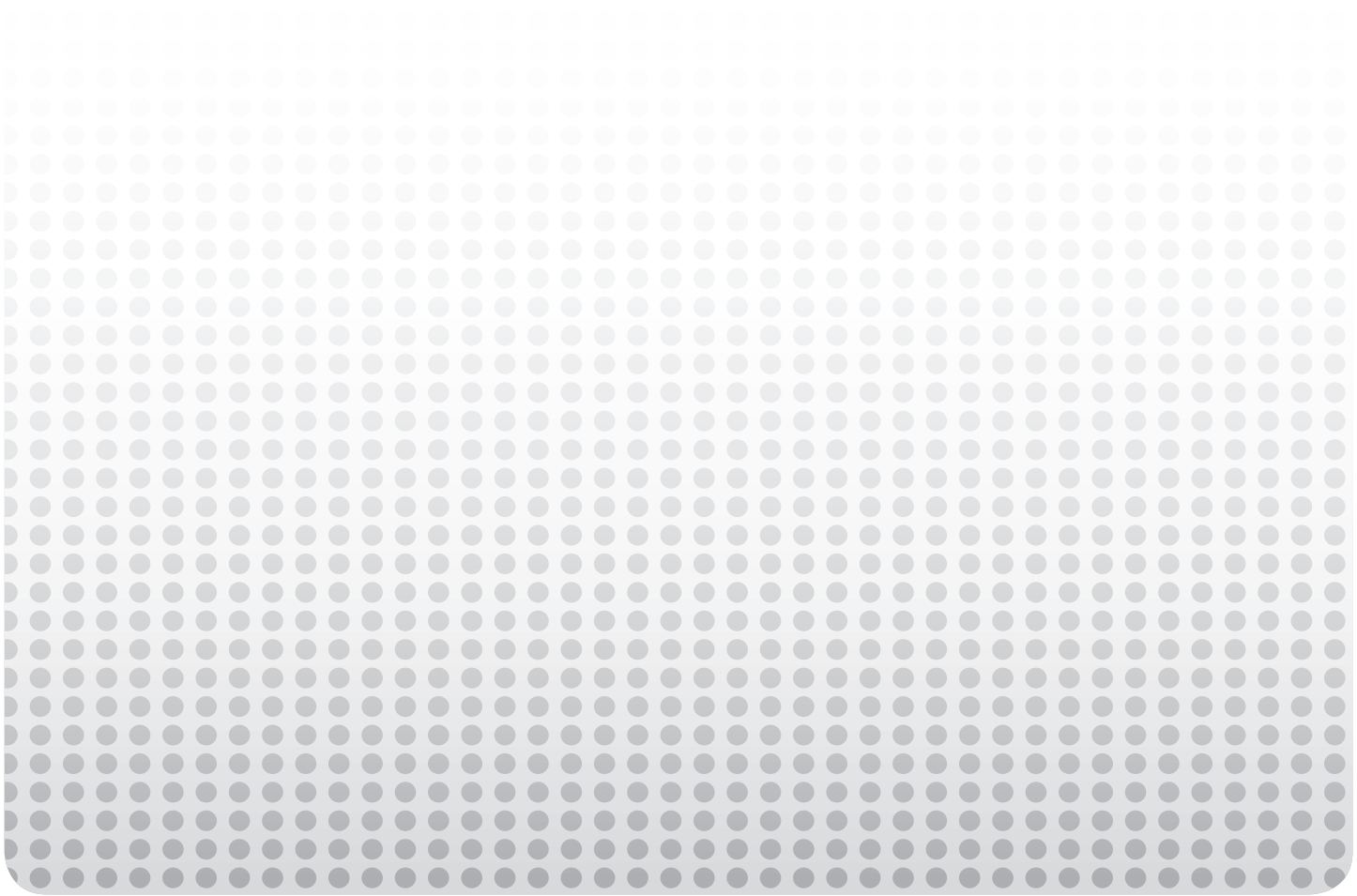
ALVEA™ SERVICES

PROTECTING CRITICAL WEBSITES AND INTERNET INFRASTRUCTURE USING INNOVATIVE CLOUD-BASED DOMAIN NAME SYSTEM MANAGED SERVICES



BUSINESSES DEMAND INTERNET CONNECTIVITY, SECURITY AND RESILIENCE TO ACHIEVE SUCCESS

Loss of access to critical Internet resources can lead to both financial losses and long-term damage to a business' reputation. By using innovative cloud-based technology, ALVEA Services™ is helping organisations reduce the cost of protecting their IT, without the need for major capital investment or deep technical knowledge.

INTRODUCTION

The Internet is possibly the most critical resource for the UK's four million public and private sector organisations. As an information-driven economy, the UK is growing increasingly dependent on Internet connectivity as tasks previously driven by call centres or surface mail move online.

