos para clientes, usuários e/ou empresas. A informação tem que estar **disponível** (para todos aqueles que necessitam acessá-la), tem que ser **confidencial** (acessível a apenas quem deve ter acesso a elas) e **íntegra** (somente pode ser alterada por pessoas autorizadas).

Autenticação

O acesso ao banco de dados se dá fazendo uso de um usuário (login) e senha. Este é o processo que é conhecido por autenticação, e caso não seja configurado corretamente, poderá ser facilmente acessado por um atacante. Existem algumas maneiras de prevenir, e aqui temos algumas sugestões:

- Usar senhas com no mínimo 8 caracteres, incluindo números e caracteres especiais;
- Não use a mesma senha em mais de um servidor de banco de dados;
- Defina uma senha para a conta de administrador do banco de dados, e não use essa conta para as aplicações que acessam o banco;
- Crie usuários e senhas específicos para cada aplicação ou tarefa.

3. O SQL Injection é um tipo de falha de segurança que se aproveita de brechas em sistemas que acessam bases de dados via SQL. Ela ocorre quando o atacante consegue inserir uma série de instruções SQL dentro de uma consulta, através de manipulação das entradas de dados de uma aplicação.

Controle de acesso

A limitação do acesso é importante para controlar qual usuário acessa cada banco de dados. Isso pode ser feito criando um usuário e senha específico para determinadas tarefas, mas não basta.

O administrador do banco de dados deve determinar qual será o acesso de cada um dos usuários. Os privilégios devem ser diferentes para cada usuário e restrições deverão ser colocadas conforme a sensibilidade que o dado tem.
Por exemplo, suponhamos que exista uma aplicação que somente faça consultas a um banco de dados. O usuário criado para acessar o banco não precisa ter permissão para fazer modificações nos dados, mas apenas ser capaz de lê-los. Enquanto isso, podemos ter outro usuário que possa realizar modificações na base de dados. Esse sim deverá ter mais permissões do que o usuário anterior. E ainda deverá ter permissão de leitura, escrita e edição, mas apenas nas tabelas que ele pode acessar, e não em toda a base de dados.

Criptografia

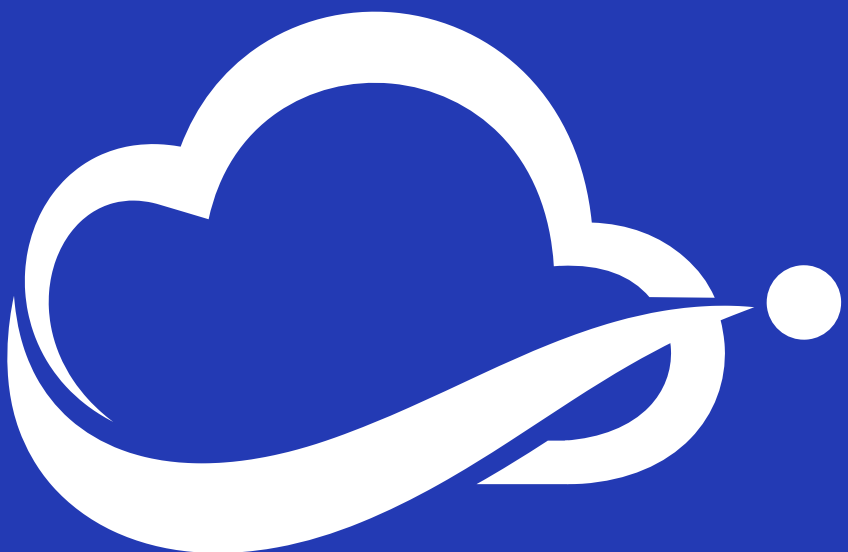
A criptografia dos dados armazenados em um banco de dados é uma parte importante para a segurança, pois teremos dados que estão armazenados e dados que estarão em trânsito, entre o servidor de banco de dados e a aplicação, que não está necessariamente no mesmo computador, fisicamente falando.

