

Securing The UK Internet:

Applications Of Domain Based Security

Abstract

The internet is relied upon by a large number of individuals and businesses within the UK. Recently, the problems of hacking, viruses, and 'spam' emails have presented users with the darker side of the internet where crooks seek to find modern methods of perpetrating crimes, and unethical sales-people blast their adverts to all, regardless of the wishes of the recipients. This paper presents a new architecture for the UK portion of the internet, based on the successful Domain Based Security model, that could provide the electronic safety and assurance that the UK requires.

1 Introduction

The internet is a remarkable business resource, supporting global instant email and immediate access to vast quantities of useful information. It can provide inexpensive Wide Area Networks (WANs) through the use of Virtual Private Networks (VPNs) to join geographically separated company offices; it can provide remote access for road-based employees; and it can facilitate efficient access to Government departments through revolutionary programmes.

The internet also comes with a price, however. The practically zero cost of sending email has resulted in its use for unsolicited electronic junk mail, known as 'spam'; new and more powerful viruses are appearing everyday that have the potential to destroy your data and, realistically, your business; the abundance of hacking material has led to a sharp increase in the numbers of amateur hackers furnished with devastating tools and unsociable intent; and the practically anonymous nature of the internet has provided those with undesirable interests the ability to browse and publish pictures and information that are illegal in the UK.

If one combines these activities with the complex nature of international computer and privacy laws, then one may realise that when crimes are committed across international boundaries the chances of prosecution are low. Low rates of prosecution generally lead to a low deterrent, which in turn leads to higher rates of crime. It is the vast geographical coverage of the internet, one of its greatest benefits, that has led to its effective lawlessness and, in turn, the threats it poses to UK businesses and individuals.

The lack of deterrent has applied more emphasis to prevention, a set of activities that are currently the responsibility of those with assets to protect, as opposed to the state. The de facto standard for all UK corporate connections to the internet involves the use of a firewall, a virus scanner and, often, an anti-spam filter. There are no cyber-cops patrolling the cyber-beat, looking for suspicious activities.

2 Tough On The Source Of Crime

The greatest challenge to the protection of UK plc from the attackers on the internet is the ability to prosecute and, therefore, deter illegal activity. Whilst hacking is illegal in the UK it is not necessarily illegal in other countries; hackers in other countries are effectively exempt of UK laws. This characteristic may be exploited by UK-based hackers by routing their attacks via other countries. Whilst this may sound like science-fiction or the plot of a mainstream movie, it is actually relatively simple to an average hacker.

The sources of crime on the internet are, ultimately, individuals. These individuals may be within the UK or in another country, and the crimes we are interested in are those perpetrated against UK businesses or individuals. The sources of crime on the internet can be simply divided into two categories:

- Crimes perpetrated by individuals connected to the internet in the UK;
- Crimes perpetrated by individuals connected to the internet outside the UK.

Due to the complications of prosecuting individuals outside the UK, it is suggested that the approach initially taken to this group is one of prevention; whilst it is suggested that the approach taken against the group within the UK should include prevention, detection, and prosecution.

The individuals perpetrating the crimes are connected to the internet by Internet Service Providers (ISPs), whether they be in the UK or not. For crimes to be perpetrated against UK businesses or organisations, the attacker's Internet Protocol packets (the malicious data traversing the internet) must pass over the portion of the internet that physically resides in the UK. This portion of the internet is effectively governed by UK law and, therefore, can be subject to any checking, restrictions or controls the UK Government wishes to place upon it.

The Critical National Infrastructure

The National Infrastructure Security Co-ordination Centre (NISCC¹) has responsibility for co-ordinating the protection of the Critical National Infrastructure (CNI). Whilst the CNI includes the IT Systems within Telecommunications, Financial and Central Government, it does not explicitly include the UK portion of the internet, although it does recognise that "the internet ... [is] beginning to underpin the fabric of the UK's infrastructure."

