Global Information Assurance Certification Paper

The Security Implications of Web Based Email
GSEC Practical Assignment Version 1.2e
Eric Trombold
July 22, 2001

Introduction

Services like Hotmail, Yahoo mail and Excite mail offer free, web based, email accessible from anywhere on the Internet.

According to a survey of 538 IT security professionals by the Computer Security Institute and the Washington D.C FBI Computer Intrusion Squad, 91 percent of the respondents reported incidents of employee abuse of Internet privileges in 2001. That is up from 79 percent in 2000. (1)

Unauthorized use of web based email services, is a component of the increasing abuse of Internet privileges, mentioned in the survey.

The use of web based email poses security challenges that every organization should consider. In most cases, the risk of allowing users to access web based email while at work will outweigh any potential benefit. Without realizing it, users are bypassing many of the information security measures of an organization by using web based email accounts.

In this paper I will discuss four areas of risk posed by the unrestricted use of web based email services and ways to manage that risk.

The Virus Threat

The most important security threat posed by the unrestricted use of web based email is the email borne computer virus.

In June 2001 one out of every 1000 emails was infected with a computer virus. That's according to Messagelabs Ltd, a U.K. based anti-virus firm. (1) This statistic illustrates that email is still the most prevalent infection mechanism for computer viruses today.

In a well protected environment, anti-virus software should be maintained at multiple levels. This is called "Defense in Depth" or layered security.

Layered Security is defined as follows:

> Layered security is a practice that combines several different security components, such as anti-virus software, firewalls and vulnerability assessment tools, to create a comprehensive and defensive barrier many times stronger than its individual parts alone. (2)

A layered security approach, as it applies to anti-virus (AV) defense, consists of AV

software installed in the following places on the network; firewall, Simple Mail Transfer Protocol (SMTP) gateway, email server, file server and user workstation.

Email traffic that progresses normally through an organization's system is scanned for viruses at the SMTP gateway and the email server before reaching the email client.

SMTP gateway virus scanning products examine email attachments for viruses before they are allowed to enter the email system. If a virus is found in a message, the email can be quarantined, striped of attachments and sent or deleted.

After passing through the SMTP gateway scanner, messages are scanned a second time by the mail server virus protection software before being transmitted to the end user's email client application.

When a user opens an infected email attachment on a web based mail system it bypasses the protection at the SMTP gateway and the mail server. This leaves only the AV software at the firewall and user workstation to prevent infection.

Assuming the virus defense is well-maintained with daily pattern file updates either of the last two lines of defense will filter out the virus. If either the AV pattern is out of date or the virus is new, then a costly infection can result.

The potential weakness in AV protection created by web based email should be considered when formulating a security policy which addresses access to web based email services from machines attached to the organization's network.

Maintaining a centralized, layered anti-virus defense which automatically updates AV pattern files will go a long way towards mitigating the risk of infection posed by the use of web based email. However, web based email access can cause an infection even in a system with a well designed AV defense. This may be reason enough for an organization to restrict its use.

The Threat to Email Content Filtering

The unauthorized emailing of proprietary information, is one of the most substantial threats to an organization. SMTP content filtering is used to prevent accidental or intentional proprietary information leakage. Content filtering products can also prevent sexist, racist or otherwise offensive email messages from entering an organization's computer system.

"In September of 2000, Dow Chemical fired 24 employees for allegedly storing or sending sexual or violent images on the companies computers." (3) This incident illustrates why many organizations are compelled to install email content filtering systems.

Email content filtering products such as GFI's Mail Essentials (www.gfi.com) look for

key words in messages that should not leave or enter the organization's system. If an email contains a key word it is quarantined for review.

Web based email circumvents an organization's content filtering systems because the email messages do not pass through the organization's SMTP gateway. Content filtering software is typically installed on the SMTP gateway system, where it scans all incoming or outgoing email messages looking for matches to the keyword list.

Web based email is a potential threat to the effectiveness of content filtering systems. If an organization is going to employ a content filter, the use of web based email should be restricted.

The Threat to Encryption Systems

Many organizations use encryption in conjunction with email to ensure the integrity of their confidential information. Most encryption systems are not set up to work with web based email clients.

Encryption is most effective when it is used to protect all sensitive email. The encryption policy should spell out for users which types of email must be encrypted.

With the exception of Hushmail, (www.hushmail.com) most web based email services do not include encryption.

It's a cumbersome process for users to encrypt their text before sending it, via web based email. If an organization is planning to allow its users to send encrypted email via a web based service, end user training needs to be developed to teach users to do it properly.

Security Lapses at Web Based Email Systems

Judging by the number of serious incidents over the years, security has been a low priority to web based email providers.

In August of 1999, a security hole in Hotmail exposed user's accounts to access without passwords. (4)

Hotmail has had a series of security problems over the years. Each of these incidents potentially compromised the security of thousands of accounts. Since 1999 Hotmail has made an effort to improve its authentication process.

