Multi-layer security vital against social media risks

By Anton Jacobsz

16 Jul 2014

Enterprises around the world are rapidly seeing the business benefits of social media. In fact, social media is becoming indispensable for business. It allows businesses to reach new and existing markets and customise and expand their strategic communications.

Anton Jacobsz,

Social media allows relatively low cost exposure, the ability to receive customer feedback quickly, helps share institutional knowledge, provides early warnings of potential product or service issues, improves collaboration and helps identify new product and service opportunities. If used properly, social media can make businesses more agile and competitive. However, the risks of social media are being vastly underestimated.

Enterprise security risks

Frost & Sullivan research has found that respondents rank social media low on their list of concerns, seeing it mostly as a productivity issue. But this is only a small part of the challenge of social media use. More importantly, social media use can lead to enterprise security risks and data loss. Among the risks are the fact that social networking sites themselves may have technical vulnerabilities, with the risk level varying from site to site.

These risks are increased by third party content such as games, applications and ads, which are often presented as part of the social networking site but are in fact external content with a large proportion of it not secure. While malicious links and third party content could present the risk of a breach, a far more common security risk associated with social media is that of social engineering.

Social media is an ideal conduit for social engineering, through which cyber criminals can later gain access to enterprise networks, or which can open the gateway to spam, file sharing and the sending of poisonous or malicious links. For example, poison links relating to topical news can direct users to malware or compromised accounts and often the user will not even know this has occurred. Users may trust the compromised accounts of friends and family, which allows outsiders to access enterprise networks. When links appear to come from trusted sources, users will let their guard down.

spear phishing attacks

A potentially massive problem is that social media can easily be used to enhance spear phishing attacks, thanks to the use of stolen personal data and personal information that users have divulged voluntarily via social media. Often, users use their family, pets or favourite sports teams' names as passwords, so information available publicly on social media can also be used to determine user names and passwords on personal and work accounts. Social behavior in humans is a powerful force that cannot be stopped, and threat actors understand this and target users effectively.

Complicating the situation is the proliferation of social media sites and the variety of devices now being used to access them. Various studies have found that the majority of users accesssocial media through their mobile devices, and many of these people also use their devices for work purposes, which further increases the risk of users and the companies they work for falling victim to malware. There has been a significant increase in the amount of mobile and cross-platform malware in circulation too.

Meanwhile, enterprises are still grappling with mobile security policies, and underestimating social media risk. Businesses can no longer afford to ignore the risks of social media. Business policy alone is not enough to protect your organisation, and simply blocking access is not appropriate either, since social media is an important business tool. Businesses now need to balance social media access for those who need it, while also limiting exposure to the risks. There is no security panacea or silver bullet, enterprises must take a multi-layered security approach, which Fortinet calls 'defence in depth'. This approach includes granular controls that limit who can access social media and when, and specified exactly which applications and functionality may be used, so reducing the attack surface while still allowing social media access by those who need it.

Block malicious links

Defence in depth should also include web filtering to automatically block malicious links posted on social media, without the IT department having to manually manage URL block lists. It should include anti-spam to block fake social media phishing emails, anti-malware as the last layer of defence to protect against social media malware, and real-time updates delivering automated, round-the-clock protection. Enterprises also need a simple consolidated platform to manage all of these complex, 'moving parts' effectively, because a lack of centralised coordinated management and automation can result in security holes. Integration into a single, unified threat management platform simplifies the network and improves security protection.

Frost & Sullivan's Global Workforce Study found that 64% of respondent companies limit employee access to social media through content filtering and website blocking technology, 51% restrict access by setting and enforcing policy and 25% have no restrictions on the use of social media by employees. Instead of imposing blanket bans, businesses should put effective technology tools in place anddefine clear social media usage policies, specifying who can access social media, what sites they can access, when they can access them, where they can access them and what devices they can use to access social media during work hours. There should be no room left for confusion. Policies should be clear, well defined and communicated to employees.

Understanding that the end user will always be the weakest link in a security architecture, training and security awareness are also important to help users make better decisions, and are the foundation for an effective social media risk mitigation strategy. It's not enough to define security policies that people will forget. Ongoing training is important, so that users understand the risks and reasons for the strategy.

ABOUT THE AUTHOR

Anton Jacobsz is the Managing Director of Fortinet distributor, Networks Unlimited