It is suggested, then, that should the UK portion of the internet be easily identifiable and separable from the non-UK portion of the internet, then this may too form part of the CNI. This subtle modification to the way the internet is viewed would have far-reaching consequences as the protection of the UK portion of the internet would then become a Government responsibility. This change would potentially allow the UK Government, businesses and individuals to regard the UK portion of the internet as less hostile, anonymous and dangerous than the majority of the internet.

3 Architectural Changes To The UK Internet

We should regard the UK portion of the internet as including the communications infrastructure that links the Internet Service Providers (ISPs) to the UK Gateways (the international connections) and the individuals and businesses who use the internet. It follows that any physical infrastructure that provides internet access residing in the UK is then ultimately part of the UK portion of the internet. Any infrastructure that provides internet connectivity outside of the UK, up to the UK Gateways, is then part of the global internet.

Domain Based Security

The concept of Domain Based Security is the process of modelling the real world in terms of IT systems, logically grouping people, resources, and infrastructure by business functions, known as domains. This modelling technique encourages the understanding of the Information Exchange Requirements (IERs) internally to a domain and between the domains. The information security requirements generally result in lesser assurance requirements within a domain (allowing for richer IERs) and higher assurance requirements between the domains (through more controlled IERs). These assurance requirements therefore generally align with the business processes where members of a domain tend to work closely together with documented interfaces between the domains.

Modelling the current UK internet, a simple domain model for a company may be as shown in figure 1, with the control device between the domains represented as a firewall.

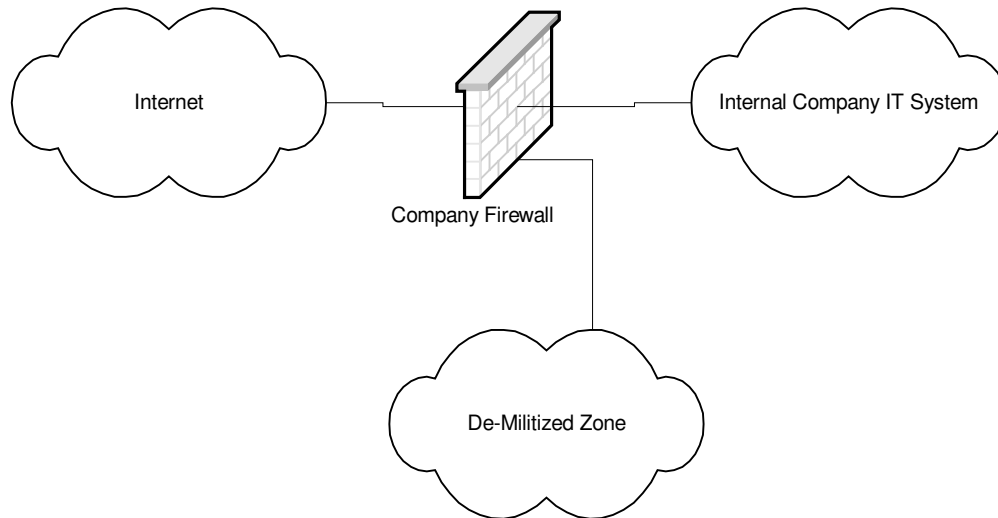


Figure 1 – Simple Domain Model for Current UK Connections

The firewall controls the information exchange between the company's IT system and the internet by:

- Limiting the services and visibility of the company IT system offered to the internet (to limit hacking);
- Forcing the majority of connections from the internet to the De-Militized Zone (DMZ) for checking and control (such as email checking for viruses and spam, and the hosting of the company web server);
- Limiting the protocols that users of the company's IT system may use when accessing the internet (such as preventing the use of network games and limiting the effects of malicious code such as viruses and trojan horses).

In this model, the entire internet is regarded as hostile, due to the potential lawlessness discussed earlier.

