

Information Security Consultancy Service Whitepaper

EWA AUSTRALIA

WHAT'S ALL THIS
.BIZ-NESS
ABOUT SECURITY?

by
Andrew Dell

For further information please contact:

infosec@ewa-australia.com

Canberra:

Level 1
214 Northbourne Ave
Braddon
ACT 2612

Tel: +61 2 62 30 6833
Fax: +61 2 6230 5833

Brisbane:

Level 30 AMP Place
10 Eagle Street
Brisbane
Queensland 4000

Tel: +61 7 3303 8592
Fax: +61 7 3303 0111

Adelaide:

Innovation House
Mawson Lakes Boulevard
Technology Park, Mawson Lakes
South Australia 5095

Tel: +61 8 8260 8261
Fax: +61 8 8260 8260

www.ewa-australia.com

WHAT'S ALL THIS .BIZ-NESS ABOUT SECURITY?

By *Andrew Dell*

We are all familiar with the traditional Internet Top Level Domains (TLD's), .com, .net, .org, .gov etc. Recently (accompanied with spectacular hype), a number of new TLD's were released on the Internet; domains such as .info, .tv, .name and .biz are rapidly establishing a presence. As a result of this, there has been significant debate over the need to increase the range of TLD's.

One school of thought suggests that it is essential, as the Internet is growing so fast that it is becoming more and more difficult to acquire .com URL relevant to a business name. Of course, more TLD's would help alleviate this. Conversely, opponents view the generation of more TLD's simply as an excuse to extort more money from industry (a 'licence to print money').

The latter argument suggests that by introducing a new TLD, the corporate world is likely to need to protect their 'brand name' regardless of the domain. For example Microsoft TM, Nike TM *et al* have absolutely no requirement to purchase or use a new domain, but to protect their reputation and to prevent misuse of their name, they will be compelled to purchase the new TLD. Whilst purchasing a TLD does not represent an excessive outlay to large companies, the combined income to TLD resellers is substantial.

One new TLD in particular has been attracting significant attention. Neulevel, Inc is the exclusive registry operator of the entire .biz domain. They have marketed their domain as superior in a number of areas; the most perplexing (or misleading) claim addresses the .biz security. Neulevel^l claim that .biz security is enhanced because:

- "Changing the details of your .BIZ address requires enhanced validation before modifications take effect", and that it will
- "Secure your peace of mind; your .BIZ name won't be hijacked and changes can't be made to your website without your approval".

Whilst these details may be technically true, the fact is that businesses who purchase a .biz domain are in no better position than any other domain to sleep well at night safe in the assumption that their website and information is secure. Here is why:

The '*enhanced*' security included in the .biz domain is based purely around the access control and authentication security of the Domain Name Service or DNS (DNS is an Internet service that translates domain names into IP addresses). Most domains (.com, .net etc) use what is known as the 'mail-from' authentication schema (which is associated with an email address) to allow users to register and modify their domains. Since it is relatively trivial for someone to fake an email, it is therefore possible to fool this 'mail-from' authentication and essentially highjack a domain (so that when you type in a website address, you actually go to a different site). The .biz TLD enforces a stronger method of authentication/authorisation to register and modify domains than does the standard 'mail-from' scheme used in the past. The registration process for .biz in Australia is described below:

UNCLASSIFIED

In Australia, MelbourneIT LTDⁱⁱ (via Internet Names World Wideⁱⁱⁱ) administers the .biz domain. When a .biz site is registered online details are entered into an e-form, and then a secure connection is established (Secure Sockets Layer, or SSL) for facilitate payment. At the completion of this registration process, the person who registered the domain is emailed a registry key (in reality an eight digit password eg. 28kU6b98) that permits the registrant to perform modifications to the domain name's registration details.

The registry key is sent in clear text (not encrypted) and is therefore not protected from unauthorised viewing. Unencrypted email has no security and it is possible that anyone who captures it can read it – exactly like a postcard in the traditional mail system. Once someone has this key, they are able to modify the details of the website registration – even alter the delegation (making your domain name point to a particular computer on the Internet), essentially stealing or highjacking the website.

Even once you have your registration key, to login and maintain your registration details - the site where you input this key is not secured by default (it is an option). Your *secret* key and logon details are once again transferred over the Internet in clear text – visible to anyone with the means and intent to view them.

Investigation suggests that many providers of traditional TLD's (.com, .net etc) now utilise exactly the same authentication mechanism as .biz – This begs the question *'so where is this enhanced security?'*

As with .com and other TLD's, the .biz domain is not immune to Social Engineering, whereby an attacker (armed with some corporate or personal information) masquerades as a legitimate site owner who has lost their access credentials and registry key. This is usually conducted over the phone, with an overworked helpdesk operator who's primary function is 'to help'!

Neulevel will have you believe that further security resides in its "...thick registry model, which offers businesses enhanced domain-name security by holding domain name data in a central, highly secure location^{iv}..." This system security is all well and good, but if the authentication and access control mechanisms can be deceived (which they can) the superior security claims of .biz are further diluted.

Whilst potentially damaging, DNS Highjacking is not a high profile security threat. In reality, it is a threat to credibility and certainly warrants defence, but does not jeopardise information on corporate systems. Any owner of a .biz site still faces the intimidating threat of their website being compromised by a determined hacker using a myriad of existing tools and exploits. Thus Neulevel's claim that "...changes can't be made to your website without your approval..." is not true, and incorrectly provides businesses with a false sense of security.

The biggest threat to an organisation with a web-presence remains the perimeter of their web-severs. The installation and maintenance of Firewalls, Anti Virus, and Intrusion Detection Systems (IDS), combined with diligent systems administration are required to aid in the defence of these systems. Additionally, whilst technology is an enabler in protecting systems, it is by no means a panacea. The best systems will fail if the underlying policy, implementation, training and culture is not also adequately addressed.

The authentication mechanisms instigated by the .biz domain are a first step. The protection of DNS details has long been a problem for the Internet

UNCLASSIFIED

industry, but to be effective these authentication mechanisms need to be correctly implemented. The registry key and account details must be protected at all times. If .biz wishes to market its enhanced security – it must be made clear that their solution cannot (and does not) ensure that “changes can’t be made to your website without your approval”. The biggest threat to security is always complacency.

-
- i www.neulevel.biz
 - ii www.melbournelT.com.au
 - iii www.inwww.com.au
 - iv www.neulevel.biz

Andrew Dell, CISSP, is the Senior Information Systems Security Consultant with Electronic Warfare Associates – Australia, specialists in Information Warfare.

Andrew can be reached at andrew.dell@ewa-australia.com,

or visit the website: www.ewa-australia.com