McAfee®
An Intel Company

SECURELY ENABLING SOCIAL MEDIA

Solution Guide

80 PERCENT

Eighty percent of companies use LinkedIn as their primary tool to find employees.[7]

Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

According to Gartner, "By 2014, social network services will replace email as the primary vehicle for interpersonal communications for 20 percent of business users."[1]

Defending Business-Critical Social Media

Challenges

Social media has changed the world. This is a cavalier statement. But simply consider how we mange business contacts, personal relationships, communication, marketing, sales, and countless other aspects of our business and personal lives. Organizations are finding that social media can help with everything from keeping employees more connected with customers and marketing strategies to creating new revenue streams and enhancing productivity. Regardless of the marketing organization making use of Twitter and Facebook, or LinkedIn being as indispensable to the sales team as their CRM solution, or even engineering taking advantage of YouTube to demonstrate new products, social media has staggering numbers, making it business critical.

- Facebook has 750 million users spending 700 billion minutes per month interacting on it[2]
- Twitter has 200 million users creating 65 million tweets per day[3]
- LinkedIn has 100 million professionals across 1 million companies[4]
- YouTube has 490 million worldwide visitors every month with 92 billion views per month[5]

The reality is that the same things that make social media enduring to us personally and professionally also make it a target for nefarious behavior. According to a recent McAfee study conducted in conjunction with Vanson Bourne, an international research consultancy, and Purdue University's CERIAS group, social media adoption rates are reaching more than 90 percent in countries such as Brazil, Spain, and India, and more than 70 percent in countries such as the United States, United Kingdom, Australia, and Canada. The world is a target-rich environment through social media. Of the 1,000 international organizations surveyed in the study, 50 percent sited security as their primary concern when it comes to social media and 70 percent of organizations experienced a security breach associated with social media including malware exposure, data loss, phishing scams, and the like. Collectively the surveyed organizations reported losses more than $1 billion USD from incidents attributed to social media.

- The financial loss associated with a social media security incident averages $2 million USD
- Large organizations averaged financial losses closer to $4.5 million USD[6]
- Sixty percent of organizations reported that the worst damage from a social media security incident was related to reputation and brand; 14 percent cited litigation costs

85 PERCENT

Eighty-five percent of organizations with more than 1,000 employees currently have a social media policy, and 80 percent allow access to social media sites.[8]

Solutions

There are a number of user-centric tactics such as employee awareness and policy setting that can be utilized to mitigate risks related to social media. However, solutions that also leverage technology are also needed and can be particularly effective in preventing both malicious and careless incidents. Three such solutions include application-aware controls, data protection and antimalware.

Application-aware controls

Consider Facebook. Allowing or disallowing access to Facebook is not as simple as a more static website. Facebook is actually comprised of hundreds of thousands of disparate applications. As such, controls that are application-aware should be leveraged since they can allow access to certain applications within websites while prohibiting access to time-wasting applications such as games. By integrating with a user database like Microsoft Active Directory, it should also be possible to apply specific rules to specific groups and individuals for more granular control of how users interact with social media applications.

Data protection

Data protection applies to many areas of security from users, including system administrators, DBAs, and other privileged groups interacting with databases, applications, and file shares to copying sensitive data to removable media such as a USB thumb drive. However, when it comes to social media, many of the controls for data protection are actually most critical for protecting organizations against careless activities perpetrated by employees and similar insiders that are negligent or indifferent to organizational policies. One example might be posting sensitive identification information such as Social Security numbers or other government IDs through a messaging interface on a site like LinkedIn. Solutions should be deployed that can detect the posting of sensitive data and block it. There should also be the ability to simply make all or some sites read-only based on the user. Another possibility could be modifying the layout of certain pages so that key features are actually removed from the user's web interface. Keeping with the LinkedIn example, controls could be put in place that would render the HTML within the browser without specific functions available like the inbox and search functions found in LinkedIn.

Antimalware

Web browsers such as Microsoft Internet Explorer, Firefox, Safari, Opera, and Chrome are powerful and complex. The same can be said about their supported applications such as Java, Flash, Shockwave, Windows Media Player, and the like. Because browsers and their applications are necessary to make total use of today's sites, everyone's got them, which means they are targets. Malware threats have grown from just under 6,000 in January 2007 to more than 56 million in January 2011, according to McAfee® Labs™. This frightening increase means that traditional signature-based antivirus solutions, also known as blacklisting, while useful against known threats, need to be augmented to provide protection against newer threats taking advantage of social media. Solutions for antimalware need to augment blacklisting with intent analysis. Capabilities for intent analysis should include the authentication of code, media type verification, and controls around behavior and reputation. Bringing these capabilities together with blacklisting, known and unknown attacks can be mitigated on the operating systems, the browsers they run, and the applications within those browsers. As such, common attacks like phishing scams utilizing links in social media that will ultimately compromise a user's system, can be thwarted by proactively evaluating the reputation of sites and analyzing the parameters of files.

Best Practice Considerations

- Embrace social media to remain competitive while leveraging security controls to mitigate risk
- Ensure that employees are aware of the risks and refresh security policies to include social media
- Implement layered control; while there are many solutions to protect from social media incidents, application-aware controls, data protection, and antimalware are essential for success
- Deploy controls that are user and application aware; granularity is a necessity
- Protect from careless and malicious users with solutions that can filter, block, and modify online interactions such as posting
- Use antimalware solutions that combine signature-based antivirus with intent analysis to address known and unknown threats

Fifty-five percent of companies believe employees accidently brought in malware or were involved in careless data loss.[9]

Value Drivers

One of the most critical perspectives of social media as it relates to security is the potential for unwanted or unplanned loss of sensitive data.

- The value of your social media security efforts is mostly rooted in cost avoidance of critical data loss as well as in the subjective area of increased user productivity. McAfee solutions can help ensure that you also are monitoring and managing users in this area which is critical for data loss as well as for demonstrating appropriate due care.
- An additional benefit of social media is as a way to improve and demonstrate to a changing demographic within the work force that your organization is progressive enough to embrace the change but in a controlled and deliberate way

Related Material from the Security Connected Reference Architecture

Level II
- Securing Mobile Devices
- Enabling Consumerization of the Workforce
- Protecting Information

Level III
- Securing Cloud-Based Communications
- Enabling Bring Your Own PC (BYOPC)
- Enforcing Endpoint Compliance
- Securing and Controlling Laptops

For more information about the Security Connected Reference Architecture, visit: www.mcafee.com/securityconnected.

About the Author

Brian Contos, CISSP, is director of global security strategy at McAfee. He is a recognized security expert with nearly two decades of security engineering and management experience. He is the author of several books, including *Enemy at the Water Cooler* and *Physical and Logical Security Convergence*. He has worked with government organizations and Forbes Global 2000 companies throughout North, Central, and South America, Europe, the Middle East, and Asia. He is an invited speaker at leading industry events like RSA, Interop, SANS, OWASP, and SecTor and is a writer for industry and business press such as *Forbes*, *New York Times*, and *The Times of London*. Brian is a Ponemon Institute Distinguished Fellow and graduate of the University of Arizona.

brian_contos@mcafee.com || http://siblog.mcafee.com/author/brian-contos/ || @BrianContos

[1] http://www.gartner.com/it/page.jsp?id=1467313
[2] http://www.cedmag.com/article-detail.cfm?id=10926254
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] http://www.scribd.com/doc/54161974/Wired-Workforce-Networked-CSR-Final
[9] http://www.mcafee.com/us/resources/data-sheets/ds-host-data-loss-prevention.pdf

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com