



## VULNERABILIDADE DE SERVIDORES

**Guilherme Martins Gonçalves**<sup>1</sup>

Anderson Santos da Silva<sup>2</sup>

Mario Oscar Steffen<sup>3</sup>

Luis Orlando Chamorro Vergara<sup>4</sup>

### RESUMO

Nenhum usuário ou dono de empresa deseja ter seus dados comprometidos por alguma vulnerabilidade de rede. Porém esses tipos de ataques já são realidade comum no mundo da tecnologia, que afetam muitas companhias, as vezes de algum modo mais grave, além de vários prejuízos em produtividade e lucros.

**Palavras-chave:** usuário, empresa, comprometidos, companhias, lucros.

### ABSTRACT

No user or business owner wants to have their data compromised by a network vulnerability. However, these types of attacks are already a common reality in the world of technology, which affect many companies, sometimes in some way more serious, in addition to several losses in productivity and profits.

**Keywords:** user, company, committed, companies, profits.

---

<sup>1</sup> Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. [guilhermemartins.m95@gmail.com](mailto:guilhermemartins.m95@gmail.com)

<sup>2</sup> Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. [anderson\\_silva@alcidesmaya.edu.br](mailto:anderson_silva@alcidesmaya.edu.br)

<sup>3</sup> Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. [mario\\_steffen@alcidesmaya.edu.br](mailto:mario_steffen@alcidesmaya.edu.br)

<sup>3</sup> Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. [luis\\_chamorro@alcidesmaya.edu.br](mailto:luis_chamorro@alcidesmaya.edu.br)



## INTRODUÇÃO

Uma empresa de hospedagem chamada Nayana, situada na Coréia do Sul, foi vítima de um ataque, afetando mais de 150 servidores de sua empresa, por conta de diversas falhas de segurança. Além de obter total controle de seus equipamentos, os criminosos possuem acesso total aos dados de seus clientes. Esse é um exemplo do que diversas empresas podem estar sofrendo a todo momento algum ataque hacker. Hoje é peça fundamental uma empresa depende tanto da tecnologia da informação, as vezes é a peça chave para o funcionamento da companhia.

Por conta disso a um crescimento muito grande em questão de ataque virtuais nos últimos anos, por conta disso estão aumentando o investimento em segurança de redes e alguns dispositivos, com isso é possível manter a empresa protegida de alguns imprevistos e ataques maliciosos.

Apesar de ser as vezes uma medida desagradável para muitos, as vezes implementação de senhas internas, para alguns acessos privados, é uma medida necessária para rastrear alguns acessos e roubos de senhas no ambiente empresarial. Ao saber com precisão quem acessou determinados arquivos, as informações ficam mais protegidas, além de permitir que o funcionário tenha mais respaldo em certos casos.

Um dos meios de backups diários de arquivos, as vezes é a melhor forma de proteger a sua empresa contra erro de sistema e também ataque de ransomware, visto que os ataques são mantidos em outro local, podendo ser recuperados conforme o que for necessário para o seu uso. É possível investir em servidores de backup ou utilizar algum tipo de serviço de armazenamento em nuvem, depende de cada caso, assim pode escolher o que é mais viável para sua empresa em aspectos técnicos e financeiro.



## CONCLUSÃO

O bloqueio automático de alguns conteúdos maliciosos ou sites que são criados com a intenção de espalhar vírus e roubar dados que podem ser utilizados por criminosos para comprometer o trabalho da sua empresa. A melhor forma de evitar isso é instalar alguns programas de segurança para bloquear conteúdos de gêneros na rede da sua empresa, outra forma é instalar softwares nos computadores para o escaneamento de downloads realizados, de modo que inutilizem possíveis malwares baixados.

Ter o sistema operacional e os programas da sua empresa atualizados é uma tarefa fundamental para a sua companhia estar protegida contra falhas de segurança. Cada vez que o seu sistema é atualizado, a empresa pode trabalhar de forma mais tranquila e com menos probabilidade de prejuízos com ataques cibernéticos.



## REFERÊNCIAS

<https://www.ethicalhacker.com.br/site/2019/08/evilgnome-novo-spyware-para-linux/> Acesso em: 25 outubro 2020.

<https://pt.wikipedia.org/wiki/Spyware> Acesso em 25 de outubro de 2020.