webnames
CORPORATE

CORPORATE DOMAIN MANAGEMENT EXPERTS

BEST PRACTICES FOR DISASTER PROOFING YOUR DNS

Every single day too many Canadian businesses experience preventable DNS disruptions of one kind or another that damage their reputation, chip away at customer confidence and cause a loss of revenue. Despite underpinning almost every aspect of a businesses' online operations, including its website, business email, web applications and more, DNS will often not get the resources or dedicated attention it deserves given its business critical importance.

Reducing DNS vulnerabilities typically falls into two categories – risk mitigation in change management and building steady state operational resiliency into a DNS infrastructure. Below are seven best practices along these two themes that, if implemented, can help a business to avoid DNS disasters and bounce back faster should they occur.

Avoid the common pitfalls

Downtime can oftentimes be traced directly back to lack of process, inexperienced admins or insufficient resourcing. This is where simple organization-wide protocols can save a lot of grief. Carefully plan and conduct your infrastructure changes during appropriate maintenance windows, taking into account DNS propagation delays, which themselves can be reduced through the management of TTL values for your DNS zones. Require senior administrators to shadow junior ones throughout an important DNS migration until confidence is rock solid. Lastly, take advantage of features such as zone file controls in case changes need to be rolled back. Avoidable mistakes are at the root of many corporate DNS outages, but on a positive note, they're also among the easiest pitfalls to prevent.

Architect diversity into your mission critical services

In the case of most businesses, all of their DNS services utilize the same software. This makes you more susceptible to system wide vulnerability should downtime occur. Where DNS is concerned, running different operating systems on different hardware can increase your resistance to software bugs or malicious attacks that take advantage of common vulnerabilities.

53% of visits are abandoned if a mobile site takes longer than 3 seconds to load.

Locate your nameservers close to your users

Three seconds. According to Google, that's how long 53% of visitors will wait for a webpage to load before leaving. While DNS is not related to internet speed or optimizing your webpages for load times, it can influence how fast a webpage appears on your device. Because every millisecond counts for visitor retention, proximity of your nameservers to the nameservers that are querying them - aka your customers - can speed up access to your website and improve user experience.

Don't put all your eggs into a single basket

If you're using a single DNS provider, or running your own out of a single facility or common backbone, you've tied the availability of your entire DNS dependant infrastructure to the uptime of a single source. If it gets taken down, so will you. Remember the 2016 attack on Dyn that broke the internet and took out tens of thousands of websites and disrupted connectivity to giants like Amazon.com, Netflix, Spotify and Twitter? Remarkably, one year later 68% of the top 100 US websites DNS still did not have redundancy in place. Don't follow their lead, get a reputable secondary DNS in place ASAP.

Configure your nameservers with security in mind

Security needs to permeate all of your DNS decisions from record configuration through to server architecture given everything that depends on its stability. Protecting your DNS means implementing a combination of risk mitigation strategies and security features to counteract a range of threats like DNS hijacking to cache poisoning. From simple practices like using a hidden master and disabling recursion are followed, through to employing domain and registrar locks to prevent unauthorized nameserver changes, all the way to utilizing transaction signatures (TSIGs) and security extensions (DNSSEC) to secure communications between nameservers and verify data integrity, a highly resilient DNS infrastructure is attainable a soliding planning and organizational will.

Supercharge your DNS redundancy

With unicast servers, redundancy is provided by two nameservers (or more) in different locations. An even better option is to use cloud based Anycast DNS. When multiple, geographically distributed nameservers are located within a cloud, users automatically connect to the closest one to reduce latency. Should a nameserver go down, its automatically removed from anycast route and user requests get seamlessly forwarded to the next closest node. The best anycast configurations, including our own, also make use of two separate clouds, each with independent hardware, transit providers and IXP connections so that if there's an outage in one, the other remains unaffected.

Double down on DDoS protection and mitigation

2017 and 2018 to date have been devastating years for DDoS attacks. According to Kaspersky Labs, 33% of organizations faced an attack in 2017, and in 2018 attacks have become stronger, more persistent and sophisticated – driving up losses and remediation costs. DDoS protection for DNS servers hasn't been optional for years, but it's now more important than ever. DDoS attacks can be effectively mitigated through the redundancy offered in an Anycast DNS strategy that uses multiple nodes, clouds and networks, or through additional volumetric DDoS protection provided by an upstream provider such as your content delivery network.

Investing in the stability of your DNS will pay dividends by safeguarding you against losses in productivity, revenue, reputation and customer loyalty. To learn more about Corporate Webnames range of DNS products, including Premium DNS, Anycast DNS services and DNSSEC, and how we can assist you in implementing some of the above recommendations, call us at 1 866 470 6820.