'Google hacking' attacks rising

Web sites are more vulnerable to "Google hacking" than many people realise and "hacking" attacks are on the rise, according to a recent study by Massey University (New Zealand) researchers. Personal information held by businesses, government departments and voluntary organizations are potentially at risk, along with operations of the websites that hold them.

Google hacking involves using the popular Google search engine to locate sensitive online information, which should be protected but is not.

Dr Ellen Rose, a senior lecturer at the Institute of Information and Mathematical Sciences, and graduate student Natalia Nehring, ran Google search queries known to return sensitive information from the Google database.

They wrote a computer program that for three months ran 170 daily queries against the Google database, looking at sites in New Zealand, Australia, the United States and the Czech Republic.

They found that sensitive data was now easier to obtain and that New Zealand sites are more vulnerable to hackers than Australian or United States sites.

The study aimed to ascertain how vulnerable we are to hackers. The researchers say any internet user can now easily find sensitive information using only a browser and a few carefully chosen keywords. They point out website administrators can use the same techniques to discover their own vulnerabilities.

Google hacking, how it works and how to protect against it is extensively reported on a range of articles that can be found through the Google search engine itself.

Dr Rose and Ms Nehring say about half of their hits pointed to sensitive information although some types of sensitive information were only available for a small window of time.

Vulnerabilities related to backup files were open the longest, followed by remote administration vulnerabilities.

They got the most hits in New Zealand in the organisational domains (.co and .org) and within the categories of error messages and backup files.

The average number of days a potential vulnerability remained open across all domains and all categories was similar in the US (48.85 days, 46 per cent from the duration of test period) and Australia (49.54 days, 50 per cent from the duration of test period) with New Zealand vulnerabilities remaining open somewhat longer (60.96 days, 57 per cent from the duration of test period). Very little vulnerability could be detected in the Czech Republic.

Dr Rose said she felt it would be unethical to name the sites where personal information could be found but Massey's own website was found to have about 50 vulnerabilities, which they had alerted the University's technology services department to.

The researchers say a more proactive approach based on building security into the design of Web applications, like the Google search engine, is required.

"Security on the Web is likely to remain an ongoing battle," Dr Rose says. "On the one side, hackers will continue to employ new tactics, using tools like Google in unforeseen ways.

"Security experts must try to minimise exposure by detecting problems and putting countermeasures, such as security audits, in place. Google hacking vulnerability should be included in these security audits."

The Massey researchers are now looking at proactive security measures that could be used by website administrators.

Source: Massey University

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.