

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Responder a um aviso de abuso: a causa, o que removeu e como não se vai repetir

Segurança

CÓDIGO

RLX-MZ-KB-2244

VERSÃO

v2026.10.21

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/2244>



A resposta curta: o relatório que lhe pedimos depois de um aviso de abuso tem **três partes: a causa e como entrou, o que encontrou e removeu, e o que fez para não se repetir**. É com ele que respondemos ao nosso fornecedor de rede dentro do prazo. Não precisa de ser longo: precisa de ser concreto. Este artigo traz um modelo para copiar, em português e em inglês.

O que escrever em cada parte

Parte	O que serve	O que não serve
Identificador do aviso	O identificador e o IP, tal como vêm no pedido de suporte.	Responder num pedido novo, sem referência ao aviso.
A causa e como entrou	«O Redis estava aberto à internet sem senha.» «Palavra-passe fraca do root no SSH; entrada vinda do IP X a DATA.»	«Fomos atacados.» «Não sabemos.»
O que encontrou e removeu	O processo, o caminho do ficheiro, a tarefa cron, o serviço, o utilizador ou a chave SSH que não eram seus.	«Limpámos o servidor.»
O que fez para não se repetir	Actualizou, fechou a porta, mudou as senhas, passou a usar chaves SSH, ou reinstalou e repôs uma cópia limpa.	«Vamos ter mais cuidado.»
Como confirmou que parou	O comando que usou e a hora (em UTC) desde a qual não vê o tráfego do aviso.	Nada: sem isto, o fornecedor não sabe se parou.

Como preparar e enviar o relatório

1

Releia o registo do aviso: a hora (em UTC), as portas e os destinos dizem-lhe o que procurar. A explicação de cada tipo de aviso está em **um aviso de abuso sobre o seu servidor**.

2

Investigue e tome notas com as horas enquanto trabalha: o que viu, o que copiou, o que apagou. Os passos estão em **o meu VPS foi invadido?**.

3

Feche a porta de entrada antes de escrever «resolvido»: actualizar, fechar a porta na firewall, mudar senhas. Sem isto, o relatório não se aguenta.

4

Preencha o modelo abaixo, com frases curtas e factos. Se não descobriu a causa, diga-o e diga o que fez por precaução (por exemplo, reinstalar).

5

Responda no mesmo pedido de suporte do aviso, antes de o prazo acabar, e na língua em que o recebeu.

6

Se ainda não tem tudo, envie o que tem antes do prazo e diga o que falta. Uma resposta parcial a tempo vale mais do que uma completa tarde.

O modelo, em português

Assunto: Aviso de abuso [identificador do aviso] - servidor [IP]

1. Causa e como entrou: [ex.: Redis aberto à internet sem senha na porta 6379; ou palavra-passe fraca do root no SSH, primeira entrada a DATA HORA UTC vinda do IP X]
 2. O que encontrei e removi: [processo e caminho do ficheiro, tarefas cron, serviços, utilizadores ou chaves SSH que não eram meus]. Guardei uma cópia para análise antes de apagar.
 3. O que fiz para não se repetir: [actualizei o sistema e a aplicação; fechei a porta na firewall; mudei as senhas; desliguei a entrada do root por senha; ou reinstalei e repus a cópia de DATA]
 4. Como confirmei que parou: [desde DATA HORA UTC não há ligações de saída para as portas do aviso; comando usado]
- Contacto para dúvidas: [nome e telefone ou e-mail]

O mesmo modelo, em inglês

Use este se recebeu o pedido de suporte em inglês. Subject: Abuse notice [notice identifier] - server [IP]

1. Cause and how it got in: [e.g. Redis open to the internet without a password on port 6379; or a weak root password over SSH, first login at DATE TIME UTC from IP X]
 2. What I found and removed: [process and file path, cron jobs, services, users or SSH keys that were not mine]. I kept a copy for analysis before deleting.
 3. What I did so it does not happen again: [updated the system and the application; closed the port in the firewall; changed the passwords; turned off root password login; or reinstalled and restored the copy from DATE]
 4. How I confirmed it stopped: [since DATE TIME UTC there are no outgoing connections to the ports in the notice; command used]
- Contact for questions: [name and phone or e-mail]

Nunca ponha senhas, chaves privadas nem dados de clientes no relatório.

Diga que mudou a senha, não qual é a nova. E não escreva que removeu a causa se só apagou o ficheiro: se o abuso voltar depois de dizer que parou, o servidor é desligado outra vez.

Se não sabe por onde entrou, a resposta honesta é «não consegui determinar a entrada; por precaução reinstalei o sistema, repus a cópia de DATA, actualizei e mudei todas as senhas». É uma resposta que fecha o caso.

Escreveu o relatório e quer que o vejamos antes de seguir? Cole-o no pedido de suporte do aviso.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

Um aviso de abuso sobre o seu servidor: o que significa, o prazo e o que precisamos de si

Porque o seu servidor foi desligado ou bloqueado depois de um aviso de abuso, e como o religar

O meu VPS foi invadido? Ver processos, cron, utilizadores, chaves SSH e pastas temporárias

Como resolver um site infectado por malware

Depois de um ataque, que cópia restaurar? Como escolher uma cópia limpa

Manter o seu VPS ou servidor dedicado seguro: as seis que contam



Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

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