Dados em trânsito

Esses dados em trânsito, quando transmitidos sem nenhum tipo de criptografia, podem ser capturados por alguém que esteja localizado entre o remetente e o destinatário. Como a informação não está cifrada, esses dados confidenciais ficam facilmente expostos. Este tipo de ataque é conhecido como ataque do homem no meio.

Dados armazenados

Os dados armazenados também devem ter uma camada de criptografia. Vamos a um exemplo: suponhamos que há uma aplicação Web, que fornece login e senha para seus usuários. Essas senhas deverão ser armazenadas de forma criptografada (apesar de que algumas aplicações salvem esse tipo de informação sensível em texto plano). Um site de comércio eletrônico, por exemplo, ao armazenar as informações de compras de seus clientes, incluindo dados de cartões de crédito e informações confidenciais, devem ter a atenção redobrada para evitar que essas informações vazem para eventuais atacantes.



O que a Hostnet **oferece?**

Respostas às falhas

A Hostnet está atenta a problemas como falhas de segurança e sites contaminados, para minimizar danos e evitar que se alastre.

Caso ocorra algo irregular no site, o departamento de infraestrutura da empresa notifica o cliente através do HelpDesk, informando os arquivos que foram identificados como maliciosos e solicitando um retorno do mesmo para que seja identificada a natureza dos arquivos encontrados.
A Hostnet faz tudo para evitar que o site contaminado seja congelado. Sabemos da importância do serviço de hospedagem contratado conosco, e o nosso desejo é evitar ao máximo danos aos visitantes do site. Mas também não podemos comprometer a estabilidade do servidor no qual o domínio está instalado. Logo, o primeiro procedimento é a remoção dos arquivos infectados, e em seguida a notificação do proprietário do site. Mas caso ocorra novamente ou o responsável não nos contacte após 48 horas, a conta é congelada e o cliente recebe uma notificação a partir do HelpDesk.
A Hostnet quer garantir sempre que o serviço de hospedagem esteja sendo feito da melhor maneira possível, e retirar do ar os sites hospedados é uma solução extrema e em último caso. Por isso, oferecemos ajuda e orientações para que o site possa ser corrigido e o problema seja solucionado.
Assim, evita-se que os problemas aumentem, a ponto do site ser punido pelo Google, ou até o bloqueio dos endereços IP da Hostnet. Vale lembrar que um único site contaminado, se não tratado imediatamente, pode causar o bloqueio de toda a faixa de endereços IP usada pela Hostnet, e com isso, todos os domínios hospedados serem também bloqueados, mesmo os que não foram contaminados.
Um site que foi marcado como contaminado também não poderá ser localizado a partir de um sistema de buscas (como o Google), e com isso seu acesso torna-se restrito. A imagem do site sairá arranhada.
A contaminação de sites só interessa a indivíduos maliciosos que desejam manipular sites de terceiros e usá-los para aplicar golpes, além de uma infinidade de outras naturezas mal intencionadas que certamente não condizem com o interesse do dono do site.
Por isso é que a Hostnet age imediatamente para identificar e corrigir falhas: para zelar pela integridade dos servidores, para orientar o responsável pelo site e proteger os usuários que acessam esse

site.
Como parte desse processo, entre outras soluções, a Hostnet usa o antivírus ClamAV, constantemente atualizado nos seus servidores Web e servidores de arquivos. No caso dos e-mails, a Hostnet usa o antivírus AMaViS (A Mail Virus Scanner). Ele é constantemente atualizado, com o objetivo de proteger as caixas postais.

Domínio Protegido

O que é o Whois?

Quando você registra um domínio (por exemplo, www.comocriarmeusite.com.br), esse registro é feito, e essa informação é adicionada a um arquivo público de dados conhecido como Whois. Nesse arquivo público estão as principais informações dos proprietários de domínios: nome, endereço de e-mail, telefone e endereço físico. Essas informações são divulgadas publicamente pelos órgãos que regulamentam o registro de domínios no mundo.
No Brasil, o órgão responsável pelo registro de domínios é o Comitê Gestor da Internet (http://cgi.br) que permite o acesso livre e irrestrito à base do Whois a partir de uma URL específica, localizada dentro do serviço Registro.BR.
Em outros países, existem diversos órgãos, pois o sistema é terceirizado. Porém, todos os registros realizados são centralizados em uma entidade sem fins lucrativos, vinculada ao governo dos EUA chamada ICANN (Corporação da Internet para Atribuição de Nomes e Números).

