GUIA PRÁTICO PARA A SEGURANÇA DO SEU SITE

GUARDTI


GUARDTI
HTTPS

GUARDTI

É uma versão segura do HTTP que utiliza um recurso de encriptação das informações trafegadas entre o usuário e o servidor do seu site, dificultando que estas informações sejam interceptadas por terceiros durante o processo de comunicação.

Em termos práticos, quando o usuário preenche um formulário e clica em “enviar”, antes de chegar ao seu

GUARDTI

destino (o servidor que hospeda o site), as informações percorrem um longo caminho, passando por diversas redes, equipamentos, servidores, dentre outros. E ao longo desse percurso as informações daquele formulário podem ser capturadas e visualizadas quando o site utiliza HTTP. Quando o site utiliza HTTPS as informações estão criptografadas, exigindo um esforço gigante para decifrá-las.

GUARDTI

Por que eu tenho que usar HTTPS no meu site?

- Aumenta a segurança na comunicação dos usuários com o site e servidores.
- Aumenta a confiança do usuário durante a navegação ao ver o tradicional “cadeadinho” em seu navegador.
- Melhora a posição do seu site no ranking de buscas, comparado aos sites que não utilizam HTTPS.
- Melhora o desempenho do seu site, garantindo melhor experiência dos usuários na navegação.

GUARDTI

Verificando e Implementando o HTTPS em seu site

- Se você não sabe se seu site possui ou não HTTPS, ou se quer saber se seu certificado está válido e e corretamente implementado, acesse o SSL TEST e execute um teste na URL do seu site: https://www.ssllabs.com/ssltest/

- A implantação de um certificado SSL é um processo técnico que envolve a validação de identidade do requisitante, a emissão de um certificado por uma autoridade certificadora e a instalação em seu servidor de aplicação.

GUARDTI

Verificando e Implementando o HTTPS em seu site

- A Let’s Encrypt é uma Autoridade Certificadora que fornece certificados válidos gratuitos.
- Seus certificados funcionam muito bem com os principais navegadores, incluindo dispositivos móveis.
- Para obter seu certificado, visite: https://letsencrypt.org/

GUARDTI

Anti-DDOS

GUARDTI

Ataques DoS (Negação de serviço) e ataques DDoS (Ataques de negação de serviço distribuído) são basicamente a mesma coisa, a única diferença existente entre os dois é a escala em que ocorre. Ataques do tipo DoS vêm de uma única fonte enquanto os DDoS vêm de fontes espalhadas pelo mundo. O segundo tipo massivo e pode gerar um volume gigantesco de de acessos.

