Control social media at work through Barracuda Networks

The newly released Barracuda Web Filter Firmware 6.0 features new application control capabilities to help organisations assess and enforce social media policy in the workplace.

Released by Loophold Security Distribution, its MD, Martin Tassev, says, "Organisations are realising that employee behaviour on social networks can impact productivity, network performance and even company security. However, prior security initiatives simply to block inappropriate content and malware are no longer sufficient. As social media becomes more ingrained in the workplace, organisations must focus on how to 'allow' social media while keeping the workplace safe."

According to the 2011 Barracuda Labs report 'Social Networking Security & Privacy', 86% of respondents felt that employee behaviour on social networks could endanger company security. Despite those concerns, social media is still widely used - 75% of respondents' workplaces allow the use of Twitter and 69% of respondents' workplaces allow the use of Facebook. The new filter allows administrators to allow social media use safely by regulating it through several new capabilities, including an upgraded application control engine with support for granular policies, Web application monitoring and archiving and enhanced SSL inspection.

Social media regulation with granular policies

The filter adds support for more than 400 profiled applications beyond the scope of traditional URL or domain filtering. For example, administrators can allow users in the organisation to login to Facebook to view and post status updates while blocking games, shares and other Facebook applications to protect their networks from viruses and malware.

This upgraded application engine builds on the existing capabilities of the Barracuda Web Filter designed to block applications at a broader level, including Skype, BitTorrent and YouTube for regulating bandwidth usage on workplace networks.

Social media monitoring and archiving

Its web application monitoring capabilities integrate with the brand's message archiver and enable the capture and retention of chat, Web-based email and social media interactions for the purpose of archiving, searching and fulfilment of e-Discovery requests. Supported interactions on Facebook include wall posts, comments, messages and chat messages. Supported interactions on Twitter include tweets and direct messages. Other platforms supported by web application monitoring include Yahoo! and Google.

"As the use of social media as evidence in forensic inquiries increases, organisations must ensure that they properly capture, preserve, search and produce the data in a manner consistent with best practices," adds Tassev. "As one of the few vendors that offer both Web security and message archiving solutions, we are well positioned to deliver ease-of-use and economics to meet this need."

Enhanced SSL Inspection

As social media networks have embraced encryption of user sessions, the filter can decrypt HTTPS traffic that is SSL encrypted when deployed in forward proxy mode. Transparent deployment of this enhanced SSL Inspection feature requires deployment of a trusted root certificate on client Web browsers. This capability builds on the existing HTTPS

filtering capabilities of the filter for inline deployments.