E como meu endereço de e-mail foi parar em listas de spam e Phishing?

Usuários mal intencionados executam scripts que varrem a Internet, atrás de endereços de e-mail válidos e que estejam disponíveis publicamente em páginas de sites. Uma das principais fontes de busca para esses scripts é a base unificada de dados do Whois.

Tem alguma maneira de evitar isso?

A Hostnet oferece o serviço Domínio Protegido. Ele existe para aumentar a privacidade dos seus dados que estão online. Em alguns casos, os dados pessoais dos usuários podem ser ocultados. O serviço oculta os dados pessoais dos clientes, que são substituídos por dados da própria Hostnet.

Logo, quando alguém, ou algum script fizer uma pesquisa no Whois, encontrarão dados genéricos fornecidos pela Hostnet, ao invés de encontrar os dados pessoais, comumente vistos.

Benefícios do serviço Domínio Protegido

- Identidade Protegida: Os dados pessoais do proprietário do domínio estão ocultos, o que lhe traz privacidade;
- Segurança Anti-fraude: Como os dados estão ocultos, a ação de usuários mal-intencionados é dificultada, no que tange às fraudes relacionadas a titularidade de domínios;
- Privacidade Anti-spam: esconder dados como número de telefone e endereço físico podem evitar que você receba contatos indesejados de empresas prospectando serviços sem a devida autorização;
- Endereço de E-mail Protegido: manter seu endereço de e-mail privado te protege dos robôs que varrem a internet buscando e-mails para práticas maliciosas.

Como contratar?

O serviço Domínio Protegido está disponível a todos os clientes que tem domínios internacionais, registrados junto à eNom, por um custo de R$ 19,90 por ano.

Link: hostnet.com/whois-protect

CDN

A Hostnet tem uma parceria comercial com a Cloudflare, uma empresa que fornece comercialmente serviços de CDN para diversas empresas e é uma referência mundial. Isto permite aumentar o desempenho e a segurança de nossos clientes. A Hostnet é a primeira empresa no Brasil a disponibilizar esse serviço para seus clientes de hospedagem compartilhada e privativa de todos os tamanhos.
A Hostnet oferece a todos os clientes o plano CloudFlare FREE, de forma gratuita. Logo, todos os clientes já estão usando-o por padrão. Mas caso seja do interesse do cliente contratar um plano CloudFlare com mais recursos, são oferecidos mais três planos, com valores mensais e recursos diferenciados. São eles:

- CloudFlare MOBILE, ao custo de R$ 9,90 por mês.
- CloudFlare PLUS, ao custo de R$ 29,90 por mês.
- CloudFlare FIREWALL, ao custo de R$ 59,90 por mês.

Além do plano básico que todos os clientes Hostnet desfrutam, os planos pagos agregam serviços como: otimização de imagens, o protocolo SPDY (desenvolvido principalmente pelo Google para aumentar o desempenho do transporte de dados pela internet), suporte a SSL e firewall com painel de controle via Web.

Maiores informações podem ser encontradas na Central de Ajuda da Hostnet [31] [32].