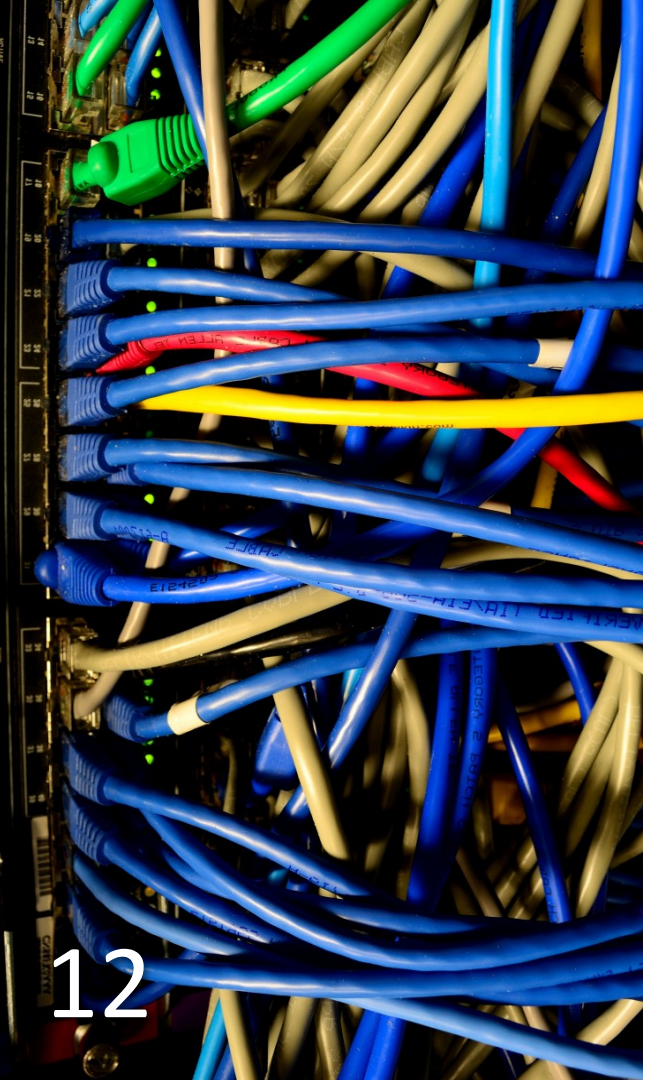
GUARDTI

Em ataques do tipo DoS ou DDoS o detrator utiliza um ou mais computadores. Ataques DoS geram um volume baixo de tráfego mas que já afeta a sua aplicação, enquanto o DDoS gera um volume grande de tráfego (na casa dos Gigabits por segundo muitas vezes). Muito mais do que a maioria dos sites podem suportar (seja em links ou em recursos computacionais).

GUARDTI

Esses ataques têm se tornado cada vez mais comum devido ao mercado de vendas de serviços de DDoS.

Ataques de DoS ou DDoS tem como objetivo interromper a entrega do seu site. Eles afetam diretamente o desempenho do seu site fazendo com que ele fique mais lento ou até mesmo inacessível, afetando diretamente seu negócio.



Os 3 tipos de ataques DoS e DDoS:

Esses 3 tipos de ataque tem basicamente a mesma função: consumir recursos do seu servidor web até deixar ele inacessível.

GUARDTI

Ataque baseado em volume

Esse é um ataque onde o invasor gera um grande volume de tráfego contra um servidor web. Geralmente é um ataque muito eficaz pois a maioria dos sites estão ou em hospedagem compartilhada ou em VPS sem a configuração correta.

GUARDTI

Ataque baseado em protocolo

O tráfego na internet é baseado em protocolos. É assim que as pessoas saem do computador delas e chegam ao seu site. Esse tipo de ataque pode se basear em técnicas como Ping of Death, SYN Flood, modificações de pacotes dentre outra variações.

GUARDTI

Ataque na camada de aplicação

Este tipo de ataque foca fragilidades no servidor web (IIS, Apache, nginx, etc) ou na aplicação, gerando um número grande de requisições em uma funcionalidade que pode onerar muito o processamento do servidor.

GUARDTI

Por que eu preciso de um Anti-DDoS?

- Para melhorar a disponibilidade e performance do seu site.
- Para manter a continuidade negocial e atividades do seu site.
- Não desapontar ou frustrar seus clientes e perder negócios.
- Tornar seu site mais profissional inibindo “brincadeiras” que podem tirar seu site do ar.

GUARDTI

Implementando um Anti-DDoS em seu site

- Se você não sabe se seu site possui ou não proteção para ataques DDoS, verifique através do link: https://siteseguro.guardti.com.br

- Existem ataques DDoS de diversos tamanhos, e a forma mais efetiva para se proteger de todos é através do uso de uma rede distribuída (geograficamente) capaz de absorver, processar, identificar e eliminar o tráfego malicioso antes ele atinja seu site e consuma todos os recursos computacionais ou de link de sua hospedagem.


GUARDTI
WAF
Web Application Firewall

GUARDTI

Um firewall de aplicações Web filtra, monitora e bloqueia o tráfego malicioso entre usuários e um website. Um WAF é diferenciado de um firewall comum, pois é capaz de filtrar o conteúdo de aplicativos web específicos, enquanto os firewalls comuns servem como um portão de segurança entre servidores.

GUARDTI

Ao inspecionar o tráfego de navegação, o WAF pode evitar ataques decorrentes de falhas de segurança nas aplicações Web, como injeção de SQL, XSS (cross-site scripting), inclusão de arquivos e configurações erradas de segurança.

