interweb

Gerado a 28/10/2026 10:52

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

O que fazemos pela segurança, DDoS incluído, e o que fica do seu lado

Segurança

CÓDIGO
RLX-MZ-KB-330

VERSÃO
v2026.09.28

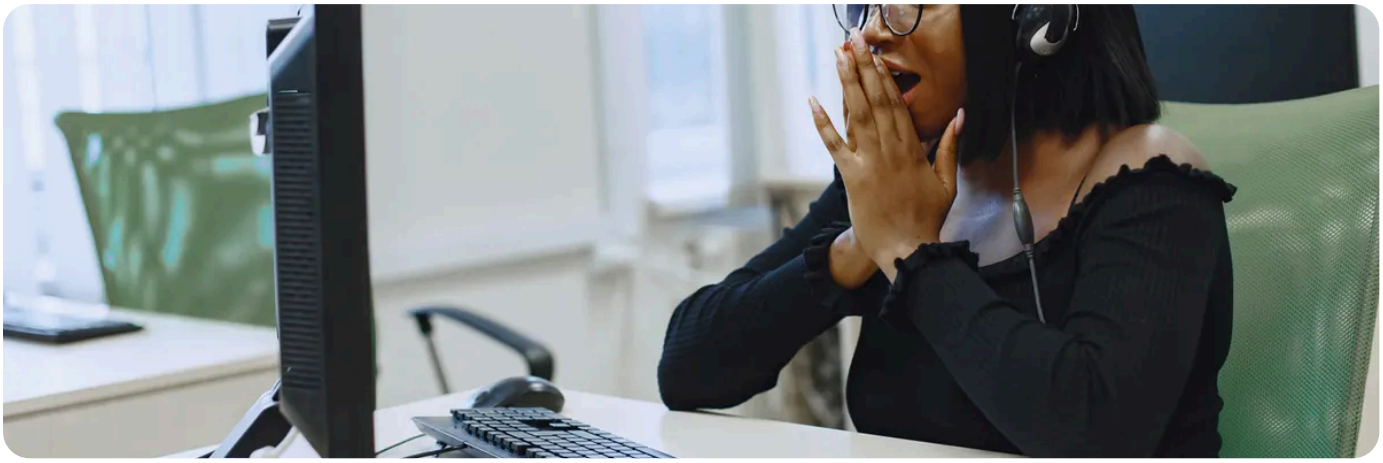
PAÍS · IDIOMA
Moçambique · Português

Interweb Moçambique
RLX Holdings, S.A. · Grupo RLX Holdings
NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

https://www.meu.interweb.co.mz/knowledgebase/330

O que fazemos pela segurança, DDoS incluído, e o que fica do seu lado

Segurança Criado em **11 de setembro de 2026** Atualizado em **28 de setembro de 2026** 4 min de leitura



Esta é uma pergunta que merece números e nomes, e não publicidade. Abaixo está o que corre nos nossos servidores, o que isso trava de facto, e - a parte que quase nenhum fornecedor escreve - **o que continua a depender de si**.

O que está a correr, pelo nome

Camada	O que faz
Firewall CSF/LFD	Filtra as ligações e bloqueia automaticamente quem repete tentativas falhadas. É o que apanha a força bruta antes de ela acertar - e também o que por vezes apanha um cliente numa rede partilhada: **porque é que o seu IP é bloqueado**
ModSecurity	Inspecciona cada pedido web e recusa os que têm forma de ataque - injeção de SQL, tentativas de leitura de ficheiros, pedidos a *.env* e a *.git*. O motor está ligado, com um conjunto de regras comercial e actualizado.
Imunify360	Analisa os ficheiros das contas à procura de código malicioso e trabalha em conjunto com a firewall, partilhando a lista de quem está a atacar a rede inteira.
Antivírus ClamAV	Verificação de ficheiros ao nível do servidor, incluindo o que entra por FTP e por e-mail.
Contas isoladas	Cada conta corre separada das outras. Um site vizinho comprometido não alcança os seus ficheiros.
SSL automático	Certificado emitido e renovado sozinho para os domínios da conta - ver **o que é um certificado SSL**
Cópias com o JetBackup	Reposição de ficheiros, bases de dados ou caixas de correio, por data - ver **como repor os seus dados**

E os ataques de negação de serviço (DDoS)?

