- Defina qual a importância da disponibilidade de serviços de TI em uma empresa de vendas pela internet. Dê um exemplo de ameaça com alto escore de risco para empresas desse tipo.

Os negócios que não dão a devida atenção para a disponibilidade de TI de seus recursos correm o risco de perder tempo, dinheiro e paciência diante de problemas que poderiam ter sido resolvidos antes. Dessa forma, é fundamental observar como está a disponibilidade e atuar não apenas para resolver erros, mas também de maneira preventiva. Ou seja, o acesso precisa ser fácil, os processos precisam ser eficientes e os sistemas devem funcionar de maneira veloz, sem travar.

Por isso, o ideal é que a empresa tenha uma alta disponibilidade de TI, para evitar atrasos e erros durante seu funcionamento. Dessa maneira, muitos transtornos e perdas são evitados.

Companhias que não observam isso precisam lidar com problemas como queda de sistemas, perda de informações, indisponibilidade de servidores ou demora no processamento de dados ou na execução de tarefas. Isso acarreta baixa produtividade, baixa qualidade do trabalho e pouca eficiência.

Portanto, faça testes relacionados a disponibilidade, confiabilidade e sustentabilidade de seus recursos de TI, monitore casos de instabilidades em redes, observe pontos como dados, softwares, hardwares, entre outros itens que o time de TI poderá avaliar.

Sem dúvidas, um exemplo de ameaça de alto escore de risco para empresas que são focadas em vendas pela internet é um ataque de negação de serviço distribuído (DDoS). Nesse tipo de ataque, os servidores da empresa são inundados com uma quantidade massiva de tráfego de rede falso, sobrecarregando os sistemas e tornando-os inacessíveis para os clientes legítimos. Um ataque DDoS pode causar interrupções significativas nos serviços online da empresa, resultando em perda de receita, danos à reputação e potencial violação de acordos de nível de serviço (SLAs) com clientes.

Para evitar que este tipo de tipo de ataque, e também outros que possuem a mesma finalidade de causar algum tipo de dano para a sua empresa desse-se seguir algumas medidas de prevenção, lembrando que mesmo com as prevenções aplicadas corretamente, ninguém está absolutamente seguro, segue algumas formas de se prevenir:

1. Implemente Firewall e Filtros de Pacotes;
2. Utilize Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS);
3. Distribua a Rede;
4. Balanceamento de Carga;
5. Utilize Serviços de Mitigação de DDoS;

6. Monitoramento de Tráfego;
7. Atualizações de Segurança;
8. Testes de Resiliência;
9. Orientação e treinamento adequando aos usuários;