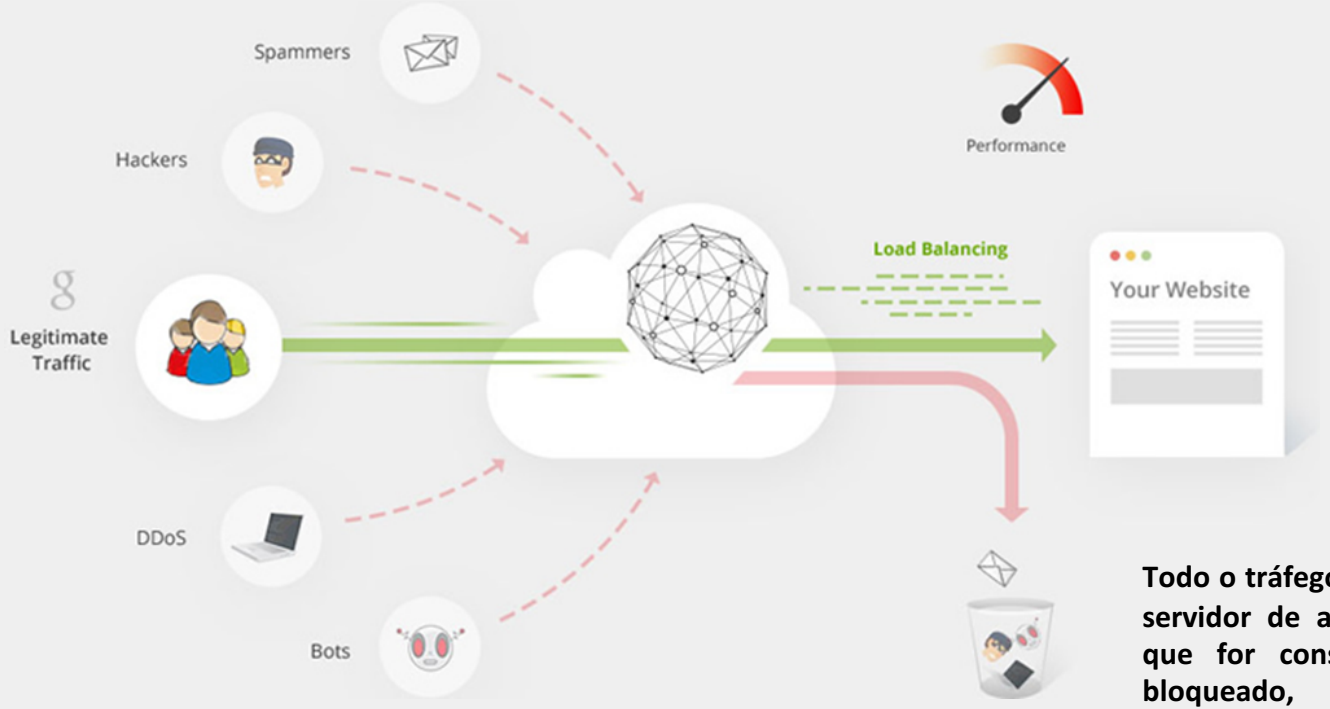
GUARDTI

Principais Benefícios:

- Bloqueia Instantaneamente Ataques Hackers
- Mitigação e Prevenção de Ataques DDoS
- Patch e Endurecimento Virtual
- Proteção da reputação da marca
- Evitar explorações de dia zero

GUARDTI

COMO O WAF FUNCIONA?



Todo o tráfego entre os usuários e o servidor de aplicação é filtrado. O que for considerado malicioso é bloqueado, permitindo somente acessos legítimos

GUARDTI

Virtual Patching & Hardening

Quando vulnerabilidades de segurança são descobertas, muitas vezes não temos tempo hábil para conseguir implantar a correção sem parar a aplicação. Através do WAF é possível a utilização de Virtual Patching e Hardening, que são regras de correção aplicadas no próprio WAF.

GUARDTI

Application Profiling

Cada site tem as suas próprias peculiaridades, isso vai depender do CMS, do servidor web e de todas as outras tecnologias que estão sendo utilizadas para entregar sua aplicação.

