Policy Management

Policy — The Foundation to Business Security

White Paper

WatchGuard® Technologies, Inc.
Published: August 2011

Next-Generation Security for Businesses

Technology growth has not only opened doors of opportunity, but has also mandated that effective IT policies be created, implemented and managed intelligently and proactively. The importance of effective security for businesses can't be understated. The networks you're being asked to set-up, maintain and secure are becoming increasingly complex every day; couple this with the amount of security-related information generated by network devices, and the amount of data under your control. With this overwhelming amount of data in your hands, how do you ensure proper network defense and actionable incident responses?

In other words, how do you effectively reduce risk? It comes down to one word… "POLICY". A comprehensive acceptable use policy (AUP) should allow your company to monitor activities on a granular level as well as to plan for anything that could potentially happen in the future. This is the foundation to business security.

As businesses are dealing with the dynamically changing attack platforms —the Internet, they must stay ahead and must define, enforce and audit the right AUP strategy that provides a clear understanding of the technologies and methods that can be adopted. This white paper addresses the basic AUP businesses should have in place for their social media needs to stay ahead of threats.

The Web and How it Changes the Security Landscape

The growth of the Internet along with the increasing use of Web 2.0 applications has changed the way we do business and communicate. Businesses today rely heavily on information technology to do business, which has also moved crime to the Internet. Cyber-crime and the influx of malware have increased. As workers find new and creative ways to use the web, organizations struggle to maintain control of the corporate network while empowering employees, partners, and other stakeholders with access to critical functionality. Managing Web 2.0 is now a priority.

> ***"Organizations are actively leveraging the power of social networks to find new business opportunities, new groups of like-minded individuals and companies, and new sources of industry specific wisdom, advice and expertise."***
> ***(Wilson, 2009)***

As collaboration increases and employees use the increasing number of tools available to them, the right security becomes a necessity. Both email and the web are essential tools that enable employees to do their jobs efficiently and expediently. However, many of the tools being used were never designed for business so it is imperative that companies implement security designed with today's environment in mind.

Growth of Social Media

Web 2.0 proved to be a game-changer for business network security. It is part of the new "culture of participation" where users access online tools to communicate, share information, download and upload files, collaborate on projects, play games, and more. The Web 2.0 universe encompasses well-known sites such as YouTube, Facebook, Skype, Twitter, Hulu, Gmail, Hotmail, and Yahoo Messenger, but it also includes hundreds of lesser known web applications – some designed purely for malicious purposes.

The expansion of online technology has brought about easy ways for businesses to collaborate and have a major impact on their customers. In particular, social media has presented inexpensive ways for businesses, especially for small to mid-size businesses, to cost-effectively maintain an online presence. However, according to a May 2011 article in The Money Times "Sales, Growth, and Social Media," more often than not, businesses use social media with all-out, full-bore emphasis on product or price. But that's not what social media is about; that's not how social media works. Relationships in social media allow and build upon personal, emotional connection. They are not built on product, price, and the like. In fact, impersonal promotions of products or services on social media don't bring in positive results.

Personal info is easily harvested these days from blogs, social networking sites such as Facebook and Twitter, or from a business's web site itself. It's as uncomplicated as searching for blog postings about buying certain products, monitoring LinkedIn for people who work for a particular organization, or capturing the names of friends on Facebook pages. One report revealed that 324 spear phishing attacks against 88 employees of the same company appeared to come from their senior executive email addresses – addresses most likely gleaned from professional networking sites.

Zeus Botnet Targeting Macy's, Nordstrom account holders, SC Magazine, December 09, 2010

To secure today's corporate environments and take back control, administrators need to identify and determine whether applications are being used for legitimate business, are malware, or fall into the gray area. In the latter case, IT professionals need the ability to control who can access certain applications and for what purposes. Web 2.0 applications such as streaming media and audio can consume large amounts of expensive corporate bandwidth. Plus, corporations in regulated industries may need to restrict the usage of Instant Messaging because they cannot comply with requirements for electronic message retention. As part of a security and regulatory compliance posture, a corporate acceptable use policy, or a combination of the two, organizations must control employee use of the full range of applications.

