Wildcard DNS

Este capítulo trata das configurações, vantagens e riscos na utilização de domínios DNS wildcard.

O que é, vantagens e riscos

Um registro DNS wildcard é uma entrada especial que utiliza o caractere asterisco (`*`) como prefixo, permitindo que qualquer subdomínio de um domínio seja resolvido automaticamente para um mesmo endpoint, sem a necessidade de criar entradas individuais no DNS. Por exemplo, uma entrada `*.dominio.ifsp.edu.br` fará com que `teste.dominio.ifsp.edu.br`, `homolog.dominio.ifsp.edu.br` ou qualquer outra combinação sejam resolvidas para o mesmo destino configurado.

Vantagens

- Simplifica a gestão de DNS em ambientes com muitos subdomínios dinâmicos;
- Reduz o trabalho operacional de criação de entradas individuais;
- Útil em plataformas que geram subdomínios automaticamente, como ambientes de desenvolvimento, plataformas SaaS e sistemas multitenants.

Riscos e considerações

Quesito de disponibilidade: Ao configurar um registro curinga (`*`), qualquer combinação de subdomínio direcionada a `*.dominio.ifsp.edu.br` será automaticamente resolvida para o endpoint definido no DNS. Assim, ataques volumétricos de requisições com este destino poderão ter as seguintes implicações técnicas:

- Isso remove uma camada natural de mitigação do protocolo e pode tornar ataques de negação de serviço (principalmente de camada 7) mais eficientes. Embora existam proteções inerentes ao protocolo (TTL, rate limiting, eventuais proteções no DNS autoritativo), o wildcard desloca a filtragem para dentro da infraestrutura interna do Campus, aumentando o consumo de recursos locais;
- Consultas a subdomínios inexistentes não serão descartadas pelo DNS e serão encaminhadas à infraestrutura do Campus;
- Isso aumenta a carga potencial sobre: servidores web, proxies reversos e aplicações backend.

Quesito de responsabilidade sobre segurança cibernética e proteção da imagem institucional: Com wildcard ativo, qualquer nomenclatura no prefixo `*.dominio` passa a "existir", gerando risco de exposição acidental de ambientes e backends de aplicações como `homolog`, `dev`, `admin`, `interno`, `banco` e `backup`, entre outros.

> Atenção ao tratamento adequado dos tipos de serviços que serão disponibilizados, seus impactos à imagem da instituição e à segurança cibernética local e institucional, que devem ser pautados pela Política de Segurança da Informação Institucional e pelas normativas do Governo Federal.

Recomendações

- Elimine serviços sensíveis expostos na internet — diminua sua superfície de ataque e aumente seu tempo de reação;
- **Jamais** permita a publicação de serviços de acesso remoto, gerenciamento de appliances e servidores diretamente na internet (SSH, Telnet, RDP, gerenciamento web, shells, etc.), assim como outros serviços sensíveis como bancos de dados, FTP, câmeras de segurança, entre outros. Em casos de necessidade, proteja estes acessos através de VPN ou de controles que impeçam o acesso pela rede pública;
- Realize as atualizações dos produtos de acordo com as recomendações de seus fornecedores;
- Revise urgentemente as versões de seus serviços expostos na internet;
- Atualize urgentemente seus plugins (ex.: nos portais institucionais e em outros softwares/plataformas locais);
- Caso esta situação dependa de terceiros, como provedores de serviços ou outros, registre esta solicitação imediatamente junto aos responsáveis.