

Visiting Web 2.0 Sites Increases Organizations' Security Risks

Jan 10, 2008, News Report

The growing popularity of so-called Web 2.0 sites is proportionally increasing the risk of malware attacks and data leakage for companies that allow employees to access social networking sites through corporate computers.

"Web 2.0 sites are vital to those we're calling 'Employee 2.0' -- the next generation of employees entering the workforce that expect the technology they grew up with and routinely use to be part of their working environment," said Steve Sheinbaum, VP of Americas for Marshal. "While managers and senior employees might not think of text chat as a vital part of their lives, young employees probably can't live without it, which means that companies are now facing decisions about their corporate culture and security with Employee 2.0 in mind."

Social networking sites such as Facebook, YouTube, Craigslist and Wikipedia, as well as Web services such as eBay and Gmail, enable self-publishing and high interaction between users through blogs, RSS feeds, podcasts and other technologies. These sites attract huge numbers of visitors, making them extremely attractive to hackers.

Moreover, the same technologies that invite user participation also make them easier to corrupt with malware such as worms that can shut down corporate networks, or spyware and keystroke loggers that can steal company data. Further, with the ability to post photos, video and audio recordings to sites, employees can inadvertently "leak" confidential company information.

Organizations are realizing how allowing access to these types of sites can compromise information security. Some companies are taking a hard line by prohibiting employees from visiting these sites and are enforcing the policy by blocking access using simple URL filters. Other companies block access and then go to the expense of setting up standalone kiosks that allow employees to visit Web 2.0 sites without exposing the network to malware attacks.

"While Web 2.0 sites clearly pose a threat to corporate network security, making them off limits to employees may not be the best solution," said Sheinbaum. "Many companies understand that being able to access social networking and Web services sites during work hours is important to overall Employee 2.0 satisfaction and may also benefit their business."