Applying Domain Based Security To Protect The UK Internet

If it is possible to accurately identify the components of the UK portion of the internet, then it is possible to define this as a domain in its own right, with the rest of the internet making up another domain. In order to do this, certain criteria are necessary:

- All domain names that refer to components of the UK internet must end in '.uk', such as .co.uk or .org.uk. Currently, a number of companies and individuals have opted for .com and .org addresses. Changing these will be the relatively simple task of adding .uk to the end of their addresses, although it is recognised that a significant cost may be involved in terms of systems configuration, stationery and corporate identity. This change will allow individuals and law enforcement agencies to easily recognise a component of the UK internet.
- The '.uk' top-level domain of the global domain name system must come under UK Government control. This will allow the withdrawal and prevention of any .uk addresses being used to identify components that are not part of the UK internet. By placing control of the .uk DNS with the UK Government, a level of trust can be

placed in all domains that exhibit a .uk address and action can be taken against any .uk address that breaks the UK law.

- Multi-national companies that have a physical UK internet presence must use a .uk address to identify their UK point of presence, and any non-uk domain addresses must reside outside of the UK internet. The owner of the .uk address will be responsible for all traffic to the UK internet from their .uk address and may be prosecuted under UK law for infringements. The multi-national company will be responsible for preventing their networks being used as a 'backdoor' to the UK internet.
- All the UK Gateways, the connections between the UK internet and the global internet, must be identified.

The UK internet may then be easily defined and, therefore, separated from the global internet. The Information Exchange Requirements between the UK internet and the global internet may then be defined. A barrier can be implemented between the UK internet and the global internet to limit the available protocols to those specified by the IERs. The simple domain model may then be as shown in figure 2, with a firewall representing the control device between the UK internet and the global internet.

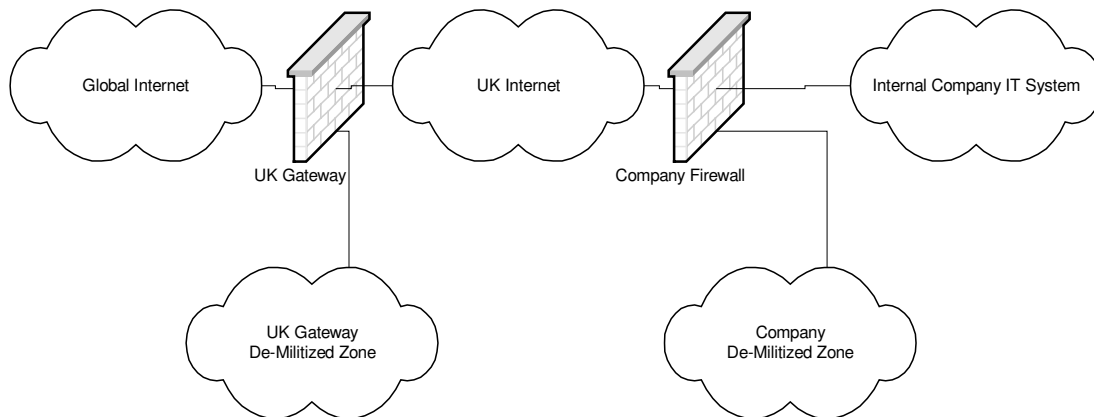


Figure 2 – Domain Model to Secure the UK Internet

It is suggested that the Information Exchange Requirements between the UK internet and the global internet are email, web browsing, and Virtual Private Networks (to support company Wide Area Networks implemented by VPNs). Virtual Private Networks are encrypted services that run over the internet and support all Internet Protocol (IP) services.

VPNs may be seen as a potential weakness to this model as protocols restricted by the UK Gateway may be allowed over a VPN. This is not as great a weakness as may be initially thought as VPNs require addresses to be specified as end-points for each VPN tunnel. These end-points require two co-ordinating authorities, effectively limiting any attack over a VPN to a known and trusted party. The VPN end-point addresses can also be recorded by the UK Gateway so any perpetrators can be traced should information or attacks be received over a VPN and relayed inside the UK.

The UK Gateway De-Militized Zone may be used to scan all emails entering the UK for viruses and spam.

Performance and Management Considerations

The performance of the UK Gateway is a major concern due to the large volumes of traffic that enter and leave the UK internet. The high-level solution could be the implementation of a number of parallel UK Gateway components, operating identically at potentially numerous locations around the UK. It is essential that all connections between the UK internet and the

global internet are controlled by the same policy, and that no uncontrolled connections are permitted.