Um ataque DDoS não tenta entrar: tenta **afogar**. Milhares de pedidos falsos ao mesmo tempo, até o servidor deixar de responder a quem é verdadeiro. É diferente de tudo o que está na tabela acima, e trava-se noutro sítio.

Os nossos servidores estão num centro de dados europeu com **filtragem de ataques volumétricos ao nível da rede** - o tráfego de ataque é absorvido antes de chegar à máquina. Sobre onde ficam exactamente, ver **onde ficam os nossos servidores**.

O que nenhum fornecedor pode prometer.
Nenhuma protecção é absoluta, e quem disser o contrário está a vender. Num ataque muito grande e dirigido, a resposta habitual da rede é deixar cair o tráfego para o endereço atacado - o que protege todos os outros e deixa o alvo indisponível durante algumas horas. É desagradável, e é a opção menos má.

Se o seu site é alvo provável.
Um site com adversidade real - política, jogos, casas de apostas, ou concorrência agressiva - ganha muito em ficar atrás de uma CDN com modo de emergência, que filtra os pedidos *antes* de eles chegarem cá. É a protecção mais eficaz que existe para este caso e a maior parte custa zero.

O que não dizemos ter

Preferimos ser verificáveis a ser impressionantes. Por isso deixamos claro o que *não* reivindicamos: não temos certificação ISO 27001, nem certificação PCI DSS, nem equipa de segurança interna dedicada, nem programa público de recompensas por falhas. Se algum concurso ou contrato seu exige um destes pontos por escrito, diga-nos antes de contratar - ver **vender online: PCI e dados de cartão**.

A parte que é sua - e é por onde entram

Vale a pena dizer isto sem rodeios: **a esmagadora maioria dos sites invadidos que vemos não foi invadida pelo servidor**. Foi pela aplicação que corre dentro dele. As causas repetem-se:

1. **WordPress, tema ou plugin desactualizado.** É a primeira causa, com folga. Uma falha conhecida é explorada por varredores automáticos poucos dias depois de ser publicada.
2. **Plugins e temas pagos obtidos de graça** em sites não oficiais. Vêm frequentemente com código acrescentado, e o preço é exactamente esse.
3. **Senhas fracas ou repetidas.** A mesma senha no site, no e-mail e numa loja qualquer que teve uma fuga - e a partir daí entra-se sem forçar nada.
4. **O computador de quem administra.** Um portátil com um ladrão de senhas instalado entrega as credenciais de FTP sem que ninguém dê por isso.

Contra isto, a firewall e o ModSecurity ajudam mas não substituem o básico: actualizar, não partilhar senhas, ligar a **verificação em duas etapas**, e desconfiar de mensagens em nosso nome - ver **como saber se um e-mail é mesmo nosso**.

Se desconfia que já aconteceu

Não comece por apagar ficheiros. Comece por **saber se o site foi mesmo comprometido** e siga depois para **como limpar um site comprometido**. E avise-nos: conseguimos ver o registo do servidor e dizer-lhe por onde entraram, o que evita que volte a acontecer pela mesma porta.

Onde acaba o nosso trabalho e começa o seu está escrito em **até onde vai o nosso apoio**.

PRECISA DE AJUDA?

Tem dúvidas sobre a segurança do seu site? Pergunte-nos.

Falar connosco →

interweb

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT	401 191 607
NUEL	105 045 974
CAE	62022
SEDE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Moçambique
CONTACTOS	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-MZ-KB-330 · v2026.09.28 · Gerado a 28/10/2026 10:52

Versão online deste documento