EXECUTIVE BRIEF

DNS Server Security Survey

Sponsored by: EfficientIP

Romain Fouchereau
June 2014

INTRODUCTION

With most organizations having some business linked to and more importantly relying on an online presence, challenges linked to DNS servers in the enterprise are one of the biggest concerns for the IT team. The results of a DNS attack can be catastrophic for any organization, resulting in business loss, stolen intellectual property, public leakage of sensitive information, and damaged reputation.

This IDC Executive Brief discusses the results of a survey conducted by IDC and EfficientIP, and looks further into the challenges, market drivers, and risks linked to DNS servers, and the threats and vulnerabilities that are inevitably linked to their deployment by organizations.

PRESENTATION OF THE SURVEY

IDC carried out a survey in three countries — France, the U.K., and the U.S. — and gathered information from 244 interviews across multiple verticals and enterprise with 500 employees or more that have deployed a DNS server in their organization, with the aim of gaining insight into thought leadership around IT security (with a particular focus on DNS security).

The country split was distributed as follows: France represented 33.2%, the U.K. 34.4%, and the U.S. 32.4%. When aggregated, the verticals were represented as follows: the public sector 26%; services 21.9%; transport, communications, and utilities 17.7%; finance 11.5%; and manufacturing 10.4%. Company sizes included 5,000 or more employees at 32.3%, 1,000–2,900 employees (31.3%), 500–999 employees (21.2%), and 3,000–4,999 employees (15.2%).

KEY FINDINGS OF THE SURVEY

The survey was divided into the following sections: security products; DNS infrastructure in the organization; how the DNS servers are managed; the threats, vulnerabilities, and attacks linked to DNS servers; and what policies and plans are in place in case of attack.

Security Products

More than a third of the companies surveyed had over 5,000 employees, and 35% had over 20 sites in their own respective countries. In a majority of cases, the purchasing decision, deployment, and management of security products are made in-house, by the IT team (general, network, or dedicated security teams).

Confirming what IDC has been seeing for many years, the most important criteria when deploying new security products are lower total cost of ownership (TCO), ease of use, and reduced downtime when installing the new products. This confirms the success of security appliances in the enterprise over pure security software, as they meet all three requirements.

A very high percentage of organizations had security appliances running on their network, but surprisingly, unified solutions (UTM or next-generation firewall) didn't take the lead in pure network security, as dedicated firewalls were still ahead with 68%, against 37% for UTM or NGFW, when IDC saw the UTM (and NGFW) market representing over 62% of total security appliance shipments in 2013 in the three surveyed countries (according to IDC's Worldwide Security Appliance Tracker results).

DNS Infrastructure and Management

While all the respondents have a DNS solution in their organization, 77% have an internal DNS server running within their local network and 71% have an external DNS server that they manage.

TABLE 1

What Types of DNS Server(s) Are Currently Installed in Your Organization?

	U.K.	U.S.	France
Appliance-based server	26.0%	34.0%	19.0%
Linux-based server	36.0%	39.0%	42.0%
Windows-based server	75.0%	80.0%	72.0%
Cloud DNS	24.0%	42.0%	26.0%
Hosted DNS	13.0%	19.0%	17.0%

Source: IDC, 2014

Just as in most other IT areas, cloud solutions are more common in the U.S. than in European countries for now, but many of the respondents had cloud-based DNS either running as a test or are planning to move there in the near future.

Table 2 shows which DNS appliance software technologies are deployed on the companies' servers (note that different technologies can run on different sites in the same company).

TABLE 2

What Type of Software Technology is Running on Your DNS Server?

