

Boas práticas de segurança com seu DNS

18. Monitore registros de DNS para ameaças à segurança

A maioria das conexões começa com uma consulta DNS. Todos os sistemas associados ao domínio devem ser configurados para usar o servidor DNS do Windows local.

Com essa configuração, você pode registrar todas as pesquisas DNS internas e externas. Quando um dispositivo cliente faz uma conexão com um site malicioso, ele registra o nome do site nos logs DNS.

Esses domínios maliciosos geralmente são domínios de caracteres estranhos e aleatórios que levantam bandeiras vermelhas.

Você pode registrar logs de acesso a web e validação de URLs de seus usuários utilizando softwares antivírus cloud como o Kaspersky, Panda, Norton, etc. Servidores Proxy também são excelentes para apoiar com as requisições de DNS.