

## CleanPipes – Sistemas e Soluções de Segurança

### PORQUE DEVO PROTEGER A MINHA EMPRESA CONTRA AS AMEAÇAS VINDAS DA INTERNET?

As ameaças e ataques de segurança realizados contra sistemas críticos a partir da Internet, têm assumido formas cada vez mais sofisticadas e disruptivas, conduzindo a que as empresas possam inesperadamente ficar com o seu negócio on-line severamente comprometido.

A forte dependência que as empresas têm da Internet para a condução do seu negócio, como sejam as empresas do sector financeiro, coloca desafios acrescidos na gestão operacional de segurança, levando ao balanceamento entre políticas que, com um nível de segurança aceitável facilitem, as transacções e os demais processos de negócio.

A ocorrência de indisponibilidade de serviços on-line, como o serviço de banca electrónica, provoca normalmente grande constrangimento junto dos seus utilizadores, uma vez que estes esperam obter acesso real-time na interacção com o seu banco através da Internet, seja em operações de

pagamentos, transferências ou, subscrição de produtos, etc. Estes serviços on-line têm sido particularmente visados por complexos ataques DDoS, amplamente evidenciados em diversos relatórios internacionais ao longo dos últimos anos.

Os incidentes de segurança além de eventuais perdas financeiras, acarretam outras questões por vezes menos tangíveis, mas não menos importantes, como sejam a credibilidade e imagem da organização no contexto onde se insere, pelo que os factores de risco e o possível impacto da ocorrência deste tipo de incidentes devem ser profundamente analisados e ponderados pela gestão de topo da empresa.

### O QUE FAZER AO NÍVEL DA PREVENÇÃO?

Se é responsável pela infra-estrutura de IT e Segurança da sua empresa, certamente já colocou algumas das seguintes questões:

- Será que em caso de indisponibilidade dos serviços on-line, a empresa funciona sem impacto para os nossos clientes?
- Quais os impactos para a organização, na eventualidade de ocorrer uma falha de segurança nos sistemas críticos?
- Quando foi realizado o ultimo briefing à

administração da empresa, acerca dos riscos e melhorias a introduzir na segurança e sistemas críticos?

- O que posso fazer para minimizar os factores de risco?

As respostas nem sempre são óbvias e podem até ser complexas e difíceis de obter, no entanto é aqui que um parceiro externo poderá contribuir para endereçar estas questões de modo mais evidente e objectivo.

A segurança dos sistemas críticos exige permanente atenção de equipas técnicas treinadas, na operação, gestão e manutenção dos diversos sistemas de segurança, só deste modo será possível minimizar os factores de risco das ameaças externas. No entanto, há ataques que pela sua complexidade e dimensão carecem da colaboração externa do ISP, como sejam os ataques do tipo DoS (Denial of Service) e DDoS (Distributed Denial of Service).

É nesta vertente que o serviço CleanPipes (acessos limpos) da PT Prime pode ser uma mais valia para as empresas. Este serviço de segurança destina-se a Clientes com acessos Internet da PT Prime ou da Telepac, com elevada largura de banda, tendo por objectivo a prevenção de ataques e limpeza

de tráfego anómalo vindo da Internet.

O serviço CleanPipes da PT Prime está suportado em plataformas de segurança de alta disponibilidade e elevada performance, que respondem eficazmente aos requisitos das empresas neste domínio.

O serviço CleanPipes é fundamental para a Segurança dos sistemas on-line das empresas, cuja utilização da Internet seja crítica para o sucesso do seu negócio, particularmente em sectores de actividade como a banca e seguros, administração pública, comunicação e media.