O application profiling vai trabalhar entendendo bem o seu tráfego e bloqueando explicitamente tudo aquilo que não se encaixa no perfil de acesso do seu aplicativo web.

GUARDTI

Machine Learning

A correlação de eventos para entender melhor os ataques é uma das grandes características que um WAF deve ter. Esse recurso permite que padrões de ataques sejam identificados e ações de mitigação mais inteligentes sejam feitas de forma automatizada, permitindo que seu site fique protegido contra ameaças emergentes, antes mesmo que elas possam afetar o seu negócio!

GUARDTI

Páginas protegidas

Com a utilização do WAF é possível que criar uma segunda camada de proteção para determinadas páginas. Você pode usar essa característica para adicionar senhas, CAPTCHA, 2FA ou até mesmo lista de permissão por IPs para liberar acesso à paginas que você gostaria de proteger.

GUARDTI

Bloqueio de bots

Outra característica importante do WAF é a detecção de tráfego malicioso de bots, que são ferramentas automatizadas de ataque usadas por hackers. Isso ajuda a impedir que seu site seja varrido por essas ferramentas automatizadas que geralmente são utilizadas em ataques massivos de malwares.

GUARDTI

Whitelisting / Blacklisting

Você pode liberar ou bloquear somente determinados endereços IPs, redes ou até mesmo países em determinada partes do seu site. Por exemplo, é possível fazer esse bloqueio para a parte administrativa do seu site, liberando somente para os IPs que você liberou.

GUARDTI

Por que eu preciso de um WAF?

- Melhorar a disponibilidade e performance do seu site.
- Para manter a continuidade negocial e atividades do seu site.
- Permitir que somente usuários legítimos acessem seu site.
- Otimizar recursos financeiros e computacionais.
- Evitar prejuízos no tratamento de incidentes, restauração de seu site e desgastes (as vezes judiciais) por vazamento de dados.

GUARDTI

Verificando e Implementando o WAF em seu site

- Se você não sabe se seu site possui ou não um firewall de aplicação, verifique através do link: https://siteseguro.guardti.com.br

- Há diversos fabricantes e fornecedores de WAF, inclusive opções gratuitas como o mod_security fornecido pela Apache. Todo o tráfego do seu site deve ser direcionado para o WAF a fim de que os acessos maliciosos não alcancem seu destino final. O WAF pode ser uma máquina ou um conjunto de máquinas dedicados para esse fim, mas também funciona como um software instalado no próprio servidor de aplicação que hospeda seu site.


GUARDTI
UPDATE

GUARDTI

Dia após dia os CMS's, plugins, sistemas operacionais e tudo o que existe para um website funcionar evolui. Da mesma forma, novos problemas ou vulnerabilidades passam a existir. É um ciclo. Portanto, uma das formas mais eficazes para evitar problemas de segurança é se manter atento às atualizações disponibilizadas pelos fabricantes ou mantenedores de tudo o que é utilizado no contexto do seu site!

GUARDTI

Verificando e Implementando Política de Update

- Estabeleça uma rotina semanal para verificar se seu CMS encontra-se atualizado, bem como plugins ou softwares de terceiros utilizados e execute as atualizações disponíveis. A maioria dos CMS's informa sobre a existência de novas versões de plugins ou do software.

- Atualizações podem impactar no funcionamento do seu site! Possua um ambiente de testes para validar que as atualizações não irão causar problemas no seu site. Sem este ambiente você pode se desencorajar a prosseguir.

