POLÍTICAS DE USO

SPAM

Por definição, Spam (Unsolicited Commercial E-mail) é basicamente o envio de mensagens eletrônicas geralmente em grande quantidade e para múltiplos destinatários, forçando-os a ler ou acessar algum tipo de propaganda, anúncio, promoção ou informação que não foram previamente solicitados.

A AFIXAR/AFXHOST é contra a prática de Spam, sendo totalmente proibida sua veiculação por nossos servidores.

Será considerado Spam, quando ocorrer:

- Envio de e-mails em massa que não tenham sido solicitados pelo destinatário.
- Uma denúncia de ISP parceiros ou usuários registrados.
- Uma denúncia de órgão anti-spam como spamcop, spamhaus entre outros.

Em caso de utilização de Spam, a ação tomada pela AFIXAR/AFXHOST será:

- A conta do domínio será suspensa e o responsável por ele será comunicado via e-mail e telefone.
- Em caso de reincidência, a conta do domínio será excluída de nossos servidores e o serviço prestado automaticamente cancelado, sendo o responsável comunicado via e-mail e telefone.
- O backup do domínio ficara disponível por 72horas, para que o responsável faça o download do seu conteúdo.

Agressão à Performance

Será considerada agressão à performance dos servidores, quando ocorrer:

- Envio em massa com mais de 300 e-mails por hora em uma hospedagem compartihada.
- Envio de e-mail com mais de 100 destinatários em uma hospedagem compartilhada.
- Uso excessivo de banco de dados seja mysql ou postgrsql superior a 50.
- Consultas simultâneas com mais de 300 segundos.
- Acesso excessivo ao site superior a 100 conexões sultanearas http sem aviso prévio.
- Mais de 30 erros de autenticação seguidos em menos de 8 minutos.
- Utilização de processamento e memória superior a 3% do servidor.
- Utilizar programas ou scripts que, por qualquer razão, prejudiquem o funcionamento normal do servidor.

Em caso de agressão à performance, a ação tomada pela AFIXAR/AFXHOST será:

- Suspensão da conta do domínio por 15 minutos em caráter de advertência.
- Se ocorrerem mais de 3 advertências seguidas, o domínio ficará suspenso durante 24 horas ou até que o responsável entre em contato conosco por e-mail ou telefone.

OBS:. O tópico de Agressão à Performance só se aplica a hospedagem de site compartilhada e revenda.

PHISHING

PHISHING se refere a uma forma de captação de dados de maneira fraudulenta. Esses dados podem ser números de cartão de créditos e de contas bancárias, senhas, contas na internet e etc. Phishing consiste, basicamente, no ato de uma pessoa se fazer passar por outra ou por uma empresa, solicitando informações confidenciais.

Em caso de Phishing, a AFIXAR/AFXHOST se reserva o direito de realizar:

- A exclusão da conta do domínio e cancelamento imediato do plano contratado.
- A comunicação ao cliente por e-mail e telefone.
- Backup do domínio ficará disponível por 72 horas, para que o responsável faça o download do seu conteúdo.

Vírus Iframe

O Vírus de Iframe é um vírus que não tem tanto poder destrutivo, mas é extremamente fácil de propagar, geralmente infecta sua máquina local, infectado seus arquivos locais e adquirindo logins e senhas de FTP gravados em seu computador. De posse dessas senhas, ele se conecta automaticamente ou aproveita conexões de ftp já abertas e infecta os arquivos do seu site , blogs ou sistemas em html e php.

Em caso de Vírus Iframe, a AFIXAR/AFXHOST se reserva o direito de realizar:

Limpeza do código inserido pelo vírus nos arquivos html e php entre outros. Caso não seja possível a remoção do código por qualquer motivo, os arquivos serão excluídos do servidor e o backup disponibilizado para download por 72horas. A mudança de todas as senhas de FTP e painel de controle existente no domínio.

É dever do usuário adquirir um software anti-vírus para a desinfecção das suas máquinas locais, a fim de evitar a reinfecção dos arquivos do domínio hospedado em nosso servidores.