Michael Stelzner in his post "How to Use Twitter to Grow Your Business," quotes Tony Hsieh, CEO of Zappos.com, as saying: "We've found that Twitter has been a great way for us to connect on a more personal level with our employees and customers.

"We use it to help build our brand, not drive direct sales. It'd be like asking how does providing a telephone number for customer service translate into new business when they are mostly non-sales-related calls.

"In the long term, Twitter helps drive repeat customers and word of mouth, but we're not looking to it as a way of driving immediate sales."

Social media campaigns should be tailored to meet different business goals, from generating new sales leads to expanding your customer base to sourcing ideas for new product development. These should be defined in your policy.

More than Just ON or OFF

Having the fine-grained application control you need means that your policy tools allow you to capture the nuances of roles and responsibilities within the company. Simple ON and OFF switches are too limiting. The goal is to deploy and maintain application control security policies so that workflow is never impeded by global caveats, while threats are never allowed into the network because a door is left open. The key to this kind of AUP management is thoughtful granularity and that's what differentiates WatchGuard Application Control.

Take Facebook, for example. Out of all the social networking sites on the Internet today, Facebook is the most popular.[1] Is there a business value in allowing Facebook? Most likely, if your business has a presence on Facebook, your marketing people would need access to keep it up to date. Does the finance department need to access Facebook? Probably not, though it could be part of your corporate culture to freely or partially allow access. With WatchGuard Application Control, a few clicks of the mouse allows you to create a policy that permits marketing to have Facebook access anytime, other employees to have access only before 9 a.m. and after 4 p.m., while disallowing access to Facebook games entirely to protect bandwidth and productivity.

Risks of Social Media to Businesses

You have a fundamental weak link in your security architecture – human interactions. Users want to trust other users. They're enticed by ads, inclined to share data, misled by scams, prone to click links and download file attachments. Behind each of these actions lies a potential threat to business security. A considerable part of your security policy management moving forward needs to focus on mitigating human behavior, yet do so without impeding critical business workflow.

This is why organizations need to address social media activities. One highly effective way to reduce your security risk is to block all access with Web 2.0 applications, but this is unrealistic. Therefore, AUPs need to be developed and implemented pertaining to application access. These can be networking programs, web applications, or just general types of businesses applications such as Microsoft Excel or Adobe Acrobat.

Today it is common for businesses to use social media vehicles throughout the organization. Many have a presence on Twitter and Facebook so blocking these is not an option. As the use of the web has increased dramatically, there has shown to be an uncontrolled environment that allows the spread of inappropriate content and even bullying within the workplace. Organizations today appear to have their corporate email systems under control, now it is time for all the social media tools.

Industry data and research shows that users increasingly use Web 2.0 tools. For example:

- In April 2010, 110 billion minutes were spent on social networking sites with the average visitor spending more than two-thirds more time than the previous year
- In April 2010, blogs and social networking sites attracted 24-percent more online users compared to the previous year

[1] http://social-networking-websites-review.toptenreviews.com/

Not only can the use of these non-business applications create havoc in the network due to malware infections and the like, employees posting on corporate Twitter and Facebook pages can expose sensitive information or post objectionable comments, which can wreak havoc on the company in other ways, such as:

- Negative PR
- Brand erosion
- Loss of consumer confidence
- Loss of business partner confidence
- Regulatory fines
- Stock market loss
- Legal fees
- Implementation of internal processes

Organizations must fully understand how social media technologies can be used within their environment and need to implement and enforce AUP. But the question remains, how do you create and develop an effective AUP?

Why an Acceptable Use Policy is Necessary

Employee productivity can be hampered and your business could be in danger with uncontrolled access to the Internet. Your IT security policy defines your business relationship to the Internet – what is allowed in, what can go out, who can access files, etc. These policies are so fundamental to business continuity in the digital age that they must be considered a top priority and take into account all business functions within an organization.