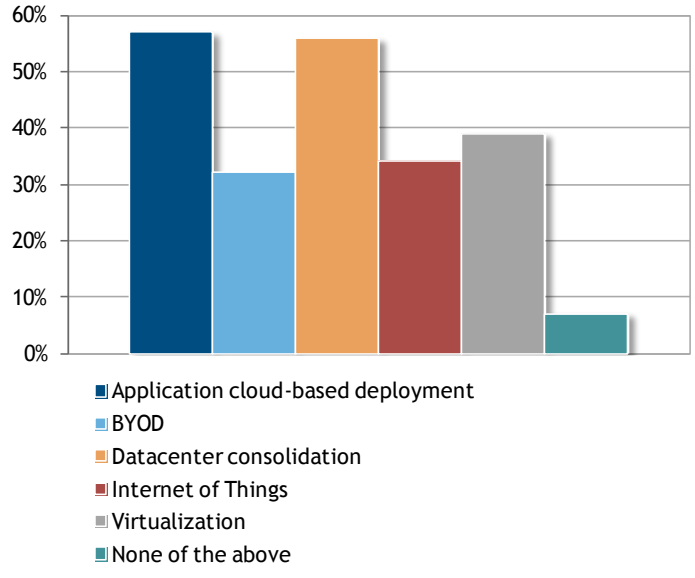
	500–999 Employees	1,000–2,999 Employees	3,000–4,999 Employees	5,000 or More Employees
BIND	25%	15%	17%	13%
Cisco Network registrar	62%	58%	51%	46%
DJBDNS	25%	22%	24%	6%
Knot	21%	21%	24%	11%
Microsoft DNS	56%	57%	61%	61%
Nominum	19%	16%	15%	6%
NSD/Unbound (NLNetLabs)	21%	16%	17%	12%
Posadis	10%	4%	12%	8%
PowerDNS	10%	6%	5%	11%

Source: IDC, 2014

As shown in Figure 1, the rise of cloud solutions, connected devices, and BYOD (bring your own device) are big market drivers for DNS solutions, as many organizations are planning to deploy DNS-related projects on their networks in the next three years.

FIGURE 1

Which of the Following DNS-Dependent IT Projects Do You Plan to Deploy in Your Organization in the Next Three Years?



Source: IDC, 2014

Most organizations manage their DNS servers in-house through their IT teams (57%), network team (37%), or dedicated security teams (30%), with only 5% of respondents using their ISP to manage them. The U.S. had the largest response in terms of having already deployed multiple technologies as a best practice, with 39% already using them as standard. The main reason for the reluctance in having multiple DNS technologies remains the fear of a complicated set-up, management, and maintenance process (cited by 50% of respondents).

A similar problem emerges with cloud solutions – 52% of organizations still prefer to have their DNS on premises and 48% said they had not deployed such solutions because they do not trust data in the cloud. 85% of respondents have the basic DNS security functions from their security appliance turned on – a very high percentage per se, but not a very good solution as these functions usually can do nothing during an attack.

Threats and Attacks

Organizations, though aware of the existing threats and the damage these can cause, when first asked do not see them as a major risk for their organizations, with almost 40% across all three countries only seeing it as somewhat dangerous (Table 3).

TABLE 3

How Would You Evaluate the Threat of an Attack on DNS Servers in General?

	U.K.	U.S.	France
1 = Not a threat at all	2%	3%	5%
2	14%	5%	25%
3	37%	33%	46%
4	37%	33%	17%
5 = Very significant threat	10%	27%	7%

Source: IDC, 2014

When asked in more depth about each threat, the average answer shifts from moderately important to very/extremely important.

TABLE 4

Percentage of Respondents That Believe a DNS Attack Likely to Create High to Very High Impact on Their Business (by Enterprise Size)

	500–999 Employees	1,000–2,999 Employees	3,000–4,999 Employees	5,000 or More Employees	All Cases
Legal issues	57%	55%	51%	59%	56%
Reputation damage	54%	67%	71%	65%	64%
Business continuity	67%	68%	68%	75%	71%
Sensitive customer information leakage	71%	65%	73%	71%	69%

Source: IDC, 2014

In terms of attacks, Table 5 shows that only 28% of all respondents said they had not been the target of a DNS attack in the last 12 months; the rest said their business had been impacted by downtime, a compromised website, or by having sensitive information publicly released.

TABLE 5

Which of the Following DNS Attacks Has Your Organization Been Subject to in the Past 12 Months?

	U.K.	U.S.	France	All Cases
Cache poisoning (data corruption)	23%	34%	20%	25%
DoS/DDoS (distributed denial of service)	25%	32%	27%	28%
DNS amplification attacks	39%	43%	37%	40%
DNS exploits	17%	28%	31%	25%
Registrar hijacking	10%	15%	15%	13%
Other	0%	0%	1%	0%
No attacks have been experienced	32%	24%	27%	28%

Source: IDC, 2014

TABLE 6

What Was the Impact for Your Company?