PHP Injection ou RFI (Remote File Include)

Sua função é basicamente explorar um erro de programação na construção do site, blog ou sistema, onde é permitida ao atacante a execução de arquivos maliciosos remotamente ,ou seja, executar arquivos que estejam fora do servidor.

Essa vulnerabilidade é altamente perigosa, pois através dela é possível ler arquivos, o código de arquivos do domínio, ter acesso a informações confidenciais, fazer upload de arquivos malicioso para o domínio, modificar arquivos entre outras práticas.

Por esse motivo, a AFIXAR/AFXHOST possui uma severa política de segurança que inibe cerca de 98% desta prática.

Porém, quando detectada tal falha de programação, mesmo que ela não esteja ou não possa ser explorado, devido à nossa política de segurança, o site, blog ou sistema que a contem, terão seu acesso bloqueado automaticamente por nossa equipe de suporte até que tal falha seja corrigida.

Caso isso ocorra, o responsável será notificado via e-mail e por telefone.

Lembramos que é de responsabilidade do usuário manter seus códigos sempre limpos, organizados e livres de erros ou falhas de programação.

Exemplo de Vulnerabilidade:

```
<?php

include('topo.php');
include('menu.php');
include($goto);

?>
```

Existem várias strings como page, goto, cmd, etc... A url ficaria http://www.vuneravel.com.br/index.php?goto=noticias.php logo ele irá carregar a página noticias.php do site. Se ela for vulnerável, como a citada acima, é possível injetar arquivos com códigos malicioso que executam comandos no servidor que esta o site se encontra.

SQL Injection

SQL Injection tem basicamente a função de explorar uma falha na programação do site, blog ou sistema, onde o atacante consegue inserir uma série de instruções SQL dentro de uma 'query' através da manipulação das entrada de dados de um site , blog ou sistema.

Essa vulnerabilidade é altamente perigosa, pois através dela é possível a manipulação do banco de dados utilizado, podendo-se deletar tabelas, inserir dados, ter acesso a informações privilegiadas entre outras práticas.

Por esse motivo, a AFIXAR/AFXHOST possui uma severa política de segurança que inibe cerca de 98% desta prática. Porém, quando detectada tal falha de programação, mesmo que ela não esteja ou não possa ser explorada, devido à nossa política de segurança, o site , blog ou sistema que a contem terão seu acesso bloqueado automaticamente por nossa equipe de suporte até que tal falha seja corrigida.

Caso isso ocorra, o responsável será notificado via e-mail e por telefone.

Lembramos que é de responsabilidade do usuário manter seus códigos sempre limpos , organizados e livre de erros ou falhas de programação.

Exemplo de Vulnerabilidade:

```
<?php

$usuario = $_POST['usuario'];
$senha = $_POST['senha'];

$query_string = "SELECT * FROM usuarios WHERE codigo = '{$usuarios}' AND
senha = '{$senha};

?>
```

As variáveis $usuario e $senha, respectivamente, recebem o conteúdo submetido por um formulário através do método POST. Se o atacante colocar no lugar do usuário "espaço em branco" e no lugar da senha " 'or 1'=1 " sua query ficaria assim :

```
SELECT * FROM usuarios WHERE codigo = '' AND senha = '' or 1='1'
```

A condição de autenticação seria satisfeita e o atacante teria acesso ao seu sistema, blog ou site sem ao menos digitar um usuário existente.

Políticas de Senhas

A maneira mais utilizada no mundo para restringir acesso a sistemas computacionais é por meio de login e senha. Por este motivo existe uma grande preocupação em sua constituição, pois, de posse desses dados, torna-se praticamente impossível a detecção de acessos indevidos.

Considerando essa informação, a AFIXAR/AFXHOST sugere algumas dicas para o sucesso da construção de suas senhas:

- Nunca use login e senha iguais.
- Nunca use números ou letras seqüenciais como 1234 ou abcd.
- Nunca use palavras corriqueiras com tmp, deus, jesus, casa, bola etc.
- Nunca use datas de aniversário ou número de telefone.
- Sempre use senhas alfanuméricas sem seqüencia definida como tg76ub290dv, 9ut85f12n90, etc.
- Se for permitido e interessante, utilizar caracteres especiais como “@!#$%&-+_]{?><=”.
- Exemplo de senha considerada forte: “@=S61slw??j1”.

