

Prezado(a) cliente,

Esta nota tem por motivo esclarecer as causas e as ações adotadas relacionadas ao maior evento de indisponibilidade da nossa história, ocorrida das 14:30 de sexta-feira até as 01:30 da madrugada de sábado.

--

Nossa operação esta atrelada ao serviço do Datacenter Tivit – Site Transamérica desde 1998, quando nesta época operávamos sobre o nome Mundo Provedor e a Tivit se chamava Optiglobe. Dentro deste datacenter operam servidores, roteadores e switches que são de nossa propriedade conectados aos roteadores e switches do próprio datacenter antes de atingirem a rede pública de computadores (Internet), através dos 4 backbones (dispositivos que ligam o Datacenter à Internet).

A Tivit nos fornece infraestrutura predial, segurança física, rede elétrica com fornecimento ininterrupto e Link de Internet redundante em contrato com 4 operadoras distintas. E nós investimos em sistemas (Windows, Linux, cPanel, Plesk, Sistemas de Firewall, etc.), servidores, e componentes de hardware (discos rígidos, memórias, fontes de alimentação, etc.) para lhe entregar os serviços.

Para mantermos o padrão de estabilidade do nosso ambiente estamos constantemente adicionando novos equipamentos em nossa rede, para atender à novos clientes e também à novas demandas dos clientes que já estão ativos em nossa base, mantendo a carga nos servidores em um limite máximo de 50%, muito a baixo da média praticada pelo mercado nacional.

Na última quinta-feira - 23/02/2017 – instalamos novos servidores no ambiente de datacenter, e no dia seguinte, sexta-feira (24/02/2017) começamos os procedimentos de atualização de sistema operacional deste equipamento com a instalação de hotfix (atualizações de correção de bugs e segurança fornecidos pelo próprio fabricante) através de acesso remoto (do nosso escritório em Alphaville-SP conectados ao servidor operando dentro da Tivit-SP).

Às 14:00 de sexta-feira, enquanto trabalhávamos nas atualizações do novo equipamento, fomos surpreendidos com a instabilidade no Link do Datacenter que acabou sendo completamente interrompido por volta das 14:30. Imediatamente abrimos uma ocorrência com a Tivit para verificação do ocorrido, e recebemos um retorno por volta das 18:00 informando que devido a um tráfego malicioso saindo de nossa rede, a Tivit realizou um bloqueio sistêmico de nossa e também à rede de outros clientes Tivit (sem esclarecimento detalhado do que estava ocorrendo e sem informar o que a Tivit estaria fazendo para solucionar o problema, já que havia deliberadamente bloqueado toda a nossa rede), apenas foi nos passado uma previsão de normalização para as 22:00.

Após às 18:00, nosso time técnico se deslocou para o ambiente da Tivit afim de prestar assistência a equipe de NOC do datacenter e também para obtenção de maiores informações sobre a ocorrência.

Entre às 18:00 e às 22:00 nosso time técnico validou o trecho do ambiente que é de nossa responsabilidade, analisando o comportamento dos nossos switches, dos nossos roteadores e o funcionamento individual dos nossos servidores.

Às 22:00 a previsão de normalização dos acessos feita pela Tivit não foi cumprida e nosso ambiente que chegou a funcionar por apenas 2 minutos, voltou a ficar completamente sem Internet. A equipe de segurança da Tivit não conseguia nos passar nenhum tipo de detalhe do que eles estavam fazendo.

Por volta das 23:30 (após 9 horas de indisponibilidade) conseguimos fazer uma conferência com a gerência do datacenter junto a equipe técnica de NOC e **nosso time** então sugeriu a equipe da Tivit uma ação para o isolamento do problema:

- 1 - Em conferência com a equipe do datacenter através de telefone, nossa equipe no local;
- 2 - Realizaria a desconexão do cabo físico de rede de todos os servidores;
- 3 – A Tivit desbloquearia a nossa saída para a Internet;
- 4 – Nossa equipe reconectaria individualmente os equipamentos enquanto a equipe de NOC nos posicionava sobre o trafego da rede, assim conseguiríamos identificar qual era o equipamento que ao ser ligado na rede causaria o tráfego malicioso;

Não levou 20 minutos do inicio desta tomada de ação para conseguirmos identificar que era o novo equipamento, que estava em atualização as 14:30 de sexta-feira, como o causador dos problemas. Isolamos este equipamento, e reconectamos todos os demais servidores. As 01:30 da madrugada o ambiente estava operando novamente dentro da normalidade sem que nenhum cliente ficasse prejudicado, uma vez que o novo equipamento ainda estava em processo de configuração e não operava nenhuma entrega de serviço à cliente.

Este caso nos mostrou a total falta de compromisso da Tivit com a nossa operação, uma vez que os procedimentos adotados para a solução poderiam ter sido realizados ainda durante a tarde de sexta-feira, caso nossa equipe tivesse sido esclarecida do motivo do problema e que se tratava de um bloqueio feito pela própria Tivit.

Outra questão importante é que o procedimento que adotamos para identificarmos o equipamento afetado poderia ter sido feito pela própria equipe de NOC da Tivit da seguinte maneira:

- 1 – Bloqueio de toda rede do Mega Provedor
- 2 – Desbloqueio individual por servidor para que se chegasse ao IP do servidor causador do tráfego malicioso
- 3 – Manter apenas o IP do servidor problemático bloqueado para o acesso a Internet



Medidas simples expostas acima, teriam afetado o nosso ambiente por poucos minutos, isolaria o servidor problemático e não teria manchado a nossa história de 19 anos de parceria com a Tivit.

Por conta deste grave ocorrido, nos vimos sem opção à não ser interromper a parceria com este fornecedor. Que se mostrou despreparado para agir neste tipo de evento e deixou toda a nossa operação inoperante de forma deliberada.

O Mega Provedor irá migrar todo o parque tecnológico para o Datacenter da multinacional Level3 - <http://www.level3.com/pt/about-us/> localizado na Rodovia Raposo Tavares, Km 25 em Cotia – SP.

O processo de migração deverá ocorrer durante o mês de março/2017 e será planejado de modo que não cause impacto à operação. Cliente que precise realizar algum ajuste serão contatados individualmente por nossa equipe antes que qualquer ação seja tomada.

Caso você tenha dúvidas relacionadas ao problema ou as ações tomadas, sinta-se livre para nos contatar através dos canais de atendimento. Todos os chamados e e-mails enviados durante o evento, serão respondidos individualmente.

Ficamos à disposição.

Cordialmente, Daniel A. de Andrade

CEO Mega Provedor

<https://www.megaprovedor.com.br>