### **QUAL O IMPACTO DE UM ATAQUE DDoS PARA A EMPRESA?**

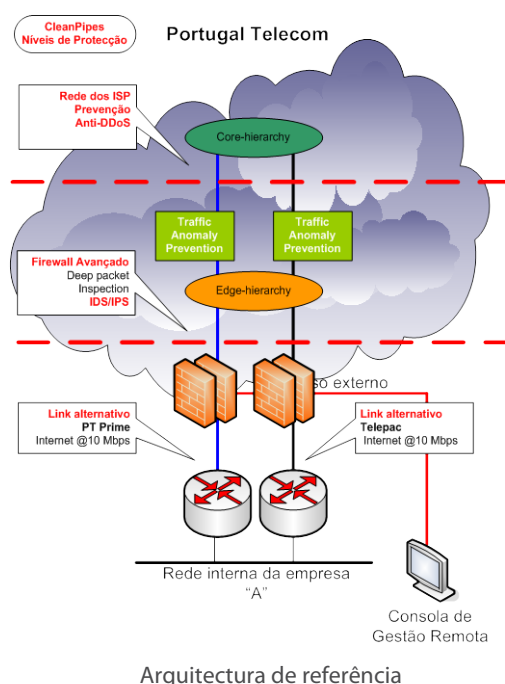
Os ataques do tipo DDoS, são extremamente difíceis de defender, uma vez que não há receitas tipo nem soluções imediatas que a empresa vítima do ataque possa activar apenas do seu lado. Perante um ataque DDoS o caos instala-se na empresa, fundamentalmente pela indisponibilidade de serviços ou aplicações críticas, podendo estes ataques atingir valores de tráfego de vários Gigabits por segundo e ter uma duração desde breves minutos até alguns dias, com eventuais repercussões nas semanas subsequentes.

Funcionalidade	Aplicação	Benefício
<b>Prevenção Anti-DDoS</b>	Identificação e mitigação de ataques DoS, DDoS, descarte de tráfego anómalo	Diminuição significativa do Risco de ataques DDoS, que causam grande indisponibilidade de serviços tipo Web, Mail, etc.
<b>Firewall Avançado na rede do ISP</b>	Firewall de baixa latência, que realiza deep packet inspection, até L7	Permite implementar e reforçar políticas de controlo de acesso ao perímetro e mitigar ataques pré-definidos
<b>Prevenção de Intrusão (IDS/IPS)</b>	Prevenção de intrusão, com base em assinaturas e anomalias de protocolo	Previne ataques embudidos ao nível aplicacional DNS e WEB, bloqueia trojans, worms e alguns padrões de vírus
<b>Filtragem de URLs e Conteúdos</b>	Controla e bloqueia o acesso e navegação a sites por categorias e listas com base em perfis	Previne a utilização abusiva da Internet aos colaboradores, evita o acesso a sites de conteúdos inapropriados
<b>Mail Security (Anti-SPAM)</b>	Implementa mecanismos de Anti-SPAM e Anti-Malware (vírus, warms) sobre o email	Resolve os problemas de SPAM e vírus associados ao email Permite uma gestão por utilizador da quarentena do SPAM
<b>Gestão de Largura de Banda</b>	Implementa uma optimização na gestão da largura de banda	Permite optimizar o acesso em função da banda disponível, utilização de protocolos e redes de acesso
<b>Gestão Remota e Logging</b>	Consola de gestão remota	Permite a gestão remota e a gestão dos logs

Para a minimizar o impacto dos ataques DDoS é fundamental que o parceiro prestador do serviço possua sistemas de prevenção adequados a ataques de larga escala, operados por equipas técnicas eficazes, devidamente suportadas por um conjunto de processos adequados à realidade da Organização.

### QUAIS AS VALÊNCIAS DO SERVIÇO CLEANPIPES?

O serviço CleanPipes, da PT Prime, está suportado numa arquitectura de processos multi-verificação, conforme arquitectura de



referência, sendo que a plataforma usa a mais recente análise comportamental e tecnologia de assinaturas para reconhecimento de ataques. Proactivamente detecta e identifica os diversos tipos de ataques, através da monitorização constante do tráfego com destino ao acesso Internet do cliente. Além da prevenção de ataques DDoS, o serviço CleanPipes permite ainda a prevenção de intrusão e firewall avançado, a filtragem URL e de conteúdos Web, a prevenção anti-spam (mail security), e uma eficiente gestão de largura de banda.

### **QUAIS SÃO OS BENEFÍCIOS DO SERVIÇO CLEANPIPES?**

O serviço CleanPipes apresenta um conjunto alargado de benefícios para as empresas clientes, que em resumo se traduzem por maior disponibilidade dos serviços críticos e consequente diminuição dos factores de risco, aliado ainda a uma maior eficácia na gestão dos recursos disponíveis e com custos operacionais globalmente mais reduzidos.