Protection Offered By The UK Gateway

The UK Gateway will provide the following protection:

- All emails entering the UK internet from the global internet will be scanned for viruses and spam. Using modern virus checking and anti-spam filters (available from a number of organisations as managed services) the majority of viruses and spam can be prevented from entering the UK internet. This will not completely remove the virus and spam risk to the UK but will certainly reduce the risk to manageable levels.
- Hacking attempts against individuals and businesses attached to the UK internet will be severely hampered by the protection provided by the firewall. Intrusion Detection Systems may be employed on the UK internet side of the UK Gateway to provide timely warning of any attacks that manage to circumvent the UK Gateway.

Protection From UK Attackers

Using the same Domain Based Security techniques as described to protect the UK internet from non-UK attackers, it is possible to develop a model that will provide protection from UK based attackers.

Currently, UK individuals and companies connect via Internet Service Providers (ISPs). The connection provided usually allows for the full Internet Protocol (IP) suite of protocols to be used in accessing the internet. It is suggested that the Information Exchange Requirements between an individual and a component of the internet are generally email, web browsing and VPNs (for remote employees accessing internal company IT systems).

Limiting access to these protocols at the ISP and checking the content of emails for viruses and spam will greatly reduce the risk to the UK internet from UK based individuals. It is suggested that the requirements of UK ISPs should be specified in law and audited on a regular basis. The model is shown in figure 3.

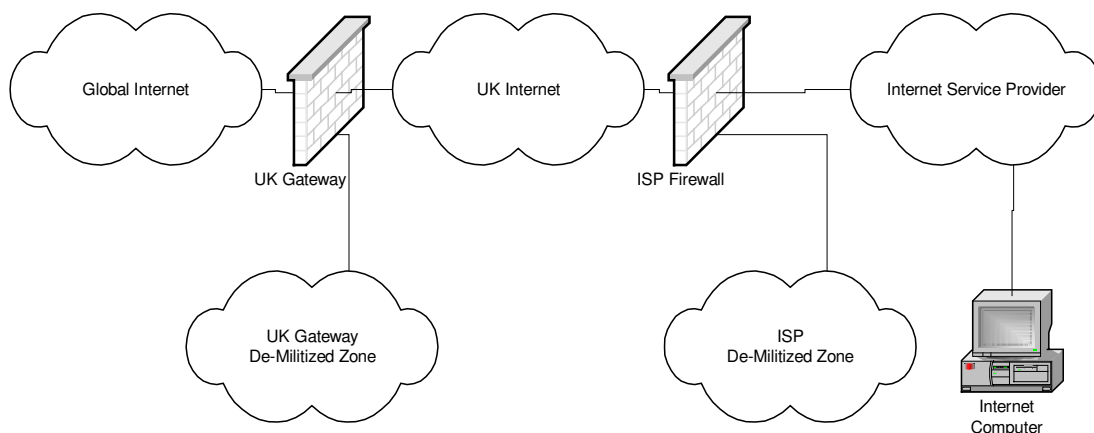


Figure 3 – Domain Model for ISP Access

The protection offered by this model includes:

- Individuals and companies connected via an ISP receive protection by the ISP firewall from hackers;

- All emails entering or leaving an ISP can be scanned for viruses and spam;
- Individuals and companies connected via an ISP will be limited to specific protocols, reducing their ability to attack other components of the UK internet.

4 Additional Benefits For Law Enforcement

The protection afforded by the UK Gateway and the ISP Firewalls will limit the threats to individuals and businesses using the internet. Crimes committed via the UK internet will be traceable to a source. If the source is based in the UK then the perpetrator can be prosecuted under UK law. The deterrent that can be created through successful prosecutions will reduce the number of UK internet based crimes leading to a safer UK internet.

Due to the expected reduced UK internet crime, and the increased tracking that will be possible, it is suggested that all internet crimes should then be reported to the police who should be furnished with the tools and the skills to trace the suspects. The result will be that internet crimes will become to be seen in the same light as traditional crimes, as opposed to complex chains of events perpetrated by untraceable individuals hidden by the anonymity of the internet.