In addition to security problems, Hotmail has had problems keeping downtime to a minimum, as have many of the other free email services. (5) If the information stored in the service is critical then the amount of downtime a service experiences is an important consideration. For these reasons, users should be prohibited from using web based email to store or send sensitive organizational information.

The Importance of an Effective Security Policy

An organization's security policy should spell out whether or not employees are allowed to use the corporate network to access personal email.

When formulating a security policy, keep in mind that it should be clear, concise, easy to read and understand. If the policy doesn't meet these goals, the policy is of no value because users won't have a clear idea of what is expected of them.

An example of a clear policy statement on web based email is as follows:

> Users of <organization>'s information system agree to not use personal web based email accounts while at work. Examples of web based email systems are: Hotmail, Yahoo mail, and Zdnet mail.

Some organizations may choose to implement a policy that permits occasional use of web based email. In this case, such a policy becomes difficult to enforce unless acceptable use is spelled out clearly. An occasional use policy might read as follows:

> Users of <organization>'s information system agree to not use personal web based email accounts while at work, except for occasional or incidental use. Occasional or incidental use is defined as not more than one access per week.

The policy should spell out the consequences of non-compliance, and how employee usage of web based email will be monitored.

In government agencies, work done on a taxpayer owned computer may be considered a public record. The public record implications of using web based email on taxpayer owned equipment should be clearly spelled out in the policy.

Most importantly, a security policy is only effective when all of the employees have read and understood it. The policy should be distributed in conjunction with an over all security awareness plan. The security awareness plan should include training so that users know what risks are being addressed by the policy.

Countermeasures to Prevent the Use of Web Based Email

If an organization decides to block access to web based email, countermeasures can be implemented by making network configuration changes. Bear in mind, countermeasures are never 100 percent effective. Therefore, they should only be implemented in conjunction with a written policy.

A firewall or filtering router's access list can be modified to block access to web based email servers. Care should be taken to identify an accurate list of web based email server IP addresses.

It's not advisable to prevent access to the entire block of IP addresses owned by a web based email provider. This will also prevent access to the other services made available by that provider. For example, in the case of Yahoo, preventing access to their entire block of addresses would also block access to their search engine.

Compiling a complete list of server addresses for all web based email services is difficult. A determined user will find a way around this countermeasure.

Internet filtering and monitoring software such as Elron Internet Manager, (www.elronsw.com) can be set up to block access to web based email sites. Elron uses dictionaries of key words and blocks access to sites which contain those key words. In order to block access to Yahoo mail add the words "Yahoo mail" to the Internet filtering software's dictionary. However, use caution since it's easy to block sites users may need to access, such as Yahoo's search engine.

The best way to ensure compliance with a security policy that restricts the use of web based email is to monitor users Internet activity. Internet monitoring software such as Elron Internet Manager or Websense (www.websense.com) can be used to restrict access to web based email sites. The ramifications of a user visiting a restricted site should be clearly spelled out in a security policy.

Significant personnel hours are required to properly maintain Internet monitoring software. The ongoing cost of ownership of an Internet monitoring system should be considered before implementing monitoring.

None of these countermeasures are effective by themselves. They should be implemented in combination and in conjunction with a clearly worded security policy.

Conclusion

By thoroughly examining the impact of web based email organizations can make an informed decision about whether to allow users to access it.

For most organizations the potential problems web based email can cause outweigh the benefits of allowing users to have access to it.

By using a well written security policy and security awareness training for all employees the message can be delivered to users as to what is expected.

Countermeasures which make it more difficult for users to access web based email should be used to compliment the security policy.

Regular audits should be conducted to ensure that the security policy is being followed.

If an organization is going to spend the time and money to develop a highly secure email system, they should not allow users to circumvent the security by using web based email.

An ongoing discussion regarding the use of web based email should be a part of all information security programs.

References

(1) “Security Statistics”, Computerworld.com http://www.computerworld.com/itresources/rcstory/1,4167,STO62002_KEY73,00.html#Anchor-VIRUS-11481

(2) Wells, Mark and Thrower, Woody “The Importance of Layered Security”, Symantec http://enterprisesecurity.symantec.com/article.cfm?articleid=767

(3) Shankland, Stephen “Dow Chemical fires 24 in email controversy” Cnet News.com http://news.cnet.com/news/0-1007-200-2787458.html

(4) Wilcox, Joe “Hotmail hole exposes free email accounts” Cnet News.com http://news.cnet.com/news/0,10000,0-1005-200-346588,00.html

(5) Festa, Paul “Free email comes at a price” Cnet News.com http://news.cnet.com/news/0,10000,0-1005-200-339330,00.html

(6) Hazari, Dr. Sunil “Secure Online Behavior, Part II: Secure Email Behavior”, Security Focus.com http://www.securityfocus.com/focus/basics/articles/sechabits2.html

(7) Avolio, Fred and Piscitello, David “Email Security”, Information Security Magazine http://www.infosecuritymag.com/articles/may01/features_email_security.shtml

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event