



Don't Let Your Sensitive Information Leak onto Social Networks

Guard Against Information Leakage with Zgate 2.0

Contents

Abstract.....	3
Social Networks.....	4
The Achilles Heel.....	4
Protect Your Data with Zgate.....	5
Filtering criteria.....	6
Analysis of file attachments.....	6
Social Networking.....	6
Content Analysis.....	6
Message Handling.....	6
Summary.....	7

Abstract

Social networking has quickly exploded from a nascent concept aimed primarily at teen computer users, to an effective means of growing and maintaining relationships with like-minded individuals, to a communications platform, and even to a business-critical tool to build partner relationships, market products and services, provide support, and foster customer loyalty.

Social networking has quickly forced its way from the living room to the boardroom, catching many IT administrators off guard and forcing them to implement policies and procedures to govern social networking in the workplace. Unfortunately, social networking is also rife with security and privacy issues which pose a challenge for organizations trying to balance the benefits of social networking with the risks it can pose to network and data security.

This white paper will discuss the risks and concerns of information leakage via social networking that IT administrators need to be aware of. Finally, we will talk about the need to guard sensitive information from being leaked via social networks or email--whether intentional or inadvertent--and how you can provide simple, cost-effective solutions for your customers.

Social Networks

Social networks have existed to some extent since the advent of the PC. Bulletin boards and Usenet newsgroups from the early days of the Internet were basically online forums for users with similar interests to share and debate information.

The social networking services of today are much more advanced. Sites like MySpace, LinkedIn, Facebook, and Twitter provide the technology backbone for users to connect with friends, family, co-workers, and others and share information, pictures, Web links, video clips, and more.

Some social network services--such as LinkedIn--have a more narrowly defined scope. LinkedIn is specifically for fostering and maintaining professional relationships. It is a place to connect with current or past co-workers, partners, and other business professionals. Leveraging the concept of six degrees of separation, LinkedIn allows users to leverage their own social network to seek information and opportunities from a friend of a friend of a friend--greatly expanding the potential pool of talent and sphere of influence.

Social networking has taken the Internet by storm. Facebook has nearly half a billion members from around the globe. Twitter, while much smaller in membership than Facebook, is the other leading social networking service. Its short, 140-character maximum status updates which can be posted from the Web, as well as through SMS text messages from any mobile phone have established Twitter as a go-to source of breaking information. During the chaos that followed the national elections in Iran, Twitter remained as virtually the only reliable source of current events.

The Achilles Heel

Social networking can be an effective tool for communication. Used properly, it allows individuals and organizations to stay engaged with a large number of people simultaneously. A status update is instantly shared with hundreds, or even thousands of members connected to your social network.

That is great when letting friends and family know that you enjoyed Iron Man 2, or when sharing that the new restaurant you tried was not really worth the money or the wait, however, it also poses a risk that sensitive information can be leaked with much greater speed and efficiency as well. A user might send a Social Security number to another user, and accidentally broadcast it to the whole social network instead.

A recent study from Consumer Reports titled [Social Insecurity](#) revealed some enlightening statistics about the risks associated with social networking. Some of the key findings include:

- An estimated 5.4 million online consumers submitted personal information to email (phishing) scammers during the past two years.
- Among adult social network users, 38 percent had posted their full birth date, including year. Forty-five percent of those with children had posted their children's photos. And 8 percent had posted their own street address.
- An estimated 5.1 million online households had experienced some type of abuse on a social network in the past year, including malware infections, scams, and harassment.

Granted, Consumer Reports is, by definition, a consumer-focused resource, however consumers are also employees which means they apply these same practices and principles at work. While some of these behaviors will only affect the individual, many could also have implications with data protection compliance mandates, or pose a security risk to the organization.

A study from Compuware found that less than one percent of data loss incidents reported over the past year were the result of an external attack or compromise. That means that 99 percent were caused by internal users--either intentionally or inadvertently. Social networking makes the risk of data leakage even higher.

