My friend and colleagues Robert L. Gezelter, CDP, has contributed some interesting articles on the fundamental resilience of Internet infrastructure. This is the first of two articles looking at the Domain Name System.

* * *

Since 9/11, there has been a renewed concern about the robustness of network infrastructure. Advanced technologies have often been in the forefront, including fault-tolerant computing, fail-safe systems, and non-stop operations. Discussions along these lines focus on making infrastructure robust, meaning hard to damage.

Although robustness is important, perhaps “resilience”, the ability to accept distortion under stress while continuing to support load, is a more fitting description of the most crucial aspects of planning for damage contingencies than robustness (which implies a philosophy of preventing distortion or shearing and subsequently failing under stress).

When an event occurs, the mission is maintaining ongoing operation without apparent interruption. Continuation of operations and containment of damage are the philosophical, policy, and strategic goals; preferably with no perceptible user impairment. As I noted in Chapter 22 of the _Computer Security Handbook, 4th Edition_, the goal is to “avoid the phone.”

When managing the response to an event, user-reported difficulties indicate incomplete or insufficient resilience. The first reports of infrastructure problems should come from internal monitoring systems; not a flurry of telephone calls from users. This is particularly true in Internet electronic commerce applications, where the majority of users are outsiders, likely to defect to other providers or suppliers and with a justifiable tendency towards going to some other organization, rather than reporting a problem and working with an organization to fix it. In some situations, the first indication of a problem may be an instantaneously inexplicable drop in page views or customer transactions.

The Internet Domain Name System (DNS), is responsible for providing the translation between Internet names (e.g. rlgsc.com) and the IP addresses associated with the name. If the name cannot be translated to an IP address the site cannot be accessed without knowing the exact IP address.

In the case of DNS, the most publicized serious concerns revolve around the root name servers, which are admittedly a government and large-scale carrier concern; well outside the scope and authority of virtually all Internet users. Less well publicized however, are issues at the firm or enterprise-level, which are well within the control of an individual enterprise. Specifically, the organization and provisioning of the name servers for an enterprise’s domains are well within the control of the individual enterprise, and are often neglected.
One of the most common misconceptions is that your organization’s DNS resolution is the responsibility of your Internet Service Provider (ISP). However, although almost every ISP provides DNS services for its customers, the degree of flexibility, resilience, and transparency varies greatly. Some ISPs will act as authoritative secondary name servers, downloading the actual DNS zones from a user maintained DNS server; some will not. Some ISPs will provide inverse DNS services on the same basis, under RFCs 1034 and 2317, with the master data being provided by the user; some will not. Some ISPs have DNS servers at multiple sites directly connected to different backbone providers to provide resilience; some do not. And finally, the degree to which these issues are visible to the customer varies, as do the consequences for an ISP failing to provide contractually required (or for that matter, advertised) degrees of resilience.

The archetypal parachute packer’s joke, “The parachute has a money back guarantee; if it fails, bring it back” applies; the guarantee is fine, but can you ever collect on the tangible and intangible damages of the failure?

In the end, the resilience of an organization’s domains devolves to the steps that the organization is willing to undertake to ensure that its domain data remain available to the Internet. This assurance takes several forms:

* Multiple levels of (at least semi-independent) DNS servers
* Monitoring to ensure that DNS results are available to the world
* Geographic diversity of DNS servers
* Routing diversity of DNS servers
* Carrier diversity of DNS servers
* Sufficient TTL (Time to Live) to ensure adequate reaction time in the event of a problem.

***

In the next article, Bob Gezelter looks at practical advice on keeping your DNS services running.

***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 Robert L. Gezelter. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.