31. https://www.hostnet.com.br/info/CDN/

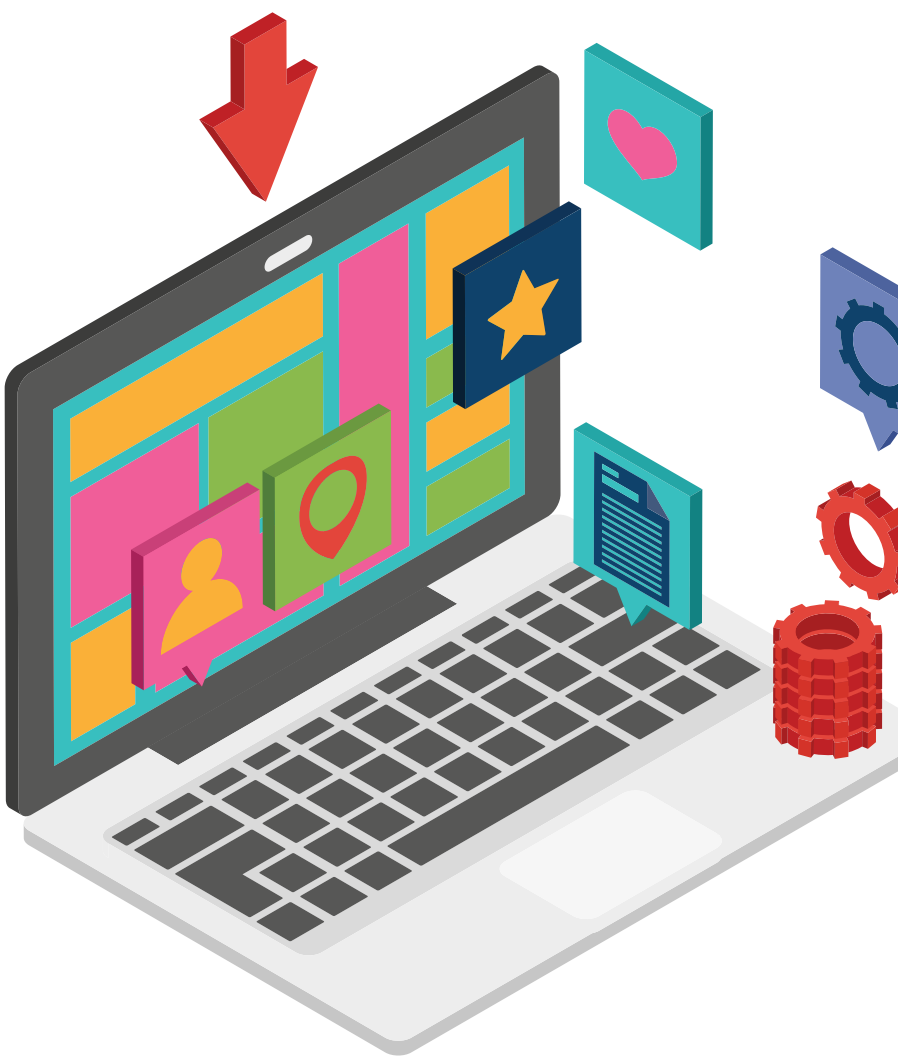
32. https:/www.hostnet.com.br/info

Atualização

A Hostnet usa como sistema operacional para os seus servidores o Ubuntu Linux, na versão LTS. Esta versão, de suporte estendido (Long Term Support), tem atualizações disponíveis por até sete anos após o seu lançamento, o que garante que o sistema está em constante evolução.

Quanto aos serviços fornecidos aos clientes, a Hostnet periodicamente promove atualizações por sua própria conta. É fato que o Wordpress, o Drupal ou o LimeSurvey instalados na conta dos clientes sejam atualizados de tempos em tempos. Versões mais novas podem trazer correções para falhas de segurança, melhorias no desempenho e novas funções adicionadas.

Quanto aos plug-ins dos serviços: recomenda-se aos usuários que usem extensões que sejam de fontes conhecidas e idôneas, para evitar sustos como falhas de segurança sendo usadas por atacantes.



Backup

A Hostnet realiza backup diário dos sites que estão hospedados. Além do backup que cada usuário deverá realizar, o backup da Hostnet torna-se uma opção caso o seu falhe.

Caso você necessite restaurar o backup a partir do que a Hostnet fez, você pode solicitá-lo através do Painel de Controle. A empresa guarda sete dias de backup incremental dos sites, e o mesmo é realizado durante o período da madrugada. Logo, se você teve um problema no seu site no dia 10, e quiser restaurar o backup feito no dia 4, pode ser feito.