Protect Your Data with Zgate

Most IT administrators have no way to know if confidential or sensitive information is being leaked. IT departments lack the tools to properly protect sensitive data, or to ensure that employees can not share it across the Internet via social networking or email. IT administrators also have no way to easily monitor network traffic and proactively intercept and block dangerous communications.

Until now, tools designed to protect data and fight information leakage have been limited to complex, rules-based applications that are cumbersome to implement and maintain, and add an undue burden to IT administrators who already have too much on their plate.

The answer to this enormous challenge is Zgate. Zgate minimizes the risk of confidential data or sensitive information being leaked through email or social networking--whether intentionally or inadvertently, and provides forensic details to investigate security incidents.

Zgate is the gatekeeper for your network. Zgate monitors and controls email and social networking communications at the network perimeter. It analyzes the contents and file attachments of outbound communications to ensure that sensitive or confidential information is not leaked. It can also be combined with external 3rd party modules to provide anti-spam and anti-malware protection as a seamless solution.

Zecurion is committed to protecting corporate data and guarding against information leaks. With Zgate, IT departments are able to automate the process and proactively prevent sensitive and confidential information from leaving the network. The software minimizes the risk of data leakage, while also providing valuable forensic data to facilitate investigation into incidents or data breaches.

Filtering criteria

The Zgate communications module allows the flexibility of customizing the filtering criteria using all of the available message fields (sender, recipient, subject, etc.), including text messages and file attachments. The user-friendly, email server filter facilitates the building of complex filter conditions and nesting with the use of logical operations (AND, OR, NOT, etc).

Analysis of file attachments

The analysis module analyzes all file attachments to determine the attachment type for more than 70 of the most common applications - Microsoft Office, OpenOffice, Adobe, AutoCAD, etc... The files are evaluated, not by their extension, which is easily changed by renaming the file, but by the internal structure of a file and the available text component.

Social Networking

Zgate social network analysis module monitors Facebook status updates, Twitter tweets, and other social networking communications to ensure employees are not sharing inappropriate or confidential information. It analyzes the message traffic to detect Social Security numbers, drivers' license numbers, birth dates, and other commonly considered sensitive information, as well as any data identified by custom rules, to prevent leaks.

Content Analysis

Zgate also contains an embedded linguistic analysis module that performs full morphological analysis allowing it to check for all forms of a given word, as well as stemming, which enables the finding of word roots allowing the analysis to disregard word endings. This process works to verify the presence or absence of words in text messages and file attachments. For example, you can create a rule prohibiting the forwarding to any external email address, emails with file attachments which also contain the word «confidential». The linguistic analysis module supports English, German, French, Italian and Russian languages.

Message Handling

After the analysis is performed by the system, the message can be passed through to the email server or social network, blocked, placed in quarantine for subsequent manual processing or placed in the archives. The system also enables the adding of text to the beginning or end of the message, deleting of attachments, and adding, deleting or changing the recipient's address.

Summary

Zecurion's solutions are successfully protecting the internal assets and intellectual property for more than 5,000 companies worldwide. Zgate, Zlock and Zserver® Suite (patent pending) have been recognized with numerous awards for technology and security protection in United States as well as internationally. Most recently, Zecurion has been recognized for innovation of its products and awarded the Critical Security Solution mark by the Risk and Network (Rant) forum in UK. (<http://www.channelweb.co.uk/crn/news/2261261/overseas-duo-scoop-help-uk>).

Zecurion is led by an executive team experienced in developing security software and deployment across the enterprise. With over 10-years of experience in developing encryption-based security solutions, Zecurion allows IT departments to efficiently protect corporate information from internal threats, as well as from loss or theft of backup storage media.

As your organization embraces the operational, marketing, and public relations benefits of social networking you will need tools to help protect intellectual property assets, or sensitive information from being leaked. Zecurion offers you a comprehensive solution to minimize the risk of your data being leaked or compromised. Zecurion Zgate provides an effective, intuitive, and cost-effective solution for monitoring outbound communications and ensuring that sensitive information stays inside the network where it belongs.

Zecurion has embraced social networking as well. You can engage with Zecurion through our [Twitter account](#), [Facebook page](#), or [LinkedIn Group](#).