Network Computing
For IT By IT

GoDaddy Outage a Harsh Reminder That Enterprises Need DNS Redundancy

Posted by Gary Hilson
September 13, 2012

A six-hour outage for GoDaddy, one of the largest website hosting companies and domain registrars, affected thousands and possibly millions of customers earlier this week and serves as a warning for enterprises not to put their DNS eggs all in one basket.

The downtime was initially thought to be the work of a hacktivist who claimed credit for launching a distributed denial-of-service attack (DDoS), but GoDaddy refuted the report, issuing a statement that said the outage was "due to a series of internal network events that corrupted router data tables."

The GoDaddy outage affected websites, email and other services, essentially crippling what was the company's phonebook for the Internet.

As the foundation of the Internet, DNS affects a wide variety of services in an era where users access a great deal of information and applications online, said Christopher Stark, CEO of cloud computing provider Cetrom. DNS outages affect not just email and websites, but cloud-based applications and connectivity tools as well.

Stark said the GoDaddy outage should be a wake-up call for IT managers and CIOs who may not have sufficient redundancy for DNS. "It is standard practice to have multiple DNS servers and one or two providers," he said.

As a provider of cloud computing services, Stark said Cetrom is in the uptime business and works with multiple partners to manage DNS to guarantee availability. Enterprises should make sure any service provider they work with has sufficient redundancy for managing DNS. DNS availability should be included as part of any disaster preparedness planning, he added.

James Frey, a research director at Enterprise Management Associates, said the best option for enterprises is to take a hybrid approach to managing DNS to balance cost and reliability. "Enterprises can choose to implement DNS in-house, in which case they won't be directly affected when an external DNS provider goes down, though this approach can be relatively resource and cost intensive," he said.

Another option is to utilize an ISP for DNS, he said. "That way, they would be largely insulated from a GoDaddy-type outage," Frey explained. "But this isn't hugely popular because ISPs often can't deliver the DNS performance that external providers can." Frey said using an external DNS provider such as GoDaddy is increasingly popular for cost-effectiveness, performance and, ironically, reliability.

First and foremost, ISPs provide local connectivity to Internet services; while DNS is commonly one service that's offered, a smaller, local ISP likely won't have DNS services that are as robust or high-performing as a provider that specializes in DNS, such as GoDaddy, said Frey. "A dedicated provider will have better distributed DNS refresh, optimized performance and, ideally, fault-tolerant and redundant architectures to assure five nines of availability."

A hybrid DNS approach uses the external DNS provider for primary directory services and an internal DNS as a failsafe; internal DNS is almost always present in some form for name resolution inside the firewall, and can be extended to maintain common and heavily used external addresses, said Frey. "If the external DNS fails, the internal DNS takes over. Performance may be degraded versus the primary external DNS, but at least it's still available."

He said external providers generally tend to be pretty reliable and have good long-term performance and availability records, so once most enterprises move to external DNS, they essentially abandon any internal DNS other than for purely internal network naming. "Prudent practices indicate that a more complex configuration could eliminate the risk, but there is definitely a cost in terms of resource overhead," said Frey.

Although the GoDaddy outage was ultimately not caused by hackers, they are still a threat to DNS availability, said Stark, adding that security must be viewed at the physical, logical and methodical levels. He said without knowing the details of GoDaddy's internal setup, enterprises should make sure they have redundancy internally and externally, and address all levels of security.

Michael Hamelin, chief security architect at firewall and security policy management vendor Tufin, said there are a number of things enterprises should do to protect themselves against hackers, including a quarterly audit of firewall rules. They should also document the reasons for any firewall changes. "Even if you don't have automation in place, firewall rules have a comments field that are often left blank when people are in a rush," he said. "A very short reference to why the change was made can prevent a rule that is critical from being accidentally deleted, or make it easy to get rid of a rule that is no longer needed."

Stark said human error such as not following rules or processes can often trump resilient technology. "Assume nothing and verify everything," he said.