INFORMATICA
INFORMATION SECURITY & RISK MANAGEMENT

INFORMATICA
INFORMATION SECURITY

INFORMATICA SECURITY MEMORANDUM

Secure Domain Management

The Top 7 Security Threats and Solutions Related to Domain Names

Domain name management is a critical part of every e-business, or any company's Internet strategy, since it is the essential element of communications. Domain names control Web site access, email communications and even internal routing. They represent the difference between being in business and being unreachable. This is the concept of 'availability', one of the three pillars of information security. The top 7 threats to domain names are listed below.

1. Domain theft

This type of malicious activity simply describes the act of stealing a domain, either by guessing the administration password, or by taking advantage of poor protection when having it transferred to a new owner.

If a domain name is registered and managed adequately, this risk is drastically reduced. Selecting strong domain management passwords and educating the domain contacts is critical in protecting the domain name.

2. Cybersquatters

People and organizations who take domain names based on their representing popular words or registered names are called cybersquatters. They keep domain names unused in order to sell them for a large profit. In many cases, they have automatic monitoring tools to determine when some of the best domain names expire, at which time they jump in and register the domains themselves. Once locked away by cybersquatters, domain names can be involved in lengthy and expensive court battles.

Unfortunately, cybersquatters have the tools and the persistence to keep trying to hijack domains for money, but the courts have often ruled in favour of the copyright owners. Make sure your company is adequately incorporated and that you can prove that you own the name in your jurisdiction. As for owning domain names that are simple, but popular words, they simply go to the first party that registers the name.

3. Domain Expiry

Once a domain has expired, getting it back can be a frustrating exercise, especially since many domain registrars place that domain in an unreachable period where it can't be registered by anyone. To avoid having your domain taken away in such circumstances, make sure that it does not expire.

To avoid missing expiry notices, ask your domain management company to send numerous notices prior to domain expiry and try to register the domain for a number of years, instead of only one. You can also select automatic renewal, to prevent expiry from taking place.

4. Unreachable Domain Contacts

When domain contacts are unreachable or do not respond, or spam filters catch the domain expiry notices, those domains simply expire, thus becoming available to others. Educate people about the importance of domain notices and see #3 above.

5. Spam and Identity theft

Using valuable email addresses when registering domain names is not prudent, as those domain records are routinely visited by 'spambots' that harvest email addresses for spam purposes. Once on a spam list, it's almost impossible to be removed and the recipient can become the target of numerous virus and identity theft attacks. If possible, use a secondary address, or ask your domain management company to handle domain issues on your behalf (if you trust them).

6. Domain Slamming

Domain slamming is the act of convincing a domain registrant that their domain is expiring and that they should renew. Unfortunately, such notices often come from 3rd parties that try to mislead and confuse domain owners into trusting them and simply agreeing to a change of registrar.

Ensure that you have a strong connection to your domain management company and only do business with them directly. You will know right away when a fake or misleading request arrives and will be able to confidently manage your domains.

7. Denial of Service

Denials of service are attacks directed specifically at owners of Web sites hosted on a particular domain. These are pooled attacks on domain names with the sole goal of making them unreachable by regular traffic. There is currently no good solution to this attack, since each request appears legitimate, but these attacks are rare and manufacturers such as Cisco are constantly working on improving router based protection against DOS.

Informatica Security Solutions works with clients to manage and protect domain names from all threats. The company offers outsourced management, Web site protection, secure, spam free email, PKI and digital certificates to secure Internet and intranet communications. (www.Informatica*Solutions*.com)