

Como usar redes VPN sem colocar em risco as informações de sua empresa

A Blockbit sinaliza alguns pontos importantes a serem levados em conta na hora de usar redes VPN gratuitas

22/03/2018 14:02:21

Conexões VPN (Virtual Private Network) permitem que usuários e empresas estabeleçam conexões sobre rede pública (internet) de forma anônima. Essa aparente vantagem, encoraja a procura pelo uso de ofertas de redes privadas gratuitas. No entanto, é importante estar alerta em relação a estas ofertas.

A preocupação com a segurança das informações compartilhadas por redes VPN voltou a ganhar destaque com notícias de que alguns aplicativos gratuitos poderiam inspecionar as informações e obter insights sobre os usuários.

Segundo Marcel Mathias, diretor de P&D da BLOCKBIT, o maior problema com as redes VPN gratuitas é o desconhecimento de quem está inspecionando o tráfego. É preciso entender:

- A aplicação de VPN é confiável?
- Quem está por trás da aplicação?
- Como a informação trafega?
- Como garantir de que a informação não é inspecionada durante a transmissão?
- Como garantir que a conexão não explora outros dados no servidor do usuário?

Com efeito, o principal benefício das redes VPN é a conexão segura das informações. Muitas vezes o usuário pensa que estar anônimo é um benefício, negligenciando o cuidado com as suas informações que trafegam nestas redes.

Para empresas, cujas informações são mais valiosas para o cibercrime, o uso de redes VPN gratuitas é um grande risco. Em uma rede pública o usuário e suas informações estão sujeitos às diversas ameaças cibernéticas, que têm como objetivo comum o uso de informações confidenciais para conversão em rendimentos.

Para empresas, usuários domésticos, a melhor opção é o uso de fornecedores confiáveis de VPN. Muitas vezes estas ofertas têm um custo, mas há outros benefícios mais relevantes do que o estado

anônimo:

- A escolha de um fabricante confiável;
- Há garantia de que os túneis criados são privados;
- O processo de autenticação do usuário é seguro;
- As conexões são criptografadas;
- Por política de segurança ou contrato, o fabricante não pode/deve explorar informações trafegadas, senão com objetivo de garantir segurança;
- Em caso de inspeção, o objetivo é identificar ameaças criptografadas;

Para o especialista da BLOCKBIT, a melhor forma de decidir pelo uso de uma VPN gratuita ou não é pesar os prós e contras. Lembrando que, para a maioria das empresas, os custos com o vazamento de informações podem incluir danos à reputação, perda de produtividade, gastos adicionais com recuperação de informações e sistemas etc. Salvando as proporções, os mesmos transtornos podem ser experimentados pelo usuário final.