Backup do site

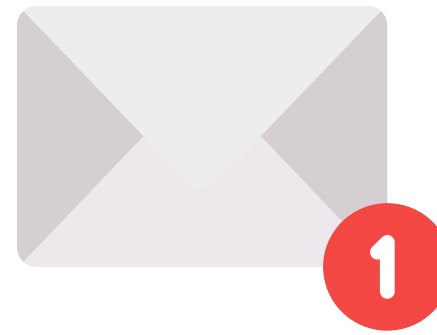
A solicitação de restauração do backup do site pode ser feita pelo Painel de Controle, a partir de Site - Backup. O cliente paga R$ 20 (a ser cobrado na próxima fatura) e o processo pode levar até oito horas para ser concluído.

Backup do banco de dados

A solicitação de restauração do backup do banco de dados pode ser feita pelo Painel de Controle, a partir de Bancos de dados - bancos MySql. O cliente paga R$ 20 (a ser cobrado na próxima fatura) e o processo pode levar até 24 horas para ser concluído – a conclusão do processo será notificada via HelpDesk.

Backup do e-mail

A solicitação de restauração do backup do e-mail pode ser feita pelo Painel de Controle, a partir de E-mail – Contas de e-mails. O custo é gratuito, e o processo pode levar até oito horas para ser concluído.



O que a Hostnet recomenda?

Conforme visto, a Hostnet adota todos os cuidados e precauções para que seus sistemas e servidores não estejam vulneráveis, e que isto afete a sua prestação de serviços de hospedagem de sites.

Entretanto, é possível que algumas vulnerabilidades, alheias aos servidores da empresa, possam ser exploradas. Por exemplo, se ocorrerem falhas na programação dos sites e sistemas hospedados ou algum script que faça uso de falhas como PHP e SQL Injection, ou ainda arquivos malicios-sos instalados no computador que realiza a manutenção do site.
Devido a essa possibilidade, fazemos algumas recomendações para todos que contrataram serviços de hospedagem conosco.

Quanto ao uso do FTP

- Troque sua senha de acesso ao serviço FTP periodicamente.
- Dê preferência à conexão usando um protocolo seguro. O serviço FTP é inseguro para os padrões atuais, use um cliente FTP (como o Filezilla) que suporte SFTP. Conecte usando o protocolo SFTP, e faça uso da porta de conexão 22 (o FTP usa as portas 20 e 21).
- Se você não tem interesse em ter acesso FTP à sua hospedagem, desabilite-a. No Painel de Controle, acesse Conta - Senhas - FTP e realize o bloqueio de acesso ao FTP do seu domínio.
- Evite usar permissões do tipo 777 (leitura, gravação e execução para o proprietário, grupo ao qual ele pertence e todos os outros) em seus arquivos e pastas. Esta permissão deve ser evitada ao máximo, use-a nas pastas onde isso é realmente necessário.

Quanto às atualizações e software

- Mantenha seu sistema sempre atualizado. É bem comum que falhas de segurança encontradas em versões mais antigas dos softwares usados, sejam corrigidas nas versões mais recentes.
- Mantenha um antivírus ativado em seu computador pessoal.
- Use um firewall em seu computador pessoal. Dessa forma, você evitará que uma falha de segurança seja explorada, ou que um programa malicioso se propague, contaminando outros.

Quanto às senhas e o acesso ao site

- Evite usar senhas fáceis, como datas de nascimento ou sequências conhecidas. Alguns exemplos de senhas fracas e ruins são: 123456, qwerty, 123123, entre outros. Ao definir uma senha, o próprio Painel de Controle irá informar se a senha é segura ou não.
- No sistema, tenha cuidado com a parte que permite que seja feito o upload para ele. Várias invasões ocorrem por falhas de segurança, e muitas vezes com o envio de scripts maliciosos.
- Procure restringir o upload de arquivos, para formatos conhecidos, como por exemplo JPG e PNG etc.