Behind the scenes, the UK has a complex infrastructure that allows citizens and businesses across the country to process millions of Internet related requests and data exchanges every second.

The loss of Internet connectivity, even for a few minutes, can dramatically and negatively impact organisations of all shapes and sizes, leading to significant financial loss or damage to reputation.

In response to the criticality of the Internet, many organisations invest heavily in IT security, resilient technology and business continuity. However, as reliance on the Internet grows, the fundamental ability of users to connect with online resources is under threat from increasingly targeted cyber-attacks. Criminals and hacktavists are targeting the core naming system used by every aspect of the Internet to steal sensitive information, disrupt legitimate web traffic, deface websites and harass vulnerable businesses online.

This white paper is designed to provide an overview of the technology, threats and possible solutions to help organisations start the process of better protecting their critical information technology systems.

Every responsible business leader should have at least a basic plan in place to help protect their business, staff and customers against potential disruption. The time and expense of creating even the most basic contingency plan is well worth the effort, as in these uncertain times it pays to be prepared.

THE DOMAIN NAME SYSTEM

The UK is one of the largest hubs on the Internet with over eight million Internet hosts and more than ten million .co.uk domains. Websites like bbc.co.uk and dailymail.co.uk are ranked in the top 100 English speaking websites in the world; quite an achievement considering there were over 610 million websites as of March 2012.

Although users think of websites in terms of the brand's name like BBC, Facebook or YouTube – underneath these names are IP addresses that are much less recognisable. For example, the BBC website is actually an IP address that translates to 212.58.244.71.

To make matters more complex, every Internet-connected device can also have a unique address out of roughly four billion possible combinations. However, with the growth of phones, pads, games consoles and other connected devices the existing 32bit IP v4 system is running out of addresses and moving to a 128bit equivalent. The new IP v6 will allow 340 trillion trillion trillion possible IP addresses.

Irrespective of whether we have billions or trillions of IP addresses, humans will continue to deal with names rather than complex numbers. The underlying infrastructure also needs a system to allow requests to be routed around this increasingly large worldwide Internet map. This Domain Name System (DNS) makes using the Internet easier by converting IP addresses to names, but this system is vulnerable to criminals, hacktavists, vandals, governments and good old fashioned human error.

Although DNS is a considerable convenience, the system can also be used to balance the load between multiple websites or other online resources. This process, known as 'round-robin' DNS, can help improve the visitor experience or ensure that traffic is pushed to redundant servers in the event of a primary server failure. The DNS system can also be manipulated to ensure that users are always able to connect to websites that are going through planned migrations or upgrades. Lastly, DNS is also a fundamental component of modern email systems.

ALVEA™ SERVICES

VULNERABILITIES AND RISKS TO THE DNS SYSTEM

Losing Internet connectivity is more common than you might imagine. Cables are damaged by construction and roadworks, underground conduits flood or catch fire, cabinets can be vandalised or key switching equipment can simply fail. Any wire-based Internet service or dedicated leased line can be subject to interruption and the loss of Internet connectivity can lead to lost revenue, productivity and damage to reputation.

So on a planet with more than 600 million websites, 15 billion Internet connected devices and trillions of data items sent every second, the DNS system which governs much of this communication is ultra-critical. Thankfully, the DNS system is not owned by a single entity but instead this combination Internet 'map' and translation system is distributed across the globe. The system is built as a hierarchy with 13 main 'root' DNS servers and an additional 130 distributed copies of these roots spread across 25 countries. There are a further 18.5 million DNS servers that contain either routing for private enterprise usage or parts of this Internet map.

This distributed architecture is designed to make the system resilient and allow data from every corner of the globe to find the right destination. However, the original DNS system was designed in the early 1980s and has stayed roughly the same over the intervening three decades. This stability has helped the Internet to grow but DNS was not designed with much inherent security and over the years, vulnerabilities have been discovered and exploited.

Cache Poisoning

To speed up the process of connecting the points on the Internet, the DNS system has lots of local copies of itself held in regional caches. These caches reside at ISPs, within company networks and even individual browsers retain caches of frequently accessed website IP addresses. This improves the performance of the Internet, and reduces the load on the various 'authoritative' or root DNS servers. However, these caches can sometimes be vulnerable to 'poisoning' attacks.

By exploiting bugs, local malware or poor configuration of DNS servers, external agents can inject fraudulent addressing information into caches. Users accessing the cache aiming to visit a targeted site would instead be redirected to a server controlled by the attacker. This could be a fake banking site that offers a close replica of the target's official site, potentially tricking users into divulging sensitive information. This is not just theoretical. In 2009, users visiting twitter.com were instead presented with a banner from the 'Iranian Cyber Army', a previously unknown group that had poisoned DNS entries to point users to their site. Cache poisoning can take place at the ISP level and cause an impact across several websites. For example in 2011, another major poisoning incident hit the websites of National Geographic, BetFair, Vodafone and Acer.