As business has evolved both email and web have become essential tools to empower employees to do their jobs effectively and efficiently. However, along with this also comes abuse. Therefore, businesses without a social media policy framework are subject to greater risks, including hacks, phishing attempts, sensitive data loss, etc.

According to a recently published white paper, three main reasons are stated for why a business needs an acceptable use policy for email and Web. All three of these areas impact an organization and its employees.

1. Sales working environment
2. Employee productivity
3. Internet security

Defining a, “strong AUP” is no trivial task. With the onslaught of threats in corporate environments, it is important to understand the nature of these threats and how to protect your business now and moving forward.

Companies are no stranger to AUPs. Employers have issued guidelines to their staff regarding the acceptable use of corporate telephones; email use and other codes of conduct. Most companies adopt a pragmatic approach and permit reasonable personal use of their telephones. Others have issued a clear edict that no personal use is permitted whatsoever. With the increased use of email and web at the workplace, these guidelines are frequently extended to all areas of information technology, eventually becoming an AUP.

These AUP policies were among the first drivers for content-orientated features in email security solutions, enabling organizations to uniformly and technically enforce these policies. These email security solutions can be used to train user behavior by alerting the user that a recent action was outside of the organization's AUP. Frequent abusers come to the attention of IT security and human resources staff, where disciplinary actions can be taken. These content features are now being used to enforce other policies such as regulatory compliance and corporate governance policies across email the web. Some organizations also have a "Business Conduct Guidelines" policy, for which the Internet-use AUP should follow.

Some basic filters that can be employed as part of an AUP include:

- Inappropriate language filters
- Inappropriate image analysis
- Dangerous file types
- Inappropriate web sites
- Overuse of non-work-related web browsing activity
- Overuse of non-work-related email

Creating and Developing an AUP

Most businesses today need to limit access to non-work related web sites to keep employees not only productive, but safe. As no two businesses are created equal, each business needs to build a customized AUP that reduces an organization's attack surface and is in line with its ideals and standards.

Where to begin can be the toughest issue of all. The minimum points to consider are:

1. Allow limited personnel use of web and email
2. Outline what is acceptable and what is not, while preserving company culture
3. Be consistent with enforcement and setting precedents
4. Identify all email with a name or email address; avoid spoofing
5. Inform staff on copyright issues relating to email or Internet documents
6. Inform staff about what is acceptable inside business hours and what is acceptable outside of business hours, if there is any difference (clearly state in policy)
7. Reserve the right to monitor all messages/files on the company network

A well-drafted and implemented Acceptable Use Policy (AUP) will educate its employees about protecting business assets and will explain security measures that will be carried out to enforce the policy. The goal of the AUP will accomplish two important objectives:

1. Maintain employees' high productivity levels, and;
2. Keep a company's computer systems safe from hackers and malware.

When designing an AUP, it is important for a company to seek input from all the key stakeholders within the organization. As with any project that a company may take on, collaboration between departments is vital to obtaining all the information necessary to generate a positive outcome including monitoring and enforcing of the AUP. Quite often departments and employees who are integral to the success of a company are overlooked during the development phase of an AUP. A study conducted by Forrester Research Group suggests that 40 percent of businesses have an application policy that was formulated wholly within IT, without the necessary input of other departments such as Human Resources, Legal Counsel, and Finance.

> ***"Two-thirds of web sites are easily compromised to install infector code, and there are 25 million web sites out there and users only go to about 100 sites per day, our web security gateway blocks at best 50% of attempts to get to malicious sites and even though users are trained not to click on suspicious stuff, 3 times out of 4 they do."***
>
> ***John Pescatore, VP Distinguished Analyst, Gartner Research***

How To Create an AUP for Social Media

It is well known that without rules chaos abounds. This is very true with the use of Web 2.0 applications, many of which were not created for business use. Today, with the explosion of Facebook, Twitter, LinkedIn and many more applications, businesses have established norms of protocol, regulation and digital behavior rules as online technology has brought about easy ways for businesses to collaborate and have a major impact on their customers.

