Best Practices in Email, Web and Social Media Security

An Osterman Research White Paper

Published January 2014

SPONSORED BY

Trustwave
EXECUTIVE SUMMARY

Email, web and social media tools are pervasive in the vast majority of organizations. For example, Osterman Research has found that the typical information worker spends 153 minutes per day working in email and 51 minutes in social media – 42.5 percent of a typical eight-hour workday – not to mention the various work-related and personal use of the web that takes place on a daily basis.

Consequently, security for all of these tools must be of paramount concern for decision makers because of the substantial opportunity that they represent for ingress of malware and other threats. For example, our research found that during just the last 12 months:

- 74 percent of organizations have been infiltrated with malware through Web surfing.
- 64 percent have experienced malware infiltration through email.
- 22 percent have experienced an accidental or malicious leak of sensitive or confidential data through email.
- 14 percent of organizations have had malware enter the corporate network through social media or other Web 2.0 apps.

Decision makers are concerned about a range of issues related to the security of their networks in the context of how email, web applications and social media are used. As a result, security for all of the venues through which threats could enter into or data could leak from an organization must be addressed as an issue of the utmost importance.

ABOUT THIS WHITE PAPER

This white paper discusses the results of a survey conducted by Osterman Research during mid-November 2013. The survey was conducted only with security-focused decision makers and influencers on the Osterman Research survey panel. A total of 157 surveys were completed across a range of industries. The median number of employees at the organizations surveyed was 1,470 and the median number of email users was 1,000.

This white paper also provides an overview of the security solutions offered by Trustwave, the sponsor of this paper. Information on the company and its relevant solutions is provided at the end of the paper.

THE STATUS QUO OF SECURITY NEEDS IMPROVEMENT

THERE IS CONCERN OVER A RANGE OF ISSUES

Osterman Research discovered a range of issues about which decision makers and influencers are quite concerned. For example, as shown in Figure 1, one-half or more of these decision makers are highly concerned about malware that can be introduced into the corporate network through employees’ web surfing or their use of personal webmail, various types of phishing attacks, and data loss through email. In addition, there are a large number of email, web and social media security issues about which decision makers are very concerned.
Figure 1
Concerns About Various Security issues
% Responding a Serious or Very Serious Concern

<table>
<thead>
<tr>
<th>Issue</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware being introduced from employees’ web surfing</td>
<td>58%</td>
</tr>
<tr>
<td>Malware being introduced from employees’ personal webmail</td>
<td>56%</td>
</tr>
<tr>
<td>Phishing attacks</td>
<td>53%</td>
</tr>
<tr>
<td>Data loss from employees sending confidential info via email</td>
<td>50%</td>
</tr>
<tr>
<td>Data loss from employees sending confidential info via cloud-based tools like Dropbox</td>
<td>48%</td>
</tr>
<tr>
<td>Malware being introduced from employees’ home computers</td>
<td>42%</td>
</tr>
<tr>
<td>Virus/worm/malware infections</td>
<td>42%</td>
</tr>
<tr>
<td>Malware being introduced from employees’ use of Web 2.0 apps</td>
<td>37%</td>
</tr>
<tr>
<td>Breaches of sensitive internal data</td>
<td>36%</td>
</tr>
<tr>
<td>Breaches of sensitive customer data</td>
<td>35%</td>
</tr>
<tr>
<td>The lag between new virus outbreaks and when our AV vendor issues an update to deal with these outbreaks</td>
<td>34%</td>
</tr>
<tr>
<td>Mobile malware</td>
<td>33%</td>
</tr>
<tr>
<td>Direct hacker attacks</td>
<td>32%</td>
</tr>
<tr>
<td>Users working at home creating security problems</td>
<td>30%</td>
</tr>
<tr>
<td>Data loss from employees sending confidential info via social media</td>
<td>30%</td>
</tr>
<tr>
<td>Spam – the amount that your organization receives</td>
<td>29%</td>
</tr>
<tr>
<td>Spam - your IP address getting blacklisted due to outbound mail attack</td>
<td>27%</td>
</tr>
<tr>
<td>Time spent by email administrators dealing with malware</td>
<td>25%</td>
</tr>
<tr>
<td>Denial-of-service attacks</td>
<td>25%</td>
</tr>
<tr>
<td>Employees viewing inappropriate content on the web</td>
<td>25%</td>
</tr>
<tr>
<td>Time spent by email administrators dealing with spam</td>
<td>23%</td>
</tr>
<tr>
<td>Spam – the amount of false positives caused by your anti-spam system</td>
<td>21%</td>
</tr>
<tr>
<td>Time spent by employees dealing with spam</td>
<td>21%</td>
</tr>
</tbody>
</table>

