Blocking social media is not the answer to IT security risks

Like email, social media platforms have become a channel for the ingress of malware and a portal for data leaks. Like email, social media platforms have become an important channel for business communication and marketing. Like email, social media is here to stay. As with email, the associated security risks need to be managed, but blocking social media sites is not the solution to managing the IT security risks associated with the use of online platforms by employees.

Image: www.freedigitalphotos.net

"Companies should formalise rules about the usage of company assets and Internet resources for online communication with formal policies that are enforced with technical mechanisms and systems that interrogate user-initiated, outbound web traffic. Such policies establish how the organisation intends to secure its infrastructures, data and, ultimately, the business," said Richard Broeke, an IT security expert of Securicom.

He said that the unfettered use of social media platforms by company employees is undoubtedly starting to affect businesses from an IT security standpoint. With social media and Web 2.0 applications, where users become creators and publishers of web content, employees create additional risk for companies when they inadvertently download malicious content or create liability when they publish inappropriate or confidential content on blogs, forums and social and business networks.

The associated risks include non-compliance with legislation about the protection and sharing of sensitive information and reputational damage arising from the dissemination of inappropriate or defamatory information relating to the company or its employees. This can also obviously have financial repercussions. Fraud is another threat arising from the distribution of business-sensitive data, such as financial information, customer information, banking details and even employee data.

Becoming more prominent

The problem is starting to become more prominent. A 2013 study by Osterman Research showed that malware had successfully infiltrated the network through Web 2.0 apps and social media for 14% of companies, and through web surfing by employees in 74% of the companies surveyed, within a 12-month period. Sensitive or confidential information had been leaked via social media in 6% of the responding companies.

Malware spread via social media, as with malicious code spread via email, varies in terms of their intent and purpose. With the more sinister types, the intention is to steal sensitive information. With these sorts of social media scams, users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions, but, when installed, they siphon information from the infected machine. Others that are less sinister are those that use "Likejacking". Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

Fake offerings

81% of all social media attacks in 2013 were fake offerings, according to Symantec. These scams invite social network

users to join a fake event or group with incentives, such as free gift cards, or the chance to win a prize. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.

The Osterman research also found that 61% of companies that allow employees to use social media platforms believe they are reasonably well protected against social media-borne malware. Some don't allow social networking at all, with 26% blocking Facebook; 27% blocking Twitter and 27% blocking Skype.

"While a lot of companies underestimate the risks, there are those on the opposite end of the continuum that block social media platforms, which isn't ideal either. Instead, companies could be monitoring and managing what they do and say online with a robust web security and monitoring solution.

"Much like phishing, many social media scams rely on some sort of action being taken by the user, such as joining a group or liking and sharing a link. That is why educating employees on safe and acceptable actions online is also important. Users need to be made aware of their employer's policy on Internet access and online behaviour. They also need to be aware that what they do online is being tracked," concluded Broeke.