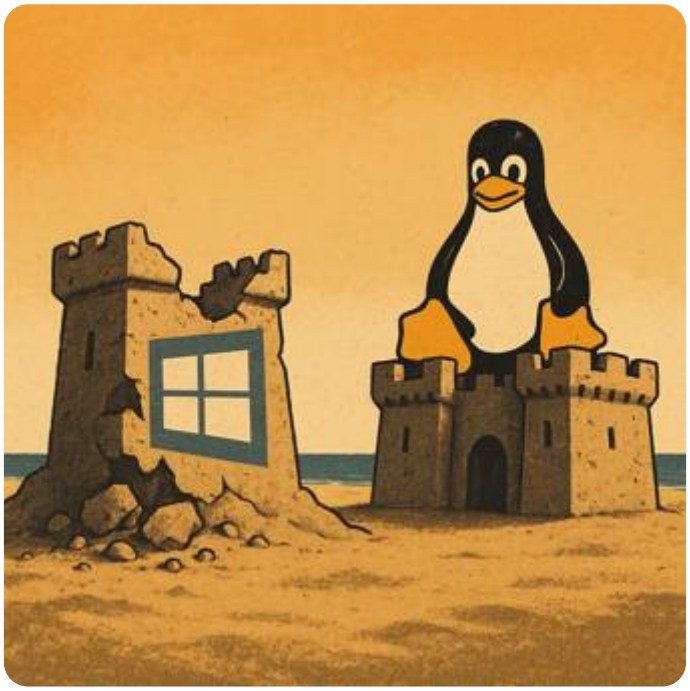
Infraestruturas tecnológicas e sistemas operativos

Publicado em 2025-09-26 10:56:44



Ataques Cibernéticos: Windows vs Linux

Box de Factos:

O ransomware *WannaCry* (2017) explorou falhas em servidores Windows e afetou mais de 200 mil sistemas em 150 países, incluindo hospitais e ministérios. Estima-se que 90% dos ataques de ransomware ainda tenham como alvo sistemas Windows.

Vivemos num mundo onde os ataques cibernéticos são mais letais do que muitas armas convencionais. Não destroem apenas computadores, mas economias, infraestruturas críticas e até a confiança das pessoas nas instituições. E quando se fala de sistemas operativos, há dois grandes universos: **Windows** e **Linux**.

Windows: a muralha de papel

O Windows, enquanto servidor, sempre foi um gigante com pés de barro. Apesar do marketing da Microsoft, a realidade técnica expõe fragilidades estruturais:

- **Herança de insegurança:** o Windows nasceu como sistema pessoal, voltado para a usabilidade, não para a segurança. Só mais tarde tentou colar camadas de proteção. É como construir um castelo em cima de areia e depois pintar muralhas de pedra.
- **Exposição a malware e ransomware:** cerca de 90% dos ataques de ransomware ao longo da última década exploraram sistemas Windows. Casos como o *WannaCry* devastaram hospitais, empresas e até ministérios.
- **Modelo de permissões frágil:** o Windows ainda hoje sofre com a tendência de conceder privilégios elevados por omissão. Um utilizador ou processo mal configurado pode transformar-se numa porta de entrada catastrófica.
- **Dependência de patches:** as "Patch Tuesdays" da Microsoft tornaram-se quase um ritual. Mas

corrigir buracos às terças não resolve o facto de os atacantes os explorarem às segundas.
- **Integração forçada:** muitas versões do Windows Server integram serviços que não são necessários (IIS, RDP exposto, etc.), aumentando a superfície de ataque.

Linux: a cidadela aberta

Do outro lado está o Linux, que reina nos servidores, na cloud e na infraestrutura crítica do mundo.

- **Arquitetura pensada para multiutilizador:** desde o início, o Linux foi desenhado para isolar utilizadores, processos e privilégios.
- **Código aberto como defesa:** o facto de o código ser público não é fraqueza, mas força. Milhares de olhos examinam-no, falhas são detetadas e corrigidas em horas.
- **Superfície mínima:** em servidores Linux, instala-se apenas o essencial. Menos portas abertas = menos ataques possíveis.
- **Diversidade:** no Linux coexistem dezenas de distribuições. Essa diversidade torna impossível a criação de um ataque universal que explore todas as variantes ao mesmo tempo.

A escolha do Castelo

No fundo, a escolha entre Windows e Linux em servidores é também um reflexo de filosofia:

- **Windows** representa o *ter*: licenças pagas, dependência de um fornecedor único, pacotes pré-fechados.
- **Linux** representa o *ser*: liberdade de escolha, transparência, comunidade.

E em segurança, o *ser* vence quase sempre.

O veredito

Não se trata de fanatismo, mas de factos: a esmagadora maioria da infraestrutura crítica mundial — desde servidores de email até supercomputadores e sistemas de satélites — corre sobre Linux. Não porque seja invulnerável, mas porque a sua arquitetura e filosofia tornam-no mais adaptado a resistir num campo de batalha digital.

> *O Windows, apesar de ainda ser usado em muitos ambientes corporativos, continua a ser a muralha de papel: imponente na fachada, frágil na essência. E num mundo onde o próximo ataque pode paralisar países inteiros, confiar num castelo de areia é suicídio tecnológico.*

Publicado por Aletheia Veritas em Fragmentos do Caos