INfiltrATION AND LEAKS ARE COMMON

Our research also discovered that malware infiltration and data leaks are quite common. For example, as shown in Figure 2, nearly three in four organizations have had malware infiltration through web surfing, nearly two-thirds have experienced a malware infection through email and more than one in five have lost sensitive or confidential data through an email-based leak – all within just the last 12 months.

In our surveys, Osterman Research has asked about security infiltrations for many years – with most of this research focused on mid-sized and large organizations – and have discovered that the web has been growing as a threat vector for the past several years, as shown in Figure 3 for the period 2007 through 2013. While we have seen period decreases in the threat level for various types of infiltrations, we are seeing continued growth in the number and severity of web-based threats.

It is also important to note that if organizations lack the capability to identify a successful security compromise, decision makers will likely never know that a particular event took place. Consequently, while decision makers have accurately acknowledged the security compromises of which they are aware, those about which they are not aware pose a much larger issue.
Clearly, the goal of any security solution is to remediate the variety of web, email, social media and other threats that can infiltrate networks, steal data, create financial losses, etc. While many organizations report that the security of various spam, malware and web security solutions are improving over time, most organizations report that their security problems are either remaining static or are actually getting worse, as shown in Figure 4.
Moreover, there remains significant room for reducing the false positive ratio generated by anti-spam systems. Clearly, even a fraction of a percentage of false positives can lead to a large number of valid messages being misclassified and unavailable for their intended business purpose. While false positives generated by anti-spam solutions are not considered "sexy" by many decision makers, the false positive problem is an enormous one that must be addressed.

For example, Osterman Research has found that the typical user receives a median of 80 emails per day. If we assume a 260-day workyear for the typical employee, each employee will receive 20,800 emails per year. An organization of 750 employees will receive 15.6 million emails annually. Based on an industry average false positive rate of 0.15% per year, that means that 23,400 valid emails each year will be falsely identified as spam and placed into quarantine or deleted. This creates two problems:

- Users must spend time searching through the spam quarantine for the mischaracterized valid emails in order to ensure that business-critical content, such as client inquiries or purchase orders, are not missed. This not only wastes employee time, but valid emails can still be missed.

- When employees search through the quarantine, they may mistakenly tag some emails as valid when, in fact, they are not. This can allow phishing emails, malware and other threats to be reintroduced back into the email system.

**SOCIAL MEDIA USE AND SECURITY**

**WHAT IS A “LEGITIMATE” SOCIAL MEDIA APPLICATION?**

The growth of social media in organizations worldwide has been phenomenal. For example, Osterman Research has found that the typical information worker employs work-related social media for 51 minutes on a typical workday – still well behind email at 153 minutes per day – but growing at a significant pace. Moreover, as shown in Figure 5, there are a significant number of social media tools that decision makers and influences consider to be "legitimate" for use in a business context.
The use of social media creates a serious conundrum for many organizations. For example, while 62 percent of organizations consider Facebook to be a legitimate application, 42 percent consider it to be risky or extremely risky for use on the corporate network. Moreover, as shown in Figure 6, less than one-third of organizations believe that they are “very well protected” against malware and other exploits that might enter through social media.