But acts of vandalism are the least of the potential worries. Cache poisoning is often the start of 'man in the middle' attacks where criminals redirect all traffic destined for a legitimate website via an intermediate server that can steal confidential information before sending it on to the legitimate server.

Distributed Denial of Service

Alongside sending users to the wrong place through cache poisoning, another common type of attack is stopping users from accessing a targeted website. This can be achieved by flooding a victimised website with huge volumes of bogus traffic to stop legitimate users from entering. Distributed Denial of Service (DDoS) attacks are typically perpetrated against a specific website but they have also been attempted against DNS service providers. More worryingly, new vulnerabilities allow these attacks to be amplified by the DNS system itself.

In 2012, the hacking group Anonymous claimed it planned to attack the entire DNS system; a claim rejected by experts based on the highly distributed nature of the system. However, newer types of attacks called DNS amplification or reflection attacks are a method of fooling a DNS server into generating lots of traffic, which can shut down access to DNS services for a connected user. In 2010, DNS Made Easy, a provider of DNS services, experienced 1.5 hours of downtime during an attack, which lasted eight hours. Amplification attacks that exploit the DNS system are a worrying trend as it is difficult to gauge how many DNS servers are vulnerable to this amplification vulnerability.

PROTECTING ONLINE ACCESSIBILITY

In the same way that many organisations backup important data or maintain redundant servers for critical websites, a growing number of organisations are also protecting accessibility. The DNS system is one of the most fundamental elements of Internet connectivity and also has an important role to play in preventing denial of service attacks. However, correctly managing DNS can also provide benefits in terms of resource efficiency, better user experience and service reliability.

Although the DNS system is a hierarchy, organisations can choose to run their own DNS servers to manage private web-based resources inside the firewall and communicate with the wider external DNS infrastructure. Organisations typically choose this route to give them more configuration options and to build flexibility and redundancy into their internal network. If they are sufficiently large, this additional control can offer operational and security benefits.

However, analysts such as the Yankee Group estimate that over 85 per cent of enterprises that manage DNS in-house do not have dedicated DNS staff. Also managing the entire DNS stack internally requires having enough resources to deal with spikes in traffic and expertise to deal with 'moves, adds and changes', as well as increasingly complex attacks against DNS.

In the event of an outage, an internally managed DNS system needs to have redundancy. This level of resilience is expensive and complex and therefore not a realistic option for all but the largest organisations.

So instead of doing DNS completely in-house, most organisations will rely on an ISP to handle some or all of these services on their behalf. This provides the benefits of economy of scale and often more resilience. However, DNS management is not a core business for ISPs and few will offer the extended services that can be delivered from in-house alternatives. ISPs are also regional, and by their very nature subject to local disruption.

The most prevalent trend for organisations that require the flexibility and additional features of an in-house DNS solution but the reliability of an ISP is to use a dedicated DNS managed service provider.

WHY CHOOSE MANAGED DNS SERVICES?

In a similar vein to the growing trend towards cloud services and remote backup, managed DNS services are built from the ground up to focus on a single task for an aggregate of users. The service model offers several key advantages in terms of security, resilience and performance when compared to in-house and ISP alternatives. Many DNS service providers will also offer additional features that can provide benefits around end-user experience and reporting, and typically charge on a pay-for-usage model, which requires minimal upfront expense.

A dedicated managed DNS service can defend against cache poisoning and DDoS attacks and includes a DNS security feature called DNSSEC that authenticates that users are communicating with the intended server and not a forgery. These services tend to run a wider range of threat prevention and detection systems with a fall-back position to mitigate the most serious of unforeseen disasters. This will include geographically dispersed servers, multiple paths and staff that constantly monitor systems.

Dedicated DNS services will also use newer IP ANYCAST technology that can deliver a consistently higher performance from any location under any traffic load conditions. This allows DNS to resolve queries at the closest or least congested server, to improve response time.

Like any other managed service, DNS providers will offer an SLA and tools to allow management and reporting. This is normally performed via a web portal to set up policies and gather service insights. This management capability should be considered as part of a wider business continuity strategy. For example, if a website experiences an outage or security breach, the DNS service provider can quickly provide re-routing or DNS changes to remedy a situation.