	U.K.	U.S.	France
Downtime	47%	45%	44%
Loss of business	32%	45%	31%
Compromised website	49%	48%	42%
Intellectual property stolen	39%	40%	41%
Sensitive information publicly released	11%	38%	31%
Sensitive customer information stolen	4%	15%	15%
Other	0%	0%	3%

Source: IDC, 2014

The methods used to mitigate the effects ranged from shutting down the server (33%), to attempting to throttle or block the DDoS traffic (27%), adding new network bandwidth (35%), switching to an alternate site (38%), closing down specific processes and connections (39%), disabling some applications (36%), asking for the ISP's help (20%), getting assistance from a service provider (18%), and applying a patch to fix the security hole used to carry the attack (14%).

Policies and Plans

In the event of a threat, only 4% of respondents have no policy at all to mitigate the attack on the DNS server, as seen in Table 7.

TABLE 7

What Policies Are Currently in Place in Case of DNS Attack?

	U.K.	U.S.	France
Policies in place through my ISP (mitigation service through them)	44%	41%	37%
List of priority traffic to authorize in case of attack	51%	59%	36%
Specialized products/services implemented against DDoS attacks	49%	49%	44%
Backup site	44%	57%	53%
Bring more power/more servers online	7%	14%	17%
Other	0%	1%	2%
No policies	4%	4%	4%

Source: IDC, 2014

When asked why they had no DNS server security in place, 67% of organizations in the U.K. and the U.S. said it was under review and would be implemented in the near future; 33% in the U.K. and France said it was for budget reasons; and a surprising 67% of French companies said they were satisfied with the basic protection offered by their firewall or intrusion-detection solutions.

These results show how little is actually being done by organizations to protect themselves. Most have been under attack in the past year, with severe consequences for their business, yet very little is being done about it and they feel that the basic protection offered by a firewall is enough. This is a real case of the wrong answer to a real problem. Firewalls are not the right technology to fight zero day vulnerabilities on DNS servers or when they are under DNS DDoS attack, as they will have no effect.

DNS Server Challenges for the Enterprise

Most companies do need an online presence to remain relevant and to stay in business, and therefore DNS servers are becoming an essential component of organizations' network infrastructures. But DNS servers and specifically how to secure them are not seen as critical and are often taken for granted through the basic security features offered by the traditional network security elements already deployed on the network, such as firewalls and intrusion detection and protection.

The main challenge for the enterprise is to identify the problems and/or threats they potentially face if they are under DNS attack, and to take action to prevent and mitigate the effects. Companies often do not know how many DNS servers are sitting on their networks, and very often there are many more DNS servers than the official number. There is also a severe lack of security investment in DNS in general that creates significant opportunities for hackers.

DNS Technology: Current State and Market Drivers

Most companies are aware of the threats, but in terms of DNS security, it really is a case of "too little, too late," when measures and solutions really should have been implemented before an attack. Often there are no real policies put in place; this is a common security problem, with prevention being the key word.

The market will continue to grow through education from vendors and ISPs, and as attacks continue to become more complex and more directly targeted at companies' core business – their intellectual property.

As with many other IT sectors, the security and DNS market is growing due to the rise of the "3rd Platform," a shift in technology that creates new IT capabilities including mobile devices and apps, cloud services, mobile broadband networks, Big Data analytics, and social technologies. According to IDC, this new platform will drive 90% of growth in the ICT market to 2020. The need for an online presence creates the need for DNS technologies for businesses to continue to run and grow.

The Importance of Policies and Response Strategy Implementation

Organizations really need to set up clear policies around their DNS security to prevent attacks and they need a strict strategy to follow in the event of such attacks, as they can have a dramatic impact on their businesses.

To protect against DNS-linked attacks and threats, organizations need to go through four stages:

- **Assess:** assess the network and establish where the risks can come from
- **Protect:** protect the network with the help of DNS hybrid technology and simplified DNS server deployment and management
- **Implement response strategy:** have a clear response mechanism in place in case of attack (throttle or block the DDoS attack, switch to alternate site and/or server, add power or servers)
- **Analysis:** it is important to analyze where the attack came from, identify the weak point, and assess how the response mechanism in place functioned and how to adjust it accordingly for the next attack

Hybrid Solutions, Multiple DNS Technologies, and High-Performance DNS

One of the most effective ways of protecting the network from DNS attacks is to use hybrid multiple technology DNS servers. This new type of solution really benefits customers as it allows them to mitigate zero day vulnerability by switching from a vulnerable technology to a more secure technology – "sound-proofing" for the future by addressing the ever-evolving nature of attacks.

Simplicity is another key word – one of the interesting findings from the survey was that respondents were wary of deploying new DNS solutions because of their complexity. Management and deployment of new DNS servers need to be simplified for the IT team, without adding cost, through centralized management consoles.