Figure 5
Perceived Legitimacy of Leading Social Media Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Legitimate</th>
<th>Not Legitimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn</td>
<td>82%</td>
<td>18%</td>
</tr>
<tr>
<td>YouTube</td>
<td>62%</td>
<td>38%</td>
</tr>
<tr>
<td>Facebook</td>
<td>62%</td>
<td>38%</td>
</tr>
<tr>
<td>Skype</td>
<td>60%</td>
<td>40%</td>
</tr>
<tr>
<td>Twitter</td>
<td>51%</td>
<td>49%</td>
</tr>
</tbody>
</table>

Figure 6
Perceived Protection Against Social Media-Borne Malware and Other Exploits

- Very well protected: 28%
- Reasonably well protected: 61%
- Not well protected at all: 9%
- Not sure: 2%
WHAT IS BEING DONE ABOUT SOCIAL MEDIA SECURITY?
In organizations that do not allow the use of specific social media services, those services currently viewed as "hot" or "trendy" are more likely to be actively blocked than passively not allowed. This includes social media tools like Facebook, Twitter and Skype. Services that used to be trendy have the opposite dynamic – they are more likely to be disallowed rather than actively blocked. Figure 7 shows what actions organizations take for various types of leading social media tools.

DEALING WITH THREATS
The number, variety and severity of various email, web and social media threats continues to grow over time. Perhaps the most notable recent event was the breach of 110 million records from a major US retailer’s credit and debit accounts as a result of malware in the company point-of-sale system, but that represents only the tip of the iceberg with regard to various types of threats that organizations can encounter.

The following provides a brief overview of some of the key threat vectors that organizations should consider:

• **Spam**
  Spam is perhaps the least “interesting” of the various email threats that face organizations, in large part because the spam proportion of all email has dropped since late 2010. However, spam continues to represent most of the email that organizations receive – for example, Trustwave found that 60.8 percent of all email was spam for the week ending December 22, 2013. This is significantly less than the 80-90 percent levels that most organizations experience prior to late 2010, but the number of unwanted emails that consume bandwidth and storage continues to be enormous.

• **Mobile platforms**
  The rapidly increasing use of smartphones and tablets is increasingly being exploited by criminals. For example, customers of a major financial services firm have been targeted with a man-in-the-middle attack (a variant of Zeus) that will install malware designed to intercept passcodes sent to BlackBerry and Symbian

---

©2014 Osterman Research, Inc.
devices via SMS as part of a two-factor authentication scheme. Moreover, the first malware that targeted the Google Android OS was discovered in August 2010, but Webroot found that 12 percent of all Android apps today are malicious. Add to this the fact that 79 percent of the top 50 iOS and Android apps "are associated with risky behavior or privacy issues". Android-focused malware, which represents the bulk of new malware variants, grew by 680,000 samples during the third quarter of 2013, an increase of one-third from the previous quarter.

- **Website threats**
  There are a variety of methods for malware to enter an organization through web surfing or the use of web-based applications. For example:

  - Cross-Site Request Forgery (CSRF) attacks innocent-looking websites to generate requests to various sites. CSRF attacks have exploited vulnerabilities in Twitter, enabling site owners to acquire the Twitter profiles of their visitors. Because Web 2.0 applications often leverage XML, XPath, JavaScript and JSON, Adobe Flash and other feature-rich internet applications, those applications are frequently vulnerable to injection attacks using these environments. These technologies can be used to evade anti-virus defenses.

  - A cross-component attack occurs when two innocuous pieces of malware code appear on the same web page – separately, they are harmless and difficult to detect, but when they appear simultaneously on a single page they can infect a user's machine with malware.

  - SQL injection attacks take place when SQL commands and meta-characters are inserted into input fields on a website, the goal of which is to execute back-end SQL code.

  - Cross-site scripting attacks embed tags in URLs – when users click on these links, malicious JavaScript code can be executed on their machines.

Another website threat is the "drive-by" download that occurs when a user visits a Web site and malware is automatically downloaded to his or her platform. In some cases, a user will visit a website and see a pop-up window – when they click the "OK" button in the popup, a Java applet, an ActiveX control, etc. will be installed on the user's computer without their consent.

A number legitimate websites have been hacked and have served up malware to unsuspecting visitors. This is a particularly serious problem for websites operated by smaller businesses – one source reported in mid-2013 that they are seeing approximately 30,000 new sites per day that are used to distribute malware.