Most companies already have some type of AUP in place, but how to make it "social media proof" is now the concern. In general, an AUP outlines the types of web sites a user may or may not visit. For example, an AUP may put a ban on social media sites such as Facebook.

If your company has an AUP and needs to add a policy that governs Web 2.0 application use, you do not want to start by blocking applications immediately. It is probably best to start with logging and reporting of application use. Work with stakeholders in your organization to develop a policy that clearly states your company's goals. If your company already has a policy in place, you might want to look at options to make the policy more granular and specific. Make sure you have a clear understanding of the applications that are used in the organization before you set up any rules that block traffic.

For example, consider these questions:

1. Is there a broad policy in place that now needs to get more specific?
2. Does the business need to limit application use by time of day, or specific business group?

Typically, these rules are very focused and explicit and are established for the Internet, Web and email within an organization. In fact, many security measures are designed to detect communications that ignore protocol—the most obvious indication that someone isn't playing by the rules. Internally,

***According to the Nielsen Company, the global average time spent per person on social networking sites is now nearly five and half hours per month (February 2010 data), with Facebook accounting for the majority of that time. In arriving at that conclusion, Nielsen measured social network usage per person across 10 countries and compared that to data from the same time last year. Results for 2011 from January's Facebook Statistics, Stats & Facts For 2011, Facebook has over 500 million users and is now used by 1 in every 13 people on earth, with over 250 million of them (over 50%) logging in every day making Facebook** *the* **number-one social network destination worldwide. Today, Facebook use accounts for nearly six hours (5:52:00) per person with the average user logging in more than 19 times per month. What does this mean for your business? With this many users and the time spent just on Facebook alone, an AUP is necessary as web traffic and web applications are the* source of so many security risks.**

organizational expectations, in the form of AUP are communicated and enforced; a sort of "if you use our network, you do things our way" document. Of course, without a means to enforce the rules, they don't mean much.

In addition to organizational and global network use policies, there are industry-specific and general compliance mandates and legislation. In order to protect privacy and control access to sensitive information, strict standards have been adopted for Web and email communications.

Social Media Risk Management Policy

As mentioned previously Social Media brings its own set of risks so the purpose of a Social Media Risk Policy is to outline the risks associated with employees using Social Media when interacting on behalf of the company. And, as mentioned previously, you must have a way to enforce the policy. This is usually outlined and is subject to disciplinary action, and can even lead to termination.

A key issue that has risen with the use of Social Media in the workplace is time spent on the activity. With people spending more than five and half hours per month on social networking sites, it is imperative that the AUP addresses time management of those involved. Today, there is a gray area of where an employee's personal social media habits overlap into their professional world.

When creating the AUP for Social Media, the benefits and communication dos and don'ts all need to be addressed.

Top Four Criteria that Must be Addressed

According to Social Media Policy Templates that are available for general consumption, the top four things that should be addressed when creating a Social Media Policy are:

1. **Benefits** - Identify the benefits and risks of engaging in a particular Social Media activity. Benefits include reaching a target audience, promotion, engaging with colleagues from related professions, raising the profile.
2. **Risks** – Identify risks such as underestimating the time, commitment or responsibility needed to make effective use of Social Media.

3. **Strategy** - Identify benefits to the organization and/or ways in which Social Media supports the business plan and/or strategic goals.
4. **Time** - Discuss the time commitment needed for Social Media activity.