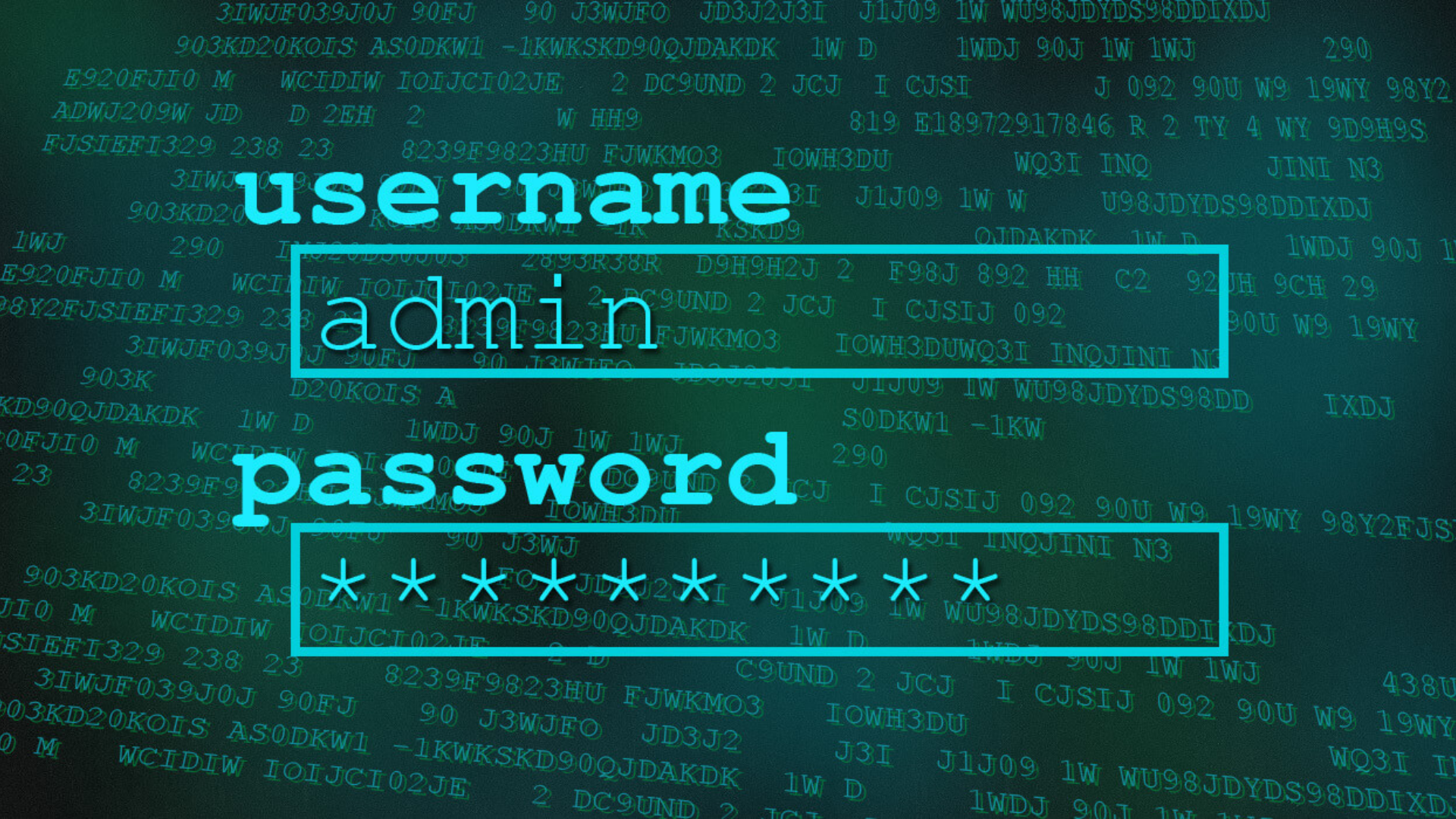
- Se um plugin foi descontinuado ou não foi atualizado durante muito tempo, considere substitui-lo ou inutiliza-lo.

GUARDTI

Verificando e Implementando uma Política de Update

- Conte com uma pessoa em sua equipe com perfil mais técnico (pode ser um freelancer) para avaliar se o ambiente que hospeda o site está atualizado. Versões antigas do Sistema Operacional (Linux ou Windows), do servidor de aplicação (APACHE, NGINX ou IIS) ou da Linguagem de Programação (PHP, ASP, etc) contém brechas que podem ser exploradas para hackear seu site.