- **Botnets**
  Botnets are responsible for a large number of successful hacking and phishing attacks against high-profile targets. For example, Citigroup, the US Senate, the International Monetary Fund, Sony, Northrup Grumman, Lockheed Martin and RSA have all been victims of botnet attacks. The consequence has been that millions of records have been exposed that will result not only in the disclosure of personal and sensitive information, but also lawsuits and other expensive remedial actions.

- **The “deperimeterized” network**
  Users working away from the corporate network, such as those working from home or in another remote site, are another source of threats. An unprotected user using a corporate asset, such as Outlook Web Access that is not accessed via a VPN, or a laptop computer that becomes infected and later is connected to the corporate network, can constitute a serious threat. This is becoming a serious problem for most organizations as users employ consumer devices like...
their personal smartphones, iPads and other traditionally consumer devices in a workplace setting.

- **User mistakes**
  Users can sometimes inadvertently install malware or compromised code on their platforms. This occurs when they download codecs, install ActiveX controls or install various applications that are intended to address some perceived need (such as a capability that IT does not support or that a user feels they must have when working from home), or when they respond to scareware and fake antivirus (rogue AV or fake AV) software. Rogue AV is a particularly dangerous type of malware, largely because it preys on users who are attempting to do the right thing – to protect their computers from viruses and other malware. Even users who are fairly experienced can be fooled by a well-crafted Rogue AV message.

- **Compromised search engine queries**
  Search engine queries that are hijacked by cybercriminals are another method for to distribute malware. This method of attack relies on poisoning search queries, resulting in the display of malware-laden sites during web queries. Search engine poisoning is especially effective for timely and popular search terms, such as the latest celebrity gossip or news about natural disasters.

- **Direct attacks**
  Direct attacks by hackers can include a number of exploits, including hackers attacking a known vulnerability in a web browser, or exploiting an older version of a browser or ActiveX control. This is a particularly serious problem for teleworkers who might employ a home computer or other personal platform that might not be updated as regularly as their work platform.

### MOVING FORWARD TO BETTER SECURITY

#### THE COST OF SECURITY

The total cost of ownership (TCO) for a security solution can vary widely based on a number of factors, including:

- The initial acquisition cost of the hardware, software or cloud service.
- The cost of IT labor required to manage the system on an ongoing basis.
- Software licensing and maintenance costs.
- The cost of any hardware that is required to run the software.
- The ability to re-use existing hardware.

Moreover, the differences in the cost between competing solutions will vary based on the various features and functions that each includes. It is important to evaluate both the TCO and the total cost of acquisition (TCA) for any security solution, since these can have significant impacts on the return-on-investment from that solution.

Our research found that security is not an inexpensive problem for organizations to address. For example, we found that the typical organization we surveyed invests 2,729 IT staff hours per year per 1,000 email users. If we assume a fully burdened annual salary for an IT staff member of $100,000, that translates to a cost of $131.22 per user per year, or $10.93 per user per month.

#### THE DISCONNECT BETWEEN CURRENT SOLUTIONS AND PREFERENCES

Our research also uncovered something of a disconnect between current security delivery models and preferences for these models, as shown in Figure 8. For example, we found that 35 percent of the organizations surveyed have on-premises, best-of-breed solutions in place, but only 16 percent actually cite this as their preferred security delivery approach. We also found that while only 14 percent use a
cloud-based and centrally managed security solution with a single interface, 24 percent actually prefer this model.

The reality for security today is that many organizations have emphasized product effectiveness criteria over simplicity. The majority has adopted multiple best-of-breed security solutions to ensure high levels of effectiveness, but this approach is not without its problems. Decision makers indicate a preference for reducing the internal complexity and overhead required when managing best-of-breed solutions, and would prefer to see an increased use of single-vendor or cloud-sourced approaches. The perceived incremental effectiveness of best-of-breed approaches is mitigating a wholesale migration to single-vendor, integrated solutions.

It is important to note, however, that the general trend seems to be moving back toward best-of-breed solutions and slightly away from centralized managed solutions. While we believe the latter will once again be the dominant choice for security management, the temporary movement back toward best-of-breed may reflect the growing number of endpoints that must be managed and the large number of point solutions currently available to address specific security requirements.