Meu site foi contaminado! E agora?

Caso isso ocorra, o que você deve fazer:

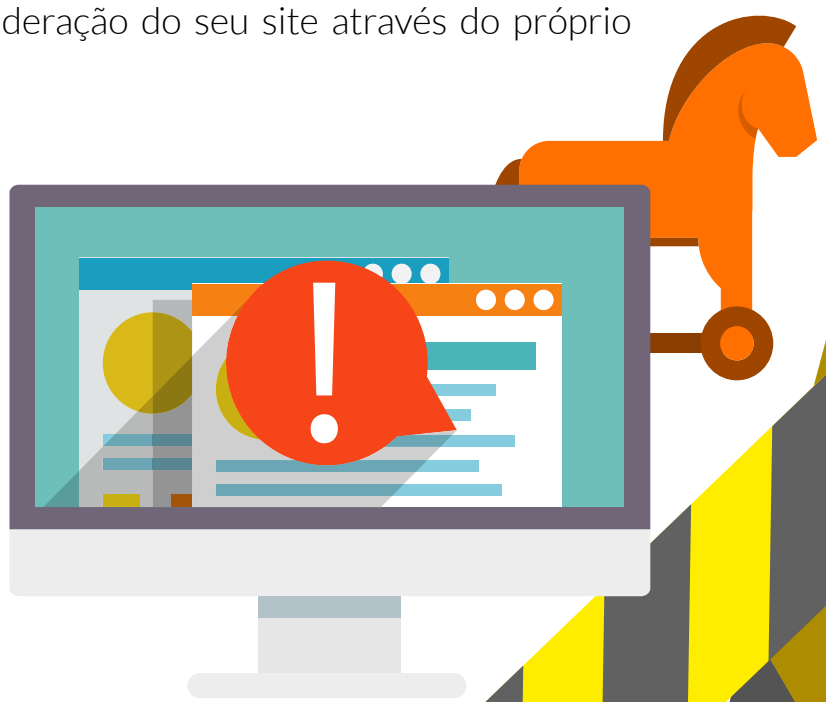
- Antes de tudo, verifique se a solução de segurança (como antivírus, firewall e anti-spyware do seu computador) está atualizada e se é confiável. Caso seja necessário, atualize as ferramentas de segurança;
- Faça o download de todos os arquivos do site para o seu computador, e passe o antivírus na pasta onde estes arquivos estão. Se um vírus for identificado, remova-o;
- Após este processo de limpeza, faça o upload dos arquivos de volta para o seu plano de hospedagem;

- Se mesmo assim continuar a ameaça, verifique com seu webmaster se no arquivo índice do seu site (index.html, index.php, etc) há algum código que executa o vírus a partir de outro local;
- Após todos estes passos, abra um chamado no HelpDesk da Hostnet solicitando uma varredura no servidor com nosso antivírus (ClamAV) para uma verificação final do caso.
- A integridade do que está no servidor FTP, assim como eventuais danos causados a terceiros, é toda de responsabilidade do proprietário do site. A Hostnet está isenta de qualquer problema decorrente da contaminação causada por estes arquivos.

Meu site foi identificado como malicioso pelo Google. Como resolvo isto?

Execute todos os passos da seção anterior, e posteriormente, faça o seguinte:

- Cadastre seu site na ferramenta de webmasters que é disponibilizada pelo Google;
- Execute os passos indicados pelo Google. A própria ferramenta indicará quais são os arquivos considerados "maliciosos" dentro do seu site;
- Verifique os arquivos mencionados e faça a limpeza, usando um cliente FTP;
- Finalmente, solicite uma reconsideração do seu site através do próprio Google Webmaster.



Realização

E-book

Seus dados estão realmente seguros?

Redação
Ricardo Jurczyk Pinheiro

Revisão
Lisane Monteiro, Mabel Antunes, Camila Jacob, Rebeca Fonseca e Ricardo Soares

Diagramação
Ramon Felinto

Imagens
freepik.com

Mais e-books em
www.hostnet.com.br