Lembramos que a política de segurança mais rigorosa se torna ineficiente, quando suas senhas são fracas e de fácil dedução.

Lembramos, também, que acessos privilegiados a seus sites, sistemas, blogs etc não devem ser feitos em redes públicas como shopping centers, lojas, lan houses e até mesmo em redes wireless sem segurança, pois é provável a presença de snifers nessas redes os quais capturam seus login e senhas para serem utilizadas posteriormente.

Se for realmente necessário o acesso por redes públicas, utilize criptografia SSL para proteger seus dados. Consulte nossa equipe de atendimento ou nossa ajuda online sobre criptografia SSL.

Ataque por força bruta

BFA (Brute Force Attacks) ocorre basicamente quando o atacante tenta descobrir a senha de acesso de um site, sistema, blog ou serviço, tentando inserir várias combinações de senhas diversas vezes.

Atualmente, já existem softwares específicos que ficam tentando várias combinações indefinidamente, a fim de conseguir acesso. Em decorrência disso, quanto mais fraca for sua senha, maior a probabilidade de sucesso por parte do atacante.

A AFIXAR/AFXHOST , pensando na segurança e na inviolabilidade dos seus serviços, possui um mecanismo de detecção chamado BFD ou (brute force detect) que detecta estas várias tentativas de senha e bloqueia e registra em log o ip do atacante, impedindo, assim, que ele continue tentando indefinidamente.

Infelizmente existem falsos positivos, ou seja, se alguns usuários de uma mesma rede errar algumas vezes suas senhas, o BFD entenderá que se trata de um ataque BFA e o IP dessa rede será bloqueado.

Caso isso ocorra, você deve seguir os seguintes passos:

Acesse o site www.ipok.com.br. Na parte superior do site, você deve visualizar "Seu IP:" anote esse número e entre em contato com nossa equipe de atendimento via e-mail, telefone ou chat. Informe ao atendente número ip para ser desbloqueado.

Práticas Proibidas

A AFIXAR/AFXHOST proíbe, sob qualquer condição, as seguintes práticas:

Transmitir ou divulgar ameaças, pornografia infantil, material racista, discriminatório ou qualquer outro que viole a legislação em vigor no Brasil.

Disponibilizar ou armazenar quaisquer materiais com direitos reservados, de propriedade intelectual ou com copyright, incluindo MP3, MPEG, ROM ou emuladores ROM, vídeos, distribuição ou divulgação de senhas para acesso de programas alheios, difamação de pessoas ou negócios, alegações consideradas perigosas ou obscenas, protegido por segredo de Estado ou outro estatuto legal.

Propagar vírus de computador ou qualquer programa de computador que possa causar danos permanentes ou temporários em equipamentos de terceiros.

Transmitir tipos ou quantidades de dados que possam causar falhas em serviços ou equipamentos nos servidores da AFIXAR/AFXHOST ou de terceiros.

Usar os servidores da AFIXAR/AFXHOST para tentar e/ou realizar acesso não autorizado a dispositivos de comunicação, informação ou computação.

Promover ou prover informação instrutiva sobre atividades ilegais, que promovam ou induzam dano físico ou moral contra qualquer grupo ou indivíduo.

Transmitir, armazenar ou divulgar qualquer material relacionado a hacking/cracking, incluindo links para outros sites.

Forjar endereços de correio eletrônico, na tentativa de responsabilizar terceiros ou ocultar a identidade ou autoria.

Violar a privacidade de terceiros.

Distribuir, via correio eletrônico, grupos de discussão, fóruns e formas similares de comunicação, mensagens não solicitadas do tipo SPAM ou 'corrente', comerciais ou não.

Fornecer dados falsos por meio de solicitação de serviços ou cadastro de conta de domínio ou e-mail.

Ação tomada pela AFIXAR/AFXHOST , se qualquer um dessas práticas for identificado:

A AFIXAR/AFXHOST se reserva o direito de cancelar ou suspender imediatamente todos os serviços prestados ao praticante, caracterizando quebra de contrato por parte do contratante por um tempo determinado ou em definitivo, como julgar pertinente.