DEPLOYING WEB GATEWAYS
Our research found that decision makers and influencers have a number of important reasons for deploying a web security gateway, although preventing malware infiltration is among the leading reasons for deploying these solutions, as shown in Figure 9.
Figure 9
Reasons for Deploying a Web Security Gateway
% Responding Important or Very Important

<table>
<thead>
<tr>
<th>Issue</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>To block malicious sites</td>
<td>84%</td>
</tr>
<tr>
<td>To prevent viruses being introduced into the network</td>
<td>83%</td>
</tr>
<tr>
<td>To reduce the amount of malware entering the network</td>
<td>82%</td>
</tr>
<tr>
<td>To reduce the amount of malware that could steal data and prevent the loss of confidential data from an outbound post</td>
<td>74%</td>
</tr>
<tr>
<td>To block unwanted content like porn or gambling from entering</td>
<td>67%</td>
</tr>
<tr>
<td>To block unwanted employee downloads</td>
<td>58%</td>
</tr>
<tr>
<td>To improve employee behavior since they are monitored</td>
<td>51%</td>
</tr>
<tr>
<td>To comply with specific or general regulatory requirements</td>
<td>50%</td>
</tr>
<tr>
<td>To reduce growth in bandwidth requirements</td>
<td>47%</td>
</tr>
<tr>
<td>To log and report on user Web surfing behavior</td>
<td>45%</td>
</tr>
<tr>
<td>To reduce corporate liability for poor employee behavior</td>
<td>41%</td>
</tr>
<tr>
<td>To block employee use of personal Webmail</td>
<td>27%</td>
</tr>
</tbody>
</table>

APPROACHES TO SECURITY DELIVERY

Osterman Research has found that decision makers anticipate making less use of on-premises servers and appliances for anti-malware, anti-spam and web security capabilities, as shown in Figure 10-12. It is important to note, however, that on-premises solutions have largely remained the dominant method for deploying security, although over time more of these solutions will shift to the cloud.

The high risk of security issues arising to malware infections gives credence to the use of multiple protection strategies – what one approach does not catch a second (or third) might. Osterman Research believes there is sufficient room for a dual approach of a cloud-based anti-malware service, combined with either on-premise servers or an anti-malware appliance.

Figure 10
Delivery Models for Anti-Malware Capability
2012-2013
Organizations are making a faster transition to cloud-based services for anti-spam than for anti-malware. That represents a significant change in the anti-spam landscape and is reflective of the benefits of eliminating spam before it ever enters the corporate network. The move to the cloud for anti-spam capabilities that is well underway could deliver on the promise of delivering a clean and valid message stream into organizations.

Figure 11
Delivery Models for Anti-Spam Capability
2012-2013

The move to the cloud for anti-spam capabilities that is well underway could deliver on the promise of delivering a clean and valid message stream into organizations.
KEY ISSUES TO CONSIDER

APPRECIATING THE RISKS

An important step in approaching best practices for security, and for IT practices in general, is to understand the risks that an organization faces. Many decision makers underappreciate these risks simply because they are too busy, they lack sufficient budget or they have not focused intently enough on the growing number of risks they face. For example, corporate decision makers may permit the unfettered use of social media without fully appreciating the risks inherent in dangerous activities like clicking on shortened URLs in Twitter or mistakenly “friending” dangerous accounts in Facebook.

While every organization has limitations in its IT resources, that simply will not be an adequate excuse not to identify key risks. Moreover, once decision makers have identified those risks, they can prioritize them and assess their current level of preparedness to face them. Identifying key projects and initiatives through various technologies, user education/training and improved policy development is an important exercise.

Decision makers face a number of risks from their employees’ use of email, web and social media platforms:

- Employees may use these tools inappropriately, such as sending sexual harassing emails, text messages, tweets, etc.

- Users can inadvertently send content that violates data breach laws, such as sending sensitive content without encryption, resulting in significant penalties, notification requirements, sanctions and other consequences.

- Organizations that allow personally-owned devices to be used for accessing corporate email, files and other content must be managed to ensure compliance with legal and regulatory obligations, as well as with various best practices to ensure that confidential or sensitive data is not intercepted by unauthorized parties.