A COMPLETE MANAGED DNS SERVICE

ALVEA Services has partnered with Neustar UltraDNS to provide ALVEA DNS Managed Services. Powered by a global, cloud-based DNS network, it fuses proprietary technologies and unmatched expertise on a network used by over 3,300 customers, including Tesco, Allianz and 60 per cent of the Alexa Top 100 websites. The solution integrates seamlessly into any existing network and relieves businesses of complex DNS management while increasing reliability, security and performance.

Performance

The ALVEA DNS Managed Service is built on a global platform consisting of strategically placed network nodes that use an Oracle database-driven infrastructure to ensure DNS requests are resolved with the latest data. Instead of the Traditional DNS infrastructure, which routes requests randomly, ALVEA DNS Service requests are routed to the nearest available geographic network node through IP ANYCAST and proprietary technology.

For more precise traffic routing, the ALVEA DNS Managed Service offers weighted load balancing that directs web traffic at the DNS level to spread demand across multiple datacentres and servers in different locations. By evenly distributing traffic, it ensures no one server is overburdened by sudden activity. The combination of technologies ensures customers receive the quickest, most accurate DNS response every day.

Reliability

The ALVEA DNS global network rapidly detects outages by continually monitoring server performance against pre-defined thresholds. The ALVEA DNS service tests connectivity from various points across the Internet and if a test fails, it concludes the corresponding server is down and initiates server failover. This failover mechanism involves automatically modifying the DNS response record for the monitored server. When a server goes down for whatever reason, DNS requests are re-routed to backup resources, ensuring traffic keeps flowing. However, when the server has been restored to service, ALVEA DNS Failover automatically recognises the server's online status and restores it to service by replacing the DNS response record with the original set.

Although often considered as a reactive service to ensure reliability, ALVEA DNS Managed Services can also be used for manual failover in emergency situations such as a cyber-attack or security breach. In less frantic instances, the system can also assist in scheduled failover for planned maintenance or webserver migration projects.

Security

The ALVEA DNS Managed Service also has built in protection against DDoS attacks. The technology mitigates costly and crippling attacks by criminals, hostile nations, political activists and angry consumers. Instead of huge volumes of spurious data taking down websites, email and other essentials, ALVEA DNS Managed Services repels the most common and dangerous DDoS attacks, using global 'scrubbing centres' to clean out harmful traffic. The cloud-based solution can scale as needed to ensure there is always enough bandwidth to ward off large-scale threats.

Reduced Cost

ALVEA DNS Managed Services benefit from a cloud-based model that requires no upfront investment in on-premise equipment, overheads for patching and updating hardware and software, and no system maintenance costs. IT departments benefit from simplified administration as the ALVEA DNS Managed Service manages responsibility for DNS while maintaining control and ensuring consistent, accurate resolution of all their Internet domains.

Greater Control

The cloud model still allows end users to stay in control through a secure web portal that provides the tools to keep each DNS environment accurate. Whether it is the addition of a new domain, customising 'Time To Live' (TTL) settings for a specific DNS resource record, or viewing usage reports, the management portal provides controls to administer your infrastructure easily and securely.

On-going Support and Compliance

As a business grows or needs change, the ALVEA portal adapts as required. The platform is designed to require little administration. All services are fully backed by stringent SLAs and are supported by experts based at the ALVEA Network Operations Centre, 24x7x365. ALVEA Services comply with ISO 27001, to ensure they meet security best practice, and the ISO 9001 standard to deliver quality management across its operations.

ALVEA™ SERVICES

WHERE TO GO FOR HELP

Even though the majority of the emerging cloud services are designed for self service, many small and medium businesses prefer to outsource much of the IT process to trusted third parties. In many cases, these value-added resellers, independent IT consultants or even larger managed IT service providers will have a much better understanding of the customer environment, as well as experience in implementing DNS and business continuity solutions.

Before rushing into any cloud service, it is always recommended that firms talk to these trusted IT suppliers who can provide an impartial assessment of its strengths, weaknesses and overall value for money. In many cases, these same trusted advisors may well have complementary services or skills to quickly setup systems, as well as on going management expertise.

ALVEA Services has a partner community of both larger and smaller IT service providers across the UK. These are organisations that offer a wide range of solutions from multiple vendors and can provide a full consultancy and support service.

ALVEA partners can also offer practical advice on how to protect critical business infrastructure based on a wide variety of budgets. ALVEA Services are able to grow or shrink as needed and allow systems to be managed by a trusted third party.

One of the key advantages of the ALVEA DNS Managed Services and Business Continuity portfolio is the integrated nature of the constituent parts. By using the power of modern technology – on-premise appliances and a cloud – ALVEA provides a unified portal to help businesses build an easy to manage solution with minimal capital outlay or technical expertise.

ALVEA™ SERVICES

Contact ALVEA

w: www.alvea-services.com
e: info@alvea-services.com
t: +44 (0)1638 569 889