- Siga nas redes sociais e visite com frequência o site ou blog sobre as ferramentas utilizadas em seu site. O Wordpress por exemplo disponibiliza informações sobre segurança e novas versões em seu blog oficial: https://wordpress.org/news/


username
admin
password
****

GUARDTI

Política de Senhas

Em torno do uso do seu site há diversas senhas que são utilizadas no dia a dia. Vamos lembrar de algumas:

- A senha do registro.br ou da instituição que lhe vendeu o domínio.
- A senha do painel de controle da sua hospedagem ou fornecedor cloud.
- A senha de administrador do site.

GUARDTI

Gerenciar ou ”decorar” tantas senhas pode ser um problema e eventualmente acabamos cometendo falhas como utilizar senhas fáceis, usar a mesma senha para vários serviços e compartilhar credenciais. Essa prática gera um enorme risco de sua senha ser descoberta e o seu site cair em mãos alheias.

Uma política de senhas serve para apoiar a gestão de tantas senhas, mantendo um nível de segurança maior para o seu site.

GUARDTI

Sugestão de Política de Senhas

Listamos a seguir um exemplo de conjunto de regras para lhe ajudar a criar a implantar sua própria política:

- Utilizar no mínimo 8 caracteres compostos por letras maiúsculas e minúsculas, números e caracteres especiais (@#$%&).

- Não utilizar palavras, nomes, frases, datas ou termos de qualquer idioma na composição da senha.

GUARDTI

- Não utilizar sequências alfanuméricas ou do teclado como 123456, 12qwaszx, abcd123, qwerty.
- Possuir uma senha para cada necessidade, jamais repetir uma senha.
- Definir uma sazonalidade para trocar as senhas. Exemplo: mensal.
- Não compartilhar as senhas. Caso necessário, trocar imediatamente após o uso.

GUARDTI

Adicionalmente, sugerimos o uso de um software para gestão de senhas. Esse tipo de software o ajudará com a tarefa de manter várias senhas distintas, sem a necessidade de decorá-las.

Há opções gratuitas:

- KeePass: https://keepass.info/
- LastPass: https://www.lastpass.com/

GUARDTI

Proteja seus Usuários/Clientes

O roubo de credenciais tornou-se uma das estratégias mais utilizadas para obter acesso privilegiado em sistemas e executar todo tipo de fraude.

Phishing, compartilhamento de links maliciosos e a disseminação de malwares são as ferramentas mais utilizadas nesse ataque. E os frequentes vazamentos de bancos de dados só contribuem com o aumento de credenciais disponíveis na internet.

GUARDTI

Segundo estudo da Intel, 97% das pessoas não seriam capazes de identificar que um email é um Phishing.

No Brasil, 89% dos executivos que participaram de uma pesquisa foram vítimas de fraudes cibernéticas em razão de Phishing ou Malware.

No 3º Trimestre de 2018 foram identificados 43,8 milhões de links maliciosos no Brasil.

Estes números colocam todos nós em risco.

GUARDTI

Como melhorar a proteção dos seus clientes/usuários?

- Criar uma política de senhas robusta para o uso de suas aplicações.
- Fazer uso de tokens de acesso (OTP).
- Implantar autenticação de 2 fatores.
- Fazer uso de soluções que realizam análise comportamental dos seus usuários, e detectam possíveis desvios/fraudes.


ROTINA DE TESTES
DE
VULNERABILIDADES
GUARDTI

Rotina de avaliação de vulnerabilidades

Uma avaliação de vulnerabilidade é o processo de identificar, quantificar e priorizar (ou classificar) as vulnerabilidades em um sistema.

A rotina de avalição de testes de vulnerabilidade deve ser executada sazonalmente em seu site, porém sem se limitar somente aos sites. É muito importante avaliar também todos os recursos utilizados para a disponibilização do seu site na internet (servidor web, sistema operacionais, banco de dados, etc). Essas avaliações são indicadas para negócios de todos os tamanhos.

Vulnerabilidade na perspectiva do gerenciamento de desastres significa avaliar as ameaças de riscos potenciais.

Modelo de Processo Contínuo para Gestão de Vulnerabilidades


GUARDTI
Quer ficar livre dos hackers e manter o seu negócio faturando?
contato@guardti.com.br