- Not adequately protecting all of the platforms from which employees work – such as personally owned laptops, smartphones or tablets – can result in malware infiltrating the corporate network. This is a growing problem as bring-your-own-device (BYOD) and bring-your-own-application (BYOA) practices increasingly take hold in most organizations.

- Not controlling the use of personally deployed applications like Dropbox can dramatically increase security-related risks on a number of levels, such as malware infiltration or data leaks.

The lack of DLP, encryption, monitoring, archiving or other capabilities can allow users to inadvertently violate corporate policies more easily. Consequently, it is critical for senior management to understand these risks before deciding on a course of action for implementing new security solutions or delivery models.

DEFINING WHERE SECURITY SHOULD TAKE PLACE

A key issue for senior managers to determine is whether or not internal management of email, web and social media security, as well as other part of the IT infrastructure, is a core competency that is central to the success of the organization. Key questions that decision makers must answer are these:

- Will managing security using on-premises infrastructure that is managed by in-house IT staff contribute more to the bottom line than using a cloud-based provider?

- Will security be improved if solutions remain on-premises?
• Should a hybrid security approach using both on-premises and cloud-based solutions be employed? If so, for which systems?

Many organizations are considering cloud delivery for various types of security services because of their sometimes lower cost, the more predictable nature of cloud service costs when compared to on-premises infrastructure, the ability to free internal IT staff for other tasks, and the advantage of blocking spam, malware, phishing emails and other unwanted content before it can reach the corporate network. Moreover, use of a hybrid security architecture enables much of this unwanted content to be eliminated in the cloud, while leaving CPU-intensive, deeper content inspection for on-premises systems.

ESTABLISHING POLICIES
Most organizations have not yet established detailed and thorough policies for the various types of email, web and social media tools they either have deployed or allow to be used. As a result, we recommend that the first step for any organization should be the development of detailed policies that are focused on all of the email, web and social media tools that are or probably will be used. These policies should focus on legal, regulatory and other obligations to:

• Monitor communications, blogs, social media posts, etc. for malware
• Encrypt content if it contains sensitive or confidential information
• Manage the use of personally owned devices that access corporate resources

Establishing policies will help decision makers not only to determine how and why each tool is being used, but it also will help to determine which capabilities can or cannot be migrated to cloud-based security solutions and which should be retained in-house. For example, if an organization determines that its policy for content retention is influenced by regulatory obligations to retain data only in certain jurisdictions, this will help determine if cloud-based archiving services can be used and, if so, which provider(s) should be used. While archiving is not an ostensibly security-related issue, security and archiving are key policy-focused decisions that should be made together.

UNDERSTANDING COSTS AND OPPORTUNITY COSTS
A key requirement in accurately evaluating whether or not to use cloud-based security solutions is for decision makers to understand the true TCO of managing the current, on-premise infrastructure. Over the years, Osterman Research has found consistently that many decision makers do not fully understand these costs and are not confident in their estimates. If decision makers do not understand accurately what it costs their organization to provide a particular service to their users, this leads to poorly informed decision-making and an inability to determine the potential cost savings and the return-on-investment from competing security solutions.

SUMMARY
Security is the most important focus area for business and IT decision makers in the context of their email, web and security solutions. Because of the significant potential for malware and other threats to impact organizations as they enter through corporate email systems, web applications, and social media tools – and the enormous potential for financial and other damage they can cause – decision makers must focus heavily on the specific solutions that will be employed, whether these solutions will be part of an integrated suite of solutions or implemented on a best-of-breed basis, and the models that will be used to deliver them.
SPONSOR OF THIS WHITE PAPER

Trustwave helps businesses fight cybercrime, protect data and reduce security risks. Trustwave content security solutions help businesses safeguard themselves against malware, targeted attacks and blended threats, while at the same time improving control over sensitive data and enhancing user productivity.

Content security solutions available from Trustwave include its Secure Web Gateway, which is available on-premise and as a managed security service, its Secure Email Gateway, available on-premise or through the cloud, and its Data Loss Prevention technology.

For more information about Trustwave, visit www.trustwave.com.