LOWERS & ASSOCIATES
International Risk Mitigation Partners
125 East Hirst Road, Suite 3C | Purcellville, VA 20132

Information Technology Risk Management Services

Protecting Your Infrastructure from Client-Side Attacks

Are you confident that your networks and systems are impervious to attack because you have Firewalls, Intrusion Detection, and Virus Protection? Or are you concerned that your people using out-of-date or unauthorized PC software are allowing malicious attackers to gain access to your corporate assets? Lowers & Associates (L&A) is able to answer that question through a Client-Side Attack Assessment.

What is a Client-Side Attack? A client-side attack leverages non-technical and social engineering techniques, un-patched workstations, and a possibly less-educated end-user community (who may act upon incoming phishing attempts or other e-mails with malicious content). Although recent trends indicate that more attention should be devoted to security on the workstation, network security efforts have traditionally been focused on securing an organization's perimeter. At the same time, the relative lack of attention to workstation security, coupled with poor user awareness, has opened new avenues of attack into an organization's network that need to be addressed.

A client-side attack assessment can test and provide insight into the effectiveness of company policies and mitigation mechanisms in place such as anti-virus, email and web filtering, content filtering, and intrusion prevention/detection. Additionally, such an assessment tests that workstation software (email client, browser client, plug-ins, etc.) is up-to-date with the latest security patches. Finally, client-side testing is a good measuring device to test the effectiveness and progress of end-user security awareness training initiatives.

During a client-side attack assessment, email addresses are 'harvested' from various sources, including the Web and other media. L&A then constructs and sends official and authentic-looking emails to selected users - from familiar addresses (such in-company, trading partners, and/or customers) - in order to launch attacks against client-side software such as web browsers, email clients, and workstation components

Our testing involves all of the following attack vectors:

- Emails containing links to malicious websites
- Emails with malicious attachments (spreadsheets, word documents, jpeg/gif, pdf)
- Emails with built-in malicious code

The interaction then entails the end-user opening an email message, clicking on a specially-crafted URL or file attachment, or browsing to a specific website. Assuming that the user takes the 'bait', an agent is deposited on the workstation, allowing for further attacks to be launched from that 'trusted' machine to other servers, databases, and so on.

In today's current IT security landscape, the endpoint is the most prevalent target. By truly simulating the attackers' technical (and nontechnical) methods, the L&A Client-Side Attack Assessment can evaluate real security risks by measuring the effectiveness of security defenses as well as user security awareness initiatives.