One of the greatest concerns about the internet is the availability of material that is illegal in the UK. Whilst efforts are made to track and prosecute UK based individuals who break laws related to this material it is currently very difficult due to the scale of the internet and the relative anonymity of the perpetrators.

The suggested modifications to the architecture of the UK internet would allow for additional controls that could help identify and trace material-based internet crimes. The UK Gateway could be programmed to record access to specified web sites known to contain material illegal in the UK. Law enforcement agencies could then simply contact the ISP to identify the individual concerned. These controls would require the UK Gateway and the ISP Firewalls to record all internet-based activity for the purposes of law enforcement.

Civil Rights Complaints

Any suggestion to regulate the internet will be met with complaints from civil rights organisations who believe that innocent people will be spied on, and that any regulation goes against the 'spirit' or the 'intention' of the internet.

Whilst it would be fairly trivial under the new architecture to monitor an individuals' internet activity, whether that be email or web browsing, it should be noted that law enforcement agencies currently have this capability through direct contact with the Internet Service Providers following the issue of a warrant. There would be no reason for the legal access requirements to individuals' internet activity to change simply because the technical challenges had been reduced or removed.

With reference to the expected claims that the new architecture goes against the spirit of the internet, it should be noted that the internet that exists today was conceived by the US Department of Defence for its own programmes. The introduction of the Joint Academic Network (JANET) into UK education establishments was provided through UK Government funds. The remainder of the UK internet was constructed by a number of commercial organisations. It would be fair to suggest that the spirit of the today's internet is mainly business, and business requires laws for protection.

5 Funding The Security Of The UK Internet

If one accepts that the majority of the use of the UK internet is for the purposes of business, and that the greatest request for greater security comes from UK business, then it may appear logical that the enhanced security is funded by UK business. It is suggested that a

new Business Internet Tax is applied to UK businesses at the point of purchase, levied by the ISPs, and payable to the Government. When spread across the breadth of the UK businesses connected to the internet, this tax should be relatively small, especially when compared to the business benefits that the security will directly provide.

With respect to the question of applying a similar tax to individuals, it is suggested that this tax be waived on two grounds: first, Government initiatives underway are encouraging more people to 'get online' and a direct tax may seem inappropriate; second, the reduction in the internet service that an individual may experience as a direct result of these security measures may effectively be compensated through the waiving of this tax.

6 Summary – Should Big Brother Be Watching?

The current internet architecture allows users and attackers from all continents the same access and privileges as legitimate users in the UK. This simple, non-geographical nature of the internet makes the responsibility for internet security a concern for all businesses that connect within the UK. In other, physical areas of society, the UK Government expends great energy to protect UK businesses, individuals, and infrastructure from crimes committed within the UK. These efforts extend to Police patrols, criminal investigations, and stringent monitoring of ports.

Internet crimes, including hacking, viruses, and spam, perpetrated from overseas and targeted at UK businesses and individuals are difficult to prevent and often impossible to prosecute. The changes to the UK portion of the internet architecture proposed in this document, based on the successful Domain Based Security model, will help prevent the vast majority of internet crimes targeted at the UK from being successful. Further, by limiting the internet facilities of individuals to those that are used by the majority (email, web browsing and Virtual Private Networking), it is possible to not only limit the internet crimes perpetrated within the UK, but will increase the tracking of the perpetrators and lead to a greater number of successful prosecutions.

It is suggested that if the UK internet is to be regarded as critical to UK business, then it should be included as part of the Critical National Infrastructure and be suitably protected by the Government. Whilst the suggestions in this paper may not meet with all ideals, it may certainly provide a starting point for discussion from which suitable protection schemes may be devised.

References

- 1 National Infrastructure Security Co-ordination Centre (www.niscc.gov.uk)

The Author

Kevin Sheldrake MIEE CISSP is an Information Security Consultant at VEGA Group PLC. He is registered with the CESG Listed Advisor Scheme, is a certified CESG CHECK Team Leader, and is a Certified Information Systems Security Professional (CISSP).