To illustrate this reluctance, the survey showed that 50% of the IT teams not planning to deploy multiple DNS technologies on their DNS servers said they prefer to use only one technology on site; another 50% said DNS technology implementation is too complicated to set up, manage, and maintain.

The Future of DNS Server Technology

The number of IP addresses for organizations will continue to grow exponentially with the Internet of Things, and threats will become increasingly sophisticated. Enterprises need to invest in the right DNS server technology to protect themselves – IDC believes that the future of DNS is in offering multiple technologies that are easier to use and manage. Also, having faster throughput (increased amount of requests per second accepted) and a hybrid on-premises and cloud-based approach to relieve some of the on-premises work will remove the need for further investment and the deployment of additional DNS servers or load balancers, and will create a better return on investment for organizations.

Some interesting results from the survey show that a good percentage of organizations in all three countries and across all verticals are thinking about, are already testing, or are using as standard for new projects multiple DNS software technologies on their DNS servers; we have seen similar results from DNS cloud implementations. Tables 10 and 11 confirm that hybrid multitechnology DNS servers are also what end users see as their long-term investment plans.

TABLE 8

Which of the Following Statements Best Describes Your Views Toward Best Practices for Implementing Multiple DNS Software Technologies on Your DNS Server Estate?

	U.K.	U.S.	France
Not aware of such best practices	7%	4%	15%
Not using, nor planning to use in the future	7%	4%	6%
Not using, but am interested in such a solution and plan to evaluate	30%	19%	14%
Not using, but in early evaluation stage	13%	9%	9%
Using in small, isolated areas (test and development, pilots)	29%	25%	42%
Using as the standard form of deployment for new applications	14%	39%	15%

Source: IDC, 2014

TABLE 9

Which of the Following Statements Best Describes Your Views Toward DNS Cloud Implementation?

	U.K.	U.S.	France
Not aware of DNS cloud	5%	4%	12%
Not using, nor planning to use in the future	13%	10%	7%
Not using, but am interested in such a solution and plan to evaluate	23%	23%	10%
Not using, but in early evaluation stage	20%	11%	19%
Using in small, isolated areas (test and development, pilots)	27%	28%	40%
Using as the standard form of deployment for new applications	12%	24%	12%

Source: IDC, 2014

EfficientIP's Portfolio and Solutions for the DDI Threats and its Challenges in the Market

French company EfficientIP is a major player in DDI solutions, and more specifically in the DNS technology market with its range of hybrid DNS appliance solutions:

- DNS Blast
- Hybrid DNS Engine (SOLIDserver DNS appliance)
- NetChange – IPLocator
- Device Manager

EfficientIP's hybrid technology incorporates another DNS engine to the main BIND, offering greater reliability in the event of an attack. Administrators can switch from one server technology to the other, offering an immediate solution to the vulnerability problem.

To increase product recognition and awareness of its solutions, EfficientIP should continue its communication and brand awareness strategy around hybrid DNS security, faster throughputs, simple administration tools, and risk management.

The difficulty will not be for end users to understand the necessity of protecting their DNS servers with multiple technologies, but rather convincing them that it will not be too costly or difficult to implement in their existing infrastructure. As for cloud-based solutions, companies need to get over their general mistrust of not having their data on the premises, though this is already changing (with more adoption in the U.S. than in Europe); this is a valid point for all cloud-based solutions, as it not only relates to security products.

CONCLUSION

IDC believes that most end users are aware to a point of the risks linked to DNS servers (82% of survey respondents were aware of and recognized the threats), but most of the budget and time is still spent on more traditional network security, and they still rely on basic security functions provided by their other security solutions. It is also essential that companies use efficient protection on their DNS servers and not only rely on firewalls that will be of very little help in the event of an attack.

Although we saw from the survey that organizations are thinking about deploying multiple technology DNS solutions in the near future or are already testing them in some areas, it is still a concern for some organizations. Vendors need to continue their discussions with end users and work on delivering simple and easy-to-use platforms to deploy. With businesses relying on online transactions and hosted services, and with the inevitable rise of BYOD, cloud computing, and the Internet of Things, more education is needed about real, effective solutions (as firewalls and IDP only offer basic security for DNS servers), as well as policies and response strategies that need to be put in place before that major attack hits the network.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

Chiswick Tower
389 Chiswick High Road
London W4 4AE, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-insights-community.com
www.idc.com