The benefits of using social media within a business can be very positive, but only if employees are educated and support business objectives and strategic goals. When a new employee joins the team it is important that they are aware of the company's policies when it comes to the use of the Internet and the ideals and standards of the business. The employee needs to be aware of the risk associated with certain Web 2.0 applications from a security standpoint as well as potential loss in productivity. When an employee chooses to work for a company, they become a representation of what the company stands for. HR needs to be sure that every employee understand that abuse of social media can result in the effects pervious listed. Communication is key! Employees must be clear about what subjects should not be discussed online, including:

- Confidential information
- Financial details
- Internal Disputes
- Legal proceedings
- Personal information
- Rumors

In other words, any comments, file-sharing or information exchanges which could undermine the credibility of our organization. All employees, especially in marketing need to understand that all comments made via Social Media is public.

Risks

Social Media opens the door to potential viruses allowing these to enter the organizational network. While Social Media (and email) provide the possible entry for viruses, these risks are usually due to the lack of employee understanding of risky behavior.

These technical risks can be reduced if employees:

- Understand what can be downloaded from the Internet. For example, screensavers are notorious for transmitting viruses.
- Avoid discussing nondisclosure of business-related content
- Avoid discussing workplace-related topics
- Avoid visiting inappropriate sites
- Avoid personal use outside the workplace, for example, sharing confidential information over the internet.

Why are Acceptable Use Policies so Hard to Create and Implement?

Most companies use a compilation of different tools made by different companies to control and monitor different parts of their Acceptable Use Policy. Therefore, companies have a lot of systems to learn, maintain, upgrade, and replace. Not only does it take a lot of know-how to piece everything together, but there is a huge cost involved. There are no economies of scale when you're running multiple systems from different companies. There's no volume discount. Piecemeal lets you spread costs over time, but the costs are always higher than buying a complete unit. And, when you're running a lot of different systems how can a company stay on top of what is actually going on? One way is to buy YET ANOTHER system, one that aggregates views and logs and data into a cool dashboard that you can show in your NOC. Companies that do have policies are often relying on a rat's nest of different systems to make that policy operational.

How WatchGuard Makes AUP Creation Easy

An "all in one solution" isn't typical for companies implementing an AUP, but this is one way in which WatchGuard stands out from its competitors. The WatchGuard Solution eliminates the hurdles, costs, and confusion that companies have to deal with all too often. WatchGuard Application Control tightens security across your extended network and adds productivity safeguards that go straight to the corporate bottom line:

- The WatchGuard VPN Tunnel only requires dragging one device onto the other, clicking "Next" three times, and just like that, you have a secure tunnel between two sites, with a strong encrypted connection from one trusted network to the other.
- Our Policy Manager Tool lets you build your configuration anywhere, anytime, connected or not.
- When you need to know what's going on RIGHT NOW, there's not a company in the world with better real-time monitoring of a firewall product than we have.
- We see reporting as one "tense" of a continuous policy that spans past, present, and future. It's part of the package. So is our centralized logging and our multi-box management. -- Take advantage of real-time and historical visibility into what's being accessed on your network to report on application usage. Use the information to demonstrate compliance, evaluate employee need, and refine acceptable use policies.
- Sophisticated Behavioral Analysis works overtime, regardless of destination address or L7 protocol, to ensure applications that exhibit certain patterns of behavior don't escape the gaze of Application Control — including encrypted applications that are specifically designed to bypass ordinary security measures.
- Exercise fine-grained control over more than 1,800 applications, organized by category. Application Control lets you drill down from application category ("P2P") to application name ("Facebook") and down to application function ("Facebook Chat").
- Real-time reporting and monitoring are included. That means no additional software to buy in order to have complete visibility into network activity.
- Application Control makes it simple to selectively allow, block, or restrict access to applications based on a user's department, job function, and time of day, and generate reports on usage.

Conclusion

There is a lot to take into consideration when creating an AUP, and making sure your policy is "Social Media Proof" is a relatively new, but important aspect in maintaining a successful and technologically progressive business. So, what does it really mean to have a Future, Present and Past Policy in place? With the WatchGuard Solution your company can now focus more on what is important. It can put its energies into making better widgets or delivering better services so you can make more money and beat your competition. Using the right tools to define your relationship to the Internet gives you that opportunity.